An image compression-encryption algorithm based on 2-D compressive sensing

Article *in* Journal of Computational Information Systems · December 2013

DOI: 10.12733/jcis8608

CITATIONS
2

READS
104

4 authors, including:

Nanrun Zhou
Nanchang University; Shanghai Jiao Tong University
142 PUBLICATIONS **1,909** CITATIONS

SEE PROFILE

Journal of Computational Information Systems 9: 24 (2013) 10057–10064
Available at http://www.Jofcis.com

An Image Compression-encryption Algorithm Based on 2-D Compressive Sensing ⋆

Yan MO [1], Aidi ZHANG [1,2], Fen ZHENG [2], Nanrun ZHOU [1,2,*]

[1] *Jiangxi Province Key Laboratory of Image Processing and Pattern Recognition, Nanchang Hangkong University, Nanchang 330063, China*

[2] *Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China*

Abstract

An image compression-encryption algorithm based on 2-D compressive sensing is proposed, which can accomplish encryption and compression simultaneously. The measurements are performed in two directions and the measurement matrices are constructed as partial Hadamard matrices, which are controlled by chaos map. The proposed algorithm is sensitive to the keys and it can resist various attacks. Simulation results verify the validity and reliability of the proposed algorithm.

Keywords: Compressive Sensing; Image Encryption; Image Compression

1 Introduction

With the development of multimedia technology, more and more important information comes from images. The security of images becomes a serious issue. Y. Liu et al proposed an image encryption method based on chaos and fractional Fourier transform [1], and L. Chen proposed a novel image encryption scheme based on Hyperchaotic sequence [2]. While transmission channels are always insecure and bandwidth-constrained. It is desired to transmit the data after encryption and compression. Some image encryption-compression algorithms based on compressive sensing (CS) [3, 4] have been proposed. An image encryption method based on compressive sensing and double random-phase encoding was proposed [5], the data volume for encryption was lowered due to the dimensional decrease properties of CS. X. Zhang and Y. Ren proposed a scheme to compress and decompress encrypted image based on CS where the orthogonal transform was a secret, yet the encryption and compression were not completed simultaneously [6]. The security analysis covered the resistance against the brute force and structured attacks was also researched

⋆The work is supported by the National Natural Science Foundation of China (Grant Nos. 61262084 and 61141007), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (Grant No. 20122BCB23002), the Natural Science Foundation of Jiangxi Province, China (Grant No. 20132BAB201019), and the Opening Project of Key Laboratory of Image Processing and Pattern Recognition (Nanchang Hangkong University), Jiangxi Province (Grant No. TX201204002).

*Corresponding author
Email address: znr21@163.com (Nanrun ZHOU).

1553–9105 / Copyright © 2013 Binary Information Press
DOI: 10.12733/jcis8608
December 15, 2013

[7]. AV Sreedhanya and KP Soman proposed a scheme where both compressive sensing and Arnold scrambling are employed to encrypt color image [8]. R. Huang, K. H. Rhee and S. Uchida proposed a parallel image encryption method based on CS where block cipher structure consisting of scrambling, mixing, S-box and chaotic lattice XOR is designed to further encrypt the quantized measurement data [9]. Due to the inevitable problem of packet loss during wireless transmission, the anti-packet loss ability of the CS-based encryption method was quantified [10].

All the above encryption-compression methods based on CS adopted the Gaussian random matrix as measurement matrix, which are unpractical. Meanwhile, some of them did not complete the compression and encryption simultaneously. What's more, some of them could not resist chosen-plaintext attack [11]. We explore a new compression-encryption algorithm based on 2-D CS where the measurements are performed in two directions and the measurement matrices are constructed as partial Hadamard matrices.

2 The Image Encryption-compression Algorithm Based on 2-D CS

Assume x is a matrix with size $N \times N$. Note the measurement as β_1, i.e.,

$$\beta_1 = \Phi_1 \Psi^{\mathrm{T}} x \tag{1}$$

where the superscript T denotes transposition, Φ_1 is an $M \times N$ measurement matrix and Ψ is an $N \times N$ orthogonal basis.

