Optica Applicata, Vol. XLVIII, No. 4, 2018
10.5277/oa180403

Image compression-encryption algorithm combining compressive sensing with log operation

Rong-Ling Chen, Ying Zhou, Ming Luo, Ai-Di Zhang, Li-Hua Gong*

Department of Electronic Information Engineering, Nanchang University,
Nanchang 330031, China

*Corresponding author: ncuglh@163.com

Based on compressive sensing and log operation, a new image compression-encryption algorithm is proposed, which accomplishes encryption and compression simultaneously. The proposed image compression-encryption algorithm takes advantage of not only the physical realizability of partial Hadamard matrix, but also the resistance of the chosen-plaintext attack since all the elements in the partial Hadamard matrix are 1, –1 or $\log 1 = 0$. The proposed algorithm is sensitive to the key and it can resist various common attacks. The simulation results verify the validity and reliability of the proposed image compression-encryption algorithm.

Keywords: image encryption, image compression, compressive sensing, log operation.

1. Introduction

Images provide a lot of information along with the development of network technology. While transmission channels are always insecure and bandwidth-constrained, so it is desired to transmit the data after encryption and compression. Recently, compressive sensing (CS) [1, 2] has been proposed as a new theory or tool. The theory has attracted much attention for its breakthrough in the traditional sampling methods. CS can accomplish sampling and compression at the same time compared with the traditional method. Because of the advantage of CS, it is of great significance that compressive sensing and image encryption algorithm are fused together to complete compression and encryption simultaneously. The secrecy properties of compressive sensing for noisy are covered in [3] and it was indicated that the inherent multidimensional projection perturbation feature made it hard to breach the privacy. Huimin Zhao and Yanmei Fang examined the security and robustness via compressive sensing based on a fingerprint watermarking signal and demonstrated that CS can provide an effective security of compression and encryption [4]. In 2017, an image encryption scheme was formulated, in which the parameters of the logistic map and the order of discrete fractional transform are the key to the image encryption algorithm [5]. Linfei Chen *et al*. took the six phase masks and the six diffraction distances as the key to the decryption process [6]. It was stated that the encryption matrix in compressive sensing based algorithms is perfectly secure if it can be seen as a one-time pad [7]. The security was investigated when eavesdroppers have no idea of the measurement matrix and a computational notion of secrecy was demonstrated [8]. Fucheng Yin *et al.* verified the effectiveness of the known plaintext attack with the dual random phase coding [9].

Some image encryption algorithms have been investigated since the potential capability of measurement matrix in CS. Compressive sensing was employed to lower the encryption data volume in an image encryption method based on double random-phase encoding due to the dimensional decrease properties of CS [10]. Kumar and Vaish compressed the image according to the importance of the image coefficients [11]. The original image was divided into blocks as one-dimensional vectors, and then the authors encrypted and compressed these vectors with CS and block Arnold scrambling [12]. Based on compressive sensing, Xinpeng Zhang *et al.* proposed an image encryption algorithm where they encrypted the original image by orthogonal transformation and then compressed by CS with a pseudo-random measurement matrix [13]. A concise pixel-permutation algorithm was used to reduce the encryption time [14]. Zhengjun Liu *et al.* adopted some physical parameters of optical system as the key to enhance the security of the color image encryption system [15]. Ponuma and Amutha put forward an image encryption scheme, where the keys depend on the input data and the initial parameters of the chaotic map [16]. In order to enhance the security of the image encryption system, Hamdi *et al.* realized multiple encryption of the image via three phases of confusion and diffusion [17], since CS-based encryption method alone fails to resist against the chosen-plaintext attack. Hence, the output of CS is again encrypted based on the multi-chaotic system [18]. A parallel image encryption method based on CS was proposed, where a block cipher structure consisting of scrambling, mixing, S-box and chaotic lattice XOR was designed to resist against the chosen-plaintext attack effectively [19]. Rawat *et al.* proposed a scheme where both compressive sensing and Arnold scrambling are employed to encrypt a digital image [20]. Nanrun Zhou *et al.* proposed a novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing, where the measurement matrices were constructed as partial Hadamard matrices [21]. Subsequently, Nanrun Zhou *et al.* introduced a new image compression-encryption scheme where the original image was compressed and encrypted simultaneously by measuring matrices in two directions [22]. Endra proposed a novel method of constructing optimized sensing matrix and exploited it to compress and encrypt images simultaneously [23]. Xingbin Liu *et al.* proposed a novel approach based on compressive sensing, where the source images were measured with the key-controlled pseudo-random measurement matrix constructed using logistic map to reduce the data and realizes the initial encryption [24]. Based on 2D compressive sensing and discrete fractional random transform (DFrRT) [25], an image compression-encryption scheme with simple operation was proposed, where the original image was measured by the measurement matrices in two orthogonal directions during the encryption process and the matrices were constructed with logistic map to control the row vectors of the Hadamard matrix [26]. In 2017, Guiqiang Hu *et al.* devised an image coding scheme, where the CS sampling and the CS reconstruction were performed in parallel [27].

