Optica Applicata, Vol. XLIX, No. 3, 2019
DOI: 10.5277/oa190308

Image compression and encryption algorithm with wavelet-transform-based 2D compressive sensing

JING-HUI FAN, XIAN-BAO LIU, YAN-BIN CHEN*

School of Information Engineering, Nanchang University,
Nanchang 330031, China

*Corresponding author: 184389774@qq.com

By combining a wavelet transform with chaos scrambling, an image compression and encryption algorithm based on 2D compressive sensing is designed. The wavelet transform is employed to obtain the sparse representation of a plaintext image. The sparse image is measured in two orthogonal directions by compressive sensing. Then, the result of 2D compressive sensing is confused by the Arnold transform and the random pixel scrambling. The combination of four-dimensional chaos and logistic map is exploited to generate the first row of the key-controlled circulant matrix. The proposed algorithm not only carries out image compression and encryption simultaneously, but also reduces the consumption of the key by controlling the generation of measurement matrix. Experimental results reveal that the proposed image compression and encryption algorithm is resistant to noise attacks with good compression performance and high key sensitivity.

Keywords: wavelet transform, compressive sensing, chaos scrambling, image encryption, image compression.

1. Introduction

The conversion between continuous-time signals and discrete-time signals is based on the set of the Nyquist sampling theorem proposed in the 20th century. This theorem indicates that the sampled signal could be perfectly reconstructed at a sampling rate greater than twice of the maximum frequency of the original low-pass signal. Besides, the sampling result requires more bandwidth during transmission. At the same time, many significant sampled data would be discarded during compression, which may result in the failure of signal reconstruction.

In 2006, DONOHO and CANDÈS *et al.* first proposed the concept of compressive sensing (CS) [1–3]. In compressive sensing, the non-adaptive linear projection of the original signal is measured to produce the measurement values. Then, an effective reconstruction algorithm is utilized to recover the original signal from the measurement values [1].

The CS theory indicates that a signal can be perfectly reconstructed even after low speed sampling, which successfully broke through the limitation of Nyquist sampling theorem.

With the development of information technology, information security has attracted more and more attention. In 2008, ORSDEMIR *et al.* provided a systematic exposition of information security about CS in both theoretical and application security by considering the security and the robustness of the CS-based encryption algorithm [4].

In 2009, DAN-HUA LIU *et al.* designed an image encryption algorithm by regarding a Gaussian random measurement matrix as the key, which exploits the fact that sparse signals in CS can recover from few incompletely sampled signals [5]. GESEN ZHANG *et al.* utilized a sparse random measurement matrix and presented an image encryption scheme based on compressive sensing [6]. In 2011, a compression and encryption algorithm was introduced, where the quality of the reconstructed image depends on the compression rate and the smoothness of the original image [7]. To overcome the problem of large secret key consumption, AIDI ZHANG *et al.* proposed a color image encryption scheme by combining CS with the Arnold transform [8]. Subsequently, NANRUN ZHOU *et al.* designed a hybrid image encryption algorithm using a key-controlled measurement matrix, which greatly reduces the key consumption and increases the key space [9]. LIANSHENG SUI *et al.* designed a series of optical image encryption schemes based on a gyrator transform, which can be implemented easily [10–12].

Many image encryption algorithms were presented by combining CS with other encryption methods such as cascaded chaotic maps [13], linear feedback shift register [14] and double random-phase encoding [15]. Chaos is widely applied to cryptosystems due to their high sensitivity to the initial parameters [16–19]. In 2016, YUSHU ZHANG *et al.* investigated the basic framework designs and the corresponding analyses of image cipher based on chaos and CS, optics and CS or based on chaos, optics and CS [20]. Obviously, the combination of CS and chaotic systems will be a promising research focus.

A novel image compression and encryption algorithm based on an orthogonal wavelet basis and key-controlled measurement matrix is designed for larger key space and higher key sensitivity by using the coupled system of four-dimensional chaos and logistic map.

2. Image compression and encryption algorithm

First, the plaintext image is divided into four blocks and then the four blocks are extended in a discrete wavelet transform, respectively [21]. Four sets of chaotic sequences are generated by the four-dimensional chaotic system. Usually, the first 500 data should be discarded to avoid the transient nature of the chaotic system. Next, four cyclic matrices are constructed by a chaotic map to represent the measurement matrices for sampling [22]. Finally, the four subimages are combined into an image in the original order and then the resulting image is confused by the Arnold transform and random pixel scrambling to obtain the ciphertext image.

2.1. Encryption process

Step 1: Plaintext image **I** is divided into four subimages $\mathbf{I}_1$, $\mathbf{I}_2$, $\mathbf{I}_3$, $\mathbf{I}_4$.

