Simultaneous image encryption and compression scheme based on compressed sensing and Hyper chaos map

Ji Xiao-yong [1,a] , Zhou Long-fu [2] , Yan Bing [1] , Bai Sen [1]

[1]Department of information Engineering, Chongqing Communication Institute;

[2]School of Software, Chongqing Institute of Engineering

[a]675722402@qq.com

Keywords: Simultaneous image encryption and compression, compressed sensing, structural measurement matrix, circulant matrix, hyper chaos map

Abstract. Since the significantly low sampling rate and the determinacy of the measurement matrix, compressed sensing (CS) technique can be used for simultaneous image encryption and compression. However, some problems such as the huge size of the measurement matrix prevent its direct application. We find the solutions to the problems and design a simultaneous image encryption and compression scheme in this paper. Block CS and structural measurement matrix are employed for faster calculating speed and smaller storage space. Simulation results show circulant matrix constructed by Chen hyper chaotic permutation has a good performance in sparse signal projection. The proposed scheme has an obviously shorter encoding time than traditional image encryption and compression methods and its compression ratio is possible to be very high but limited by the current level of reconstruction technique. Security analysis also shows the proposed scheme has a robust security performance.

1. Introduction

Researchers devoted themselves on developing the image encryption and compression schemes in the past decades and many methods have been reported[1-3]. However, these algorithms suffer from the high computation complexity and compression ratio reduction caused by the embedded encryption[4]. We can find these compression methods have a common principle that is reducing redundancy, i.e., original signals can be divided into important component and unimportant component and we can recovery the initial image only with the information of the important part. Hence, there exists another way of compression that is directly storing the important component of the initial signal. This point is verified in the compressed sensing (CS) theory.

The CS is a new signal sampling paradigm which breaks through the limit of Nyquist rate in classical Shannon infor-mation theory. It was first proposed by Donoho[5], Can-des[6], and Tao[7] on the basement of signal decomposition and approximation theory. Compared to the conventional compression technique, the CS method can be used to ac-quire the compressed signal by projecting the sparse signal into low-dimensional space with a measurement matrix. We can reconstruct the initial signal with a few coefficients called sampled vector and the reconstruction relies on the knowledge of the measurement matrix used for sampling. Inspired by this, we find the CS technique can be utilized to design image encryption and compression scheme.

Measurement matrix is the key component of the scheme. It is pointed that the measurement matrix should satisfy the restricted isometry property (RIP)[8] or RIPless theory[9] so that the sampled vector could be successfully reconstructed. The common used random measurement ma-trix such as random iid Gaussian matrix is not suitable in image compression for its huge size and storage space. Therefore, we use the block CS and structurally circulant matrix to solve the problem. Compared to the global CS, block CS obviously narrows the size of the measurement matrix but the size is still relatively large which makes the measurement matrix inappropriate to be set as the key to the encryption. So, we adopt the structurally circulant matrix to measure the sparse signal. A hyper chaotic permutation is used to construct the circulant matrix. Due to the special structure, there is no

need to store the whole measurement matrix and the initial values of the hyper chaotic system can be set as the key.

Some CS based image encryption algorithms have been reported[10-14]. Orsdemir et al.[10]analyze the security and robustness of the CS based encryption algorithm and verify this method is secure enough to resist brute force and struc-tured attacks. Encryption methods based on CS are provided in[11-13], but the measurement matrices in these methods are all random matrices which are not easy to store. Endra and Rudy[14] proposed a simultaneous image compression-encryption scheme based on CS by using a novel method of optimized sensing matrix. However, we cannot find any dis-cussion on how to save the measurement matrix and they did not give the evaluation about compression performance. We propose the simultaneous image encryption and compression scheme and simulation results show that our scheme has a robust security performance and good compression performance.

