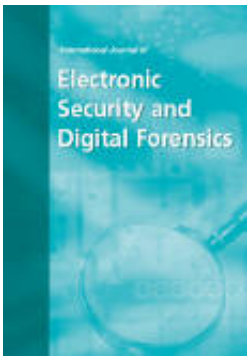


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

Image encryption based on 3D Arnold and elementary cellular automata method

Rui Yang, Lijuan Feng, Jiangjiang Li

DOI: 10.1504/IJESDF.2024.10052835

Article History:
Received: 10 October 2022
Accepted: 15 November 2022
Published online: 12 January 2024

Image encryption based on 3D Arnold and elementary cellular automata method

Rui Yang*

School of Electronic and Electrical Engineering,
Zhengzhou University of Science and Technology,
Zhengzhou 450000, China
and
Intelligent Information Processing and Control Engineering
Technology Research Center of Henan Province,
Zhengzhou 450000, China
Email: yangruishiu@qq.com
*Corresponding author

Lijuan Feng and Jiangjiang Li

School of Electronic and Electrical Engineering,
Zhengzhou University of Science and Technology,
Zhengzhou 450000, China
Email: 857003841@qq.com
Email: 1124905128@qq.com

Abstract: The traditional image encryption methods have some problems, such as poor security and inefficient encryption. This paper proposes a new image encryption method based on 3D Arnold-oriented elementary cellular automata. The new image encryption method first uses 3D Arnold to scramble pixel positions. Then, the elementary cellular automata based on quad-tree decomposition is used to further confuse the scrambled images at the specific level to obtain ciphertext images. The experiment results show that this new method can achieve good encryption effect with fewer iteration times and has strong sensitivity to plaintext and key. It also can effectively resist differential attack.

Keywords: image encryption; elementary cellular automata; ECA; 3D Arnold; quad-tree decomposition.

Reference to this paper should be made as follows: Yang, R., Feng, L. and Li, J. (2024) 'Image encryption based on 3D Arnold and elementary cellular automata method', *Int. J. Electronic Security and Digital Forensics*, Vol. 16, No. 1, pp.97–111.

Biographical notes: Rui Yang is with School of Electronic and Electrical Engineering, Zhengzhou University of Science and Technology. She graduated from Wuhan University. Her major is intelligent control.

Lijuan Feng is with School of Electronic and Electrical Engineering, Zhengzhou University of Science and Technology. Her major is intelligent control, image processing.

Jiangjiang Li graduated from Henan University of Technology, majoring in Control Science and Engineering. He had published several papers related to the research.

1 Introduction

With the rapid development of computer network communication technology, information security has attracted more attentions. The traditional encryption method can be effectively applied to the encryption with a small amount of data, but it is extremely inefficient for the image with a large amount of data. At present, in order to fully adapt to the characteristics of image data, the chaotic dynamics system is proposed to be applied into digital image encryption, which has attracted the attention from many researchers (Feizi-Derakhsh and Kadhim, 2022; Ma et al., 2019).

Chaotic system is a complex nonlinear system, which has many good performances consistent with the requirements of cryptography. Because it is extremely sensitivity to initial values and system parameters, it has the features of unpredictability and pseudo-randomness (Zhao, 2022). Therefore, chaos theory has been widely used in the field of digital image encryption. Cao et al. (2011) used Logistic system to generate random permutation with uniform distribution to drive the image to generate scrambled image. Song et al. (2013) proposed a new image encryption algorithm based on the combination of Baker map and space-time chaos. Belazi et al. (2016) proposed a new image encryption method based on substitution permutation networks and chaos. Enayatifar et al. (2015) used 3D chaotic map to scramble image pixels, and then used 2D second-order cellular automata to confuse images.

Cellular Automata (CA) is a concept in the study of self-organising characteristics system (Wacker, 2019). CA has discrete dynamic behaviour, and its state and space-time are characterised by discretisation. The interaction between cells in CA satisfies the random and diffusion characteristics of cryptography, so CA is very suitable for image encryption.

