Optica Applicata, Vol. XLIX, No. 3, 2019
DOI: 10.5277/oa190307

Compressive-sensing-based double-image encryption algorithm combining double random phase encoding with Josephus traversing operation

Hao Jiang[1, 2], Zhe Nie[2*], Nanrun Zhou[1, 3], Wenquan Zhang[1]

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

[2]School of Computer Engineering, Shenzhen Polytechnic, Shenzhen, Guangdong 518055, China

[3]Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai Jiao Tong University, Shanghai 200240, China

[*]Corresponding author: niezhe@szpt.edu.cn

A double-image encryption scheme based on compressive sensing is designed by combining a double random phase encoding technique with Josephus traversing operation. Two original images are first compressed and encrypted by compressive sensing in the discrete wavelet domain and then connected into a complex image according to the order of the alternate rows. Moreover, the resulting image is re-encrypted into stationary white noise by a double random phase encoding technique. Lastly, Josephus traversing method is utilized to scramble the transformed image. The initial states of the Henon chaotic map are the secret keys of this double-image encryption algorithm, which can be used to control the construction of the measurement matrix in compressive sensing and generation of the random-phase mask in double random phase encoding. Simulation results show that the proposed double-image encryption algorithm is effective and secure.

Keywords: image encryption, compressive sensing, double random phase encoding, Josephus traversing.

1. Introduction

With the significant development of information and signal processing technologies, the image encryption has received much attention in the field of image processing. To protect the image information from leakage, a series of image encryption strategies concentrating on various aspects have been designed, such as chaos [1–4], DNA sequence [5, 6], fractional Fourier transform [7, 8], gyrator transform [9, 10], and Brownian motion [11]. Although the methods adopted in the above encryption schemes are different, they share a common purpose of trying to transform the plaintext image into white Gaussian noise.

Compressive sensing (CS) theory as a new sampling technique is considered to be able to encrypt and compress a signal simultaneously [12, 13]. In recent years, CS has been introduced into the domain of information security. For this reason, many CS-based image cryptosystems have been designed [14–18]. HUANG *et al*. proposed a parallel image encryption method based on CS and block cipher structure consisting of scrambling, mixing, S-box and chaotic block-wise XOR [14]. To reduce the secret key consumption, ZHOU *et al*. first presented the utilization of the chaotic map to generate the original row vector of a circulant matrix, so as to control the construction of the measurement matrix in CS [15]. Subsequently, they proposed a simultaneous image encryption-compression scheme combination 2D CS with hyper-chaotic system, where the plaintext image is first compressed and encrypted by the measurement matrices in two directions and then re-encrypted by the cycle shift operation controlled by hyperchaos [16]. A visually secure image encryption algorithm incorporating CS with watermarking was demonstrated in [17], in which the compressed image is embedded into a carrier image to obtain the final cipher image. ZHOU *et al*. put forward an optical image compression and encryption scheme with the fractional Mellin transform based on 2D CS, which overcame the security risk of image cryptosystems that relies solely on linear transformations [18].

As the first optical image encryption technology, double random phase encoding (DRPE) [19] was considered to be effective in combination with CS. LU *et al*. employed the DRPE technique to encrypt the measured values and then the resulting image is embedded into a host image [20]. Furthermore, a secure DRPE-based block CS was proposed which can achieve great ability of resisting the chosen-plaintext attack [21]. HU *et al*. developed his image compression-encryption by using DRPE and CS with a novel measurement matrix updating mechanism, where the CS measurement matrix is never re-used [22].

Nowadays, a rapid increase of image information means the requirement of faster image processing speed, and double-image encryption even multi-image encryption become popular. LIU *et al*. used Arnold transform to scramble the values of a complex function composed of two original images, and the changed complex function is re-encrypted by discrete fractional angular transform [23]. A double image encryption algorithm based on random pixel exchanging and phase encoding was presented in [24], where the random matrix in pixel exchanging is also utilized in the process of phase encoding. Using discrete fractional random transform and logistic maps, SUI *et al*. investigated a double-image encryption scheme based on the asymmetric technique which has a high resistibility to various attacks [25]. Soon they defined a new discrete fractional transform called the discrete multiple-parameter fractional angular transform and combined the two-coupled logistic map to effectively encrypt two plaintext images [26].

In this paper, an improved CS-based double-image encryption method by combining DRPE with Josephus traversing operation is designed. Henon map is chosen to construct a pair of measurement matrices first. Then, two plaintext images are measured by compressive sensing to accomplish compression and encryption simultaneously.

Next, the compressed images are cross-linked in the vertical direction. DRPE is utilized to re-encrypt the composite image, where the measurement matrices in CS act as the random-phase masks in DRPE. Lastly, the resulting image is scrambled with the help of Josephus traversing operation. Numerical simulations demonstrate the availability and the confidentiality of the proposed double-image encryption algorithm.

The remainder of this paper is organized as follows. In Section 2, the proposed CS-based double-image encryption algorithm is described in detail. The experimental results and security analyses are stated in Section 3. Our work is concluded in the last Section.

2. CS-based double-image encryption combining double random phase encoding with Josephus traversing operation

Figure 1 shows the order of Josephus traversing operation, while the proposed double -image encryption algorithm is also illustrated in Fig. 2**a**. Assume that $\mathbf{C}_i$ (i = 1, 2)

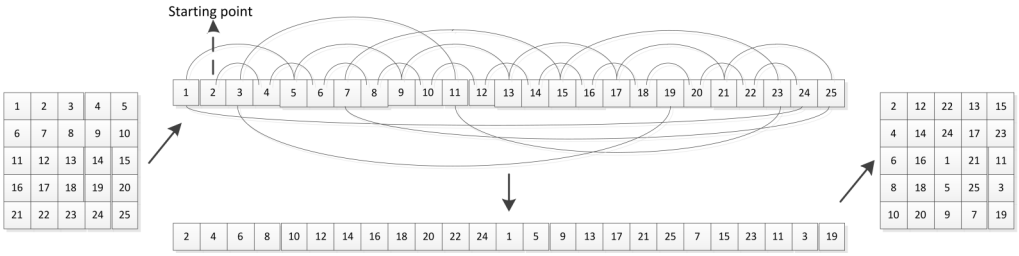

Fig. 1. The order of Josephus traversing operation with starting position (1, 2) and counting period 2.