Step 2: Four sparse images $\mathbf{S}_1$, $\mathbf{S}_2$, $\mathbf{S}_3$, $\mathbf{S}_4$ are produced by performing the wavelet transform on $\mathbf{I}_1$, $\mathbf{I}_2$, $\mathbf{I}_3$, $\mathbf{I}_4$, respectively.

Step 3: Eight chaotic sequences are generated by the coupled system of four-dimensional chaos and logistic map, then the eight chaotic sequences are utilized to build the corresponding cyclic matrices as the measurement matrices $\mathbf{\Phi}_1$, $\mathbf{\Phi}_2$, ..., $\mathbf{\Phi}_8$, respectively.

The four-dimensional chaotic system is [23]:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) - x_1 x_3 x_4 + u \\ \dot{x}_3 = -c x_3 + x_1 x_2 x_4 \\ \dot{x}_4 = -d x_4 + x_1 x_2 x_3 \end{cases} \tag{1}$$

If the parameters a, b, c, d and u are taking 35, 10, 1, 10 and 8, respectively, then the four-dimensional chaotic system will present a good chaos phenomenon. The cyclic matrix is given as

$$\begin{cases} \mathbf{Q}(i, 1) = \lambda\,\mathbf{Q}(i-1, N) \\ \mathbf{Q}(i, 2:N) = \mathbf{Q}(i-1, 1:N-1) \end{cases} \tag{2}$$

where $\lambda > 1$.

Step 4: Sparse images $\mathbf{S}_1$, $\mathbf{S}_2$, $\mathbf{S}_3$, $\mathbf{S}_4$ are measured by $\mathbf{\Phi}_1$, $\mathbf{\Phi}_2$, ..., $\mathbf{\Phi}_8$, respectively, to obtain four measurements $\mathbf{Y}_1$, $\mathbf{Y}_2$, $\mathbf{Y}_3$, $\mathbf{Y}_4$ according to following equations:

$$\begin{cases} \mathbf{Y}_1 = \mathbf{\Phi}_1 \mathbf{S}_1 \mathbf{\Phi}_2 \\ \mathbf{Y}_2 = \mathbf{\Phi}_3 \mathbf{S}_2 \mathbf{\Phi}_4 \\ \mathbf{Y}_3 = \mathbf{\Phi}_5 \mathbf{S}_3 \mathbf{\Phi}_6 \\ \mathbf{Y}_4 = \mathbf{\Phi}_7 \mathbf{S}_4 \mathbf{\Phi}_8 \end{cases} \tag{3}$$

and then $\mathbf{Y}_1$, $\mathbf{Y}_2$, $\mathbf{Y}_3$, $\mathbf{Y}_4$ are combined into an image **P**.

Step 5: The encryption image **K** is generated by performing the Arnold transform on image **P** with l times.

Step 6: Logistic map is employed to obtain an array **h** of length $m + n$, then the first m elements in **h** are intercepted as an array $\mathbf{h}_1$ and the last n elements in **h** are intercepted as an array $\mathbf{h}_2$.

Two random sequences $\mathbf{r} = [r_1, r_2, ..., r_m]$ and $\mathbf{d} = [d_1, d_2, ..., d_n]$ are constructed according to the ascending order of $\mathbf{h}_1$ and $\mathbf{h}_2$, respectively. Finally, the ciphertext image $\mathbf{K}'$ is produced by random pixel scrambling,

$$\mathbf{K}'(i, j) = \mathbf{K}(r_i, d_j) \tag{4}$$

where $1 \le i \le m$, and $1 \le j \le n$.

2.2. Decryption process

Step 1: The randomly scrambled pixels are restored as follows:

$$\mathbf{H}(r_i, d_j) = \mathbf{K}'(i, j) \tag{5}$$

where $1 \le i \le m$, and $1 \le j \le n$.

Step 2: Resulting image $\mathbf{P}'$ is produced by adopting the Arnold transform on the encryption image $\mathbf{H}$.

Step 3: Resulting image $\mathbf{P}'$ is divided into the four subimages $\mathbf{C}_1$, $\mathbf{C}_2$, $\mathbf{C}_3$, $\mathbf{C}_4$.

Step 4: $\mathbf{C}_v$ $(1 \le v \le 4)$ is processed by the NSL$_0$ algorithm to generate $\mathbf{R}_v$ $(1 \le v \le 4)$.

Step 5: With the inverse wavelet transform on $\mathbf{R}_v$ $(1 \le v \le 4)$, $\mathbf{I}_1'$, $\mathbf{I}_2'$, $\mathbf{I}_3'$, $\mathbf{I}_4'$ are reconstructed, respectively.

