Optica Applicata, Vol. XLIX, No. 4, 2019
DOI: 10.37190/oa190402

Image compression and encryption algorithm based on advanced encryption standard and hyper-chaotic system

Zhe Nie[1], Zheng-Xin Liu[2], Xiang-Tao He[2], Li-Hua Gong[2*]

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

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

[*]Corresponding author: lhgong@ncu.edu.cn

An image compression and encryption algorithm by combining the advanced encryption standard (AES) with the hyper-chaotic system is designed, in which Arnold map is employed to eliminate part of the block effect in the image compression process. The original image is compressed with the assistance of a discrete cosine transform and then its transform coefficients are encrypted with the AES algorithm. Besides, the hyper-chaotic system is adopted to introduce the nonlinear process for image encryption. Numerical simulations and theoretical analyses demonstrate that the proposed image compression and encryption algorithm is of high security and good compression performance.

Keywords: hyper-chaotic system, advanced encryption standard, discrete cosine transform, image encryption, image compression.

1. Introduction

Chaotic systems have been widely applied in the field of image encryption [1–5]. In 1989, a chaotic system was deduced in the encryption scheme [1]. Subsequently, two-dimensional chaotic maps were also adopted in image encryption, where the image was encrypted by scrambling and diffusion operations [2]. Cat maps were extended to a three -dimensions case and the image encryption scheme based on 3D chaotic cat maps improved considerably in terms of security [3]. In 2012, Kanso and Ghebleh proposed a new 3D hyper-chaotic map, which could improve the security of the system by multiple rounds of image encryption [4]. An efficient self-adaptive model for the chaotic image encryption algorithm was proposed, where the keystream generated in permutation and diffusion operations was dependent on the plaintext image [5]. Chen *et al.* put forward an algorithm for scrambling and encrypting images in both the spatial do-

main and the transform domain [6]. Although the low dimensional chaotic system can be applied in image encryption, its security cannot be guaranteed.

The security requirements of image encryption algorithms have been increasing continuously, since more and more private images need to be transmitted over public network. Hyper-chaotic system is a more suitable tool to confuse the relation between the plaintext image and the ciphertext image [7]. In 2012, ZHU proposed an image encryption scheme based on a hyper-chaotic sequence, where the chaotic key stream related to the plaintext makes it more difficult to break the encryption system [8]. YE and WONG introduced a time delay into the generation of pseudo-random sequences to improve the encryption performance with two kinds of diffusion operations, *i.e.*, the forward operation and the reverse operation [9]. Subsequently, HUANG and YE designed an image encryption scheme combining the DNA sequence with the hyper-chaotic system, which transformed the pseudo-random sequence into the DNA sequence for an image diffusion operation [10]. In 2015, an image encryption scheme based on a cat map and hyper-chaotic system was formulated with the generated key stream related to the plaintext image [11]. Then, a series of image encryption schemes based on various hyper-chaotic systems has been proposed, which improved the encryption performance to a certain extent [12–15]. ZHOU *et al*. employed a hyper-chaotic system to compress and encrypt the original image for higher security [14]. LIU *et al*. put forward an image encryption algorithm integrating the hyper-chaotic system with the dynamic S-box, where the dynamic S-box was constructed to pursue a good confusion effect [16]. However, ZHANG *et al*. found that the image encryption algorithm of LIU *et al*. is weak in resisting the chosen-plaintext attack and improved the security of the image encryption algorithm by modifying the key stream [17]. ZHAN *et al*. introduced the hyper-chaotic sequence into almost all the encryption steps [18]. WANG *et al*. presented a new image encryption scheme with the SHA-3 algorithm and chaotic system to improve the encryption speed [19]. LI *et al*. proposed a modified integral imaging reconstruction and encryption scheme with an improved SR reconstruction algorithm, where heterogeneous monospectral cameras were utilized to acquire the multispectral color image [20]. Hyper-chaotic system satisfies the high security requirement of image encryption, but the encryption process for images with large data will become complicated correspondingly.

In the process of modern information transmission, the rapidly growing demand on transmitting images via public network has raised a lot of interest in image compression and encryption. Therefore, a number of image compression and encryption schemes has been investigated [21–23]. In 2010, SAPNA and JITHIN devised a selective image encryption algorithm based on the discrete cosine transform and stream cipher [24]. To enhance the robustness of the selective image encryption algorithm, a new image encryption method was constructed by MIRZAEI *et al*. [25]. In 2013, ZHU *et al*. introduced an image encryption–compression scheme by shuffling the plaintext image with the hyper-chaotic system and Chinese remainder theorem [26]. ZHANG *et al*. presented an image encryption algorithm combining compressive sensing with the Arnold trans-

form to compress and encrypt the original image [27]. In addition, ZHOU *et al*. put forward an image compression and encryption algorithm by considering the Hadamard matrix as the measurement matrix [28]. A chaotic image encryption scheme was proposed by scrambling the DCT coefficient matrix with logistic map [29]. ZHOU *et al*. designed an image encryption algorithm based on compressive sensing and discrete fractional random transform, where logistic map was used to construct two random matrices for compressive sensing [30]. An image encryption algorithm was proposed by combining the DCT with 2D chaotic map to solve the problem of poor security and small key space in one-dimensional chaotic cryptosystems [31]. In 2015, an image compression and encryption algorithm was devised, in which the chaotic system was employed to generate pseudo-random measurement matrices [32]. To further improve the security and the compression performance of image encryption schemes, TONG *et al*. presented a color image compression and encryption scheme based on the hyper-chaotic system, where the dictionary of discrete cosine transform was exploited to represent the color image sparsely [33]. On this basis, ZHANG and TONG utilized the key stream generator and hyper-chaotic system to encrypt the image with scrambling and diffusion operations and compress the image data via the Huffman coding [34]. In 2017, a compression and encryption scheme was designed, in which the Hadamard matrix was constructed controlled by a logistic map [35]. GONG *et al*. designed a new image compression and encryption scheme with the hyper-chaotic system and discrete fractional random transform [36]. In this paper, an image compression and encryption algorithm based on the advanced encryption standard (AES) and hyper-chaotic system is introduced. Discrete cosine transform is exploited to compress the image, and then the compressed image is encrypted by the AES and hyper-chaotic system.