2. Basic concepts

2.1. Compressed sensing

Sparse signal or signals which are able to be sparse repre-sented could be accurately reconstructed from limited meas-urements[15]. Consider a one dimension vector represent-ing a signal with a length of . In common is not sparse but it would be sparse represented by some transformations such as discrete cosine transform (DCT) and discrete wave-let transform (DWT), etc. The sparse representation can be expressed as

$$\mathbf{X} = \mathbf{\Psi S} \tag{1}$$

where $\mathbf{\Psi}$ is the orthogonal sparse matrix with a size of $N \times N$. The 1-D vector $\mathbf{X}$ is compressible[15] and it is compressed as the following form

$$\mathbf{Y} = \mathbf{\Phi X} \tag{2}$$

where $\mathbf{\Phi}$ is incoherence measurement matrix with a size of $M \times N$ and M is much less than N . $\mathbf{Y}$ is the result of the linear projection and its length is M . But not any $\mathbf{\Phi}$ is appropriate for the linear measuring. To successfully reconstruct the original signal, $\mathbf{\Phi}$ should satisfy RIP. Because it is difficult to make the verification using RIP theory[16], RIPless theory is proposed[9] and $\mathbf{\Phi}$ satisfying isotropy property and incoherence property could be used for projection and reconstruction.

The recovery of the signal is an optimization problem. Many alternative models and relative reconstruction algo-rithm are proposed and we choose the minimum total varia-tion (min TV) algorithm here[7]. Equation (3) is the model.

$$\mathbf{S}_{opt} = \arg\min_{\mathbf{S}} \|\mathbf{S}\|_{BV} \quad \text{s. t.} \|\mathbf{Y} - \mathbf{\Phi\Psi S}\|_2 \le \varepsilon \tag{3}$$

where total variation norm is defined as following.

$$\|g\|_{BV} = \sum_{t_1, t_2} \sqrt{|D_1 g(t_1, t_2)|^2 + |D_2 g(t_1, t_2)|^2} \tag{4}$$

where $g(t_1, t_2)$ is the corresponding pixel value of image g . $D_1 = g(t_1, t_2) - g(t_1 - 1, t_2)$ and $D_2 = g(t_1, t_2) - g(t_1, t_2 - 1)$.

2.2. Circulant matrix

The matrix created on the basis of a permutation $\{b_i\}_{i=1}^{N}$ with a structure like Equation (5) is called the circulant matrix.

$$\mathbf{C} = \begin{bmatrix} b_1 & b_2 & b_3 & \cdots & b_N \\ b_N & b_1 & b_2 & \cdots & b_{N-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_k & \cdots & b_1 & \cdots & b_{k-1} \end{bmatrix} \tag{5}$$

When it comes to a two dimensions signal like an image, the size of the measurement matrix is too large to store. Researchers began to use the structural random matrix to replace the common used

random measurement matrix. [17, 18] used the structural random matrix to measure the signal and it is shown that storage space and projecting time are obviously reduced. Circulant matrices are used in[19, 20] to modify the computation performance of CS and[21] proved the circulant matrix based on chaotic permutation could be used as a measurement matrix.

2.3. Chen hyper chaos map

Hyper chaotic systems are well known for their excellent characteristic like pseudorandom and initial value sensitivity, etc. Chen hyper chaotic system is defined as follows.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy + r\sin(\cos(w)) \\ \dot{z} = xy - bz \\ \dot{w} = \varphi \end{cases} \tag{6}$$

where $(x, y, z) \in R^3$, $a, b, c, r \in R^1$ and φ is a variable parameter which determines the chaotic attractor and bifurcations of system (6). When $a = 35, b = 3,\ c = 28,\ r = 35$ and $0 \le \varphi \le 8.90$ the system is hyper chaotic [22]. Hyper chaotic system has a higher instability and a better security performance[23]. Moreover the randomness of hyper chaos map can be utilized in measurement matrix construction.

3. Simultaneous image encryption and compression

In this section we give the detailed steps of the proposed scheme.