Step 6: $\mathbf{I}_1'$, $\mathbf{I}_2'$, $\mathbf{I}_3'$, $\mathbf{I}_4'$ are combined into an image $\mathbf{I}'$ in the original order.

3. Algorithm analysis

3.1. Key sensitivity and key space

The four initial values k_1, k_2, k_3, k_4 of the coupled system of four-dimensional chaos and logistic map are the main keys of the proposed image compression and encryption algorithm. Besides, the initial state k_5 of random pixel scrambling is also regarded as the main key.

The secondary key, *i.e.*, l is the number of Arnold transforms executed.

The gray images *Peppers* and *Cameraman* with resolution 256 × 256 are selected as the plaintext images in the experiment. The parameters are set to $l = 6$, $k_1 = 0.05$, $k_2 = 0.23$, $k_3 = 3.24$, $k_4 = 13.7$ and $k_5 = 0.22$.

We performed experiments in the case that one of the secret keys was slightly changed while the others remain unchanged. Simulation results are shown in Fig 1. Obviously, the decryption image is cluttered as long as any one of secret keys undergoes a tiny perturbation. Attackers cannot capture any useful information about the original image from Fig 1. Figure 2 exhibits the encryption image and the corresponding decryption image with the correct secret keys.

The mean square error (MSE) [24] is employed to evaluate the quality of the decryption image. The MSE value between the decryption image and the corresponding original image is calculated and displayed in Fig 3. From Fig 3, one can see that a little change in the secret keys will result in a mutation in the MSE value. Figure 4 shows the same regularity. Thus, the proposed image compression and encryption algorithm is highly sensitive to the key.

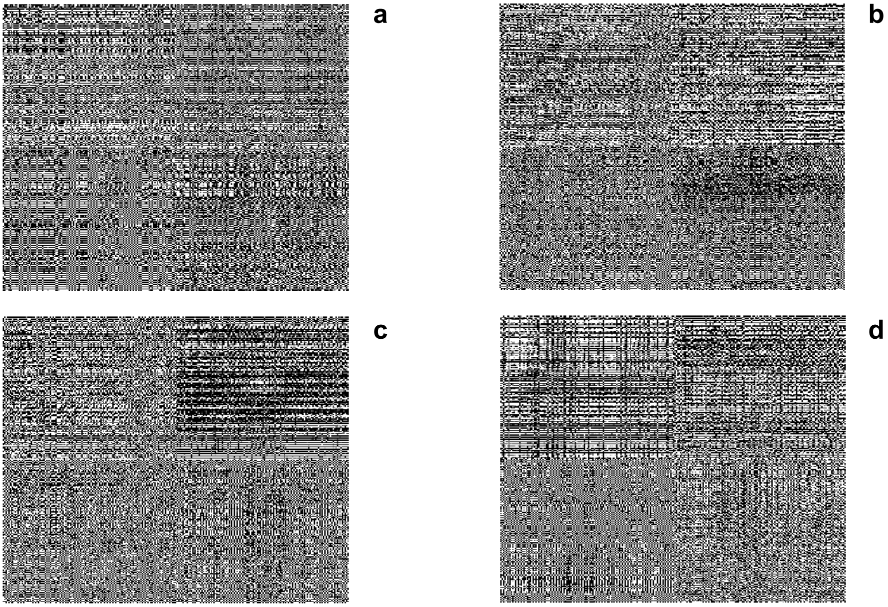


Fig. 1. Error decryption image *Peppers*: $k_1 = 0.05 \times 10^{-15}$ (**a**), $k_2 = 0.23 \times 10^{-15}$ (**b**), $k_3 = 3.24 \times 10^{-15}$ (**c**), and $k_4 = 13.7 \times 10^{-15}$ (**d**).