The remainder of this paper is structured as follows. Discrete cosine transform is introduced in Section 2. The proposed image compression and encryption algorithm based on the AES and hyper-chaotic system is described in detail in Section 3. Simulation results and analyses are provided in Section 4. Finally, a brief conclusion is drawn in Section 5.

2. Discrete cosine transform

For given u and i ($u = 0, 1, ..., M-1$ and $i = 0, 1, ..., M-1$), one-dimensional discrete cosine transform can be expressed as:

$$G(u) = f(u) \sum_{i=0}^{M-1} g(i) \cos \frac{(i + 0.5)\pi u}{M} \tag{1}$$

$$f(u) = \sqrt{\frac{1 + \operatorname{sgn}|u|}{M}} = \sqrt{\frac{1 + |\operatorname{sgn} u|}{M}} \tag{2}$$

where $G(u)$ represents the discrete cosine transform coefficients, u represents generalized frequency variables and $\operatorname{sgn}(x)$ is the symbolic function.

For an image $g(i,j)$ of size $M \times N$, the two-dimensional discrete cosine transform can be written as

$$G(u,v) = f(u)f(v)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} g(i,j)\cos\left[\frac{(i+0.5)\pi u}{M}\right]\cos\left[\frac{(j+0.5)\pi v}{N}\right] \quad (3)$$

3. Image compression and encryption algorithm based on AES and hyper-chaotic system

The encryption and decryption process of the proposed image compression and encryption algorithm is shown in Fig. 1, and the specific steps are described as follows.

1) The original image G is segmented into sub-image blocks of size 8×8.

2) The i-th image block is disturbed with the Arnold transform to generate a new image block G_i. The scrambling process eliminates part of the block effect due to the DCT. The Arnold map can be defined as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (4)$$

where x_n, y_n represent the location of pixels before being scrambled; x_{n+1} and y_{n+1} represent the location of pixels after being scrambled; N is the number of iterations.

3) The DCT matrix $\mathbf{T}$ of size 8×8 is generated according to the discrete cosine transform theory.

4) The DCT matrix is used to process G_i,

$$\mathbf{H} = \mathbf{T} \times G_i \times \mathbf{T}' \quad (5)$$

5) The DCT coefficient matrix $\mathbf{H}$ is quantified and encoded to determine the compression ratio.

6) The quantized DCT coefficients of each block are scrambled by the AES algorithm, except the DC element. The specific process is shown in Fig. 2, where XOR op-

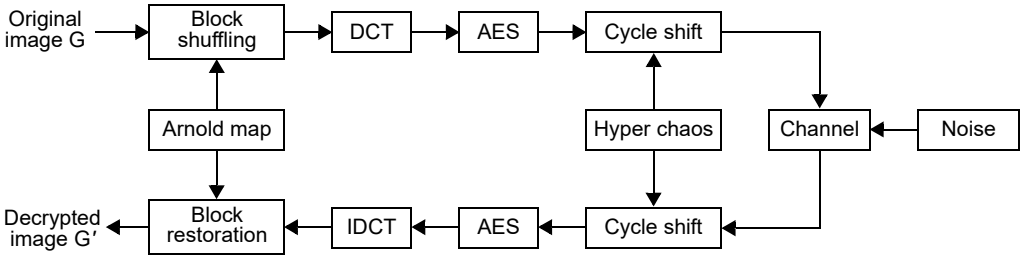

Fig. 1. The encryption and decryption process.

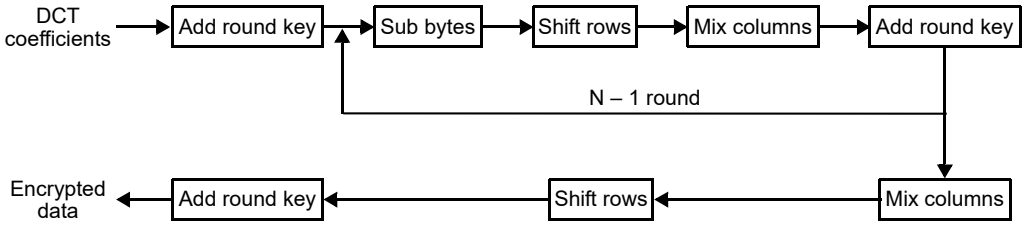

Fig. 2. The encryption process of AES algorithm.

eration is utilized in the step of Add Round Key to simplify the encryption process. Parameter N is determined by the number of bits in an AES algorithm.

The hyper-chaotic system is

$$\begin{cases} x' = a_1(y - x) + w \\ y' = dx + ey - xz \\ z' = x^2 - nz \\ w' = b_1 x + cw \end{cases} \tag{6}$$

where a_1, d, e, n, b_1 and c are used as control parameters for the hyper-chaotic system. Let h represent anyone of x, y, z and w. The initial input parameter h_0 of the hyper -chaotic system is adopted to produce the hyper-chaotic sequence h_s.

7) The chaotic sequence h_s is transformed into an integer sequence h_s^*,

$$h_s^* = \left| \left\lfloor (h_s - \lfloor h_s \rfloor) \times 10^{15} \right\rfloor \right| \bmod 256 \tag{7}$$

where $\lfloor h_s \rfloor$ represents the maximal integer not greater than h_s.