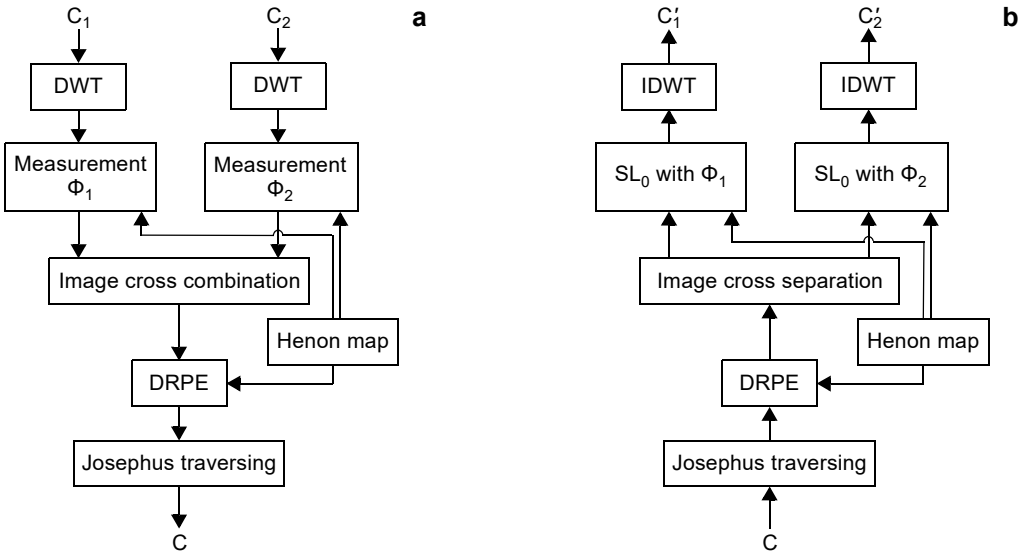

Fig. 2. Flow chart of the proposed algorithm: encryption (**a**) and decryption (**b**) procedure.

represent two original images with the size of $N \times N$ pixels, respectively. The double -image encryption process is described as follows.

Step 1: Two plaintext images $\mathbf{C}_1(x, y)$ and $\mathbf{C}_2(x, y)$ are extended in $\mathbf{\Psi}$ domain, respectively, where $\mathbf{\Psi}$ is set to be the discrete wavelet transform (DWT). Then, two sparse matrices are obtained as

$$\begin{cases} \mathbf{S}_1 = \mathbf{\Psi}^{\mathrm{T}}\mathbf{C}_1 \\ \mathbf{S}_2 = \mathbf{\Psi}^{\mathrm{T}}\mathbf{C}_2 \end{cases} \tag{1}$$

where T represents the transpose operation.

Step 2: With the values of the initial conditions x_0, y_0, α, β and the iteration times $2N$, the Henon map is described as [27]

$$\begin{cases} x_{m+1} = 1 - \alpha x_m^2 + y_m \\ y_{m+1} = \beta x_m \end{cases} \tag{2}$$

two random sequences $\mathbf{x} = [x_1, x_2, ..., x_{2N}]$ and $\mathbf{y} = [y_1, y_2, ..., y_{2N}]$ can be generated. The first N elements of $\mathbf{x}$ are discarded to reduce the correlation among the elements, *i.e.*, $\mathbf{x}' = [x_N, x_{N+1}, ..., x_{2N}]$. With another pair of seeds x_1 and y_1, the chaotic sequence $\mathbf{z}' = [z_N, z_{N+1}, ..., z_{2N}]$ is obtained in the same way.

Step 3: The first row vector of a circular matrix $\mathbf{\Phi}$ is built by $\mathbf{x}'$ and $\mathbf{z}'$, respectively. The random matrices $\mathbf{\Phi}_1$ and $\mathbf{\Phi}_2$ of the size $N \times N$ can be constructed by an iterative operation, *i.e.*,

$$\begin{cases} \mathbf{\Phi}_i(j, 1) = \mu\mathbf{\Phi}_i(j-1, N) \\ \mathbf{\Phi}_i(j, 2:N) = \mathbf{\Phi}_i(j-1, 1:N-1) \end{cases} \tag{3}$$

where $i = 1, 2$, and $2 \le j \le N$, and $\mu > 1$.

Step 4: The upper half of the matrix $\mathbf{\Phi}_1$ and the lower half of the matrix $\mathbf{\Phi}_2$ are respectively extracted to obtain the measurement matrices $\mathbf{\Phi}_3$ and $\mathbf{\Phi}_4$ of the size $M \times N$, *i.e.*,

$$\begin{cases} \mathbf{\Phi}_3(1:M, 1:N) = \mathbf{\Phi}_1(1:N/2, 1:N) \\ \mathbf{\Phi}_4(1:M, 1:N) = \mathbf{\Phi}_2(N/2+1:N, 1:N) \end{cases} \tag{4}$$

where $M = N/2$. By performing the linear projection measurement on $\mathbf{S}_i$ ($i = 1, 2$) with $\mathbf{\Phi}_j$ ($j = 3, 4$), respectively, the $M \times N$ measurements $\mathbf{B}_1$ and $\mathbf{B}_2$ are produced,

$$\begin{cases} \mathbf{B}_1 = \mathbf{\Phi}_3\mathbf{S}_1 \\ \mathbf{B}_2 = \mathbf{\Phi}_4\mathbf{S}_2 \end{cases} \tag{5}$$

Step 5: The measurements $\mathbf{B}_1$ and $\mathbf{B}_2$ in the horizontal direction are combined to form an enlarged one, *i.e.*, $\mathbf{B} \in R^{N \times N}$. The odd row vectors of matrix $\mathbf{B}$ are composed

of row vectors of matrix $\mathbf{B}_1$ successively, meanwhile the row vectors of matrix $\mathbf{B}_2$ act as the even row vectors of matrix $\mathbf{B}$ in sequence, *i.e.*,

$$\begin{cases} \mathbf{B}(2 \times i - 1, :) = \mathbf{B}_1(i, :), & i = 1, 2, \ldots, N \\ \mathbf{B}(2 \times i, :) = \mathbf{B}_2(i, :), & i = 1, 2, \ldots, N \end{cases} \tag{6}$$