Taking advantage of the facts that all the elements in the Hadamard matrix are 1 or –1 and log 1 = 0, we explore a new compression-encryption algorithm based on CS and log operation, which can encrypt and compress an image simultaneously and resist the so-called chosen-plaintext attack. The simulation results show that the proposed algorithm has good security and compression performance.

2. Image compression-encryption algorithm based on CS and log operation

The measurement matrix Φ is constructed as a partial Hadamard matrix and controlled by a logistic map. The logistic map is defined as:

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

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

The construction steps are as follows:

1) Generate a sequence of length $2N$ by logistic map with initial condition r, abandon the preceding N elements to obtain the index sequence $s = [s_1, s_2, ..., s_\mathrm{N}]$;

2) Sort the nature sequence $n = [1, 2, ..., N]$ with the index sequence s, note the sorted sequence as $p = [p_1, p_2, ..., p_\mathrm{N}]$, where $p_i \in [1, N]$;

3) Generate the Hadamard matrix H of order N, and choose the row vectors, $H(p_1, :)$, $H(p_2, :)$, ..., $H(p_\mathrm{M}, :)$, to group into the measurement matrix Φ, *i.e.*,

$$\Phi = \begin{bmatrix} H(p_1, :) \\ H(p_2, :) \\ \vdots \\ H(p_M, :) \end{bmatrix} \tag{2}$$

where $H(p_i, :)$ denotes the p_i-th row vector of H.

The proposed image compression-encryption algorithm is fitted to operate on the image whose length and width both are the multiples of 4 since the measurement matrix is constructed as a partial Hadamard matrix. The proposed image compression-encryption algorithm is illustrated in Fig. 1, and the image compression-encryption steps are as follows:

1) Extend x in the Ψ domain to obtain α.

2) Construct the measurement matrix Φ and measure α to obtain y. To enhance the security, not x but α is measured by Φ, *i.e.*,

$$y = \Phi\alpha = \Phi\Psi^\mathrm{T}x \tag{3}$$

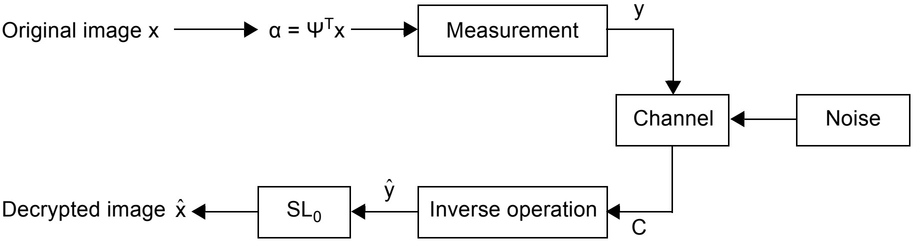


Fig. 1. Image compression-encryption algorithm.