8) A new hyper-chaotic sequence $P = \{p_1, p_2, ..., p_n\}$ is formed by chaotic sequences. If $w_s^* \bmod 4 = 0$, then p_s takes x_s^* to perform circular shift operations. The other three results correspond to the other three chaotic sequences. $w_s^7 w_s^6 ... w_s^0$ represents the integer p_s, $w_s^t \in \{0, 1\}$, $s = 1, 2, ..., n$, and $t = 0, 1, ..., 7$.

9) The pseudo-random matrix $\mathbf{M}$ is produced by the hyper-chaotic system

$$\mathbf{M} = \{M_t | M_t = \text{round}(10^4 y_t \bmod 8), \ t = 0, 1, ..., 7\} \tag{8}$$

10) The final encrypted image is obtained by disturbing the image after the AES algorithm with the cycle shift operation and the pseudo-random sequence.

In the decryption process, the inverse cycle shift operation and the inverse AES algorithm are successively executed to decrypt the encrypted image. Then the inverse DCT is utilized to restore the resulting image. Finally, the decrypted image G' can be obtained by the inverse scrambling operation.

Besides, for the color image to be encrypted, it can be divided into R, G and B components. Then the components are compressed and encrypted respectively, and the three encrypted images are merged to produce the final color encrypted image.

4. Simulation results and analyses

The proposed image compression and encryption algorithm based on the AES and the hyper-chaotic system is simulated in MATLAB 2012(a). The gray images *Lax*, *Woman* and *Peppers* of size 256 × 256 are served as the test images, shown in Figs. 3**a**, 3**d** and 3**g**. The key parameters are set as: $x_0 = 0.2$, $y_0 = 0.3$, $z_0 = 0.4$ and $w_0 = 0.5$. The encrypted images *Lax*, *Woman* and *Peppers* are given in Figs. 3**b**, 3**e** and 3**h**. As can be observed from the figures, the encrypted images do not show any visually valuable information about the original images. The correct decrypted images are shown in Figs. 3**c**, 3**f** and 3**i**.

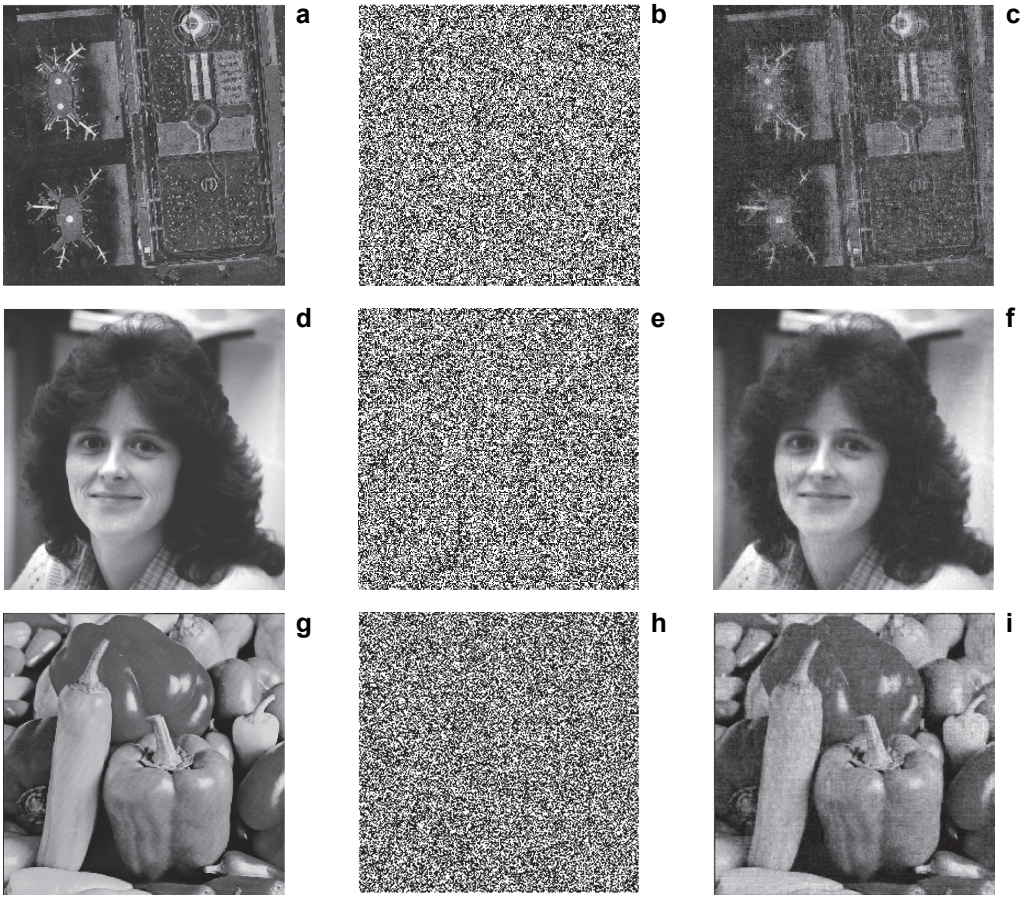

Fig. 3. Test results: *Lax* (**a**), encrypted *Lax* (**b**), decrypted *Lax* (**c**); *Woman* (**d**), encrypted *Woman* (**e**), decrypted *Woman* (**f**); *Peppers* (**g**), encrypted *Peppers* (**h**), and decrypted *Peppers* (**i**).