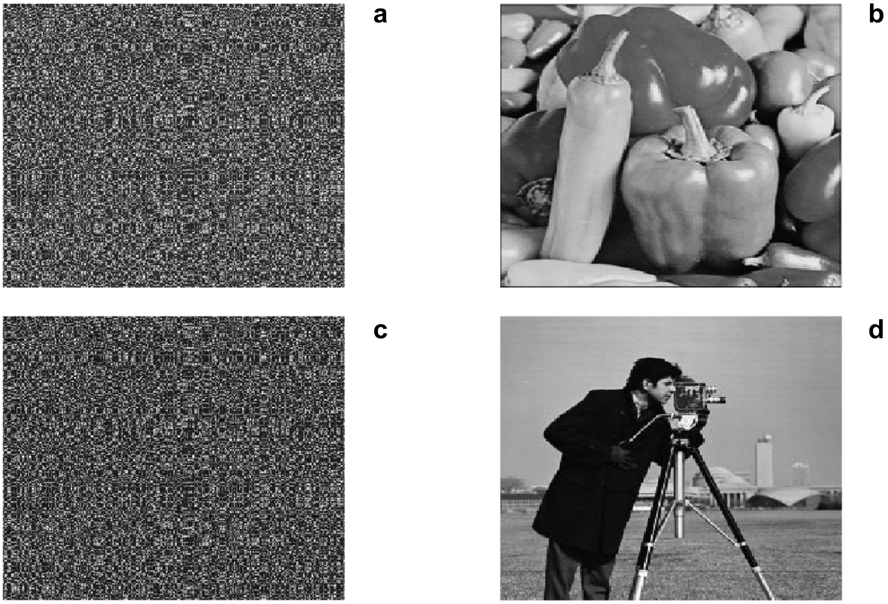


Fig. 2. Test result: encryption image *Peppers* (**a**), correct decryption image *Peppers* (**b**), encryption image *Cameraman* (**c**), correct decryption image *Cameraman* (**d**).

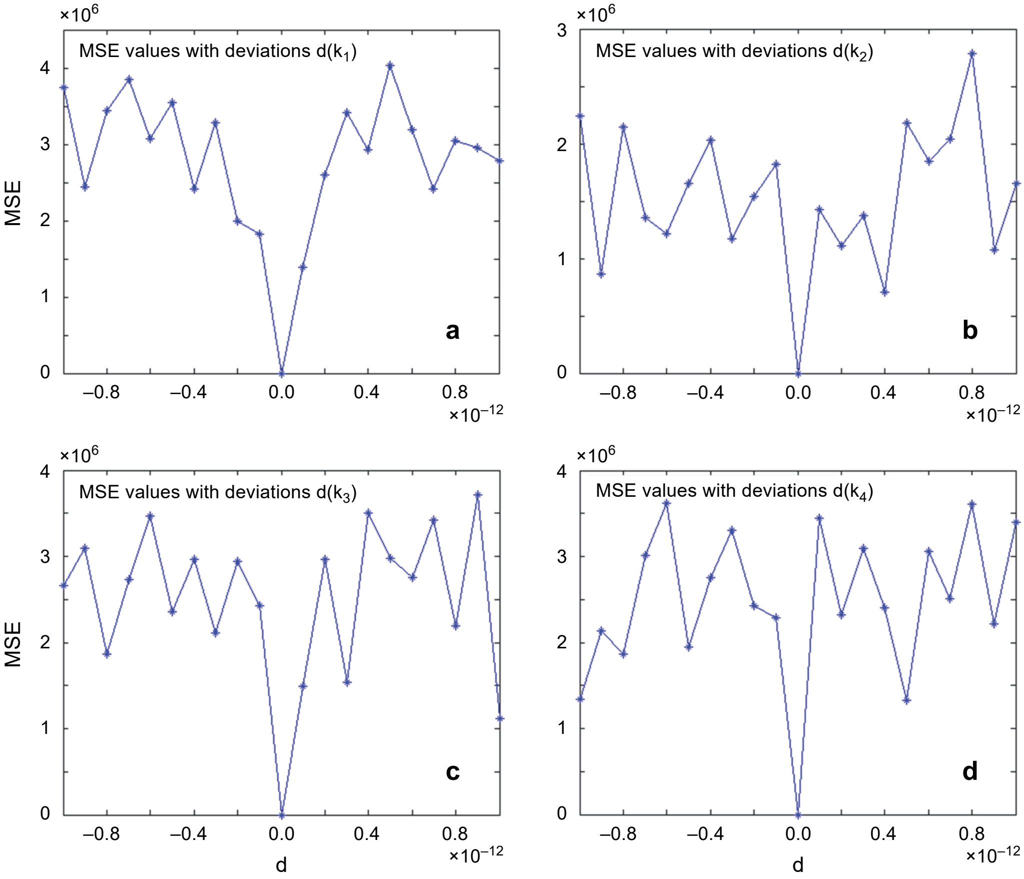


Fig. 3. MSE curves: k_1 (**a**), k_2 (**b**), k_3 (**c**), and k_4 (**d**).

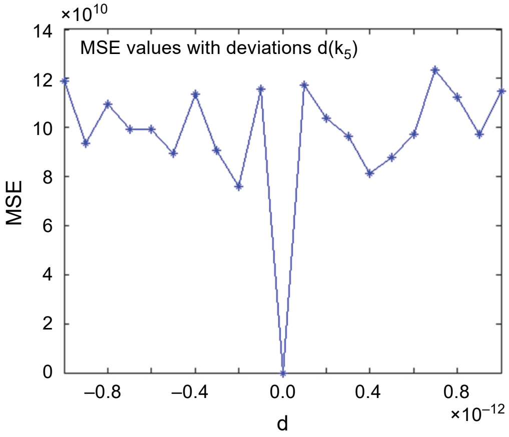


Fig. 4. MSE curves for k_5.