Step 6: By applying the double random phase encoding technique on the measurement $\mathbf{B}$ and taking the normalization of the random matrices $\mathbf{\Phi}_1$ and $\mathbf{\Phi}_2$ as the random-phase masks $\mathbf{M}_1$ and $\mathbf{M}_2$, respectively, the result $\mathbf{D}$ can be obtained as

$$\mathbf{D} = \mathrm{DRPE}(\mathbf{B}) \tag{7}$$

Step 7: The complex image $\mathbf{D}$ is further scrambled by Josephus traversing method with the starting point $\mathbf{D}(1, 1)$ and the counting space $N/2$ to form the final encryption image $\mathbf{C}$,

$$\mathbf{C} = \text{Josephus traversing}(\mathbf{D}(1, 1), N/2) \tag{8}$$

The decryption algorithm is depicted in Fig. 2**b**, which is similar to that of the encryption procedure but in the reverse order. The ciphertext image is first performed by Josephus traversing operation, and then the enlarged image can be obtained after the decoding of double random phase encoding. With image separation, two halves are reconstructed, and the plaintext images can be retrieved approximately via smoothed l_0 norm algorithm [28] and inverse DWT.

3. Experimental results and security analyses

The efficiency and the security performance of the proposed double-image encryption algorithm are demonstrated with Matlab 2010(b) platform on a 64-bit personal computer. All the original images selected in the simulations are grayscale images with resolution 256 × 256. Specially, the resulting image of the encryption process is of the size 256 × 256, which means no more transmission bandwidth and storage space in our scheme.

3.1. Encryption result and decryption result

Generally, an ideal image encryption system should be able to encrypt plaintext images into random-like ciphertext images. In order to prove the efficiency of the proposed double-image encryption algorithm, two digital images *Baboon* and *Peppers* shown in Figs. 3**a** and 3**b**, respectively, are chosen as test images. The setting of the simulation parameters is as follows: $x_0 = y_1 = 0.1$, $x_1 = y_0 = 0.2$, $\alpha = 1.4$, $\beta = 0.3$, $\mu = 2$. Figure 3**c** shows the encryption result for the test images. It is completely unrecognized and does not reveal any meaningful information about the original images. The decryption im-

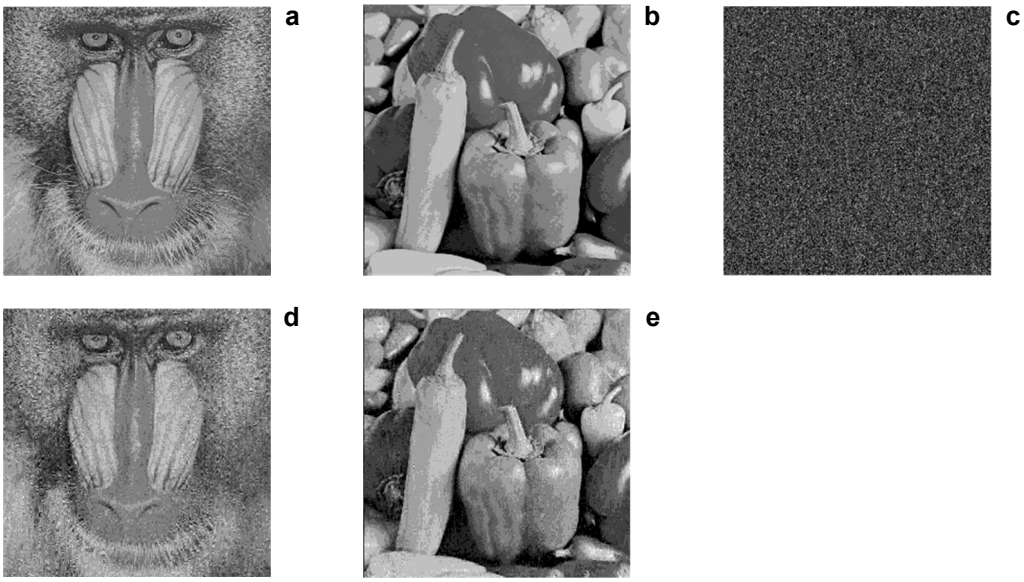

Fig. 3. Results of test images: *Baboon* (**a**), *Peppers* (**b**), encryption *Baboon–Peppers* (**c**), decryption *Baboon* (**d**), and decryption *Peppers* (**e**).

ages with the all correct keys are really visible, as given in Figs. 3**d** and 3**e**, respectively. This indicates that our double-image encryption algorithm has a satisfactory encryption and decryption effect.

3.2. Histogram analysis

Considering that the histogram analysis is an essential criterion to evaluate the validity of a cryptosystem, we simulate the image histogram of the proposed double-image encryption algorithm in this section. Figures 4**a** and 4**b** exhibit the histograms of *Baboon*

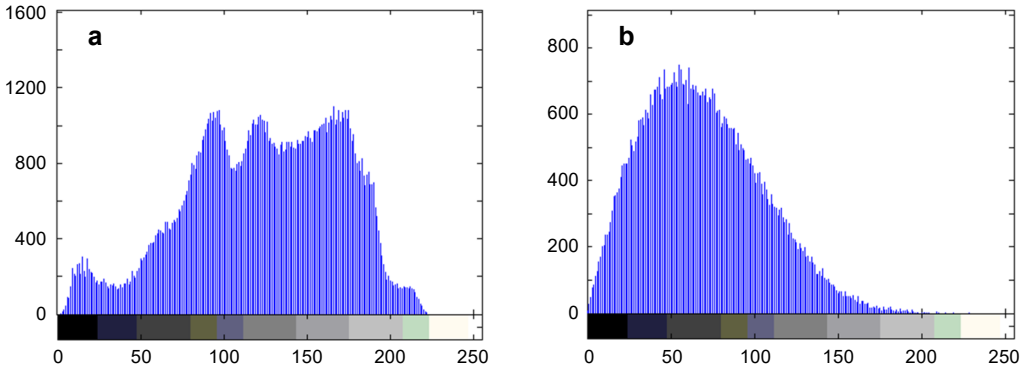

Fig. 4. Continued on the next page.

