An Image Encryption Algorithm Based on Compressive Sensing and M Sequence

YUQIANG DOU AND MING LI

Big Data Engineering Laboratory for Teaching Resources and Assessment of Education Quality of Henan Province, Henan Normal University, Xinxiang 453007, China
Corresponding author: Yuqiang Dou (douyuqiang@htu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62072159 and Grant U1804164, and in part by the Ph.D. Scientific Research Foundation of Henan Normal University under Grant qd18027.

ABSTRACT In this article, a new image encryption algorithm based on compressive sensing (CS) and M sequence is proposed to decrease the image communication load and improve the security of image communication in the internet of things. Most of the available image encryption schemes are based on chaotic systems to shuffle the image pixels. Before shuffling the image pixels, the random sequence, which is produced by a chaotic system, need to be sorted. This sorting operation is avoided by utilizing a modified linear feedback shift register (LFSR) state sequence. Then, the security of the proposed scheme is improved by combining CS with an improved 1D chaotic system, which is used to construct a measurement matrix. The computational complexity is reduced by the use of the improved 1D chaotic system. Simultaneously, the amount of image data is reduced. Simulation results and performance analyses demonstrate that the proposed encryption scheme can greatly reduce the amount of image data and has good security and robustness.

INDEX TERMS M sequence, compressive sensing, image encryption, improved 1D chaotic map.

I. INTRODUCTION

Image encryption is a critical issue for confidentiality and security. Chaotic maps have been widely used in image encryption owing to the characteristics of high sensitivity to initial conditions and control parameters in [1]–[4]. In the recent years, some other technologies have been combined with chaotic systems to encrypt images. For example, the sensitivity mechanism is built up by utilizing the information entropy of the plain-image in [5]. A novel image encryption algorithm is introduced based on the two-dimensional logistic map and the Latin square image cipher in [6]. An image encryption scheme combining chaos-memory cellular automata and weighted histogram is proposed in [7]. DNA computing in [8]–[11] is applied to chaos based image encryption system due to its several good characteristics, such as massive parallelism, huge storage and ultralow power consumption, etc. With the development of the internet of things, the amount of image data is constantly increasing and the images needs to be compressed. Hence, compressive sensing becomes a hotspot.

Compressive sensing (CS) is a novel sampling paradigm. The concept of CS was formally proposed by Candès and Donho in 2006 in [12], [13]. The theory of CS mainly includes three aspects: sparse representation, measurement matrix and signal reconstruction. Measurement matrix needs to satisfy Restricted isometry property (RIP) in [14] or the robust null space property (RNSP) in [15], [16]. As for measurement matrix it can be Gaussian, Bernoulli and Fourier in [17], or binary measurement matrix in [15]. As for reconstruction algorithms, by using $l_1$ norm minimization the original signal can be exactly recovered by solving a simple convex optimization problem through linear programming in [18], [19]. Some reconstruction techniques are based on $l_0$ norm minimization such as Matching Pursuit (MP) in [20], Orthogonal Matching Pursuit (OMP) in [21] and SL0 algorithm in [22]. A sparse recovery algorithm by utilizing the probability-based prior information is proposed in [23] for compressed sensing system.

Recently, it is necessary to compress and encrypt plain images simultaneously and many novel encryption schemes based on CS and chaotic systems have been proposed [24]–[34]. A novel digital image information encryption method based on CS and Arnold transformation is...
proposed in [25]. To further enhance the performance, the double random phase encoding (DRPE) optical encryption technique is utilized. An efficient image compression-encryption scheme based on Chen’s hyper-chaotic system and 2D compressive sensing is proposed in [26], in which the hyper-chaotic system is used to generate two measurement matrices. A novel encrypted compressive sensing of images based on fractional order hyper chaotic Chen system and DNA operation is proposed in [27] in which 4-Dimensional Fractional order hyper chaotic chen system is used to generate the measurement matrix. A game-of-life-based scrambling method (PDGSM) in [28] is introduced to shuffle the sparse coefficient matrix of the plain image, in which the respective permutation matrix is constructed by the rules of game of life.

In this encryption scheme, chaotic sequences are generated by adopting multi-dimensional chaotic maps. Owing to the complex structure and multiple parameters of the multi-dimensional chaotic maps, the difficulty of implementation and the computation complexity increase. On the contrary, 1D chaotic maps in [35]–[40] have the advantages that their structures are simple and they are easy to implement. In this article, an improved 1D chaotic map in [41] is used to construct the measurement matrix for compressed sensing.

Linear feedback shift register (LFSR) have been widely used in modern communication systems, coding theory and cryptography. The mathematical theory of M sequences is firstly described in [42]. A pseudo random n-order M sequence is the longest linear feedback of a shift register sequence of 2^n−1 length in which consecutive n-length strings exactly experience all binary n-length strings in [43]. To improve the linear complexity of LFSR sequences, nonlinear feedback shift register sequences (NLFSR) are presented such as [44], [45]. However, NLFSR sequences don’t experience all binary n-length strings only once.