Table 1. Comparison of key space.

Algorithm	Proposed algorithm	Algorithm in [25]	Algorithm in [26]	Algorithm in [27]
Key space	$\geq 10^{83}$ (2^{275})	$\leq 2^{96}$	$\approx 2^{200}$	10^{48}

According to the simulation results, the key space of k_i $(1 \leq i \leq 4)$ is approximately 10^{15} while the key space of k_5 is about 10^{13}. Therefore, the value of the key space is

$$S = \sum_{i}^{5} k_i \geq 10^{73} \tag{6}$$

As shown in Table 1, the proposed image compression and encryption algorithm has larger key space than the image encryption schemes in [25–27]. It is clear that the key space is sufficient to resist the brute-force attack.

3.2. Statistical analysis

A common method to evaluate the performance of image encryption algorithms is gray-scale histogram analysis.

If the gray-scale histogram of an encryption image with an algorithm is evenly distributed or the encryption images of different original images have similar gray-scale histograms, then it can be said that the cryptosystem is secure against the histogram attack. As shown in Figs. 5 and 6, the gray-scale histograms of encryption images *Cameraman* and *Peppers* are very similar while the histograms of the corresponding original images show completely different distributions. In addition, a series of parallel

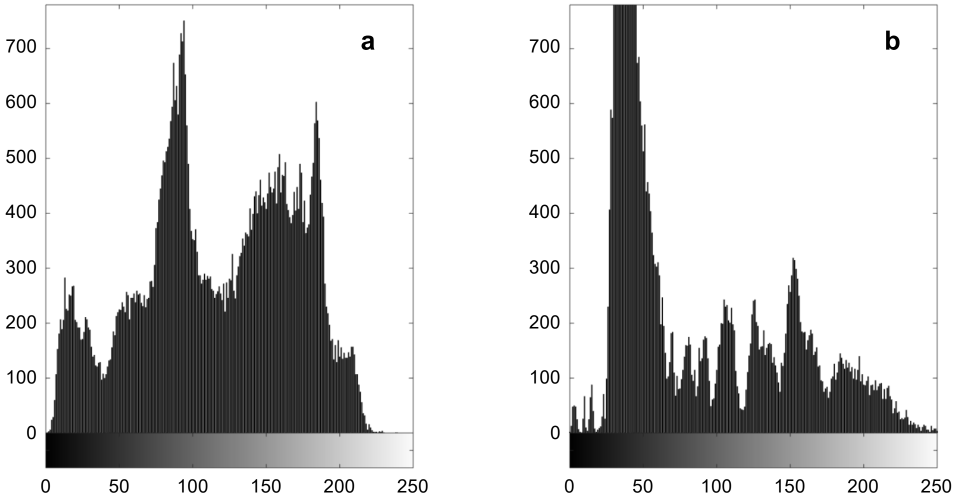


Fig. 5. Gray-scale histogram: *Peppers* (**a**), and encryption *Peppers* (**b**).

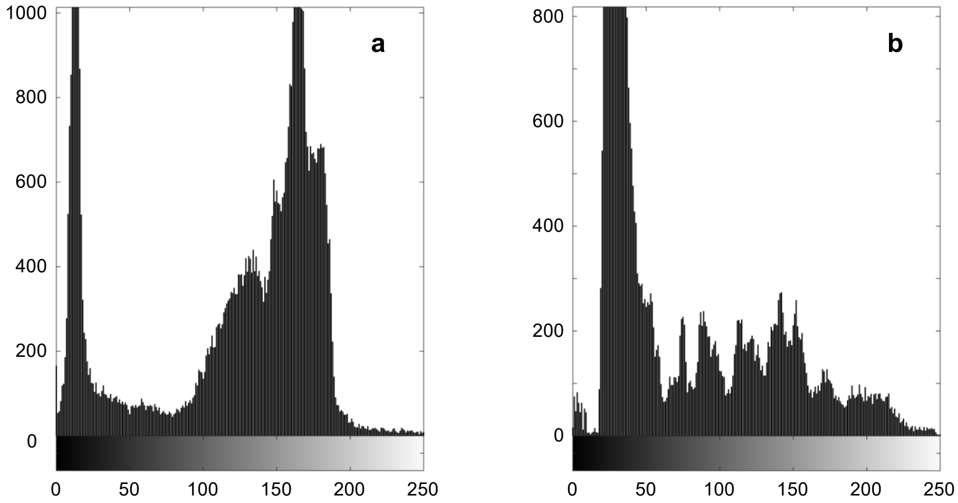


Fig. 6. Gray-scale histogram: *Cameraman* (**a**), and encryption *Cameraman* (**b**).

experiments show the same characteristics. This indicates that the proposed image compression and encryption algorithm is effective, and it is difficult for the attackers to obtain beneficial information by analyzing the gray-scale histograms.

