Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 6764052, 10 pages
https://doi.org/10.1155/2018/6764052

Research Article

Image Encryption Technique Combining Compressive Sensing with Double Random-Phase Encoding

Huiqing Huang [1,2] **and Shouzhi Yang** [1]

[1] *Department of Mathematics, Shantou University, Shantou, Guangdong 515063, China*
[2] *School of Mathematics, Jiaying University, Meizhou, Guangdong 514015, China*

Correspondence should be addressed to Shouzhi Yang; szyang@stu.edu.cn

Received 8 June 2017; Revised 9 September 2017; Accepted 22 January 2018; Published 3 April 2018

Academic Editor: Tomasz Kapitaniak

A new image compression-encryption method based on compressive sensing and double random-phase encoding is proposed, which can complete image compression and encryption simultaneously. We utilize the hyperchaotic system to generate a measurement matrix and two random-phase masks first. Then the original image is measured by measurement matrix to accomplish encryption and compression at the same time, next the compressed image is reencrypted by the double random-phase encoding technique with the two random-phase masks, and lastly the resulting image is confused and diffused by using hyperchaotic system simultaneously. Some numerical simulations verify the validity and the reliability of the proposed algorithm.

1. Introduction

With the development of network and communication technology, encryption technique becomes more and more important for the information security and network security. It is one of the most important methods in protecting network security, which can prevent the illegal easy stealing, distorts, duplicates, and spreads of sensitive information. In 1989, a typical image encryption method with advantages of good performance and high security was based on chaos theory which was proposed by Matthews [1]. Subsequently, all kinds of chaos-based image encryption techniques have been reported [2–7]. Guan et al. employed Arnold cat map and Chen's chaotic system to shuffle the positions and change the gray values of image pixels [3]. In [2], Chen et al. proposed a symmetric image encryption scheme based on 3D chaotic cat maps. Gao and Chen proposed a novel image encryption algorithm based on hyperchaos, which uses a new image total shuffling matrix to shuffle the pixel positions of the plain image and then the states combination of hyperchaos is used to change the gray values of the shuffled-image [6]. A chaos-based image encryption algorithm with variable control parameters is proposed [7].

The double random-phase encoding (DRPE) was first proposed in 1995 [8]; since then, many researchers have proposed and analyzed a lot of encryption algorithms based on DRPE [9–14]. In [9], Zhang and Karim proposed a new encryption technique to encrypt color images using existing optical encryption systems for gray-scale images. Subsequently, Unnikrishnan et al. proposed an optical architecture that encodes a primary image to stationary white noise by using two statistically independent random-phase codes, the encoding is done in the fractional Fourier domain, and the optical distribution in any two planes of a quadratic phase system is related by fractional Fourier transform of the appropriately scaled distribution in the two input planes [10]. After that, a lensless optical security system based on double random-phase encoding in the Fresnel domain was designed [11]. To enhance security further, a novel image encryption method is proposed by utilizing random-phase encoding in the fractional Fourier domain to encrypt two images into one encrypted image with stationary white distribution [12].

Recently, encryption methods [15–18] based on compressive sensing (CS) [19, 20] have been widely studied. Zhang et al. proposed a new color image encryption algorithm combining compressive sensing with Arnold transform, which

can encrypt the color image into a gray image [15]. In [16], an image information encryption method based on compressive sensing and double random-phase encoding is proposed. Lately, Zhou et al. proposed a novel image compression-encryption scheme by combining 2D compressive sensing with nonlinear fractional Mellin transform [17]. To overcome the low-security and reduce the possible transmission burden, an efficient image compression-encryption scheme based on hyperchaotic system and 2D compressive sensing is proposed [18].

In this paper, a new image encryption method based on CS and DRPE technique is proposed which can accomplish encryption and compression at the same time. In this scheme, the original image is measured by the measurement matrix first, where the measurement matrix is controlled by hyperchaotic system with initial conditions. And then the two random-phase masks generated by the hyperchaotic system performs DRPE with the compressed image. Lastly, the resulting image is confused and diffused by using hyperchaotic system simultaneously.

2. Preliminaries for Proposed Technique

In this section, some preliminaries about the CS theory and DRPE technique used in image encryption algorithm are introduced.

2.1. Compressive Sensing. CS is a new sample theory, which can reconstruct original signal by directly sampling a sparse or compressible signal at a rate much lower than the Nyquist rate. For a 1D signal x in R^N with length N could be represented as

$$x = \sum_{i=1}^{N} \alpha_i \Psi_i = \Psi\alpha \quad \text{or } \alpha = \Psi^T x, \tag{1}$$

where Ψ is the $N \times N$ matrix with $\{\Psi_i\}_{i=1}^N$ as columns and α_i is the coefficient sequence of signal x. Suppose that M measurements of x are taken through the following linear measurement:

$$y = \Phi x = \Phi\Psi\alpha, \tag{2}$$

where Φ is an $M \times N$ measurement matrix incoherent with basis matrix Ψ. In fact, the magic of CS is that Φ can be designed such that x can be recovered approximately form the measurements y when the matrix $\Phi\Psi$ satisfies the Restricted Isometry Property (RIP) [22].

To recover the signal x from y, it is required to solve the optimal problem below:

$$\begin{aligned} \min \quad & \|\alpha\|_0 \\ \text{s.t.} \quad & y = \Phi x. \end{aligned} \tag{3}$$

The problem above can be solved by greed iterative algorithm, one of the most commonly used algorithms is the orthogonal matching pursuit (OMP) method [23].

2.2. Double Random-Phase Encoding. In 1995, Refregier and Javidi proposed the DRPE technique [8]. The encoded image is obtained by random-phase encoding in both the input and the Fourier planes. If two random-phase masks are used to encrypt the image in the input and Fourier planes, respectively, the input image is transformed into a complex-amplitude stationary white noise.