Consider an image $\mathbf{I}$ with a size of $M \times N$ and the size of the block is $B \times B$. $\mathbf{\Phi}$ is the measurement matrix with the size of $H \times G$ where $G = B^2$ and $H = round(G \times p)$. For a fast computation speed and good compression performance we set $B = 16$ and $p = 10\%$. Firstly, we construct $\mathbf{\Phi}$ on the basis of the hyper chaotic permutation $\{b_i\}_{i=1}^{G}$. The initial values of Chen hyper chaos map are set as $x_1(1) = 1,\ y_1(1) = 4,\ z_1(1) = 7$ and the parameters are set as $a = 35, b = 3,\ r = 35,\ \varphi$=2.4. We iterate the Equation (6) $(G + k)$ times and gain the hyper chaotic permutation $\{b_i\}_{i=1}^{G}$ from the permutation $\{x_i\}_{i=1}^{G+k}$ following the Equation (7).

$$b_i = x_{i+k} \qquad i = 1, 2, \cdots, G. \tag{7}$$

where k is the starting point of $\{b_i\}_{i=1}^{G}$ and we set $k = 1000$ for a better hyper chaotic effect. $\mathbf{\Phi}$ is constructed by means of row shifting on the basis of the permutation $\{b_i\}_{i=1}^{G}$. It could be proved that $\mathbf{\Phi}$ satisfies the RIPless theory by isotropy property and incoherence property verification used in[21]and we can construct different measurement matrices by changing the starting point . The initial values of and are the keys to the proposed scheme.

Secondly, we encrypt and compress the image $\mathbf{I}$. The diagram is shown as Fig. 1. We describe step by step.

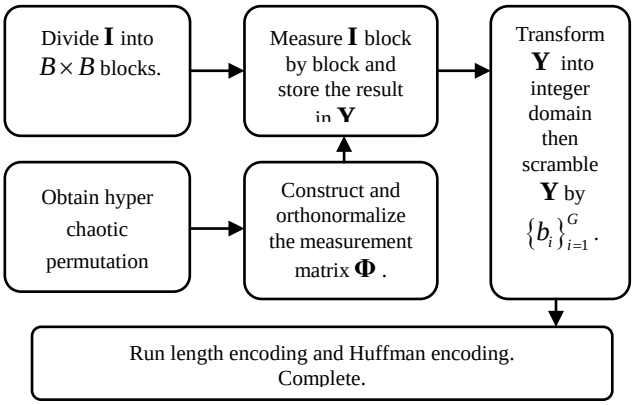


Fig.1 The diagram of the proposed scheme

Step 1: Pad zeros if the size of $\mathbf{I}$ is not integer multiples of B and divide $\mathbf{I}$ into $B \times B$ blocks. Then, generate the hyper chaotic permutation $\{x_i\}_{i=1}^{G+k}$ and gain $\{b_i\}_{i=1}^{G}$ following Equation (7). Then, construct and orthonormalize $\mathbf{\Phi}$.

Step 2: Measure the plain image $\mathbf{I}$ block by block and store the result in $\mathbf{Y}$. $\mathbf{Y}$ is a double matrix and we transform $\mathbf{Y}$ into integer domain by the following command. $\mathbf{Y} = round(\mathbf{Y} \times 10000)$.

Step 3: Scramble $\mathbf{Y}$ on the basis of $\{b_i\}_{i=1}^{G}$.

Step 4: Execute run length encoding and Huffman encoding and complete the compression

Because this is a symmetric scheme, decryption and decompression is the inverse process of the afore-steps.

4. Simulation results and performance evaluations

In this section, compression ratio, running time of compression and results of encryption and decryption are given. We also provide the comparison between the proposed scheme and other image encryption and compression methods. At last, we analyze the key space and key sensitivity to varify the security performance of the proposed method. Test images are Aerial, Boat, Goldhall, Pentagon, Lena and Pepper. All experiments are proceeded in Matlab 2013 Ra.

4.1. Compression ratio

Ignoring the influence of entropy encoding, the theoretical compression ratio (CR) of our scheme is defined as

$$CR_{theoretical} = \frac{G}{H} \tag{8}$$

where G and H are defined in Section 3. When sampling rate $p = 10\%$, $CR_{theoretical}$ equals to 10. In common, the compression ratio (CR) is defined as

$$CR = \frac{\text{The number of bits of plain image}}{\text{The number of bits of cipher image}} \tag{9}$$

The compression comparison between the proposed scheme and other image encryption and compression methods is shown in Table 1.