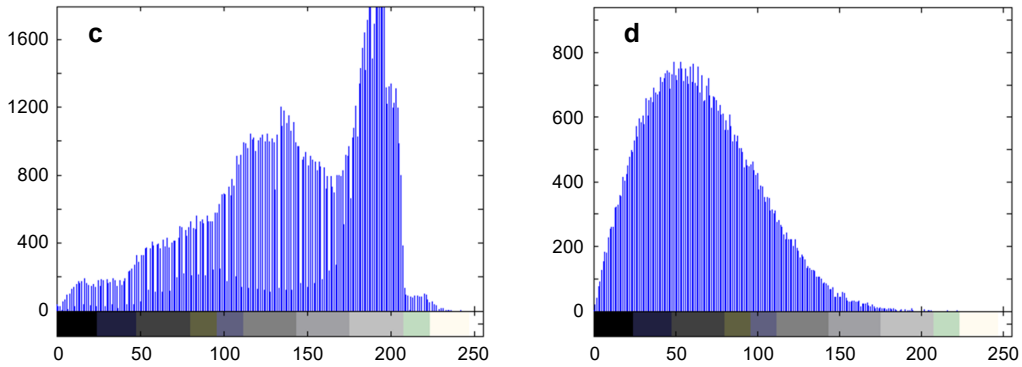

Fig. 4. Histogram: *Baboon–Peppers* (**a**), encryption *Baboon–Peppers* (**b**), *Plane–Couple* (**c**), and encryption *Plane–Couple* (**d**).

–Peppers and *Plane–Couple*, respectively. The histograms of the corresponding encryption images are displayed in Figs. 4**c** and 4**d**. Obviously, the histograms of the ciphertext images are similar to each other and differ from the histograms of the corresponding plaintext images. Hence, the proposed double-image encryption algorithm has a strong ability of defending the statistical attack.

3.3. Correlation analysis

For a normal original image, two adjacent pixels are usually highly correlated. Whereas, due to the confusion effect of the encryption process, the cipher image should have a weak correlation. A certain pairs of adjacent pixels in horizontal, vertical, and diagonal directions are randomly extracted to calculate the correlation coefficients as

$$c_{mn} = \frac{\sum_{j=1}^{N}(m_j - \overline{m})(n_j - \overline{n})}{\sqrt{\sum_{j=1}^{N}(m_j - \overline{m})^2 \sum_{j=1}^{N}(n_j - \overline{n})^2}} \tag{9}$$

where

$$\overline{m} = \frac{1}{N}\sum_{j=1}^{N} m_j$$

$$\overline{n} = \frac{1}{N}\sum_{j=1}^{N} n_j$$

Figures 5**a**, 5**b**, 5**d** and 5**e** show the correlations among two horizontally adjacent pixels in the four original images, respectively, which are similar to linear distribution. As given in Figs. 5**c** and 5**f**, the correlations of horizontally adjacent pixels in the corresponding encryption image are significantly reduced. The Table lists the correlation coefficients of the proposed double-image encryption algorithm and the algorithm