Let $f(x, y)$ denote the image to be encoded and $g(x, y)$ denote the encoded image. $\phi(x, y)$ and $\varphi(u, v)$ stand for the key function in the spatial and frequency domain, respectively, and the values of which are distributed from 0 to 1 with uniform probability.

The encoding and decoding procedures are shown as follows:

$$\begin{aligned} g(x, y) &= \mathcal{F}^{-1}\{\mathcal{F}\{f(x, y)\exp[i2\pi\phi(x, y)]\} \\ &\quad \cdot \exp[i2\pi\varphi(u, v)]\}, \\ f(x, y) &= \mathcal{F}^{-1}\{\mathcal{F}\{g(x, y)\}\exp[-i2\pi\varphi(u, v)]\} \\ &\quad \cdot \exp[-i2\pi\phi(u, v)], \end{aligned} \tag{4}$$

where $\mathcal{F}$ and $\mathcal{F}^{-1}$ represent the 2D fast Fourier transformation and inverse 2D fast Fourier transformation, respectively.

2.3. Hyperchaotic System. In the proposed encryption scheme, a new hyperchaotic system generated from Gao et al.'s chaotic system is used in key scheming, which is defined by [24]

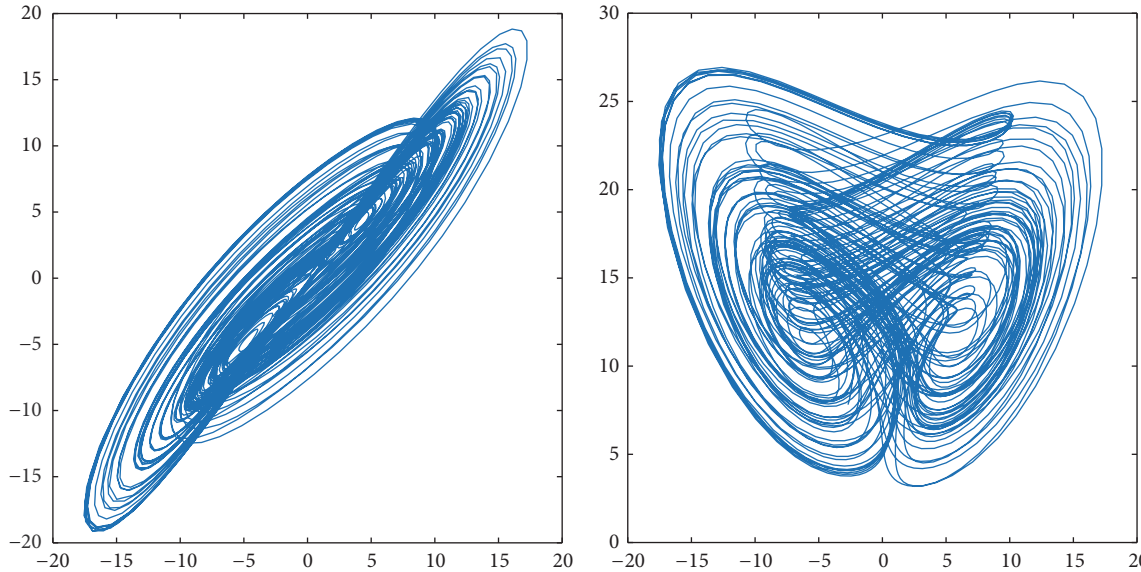
$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= dx - xz + cy - h, \\ \dot{z} &= xy - bz, \\ \dot{h} &= x + k, \end{aligned} \tag{5}$$

where a, b, c, d, and k are the control parameters of the hyperchaotic system. When $a = 36$, $b = 3$, $c = 8$, $d = -16$, and $-0.7 \le k \le 0.7$, the system is in a hyperchaotic state. The hyperchaos attractors are shown in Figure 1. With parameters $a = 36$, $b = 3$, $c = 8$, $d = -16$, and $k = 0.2$, its Lyapunov exponents are $\lambda_1 = 1.552$, $\lambda_2 = 0.023$, $\lambda_3 = 0$, and $\lambda_4 = -12.573$, respectively. Since the hyperchaotic system has two positive Lyapunov exponents, the prediction time of the hyperchaotic system is shorter than the original chaotic system [25]; as a result, it is safer than chaos in security algorithm. Because of this advantage of the hyperchaotic system, we will use it to generate the keys in the compression and encryption stage of our algorithm.

3. The Proposed Image Encryption Scheme

This section presents the proposed scheme for image encryption by using CS and DRPE. Assume that the size of original image X is $N \times N$. The procedure of encryption is given as follows.

Step 1. Confirm the values of the initial conditions x_{10}, y_{10}, z_{10}, h_{10}, k_{10} and iterate the hyperchaotic system for a suitable



(a) x-y plane (b) x-z plane

FIGURE 1: Hyperchaos attractors of system (5) with $k = 0.2$.

times by Runge-Kutta algorithm to avoid the harmful effect of transient procedure.

Step 2. The hyperchaotic system is iterated, and as a result, four hyperchaotic sequences $\{x_{1i}\}$, $\{y_{1i}\}$, $\{z_{1i}\}$, and $\{h_{1i}\}$ would be generated, respectively. And then transform these sequences into sequences $\{\eta_i'\}$, η_i that can be replaced by x_{1i}, y_{1i}, z_{1i}, and h_{1i}.

$$\eta_i' = 10^k \eta_i - \text{round}\left(10^k \eta_i\right). \tag{6}$$

Step 3. The hyperchaotic sequences are exploited to construct the measurement matrix Φ. By taking MN successive elements of the hyperchaotic sequences, we convert it into measurement matrix Φ of size $M \times N$.

Step 4. The original image X is extended in the Ψ domain and then performed the projection measurement in Φ to obtain $Y = \Phi\Psi^T X$, where Ψ is set to be wavelet transform.

