Color image encryption via compressive sensing and chaotic systems

Kaige Zhu* *and Jinli* Cheng

School of Computer and Information Engineering, Henan University, Kaifeng 475004, China

Keywords: Encryption, Compressive sensing, Chaotic systems.

Abstract. In this paper, we design a color image encryption algorithm based on chaotic system and block compressive sensing. Firstly, the sparse representation of the plain-image is obtained by an adaptive learning dictionary. Secondly, the key streams are produced from two excellent low-dimensional chaotic maps, where updating the initial values and parameters rely on the SHA-384 and the input image. Thirdly, three measurement matrices of R, G, B components are constructed from the chaotic sequences, respectively. Finally, a random rows and columns diffusion method is performed on the encrypted image. Experimental results and safety analysis prove that the proposed scheme has excellent performance.

1 Introduction

Compressive Sensing (CS) theory is one of the methods of digital images encryption, which can achieve compression and encryption simultaneously. In [1], a CS image encryption algorithm was proposed, where the measurement matrix is constructed via logistic map. The chaotic system had a pivotal role in constructing the measurement matrix because their chaotic sequences are random and deterministic signal. Subsequently, Gong et al. [2] put forward an image compression and encryption algorithm based on chaotic system, which had a good ability on resistance the known plaintext attacks. However, the measurement matrix was generated from low-dimensional chaotic systems with the simple structures, which greatly reduce the security and the sensitive of the algorithms. To solve this problem, high-dimensional chaotic maps were applied in the image encryption methods [3-5]. The Chen's hyperchaotic system was performed on the 2D CS-based image encryption algorithm in [3]. Chai et al. [4] explored a new magnetic controlled memristive chaotic system to construct the circular measurement matrix and encrypt the image, which can enhance the security. Recently, Xu et al. [5] also applied a hyper-chaotic system to encrypt image, which achieved an acceptable compression effects. Unfortunately, these complex chaotic maps increased the computation complexity, and the constructed measurement matrices are single, which would reduce the security and sensibility of cryptosystem. In the current studies, most of them employed the fixed dictionary such as DWT to represent different images sparsely, and the

* Corresponding author: 1520156473@qq.com

attained dictionaries are identical and has an influence on the recovering the image.

Motivated by the above analysis, we propose an image encryption algorithm by means of two simple improved chaotic systems, the adaptive learning dictionary algorithm and a random diffusion of rows and columns process. Compared with the existing schemes, our method has a higher security and a better image reconstruction effect. Numerical experiments have verified the feasibility and validity of the proposed algorithm.

2 Preliminaries

2.1 Compressive sensing

A signal x with size $N \times N$ is sparse in a $N \times N$ transform domain Ψ, and a measurement matrix ϕ $M \times N$ $(M < N)$ which is uncorrelated with Ψ is used to yield the measurement y in linear projection [6] as follows:

$$y = \varphi x = \varphi \psi s = As \quad , \tag{1}$$

where A is the sensing matrix, s is the sparse coefficient. x can be recovered by:

$$\min \| s \|_0 \ \text{ subject to } y = As \quad . \tag{2}$$

Obviously, the signal reconstruction is an ill-posed inverse problem. To overcome this problem, we adopt the Iterative Reweighted Least Squares algorithm (IRLS) [7], which is based on minimum norm with weight iteration.

2.2 Chaotic systems

In this paper, two chaotic maps with excellent performance, i.e., LSS and LASM [8], are used to image encryption, which are separately described as follows:

$$X_{n+1} = \left(rX_n(1 - X_n) + (4 - r)\sin(\pi X_n)/4 \right) \bmod 1 \quad , \tag{3}$$

$$\begin{cases} Y_{n+1} = \sin(\pi\mu(Z_n + 3)Y_n(1 - Y_n)) \\ Z_{n+1} = \sin(\pi\mu(Y_{n+1} + 3)Z_n(1 - Z_n)) \end{cases} , \tag{4}$$

where $r \in (0,4]$, $\mu \in [0,\ 1]$, $X_n, Y_n, Z_n \in (0,1)$.