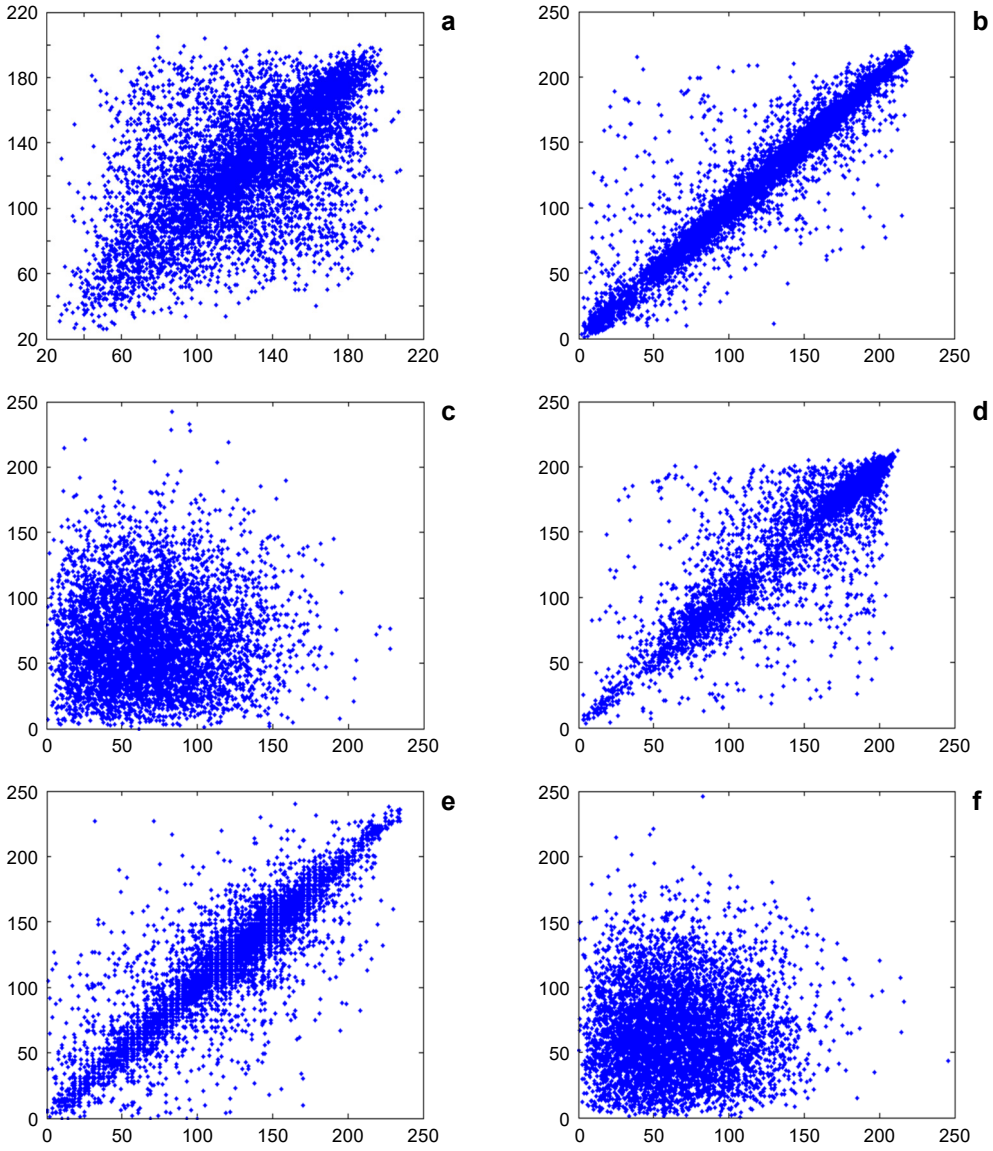

Fig. 5. Correlation of two horizontally adjacent pixels: *Baboon* (**a**), *Peppers* (**b**), encryption *Baboon–Peppers* (**c**), *Plane* (**d**), *Couple* (**e**), and encryption *Plane–Couple* (**f**).

in [29], which indicates that our scheme is more effective in destroying the correlation. Overall, the statistical attack on our double-image encryption algorithm is invalid.

3.4. Key sensitivity analysis

In key sensitivity analysis, mean square error (MSE) is employed as the criterion to evaluate the quality of the decryption image. Figure 6 shows the decryption images *Baboon*

T a b l e. Correlation coefficients of adjacent pixels.

Algorithm	Image	Horizontal	Vertical	Diagonal
	Baboon	0.6497	0.7133	0.6348
	Peppers	0.9560	0.9462	0.9202
	Baboon–Peppers	0.8583	0.8805	0.8263
Proposed scheme	Encryption *Baboon–Peppers*	0.0098	–0.0245	–0.0036
Reference [29]	Encryption *Baboon–Peppers*	0.0128	0.0897	0.0336
	Plane	0.9140	0.9158	0.8610
	Couple	0.8985	0.8813	0.8137
	Plane–Couple	0.9192	0.9161	0.8609
Proposed scheme	Encryption *Plane–Couple*	0.0375	–0.0160	–0.0205
Reference [29]	Encryption *Plane–Couple*	0.0594	0.1145	0.0847

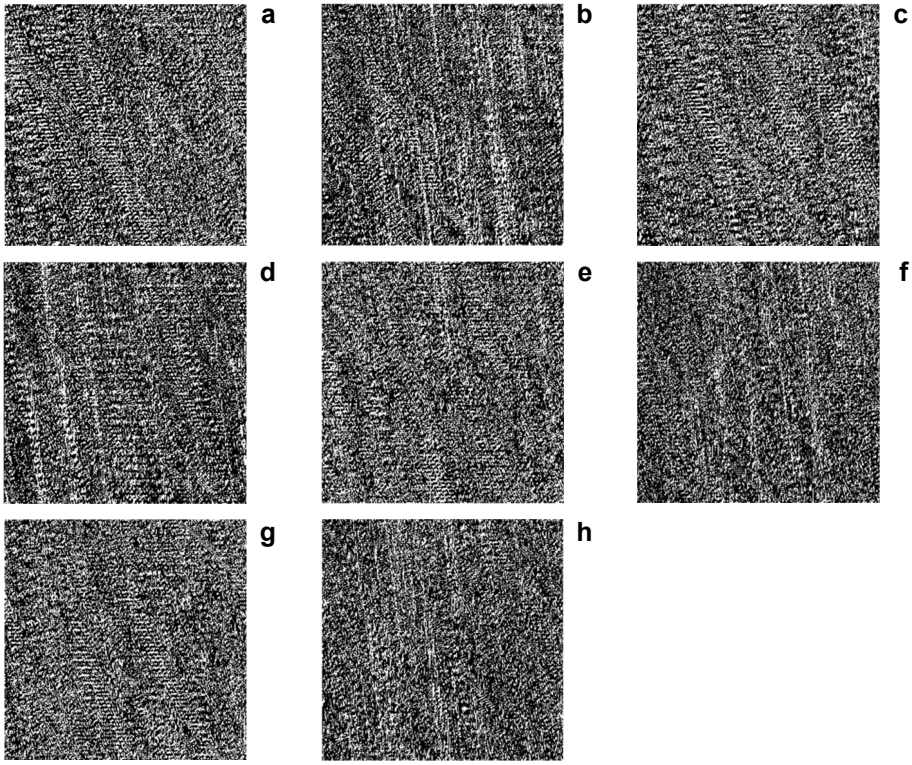

Fig. 6. Decryption images *Baboon* and *Peppers* with wrong key: $x_0 = 0.1000001$ (**a**, **b**), $y_0 = 0.2000001$ (**c**, **d**), $x_1 = 0.2000001$ (**e**, **f**), and $y_1 = 0.1000001$ (**g**, **h**).

and *Peppers* with the modified key, and it can be observed that each of them presents a disorganized distribution without any regularity. The MSE curves with deviations d to the correct keys are displayed in Fig. 7. Only when the secret key deviation approaches zero indefinitely, the MSE value tends to be minimum as expected.