Table 1 Compression Ratios

	The proposed scheme	The method in[1]	The method in [3]	Simple JPEG
Aerial	10.2611	4.4364	1.5323	5.4635
Boat	11.4137	6.3576	3.4212	8.5759
Pentagon	11.5682	8.3342	5.4500	9.4543
Lena	11.6978	8.9613	6.0845	10.6429
Peppers	11.5922	8.0812	5.1354	10.5361

From Table 1, it seems that there is no obvious advantage for the proposed scheme in compression ratio. This is because we did not set the sampling rate as low as possible. In theory, the compression ratio of the proposed scheme could be very high only if the sampling rate is low enough. However, in current level of reconstruction technique, the reconstruction quality obviously reduces when the sampling rate drops. Therefore, the current compression ratio of CS based image encryption and compression methods would not be very high but there exists the possibility. In addition, its computation complexity is very low and its compression performance is not influenced by the embedded encryption.

4.2. Running time of compression

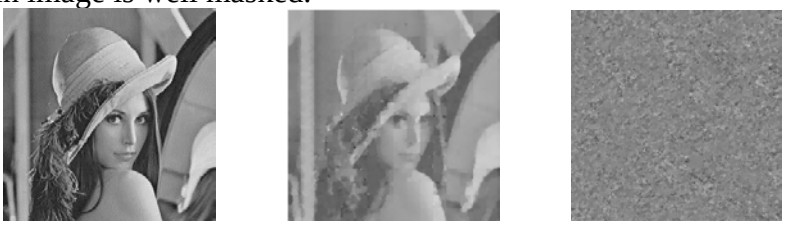
Table 2 shows the running time of compression in several image encryption and compression schemes. Due to the low computational complexity, our scheme speeds less time during compression.

Table 2 Runing time of compression

	The proposed scheme	The method in[1]	Simple JPEG
Aerial	0.1054s	1.2655s	1.0012s
Boat	0.0973s	0.6678s	0.6175s
Goldhall	0.0934s	1.1547s	0.9856s
Lena	0.0853s	0.6630s	0.5263s
Peppers	0.0976s	0.7079s	0.5372s

4.3. Results of encryption and decryption

We take the Lena image as the example. Fig. 2(a) is the original Lena image and Fig. 2(b) the decryption image with the right keys. It is shown that we can decrypt the image correctly by the proposed scheme but the reconstruction quality is not good for the low sampling rate. What's more, the reconstruction time is too long which needs to be improved. Fig. 2(c) is the encrypted image. We can see that the plain image is well masked.



(a) (b) (c)

Fig. 2 Results of encryption and decryption

The initial values of x_1, y_1, and z_1 are the keys to the proposed scheme. Assume that the computational precision of the 64-bit double-precision number is about 10^{-14}, the key space is $10^{14} \times 10^{14} \times 10^{14} = 10^{42}$ which is relatively large. We set the initial value of $x_1(1) = 1.000003$ and decrypt the encrypted Lena image and the result is demonstrated in Fig. 2(c). It shows that the proposed scheme is key sensitivity.

5. Conclusion

In this paper, we proposed a simultaneous image encryption and compression scheme and gain well compression performance and robust security performance. During the experiments we also find some aspects such long reconstruction time and the limit of reconstruction quality waiting to be improved. The next work should be focused on reducing the recovery time and enhancing the level of reconstruction quality. With the development of CS technique, we believe the proposed scheme has greatness inside it.

Acknowledgements

The work on this paper was supported by National Natural Science Foundation of China (Grant No.61272043), Basic & Frontier Project of Chongqing (Project No. cstc2013jjB40009), innovation project of graduate students (CYS14203).