Extend the transposition of β_1 in Ψ domain, one can obtain

$$\beta_2 = \Psi^{\mathrm{T}} \beta_1^{\mathrm{T}} = \Psi^{\mathrm{T}} x^{\mathrm{T}} \Psi \Phi_1^{\mathrm{T}} = \beta \Phi_1^{\mathrm{T}} \tag{2}$$

where $\beta = \Psi^{\mathrm{T}} x^{\mathrm{T}} \Psi$. One can see that the term $\Psi^{\mathrm{T}} x^{\mathrm{T}} \Psi$ behaves like a 2-D Ψ transformation. Perform the measurement on β_2 with another measurement matrix Φ_2,

$$y = \Phi_2 \beta_2 = \Phi_2 \beta \Phi_1^{\mathrm{T}} \tag{3}$$

the $N \times N$ matrix x is compressed to be an $M \times M$ matrix y which behaves like the result of a 2-D transformation. Thus it can be called 2-D CS.

With the above analysis, the proposed algorithm can be illustrated as Fig. 1, and the encryption steps are as follows:

1. Extend x in 2-D Ψ domain to obtain $\beta = \Psi^{\mathrm{T}} x \Psi$;
2. Construct the measurement matrices Φ_1 and Φ_2;
3. Perform the operation $y = \Phi_2 \beta \Phi_1^{\mathrm{T}}$ to obtain the encrypted image.

Performing the reconstruction algorithm SL0 [12] once in two directions respectively, one can obtain $\widetilde{\beta}$ which is the approximation of β, then taking the 2-D Ψ domain inverse transformation, one can obtain $\widetilde{x}$ which is the decrypted image. The sensor matrices in twice SL0 are Φ_2 and Φ_1, respectively.

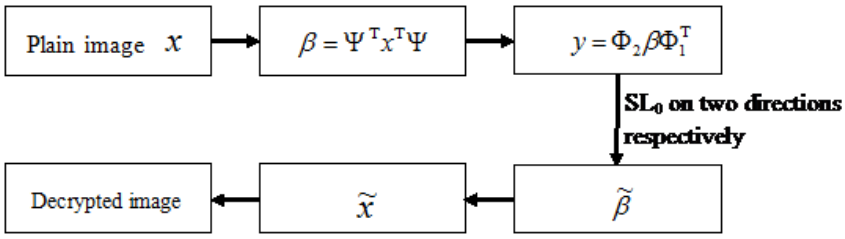


Fig. 1: The proposed image encryption algorithm

The measurement matrices Φ_1 and Φ_2 are controlled by logistic map and constructed as partial Hadamard matrices thus they are practical. The logistic map is defined as:

$$x_{n+1} = \mu x_n(1 - x_n),\ x_n \in [0, 1] \tag{4}$$

when $\mu \in [3.57, 4]$, it becomes chaotic.

Take the construction of Φ_1 as example, the steps are as follows:

1. Generate a sequence with length $2N$ by logistic map with initial condition x_{01}, abandon the preceding N elements to obtain the index sequence $s = [s_1, s_2, \ldots, s_N]$;
2. Sort the nature sequence $n = [1, 2, \ldots, N]$ with the index sequence s, note the sorted sequence as $p = [p_1, p_2, \ldots, p_N]$, where $p_i \in [1, N]$;
3. Generate the Hadamard matrix H of order N, and choose the row vectors to group into the measurement matrix Φ_1, i.e.,

$$\Phi_1 = \begin{pmatrix} H(p_1, :) \\ H(p_2, :) \\ \vdots \\ H(p_M, :) \end{pmatrix} \tag{5}$$

where $H(p_i, :)$ denotes the p_i-th row vector of H. With another initial condition x_{02}, Φ_2 can be constructed.