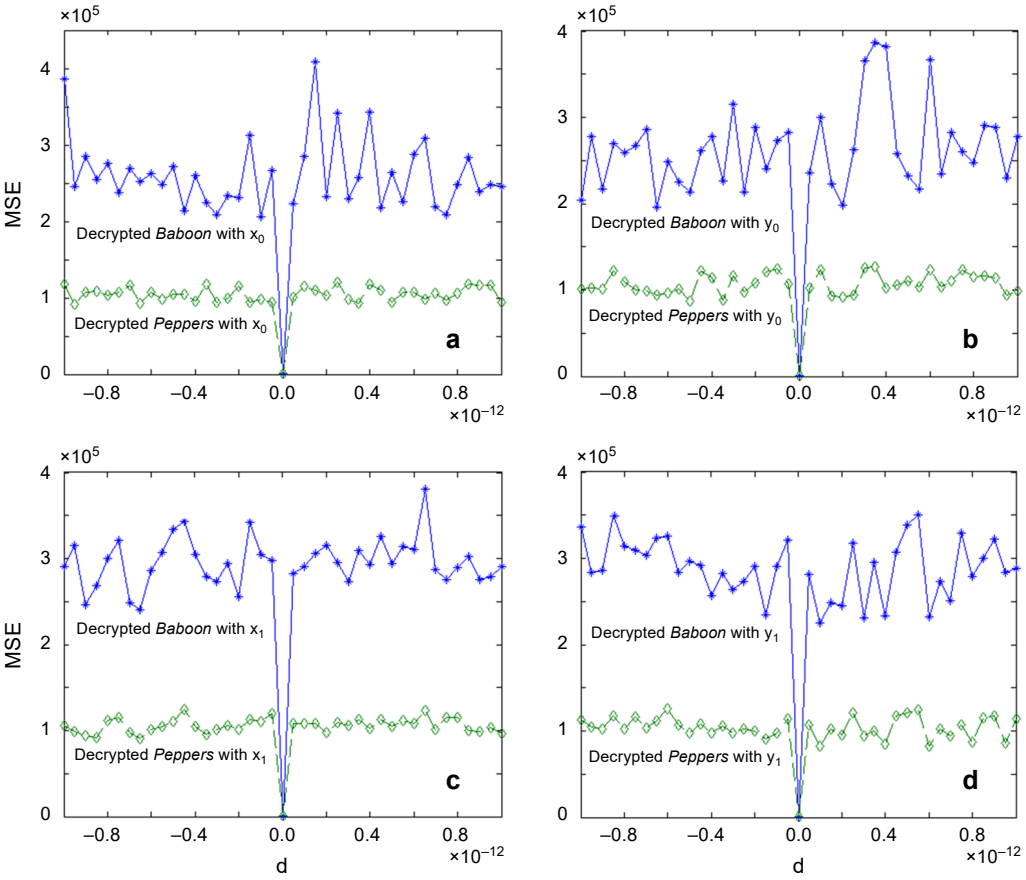

Fig. 7. MSE for the deviation of correct key: x_0 (**a**), y_0 (**b**), x_1 (**c**), and y_1 (**d**).

The above experimental results prove that the proposed double-image encryption algorithm is extremely sensitive to the key. In this case, even a micro-deviation from the correct secret key will result in the failure of the original image reconstruction. Thus, an unauthorized user cannot capture any useful information about the plaintext image unless he possesses all the correct keys.

3.5. Key space analysis

The key space is defined as the set of all possible effective keys that can be used in the encryption process. In fact, its size determines whether the brute-force attack on a cryptosystem is successful [30]. In the proposed double-image encryption algorithm, the initial conditions of the Henon chaotic map (x_0, y_0, x_1, y_1) are main keys. Suppose their respective key space is s_1, s_2, s_3, and s_4. According to Fig. 7**a**, the space s_1 of x_0 is around 1×10^{15}. Likewise, each key space s_i ($i = 2.\ 3.\ 4$) is about 1×10^{15} as shown

in Fig. 7, therefore the total key space $\sum_{i=1}^{4} s_i$ is up to 10^{60}. The adversary has to search at least 2^{195} possible combinations for the accurate keys, which demonstrates that the proposed double-image encryption algorithm provides a reliable resistance to the brute -force attack.

3.6. Noise attack analysis

In the process of image transmission, the ciphertext is susceptible to noise. Thus the robustness of our double-image encryption algorithm against the noise attack is also tested. Assume the encryption image **C** is affected by noise,

$$\mathbf{C}' = \mathbf{C} + k\,\mathbf{N} \tag{10}$$

where $\mathbf{C}'$ represents the noisy encryption image, k is a control parameter of the noise intensity, and **N** denotes the white Gaussian noise with zero-mean and unit standard deviation. Figure 8 illustrates the decryption images with a noise intensity coefficient equal to 5, 10, 15 and 20, respectively. Besides, the MSE curves are computed and shown in Fig. 9. From the simulation results, although the quality of the retrieved image decreases with the increase of noise level, it is still recognizable and retains most of the features of the original image. In conclusion, the proposed double-image encryption algorithm can withstand the noise attack to an extent.

3.7. Occlusion attack analysis

To demonstrate the performance of the proposed double-image encryption algorithm against the occlusion attack, the encryption images with 10 × 10, 16 × 16 and 20 × 20 data

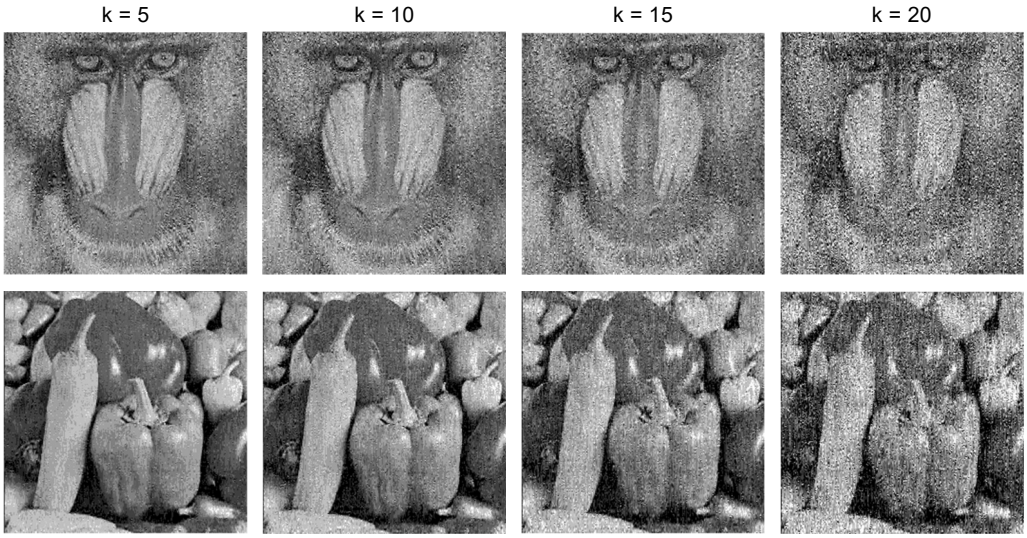

Fig. 8. Decryption images *Baboon* and *Peppers* with noise intensity coefficient equal to 5, 10, 15, and 20.