Step 5. Divide the measurement Y into two equal blocks; that is, $Y = [Y_1, Y_2]$. Each block has size $M \times (N/2)$. We can add a random column to Y if N is not an even number.

Step 6. The hyperchaotic sequences are exploited to construct the random-phase masks M_1 and M_2. Take the construction of the random-phase mask M_1, for example, and the steps are as follows:

(1) By taking $MN/2$ successive elements of the sequence $\{y_{1i}'\}$, we convert it into a random matrix Q_1 of size $M \times (N/2)$.

(2) Let $M_1(x, y) = \exp(i2\pi Q_1)$.

With another sequence $\{z_{1i}'\}$, the random-phase mask M_2 could be constructed in the same way.

Step 7. Combine Y_1 and Y_2 to obtain the complex-amplitude image:

$$A = Y_1 + Y_2 i. \tag{7}$$

Step 8. A is first multiplied by the first random-phase mask M_1, then transformed by 2D fast Fourier transformation (FFT), and multiplied by the second random-phase mask M_2 and inverse 2D fast Fourier transformation. Thus, we obtain the intermediate encryption result $B = [B_1, B_2]$, which is given by

$$\begin{aligned} B_1 &= \text{ER}\left\{\mathcal{F}^{-1}\left[\mathcal{F}\left[A \cdot M_1\right] \cdot M_2\right]\right\}, \\ B_2 &= \text{EI}\left\{\mathcal{F}^{-1}\left[\mathcal{F}\left[A \cdot M_1\right] \cdot M_2\right]\right\}, \end{aligned} \tag{8}$$

where ER{} denotes the extracting real part operator and EI{} denotes the extracting imaginary part operator.

Step 9. All pixels of B are mapped into an integer range from 0 to 255.

$$\begin{aligned} C_1 &= \text{round}\left[255 \times \frac{B_1 - \min B}{\max\left(B - \min B\right)}\right], \\ C_2 &= \text{round}\left[255 \times \frac{B_2 - \min B}{\max\left(B - \min B\right)}\right]. \end{aligned} \tag{9}$$

And then arrange the pixels from row to column, and we can get two sequences of C_1, C_2, shown as follows:

$$\begin{aligned} C_1 &= \left\{c_{11}, c_{12}, \ldots, c_{1(MN/2)}\right\}, \\ C_2 &= \left\{c_{21}, c_{22}, \ldots, c_{2(MN/2)}\right\}. \end{aligned} \tag{10}$$

Step 10. Confirm the values of the initial conditions x_{20}, y_{20}, z_{20}, h_{20}, k_{20} and iterate the hyperchaotic system for a

suitable times by Runge-Kutta algorithm. Four hyperchaotic sequences $\{x_{2i}\}$, $\{y_{2i}\}$, $\{z_{2i}\}$, and $\{h_{2i}\}$ will be generated, respectively.

Step 11. Transform the four hyperchaotic sequences $\{x_{2i}\}$, $\{y_{2i}\}$, $\{z_{2i}\}$, and $\{h_{2i}\}$ into integer sequences w_i^*, w can be replaced by x_2, y_2, z_2, and h_2.

$$w_i^* = \text{floor}\left(10^k w_i\right) \bmod 256, \tag{11}$$

where mod returns the remainder after division.

Step 12. Took $MN/2$ successive elements of sequences $\{x_{2i}^*\}$, $\{y_{2i}^*\}$, $\{z_{2i}^*\}$, and $\{h_{2i}^*\}$, respectively. And we can get four new sequences D_1, D_2, D_3, and D_4.

$$\begin{aligned} D_1 &= \{d_{11}, d_{12}, \ldots, d_{1(MN/2)}\}, \\ D_2 &= \{d_{21}, d_{22}, \ldots, d_{2(MN/2)}\}, \\ D_3 &= \{d_{31}, d_{32}, \ldots, d_{3(MN/2)}\}, \\ D_4 &= \{d_{41}, d_{42}, \ldots, d_{4(MN/2)}\}. \end{aligned} \tag{12}$$

Step 13. Perform pixel value diffusion according to (14), and we can get H_1 and H_2.

$$\begin{aligned} H_1 &= \{h_{11}, h_{12}, \ldots, h_{1(MN/2)}\}, \\ H_2 &= \{h_{21}, h_{22}, \ldots, h_{2(MN/2)}\}, \end{aligned} \tag{13}$$

where

$$\begin{aligned} h_{1i} &= \left(\left(c_{1i} + c_{1(i-1)} + c_{2(i-1)} + h_{1(i-1)} + h_{2(i-1)} + d_{1i}\right)\right. \\ &\quad \left.\cdot \bmod 256\right) \oplus d_{2i}, \\ h_{2i} &= \left(\left(c_{2i} + c_{2(i-1)} + c_{1(i-1)} + h_{1(i-1)} + h_{2(i-1)} + d_{3i}\right)\right. \\ &\quad \left.\cdot \bmod 256\right) \oplus d_{4i}. \end{aligned} \tag{14}$$

Here $i = 1, 2, \ldots, MN/2$ and initial values c_{10}, c_{20}, h_{10}, and h_{20} are keys. The symbol $\oplus$ represents the exclusive OR operation bit-by-bit.

Step 14. Reshape the sequences H_1, H_2 and obtain the two matrices E_1, E_2 with the size $M \times (N/2)$.

$$E_1 = \frac{H_1}{255} \times \max(B - \min B) + \min B, \tag{15}$$

$$E_2 = \frac{H_2}{255} \times \max(B - \min B) + \min B. \tag{16}$$

In the encryption process, $E = [E_1, E_2]$ is saved for encrypted image. In the decryption process, the encrypted image is first performed by the inverse diffusion process, and then original image information is reconstructed approximately via OMP algorithm after the decryption of double random-phase encoding.