It is equivalent to presume that $\Phi\Psi^{\mathrm{T}}$ is the measurement matrix, and the sensor matrix $\Theta = \Phi$. Thus the attacker needs both Φ and Ψ, or else he/she cannot reconstruct x even if α is available.

3) If $y(i,j) \neq 0$, perform the following operation on y to obtain the encrypted image C

$$C = \frac{\left(\frac{y}{|y|}\log|y| + K\right) \times 255}{2K} \tag{4}$$

where $|\cdot|$ denotes absolute value, and $K = \mathrm{ceil}[\max(y)]$; the function $\max(A)$ returns the largest element in A and the function $\mathrm{ceil}(A)$ rounds A to the nearest integer greater than or equal to A. The log operation is performed on the measurement to resist the chosen-plaintext attack since the elements in the measurement matrix are 1 or –1 and $\log 1 = 0$. And all the elements in y would be in [0, 255], which is the range of the pixel values of images.

Image $\hat{y}$ can be obtained by performing the inverse operation on the encrypted image

$$\hat{y} = \frac{2KC/255 - K}{|2KC/255 - K|} \times 10^{2KC/255 - K} \tag{5}$$

Then one can obtain the decryption image with the SL_0 algorithm [28].

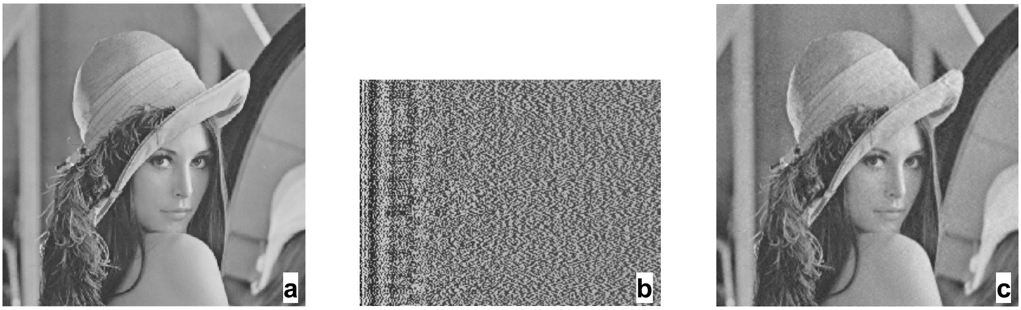


Fig. 2. *Lena* (**a**), encryption *Lena* (**b**), and decryption *Lena* (**c**).

3. Simulation and discussion

The gray image *Lena* with resolution 256 × 256 is served as the test image, which is shown in Fig. 2**a**. Without loss of generality, 2D DCT is adopted as Ψ and Φ are $M \times N$ ($M = 192$, $N = 256$) partial Hadamard matrices. The parameters r and μ in simulation are 0.11 and 3.99, respectively. The encrypted image is shown in Fig. 2**b**, and the corresponding decryption image is shown in Fig. 2**c**.

3.1. Performance of compression

To measure the quality of the decryption digital image, the peak-to-peak signal-to-noise ratio (PSNR) is used:

$$\mathrm{PSNR} = 10\log\frac{255^2}{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left[R(i,j)-I(i,j)\right]^2} \tag{6}$$

where $R(i,j)$ and $I(i,j)$ are the pixel values in the decryption image and the original one, respectively. The experimental results show that the quality of the decryption digital image is acceptable and the PSNR value is about 35.8940 dB. The results for different compression ratios are compiled in Table 1. The quality of the reconstructed image is acceptable to some degree even if the compression ratio is 4:1. And the compression performance would be better with the development of reconstruction algorithm in CS.

The PSNRs of the decryption images under different sampling ratios are shown in Table 2. It can be seen that the proposed scheme has a higher peak signal-to-noise ratio when the compression ratio is same. Therefore, the proposed image compression and encryption scheme has better compression performance.

