Encryption Analysis of Different Measurement Matrices Based on Compressed Sensing

Mengna Shi, Shiyu Guo, Chao Li, Yanqi Zhou, and Erfu Wang(✉)

Key Lab of Electronic and Communication Engineering,
Heilongjiang University, No. 74 Xuefu Road, Harbin, China
efwang_612@163.com

Abstract. The randomness of the traditional measurement matrix in compressed sensing is too strong to be implemented on hardware, and when compressed sensing is used for image encryption, the measurement matrix transmitted as a key will consume time and storage space. Combined with the sensitivity of the chaotic system to the initial value, this paper uses Logistic-Chebyshev chaotic map to obtain random sequences with fewer parameters and construct measurement matrix. To test the measurement performance of the chaotic matrix, compare it with the Gaussian measurement matrix and the Bernoulli measurement matrix in the same compression encryption scheme. Pixel scrambling operation is carried out on the compressed image to complete the final encryption step, and the encrypted image is obtained. The reconstruction algorithm adopts the orthogonal matching tracking method to restore the image. The experimental simulation results show that the chaotic matrix has more advantages than the other two random matrices in image quality, and the encryption and decryption time is shorter.

Keywords: Compressed sensing · Measurement matrix · Chaotic system · Encryption

1 Introduction

In the scope of computer networks, information transmission in the channel is vulnerable to attack. Therefore, information security becomes the focus. When the information demand increases, the processing efficiency in the process of information acquisition is required higher [1, 2]. In 2006, the compressed sensing theory published by Candes and Donoho et al. broke the Nyquist conventional signal sampling technology and realized signal compression through uncorrelated observation of sparse signals, where the observed measurement matrix had to satisfy the condition of restricted isometry property (RIP) [3]. In recent years, compressed sensing is often applied to encryption [4]. Chaotic system is sensitive to the initial value, and the pseudo-random sequence can be generated with fewer parameters to construct the measurement matrix. This paper compared the reconstruction image quality of chaotic

This work was supported by the Natural Science Foundation of Heilongjiang Province, China (no. LH2019F048).

S. Shi et al. (Eds.): AICON 2020, LNICST 356, pp. 63–69, 2021.
https://doi.org/10.1007/978-3-030-69066-3_6

matrix, Gaussian matrix, and Bernoulli matrix as measurement matrices in the same compressed encryption scheme. The simulation results show that the chaotic matrix is feasible as a measurement matrix in compression and encryption.

2 Theoretical Basis

2.1 Compressed Sensing Model

Compressed sensing, as a new signal sampling theory, utilizes the sparse characteristics of signals to obtain discrete samples of signals with random sampling under the condition that the sampling rate is much lower than Nyquist sampling rate, and restores the signal through a nonlinear reconstruction algorithm. Different from traditional compression, compressed sensing is the simultaneous sampling and compression, that is, the sampling value is the compressed value, which greatly reduces the number of transmission, transmission time and storage space.

If the N-dimensional signal x can be expanded under a certain set of sparse basis $\{\psi_i\}_{i=1}^{N}$, that is:

$$x = \sum_{i=1}^{N} s_i \psi_i, \tag{1}$$

where the expansion coefficient $s_i = <x, \psi_i> \;\; = \psi_i^T x$ can be written in matrix form to obtain:

$$x = \psi s, \tag{2}$$

where ψ is an $N \times N$-dimensional sparse basis matrix, s is an N-dimensional sparse coefficient vector, and the number of non-zero coefficients in s is much smaller than N. Use a matrix ϕ that is not related to the sparse basis to project the signal x. The mathematical expression is as follows:

$$y = \phi x, \tag{3}$$

where ϕ is an $M \times N$-dimensional matrix ($M \ll N$), and y is an M-dimensional observation vector. Then the complete compression process of signal x is

$$y = \phi \psi s, \tag{4}$$

and the essence of compressed sensing is to reduce the dimensionality of the signal, from N dimension to M dimension.