4. Numerical Simulation and Analysis

We illustrate the performance of the proposed image encryption algorithm by means of a series of numerical simulations. In the numerical simulations, the gray image "Lena" and "Cameraman" with 256 × 256 pixels, shown in Figures 2(a) and 2(d) serve as the test images of the image encryption scheme combining CS with DRPE. Ψ is designed 256 × 256, 2D wavelet transform matrix which has the same size with image "Lena" and "Cameraman", and Φ is an 192 × 256 measurement matrix. Therefore, the size of the ciphered image is 192 × 256. For convenience, the encryption key 1 $(x_{10}, y_{10}, z_{10}, h_{10}, k_{10})$ and key 2 $(x_{20}, y_{20}, z_{20}, h_{20}, k_{20})$ are fixed at $(1, 0.1, 1.3, 4, 0.2)$ and $(0.4, 2.1, 0.3, 0.4, 0.6)$, respectively. And they are also the decryption keys. The encrypted "Lena" and "Cameraman" are shown in Figures 2(b) and 2(e). The decrypted image with the correct keys are shown in Figures 2(c) and 2(f).

In order to verify the results of the investigation, the peak signal-to-noise ratio (PSNR) between the original image and decryption image is used for measuring the quality of decrypted digital image as described:

$$\text{PSNR} = 10 \log \frac{255^2}{(1/N^2) \sum_{i=1}^{N} \sum_{j=1}^{N} \left[R(i,j) - I(i,j)\right]^2}, \tag{17}$$

where $R(i, j)$ and $I(i, j)$ denote the values of reconstructed image and original image at pixel (i, j), respectively. The experimental result demonstrates that the quality of the decrypted image is very good and the PSNR is 30.84 dB. From Table 1, the quality of the decrypted image is acceptable for different compression ratios, it means that the compression ability of the proposed algorithm is very well.

4.1. Statistical Analysis Attack. We test the statistical analysis of the proposed image encryption scheme from the histograms of the encrypted images of different images and the correlations of adjacent pixels of the original image and its corresponding encrypted image.

The histograms of "Lena" and "Cameraman" are shown in Figures 3(a) and 3(c), respectively, while Figures 3(b) and 3(d) display the histograms of their corresponding encrypted images, respectively. Although the two images are markedly different, the histograms of their encrypted images are very similar. In general, an effective and safe image encryption algorithm should make the encrypted images corresponding to different original images have similar histograms. In other words, the attacker cannot get any useful information by analyzing the histograms of the encrypted images. Therefore, the proposed algorithm is effectively resistant to the basic statistical analysis attack.

The correlation coefficient C_{xy} of any two adjacent pixels is calculated as follows:

$$C_{xy} = \frac{\sum_{i=1}^{N} (x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\left(\sum_{i=1}^{N} (x_i - \overline{x})^2\right)\left(\sum_{i=1}^{N} (y_i - \overline{y})^2\right)}}, \tag{18}$$

where $\overline{x} = (1/N) \sum_{i=1}^{N} x_i$ and $\overline{y} = (1/N) \sum_{i=1}^{N} y_i$. The correlation coefficients of the proposed algorithm and the

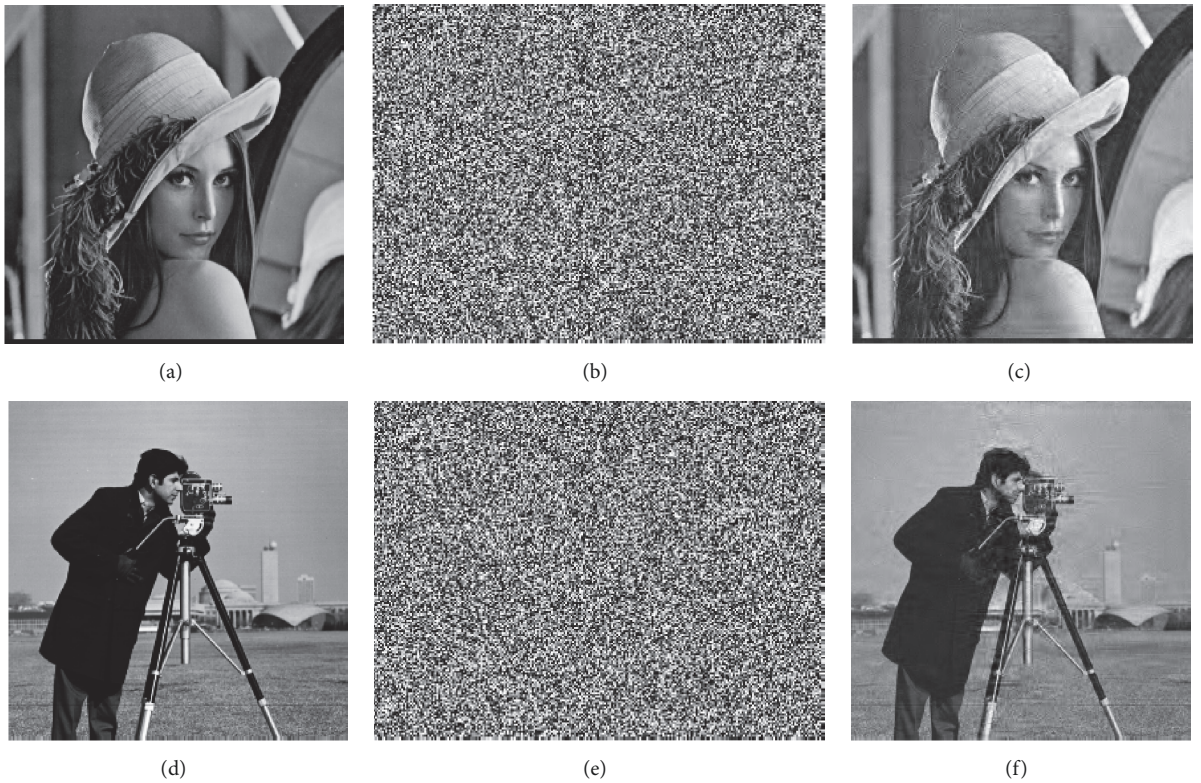


Figure 2: Results of encryption and decryption process.