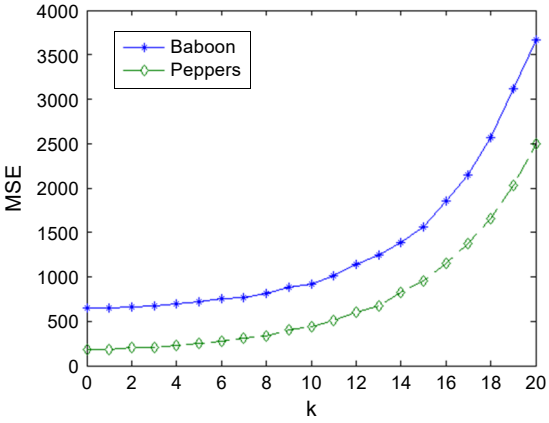

Fig. 9. MSE curves under different noise intensity coefficients.

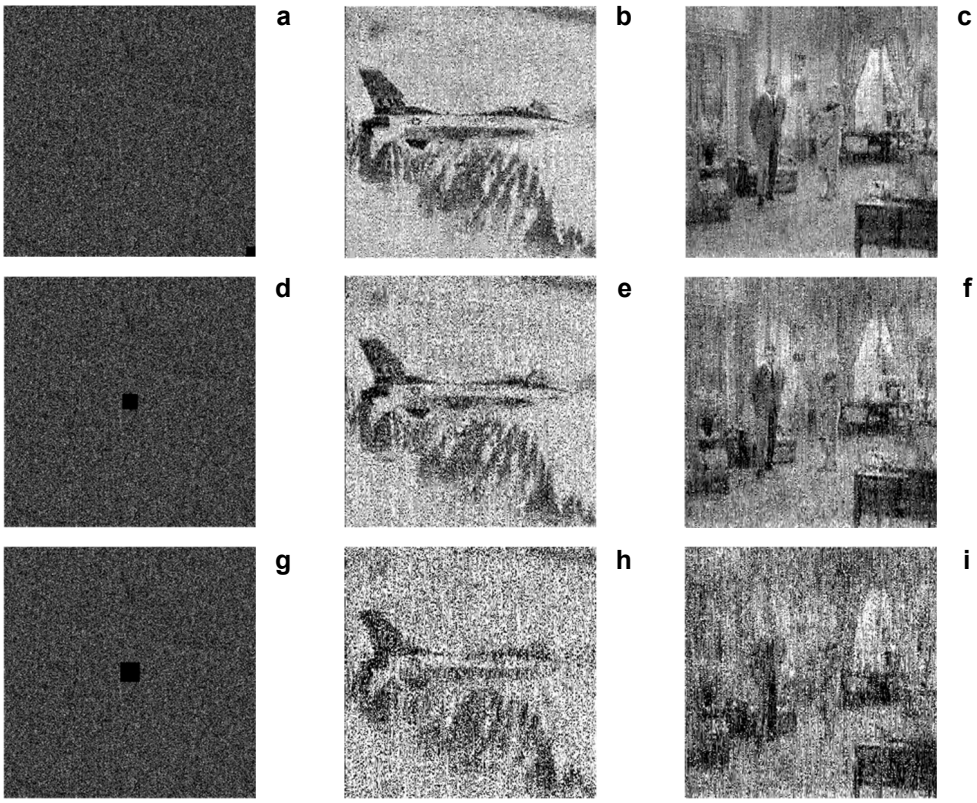

Fig. 10. Robustness against occlusion attack: 10 × 10 pixels occlusion in the corner (**a**), and reconstructed images from **a** (**b**, **c**), 16 × 16 pixels occlusion in the center (**d**), and reconstructed images from **d** (**e**, **f**), 20 × 20 pixels occlusion in the center (**g**), and reconstructed images from **g** (**h**, **i**).

loss are displayed in Figs. 10**a**, 10**d** and 10**g**, respectively. The corresponding decryption images with correct keys are shown in (**b**, **c**), (**e**, **f**) and (**h**, **i**), respectively. From the series of Fig. 10, one can find that each reconstructed image can be identified even if its surface is blurry. It suggests that our double-image encryption algorithm can resist the occlusion attack in some degree.

4. Conclusion

An improved CS-based double-image encryption algorithm combining a double random phase encoding technology with Josephus traversing operation is proposed. The circular matrix controlled by the Henon chaotic map is employed to construct the measurement matrix in DWT-based compressive sensing and the random-phase mask in double random phase encoding. Two plaintext images are compressed and encrypted via compressive sensing in the discrete wavelet domain severally and combined into a synthetic image with the same size as original images. Besides, the double random phase encoding technique is utilized to smooth the intermediate resulting image to a "white noise" for the purpose of re-encryption. Finally, the transformed image is further confused and diffused by Josephus traversing operation. Experimental results verify that the proposed double-image encryption algorithm not only has high efficiency and security, but also has strong robustness against various attacks. In addition, it can encrypt two original images at the same time without adding additional transmission bandwidth and is easy to implement with optical devices.

Acknowledgments – This work is supported by the National NSFC (Grant Nos. 61861029 and 61462061), the Major Academic Discipline and Technical Leader of Jiangxi Province (Grant No. 20162BCB22011), the Natural Science Foundation of Jiangxi Province (Grant No. 20171BAB202002), the Cultivation Plan of Applied Research of Jiangxi Province (Grant No. 20181BBE58022) and the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant Nos. AGK2018002 and AGK201602).