3 Simulation and Discussion

The proposed algorithm is fitted to operate on the image whose length and width both are the multiples of 4 since the measurement matrices are constructed as partial Hadamard matrices. So the gray image 'Lena' with resolution 256×256, which is shown as Fig. 2(a), is served as the test image. Without loss of generality, the original image is extended with 2-D DCT, Φ_1 and Φ_2 are $M \times N$ ($M = 192$, $N = 256$) partial Hadamard matrices. The parameters in simulation are $x_{01} = 0.11$, $x_{02} = 0.24$ and $\mu = 3.99$, where x_{01} and x_{02} are the initial conditions corresponding to Φ_1 and Φ_2, respectively. Fig. 2(b) is the encrypted and compressed Lena and Fig. 2(c) is the correct decrypted Lena. Fig. 2(d)–(f) are the decrypted images with wrong $x_{01} = 0.11 + 10^{-16}$ and wrong $x_{02} = 0.24 + 10^{-16}$, respectively.

(a) (b) (c) (d) (e)

Fig. 2: (a) Lena; (b) encrypted Lena; (c) decrypted Lena; (d) decrypted Lena with wrong x_{01}; (e) decrypted Lena with wrong x_{02}

3.1 Statistical analysis

Statistical analysis has been performed with the proposed encryption and compression algorithm, which is shown by a series of tests on the histograms of images and on the correlations.

To measure the correlations of adjacent pixels in the original Lena and the encrypted Lena, 8000 pairs of two adjacent pixels are selected in horizontal, vertical and diagonal directions, respectively. The correlation coefficient can be obtained by

$$\mathrm{C} = \frac{\sum_{i=1}^{N}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{N}(x_i - \overline{x})^2 \sum_{i=1}^{N}(y_i - \overline{y})^2}} \tag{6}$$

where $\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$. The results are compiled in Table 1.

Table 1: Correlation coefficients of adjacent pixels

Correlation coefficient	Horizontal	Vertical	Diagonal
original Lena	0.9590	0.9217	0.9071
encrypted Lena	0.0158	0.2608	−0.0205
original Baboon	0.6477	0.7201	0.6231
encrypted Baboon	0.1087	0.1107	0.0101

It can be seen that the correlation of the encrypted images are much weaker than that of the original images, which demonstrates that attackers cannot obtain useful information according the statistical analysis.

Fig. 3 shows the histograms for the original images and the encrypted images. The histograms of different images are obviously different while the histograms of their corresponding encrypted images are similar. It further proves that the proposed algorithm can resist the attacks from statistical analysis.