4.1. Histograms

Histogram is a common measure of statistical characteristics of digital images. It is well known that an acceptable image encryption algorithm must ensure the histograms of different encrypted images uniformed or similar to each other as possible. Figures 4**a**, 4**c** and 4**e** are the histograms of images *Lax*, *Woman* and *Peppers*, respectively, while Figs. 4**b**, 4**d** and 4**f** show the histograms of their corresponding encrypted images, respectively. It can be observed that the histograms of the encrypted images are similar although those of different plaintext images are apparently different. Therefore, the

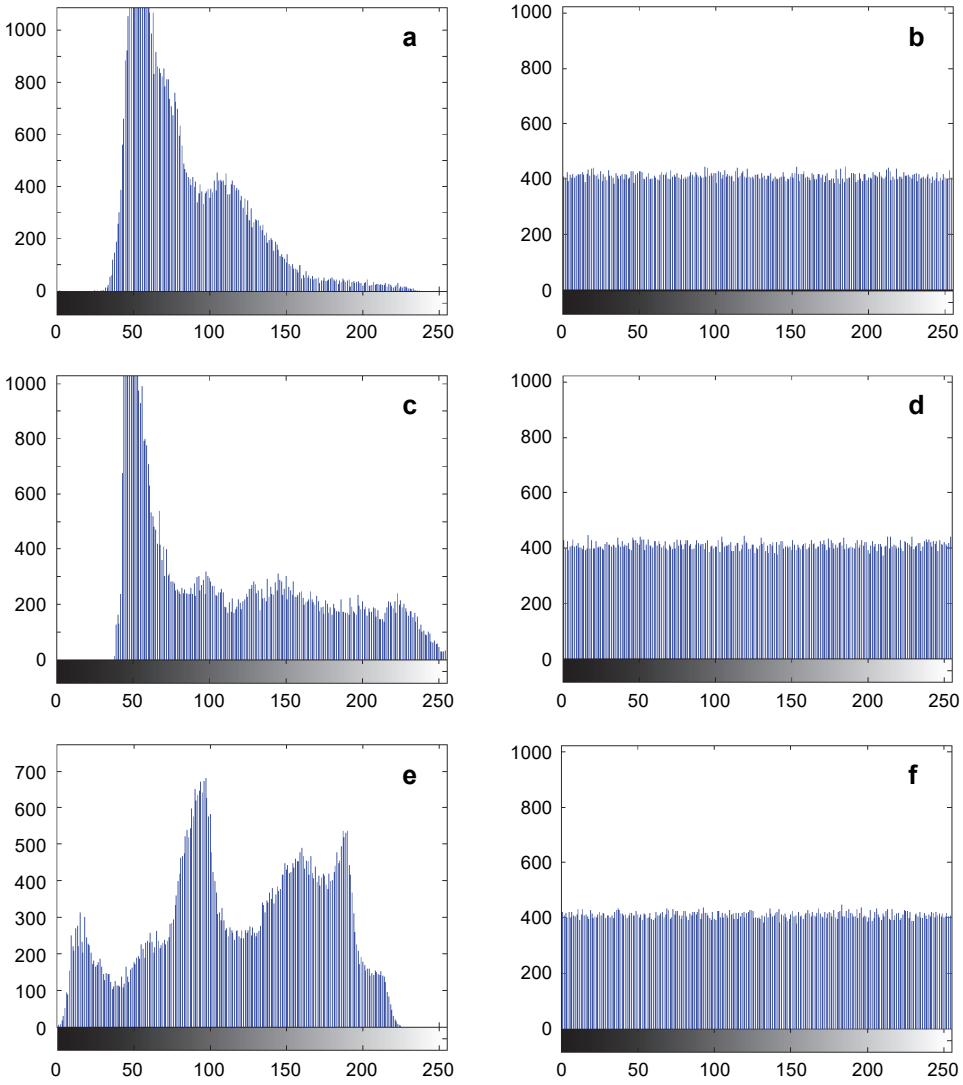

Fig. 4. Histograms: *Lax* (**a**), encrypted *Lax* (**b**); *Woman* (**c**), encrypted *Woman* (**d**); *Peppers* (**e**), and encrypted *Peppers* (**f**).

proposed image compression and encryption algorithm can resist the statistical analysis attack.

4.2. Adjacent pixel correlation

The correlation between two adjacent pixels in the original image is very high. Generally, the correlation between two adjacent pixels in the encrypted image should be much weaker than that in the original image. To test the correlation between any two adjacent pixels of the test image, 7 000 pairs of adjacent pixels are extracted from the plaintext image and the encrypted image, respectively. The correlation coefficient can be calculated as

$$r_{ab} = \frac{|\mathrm{cov}(a, b)|}{\sqrt{\frac{1}{M}\sum_{i=1}^{M}\left[a_i - E(a)\right]^2}\sqrt{\frac{1}{M}\sum_{i=1}^{M}\left[b_i - E(b)\right]^2}} \tag{9}$$

$$\mathrm{cov}(a, b) = \frac{1}{M}\sum_{i=1}^{M}\left[a_i - E(a)\right]\left[b_i - E(b)\right] \tag{10}$$

$$E(a) = \frac{1}{M}\sum_{i=1}^{M} a_i \tag{11}$$

where a and b represent the pixel values of two adjacent pixels; $E(a)$ and $\mathrm{cov}(a, b)$ represent the average value and the covariance value, respectively. The correlation coefficients of the proposed image compression and encryption algorithm and the algorithms in [29, 31] are compiled in Table 1, which shows that the proposed image compression and encryption algorithm has better performance than the other two algorithms. Figures 5**a**, 5**c** and 5**e** are the correlation distribution of two adjacent pixels of the test images *Lax*, *Woman* and *Peppers*, respectively. Figures 5**b**, 5**d** and 5**f** are the cor-

T a b l e 1. Correlation coefficient of adjacent pixels.