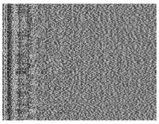
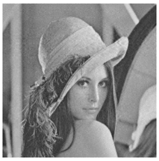
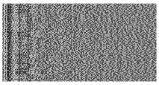
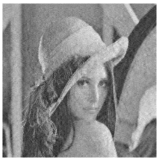
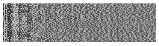
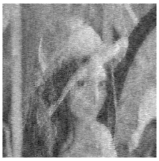
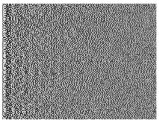
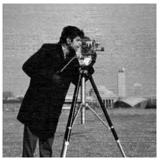
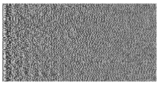
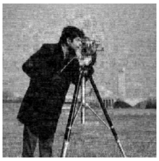
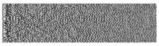
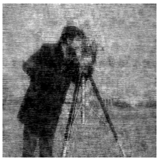
3.2. Statistical analysis

Statistically, the correlation of two adjacent pixels in a meaningful digital image is usually close to 1, while that of the encrypted image should be as little as possible or even close to 0. To measure the correlations of adjacent pixels, 16000 pairs of two adjacent pixels are selected randomly in horizontal, vertical and diagonal directions, respectively. The correlation coefficient can be obtained by

$$\mathrm{CC} = \frac{\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{N}(x_i-\bar{x})^2\sum_{i=1}^{N}(y_i-\bar{y})^2}} \tag{7}$$

where x_i and y_i represent two adjacent pixels value, the mean values $\bar{x}$ and $\bar{y}$ correspond to $\frac{1}{N}\sum_{i=1}^{N}x_i$ and $\frac{1}{N}\sum_{i=1}^{N}y_i$, respectively. The results are compiled in Table 3. It

T a b l e 1. The results of different compression ratios.

Compression ratio	Compressed and encrypted image	Decryption image	PSNR [dB]
4:3			35.8490
2:1			32.0432
4:1			29.7391
4:3			32.9292
2:1			30.2002
4:1			29.1040

can be seen that the proposed algorithm has a smaller correlation coefficient of the encryption image than that of the original image. Thus, the proposed image compression and encryption scheme has a good encryption property in terms of correlation.

T a b l e 2. PSNRs of the decryption images under different compression ratios.

Compression ratio	4:3	2:1	4:1
The proposed algorithm	35.8490	32.0432	29.7391
Ref. [22]	30.4936	24.8739	17.4172
Ref. [26]	30.6295	25.6473	17.4287

Table 3. Correlation coefficient.

	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Lena	0.9590	0.9217	0.9017
The proposed algorithm	0.0678	0.0557	0.0233
Ref. [26]	0.0909	0.2389	0.0126
Cameraman	0.9585	0.9346	0.9063
The proposed algorithm	0.0466	0.0226	0.0229
Ref. [26]	0.1284	0.2637	–0.0158

It is the best if the values in the histogram of the encrypted images are fairly uniformly distributed, or the histograms of the encrypted images corresponding to the different original images are similar to each other. Figures 3**a**–3**d** show the histograms of images *Lena*, encrypted *Lena*, *Cameraman* and encrypted *Cameraman*, respectively. The histograms of different original images are obviously different, while their encrypted images have similar histograms. After a large number of parallel experiments, it is found that the histograms of the encrypted images of different original images are also similar