3 The proposed encryption scheme

3.1 Generating the sparse dictionaries

Suppose a color image I with size $M \times N$. The R, G, B components of I are denoted as $imgR$, $imgG$, $imgB$, respectively. We divide three components $imgR$, $imgG$ and $imgB$ into $B \times B$ non-overlapping blocks, and convert the image blocks into the vectors with $B^2 \times 1$. After image segmentation, different image blocks have some similar properties. So we

calculate the variance values of all blocks, and the image blocks with large variance are selected as the parameters of the Method of Optimal Directions (MOD) algorithm [9], where the number of chose blocks is N. And use the MOD algorithm to get the sparse dictionaries D_i with size $B^2 \times N$, where $i = R, G, B$.

3.2 Generating the key streams for pixel-level diffusion

Step1 Employ the SHA-384 and the plain image I to update the initial values x_0, y_0, z_0 and the parameters r_0, μ_0 as follows:

$$r = r_0 - (h_1 - h_2)/2^8, \tag{5}$$

$$\mu = \mu_0 + (h_3 - h_4)/2^8, \tag{6}$$

$$x_1 = x_0 - h_5 \oplus (h_7 - h_6)/2^8, \tag{7}$$

$$y_1 = y_0 + \mathrm{mod}(h_8 + h_9 / h_{10}, 1), \tag{8}$$

$$z_1 = z_0 - \mathrm{mod}(h_{11} / h_{12}, 1), \tag{9}$$

where h_i denotes the hash values, $i = 1, 2, \cdots 12$. $\oplus$ represents an exclusive OR, and $\mathrm{mod}(x, y)$ returns the remainder after division.

Step 2 Use r, μ, x_1, y_1 and z_1 to iterate LSS and LASM for $l_0 + m \times N$ times, where $l_0 = 1000$, $m = \frac{M}{B} \times \lceil r \times B \rceil$, and r is the compression ratio of blocks. In order to alleviate the harmful effect of the transient, we discard the former 1000 values and get three key streams x, y, z with length $m \times N$.

Step 3 To enhance the sensitivity of the system, we recombine the sequences x, y and z by:

$$x1 = \left[x_1, x_2, \cdots, x_{mN/2}, y_{mN/2+1}, y_{mN/2+2}, \cdots, y_{3mN/4}, z_{3mN/4+1}, z_{3mN/4+2}, \cdots, z_{mN}\right], \tag{10}$$

$$y1 = \left[y_{mN/2+1}, y_{mN/2+2}, \cdots, y_{mN}, x_{3mN/4+1}, x_{3mN/4+2}, \cdots, x_{mN}, z_{mN/2+1}, z_{mN/2+2}, \cdots, z_{3mN/4}\right], \tag{11}$$

$$z1 = \left[z_1, z_2, \cdots, z_{mN/2}, y_{mN/2+1}, y_{3mN/4+1}, y_{3mN/4+2}, \cdots, y_{mN}, x_{mN/2+1}, x_{mN/2+2}, \cdots, x_{3mN/4}\right]. \tag{12}$$

Step 4 To get the ideal pseudo-random sequences, the chaotic sequences $x1$, $y1$ and $z1$ are further processed as follows:

$$X' = 10^{\alpha} \times x1 - \mathrm{floor}(10^{\alpha} \times x1), \tag{13}$$

$$Y' = 10^{\beta} \times y1 - \text{floor}(10^{\beta} \times y1), \tag{14}$$

$$Z' = 10^{\lambda} \times z1 - \text{floor}(10^{\lambda} \times z1), \tag{15}$$

where α=5, β= 6, λ=7.

Step 5 Sort the sequences X', Y' and Z' with length $m \times N$ in ascending order, and get the index sequences $Index1$, $Index2$ and $Index3$. Similarly, sort respectively the sequences X', Y' and Z', and obtain the index sequences $IndRm$, $IndGm$, $IndBm$ with length m and $IndRn$, $IndGn$ and $IndBn$ with length N.

Step 6 To get the key streams for modifying the pixel values of the image, we convert the sequences $Index1$, $Index2$ and $Index3$ into three matrices $IndexR$, $IndexG$ and $IndexB$ with size $m \times N$, respectively. We quantize three matrices $IndexR$, $IndexG$ and $IndexB$ into the range of $[0,255]$, and get three matrices SKR, SKG and SKB.

3.3 Encryption process

Step 1 Input a color image I with $M \times N$, and employ MOD in Section 3.1 to generate the sparse dictionaries.

Step 2 To construct three measurement matrices of R, G, B components, we sample the chaotic sequences $x1$, $y1$ and $z1$ with intervals d, where d=3, and get three measurement matrices ϕR, ϕG and ϕB with size $\left(\lceil r \times B \rceil \times B\right) \times B^2$.