The Compressed sensing reconstruction of the signal x is achieved by solving underdetermined set of equations, which is a l_0 norm minimization problem. The l_0

norm solution is an NP hard problem, so it is often converted to a l_1 norm minimization solution, denoted by

$$\min\|s\|_1 s.t. y = \phi\psi s. \tag{5}$$

Commonly used reconstruction methods include base pursuit method, gradient projection method, orthogonal matching pursuit method, etc. In this paper, orthogonal matching pursuit (OMP) method is used [5–7].

2.2 Chaotic Mapping

Chaos is a kind of nonlinear dynamic system, which is generated by control parameters within a certain range, and is sensitive to initial conditions. The sequence generated by the chaotic system is unpredictable. One-dimensional Logistic mapping is defined as follows

$$x_{n+1} = \mu x_n(1 - x_n). \tag{6}$$

When $\mu \in (3.5699456, 4]$, $x_n \in (0, 1)$, the system is chaotic state [8]. One-dimensional Chebyshev mapping is defined as follows

$$x_{n+1} = \cos(t. \arccos x_n). \tag{7}$$

Where t is the order of Chebyshev. When $x_n \in (-1, 1)$, $t \geq 2$, this system is chaotic [9]. The Logistic-Chebyshev chaotic system is defined as follows

$$x_{n+1} = \mathrm{mod}((ax_n(1 - x_n) + ((4 - a)/4) * \cos(b. \arccos x_n)), 1). \tag{8}$$

When $a \in (0, 4]$, $b \in N$, $x_n \in (0, 1)$, the system is in chaos.

2.3 Measurement Matrix

The quality of signal reconstruction in compressed sensing depends on the measurement matrix. When the measurement matrix satisfies the RIP condition, M measurements and measurement matrices can be used to recover the original signal. Common random class matrices satisfy the RIP characteristics, but the strong randomness of these matrices is limited by hardware conditions in practical application, and in the decryption process, the whole measurement matrix as key transmission and storage will waste resources [10]. Chaotic systems use fewer parameters to obtain random sequences, and consequently, when the chaotic matrix is used for compressed sensing, it overcomes the drawback of the large transmission volume of the traditional random matrix. In this paper, Gaussian matrix, Bernoulli matrix and chaotic matrix generated by Logistic-Chebyshev system are tested and compared for image compression and encryption.

3 Encryption Scheme

In compression encryption, we uniformly use discrete wavelet transform to sparse the plain image P with the size of $N \times N$, and use different measurement matrices of size $M \times N$ for observation [11]. To simplify the encryption step, we scrambling the compressed image to obtain the cipher image C [12]. The scrambling steps are as follows.

Step 1: After the Logistic system discards the first 1000 iteration values, the chaotic sequence L with length $M * N$ is generated.

Step 2: sort L to obtain index sequence L'.

Step 3: permutation the pixels of compressed image according to the position of L' to obtain encrypted image C with the size of $M \times N$.

The overall structure of encryption and decryption is shown in Fig. 1. Image decryption is the inverse step of encryption, and the reconstruction algorithm is OMP.

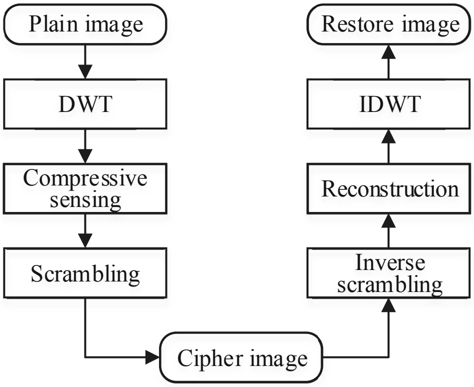

Fig. 1. The overall structure of encryption and decryption.