In recent years, cellular automata have been favoured by researchers in the world. For example, Hosseini et al. (2014) proposed an encryption scheme based on elementary cellular automata (ECA). Enayatifar et al. (2015) proposed a new image encryption algorithm using a hybrid model of deoxyribose and cellular automata, which had strong anti-attacking. According to the characteristics of image file types, Chai et al. (2017) proposed an image encryption algorithm based on one-dimensional trigger-cell automata. Wang and Luan (2013) proposed an image encryption algorithm based on chaos and cellular automata, first using chaotic sequence to encrypt the image, and then using cellular automata for secondary encryption.

In this paper, our main contributions are as follows: 3D Arnold map is used to carry out random iteration on digital images. In order to reduce the number of iterations, quad-tree decomposition method is introduced to carry out elementary cellular automata evolution under different rules for each part. Finally, the encrypted images are obtained.

This paper is organised as follows. In Section 2, 3D Arnold and cellular automata are introduced. Section 3 illustrates the proposed image encryption method. In Section 4, experiments are conducted to demonstrate the effectiveness of the proposed method. Section 5 concludes this paper.

2 Preliminaries

2.1 3D Arnold

Chaotic map plays an important role in image encryption because of its high sensitivity to initial values. The 2D chaotic map is a generalisation of a nonlinear map, which is called generalised cat map, and it is a reversible chaotic map. The formula of generalised cat map is shown in equation (1)

$$\begin{pmatrix} x_n+1 \\ y_n+1 \end{pmatrix} = A \bullet \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\text{mod } N) \tag{1}$$

Since det(A) = 1, the map is an area-preserving map (there are no attractors), and it is an one-to-one map. In generalised cat map, the eigenvalues of matrix A are $\lambda_1 = (3+\sqrt{5})/2 > 1$ and $\lambda_2 = (3-\sqrt{5})/2 < 1$ respectively, so its Lyapunov exponents: $\gamma_1 = \ln \lambda_1 > 0$, $\gamma_2 = \ln \lambda_2 < 0$. γ_1 is positive indicating that the map is chaotic, which means that the map results are highly sensitive to the initial values. When $a = b = 1$, it is the Arnold transformation. In this paper, a 3D generalised Arnold map is selected. Compared with the 2D Arnold map, the key space can be expanded and the iteration speed can also be improved, which can be applied to various image encryption algorithms. The general form of 3D generalised Arnold map is as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \text{mod}(N) \tag{2}$$

where det(A) = 1, matrix A is expressed as follows. First let det(A') = 1, A' is:

$$A' = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{bmatrix} \tag{3}$$

Let $A = A'^2$, so matrix A is:

$$A = \begin{bmatrix} 3 & 5 & 6 \\ 5 & 9 & 11 \\ 6 & 11 & 14 \end{bmatrix} \tag{4}$$

Finally, the three-dimensional Arnold representation used for the encryption algorithm in this paper is:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 3 & 5 & 6 \\ 5 & 9 & 11 \\ 6 & 11 & 14 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \text{mod}(N) \tag{5}$$

2.2 Cellular automata

2.2.1 Elementary cellular automata

One-dimensional elementary cellular automata (1DECA) are a special class of discrete dynamical systems consisting of one dimensional array N composed of finite cell objects. The state of each cell at time $t + 1$ is determined by the state of its neighbourhood cells at time t and the local evolution rule F. Figure 1 shows a simple spatial arrangement structure of elementary cellular automata, which is composed of three neighbourhood cells and eight neighbourhood cell state combinations, so there are $2^8 = 256$ rules. The state $S \in \{0, 1\}$ of each cell at time $t + 1$ is represented by equation (6).

$$S_i^{t+1} = F\left(S_{i-1}^t, S_i^t, S_{i+1}^t\right) \tag{6}$$

where S_i^t represents the state of the cell at the position i at time t. Table 1 lists the local state transition rules represented by the one-dimensional cellular automata of rule 90.