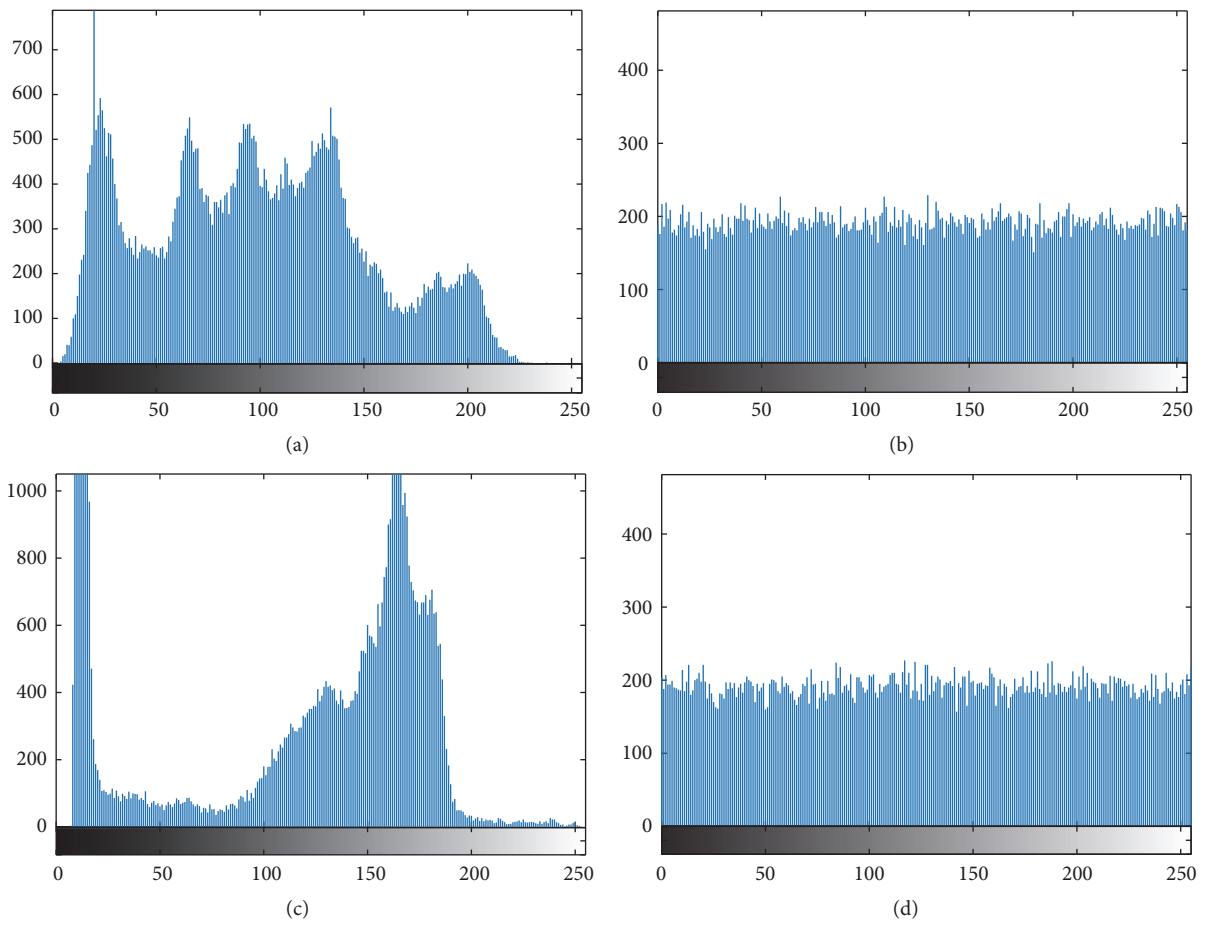


Figure 3: Histograms: (a) "Lena"; (b) encrypted "Lena"; (c) "Cameraman"; (d) encrypted "Cameraman".

Table 1: The results of different compression ratios.

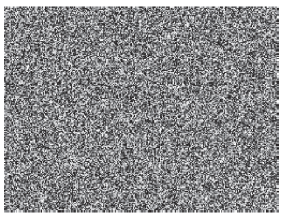
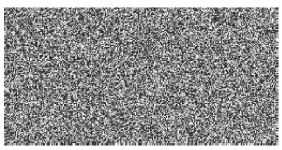
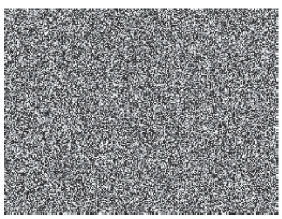
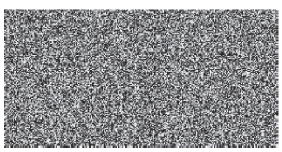
Compression ration	Compressed and encrypted image	Decrypted image	PSNR (dB)
4 : 3			30.84
2 : 1			26.19
4 : 3			27.93
2 : 1			24.23

Table 2: Correlation coefficients of adjacent pixels.