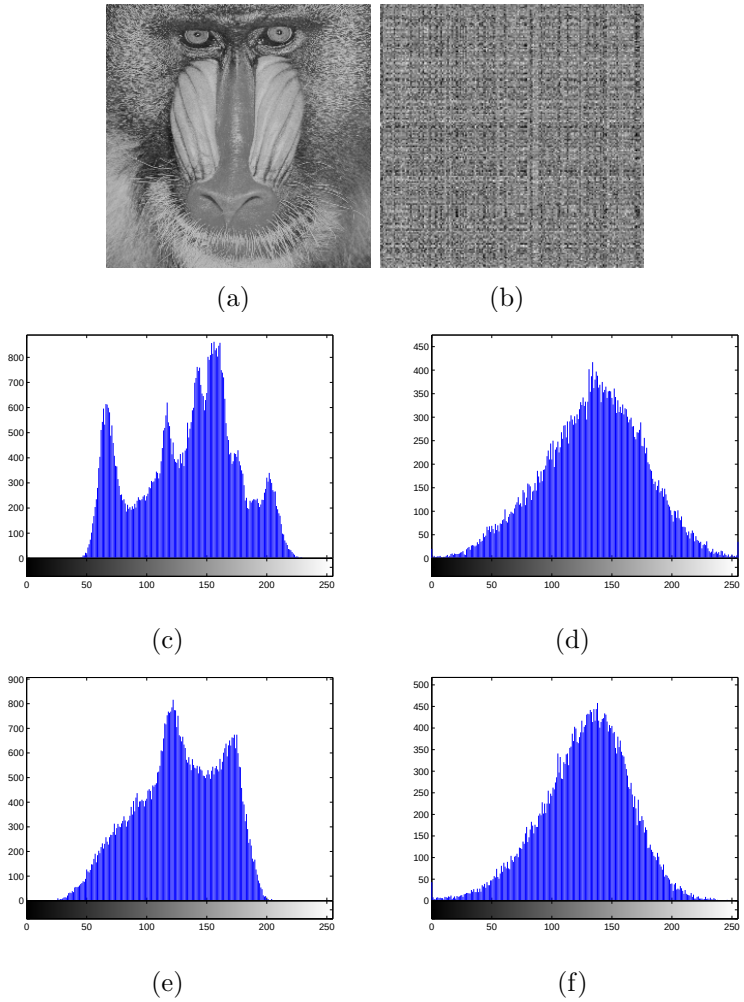


Fig. 3: (a) Baboon; (b) encrypted Baboon; (c) histogram of Lena; (d) histogram of encrypted Lena; (e) histogram of Baboon; (f) histogram of encrypted Baboon

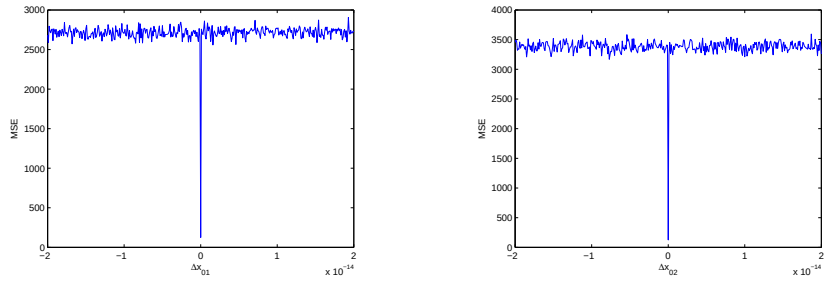
3.2 Key sensitivity analysis

To express the quality of the decrypted image, the mean square error (MSE) between the decrypted image and the original one is introduced as

$$\mathrm{MSE} = \frac{1}{L \times H} \sum ((I(x,y) - D(x,y))^2 \tag{7}$$

where $L \times H$ represents the total number of pixels of the image, $I(x,y)$ and $D(x,y)$ denote the values of the input image and the output image at the pixel, respectively.

Fig. 4(a) shows the MSE curve for x_{01} and Fig. 2(d) gives the decrypted image with correct x_{02} and incorrect $x_{01} = 0.11 + 10^{-16}$. It can be seen that the decrypted image cannot show any information of the original image even if a very small error x_{01} occurs. And the similar scenario happens to x_{02}. Thus the proposed algorithm is very sensitive to the keys.



(a) (b)

Fig. 4: (a) MSE curve for x_{01}; (b) MSE curve for x_{02}

3.3 Key space analysis

The encryption system should be secure even if everything except the key is known by eavesdropper. Hence, the key space should be large enough. In the proposed algorithm, x_{01} and x_{02} are used as keys. Here, the key space is calculated for x_{01} as:

Generate two different sequences λ and $\widetilde{\lambda}$ with length N by using x_{01} and $x_{01}+\Delta$ as initial values, define mean absolute error between two sequences as

$$\mathrm{MAE}(\lambda,\widetilde{\lambda})=\frac{1}{N}\sum|\lambda-\widetilde{\lambda}| \tag{8}$$

The key space for x_{01} is equal to $\frac{1}{\Delta_0}$, where Δ_0 is the value of Δ for $\mathrm{MAE}=0$. The simulation shows that Δ_0 comes out to be 1×10^{-17}, i.e., the key space of x_{01} or x_{02} is 1×10^{17}. Thus, the total key space is 1×10^{34}, which is very large. If one wants to construct the correct measurement matrices by exhausting the keys, he must calculate 10^{34} times which would take much time. While if he wants to exhaust all the 192×256 partial Hadamard matrices, he would try $A_{256}^2=(\frac{256!}{64!})^2$ times, which is a very huge number, thus the proposed algorithm can resist brute-force attack.