Figure 1 One-dimensional cellular automata space

Table 1 State transition of rule 90

$S_{i-1}^t S_i^t S_{t+1}^t$	S_i^{t+1}	$S_{i-1}^t S_i^t S_{t+1}^t$	S_i^{t+1}
111	0	011	1
110	1	010	0
101	0	001	1
100	1	000	0

2.2.2 Reverse cellular automata

Reverse cellular automata (RCA) (Zhang et al., 2016; Zheng et al., 2012) refer to a cellular automata in a given initial state configuration C_0, after some evolutionary rule F making n transitions, then the new state configuration C_n is obtained. So n is taken as the initial state. After n transitions by evolution rule F^{-1}, the initial configuration C_0 of the cellular automata can be obtained. The following rules are:

$$\begin{cases} C_n = F(C_0) \\ C_0 = F^{-1}(C_n) \end{cases} \tag{7}$$

The local rule F and F^{-1} in formula (7) can be the same. It is found that in the 256 rules of classical one-dimensional cellular automata, only six rules are reversible. They are nos. 15, 51, 85, 170, 204 and 240, and their reversibility is related to the boundary conditions. Because the number of reverse rules is too small, the security of image encryption cannot be guaranteed. In order to solve this problem, Wolfram proposed a scheme to construct such reverse cellular automata (RCA), that is, the state S_i^{t+1} of the i^{th} cell at time $t + 1$ is determined by the corresponding state value S_i^t at time t, the state values of its three neighbouring cells and the corresponding cell state value S_i^{t-1} at time $t - 1$. Its formula is as follows:

$$F: S_i^{t+1} = \begin{cases} F_E\left(S_{i-1}^t, S_i^t, S_{i+1}^t\right) & S_i^{t-1} = 0 \\ 1 - F_E\left(S_{i-1}^t, S_i^t, S_{i+1}^t\right) & S_i^{t-1} = 1 \end{cases} \tag{8}$$

where F_E is the elementary cellular automata rule. Since S_i^{t+1} is either 0 or 1, there are 16 possible combinations of RCAs that are more complex than ECA. The corresponding ECA rules are numbered with the symbol R to distinguish them. For example, Table 2 lists the local state transition rule corresponding to ECA of rule 75, which constructs a local state transition rule with RCA 75R.

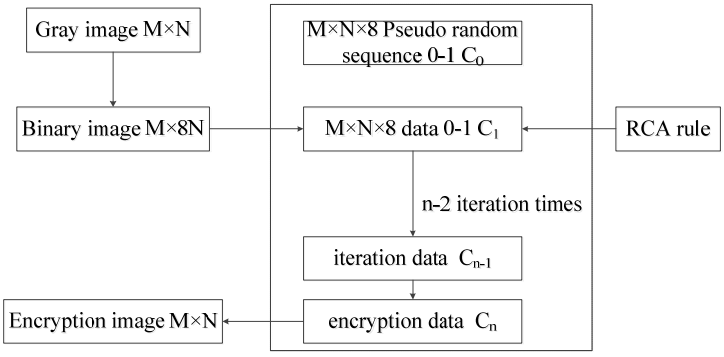
Table 2 RCA 75R

$S_{i-1}^t S_i^t S_{i+1}^t$	S_i^{t+1}	
	$S_i^{t-1} = 0$	$S_i^{t-1} = 1$
111	0	1
110	1	0
101	0	1
100	0	1
011	1	0
010	0	1
001	1	0
000	1	0

2.2.3 Reverse cellular automata encryption and decryption algorithm

The number of rules to construct RCA is large, and it can form more complex evolutionary behaviour, so it is suitable for image encryption. When RCA encryption is applied, the $M \times N$ plaintext image is firstly executed with one-dimensional, and then each pixel is represented as 8-bit binary data to be encrypted, denoted as C_1. At the same time, the pseudo-random 0-1 sequence with size of $8 \times M \times N$ is generated as the initialisation state of RCA, denoted as C_0. Then, $n - 1$ iterations are conducted to obtain C_n, and converted to the encrypted image. The RCA encryption process is shown in Figure 2.