Algorithm	Image	*H* direction	*V* direction	*D* direction
	Woman	0.9902	0.9891	0.9826
Proposed algorithm	Encrypted *Woman*	0.0254	0.0193	0.0075
Reference [29]	Encrypted *Woman*	−0.5759	0.4837	0.5269
Reference [31]	Encrypted *Woman*	0.1583	0.0874	−0.1296
	Peppers	0.9297	0.9139	0.8837
Proposed algorithm	Encrypted *Peppers*	0.0059	0.0031	0.0127
Reference [29]	Encrypted *Peppers*	−0.6453	0.5273	0.6532
Reference [31]	Encrypted *Peppers*	0.1739	0.0937	−0.1759

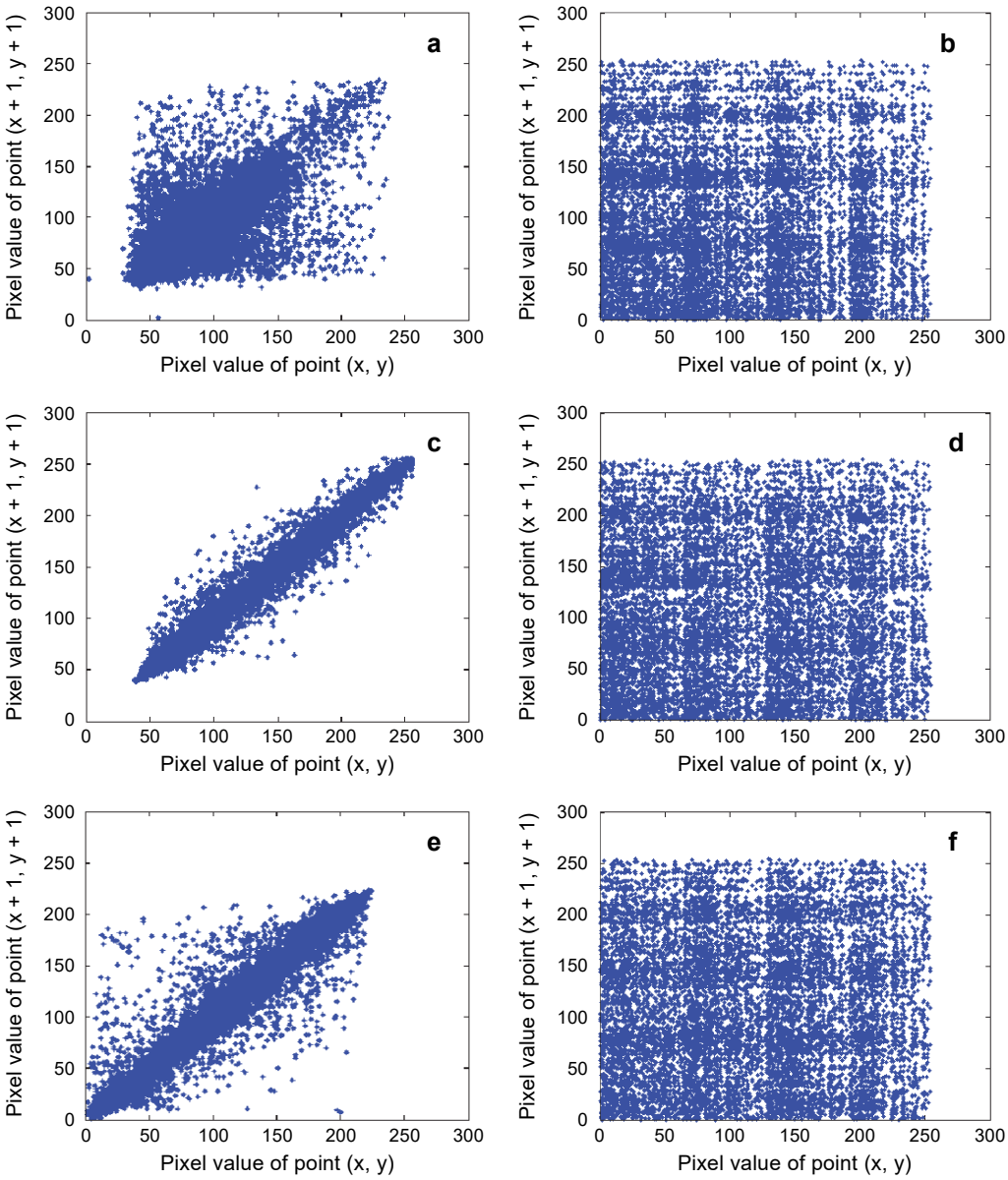

Fig. 5. Correlation distribution of two diagonally adjacent pixels: *Lax* (**a**), encrypted *Lax* (**b**); *Woman* (**c**), encrypted *Woman* (**d**); *Peppers* (**e**), and encrypted *Peppers* (**f**).

relation distribution between two adjacent pixels of the encrypted images. Moreover, it can be concluded that the attacker cannot obtain any valuable information from the encrypted image by merely analyzing the correlation of two adjacent pixels.