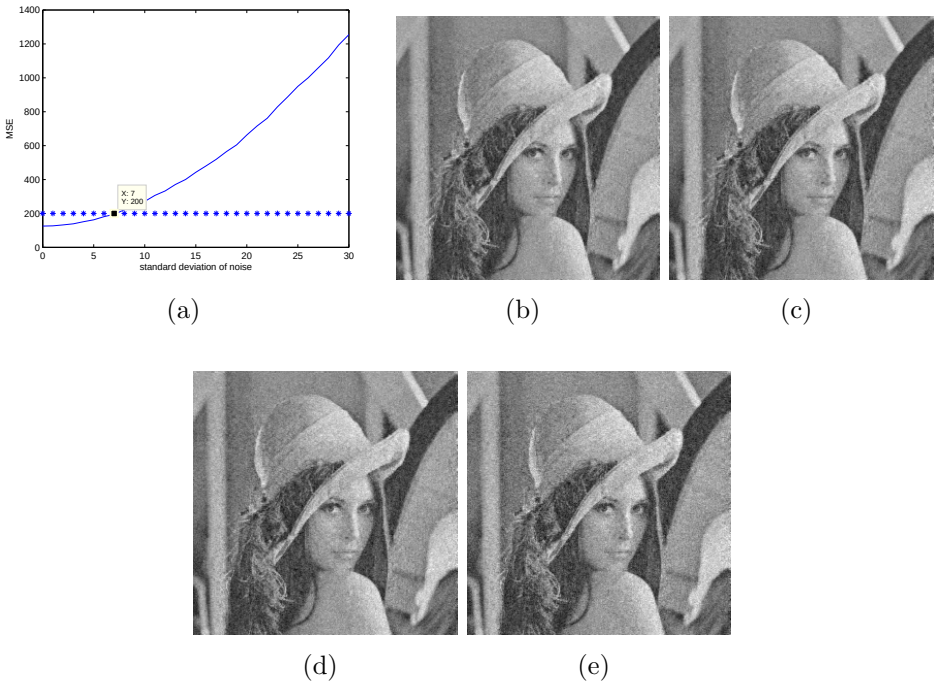
3.4 Noise attack

It is inevitable that the encrypted image would be impacted by noise at the stage of image processing and image transmission. The encrypted image is contaminated by noise as

$$C'=C+kG \tag{9}$$

where C' and C are the noisy encrypted image and the encrypted image, respectively. k indicates the the noise strength, and G is the white Gaussian noise with zero-mean and identity standard deviation.

The Gaussian noises with different noise strengths are added to the encrypted image, and the deviation of MSE versus noise strength is shown in Fig. 5(a). Fig. 5(b)–(e) show the decrypted images with $k=1$, 3, 5, and 7. It is easy to find that the decrypted images can still be recognized with some level of noise.



(a) (b) (c)

(d) (e)

Fig. 5: Result of noise attack: (a) MSE curve, (b)k=1 , (c) k=3, (d) k=5, (e) k=7

3.5 Chosen-plaintext attack

Assume the attacker has known Ψ, when he tries to attack the algorithm with the chosen-plaintext attack, i.e. β is set as $\mathbf{I}_{M\times M}$, where $\mathbf{I}_{M\times M}$ is a unit matrix, he obtains

$$y_{\mathbf{I}} = \Phi_2 \Phi_1^{\mathrm{T}} \tag{10}$$

Φ_i can be written as:

$$\Phi_i = \begin{pmatrix} \phi_{i1}^{\mathrm{T}} & \phi_{i2}^{\mathrm{T}} & \dots & \phi_{iM}^{\mathrm{T}} \end{pmatrix}^{\mathrm{T}}, \ i = 1, 2 \tag{11}$$

where ϕ_{ij} is one of the row vectors of Hadamard matrix of order N.