Figure 2 RCA encryption process

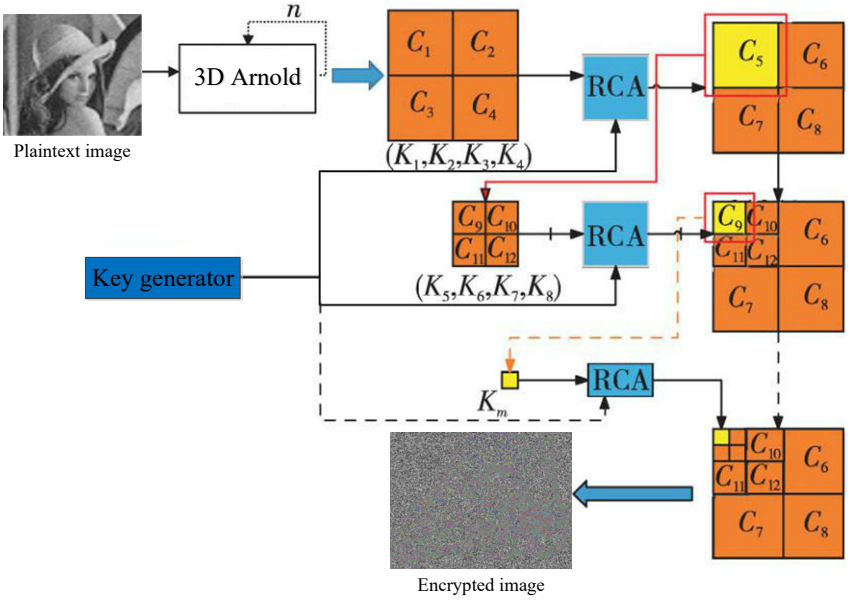


The decryption process is the inverse process of the encryption process. C_n and C_{n-1} are taken as C_0' and C_1' during the decryption respectively. Then, the C_n' is obtained through $n-1$ iterations under the RCA evolution rules. The decryption result can be obtained by converting the previous sequence C_{n-1}'.

3 Proposed image encryption process

The new algorithm designed in this paper makes full use of the characteristics of elementary cellular automata for image encryption, which presents a simple structure, strong parallelism encryption and decryption algorithm with better information hiding effect, fast execution speed and good security performance.

Figure 3 Encryption scheme based on 3D chaotic mapping and RCA (see online version for colours)



The process of proposed algorithm is as follows. The digital image is iterated with n ($n \geq 5$) 3D Arnold mapping operations to achieve pixel scrambling. In order to reduce the number of iterations, this paper introduces the quadtree decomposition method and uses the cellular automata transformation under different transformation rules to achieve better pixel confusion effect. The encryption process is shown in Figure 3.

3.1 Pixel scrambling

The 3D Arnold map is scrambled n times. The research shows that the 3D Arnold transformation is periodic under different order N. For digital images with size 256×256, the scrambling period $T_{256} = 192$. For 512×512 pixel digital images, the scrambling period $T_{512} = 384$, so the iteration number n cannot be too large, because it greatly affects the encryption rate and scrambling effect. The iteration number n ($n \geq 5$) of the scrambling in this paper is generated by the random generator.

3.2 Pixel confusion

After scrambling the above pixels, the scrambled image $A_{M\times N}$ is obtained, and the reverse cellular automata is further used to encrypt the image pixel values. The specific encryption process is as follows:

1 Binarise the scrambled image $A_{M\times N}$ and represent each pixel with 8-bit binary to get $B_{M\times 8N}$.

2 Use quadtree decomposition to decompose the image $B_{M\times 8N}$ into four sub-graphs C_i ($i = 1, 2, 3, 4$) with same size.