M-sequences have attracted much attention due to their good randomness properties [46]–[49]. Based on the knowledge of finite fields, many research results about M-sequences have been obtained in [47], [48]. As for constructing M-sequences, some combinatorial algorithms are presented in [52]–[54]. Recently, the new construction method by the semi-prefer-XOR rule is proposed in [55]. In general, M sequence can be used in MIMO radar systems in [56], magneto-acoustic imaging in [57] and stream cipher in [58].

According to the above analyses, a novel image compression and encryption algorithm is introduced based on compressed sensing, M sequence and the improved 1D chaotic system. For the meantime, the computational complexity is reduced by the use of the improved 1D chaotic system.

Furthermore, the SHA-512 hash function value of the plain image is used to produce the control parameters of the improved 1D map and linear feedback shift register (LFSR) to increase the correlation of the proposed encryption scheme and the plain image.

This article is organized as follows. In Section II a brief introduction about compressive sensing is firstly given. Then, M sequence and the improved chaotic map are elaborated. The proposed image encryption scheme is explained in Section III. In Section IV, the experimental results and the performance of the proposed scheme are discussed. Finally, the conclusion is drawn in Section V.

II. PRELIMINARIES
A. M SEQUENCE
The logic expression is of n-order LFSR as the following

\[ a_n = C_1 a_{n−1} \oplus C_2 a_{n−2} \oplus C_3 a_{n−3} \oplus \cdots \oplus a_0 \]  

(1)

where \( \oplus \) represents module-2 sum. The flow is shown in Fig.1. Each register state will change as the clock triggers.

![FIGURE 1. n-order LFSR flow.](image)

Move \( a_n \) from the left to the right of Equation 1 and the following equation is obtained

\[ 0 = \sum_{i=0}^{n} C_i a_{n−i}. \]  

(2)

Define a polynomial of \( F(x) \) corresponding to Equation (3) as below

\[ F(x) = \sum_{i=0}^{n} C_i x^i \]  

(3)

which is called characteristic polynomial. If the characteristic polynomial is a primitive one, the pseudo random sequence generated by the LFSR will have a \( 2^n−1 \) length period and it will be called M sequence.
The polynomial $F(x)$ of degree $n$ is a primitive polynomial if
1. $F(x)$ is irreducible.
2. $F(x)$ is exactly divisible by $x^m + 1$ where $m = 2^n - 1$.
3. $F(x)$ cannot be divisible by $x^q + 1$ where $q < m$

The coefficients of $F(x)$ can be treated as a secret key. The LFSR state sequence can be noted as $S = (a_{n-1}a_{n-2}a_{n-3} \cdots a_0)$ where the period length of $S$ is $2^n - 1$. $S$ can also be treated as a secret key. Convert $S$ into a decimal number of $DS$ by Equation (4).

$$DS = a_{n-1} \times 2^{n-1} + a_{n-2} \times 2^{n-2} + a_{n-3} \times 2^{n-3} + \cdots + a_0 \quad (4)$$

$DS$ will experience all the integers from 1 to $2^n - 1$ and each value will be experienced only once in each cycle. The state transition table is shown in Table 1. As can be seen from Table 1, $DS$ will experience all the integers from 1 to 15 and each value will be experienced only once in each cycle.

| clock tick | $a_0$ | $a_1$ | $a_2$ | $a_3$ | $S$ | $DS$ |
|------------|-------|-------|-------|-------|-----|-----|
| 0          | 1     | 0     | 0     | 0     | 0   | 8   |
| 1          | 0     | 0     | 0     | 1     | 1   | 0   |
| 2          | 0     | 0     | 1     | 0     | 0   | 2   |
| 3          | 0     | 1     | 0     | 0     | 0   | 4   |
| 4          | 1     | 0     | 0     | 1     | 1   | 9   |
| 5          | 0     | 0     | 1     | 1     | 0   | 3   |
| 6          | 0     | 1     | 1     | 0     | 0   | 6   |
| 7          | 1     | 1     | 0     | 1     | 1   | 13  |
| 8          | 1     | 0     | 1     | 0     | 1   | 10  |
| 9          | 0     | 1     | 0     | 1     | 0   | 5   |
| 10         | 1     | 0     | 1     | 1     | 1   | 11  |
| 11         | 0     | 1     | 1     | 1     | 1   | 7   |
| 12         | 1     | 1     | 1     | 1     | 1   | 15  |
| 13         | 1     | 1     | 1     | 0     | 1   | 14  |
| 14         | 1     | 1     | 0     | 0     | 0   | 12  |
| 15         | 1     | 0     | 0     | 0     | 0   | 8   |