Step 3 The matrices $blockmatrix_i$ are projected and measured by the measurement matrices in column to get measurements y_i, where $i = R, G, B$. And transform them into three matrices yRR, yGG and yBB with $m \times N$, where $m = \frac{M}{B} \times \lceil r \times B \rceil$.

Step 4 The key streams $Index2$, $Index1$ and $Index3$ are applied to shuffle the positions of yRR, yGG and yBB, and obtain three $m \times N$ matrices $yR1$, $yG1$ and $yB1$.

Step 5 To further strengthen the security of the algorithm, the key streams SKR, SKG and SKB are employed to modify the pixel values of $yR1$, $yG1$ and $yB1$ as follows:

$$yR2(i,\ :) = yR1(IndRm(i),\ :) \oplus SKR(i,:), \tag{16}$$

$$yG2(i,\ :) = yG1(IndGm(i),\ :) \oplus SKG(i,:), \tag{17}$$

$$yB2(i,\ :) = yB1(IndBm(i),\ :) \oplus SKB(i,:), \tag{18}$$

$$CR(:, j) = yR2(:,\ IndRn(j)) \oplus SKR(:, j), \tag{19}$$

$$CG(:, j) = yG2(:,\ IndGn(j)) \oplus SKG(:, j), \tag{20}$$

$$CB(:, j) = yB2(:, IndBn(j)) \oplus SKB(:, j), \tag{21}$$

where $1 \le i \le m$, $1 \le j \le N$, the matrices CR, CG and CB are three components of the final encrypted image.

4 Simulation results

We choose the 'Lena' image with size 256×256 as the test image, which is displayed in Fig. 1(a). The initial values are set as follows: $\gamma_0 = 3.578196573421804$, $\mu_0 = 0.766936472082413$, $x_0 = 0.273642281087165$, $y_0 = 0.322934593157826$, $z_0 = 0.608100359832734$, $B = 8$ and the compression ratio of blocks r is 0.4. In other words, the total compression ratio is 50%, and the encryption results are shown in Fig. 1(b). One can clearly see that the cipher image is noise-like images and the corresponding decrypted image in Fig. 1(c) is almost identical to the original image (Fig. 1(a)). Therefore, our algorithm is feasible and has high reconstruction accuracy.

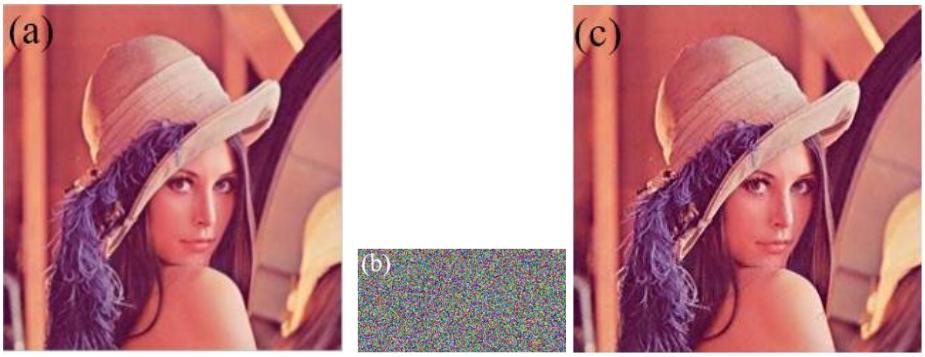

Fig. 1. Experience results: (a) Lena plain-image, (b) The cipher image; (c) The corresponding decrypted image.

5 Performance and security analysis

5.1 Compressive sensing analysis

The peak signal-to-noise ratio (PSNR) is an important indicator to assess image quality. PSNR is defined as follows:

$$PSNR = 20\log_{10}\left(MaxI / \sqrt{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[X(i,j) - Y(i,j)]^2} \right), \tag{22}$$

where $MaxI$ denotes the maximum value, X and Y separately represent the original image and the processed image. Generally, the human eyes cannot differentiate between the original and processed images when $PSNR \ge 30dB$ [10]. Table 1 provides the PSNR values for the different methods. We can apparently see that our method is superior to other schemes in [4, 5, 11, 12] in terms of reconstructed image quality.

Table 1. PSNRs (dB) for the different methods.