3 The initial pseudo-random sequence Q_m and the key K_i generated by the key generator, where $m = 1$ and K_i is the local conversion rule of RCA.

4 Take C_i ($i = 1, 2, 3, 4$) as initial state Q_m and evolve according to RCA rule K_i to obtain new C_i ($i = i + 4$). At this time, C_i represents C_5, C_6, C_7 and C_8. C_6, C_7 and C_8 are used as encrypted images,

5 Then quadtree is used to decompose the C_5 in the upper left corner into four sub-graphs C_i ($i = i + 4$) with equal size. At this time, C_i represents C_9, C_{10}, C_{11} and C_{12}.

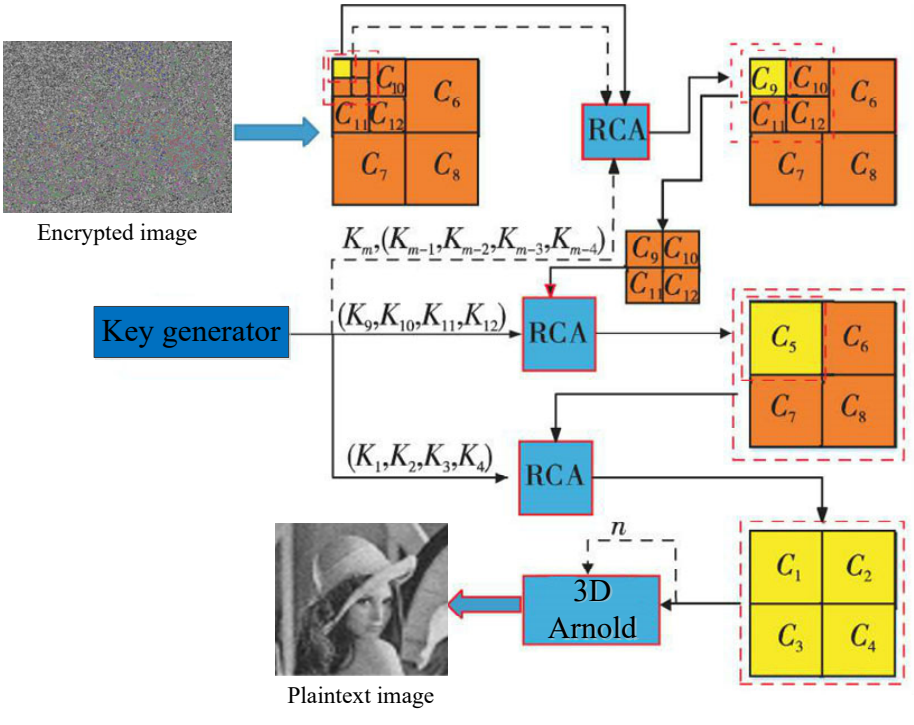
6 Repeat steps 3~5, the iteration number is m ($m = 1, 2, 3, \ldots$), $i = m \times i + 4$, until the size of image C_i is 8×8.

7 Fuse all sub-encrypted graphs to obtain the final encrypted image.

3.3 Key selection

(M, N, n, K_i, Q_m, L, i, m) is selected as the key, where M and N are the size of the row and column of the input image respectively. n is the number of 3D Arnold map scrambling. K_i is the RCA local transformation rule of the sub-graph of block i. Q_m is the initialisation sequence corresponding to the m^{th} quadtree decomposition. L is the number of RCA iterations.