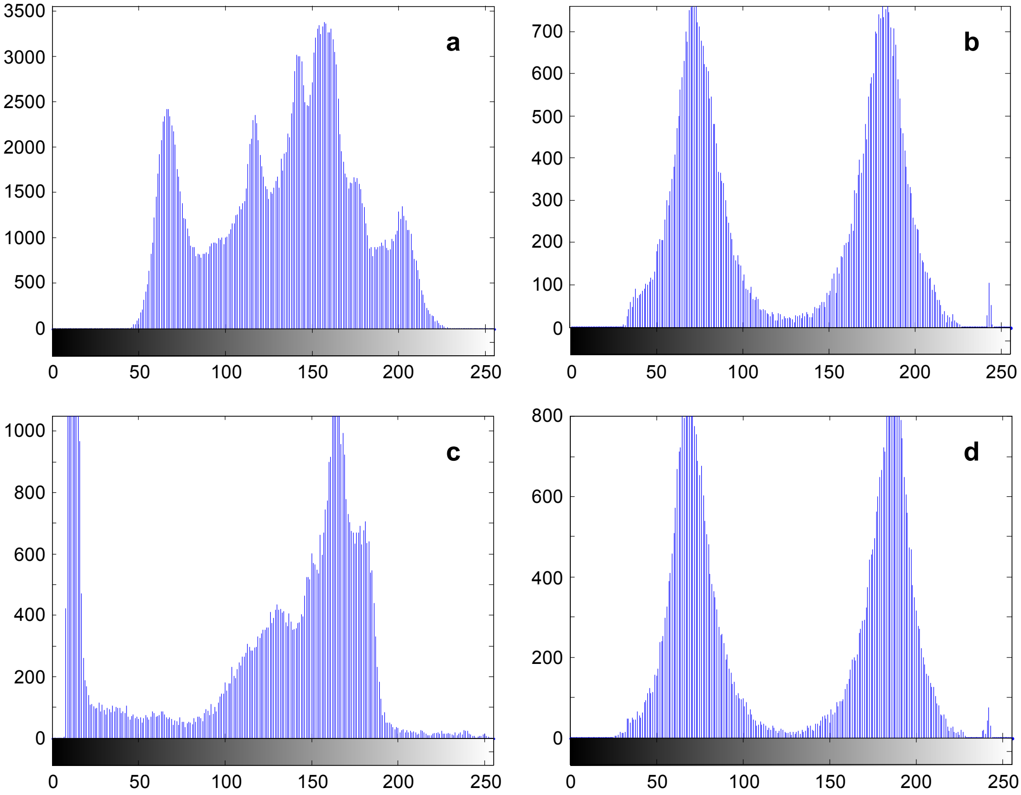


Fig. 3. Histograms: *Lena* (**a**), encrypted *Lena* (**b**), *Cameraman* (**c**), and encrypted *Cameraman* (**d**).

to Figs. 3**b** and 3**d**. That is to say, the proposed image compression and encryption algorithm can frustrate the statistical analysis attack.

3.3. Key sensitivity

The algorithm succeeds the sensitivity of logistic map to the initial value, thus it is very sensitive to the key. In order to evaluate the difference between the decryption image and the original image, the mean square error (MSE) between the decryption image and the original one is introduced as

$$\text{MSE} = \frac{1}{L \times H} \sum_{x,\,y} \Big[I(x,y) - D(x,y) \Big]^2 \tag{8}$$

where $L \times H$ represents the total number of pixels of the image, $I(x,y)$ and $D(x,y)$ denote the pixel values at point (x, y) of the input image and the output image, respectively. The larger MSE means the greater differences between the decryption image and the original image. Figure 4 shows the MSE curves for r. One can see that the MSE value is very large with a little deviation $\Delta = 1 \times 10^{-16}$ to r, and the MSE value is very small if and only if r is correct, thus the decryption image can only be recognized when the key is correct, *i.e.*, the proposed image encryption algorithm is sensitive enough to the key.

