ATLANTIS PRESS
Advances in Intelligent Systems Research, volume 136
4th International Conference on Sensors, Mechatronics and Automation (ICSMA 2016)

Digital Image Multiple Encryption Algorithm based on Compressive Sensing

Zhan Yu[1, a], Changlun Zhang[1, b], Hengyou Wang[1, c], Nan Ning[1, d]

[1]Beijing University of Civil Engineering and Architecture, Beijing, 102616, China

[a]email: 2107010415004@stu.bucea.edu.cn, [b]email: zclun@bucea.edu.cn,

[c]email: wanghengyou@bucea.edu.cn, [d]email: ningnan@stu.bucea.edu.cn

Keywords: Image Encryption; Compressive Sensing; Arnold Transform; Logistic Map

Abstract. We propose a new method for the efficiency and the security of digital image transmission, termed digital image multiple encryption algorithm based on compressive sensing. Compressive sensing is utilized to compress and encrypt a digital image with the random measurement matrix as key, Arnold transform and Logistic map are used to encrypt the image again to realize the multiple encryption of image. The experimental results show that the encryption algorithm has such features as high key sensitivity, low data volume and can resistance some common attack.

Introduction

With the rapid development of internet, the security of digital image becomes more and more important. Many images are private or confidential and image transmission also consumes a lot of energy. So it is necessary to take some measures to compress image data and protect sensitive image data.

Donoho et al [1-3] proposed a theory called compressive sensing (CS), which is a new technology in the field of signal processing. CS has a profound impact in image processing areas. Reconstruction algorithm researches on CS have made a lot of achievements, some scholars proposed Orthogonal Matching Pursuit (OMP) [4] committed to CS reconstruction problem, but reconstruction speed of this algorithm is relatively slow. In order to improve the computing speed, some scholars proposed Gradient Pursuits (GP) [5], but its precision is low. On the basis of GP, Blumensath introduced conjugate direction and weak atomic threshold selection strategy in order to improve the reconstruction accuracy, proposed stage wise weak gradient pursuits (SWCGP) [6], but the reconstruction accuracy is still not good enough. In [7], a new image compression algorithm was proposed in order to improve reconstruction speed under premise of guaranteeing reconstruction precision.

Image encryption technology has been put into study in recent years. Guo [8] proposed an Arnold double scrambling image encryption technology, image pixel values were scrambled with two-dimensional Arnold transform. Although this method increased key space, it difficult to meet some image that requires relatively high security. Tang Z [9] proposed that security of image could be increased by applying R, G and B three components of image to block Arnold transform. Indeed, this method can improve security of image, but attacker may reconstruct part of image information as long as a component is decrypted. Jiang [10] proposed a 3SMA, which uses three different round key. Each round, two color components of the clear text image were encrypted. This algorithm has greatly improved key space, but pixel values do not change so that attacker may find useful information through comparison of clear text image and cipher text image to break encryption system.

A digital image encryption algorithm based on CS is proposed. We design a pixel value diffusion method in order to improve 3SMA. The multiple encryption of digital image is realized via CS and the improved method, and so the correlation between clear text image and cipher text image is destroyed.

Design and implementation of algorithm

Image is compressed sensing via the algorithm proposed in [7], and we improve 3SMA by adding a pixel value diffusion method to 3SMA.

Proposed pixel value diffusion method. In order to achieve diffusion, Chaotic sequence a_k, b_k are generated by chaotic system according to Eq. 1:

$$a_{k+1} = \lambda a_k(1 - a_k),\ a_k \in (0,1),\ \lambda \in [0,4], \quad (1)$$

so the generated sequence a_k , b_k are completely disorder. Then, the sequence a_k ,b_k are enlarged and rounded through a zoom factor to get two integer sequence e_1, e_2 :

$$e_1(k) = \text{round}(256 * a(k)),\ e_2(k) = \text{round}(256 * b(k)), \quad (2)$$

and a linear operation and a rounded operation are conducted on the integer sequence e_1, e_2 as:

$$Z(k) = \text{round}(\alpha e_1(k) + (1 - \alpha)e_2(k)). \quad (3)$$

Therefore, the pixel value diffusion is realized via a xor operation as:

$$y_2(k) = Z(k) \oplus y(k), \quad (4)$$

where y(k) is cipher text image. The inverse of the diffusion is as follows:

$$y(k) = Z(k) \oplus y_2(k). \quad (5)$$

Generation of key. In consideration of basic requirements of cryptography, cipher text should have a close relationship with key. key used in proposed algorithm is composed of 12 parameters: random seed parameters Se that is used to generate measurement matrix, compression radio P, N, T, r, a, b are used in scrambling pixel position, a_0,b_0,λ_1,λ_2,α are used in pixel value diffusion. These parameters need to satisfy: Se, N, T, r, a, b are positive integer, $P \in (0,1)$, $a_0 \in (0,1)$, $b_0 \in (0,1)$, $\lambda_1 \in [0,4]$, $\lambda_2 \in [0,4]$, $\alpha \in (0,1)$.

The encryption algorithm. The improved image encryption algorithm is as follows:

Step1: Get gray value matrix x according to clear text image and generate a key K = (Se, P, N, T, r, a, b, a_0, b_0, λ_1, λ_2, α).

Step2: Get measurement matrix Φ [7] according to Se and P as

$$\Phi = (T^2)^{-1}(T^2\varphi)^z, \quad (6)$$

where φ is a gauss random matrix, T^2 is a two-dimensional transform, let $(T^2\varphi)^z$ denote the vector by setting the last n – m columns of $T^2\varphi$ to be zeros. We can get observation matrix y [7] as

$$y_{m\times m} = \Phi_{m\times n} x_{n\times n} \Phi^t_{m\times n}. \quad (7)$$

Step 3: Matrix y is stored in a single dimensional array A in the form of a row main sequence, pixel coordinates are array subscript and resolve the pixel coordinates to two-tuples according to Eq. 8 [10]:

$$x = \text{floor}(C/r),\ y = c \bmod r, \quad (8)$$

where C is the coordinate, floor is rounding down function.

Step 4: T Arnold transform is conducted on the two-tuples coordinates pair to get new two-tuples (x_T, y_T) and merge (x_T, y_T) into a new number C_T according to Eq. 9 [10]:

$$C_T = x_T \times r + y_T. \quad (9)$$

Step 5: The array A is ascending sorted with C_T as key, remove all coordinates of A, all pixel values are imported in order to get cipher text image y_1.

Step 6: Two chaotic sequences a, b are generated according to Eq. 1 and chaotic sequences a, b are rounded according to Eq. 2 to get scrambled matrix e_1 and scrambled matrix e_2. We can get scrambled matrix Z according to Eq. 3.

Step 7: Xor operation is conducted on scrambled matrix Z and cipher text image y_1 according to Eq. 4 to get final cipher text image y_2.

The decryption algorithm. The improved image decryption algorithm is as follows:

Step 1: Get gray value matrix y_2 and the key K = (Se, P, N, T, r, a, b, a_0, b_0, λ_1, λ_2, α) according to cipher text image.

Step 2: Two chaotic sequences a, b are generated according to Eq. 1 and chaotic sequences a, b are rounded according to Eq. 2 to get scrambled matrix e_1 and scrambled matrix e_2. We can get scrambled matrix Z according to Eq. 3.

Step 3: Xor operation is conducted on scrambled matrix Z and cipher text image y_2 according to Eq. 5 to get cipher text image y_1.

Step 4: Build an r order abstract matrix V, T transform is conducted on V and record pixel position on a swap table.

Step 5: Matrix y_1 is stored in a single dimensional array A′ in the form of a row main sequence, move the pixels of A′ back to the original coordinates according to the swap table, we get matrix y via sequential outputting A′ after moving its pixels.

Step 6: Get measurement matrix Φ [7] according to Se and P.