Figure 4 Decryption scheme based on 3D chaotic mapping and RCA (see online version for colours)



3.4 *Decryption process*

The decryption process is the reverse operation of the encryption process. For the ciphertext image with the size of $M \times N$, the pixel value is decrypted first. Before encryption, the image is restored layer by layer according to the inverse process of quadtree decomposition, initialisation sequence Q_m and RCA evolution. Then the plaintext image is obtained through the reverse 3D Arnold map transformation. The decryption process is shown in Figure 4.

4 Experiment and analysis

The experiment is conducted on Windows10, MATLAB 7a, memory is 60G, one GPU. The key set used in the proposed algorithm is (256, 256, 5, K_i, Q_m, i, 3), where $K_i = \{75R, 90R, 105R, 150R\}$. After each quadtree decomposition, the rules in K_i change one time around the loop. $Q_m = \{Q_1, Q_2, Q_3\}$ represents the pseudo-random sequence 0-1 of one-dimensional array with size 2^{14}, 2^{12}, 2^{10}, respectively, i = {1, 2, 3, 4, …, 10, 11, 12}. The Lena image with a size of 256 × 256 is encrypted. The encryption process is shown in Figure 5.

Figure 5 Encryption process for Lena image, (a) plaintext image (b) scrambling image (c) encrypted image

(a) (b) (c)

3D Arnold map transformation is performed five times for the encrypted image to form a scrambled image. Then quadtree decomposition is performed three times. After each decomposition, RCA transformation and encryption are performed for each part of the sub-graph to obtain ciphertext image. The encryption effect shows that the proposed algorithm can realise information encryption with high efficiency and security in the case of less scrambling iteration times and RCA conversion times.

During decryption, the pixel value of ciphertext image is inversely transformed by RCA under the same rule, and then the decrypted image is obtained through inverse 3D-Arnold map conversion.

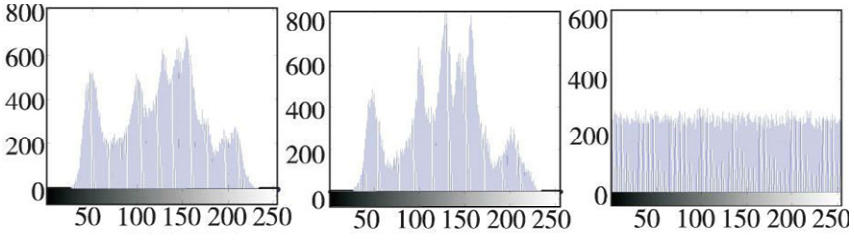
4.1 Key space analysis

The key space refers to the total number of different passwords that can be used by the cryptographic system. It can be seen from Section 3.3 that the key composition in this paper is (M, N, n, K_i, Q_m, L, i, m), and the key space is $2^8 \times 2^8 \times n \times 2^{32} \times 2^{40} \times 1 \times 12 \times 5 \approx n \times 2^{94}$. Therefore, the key space increases with the number of iterations. If the one-dimensional cellular automata is extended to the two-dimensional Moor-type cellular automata, the key space will increase to 2^{512}, then the key space of the algorithm in this paper is sufficient to resist exhaustive attack.

4.2 Histogram analysis

Figure 6 is the histogram of Lena image in the encryption process. Although it can be seen from Figure 5(b) that the plaintext image has a good scrambling effect in the scrambling stage, and the comparison analysis of Figures 6(a) and 6(b) shows that it is almost global scrambling, it also clearly reflects that the histogram distribution is not uniform. Therefore, only the pixel scrambling cannot achieve good encryption effect, and the pixel value confusion is needed. After quadtree decomposition and reverse cellular automata conversion, the encrypted image is obtained. It can be seen from Figure 6(c) that the histogram distribution is relatively uniform, which means that the ciphertext image pixel values obtained by the encryption algorithm in this paper are almost uniformly distributed. If the pixel values are more random, the resistance to statistical analysis is stronger.