3.4. Noise attack

It is inevitable that the noises at the stage of image processing and image transmission would directly impact the quality of the decryption image. Suppose the encrypted image is contaminated by the noises as:

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

where C' and C are the noisy encrypted image and the intact original encrypted image, respectively, k is a coefficient related to the noise intensity, and G is the white Gaussian

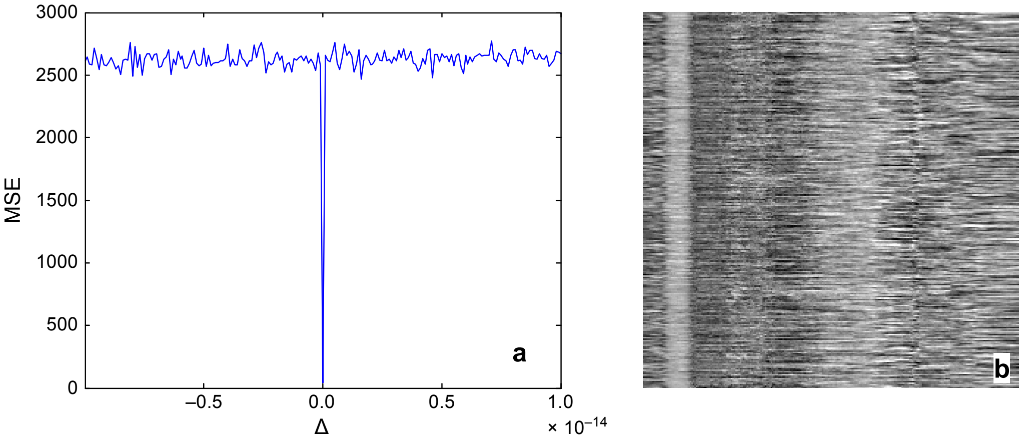


Fig. 4. MSE curve for the key (**a**), and decryption *Lena* with wrong $r = 0.11 + 10^{-16}$ (**b**).

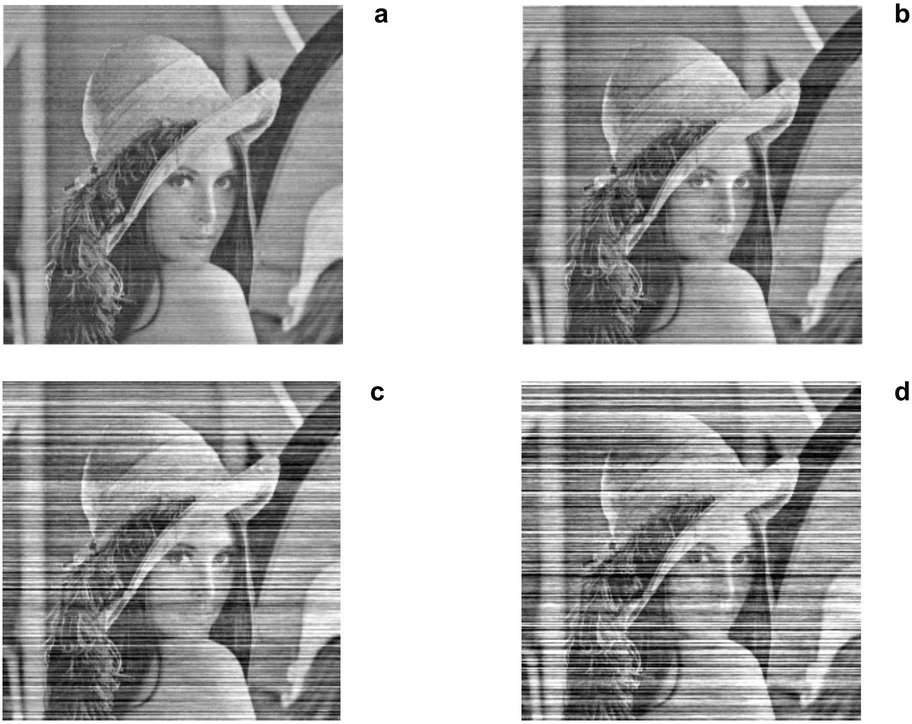


Fig. 5. The results of noise attacks with different noise strengths $k = 1$ (**a**), $k = 2$ (**b**), $k = 3$ (**c**), and $k = 4$ (**d**).

noise with zero-mean and identity standard deviation. The results of noise attacks with different noise intensities are shown in Fig. 5. The quality of the decryption images does not degrade too much and the decryption image from the contaminated encrypted image with $k = 4$ is still acceptable.