4.3. Compression performance

The proposed image compression and encryption algorithm can compress and encrypt the image simultaneously. To evaluate the quality of the decrypted images, the peak signal-to-noise ratio (PSNR) is employed. The decrypted images with different compression ratios are shown in Fig. 6. Table 2 lists the PSNR values for the decrypted

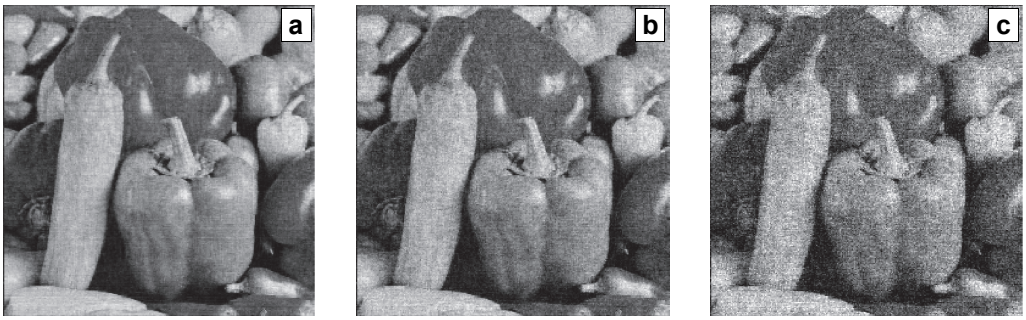

Fig. 6. Decrypted images with different compression ratios: 70.31% (**a**), 43.75% (**b**), and 23.43% (**c**).

T a b l e 2. Peak signal-to-noise ratio under different compression ratios.

	Compression ratio		
	70.31%	43.75%	23.43%
Proposed algorithm	32.6573	27.8951	19.6375
Reference [14]	28.7683	22.9375	16.7549
Reference [35]	29.2475	24.2763	17.0574

images with different compression ratios. It is shown that the proposed image compression and encryption algorithm has a good performance in compression analysis and is better than the algorithms in [14] and [35].

4.4. Key space and key sensitivity

The key space of a secure and effective image encryption algorithm should be large enough to make the exhaustive attack impractical or invalid. The initial value h_0 of the hyper-chaotic system is the key of the proposed image compression and encryption algorithm. Simulation results display that the sensitivity of parameter h_0 is up to 10^{-15}. In addition, the period of Arnold transform is 6 when the original image is segmented into the sub-image blocks of size 8×8. Obviously, the key space of the proposed image compression and encryption algorithm is greater than 2^{100} which is large enough to resist the exhaustive attack.

A good image encryption algorithm should be sensitive to the keys. The key sensitivity can be evaluated by comparing the decrypted images obtained with slight change

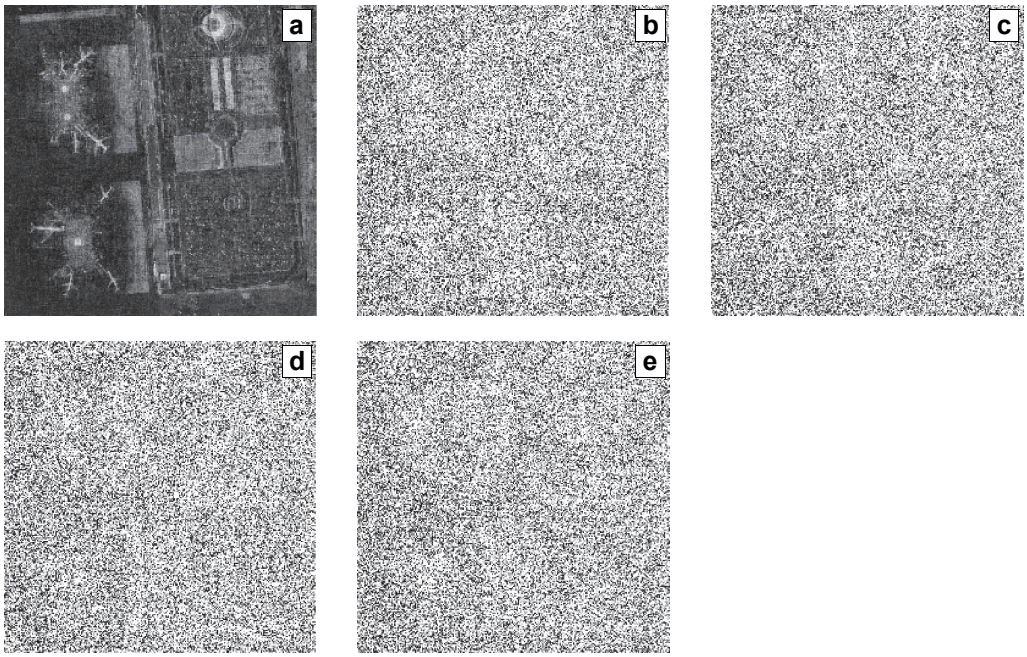

Fig. 7. Decrypted images with different keys: correct key (**a**), $x_0 = 0.2 + 10^{-15}$ (**b**), $y_0 = 0.3 + 10^{-15}$ (**c**), $z_0 = 0.4 + 10^{-15}$ (**d**), and $w_0 = 0.5 + 10^{-15}$ (**e**).

to the keys. And it can be concluded that the minimal variation of the initial input value is 10^{-15} from the results. Figures 7**a** shows the decrypted image with the correct key and Figs. 7**b**–7**e** are the decrypted images when one of the four initial values of the hyper-chaotic system is altered slightly and the remaining three initial values remain unchanged. To sum up, the proposed image compression and encryption algorithm is sensitive enough to the keys.

4.5. Robustness

During the process of image transmission, the encrypted images are affected inevitably by noises. When the noise is serious, the decrypted image will be distorted. To evaluate the effect of noise on the proposed image compression and encryption algorithm, it is assumed that the encrypted image is contaminated by Gaussian noise as

$$I' = I + kG \tag{12}$$

where I' and I are the noisy encrypted image and the pure encrypted image, respectively, k is the coefficient related to noise intensity.