4 Simulation Results and Analysis

We use Matlab R2016a to verify the performance of the proposed chaotic matrix, the simulation experiments are carried out in a desktop computers with Windows7 operating system, 3.30 GHz CPU and 4 GB RAM. Lena with the size of 256 × 256 was selected as the test image, and 190 × 256 sized the measurement matrix. The Logistic chaotic system parameters used for scrambling are set as $\mu = 3.99$, $x_0 = 0.8326$, The Logistic-Chebyshev chaotic system used to construct the measurement matrix, its parameters set to $a = 3.99$, $b = 20$, $x_0 = 0.23$. Encryption and decryption are carried out according to the method in Sect. 3. Figure 2 is a simulation diagram of encryption and decryption of test images compressed with different measurement matrices. It can be seen from Fig. 2 that the reconstruction of the chaotic matrix is as clear as the other two random matrices.

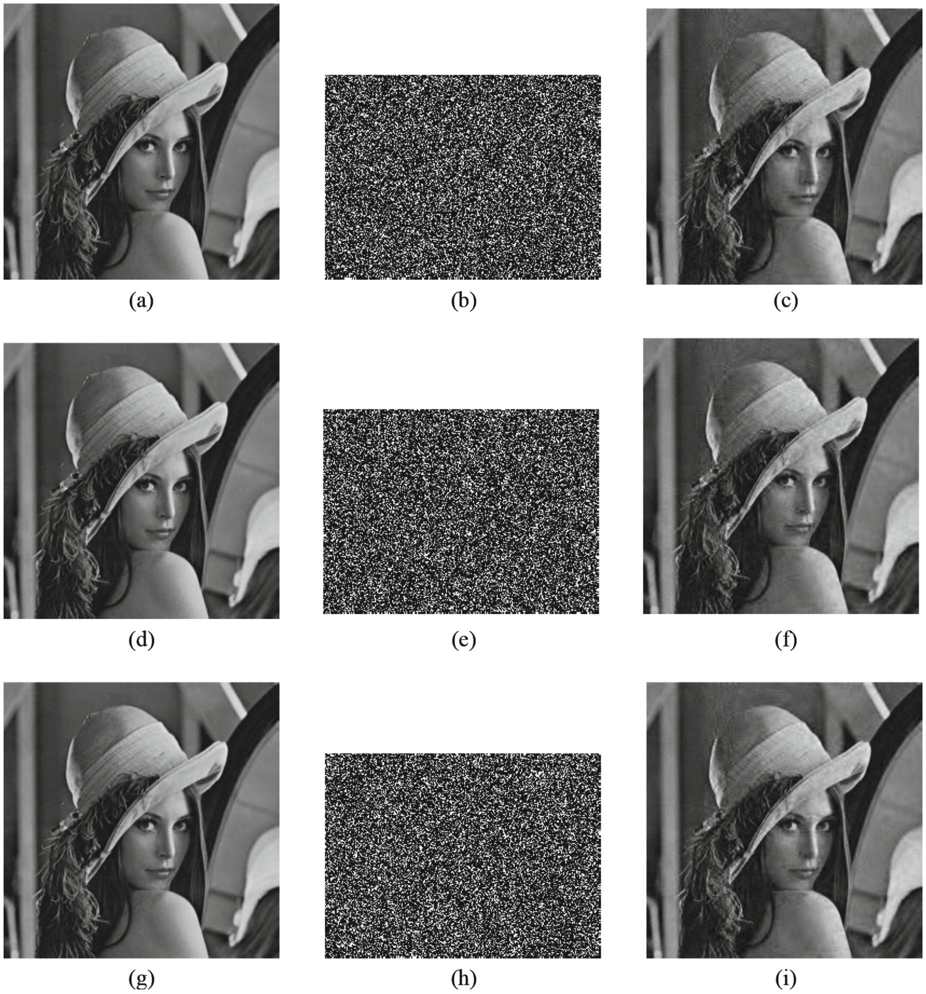

Fig. 2. (a) Test image; (b) Encrypted image of Gaussian matrix measurement; (c) Restore image; (d) Test image; (e) Encrypted image of Bernoulli matrix measurement; (f) Restore image; (g) Test image; (h) Encrypted image of chaotic matrix measurement; (i) Restore image.