REFERENCES

[1] Zhang, Y., D. Xiao, H. Liu, and H. Nan, GLS coding based security solution to JPEG with the structure of aggregated compression and encryption. Communications in Nonlinear Science and Numerical Simulation. 19(5): p. 1366-1374, 2014.

[2] Hermassi, H., R. Rhouma, and S. Belghith, Joint compression and encryption using chaotically mutated Huffman trees. Communications in Nonlinear Science and Numerical Simulation. 15(10): p. 2987-2999, 2010.

[3] Wharton, E.J., K. Panetta, and S.S. Agaian. Simultaneous Encryption/Compression of Images Using Alpha Rooting. in DCC. 2008.

[4] Wong, K.-W. and C.-H. Yuen, Embedding compression in chaos-based cryptography. Circuits and Systems II: Express Briefs, IEEE Transactions on. 55(11): p. 1193-1197, 2008.
[5] Donoho, D.L., Compressed sensing. Information Theory, IEEE Transactions on. 52(4): p. 1289-1306, 2006.
[6] Candès, E.J. Compressive sampling. in Proceedings oh the International Congress of Mathematicians: Madrid, August 22-30, 2006: invited lectures. 2006.
[7] Candès, E.J., J. Romberg, and T. Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information. Information Theory, IEEE Transactions on. 52(2): p. 489-509, 2006.
[8] Candes, E.J., The restricted isometry property and its implications for compressed sensing. Comptes Rendus Mathematique. 346(9): p. 589-592, 2008.
[9] Kueng, R. and D. Gross, RIPless compressed sensing from anisotropic measurements. Linear Algebra and its Applications. 441: p. 110-123, 2014.
[10] Orsdemir, A., H.O. Altun, G. Sharma, and M.F. Bocko. On the security and robustness of encryption via compressed sensing. in Military Communications Conference, 2008. MILCOM 2008. IEEE. 2008. IEEE.
[11] Huang, R. and K. Sakurai. A robust and compression-combined digital image encryption method based on compressive sensing. in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011 Seventh International Conference on. 2011. IEEE.
[12] Athira, V., S. George, and P. Deepthi. A novel encryption method based on compressive sensing. in Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on. 2013. IEEE.
[13] Soman, K. Secrecy of cryptography with compressed sensing. in 2012 International conference on advances in computing and communications (ICACC). 2012.
[14] Endra, R.S. Compressive sensing-based image encryption with optimized sensing matrix. in Computational Intelligence and Cybernetics (CYBERNETICSCOM), 2013 IEEE International Conference on. 2013. IEEE.
[15] Candes, E. and J. Romberg. Signal recovery from random projections. in Proc. SPIE. 2005.
[16] Baraniuk, R., M. Davenport, R. DeVore, and M. Wakin, A simple proof of the restricted isometry property for random matrices. Constructive Approximation. 28(3): p. 253-263, 2008.
[17] Do, T.T., T.D. Tran, and L. Gan. Fast compressive sampling with structurally random matrices. in Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on. 2008. IEEE.
[18] Candes, E. and J. Romberg. Robust signal recovery from incomplete observations. in Image Processing, 2006 IEEE International Conference on. 2006. IEEE.
[19] Bajwa, W.U. Geometry of random Toeplitz-block sensing matrices: bounds and implications for sparse signal processing. in SPIE Defense, Security, and Sensing. 2012. International Society for Optics and Photonics.
[20] Romberg, J. and R. Neelamani, Sparse channel separation using random probes. Inverse Problems. 26(11): p. 115015, 2010.
[21] Jing-Bo, G. and W. Ren, Construction of a circulant compressive measurement matrix based on chaotic sequence and RIPless theory. 2014.
[22] Ji, X.-y., S. Bai, Y. Guo, and H. Guo, A new security solution to JPEG using hyper-chaotic system and modified zigzag scan coding. Communications in Nonlinear Science and Numerical Simulation. 22(1): p. 321-333, 2015.
[23] Zhang, Q., L. Guo, and X. Wei, A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-International Journal for Light and Electron Optics. 124(18): p. 3596-3600, 2013.