Step 7: The original image x is reconstructed according to Eq. 10.

$$x = (T^2)^{-1}(((\Phi^S)^{-1})^t T^2(y)(\Phi^s)^{-1}), \quad (10)$$

where let Φ^S denote the vector by discarding the zero columns of $(T^2\varphi)^z$.

Experimental analysis

In this paper, clear text images adopted Lena and Cameraman of size 256×256, Barbara of size 512×512, all simulations were conducted in MATLAB-2010a with an Inter CPU Core i5-3470 and 8 GB RAM under OS Windows 7 Ultimate edition 64-bit. The selected key is as: K = (Se, P, N, T, r, a, b, a_0, b_0, λ_1, λ_2, α) = (123456, 0.5, 500, 200, 300, 3, 5, 0.3, 0.6, 3.6, 3.7, 0.5).

Gray level histogram analysis. For image processing, the gray histogram is a kind of data form to describe the spatial distribution law of image pixel value. Gray histogram of plain text image and cipher text image is shown in Fig 1, from Fig 1(b), distribution of the pixels of the original image is dispersed. from Fig 1(d), the pixel value of the encrypted image is mostly distributed in 0 and 255 pixel, the distribution is very concentrated. The gray histogram of the encrypted image is very different from that of the original image, so it can resist some statistical analysis.

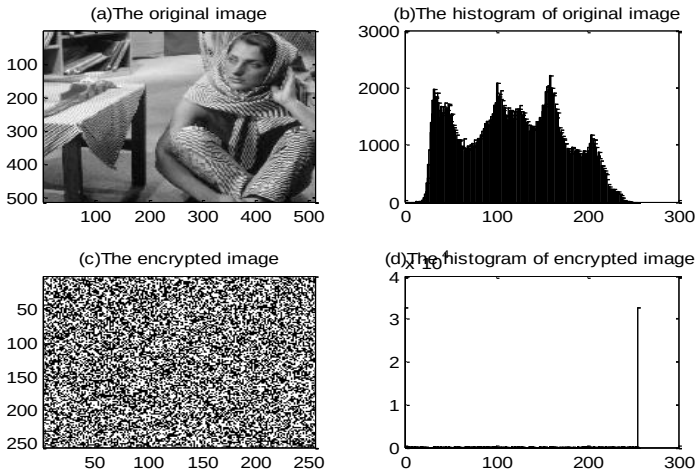


Fig.1. gray histogram of encrypted image and original image

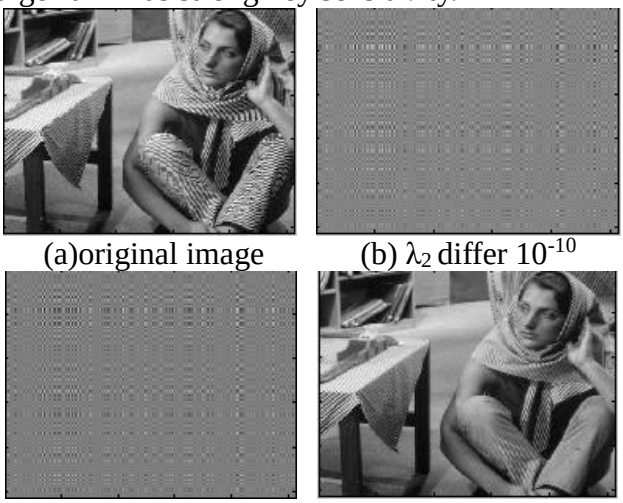
Adjacent pixel correlation analysis. The correlation between the adjacent pixels of an original image can reflect degree of image scrambling. We calculate the correlation coefficient of the adjacent pixels, the calculation results are shown in Table 1, from Table 1, the correlation coefficient between adjacent pixels of the clear text is about 0.9. But the correlation coefficient between adjacent pixels of the cipher text is close to 0. Therefore, the encryption algorithm can

effectively remove correlation of the clear text image and can resist some statistical attack.