References

[1] Qiwen Ran, Lin Yuan, Tieyu Zhao, *Image encryption based on nonseparable fractional Fourier transform and chaotic map*, Optics Communications **348**, 2015, pp. 43–49, DOI: 10.1016/j.optcom.2015.03.016.

[2] Chengqi Wang, Xiao Zhang, Zhiming Zheng, *An efficient image encryption algorithm based on a novel chaotic map*, Multimedia Tools and Applications **76**(22), 2017, pp. 24251–24280, DOI: 10.1007/s11042-016-4102-y.

[3] Xingyuan Wang, Hui-Li Zhang, *A color image encryption with heterogeneous bit-permutation and correlated chaos*, Optics Communications **342**, 2015, pp. 51–60, DOI: 10.1016/j.optcom.2014.12.043.

[4] 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, DOI: 10.5277/oa170113.

[5] XIANGJUN WU, KUNSHU WANG, XINGYUAN WANG, HAIBIN KAN, *Lossless chaotic color image cryptosystem based on DNA encryption and entropy*, Nonlinear Dynamics **90**(2), 2017, pp. 855–875, DOI: 10.1007/s11071-017-3698-4.

[6] XIULI CHAI, YIRAN CHEN, BROYDE L., *A novel chaos-based image encryption algorithm using DNA sequence operations*, Optics and Lasers in Engineering **88**, 2017, pp. 197–213, DOI: 10.1016/j.optlaseng.2016.08.009.

[7] 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, DOI: 10.5277/oa170112.

[8] ZHENGJUN LIU, HANG CHEN, BLONDEL W., ZHENMIN SHEN, SHUTIAN LIU, *Image security based on iterative random phase encoding in expanded fractional Fourier transform domains*, Optics and Lasers in Engineering **105**, 2018, pp. 1–5, DOI: 10.1016/j.optlaseng.2017.12.007.

[9] HANG CHEN, TANOUGAST C., ZHENGJUN LIU, SIELER L., *Asymmetric optical cryptosystem for color image based on equal modulus decomposition in gyrator transform domains*, Optics and Lasers in Engineering **93**, 2017, pp. 1–8, DOI: 10.1016/j.optlaseng.2017.01.005.

[10] YANG WEI, AIMIN YAN, JIABIN DONG, ZHIJUAN HU, JINGTAO ZHANG, *Optical image encryption using QR code and multilevel fingerprints in gyrator transform domains*, Optics Communications **403**, 2017, pp. 62–67, DOI: 10.1016/j.optcom.2017.06.087.

[11] XIULI CHAI, *An image encryption algorithm based on bit level Brownian motion and new chaotic systems*, Multimedia Tools and Applications **76**(1), 2017, pp. 1159–1175, DOI: 10.1007/s11042-015-3088-1.

[12] DONOHO D.L., *Compressed sensing*, IEEE Transactions on Information Theory **52**(4), 2006, pp. 1289–1306, DOI: 10.1109/TIT.2006.871582.

[13] CANDES 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.

[14] 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, DOI: 10.1007/s11042-012-1337-0.

[15] 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.

[16] 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.

[17] XIULI CHAI, ZHIHUA GAN, YIRAN CHEN, YUSHU ZHANG, *A visually secure image encryption scheme based on compressive sensing*, Signal Processing **134**, 2017, pp. 35–51, DOI: 10.1016/j.sigpro.2016.11.016.

[18] 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, DOI: 10.1016/j.optcom.2014.12.084.

[19] REFREGIER P., JAVIDI B., *Optical image encryption based on input plane and Fourier plane random encoding*, Optics Letters **20**(7), 1995, pp. 767–769, DOI: 10.1364/OL.20.000767.

[20] 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.

[21] HONG LIU, DI XIAO, YANBING LIU, YUSHU ZHANG, *Securely compressive sensing using double random phase encoding*, Optik **126**(20), 2015, pp. 2663–2670, DOI: 10.1016/j.ijleo.2015.06.079.

[22] GUIQIANG HU, DI XIAO, YONG WANG, TAO XIANG, QING ZHOU, *Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes*, Optics and Lasers in Engineering **98**, 2017, pp. 123–133, DOI: 10.1016/j.optlaseng.2017.06.013.

[23] ZHENGJUN LIU, MIN GONG, YONGKANG DOU, FENG LIU, SHEN LIN, AHMAD M.A., JINGMIN DAI, SHUTIAN LIU, *Double image encryption by using Arnold transform and discrete fractional angular transform*, Optics and Lasers in Engineering **50**(2), 2012, pp. 248–255, DOI: 10.1016/j.optlaseng.2011.08.006.

[24] Zhengjun Liu, Yu Zhang, She Li, Wei Liu, Wanyu Liu, Yanhua Wang, Shutian Liu, *Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains*, Optics and Laser Technology **47**, 2013, pp. 152–158, DOI: 10.1016/j.optlastec.2012.09.007.

[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, DOI: 10.1016/j.optlaseng.2013.12.001.

[26] Liansheng Sui, Kuaikuai Duan, Junli Liang, *Double-image encryption based on discrete multiple -parameter fractional angular transform and two-coupled logistic maps*, Optics Communications **343**, 2015, pp. 140–149, DOI: 10.1016/j.optcom.2015.01.021.

[27] Hénon M., *A two-dimensional mapping with a strange attractor*, [In] *The Theory of Chaotic Attractors*, Hunt B.R., Li TY., Kennedy J.A., Nusse H.E. [Eds], Springer, New York, NY, 1976, pp. 94–102, DOI: 10.1007/978-0-387-21830-4_8.

[28] Mohimani 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, DOI: 10.1109/TSP.2008.2007606.

[29] Nanrun Zhou, Jianping Yang, Changfa Tan, Shumin Pan, Zhihong Zhou, *Double-image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform*, Optics Communications **354**, 2015, pp. 112–121, DOI: 10.1016/j.optcom.2015.05.043.

[30] Alvarez G., Shujun Li, *Some basic cryptographic requirements for chaos-based cryptosystems*, International Journal of Bifurcation and Chaos **16**(8), 2006, pp. 2129–2151, DOI: 10.1142/S0218127406015970.

Received August 5, 2018
in revised form September 17, 2018