3.5. Chosen-plaintext attack

If an attacker knows the used algorithm and possesses a certain amount of plaintext information, the attacker can crack the correct key of a linear encryption system. Compressive sensing is a linear operation process, thus the attacker can obtain key information in the above case. Under the known compressive sensing theory, the attacker will choose a unit matrix as the original image, and then measure the unit matrix to generate a measurement matrix. Finally, the attacker *Eve* uses the measurement matrix to reconstruct the image which she wants to steal.

However, as for the proposed image compression and encryption algorithm, if the attacker Eve tries to attack the proposed algorithm with the chosen-plaintext attack, *i.e.*, α is set as $\mathbf{I}_{N \times N}$, which is an $N \times N$ unit matrix, then she would only obtain

$$y_{\mathbf{I}} = \left(\frac{\Phi}{|\Phi|} \log(\Phi) + K \right) \times 255/K \tag{10}$$

Since all the elements in Φ are 1 or –1, thus y_{I} is **0**, the attacker cannot obtain the correct measurement matrix to decrypt the image.

4. Conclusion

We propose an image compression-encryption algorithm by combining compressive sensing with log operation to implement compression and encryption operations simultaneously. The proposed algorithm is practical since the measurement is constructed as a partial Hadamard matrix, which is controlled by logistic map. The proposed algorithm can resist the chosen-plaintext attack by taking advantage of the fact that all the elements in measurement matrix are 1 or –1 and $\log 1 = 0$. We demonstrate the proposed image compression-encryption algorithm with high security and good compression performance with simulation results.

Acknowledgments – The work is supported by the National Natural Science Foundation of China (Grant No. 61462016), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), the Cultivation Plan of Applied Research of Jiangxi Province (Grant No. 20181BBE58022) and the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002).

References

[1] DONOHO D.L., *Compressed sensing*, IEEE Transactions on Information Theory 52(4), 2006, pp. 1289–1306.

[2] CANDES E.J., *Compressive sampling*, Marta Sanz Solé **17**(2), 2006, pp. 1433–1452.

[3] NANRUN ZHOU, AIDI ZHANG, JIANHUA WU, DONGJU PEI, YIXIAN YANG, *Novel hybrid image compression-encryption algorithm based on compressive sensing*, Optik 125(18), 2014, pp. 5075–5080.

[4] HUIMIN ZHAO, YANMEI FANG, *On the security and robustness with fingerprint watermarking signal via compressed sensing*, International Journal of Security and its Applications **9**(1), 2015, pp. 221–236.

[5] JING YU, YUAN LI, XINWEN XIE, NANRUN ZHOU, ZHIHONG ZHOU, *Image encryption algorithm by using the logistic map and discrete fractional angular transform*, Optica Applicata 47(1), 2017, pp. 141–155.

[6] LINFEI CHEN, GUOJUN CHANG, BINGYU HE, HAIDAN MAO, DAOMU ZHAO, *Optical image conversion and encryption by diffraction, phase retrieval algorithm and incoherent superposition*, Optics and Lasers in Engineering 88, 2017, pp. 221–232.

[7] DRORI I., *Compressed video sensing*, BMVA Symposium on Video **11**(4), 2008, pp. 1–2.

[8] CHAO WANG, DAPENG LIANG, *Secrecy of compressed sensing measurements*, Telecommunication Engineering, 2010.

[9] FUCHENG YIN, QI HE, ZHENGJUN LIU, *A known-plaintext attack on iterative random phase encoding in fractional Fourier domains*, Optica Applicata 47(1), 2017, pp. 131–139.