The measurement matrices are constructed as partial Hadamard matrices,

$$y_{\mathbf{I}} = \begin{pmatrix} \phi_{21}\phi_{11}^{\mathrm{T}} & \phi_{21}\phi_{12}^{\mathrm{T}} & \dots & \phi_{21}\phi_{1M}^{\mathrm{T}} \\ \phi_{22}\phi_{11}^{\mathrm{T}} & \phi_{22}\phi_{12}^{\mathrm{T}} & \dots & \phi_{22}\phi_{1M}^{\mathrm{T}} \\ \vdots & \vdots & \dots & \vdots \\ \phi_{2M}\phi_{11}^{\mathrm{T}} & \phi_{2M}\phi_{12}^{\mathrm{T}} & \dots & \phi_{2M}\phi_{1M}^{\mathrm{T}} \end{pmatrix} \tag{12}$$

since ϕ_{2a} and ϕ_{1b} both are ones of the row vectors of Hadamard matrix of order N,

$$\phi_{2a}\phi_{1b}^{\mathrm{T}} = \begin{cases} 0 & \phi_{1b} \neq \phi_{2a} \\ N & \phi_{1b} = \phi_{2a} \end{cases} \tag{13}$$

one cannot figure out ϕ_{1b} and ϕ_{2a}, that is to say, he cannot obtain Φ_1 and Φ_2. Thus the chosen plain-text attack is not effective.

4 Conclusion

An image compression-encryption algorithm based on 2-D compressive sensing is proposed, which can complete compression and encryption simultaneously. The measurement are performed in two directions. The algorithm is practical due to the measurement matrices are constructed as partial Hadamard matrices. The simulation results show that the proposed algorithm is resistant to statistical analysis and brute-force attack, robust against noise attacks and has the ability to resist the chosen-plaintext attack.

References

[1] Y. Liu, J. Lin, J. Fan and N. Zhou, Image encryption based on cat map and fractional Fourier transform, Journal of Computional Information Systems, 18 (2012) 7485–7492.

[2] L. Chen, A novel image encryption scheme based on Hyperchaotic sequences, Journal of Computational Information System, 10 (2012) 4159–4167.

[3] D.L. Donoho, Compressed sensing, IEEE Transactions on Information Theory, 52 (2006) 1289–1306.

[4] E.J. Cands, Compressive sampling, International Congress of Mathematicians, (2006) 1433–1452.

[5] 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, 2012.

[6] X. Zhang, Y. Ren, G. Feng and Z. Qian, Compressing encrypted image using compressive sensing, 2011 Seventh International Conference on Intelligent Information Hiding and Multimedias Signal Processing (IIH-MSP), (2011) 222–225.

[7] A. M. Abdulghani, E. Rodriguze-Villegas, Compressive sensing: from "compressing while sampling" to "compressing and securing while sampling", 32nd Annual International Conference on IEEE EMBS, (2010) 1127–1130.

[8] A. V. Sreedhanya and K. P. Soman, Secrecy of cryptography with compressed sensing, International Conference on Advances in Computing and Communications, (2012) 207–210.

[9] R. Huang, K. H. Rhee and S. Uchida, A parallel image encryption method based on compressive sensing, Multimedia Tools and Applications, (2012) 1–23.

[10] D. H. Gao, D. H. Liu, G. M. Shi and M. Gao, A robust image encryption scheme over wireless channels, International Conference on Wireless Communication & Signal Processing, (2009) 1–6.

[11] F. Aann, C. Albertina, J. N. Thomas and J. Bahram, Resistance of the double random phase encryption against various attacks, Optics Express, 15 (2007) 10253–10265.

[12] H. Mohimani, M. Babaie-Zadeh and C. Jutten, A fast approach for overcomplete sparse decomposition based on smoothed l0 norm, IEEE Transactions on Signal Processing, 57 (2009) 289–301.