Algorithm	Image	Horizontal	Vertical	Diagonal
Proposed algorithm [21]	Lena	0.9663	0.9491	0.9250
	Encrypted Lena	0.0005	−0.0013	−0.0011
	Encrypted Lena	0.0198	0.0141	0.0026
Proposed algorithm [21]	Cameraman	0.9592	0.9227	0.9272
	Encrypted Cameraman	0.0017	0.0021	−0.0038
	Encrypted Cameraman	0.0128	0.0061	0.0057

algorithm in [21] are compiled in Table 2, which indicated that the proposed algorithm possesses better property than the algorithm in [21]. Figures 4(a)–4(d) show the correlation distribution of two vertically adjacent pixels in the original "Lena," the encrypted "Lena," the original "Cameraman," and the encrypted "Cameraman," respectively. The adjacent pixels of the original in each direction are tightly correlated and the correlation coefficients are all greater than 0.92 in each direction, while the correlation of the encrypted image is almost smaller than 0.004 in each direction.

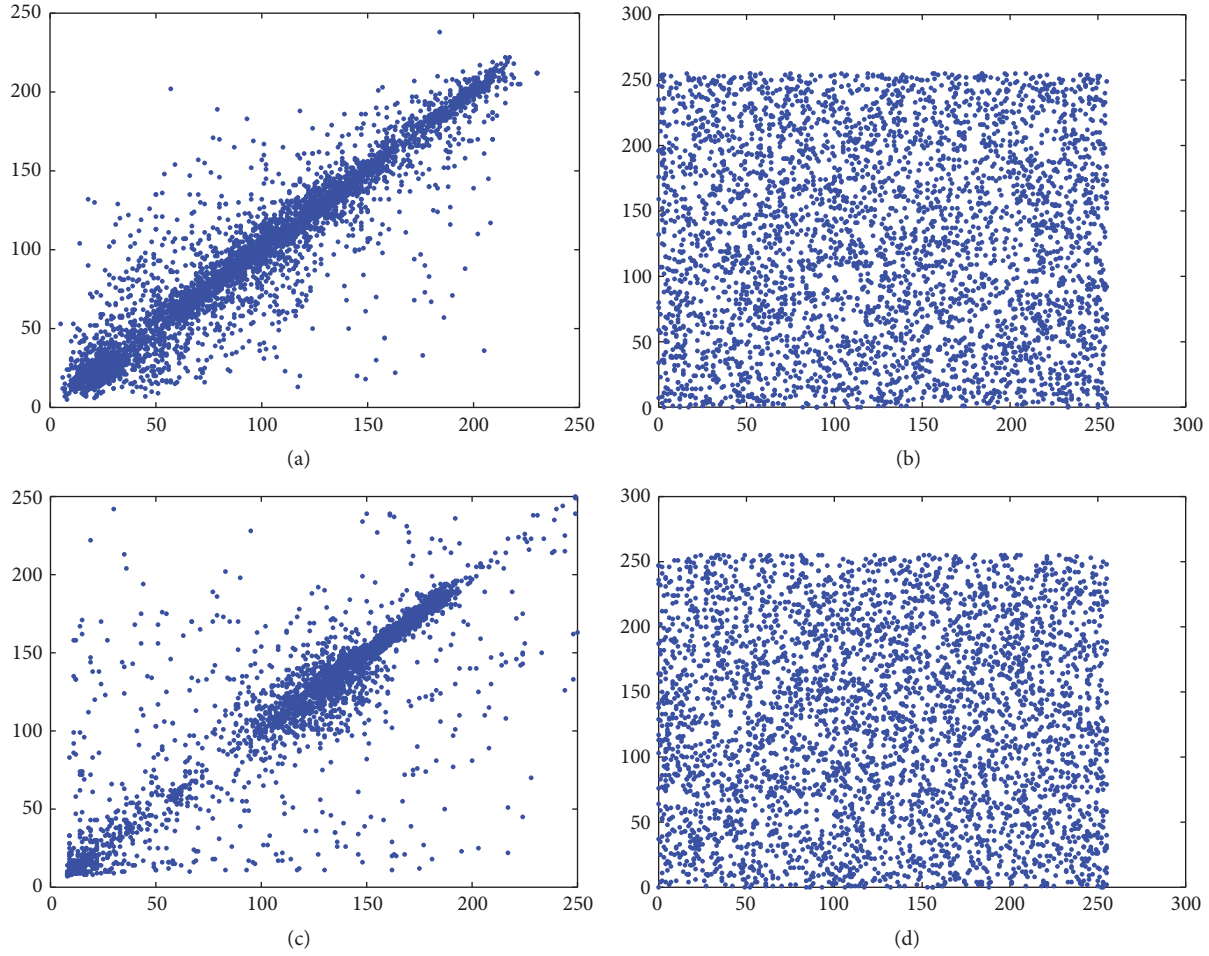


Figure 4: Correlation distribution of two vertically adjacent pixels: (a) "Lena"; (b) encrypted "Lena"; (c) "Cameraman"; (d) encrypted "Cameraman".

4.2. Key Space and Sensitivity Analysis. It is generally known that an effective encryption algorithm should be still secure even if the eavesdroppers know everything except the key. It requires that the key space should be large enough to resist brute-force attacks. In this proposed algorithm, x_{10}, y_{10}, z_{10}, h_{10}, k_{10}, x_{20}, y_{20}, z_{20}, h_{20}, and k_{20} are used as main keys. Here, the key space is calculated for x_{10} to generate two different sequences x and x' by using x_{10} and $x_{10}+\triangle_{x_{10}}$ as initial values and both sequences are of length N; define mean absolute error between the two sequences as [26]

$$\mathrm{MAN}\left(x, x'\right) = \frac{1}{N}\sum\left|x - x'\right|. \tag{19}$$

The key space of x_{10} is equal to $1/\triangle_0$, where $\triangle_0$ is the value of $\triangle_{x_{10}}$ for MAE = 0. The simulation results show that $\triangle_0$ comes out to be 10^{-15}; that is, the key space of x_{10} is 10^{15}, and so are y_{10}, z_{10}, h_{10}, x_{20}, y_{20}, z_{20}, and h_{20}. Similarly, the key space of k_{10} and k_{20} is about 10^{16}. Thus, the total key space is 10^{152}, which is large enough to withstand the brute-force attack.