Image	CR	Ref [4]	Ref [5]	Ref [11]	Ref [12]	Ours
Lena	25%	26.06	26.52	6.42	22.62	29.25
	50%	29.82	29.23	29.23	26.87	36.38
	75%	29.56	29.22	33.95	30.82	43.47

5.2 Key space analysis

The designed algorithmm mainly involves the secret keys γ_0, μ_0, x_0, y_0 and z_0. If the computational precision is 10^{-15}, the key space of our method is $10^{75} \approx 2^{250}$, which is larger than those in [3, 5]. Apparently, the key space of our method is large enough to resist the brute force attacks.

5.3 Secret key sensitivity analysis

In the sensitivity analysis, a very slight change $(\triangle=10^{-15})$ is applied to the secret key γ_0, for example, $\gamma_0' = \gamma_0 - \Delta$. γ_0' is applied to decrypt the encrypted image Fig. 1(b). Fig. 2 gives the simulation results. From Fig. 2(a), we do not find any information of Lena, and their difference rate between Fig. 1(c) and Fig. 2(a) is more than 99%. The simulation results show that our algorithm is very sensitive to the secret keys.

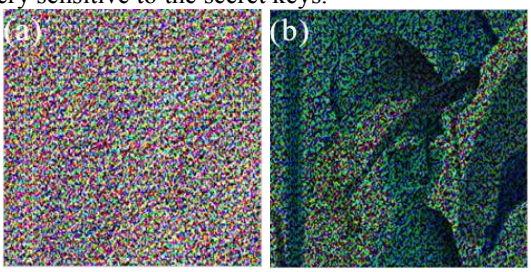

Fig. 2. Key sensitivity analysis: (a) Lena decrypted image with the modified key γ_0'; (b) Differential image between (a) and Fig. 1(c).

6 Conclusion

In this paper, an encryption scheme is proposed using compressive sensing and chaotic maps. On the one hand, the scheme uses CS to reduce the size of cipher image and improve the accuracy of image reconstruction. On the other hand, the key streams are utilized to re-encrypt the compressed image, which greatly improves the security of encryption algorithm. Experimental results and security analysis have demonstrated that the proposed method has a satisfactory performance.

References

1. N. Zhou, A. Zhang, F. Zheng, Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, J. Optics & Laser Technology. 62 (2014) 152-160.

2. L. Gong, K. Qiu, C. Deng, An image compression and encryption algorithm based on chaotic system and compressive sensing, J. Optics & Laser Technology. 115 (2019) 257-267.
3. J. Chen, Y. Zhang, L. Qi, Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression, J. Optics & Laser Technology. 99 (2018) 238-248.
4. X. Chai, X. Zheng, Z. Gan, An image encryption algorithm based on chaotic system and compressive sensing, J. Signal Processing. 148 (2018) 124-144.
5. Q. Xu, K. Sun, C. Cao, A fast image encryption algorithm based on compressive sensing and hyperchaotic map, J. Optics and Lasers in Engineering. 121 (2019) 203-2.
6. E. Candes, J. Romberg, T. Tao, Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, J. arXiv preprint math/0409186 (2004).
7. R. Wolke, H. Schwetlick, Iteratively reweighted least squares: algorithms, convergence analysis, and numerical comparisons, J. SIAM journal on scientific and statistical computing. 9 (1988) 907-921.
8. X. Wu, K. Wang, X. Wang, Lossless chaotic color image cryptosystem based on DNA encryption and entropy, J. Nonlinear Dynamics. 90 (2017) 855-875.
9. K. Engan, S. O. Aase, J. H. Husoy, Method of optimal directions for frame design[C]//1999 IEEE International Conference on Acoustics, Speech, and Signal Processing, Proceedings, ICASSP99 (Cat. No. 99CH36258), IEEE. 5 (1999) 2443-2446.
10. Q. Huynh-Thu, M. Ghanbari, Scope of validity of PSNR in image/video quality assessment. J. Electronics letters. 44 (2008) 800-801.
11. L. Yaru, W. Jianhua, Image encryption based on compressive sensing and variable parameter chaotic mapping, J. Journal of Optoelectronics·Laser, Tianjin. 26 (2015) 605-610.
12. N. Zhou, A. Zhang, J. Wu, Novel hybrid image compression–encryption algorithm based on compressive sensing, J. Optik-International Journal for Light and Electron Optics. 125 (2014) 5075-5080.