### B. COMPRESSION SENSING

If a signal of $s$ in $\mathbb{R}^N$ can be sparsely represented by an orthogonal basis in CS theory [12], which means its most weighting coefficients are zeros or close to zero, $s$ can be expressed as Equation 6

$$s = u^T \xi$$

(6)

where $\Psi$ is the orthogonal basis matrix and $\xi$ is the weighting coefficient vector in $\mathbb{R}^N$. The measurement result $y$ can be obtained by a measurement matrix $\Phi$ with size $M \times N$ as the following formula

$$y = \Phi \xi = \Theta \xi$$

(7)

This problem can be solved by the algorithms such as Matching Pursuit (MP) in [20], Orthogonal Matching Pursuit (OMP) in [21] and SLO algorithm in [22].

### C. IMPROVED 1D CHAOTIC MAP

1D chaotic maps have simple structures, so that they are widely used in image encryption such as Logistic, Sine and Chebyshev maps. To improve the chaotic performance of 1D chaotic maps the new chaotic map is introduced in [36] which is defined by the following equation

$$x_{n+1} = F_{\text{chaos}}(u, x_n) \times 2^k - \text{floor} \left( F_{\text{chaos}}(u, x_n) \times 2^k \right)$$

(9)

where $F_{\text{chaos}}(u, x_n)$ is one of 1D chaotic maps as Logistic map, Sine map and Chebyshev map. $x_n$ is the output chaotic sequence, which is acquired by iterating the new chaotic system $M \times 3N + N_0$ times and discarding the former $N_0$ elements. $u \in (0, 10]$ and $k \in [8, 20]$ are the control parameters. $x_0$ is the initial value. The parameters of $x_0$, $u$ and $k$ are utilized as the security keys.

- **Logistic-Logistic system (LLS)**

The logistic map, which is a simple dynamic nonlinear equation with complex chaotic behavior, is one of the famous 1D chaotic system. It can be expressed in the following equation

$$x_{n+1} = F_L(u, x_n) = u \times x_n \times (1 - x_n)$$

(10)

where $u$ is a control parameter with range of $u \in (0, 4]$. $x_0$ is the initial value of chaotic map, and $x_n$ is the output chaotic sequence. LLS is defined as

$$x_{n+1} = u \times x_n \times (1 - x_n) \times 2^k - \text{floor} \left( u \times x_n \times (1 - x_n) \times 2^k \right)$$

(11)

- **Sine-Sine system (SSS)**

The Sine map is one of 1D chaotic maps and has a similar chaotic behavior with the Logistic map. The definition can be described by the following equation.

$$x_{n+1} = F_S(r, x_n) = r \times \sin(\pi \times x_n)$$

(12)
where parameter $r \in (0, 1]$ and $x_n$ is the output chaotic sequence. SSS is defined as the following equation

$$x_{n+1} = r \times \sin (\pi \times x_n) \times 2^k - \text{floor} \left( r \times \sin (\pi \times x_n) \times 2^k \right)$$ (13)

- Chebyshev-Chebyshev system (CCS)
The Chebyshev map is also one of 1D chaotic systems and can be described by the following equation.

$$x_{n+1} = F_C (a, x_n) = \cos (a \times \arccos x_n)$$ (14)

where parameter $a \in N$. CCS is defined as

$$x_{n+1} = \cos (a \times \arccos x_n) \times 2^k - \text{floor} \left( \cos (a \times \arccos x_n) \times 2^k \right)$$ (15)

The dynamical analysis in [39] has shown that the improved 1D chaotic systems have excellent chaotic behaviors. For example, the bifurcation diagram and Lyapunov exponent of LLS are shown in Fig.2 and Fig.3, which indicate that The chaotic range of LLS is (0, 10) and is much larger than Logistic System.

![FIGURE 2. The bifurcation diagram of (a)Logistic map; (b)LLS.](image)

![FIGURE 3. The Lyapunov exponent of (a)Logistic map; (b)LLS.](image)

### III. PROPOSED IMAGE ENCRYPTION SCHEME

#### A. GENERATION OF THE INITIAL CONDITION OF THE IMPROVED 1D CHAOTIC MAP

SHA–512 hash function is used to generate the control parameters of the 1D improved map for establishing the relationship between the encryption scheme and the plain image. A sequence of hexadecimal value that consists of 512 bits is generated by the SHA–512 hash function. The 512-bit hash value of the plain image is divided into 8-bit blocks which can be converted to 64 decimal numbers: $h_1$, $h_2$, · · · , $h_{64}$. The corresponding initial values are computed via

$$x_0 = h_1 \otimes h_2 \otimes \cdots \otimes h_6 + 1$$

$$u = h_6 \otimes h_7 \otimes \cdots \otimes h_{10} \times 10 + t_2$$

$$k = \frac{h_{11} \otimes h_{12} \otimes \cdots \otimes h_{15}}{64} \times 3 + 8 + t_3$$ (16)

t_1, t_2 and t_3 are the external keys.