A qualified cryptosystem is generally considered to be able to eliminate the strong correlation between the adjacent pixels of the original image.

Table 2. Correlation coefficient of adjacent pixels.

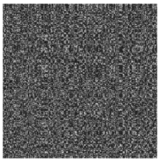
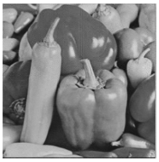
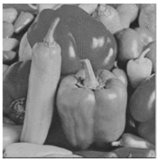
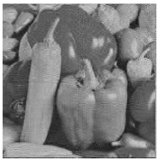
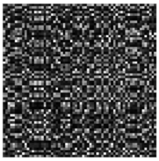
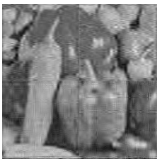
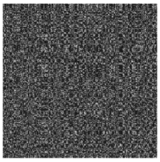
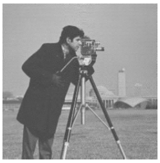
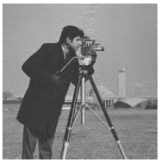
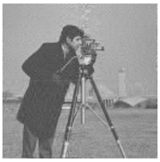
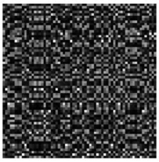
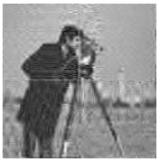
Image	Horizontal direction	Vertical direction	Diagonal direction
Peppers/encryption *Peppers*	0.9687/–0.0459	0.9628/–0.0235	0.9323/0.0125
Cameraman/encryption *Cameraman*	0.9722/–0.0375	0.9467/–0.0340	0.9164/–0.0019

By comparing the coefficients of correlation between the original image and the corresponding encryption image in the horizontal, vertical and diagonal directions as shown in Table 2, one can find that the proposed image compression and encryption algorithm can greatly weaken the correlation between the adjacent pixels of the original image. This makes it impossible for an unauthorized user to infer the information about the original image.

3.3. Compression ratio analysis

Table 3 lists the peak-signal-to-noise-ratio (PSNR) [28] values with different compression ratios of the proposed image compression and encryption algorithm. When the compression ratio is 6.25%, the decryption image is still discernible and retains most of the features of the original image. Thus, the proposed image compression and en-

T a b l e 3. Image compression ratio analysis.

Original image	Compression ratio	Encrypted and compressed image	Decryption image	PSNR [dB]
	75%			31.1337
	50%			28.1680
	25%			25.0493
	6.25%			22.3369
	75%			27.2663
	50%			25.3169
	25%			23.2224
	6.25%			20.6876

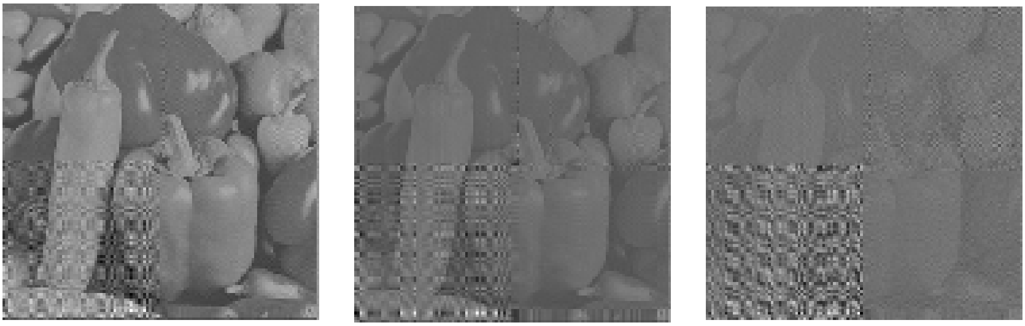


Fig. 7. Image *Peppers* recovered from Gaussian noise pollution.