Figure 8 shows the decrypted images under different noise intensities. Although the decrypted images become fuzzier with the increase in noise intensity, the effective

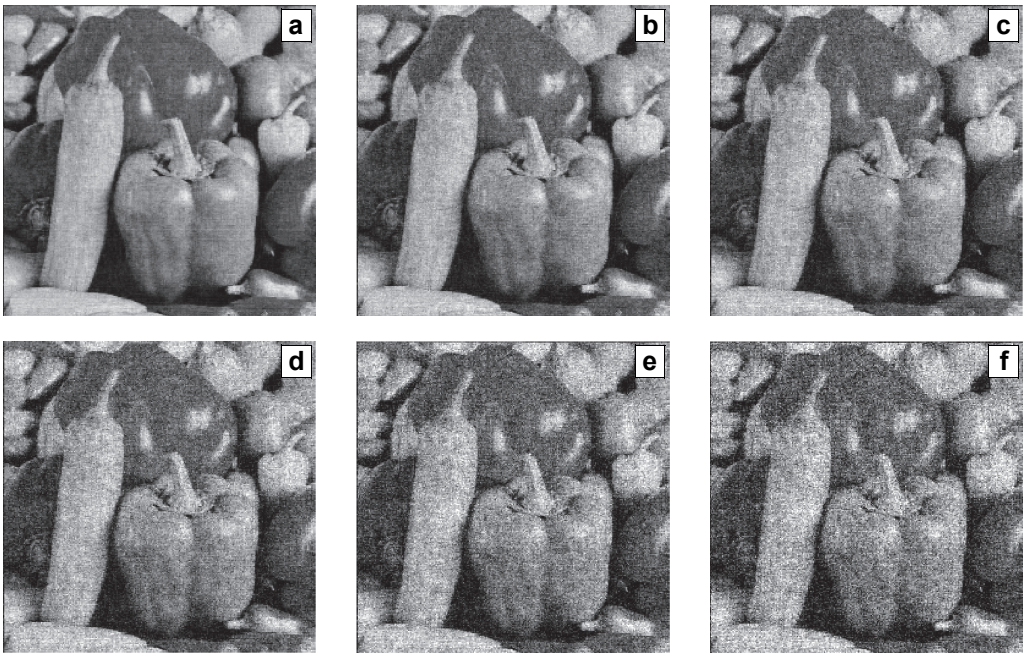

Fig. 8. Decrypted images with different noise intensities: $k = 1$ (**a**), $k = 5$ (**b**), $k = 10$ (**c**), $k = 15$ (**d**), $k = 20$ (**e**), and $k = 25$ (**f**).

information about the original image can still be recognized. Therefore, it can be considered that the proposed image compression and encryption algorithm has a high robustness against noise attacks.

5. Conclusion

An image compression and encryption algorithm based on the hyper-chaotic system, discrete cosine transform and AES is investigated. The hyper-chaotic system and AES are utilized to encrypt the DCT coefficients repeatedly. Meanwhile, the nonlinear process of the hyper-chaotic system is adopted to enhance the security of the proposed image compression and encryption algorithm. The proposed image compression and encryption algorithm weakens the block effect in image compression process with the Arnold map, and reduces the encoding bit rate for image transmission with the DCT. Simulation results indicate that the proposed image compression and encryption scheme is effective and secure against the statistical analysis attack, exhaustive attack and noise attack.

Acknowledgments – This work is supported by the National Natural Science Foundation of China (grant Nos. 61861029 and 61262084), 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 Department of Education of Guangdong Province Technological Innovation Program (grant No. 2017GKTSCX060).

References

[1] MATTHEWS R., *On the derivation of a "Chaotic" encryption algorithm*, Cryptologia **13**(1), 1989, pp. 29–41, DOI: 10.1080/0161-118991863745.

[2] FRIDRICH J., *Symmetric ciphers based on two-dimensional chaotic maps*, International Journal of Bifurcation and Chaos **8**(6), 1998, pp. 1259–1284, DOI: 10.1142/S021812749800098X.

[3] GUANRONG CHEN, YAOBIN MAO, CHUI C.K., *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos, Solitons and Fractals **21**(3), 2004, pp. 749–761, DOI: 10.1016/j.chaos.2003.12.022.

[4] KANSO A., GHEBLEH M., *A novel image encryption algorithm based on a 3D chaotic map*, Communications in Nonlinear Science and Numerical Simulation **17**(7), 2012, pp. 2943–2959, DOI: 10.1016/j.cnsns.2011.11.030.

[5] XIAOLING HUANG, GUODONG YE, *An efficient self-adaptive model for chaotic image encryption algorithm*, Communications in Nonlinear Science and Numerical Simulation **19**(12), 2014, pp. 4094–4104, DOI: 10.1016/j.cnsns.2014.04.012.

[6] JUN-XIN CHEN, ZHI-LIANG ZHU, CHONG FU, HAI YU, *Optical image encryption scheme using 3-D chaotic map based joint image scrambling and random encoding in gyrator domains*, Optics Communications **341**, 2015, pp. 263–270, DOI: 10.1016/j.optcom.2014.12.045.

[7] TIEGANG GAO, ZENGQIANG CHEN, *A new image encryption algorithm based on hyper-chaos*, Physics Letters A **372**(4), 2008, pp. 394–400, DOI: 10.1016/j.physleta.2007.07.040.

[8] CONGXU ZHU, *A novel image encryption scheme based on improved hyperchaotic sequences*, Optics Communications **285**(1), 2012, pp. 29–37, DOI: 10.1016/j.optcom.2011.08.079.

[9] GUODONG YE, KWOK-WO WONG, *An image encryption scheme based on time-delay and hyperchaotic system*, Nonlinear Dynamics **71**(1–2), 2013, pp. 259–267, DOI: 10.1007/s11071-012-0658-x.