#### B. GENERATION OF THE INITIAL CONDITION OF LFSR

If LFSR is $n$-order, there should be the condition of $2^n - 1 \geq M \times N$ where $M \times N$ is the pixel number of the plain image. The initial state can be acquired by selecting $n$ bit binary values from 512 bit hash values.

#### C. PROCESS OF ENCRYPTION ALGORITHM

As shown in Fig. 4, the steps for the encryption algorithm can be described as follows.

- Step 1: The SHA-512 hash function of the plain image is generated and the secret keys are obtained according to Part A and Part B of section III.
- Step 2: The sparse coefficients matrix $\alpha$ is obtained by transform the plain image $I$ into discrete wavelet transform (DWT) domain of $\Psi$.
- Step 3: Convert $\alpha$ into the 1D image pixel matrix $P = \{p_1, p_2, \cdots, p_{M \times N}\}$ with length $M \times N$.
- Step 4: The $n$-order LFSR state sequence $DS$ is obtained by selecting a primitive polynomial of $F (x)$ according to the initial value. The permutation position sequence $T$ is obtained by Algorithm 1.

**Algorithm 1 Obtain the Permutation Sequence DS**

1: Input: Initial condition
2: set $k = 0$
3: for $i$ from 1 to $2^n-1$
4: \[ S (i) = (a_{n-1} a_{n-2} a_{n-3} \cdots a_0) ; \]
5: \[ DS (i) = a_{n-1} \times 2^{n-1} + a_{n-2} \times 2^{n-2} + a_{n-3} \times 2^{n-3} + \cdots + a_0 \]
6: \[ \text{if } DS(i) \leq M \times N \]
7: \[ T(k) = DS(i) ; \]
8: \[ k = k+1 ; \]
9: end
10: end

- Step 5: Obtain the permuted image pixel vector $P' = \{p'_1, p'_2, \cdots, p'_{M \times N}\}$ by the permutation position vector $T$ according to the following equation.

$$P' (i) = P(T (i)) .$$ (17)

- Step 6: Reshape $P'$ into Matrix $U$ with size $M \times N$. The measurement matrix $\Phi$ of size $M \times N$ is constructed by the improved chaotic sequence $X$ according to [39] with the initial condition of $(x_0, u, k)$. The measurement result $Y$ is acquired by

$$Y = \Phi U .$$ (18)
Step 7: Q is obtained by quantifying the elements of matrix Y into the range from 0 to 255 with the sigmoid function in [60].

Step 8: The diffusion matrix W is obtained by the following equation

\[ W(i) = \text{mod} \left( \text{floor} \left( X(i) \times 10^{14} \right), 256 \right) \].

(19)

Step 9: Reshape matrix Q into a sequence of Q’ and obtain the diffused sequence C by the following equations.

\[
\begin{align*}
C(1) &= \text{mod} \left( C(0) + Q'(1) + W(1), 256 \right) \\
C(i) &= \text{mod} \left( C(i-1) + Q'(i) + W(i), 256 \right)
\end{align*}
\]

(20)

Step 10 Reshape sequence C into matrix C’ with the same size of Y and C’ is the final encrypted image.

**D. PROCESS OF THE DECRYPTION ALGORITHM**

The decryption procedure is the reverse of encryption process. The flowchart of the decryption is shown in Fig. 5. The detailed process is as follows.

Step 1: Produce the chaotic sequence X according to [36] with the secret keys and obtain W according to X. Matrix Q is obtained by executing the inverse diffusion process.

Step 2: Y is obtained by executing the inverse quantization according to the inverse sigmoid function.

Step 3: Construct the measurement matrix \( \Phi \) and reconstruct the matrix \( U \) from Y by SL0 algorithm.

Step 4: Obtain the LFSR state sequence DS and acquire the permutation sequence T according to Algorithm 1.

Step 5: Obtain the sparse coefficient matrix \( \alpha \) and acquire the original plain image by inverse discrete wavelet transform (IDWT).

**IV. SIMULATIONS AND SECURITY ANALYSIS**

Simulation results and security analyses of the proposed encryption scheme are given out in this section. Eight grayscale images, including ‘Lena’, ‘Pepper’, ‘Baboon’, ‘Boat’, ‘man’, ‘Lake’, ‘Run’ and ‘Sat’, which are shown in Fig. 6,
A. ENCRYPTION RESULTS AND DECRYPTION RESULTS FOR DIFFERENT IMAGES

Five plain gray images are utilized as the test images including ‘Lena’, ‘Pepper’, ‘Baboon’, ‘Run’ and ‘Sat’.