Peak signal-to-noise ratio (PSNR) is often used to evaluate the quality of image compression reconstruction, which can be obtained from the definition

$$PSNR = 10\lg\frac{255\times 255}{\frac{1}{MN}\sum_{i=1}^{M}\sum_{i=1}^{N}\left(P(i,j) - C(i,j)\right)^2}, \tag{9}$$

where P is a test image, C is an encrypted image, and M and N are the height and width of the encrypted image respectively [13]. Table 1 lists the PSNR of different decrypted images and encryption and decryption time. The results show that for the three measurement matrices, the chaotic matrix has higher reconstruction performance, shorter time and less key required, which is more suitable for practical application compared with the random matrix.

Table 1. PSNR and time comparison of decrypted images.

Measurement matrix	PSNR (dB)	Time(s)
Gaussian matrix	30.6039	6.4374
Bernoulli's matrix	30.6448	6.7368
Chaotic matrix	30.9052	6.3071

5 Conclusion

Applying the new sampling technology of compressed sensing to the field of cryptography will reduce the transmission time and storage space in the encryption and decryption process. However, the traditional random measurement matrix in compressed sensing is not conducive to hardware implementation. With the natural pseudo-randomness of chaotic system, and the Logistic-Chevbyshev system is utilized through fewer keys to construct a measurement matrix. The image quality is compared with that of Gaussian random matrix and Bernoulli matrix by simulation experiment. The simulation results show that the image reconstructed by chaotic matrix improves the accuracy, which indicates that the measurement matrix constructed by chaotic system has better application potential than the traditional matrix in the field of encryption based on compressed sensing.

References

1. Safa, N.S., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Comput. Secur. **56**, 70–82 (2016)
2. Li, Z., Xu, W., Zhang, X., et al.: A survey on one-bit compressed sensing: theory and applications. Front. Comput. Sci. **12**(2), 217–230 (2018)
3. Candès, E.J., Wakin, M.B.: An introduction to compressive sampling. IEEE Sig. Process. Mag. **25**(2), 21–30 (2008)
4. Cambareri, V., Mangia, M., Pareschi, F., et al.: Low-complexity multiclass encryption by compressed sensing. IEEE Trans. Sig. Process. **63**(9), 2183–2195 (2015)
5. Ujan, S., Ghorshi, S., Pourebrahim, M, et al.: On the use of compressive sensing for image enhancement. In: 2016 UKSim-AMSS. In: 18th International Conference on Computer Modelling and Simulation (UKSim), Cambridge, UK, pp. 167–171. IEEE (2016)
6. Liu, J.K., Du, X.L.: A gradient projection method for the sparse signal reconstruction in compressive sensing. Appl. Anal. **97**(12), 2122–2131 (2018)
7. Wen, J., Zhou, Z., Wang, J., et al.: A sharp condition for exact support recovery with orthogonal matching pursuit. IEEE Trans. Sig. Process. **65**(6), 1370–1382 (2016)
8. Kong, X., Bi, H., Lu, D., et al.: Construction of a class of logistic chaotic measurement matrices for compressed sensing. Pattern Recogn. Image Anal. **29**(3), 493–502 (2019)

9. Zhu, S., Zhu, C., Wang, W.: A novel image compression-encryption scheme based on chaos and compression sensing. IEEE Access **6**, 67095–67107 (2018)
10. Candes, E.J., Tao, T.: Near-optimal signal recovery from random projections: Universal encoding strategies? IEEE Trans. Inf. Theor. **52**(12), 5406–5425 (2006)
11. Yao, S., Chen, L., Zhong, Y.: An encryption system for color image based on compressive sensing. Opt. Laser Technol. **120**, 105703 (2019)
12. Wang, X., Gao, S.: Application of matrix semi-tensor product in chaotic image encryption. J. Franklin Inst. **356**(18), 11638–11667 (2019)
13. Yuan, X., Zhang, L., Chen, J., et al.: Multiple-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing. Appl. Phys. B **125**(9), 174 (2019)