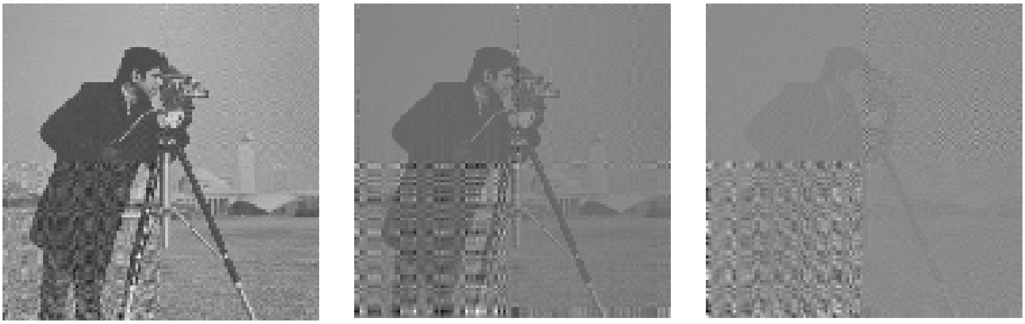


Fig. 8. Image *Cameraman* recovered from Gaussian noise pollution.

cryption algorithm has a good compression performance, which is helpful for storage or transmission.

3.4. Noise attack analysis

Considering that images are vulnerable to noise interference during processing, transmission, and storage, a good image encryption scheme should have a strong anti-jamming capability. When the encryption images *Peppers* and *Cameraman* are added with Gaussian noise with the mean and the standard deviation being $\mu_1 = 10^4$, $\delta_1 = 10^3$ or $\mu_2 = 10^5$, $\delta_2 = 10^3$ or $\mu_3 = 10^5$, $\delta_3 = 10^4$ during transmission, respectively, the decryption images are shown in Figs. 7 and 8. It demonstrates that the proposed image compression and encryption algorithm has a high anti-noise ability.

4. Conclusion

A new image encryption-compression algorithm based on an orthogonal wavelet basis and measurement matrix is proposed. The proposed algorithm dramatically reduces the key consumption by controlling the generation of measurement matrix while implementing image compression and encryption simultaneously. Due to the introduction of chaotic system, the sensitivity of the key is extremely high. The key space is large enough to resist the brute-force attack and the correlation between adjacent pixels in the ciphertext image is low. The security analyses verified that the proposed image compression and encryption algorithm can effectively resist statistical attack and noise attack. All in all, the proposed algorithm performs well in compression and security.

Acknowledgments – This work is supported by the National Natural Science Foundation of China (grant Nos. 61861029 and 61462061), 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, DOI: 10.1109/TIT.2006.871582.

[2] Candès E.J., Romberg J., Tao T., *Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information*, IEEE Transactions on Information Theory **52**(2), 2006, pp. 489–509, DOI: 10.1109/TIT.2005.862083.

[3] Baraniuk R.G., *Compressive sensing*, IEEE Signal Processing Magazine **24**(4), 2007, pp. 118–121, DOI: 10.1109/MSP.2007.4286571.

[4] Orsdemir A., Altun H.O., Sharma G., Bocko M.F., *On the security and robustness of encryption via compressed sensing*, [In] *MILCOM 2008 – 2008 IEEE Military Communications Conference*, 2008, pp. 1–7, DOI: 10.1109/MILCOM.2008.4753187.

[5] Dan-hua Liu, Guang-ming Shi, Da-hua Gao, Min Gao, *A robust image encryption scheme over wireless channels*, [In] *2009 International Conference on Wireless Communications & Signal Processing*, 2009, pp. 1–6, DOI: 10.1109/WCSP.2009.5371631.

[6] Gesen Zhang, Shuhong Jiao, Xiaoli Xu, *Application of compressed sensing for secure image coding*, [In] *Wireless Algorithms, Systems, and Applications, WASA 2010, Lecture Notes in Computer Science*, Pandurangan G., Anil Kumar V.S., Ming G., Liu Y., Li Y. [Eds.], Vol. 6221, Springer, Berlin, Heidelberg, 2010, pp. 220–224, DOI: 10.1007/978-3-642-14654-1_27.

[7] Xinpeng Zhang, Yanli Ren, Guorui Feng, Zhenxing Qian, *Compressing encrypted image using compressive sensing*, [In] *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2011, pp. 222–225, DOI: 10.1109/IIHMSP.2011.12.

[8] Aidi Zhang, Nanrun Zhou, Lihua Gong, *Color image encryption algorithm combining compressive sensing with Arnold transform*, Journal of Computers **8**(11), 2013, pp. 2857–2863, DOI: 10.4304/jcp.8.11.2857-2863.

[9] 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, DOI: 10.1016/j.optlastec.2014.02.015.

[10] Liansheng Sui, Minjie Xu, Ailing Tian, *Optical noise-free image encryption based on quick response code and high dimension chaotic system in gyrator transform domain*, Optics and Lasers in Engineering **91**, 2017, pp. 106–114, DOI: 10.1016/j.optlaseng.2016.11.017.