The encrypted and corresponding decrypted results are illustrated in Figs. 7-11 where compression ratio is changing from 0.25 to 0.75. Compression ratio (CR) is the image volume ratio between compressed image and plain image which is computed according to the following equation

$$\text{CR} = \frac{h_c \times w_c}{h_I \times w_I}$$

where \(h_I\) and \(w_I\) denote the height and width of the original image and \(h_c\) and \(w_c\) are that of the cipher image.

According to Figs. 7-11, it is evident that the cipher images are unrecognizable and the image data amount is reduced according to CR. Compared to the original images, the decrypted images have preserved the main information of the original images and they become more similar when CR is increasing.

B. PSNR AND SSIM ANALYSIS

The quality of the reconstructed image is evaluated by the Peak Signal to Noise Ratio (PSNR) which is calculated by
TABLE 2. Comparison of PSNR of reconstructed image LENA for different measuring matrix.

| CR  | Ours   | Ref[29] | Ref[30] | Ref[34] | Ref[35] |
|-----|--------|---------|---------|---------|---------|
| 0.8 | 37.2572| 33.4860 | 31.3651 | 31.6379 | 33.4866 |
| 0.7 | 35.6192| 31.8573 | 29.8214 | 30.7185 | 33.2777 |
| 0.6 | 34.1511| 28.7145 | 29.1454 | 28.9124 | 32.1281 |
| 0.5 | 31.2584| 27.7421 | 29.4645 | 26.8721 | 32.3287 |
| 0.4 | 28.6378| 22.3143 | 28.7865 | 24.8567 | 30.2356 |
| 0.3 | 25.8823| 19.1271 | 27.5237 | 23.6130 | 27.6985 |
| Average | 32.1343| 27.2069 | 29.3511 | 27.7684 | 30.2809 |

FIGURE 9. Cipher images (a1)-(c1) of Baboon when CR = 0.25, 0.5 and 0.75; Decrypted images: (a2)-(c2) when CR = 0.25, 0.5 and 0.75;

FIGURE 10. Cipher images (a1)-(c1) of Baboon when CR = 0.25, 0.5 and 0.75; Decrypted images: (a2)-(c2) when CR = 0.25, 0.5 and 0.75;

FIGURE 11. Cipher images (a1)-(c1) of Baboon when CR = 0.25, 0.5 and 0.75; Decrypted images: (a2)-(c2) when CR = 0.25, 0.5 and 0.75;

The following formula

$$\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{\frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [X(i,j) - X'(i,j)]^2} \right)$$  \hspace{1cm} (22)

where $X(i,j)$ is the plain image and $X'(i,j)$ is the reconstructed image. The image of ‘Lena’ is used to verify our proposed encryption scheme. The PSNR values are listed in Table 2 with the different CR values. As can be seen from Table 2, the quality of the reconstructed image of the proposed scheme is better than the encryption schemes in [29], [30], [34], [35].

The Structural Similarity (SSIM) is used to evaluate the similarity of two images which is defined by

$$\text{SSIM} = \frac{(2\mu_X\mu_{X'} + C_1)(2\sigma_{XX'} + C_2)}{\mu_X^2 + \mu_{X'}^2 + C_1}\left( \frac{\sigma_{XX'}^2}{\sigma_X^2 + \sigma_{X'}^2 + C_2} \right)$$  \hspace{1cm} (23)

where $\mu_X$ and $\mu_{X'}$ represent the average values of the plain image $X$ and the reconstructed image $X'$. $\sigma_X$ and $\sigma_{X'}$ are the corresponding standard deviations. $\sigma_{XX'}$ is the cross-covariance of $X$ and $X'$. $C_1$ and $C_2$ are constants. The similarity between $X$ and $X'$ is higher when the SSIM value is higher. The images of ‘Baboon’, ‘Boat’, ‘Lake’, ‘man’, ‘Peppers’, ‘Run’ and ‘Sat’ are utilized to verify our proposed scheme. The SSIM values of our proposed scheme are higher than the schemes in [29], [30], [34], [35] according to Table 3.

C. HISTOGRAM ANALYSIS

Histogram graphically represents the distribution of the pixel values of an image. It is needed that the histogram of the encrypted image has a uniform distribution. Fig. 12 shows that the histograms of the plain images and the histograms...
TABLE 3. SSIM of different algorithms.

| Image  | Ours   | Ref.[29] | Ref.[30] | Ref.[34] | Ref.[35] |
|--------|--------|----------|----------|----------|----------|
| Baboon | 0.9841 | 0.5420   | 0.9823   | 0.4616   | 0.8774   |
| Boat   | 0.9875 | 0.5753   | 0.9961   | 0.4767   | 0.8224   |
| Lake   | 0.9912 | 0.5783   | 0.9965   | 0.4496   | 0.8201   |
| Man    | 0.9891 | 0.6049   | 0.9931   | 0.4654   | 0.8574   |
| Peppers| 0.9985 | 0.6427   | 0.9727   | 0.5242   | 0.8376   |
| Run    | 0.9986 | 0.9874   | 0.8451   | 0.6318   | 0.4841   |
| Sat    | 0.9824 | 0.9861   | 0.8493   | 0.6276   | 0.4979   |
| Average| 0.9902 | 0.9877   | 0.8442   | 0.6004   | 0.4799   |

FIGURE 12. a1-d1: histograms of four plain images; a2-d2: histograms of corresponding cipher images.

of their corresponding encrypted images are uniform. Hence, the proposed scheme is robust against statistical attacks.