[10] PEI LU, ZHIYONG XU, XI LU, XIAOYONG LIU, *Digital image information encryption based on compressive sensing and double random-phase encoding technique*, Optik 124(16), 2013, pp. 2514–2518.

[11] KUMAR M., VAISH A., *An efficient encryption-then-compression technique for encrypted images using SVD*, Digital Signal Processing 60, 2017, pp. 81–89.

[12] NANRUN ZHOU, HAOLIN LI, DI WANG, SHUMIN PAN, ZHIHONG ZHOU, *Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform*, Optics Communications 343, 2015, pp. 10–21.

[13] XINPENG ZHANG, YANLI REN, GUORUI FENG, ZHENXING QIAN, *Compressing encrypted image using compressive sensing*, 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE Computer Society, 2011, pp. 222–225.

[14] Xiaowei Li, Dan Xiao, Qiong-Hua Wang, *Error-free holographic frames encryption with CA pixel -permutation encoding algorithm*, Optics and Lasers in Engineering 100, 2018, pp. 200–207.

[15] Zhengjun Liu, Cheng Guo, Jiubin Tan, Wei Liu, Jingjing Wu, Qun Wu, Liqiang Pan, Shutian Liu, *Securing color image by using phase-only encoding in Fresnel domains*, Optics and Lasers in Engineering 68, 2015, pp. 87–92.

[16] Ponuma R., Amutha R., *Compressive sensing based image compression-encryption using novel 1D-chaotic map*, Multimedia Tools and Applications 77(15), 2018, pp. 19209–19234.

[17] Hamdi M., Rhouma R., Belghith S., *A selective compression-encryption of images based on SPIHT coding and Chirikov standard map*, Signal Processing 131, 2017, pp. 514–526.

[18] Mahmood M.K., Shehab J.N., *Image encryption and compression based on compressive sensing and chaos*, International Journal of Computer Engineering and Technology **5**(1), 2014, pp. 68–84.

[19] Huang R., Rhee K.H., Uchida S., *A parallel image encryption method based on compressive sensing*, Multimedia Tools and Applications 72(1), 2014, pp. 71–93.

[20] Rawat N., Kim B., Kumar R., *Fast compressive sensing based digital image encryption technique using structurally random matrices and Arnold transform*, Optik **127**(4), 2016, pp. 2282–2286.

[21] Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong, *Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing*, Optics and Laser Technology 62, 2014, pp. 152–160.

[22] Nanrun Zhou, Shumin Pan, Shan Cheng, Zhihong Zhou, *Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing*, Optics and Laser Technology 82, 2016, pp. 121–133.

[23] Endra R.S., *Compressive sensing-based image encryption with optimized sensing matrix*, 2013 IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM), IEEE, 2014, pp. 122–125.

[24] Xingbin Liu, Wenbo Mei, Huiqian Du, *Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos*, Optics Communications 366, 2016, pp. 22–32.

[25] Liansheng Sui, Haiwei Lu, Zhanmin Wang, Qindong Sun, *Double-image encryption using discrete fractional random transform and logistic maps*, Optics and Lasers in Engineering 56, 2014, pp. 1–12.

[26] Juan Deng, Shu Zhao, Yan Wang, Lei Wang, Hong Wang, Hong Sha, *Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform*, Multimedia Tools and Applications 76(7), 2017, pp. 10097–10117.

[27] Guiqiang Hu, Di Xiao, Yong Wang, Tao Xiang, *An image coding scheme using parallel compressive sensing for simultaneous compression-encryption applications*, Journal of Visual Communication and Image Representation 44, 2017, pp. 116–127.

[28] Mghimani H., Babaie-Zadeh M., Jutten C., *A fast approach for overcomplete sparse decomposition based on smoothed ℓ^0 norm*, IEEE Transactions on Signal Processing 57(1), 2009, pp. 289–301.

Received November 20, 2017
in revised form January 28, 2018