As is well known, a good image encryption algorithm should be sensitive to the keys, which means that a tiny change in the keys would lead to a great distortion in the decrypted images visually. So in order to measure the differences of two image, the mean square error (MSE) is employed here. The MSE between decrypted image and original image is defined as follows [12]:

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I\left(i,j\right) - H\left(i,j\right)\right]^2, \tag{20}$$

where N and M are the sizes of the images and $I(i, j)$ and $H(i, j)$ denote the values of the original and the decrypted image of the pixel (i, j), respectively. To analyze the key sensitivity, eleven groups of keys are used to decrypt the encrypted "Lena," and the calculated MSE values between the original "Lena" and its corresponding decrypted "Lena" are shown in Table 3. It is noted from Table 3 that the MSE is very large with deviation 10^{-15} to one parameter of $(x_{10}, y_{10}, z_{10}, h_{10}, k_{10}, x_{20}, y_{20}, z_{20}, h_{10}, k_{20})$, and the MSE is small only when the keys are correct. In other words, the decrypted image can be recognized only when the keys are correct; that is, the proposed scheme is very sensitive to the keys. The simulation results of five sets of keys are shown in Figures 2(c) and 5. Figure 2(b) is the decrypted image with the correct keys. Figure 5 shows the decrypted "Lena"

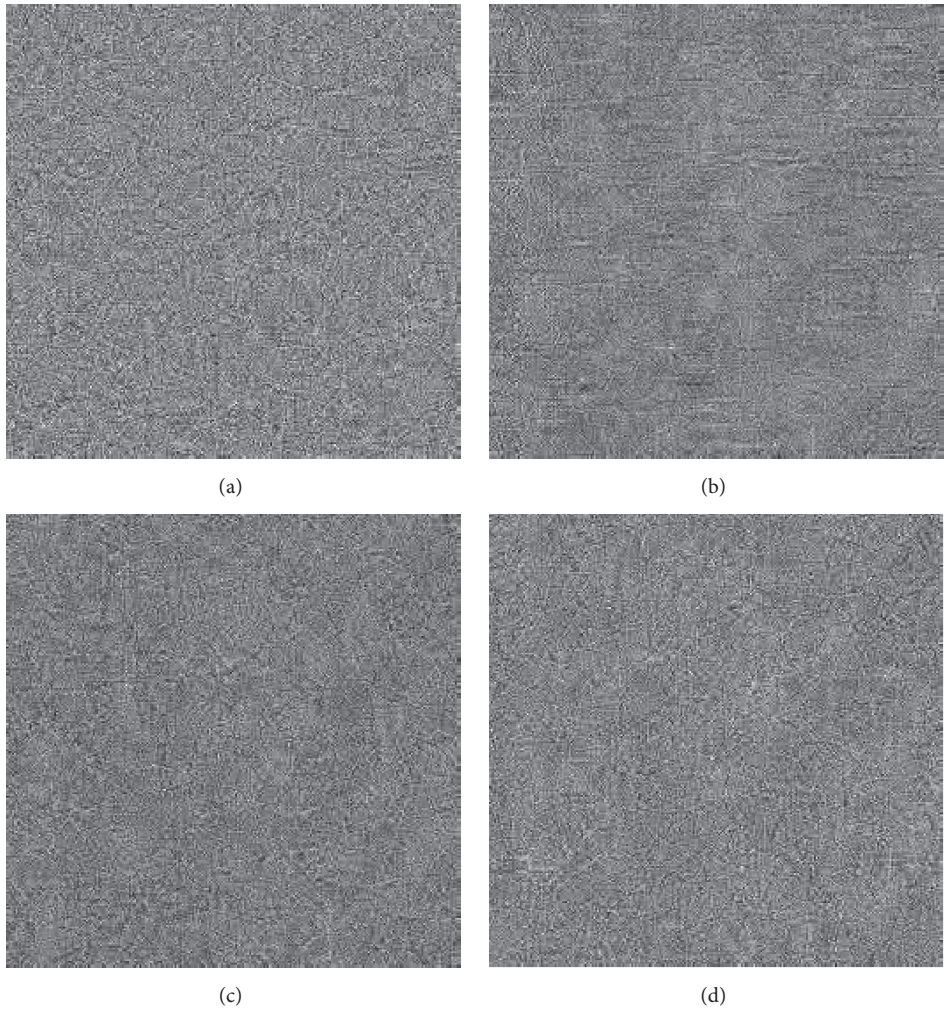


Figure 5: Decrypted "Lena" with (a) incorrect independent parameter x_{10}; (b) incorrect decryption key k_{10}; (c) incorrect decryption key x_{20}; (d) incorrect decryption key k_{20}.

Table 3: The values of MSE between the original "Lena" and its corresponding decrypted "Lena."

	Correct keys	Incorrect x_{10}	Incorrect y_{10}	Incorrect z_{10}	Incorrect h_{10}	Incorrect k_{10}
MSE	53.6	2.65×10^4	2.59×10^4	2.39×10^4	2.49×10^4	2.34×10^4
	Incorrect x_{20}	Incorrect y_{20}	Incorrect z_{20}	Incorrect h_{20}	Incorrect k_{20}	
MSE	6.65×10^4	6.83×10^4	6.95×10^4	6.67×10^4	6.72×10^4	

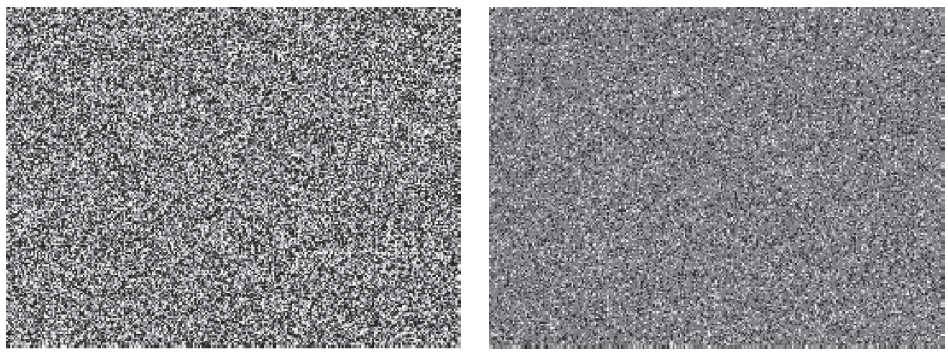
with the incorrect keys deviated 10^{-15} from one parameter of $(x_{10}, k_{10}, x_{20}, k_{20})$, respectively.