D. PIXEL CORRELATION ANALYSIS

It is well-known that there are high correlations between the adjacent pixels, and a secure encryption algorithm should reduce the correlation to improve the ability of resistance to statistical attacks. The correlation coefficient is defined according to the following equation

$$\text{Cor}(x, y) = \frac{\sum_{i=1}^{M} (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{M} (x_i - E(x))^2 \sum_{i=1}^{M} (y_i - E(y))^2}}$$  \hspace{1cm} (24)

where $E(x) = \frac{1}{M} \sum_{j=1}^{M} x_j$, $E(y) = \frac{1}{M} \sum_{j=1}^{M} y_j$, $x$ and $y$ are gray values of the adjacent pixels in the images and $M$ is the total number randomly chosen from the test image.

The correlation diagram among adjacent pixels at horizontal, vertical and diagonal directions of the plain image of ‘Lena’ and the corresponding cipher image with CR equal to 0.5 are shown as in Fig.13. The size of cipher images are $128 \times 256$.

Table 4 shows the correlation coefficients of horizontally, vertically and diagonally of the plain images of ‘Baboon’, ‘Boat’, ‘Lake’, ‘man’, ‘Peppers’, ‘Run’ and ‘Sat’ and the corresponding cipher image with CR equal to 0.5. According to Table 4 the correlation coefficients of plain image are near 1 and those of the cipher images are almost equal to 0 which means the correlation between the adjacent pixels has been greatly reduced.

E. KEY SPACE ANALYSIS

The key space of an image encryption scheme, which can resist brute-force attacks, should be more than $2^{100}$ in [59]. In this article the secret keys of the proposed encryption algorithm mainly include: $x_0 \in (0, 1], u_1 \in (0, 10], k_1 \in [8, 20], S$ and the coefficient of $F(x)$. $S$ is generally larger than $2^{16}$. If the computational precision of the computer is $10^{-14}$, the key space is about $10^{14} \times 10^{14} \times 10 \times 2^{16} \times \lambda \approx \lambda 2^{112}$.

Hence, the key space of our method is large enough to resist all kinds of brute-force attacks.

F. KEY SENSITIVITY ANALYSIS

A good encryption scheme should be very sensitive to secret keys. The sensitivity can be evaluated by Number of pixel change rate (NPCCR) and unified average change intensity (UACI) which are defined by the
The image of ‘Lena’ is used to verify key sensitivity. After slightly changing the value of parameter $x_0$ from 0.5321 to 0.53210000000001 the obtained NPCR and UACI between the cipher images are 99.6570 and 33.3159. After slightly changing the value of parameter $x_0$ from 0.5321 to 0.53209999999999, the obtained NPCR and UACI between the cipher images are 99.6151 and 33.2703. After slightly changing the value of parameter $u_1$ from 5.43740000000001 to 5.43739999999999 the obtained NPCR and UACI between the cipher images are 99.5789 and 33.3727. After slightly changing the value of parameter $u_1$ from 5.43740000000001 to 5.43739999999999 the obtained NPCR and UACI between the cipher images are 99.5903 and 33.3532. The results show that the proposed encryption scheme is highly sensitive to a slight change of the secret keys.