Table 1 Correlation of adjacent pixels

image	horizontal		vertical		diagonal	
	clear text	cipher text	clear text	cipher text	clear text	cipher text
Lena	0.9286	-0.0514	0.9637	-0.0509	0.9077	0.0064
Cameraman	0.9431	-0.0301	0.9589	-0.0222	0.9179	-0.0049
Barbara	0.8947	-0.0072	0.9546	-0.0317	0.8764	-0.0765

Key sensitivity analysis. The sensitivity of key is also an important aspect to judge strength of the encryption algorithm. From Fig 2, when only a or λ_2 has minor change and other parameters remain unchanged, original image cannot be reconstructed. The rest parameters have been tested, the results show that although any of parameters has small change, the original image cannot correctly decrypted, So the algorithm has strong key sensitivity.



(a)original image (b) λ_2 differ 10^{-10}

(c) a differ 1 (d) decrypted image

Fig.2. Key sensitivity test

Compared with chaotic scrambling encryption method. The typical chaotic scrambling image encryption [11-12] is selected for experimental comparison. The chaotic sequences are generated by using Logistic system. We use Eq. 1 to generate the chaotic scrambling sequence, $\lambda = 3$, $x_1 = 0.3412$ are key, then encrypted image with the key. As shown in Table 2, proposed encryption algorithm has a larger key space and can stronger resistance to attack, however it is inevitable that some information is lost due to the use of CS in the process of image sampling, so the information entropy of the encrypted image is smaller than that of the original image. The speed of encryption and decryption is slowed down and it also shows that the encryption and decryption of this paper need more work and time.

Table 2 Compared with chaotic scrambling encryption algorithm

Contrast properties	Proposed encryption algorithm	chaotic scrambling encryption algorithm
Gray histogram	completely chaos	no change
Anti attack ability	Stronger	weaker
Key space	$\leq 2^{96}$	$\leq 2^{50}$
Information entropy	7.4323（reduced）	8.3242（no change）
Encryption time	12.7234	1.2343
Decryption time	30.2123	1.4359

Conclusions

In order to reduce the transmission of digital image and improve the security of image transmission,

this paper proposes an improved image encryption algorithm based on CS. In the encryption process, CS can effectively reduce image transmission and image is encrypted again by proposed algorithm. Experimental results show that proposed multiple encryption method can effectively enhance the reliability of image, so it can be used in digital image encryption.

Acknowledgement

This work was financially supported by the National Nature Science Foundation of China (Project No. 61502024) and Beijing Municipal Education Commission on Projects (SQKM201510016013).

References

[1] David Donoho, Yaakov Tsaig: Signal Processing. Forum Vol. 533-548 (2006), p. 86

[2] DL Donoho: IEEE Trans Info Theory. Forum Vol. 1289-1306 (2006), p. 52

[3] E J Candes, J Romberg and T Tao: IEEE Trans Info Theory. Forum Vol. 489-509(2006), p. 52

[4] Tropp J A, Gilbert A C: IEEE Trans on Information Theory. Forum Vol. 4655-4666(2008), p. 53

[5] Blumensath T, Davies ME: IEEE Transactions on Signal Processing. Forum Vol. 2370-2382(2008), p. 56

[6] Blumensath T, Davies M E: IEEE Transactions on Signal Processing. Forum Vol. 4333-4346(2009), p. 57

[7] CS Lu,HW Chen: Information Sciences. Forum Vol. 33-47(2015), p. 325

[8] Linqin Guo, Xinrong Zhang: Computer Applications and Software. Forum Vol. 264-266(2010), p. 27(In Chinese)

[9] Tang Z, Zhang X: Journal of Multimedia. Forum Vol. 202-206(2011), p. 6 (In Chinese)

[10] Fan Jiang, Xiaotian Wu and Wei Sun: Journal of Computer Applications. Forum Vol. 726-731,745 (2015), p. 35 (In Chinese)

[11] Guodong Ye: Pattern Recognition Letters. Forum Vol. 347-354(2010), p. 31 (In Chinese)

[12] Manjunath Prasad, K L Sudha: Computer Science &.Information Technology. Forum Vol. 169-179 (2011), p. 4