[11] Liansheng Sui, Bei Zhou, Zhanmin Wang, Ailing Tian, *An optical color image watermarking scheme by using compressive sensing with human visual characteristics in gyrator domain*, Optics and Lasers in Engineering **92**, 2017, pp. 85–93, DOI: 10.1016/j.optlaseng.2017.01.003.

[12] Liansheng Sui, Xiao Zhang, Ailing Tian, *Optical multiple-image authentication scheme based on the phase retrieval algorithm in gyrator domain*, Journal of Optics **19**(5), 2017, article ID 055702, DOI: 10.1088/2040-8986/aa6506.

[13] Yushu Zhang, Jiantao Zhou, Fei Chen, Leo Yu Zhang, Di Xiao, Bin Chen, Xiaofeng Liao, *A block compressive sensing based scalable encryption framework for protecting significant image regions*, International Journal of Bifurcation and Chaos **26**(11), 2016, article ID 1650191, DOI: 10.1142/S0218127416501911.

[14] GEORGE S.N., PATTATHIL D.P., *A secure LFSR based random measurement matrix for compressive sensing*, Sensing and Imaging **15**(1), 2014, article ID 85, DOI: 10.1007/s11220-014-0085-9.

[15] 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, DOI: 10.1016/j.ijleo.2012.08.017.

[16] 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, DOI: 10.1016/j.optlastec.2016.02.018.

[17] LIHUA GONG, CHENGZHI DENG, SHUMIN PAN, NANRUN ZHOU, *Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform*, Optics and Laser Technology **103**, 2018, pp. 48–58, DOI: 10.1016/j.optlastec.2018.01.007.

[18] 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, DOI: 10.1016/j.optcom.2015.12.024.

[19] GEORGE S.N., PATTATHIL D.P., *A novel approach for secure compressive sensing of images using multiple chaotic maps*, Journal of Optics **43**(1), 2014, pp. 1–17, DOI: 10.1007/s12596-013-0147-8.

[20] YUSHU ZHANG, LEO YU ZHANG, JIANTAO ZHOU, LICHENG LIU, FEI CHEN, XING HE, *A review of compressive sensing in information security field*, IEEE Access **4**, 2016, pp. 2507–2519, DOI: 10.1109/ACCESS.2016.2569421.

[21] MALLAT S.G., ZHANG Z.F., *Matching pursuits with time-frequency dictionaries*, IEEE Transactions Signal Processing **41**(12), 1993, pp. 3397–3415, DOI: 10.1109/78.258082.

[22] BAJWA W.U., HAUPT J.D., RAZ G.M., WRIGHT S.J., NOWAK R.D., *Toeplitz-structured compressed sensing matrices*, [In] *2007 IEEE/SP 14th Workshop on Statistical Signal Processing*, 2007, pp. 294–298, DOI: 10.1109/SSP.2007.4301266.

[23] GUOYUAN QI, GUANRONG CHEN, *Analysis and circuit implementation of a new 4D chaotic system*, Physics Letters A **352**(4–5), 2006, pp. 386–397, DOI: 10.1016/j.physleta.2005.12.030.

[24] LIANSHENG SUI, KUAIKUAI DUAN, JUNLI LIANG, *A secure double-image sharing scheme based on Shamir's three-pass protocol and 2D sine logistic modulation map in discrete multiple-parameter fractional angular transform domain*, Optics and Lasers in Engineering **80**, 2016, pp. 52–62, DOI: 10.1016/j.optlaseng.2015.12.016.

[25] ZHAN YU, CHANGLUN ZHANG, HENGYOU WANG, NAN NING, *Digital image multiple encryption algorithm based on compressive sensing*, [In] *Proceedings of the 2016 4th International Conference on Sensors, Mechatronics and Automation (ICSMA 2016)*, Advances in Intelligent Systems Research, Vol. 136, 2016, pp. 657–661, DOI: 10.2991/icsma-16.2016.114.

[26] 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, DOI: 10.1016/j.jvcir.2017.01.022.

[27] YE ZHANG, BIAO XU, NANRUN ZHOU, *A novel image compression–encryption hybrid algorithm based on the analysis sparse representation*, Optics Communications **392**, 2017, pp. 223–233, DOI: 10.1016/j.optcom.2017.01.061.

[28] NANRUN ZHOU, HAO JIANG, LIHUA GONG, XINWEN XIE, *Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging*, Optics and Lasers in Engineering **110**, 2018, pp. 72–79, DOI: 10.1016/j.optlaseng.2018.05.014.

Received July 16, 2018
in revised form September 30, 2018