[10] XIAOLING HUANG, GUODONG YE, *An image encryption algorithm based on hyper-chaos and DNA sequence*, Multimedia Tools and Applications **72**(1), 2014, pp. 57–70, DOI: 10.1007/s11042-012-1331-6.

[11] JIAN ZHANG, *An image encryption scheme based on cat map and hyperchaotic Lorenz system*, IEEE International Conference on Computational Intelligence and Communication Technology, 2015, pp. 78–82, DOI: 10.1109/CICT.2015.134.

[12] JIAN ZHANG, DEZHI HOU, HONGE REN, *Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system*, Mathematical Problems in Engineering, Vol. 2016, 2016, article ID 6408741, DOI: 10.1155/2016/6408741.

[13] XIANGJUN WU, DAWEI WANG, KURTHS J., HAIBIN KAN, *A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system*, Information Sciences **349–350**, 2016, pp. 137–153, DOI: 10.1016/j.ins.2016.02.041.

[14] 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.

[15] XIULI CHAI, ZHIHUA GAN, KANG YANG, YIRAN CHEN, XIANXING LIU, *An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations*, Signal Processing: Image Communication **52**, 2017, pp. 6–19, DOI: 10.1016/j.image.2016.12.007.

[16] YANG LIU, XIAOJUN TONG, JING MA, *Image encryption algorithm based on hyper-chaotic system and dynamic S-box*, Multimedia Tools and Applications **75**(13), 2016, pp. 7739–7759, DOI: 10.1007/s11042-015-2691-5.

[17] XUANPING ZHANG, WEIGUO NIE, YOULING MA, QINQIN TIAN, *Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box*, Multimedia Tools and Applications **76**(14), 2017, pp. 15641–15659, DOI: 10.1007/s11042-016-3861-9.

[18] KUN ZHAN, DONG WEI, JUNHUI SHI, JUN YU, *Cross-utilizing hyperchaotic and DNA sequences for image encryption*, Journal of Electronic Imaging **26**(1), 2017, article ID 013021, DOI: 10.1117/1.JEI.26.1.013021.

[19] XINGYUAN WANG, SIWEI WANG, YINGQIAN ZHANG, CHAO LUO, *A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems*, Optics and Lasers in Engineering **103**, 2018, pp. 1–8, DOI: 10.1016/j.optlaseng.2017.11.009.

[20] XIAOWEI LI, YING WANG, QIONG-HUA WANG, YANG LIU, XIN ZHOU, *Modified integral imaging reconstruction and encryption using an improved SR reconstruction algorithm*, Optics and Lasers in Engineering **112**, 2019, pp. 162–169, DOI: 10.1016/j.optlaseng.2018.09.015.

[21] TAUBMAN D., *High performance scalable image compression with EBCOT*, IEEE Transactions on Image Processing **9**(7), 2000, pp. 1158–1170, DOI: 10.1109/83.847830.

[22] MANICCAM S.S., BOURBAKIS N.G., *Lossless image compression and encryption using SCAN*, Pattern Recognition **34**(6), 2001, pp. 1229–1245, DOI: 10.1016/S0031-3203(00)00062-5.

[23] ALFALOU A., BROSSEAU C., *Optical image compression and encryption methods*, Advances in Optics and Photonics **1**(3), 2009, pp. 589–636, DOI: 10.1364/AOP.1.000589.

[24] SAPNA SASIDHARAN, JITHIN R., *Selective image encryption using DCT with stream cipher*, International Journal of Computer Science and Information Security **8**(4), 2010, pp. 268–274.

[25] MIRZAEI O., YAGHOOBI M., IRANI H., *A new image encryption method: parallel sub-image encryption with hyper chaos*, Nonlinear Dynamics **67**(1), 2012, pp. 557–566, DOI: 10.1007/s11071-011-0006-6.

[26] HEGUI ZHU, CHENG ZHAO, XIANGDE ZHANG, *A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem*, Signal Processing: Image Communication **28**(6), 2013, pp. 670–680, DOI: 10.1016/j.image.2013.02.004.

[27] 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.

[28] 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, DOI: 10.1016/j.ijleo.2014.06.054.

[29] YING CHU, XIAOMAN WANG, PENG LIU, SHUCHANG LIU, ZHIQIANG HAN, *Research on chaos encryption method in image DCT domain*, Journal of Image and Signal Processing **3**(4), 2014, pp. 105–112, DOI: 10.12677/jisp.2014.34014.

[30] 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.

[31] AWAD A.M., HASSAN R.F., SAGHEER A.M., *Chaos image encryption based on DCT transforms and Henon map*, International Journal of Computer Applications **127**(11), 2015, pp. 1–7, DOI: 10.5120/ijca2015906532.

[32] XIAOLING HUANG, GUODONG YE, HUAJIN CHAI, OU XIE, *Compression and encryption for remote sensing image using chaotic system*, Security and Communication Networks **8**(18), 2015, pp. 3659–3666, DOI: 10.1002/sec.1289.

[33] XIAO-JUN TONG, MIAO ZHANG, ZHU WANG, JING MA, *A joint color image encryption and compression scheme based on hyper-chaotic system*, Nonlinear Dynamics **84**(4), 2016, pp. 2333–2356, DOI: 10.1007/s11071-016-2648-x.

[34] MIAO ZHANG, XIAOJUN TONG, *Joint image encryption and compression scheme based on a new hyper-chaotic system and curvelet transform*, Journal of Electronic Imaging **26**(4), 2017, article ID 043008, DOI: 10.1117/1.JEI.26.4.043008.

[35] 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, DOI: 10.1007/s11042-016-3600-2.

[36] 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.

Received October 31, 2018
in revised form December 2018