4.3. Differential Analysis. We have also measured the number of pixels change rate (NPCR) to see the influence of changing a single pixel in the original image on the encrypted image by the proposed algorithm. The NPCR measures the percentage of different pixel numbers between the two images. We take two encrypted images, C_1 and C_2, whose corresponding original images have only one-pixel difference, respectively. We define a two-dimensional array D, having the same size as the image C_1 or C_2. Then, $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$; namely, if $C_1(i, j) = C_2(i, j)$, then $D(i, j) = 1$; otherwise, $D(i, j) = 0$. The NPCR is evaluated by the following equation [2]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i, j)}{N \times M} \times 100\%, \tag{21}$$

where N and M are the width and height of C_1 or C_2.

In the proposed scheme, a small difference in the plain image can affect the whole cipher image. The percentage of pixel changed in the cipher image is 100% even with a one-bit difference in the plain image (here, we randomly choose a pixel at position (146, 12)), Figure 6(a) shows the cipher image corresponding to only one-pixel difference in the original "Lena", and the difference image between Figures



(a) (b)

Figure 6: The cipher image corresponding only one-pixel difference in the original "Lena" and difference image.

2(b) and 6(a) is shown in Figure 6(b). Thus, the proposed encryption scheme is able to resist the differential attack.

5. Conclusion

A new image compression-encryption algorithm combining compressive sensing with double random-phase encoding is proposed. We utilize the characteristics of the CS theory to cutdown the size of the original image proportionally in the encryption process. Then, the transformed image information can be reencrypted by DRPE technique where the random-phase masks are generated by the hyperchaotic system. Lastly, the resulting image is confused and diffused by using hyperchaotic system simultaneously. The simulation results indicate that the proposed scheme can resist statistical analysis, brute-force attack, and differential attack due to its considerably large key space.

Conflicts of Interest

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

Acknowledgments

The authors thank Ruisong Ye for his help in polishing the paper. The authors would like also to thank the support from National Science Fund of China (Grants nos. 11071152, 11601188, 11701355) and the Natural Science Foundation of Guangdong Province (Grant no. 2015A030313443), China.

References

[1] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[2] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[3] Z. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1–3, pp. 153–157, 2005.

[4] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[5] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons & Fractals*, vol. 40, no. 5, pp. 2191–2199, 2009.

[6] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[7] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," *Chaos, Solitons & Fractals*, vol. 41, no. 4, pp. 1773–1783, 2009.

[8] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Expresss*, vol. 20, no. 7, pp. 767–769, 1995.

[9] S. Zhang and M. A. Karim, "Color image encryption using double random phase encoding," *Microwave and Optical Technology Letters*, vol. 21, no. 5, pp. 318–323, 1999.

[10] G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Expresss*, vol. 25, no. 12, pp. 887–889, 2000.

[11] G. H. Situ and J. J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Expresss*, vol. 29, no. 14, pp. 1584–1586, 2004.

[12] R. Tao, Y. Xin, and Y. Wang, "Double image encryption based on random phase encoding in the fractional Fourier domain," *Optics Express*, vol. 15, no. 24, pp. 16067–16079, 2007.

[13] Z. Liu, S. Li, W. Liu, Y. Wang, and S. Liu, "Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding," *Optics and Lasers in Engineering*, vol. 51, no. 1, pp. 8–14, 2013.

[14] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Processing*, vol. 11, no. 4, pp. 211–216, 2017.

[15] A. Zhang, N. Zhou, and L. Gong, "Color image encryption algorithm combining compressive sensing with arnold transform," *Journal of Computers*, vol. 8, no. 11, pp. 2857–2863, 2013.

[16] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on Compressive Sensing and double random-phase encoding technique," *Optik - International Journal for Light and Electron Optics*, vol. 124, no. 16, pp. 2514–2518, 2013.

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

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

[19] E. J. Candes, J. Romberg, and T. Tao, "Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 52, no. 2, pp. 489–509, 2006.

[20] D. L. Donoho, "Compressed sensing," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[21] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression-encryption algorithm based on compressive sensing," *Optik - International Journal for Light and Electron Optics*, vol. 125, no. 18, pp. 5075–5080, 2014.

[22] E. J. Candes and T. Tao, "Decoding by linear programming," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 51, no. 12, pp. 4203–4215, 2005.

[23] R. G. Baraniuk, "Compressive sensing," *IEEE Signal Processing Magazine*, vol. 24, no. 4, pp. 118–121, 2007.

[24] T. Gao, Z. Chen, Z. Yuan, and G. Chen, "A hyperchaos generated from Chen's system," *International Journal of Modern Physics C*, vol. 17, no. 4, pp. 471–478, 2006.

[25] S. Yanchuk and T. Kapitaniak, "Symmetry-increasing bifurcation as a predictor of a chaos-hyperchaos transition in coupled systems," *Physical Review E: Statistical, Nonlinear, and Soft Matter Physics*, vol. 64, no. 5, Article ID 056235, 2001.

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