**TABLE 4. Comparison of correlation coefficient with other schemes.**

| Test Image | Direction | Plain Image | Cipher Image  |
|------------|-----------|-------------|---------------|
|            |           | proposed    | Ref.[24] | Ref.[34] | Ref.[35] |
| Baboon     | Horizontal | 0.8857      | -0.0041 | 0.0074 | -0.0235 | 0.0003 |
|            | Vertical   | 0.8309      | -0.0021 | 0.0164 | 0.0234 | -0.0162 |
|            | Diagonal   | 0.7956      | 0.0006  | 0.0108 | -0.0193 | 0.0134 |
| Boat       | Horizontal | 0.9223      | 0.0051  | 0.0200 | 0.0264 | -0.0037 |
|            | Vertical   | 0.9440      | -0.0039 | 0.0030 | 0.0154 | -0.0177 |
|            | Diagonal   | 0.8742      | 0.0020  | -0.0443 | 0.0308 | -0.0131 |
| Lake       | Horizontal | 0.9587      | -0.0003 | 0.0146 | -0.0118 | -0.0005 |
|            | Vertical   | 0.9570      | 0.0037  | 0.0086 | -0.0199 | 0.0179 |
|            | Diagonal   | 0.9321      | 0.0029  | -0.0101 | 0.0005 | 0.0291 |
| Man        | Horizontal | 0.9455      | 0.0020  | -0.0038 | 0.0324 | 0.0072 |
|            | Vertical   | 0.9574      | -0.0033 | -0.0066 | 0.0137 | 0.0062 |
|            | Diagonal   | 0.9071      | 0.0001  | -0.0045 | -0.0152 | 0.0127 |
| Peppers    | Horizontal | 0.9636      | 0.0101  | 0.0233 | 0.0325 | 0.0001 |
|            | Vertical   | 0.9757      | -0.0053 | -0.0077 | -0.0192 | 0.0315 |
|            | Diagonal   | 0.9414      | -0.0068 | 0.0078 | 0.0133 | -0.0035 |
| Run        | Horizontal | 0.9833      | -0.0021 | -0.0056 | 0.0250 | 0.0012 |
|            | Vertical   | 0.9903      | 0.0027  | -0.0065 | -0.0081 | 0.0123 |
|            | Diagonal   | 0.9751      | -0.0012 | -0.0031 | 0.0107 | -0.0027 |
| Sat        | Horizontal | 0.9491      | 0.0015  | 0.0197 | 0.0530 | 0.0011 |
|            | Vertical   | 0.9242      | -0.0033 | -0.0053 | -0.0127 | 0.0281 |
|            | Diagonal   | 0.9099      | -0.0005 | 0.0069 | 0.0076 | -0.0024 |
| Average    | Horizontal | 0.9440      | 0.0017  | 0.0108 | 0.0191 | 0.0008 |
|            | Vertical   | 0.9399      | -0.0016 | 0.0011 | -0.0011 | 0.0089 |
|            | Diagonal   | 0.9051      | -0.0004 | -0.0046 | 0.0036 | 0.0042 |

Following formulas.

\[
\text{NPCR} = \left( \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| D(i, j) \right| \right) \times 100\%
\] (25)

\[
\text{UACI} = \left( \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|c_1(i, j) - c_2(i, j)|}{255} \right) \times 100\%
\] (26)

where

\[
D(i, j) = \begin{cases} 
0 & \text{if } c_1(i, j) = c_2(i, j) \\
1 & \text{if } c_1(i, j) \neq c_2(i, j)
\end{cases}
\]

and $c_1$ and $c_2$ are the encrypted images corresponding to two slightly different keys.
TABLE 5. Comparison of entropy with other schemes.

| Test Image | Entropy of Plain Image | Entropy of Cipher Image |
|------------|-----------------------|-------------------------|
|            | proposed              | Ref.[24]                | Ref.[34]                | Ref.[35]                |
| Baboon     | 7.2288                | 7.9964                  | 7.9938                  | 7.989                   | 7.9949                  |
| Boat       | 7.0565                | 7.9963                  | 7.9939                  | 7.9885                  | 7.9944                  |
| Lake       | 7.4584                | 7.9966                  | 7.9949                  | 7.989                   | 7.9939                  |
| Man        | 7.2883                | 7.9965                  | 7.9942                  | 7.9883                  | 7.9942                  |
| Peppers    | 7.57                  | 7.9958                  | 7.9938                  | 7.9887                  | 7.9931                  |
| Run        | 7.3893                | 7.9942                  | 7.9943                  | 7.9886                  | 7.9935                  |
| Sat        | 6.7329                | 7.9946                  | 7.9941                  | 7.9889                  | 7.9932                  |
| Average    | 7.3916                | 7.9958                  | 7.9941                  | 7.9887                  | 7.9939                  |

G. INFORMATION ENTROPY ANALYSIS

The information entropy formula is as the following

\[ H(x) = \sum_{i=1}^{v} p(x_i) \log_2(p(x_i)) \]  

(27)

where \( p(x_i) \) is the probability of a message of \( x_i \) and \( v \) is the number of the messages of the information source. For an image with 256 gray levels, \( v \) is equal to 256. Table 5 presents the information entropies of the plain images and cipher images (CR = 0.75). The last row gives out the average values of the information entropies of the plain images and cipher images. The information entropies of the corresponding cipher images are all more than 7.99 as shown in Table 5.

H. ROBUSTNESS ANALYSIS

Cipher images are easily influenced by noise and data loss during image transmission. A good image encryption scheme should be able to resist these attacks. The image of ‘milkdrop’ is used to test the ability of the proposed encryption scheme. At first, the image is encrypted by the proposed scheme and the encrypted image is shown as Fig.14 (a1) Then, Fig.14 (a1) is attacked by ‘salt&pepper’ noise whose intensity is 0.0001 and the result is shown as Fig.14 (b1). At last Fig.14 (a1) is cropped with data loss size of 64 × 64.
the cropped encrypted image is shown as Fig.14 (c1). The corresponding decrypted images are shown as Fig.14 (a2, b2, c2). As can be seen, they contain the main information of the original image when noise and crop attacks occur.

V. CONCLUSION
In this article the modified LFSR state sequence is utilized to shuffle the sparse coefficient matrix of the plain image and good permutation effect has been achieved. Then, the amount of image data is greatly reduced by the use of CS. For the meantime, CS is combined with the improved 1D chaotic system, by which the security of the proposed encryption scheme is improved. The improved 1D chaotic is used to construct the measurement matrix and the initial parameters are used as the secret keys. Simulation results demonstrate that the proposed encryption scheme can reduce the amount of image data and improve the security of image communication simultaneously. Performance analyses demonstrate that the proposed encryption scheme has a large key space and high sensitivity and good robustness to noise and data loss. For the meantime, our scheme can resist statistical attack and differential attack.

REFERENCES
[1] Y. Zhang, D. Xiao, Y. Shu, and J. Li, “A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations,” Signal Process., Image Commun., vol. 28, no. 3, pp. 292–300, Mar. 2013.
[2] Y. Zhang and D. Xiao, “Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform,” Opt. Lasers Eng., vol. 51, no. 4, pp. 472–480, Apr. 2013.
[3] G. Ye and K.-W. Wong, “An efficient chaotic image encryption algorithm based on a generalized Arnold map,” Nonlinear Dyn., vol. 69, no. 4, pp. 2079–2087, Sep. 2012.
[4] O. Mirzaei, M. Yaghoobi, and H. Irani, “A new image encryption method: Parallel sub-image encryption with hyper chaos,” Nonlinear Dyn., vol. 67, no. 1, pp. 557–566, Jan. 2012.
[5] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, “A chaotic image encryption algorithm based on information entropy,” Int. J. Bifurcation Chaos, vol. 28, no. 1, Jan. 2018, Art. no. 1850010.
[6] M. Machkour, A. Saaidi, and M. L. Bennaïti, “A novel image encryption algorithm based on the two-dimensional logistic map and the Latin square image cipher,” 3D Res., vol. 6, Oct. 2015, Art. no. 36.
[7] A. Souyah and K. M. Farah, “An image encryption scheme combining chaos-memory cellular automata and weighted histogram,” Nonlinear Dyn., vol. 86, no. 1, pp. 639–653, Oct. 2016.
[8] A. Jain and N. Rajpal, “A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps,” Multimedia Tools Appl., vol. 75, no. 10, pp. 5455–5472, May 2016.
[9] K. Zhan, D. Wei, J. Shi, and J. Yu, “Cross-utilizing hyperchaotic and DNA sequences for image encryption,” J. Electron. Imag., vol. 26, no. 1, Feb. 2017, Art. no. 013021.
[10] X. Huang and G. Ye, “An image encryption algorithm based on hyperchaos and DNA sequence,” Multimedia Tools Appl., vol. 72, no. 1, pp. 57–70, Sep. 2014.
[11] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, “Selective encryption for gray images based on chaos and DNA complementary rules,” Multimedia Tools Appl., vol. 74, no. 13, pp. 4655–4677, Jul. 2015.
[12] D. L. Donoho, “Compressed sensing,” IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.
[13] R. Baraniuk, “Compressive sensing [lecture notes],” IEEE Signal Process Mag., vol. 24, no. 4, pp. 118–121, Jul. 2007.
[14] E. J. Candès and T. Tao, “Near-optimal signal recovery from random projections: Universal encoding strategies?” IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.
[15] M. Lotfi and M. Vidyasagar, “A fast noniterative algorithm for compressive sensing using binary measurement matrices,” IEEE Trans. Signal Process., vol. 66, no. 15, pp. 4079–4089, Aug. 2018.
[16] M. Lotfi and M. Vidyasagar, “Compressed sensing using binary matrices of nearly optimal dimensions,” IEEE Trans. Signal Process., vol. 88, pp. 3008–3021, 2020.
[17] E. J. Candès, “The restricted isometry property and its implications for compressed sensing,” Comp. Rendus Mathematique, vol. 346, nos. 9–10, pp. 589–592, May 2008.
[18] S. Qaisar, R. M. Bilal, W. Iqbal, M. Maureen, and S. Lee, “Compressive sensing: From theory to applications, a survey,” J. Commun. Netw., vol. 15, no. 5, pp. 443–456, Oct. 2013.
[19] E. J. Candès and T. Tao, “Decoding by linear programming,” IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.
[20] S. Mallat and Z. Zhang, “Matching pursuits with time-frequency dictionaries,” IEEE Trans. Signal Process., vol. 41, no. 12, pp. 3397–3415, Dec. 1993.