Figure 6 Histogram of encryption process, (a) histogram of plaintext image (b) histogram of scrambling image (c) histogram of encrypted image



(a) (b) (c)

4.3 Correlation analysis

The correlation coefficient can measure the degree of correlation between adjacent pixels. If the correlation coefficient is close to 0, the ciphertext performance is better. The correlation coefficient is calculated according to equation (5). 2,000 pairs of adjacent pixel points are randomly selected in horizontal, vertical and diagonal directions respectively to analyse their correlation (Karim et al., 2022; Li et al., 2022). Figure 7 shows the correlation comparison between the adjacent pixels of the original Lena image and the encrypted image in three directions. It can be seen that the random pixels of the encrypted image in three directions have low correlation. At the same time, Table 3 shows the comparison of correlation coefficient after Lena image is encrypted by the proposed algorithm and other methods GSAPSO-MQC (Yin and Li, 2020), NLCC (Hou et al., 2020), CDDM (Teng et al., 2019) and SNNPST (Tan et al., 2022). The results show that the correlation between adjacent pixels of ciphertext image obtained by the proposed algorithm is lower, so the ciphertext is more secure.

$$\rho_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

where

$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]$$

$$E(x) = \frac{1}{N} \times \sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left[x_i - E\left(x_i\right)\right]^2.$$

Figure 7 Correlation analysis comparison (see online version for colours)

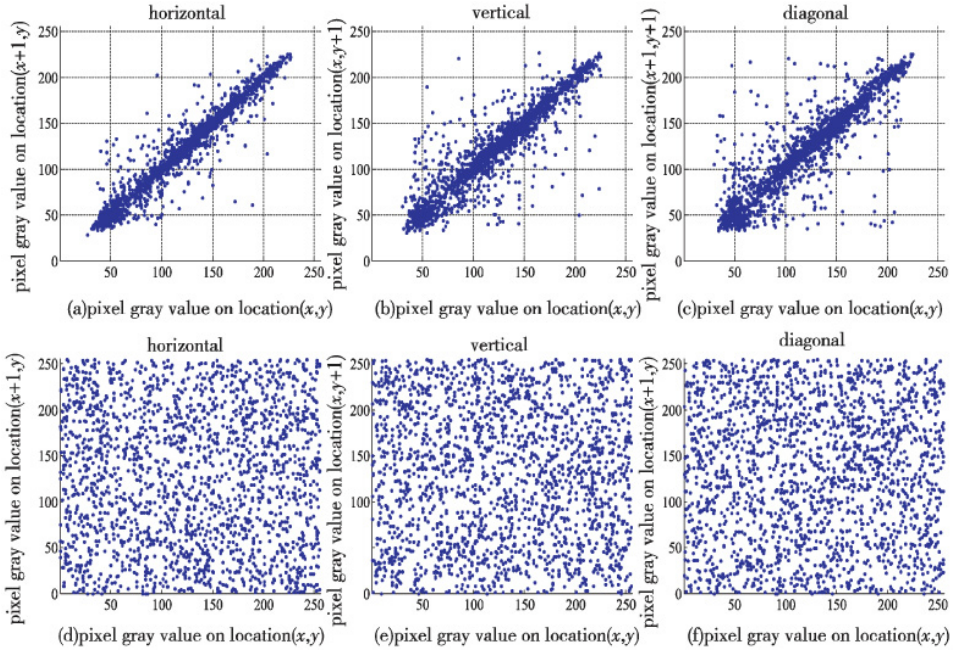


Table 3 Correlation coefficient comparison with different methods

Direction	*Plaintext*	*Proposed*	*GSAPSO–MQC*	*NLCC*	*CDDM*	*SNNPST*
Horizontal	0.9558	0.0025	–0.0067	–0.0048	0.0011	–0.0053
Vertical	0.9297	0.0065	–0.0089	–0.0113	0.0007	–0.0096
Diagonal	0.9156	0.0046	0.0425	–0.0046	0.0012	–0.0318

4.4 Information entropy analysis

The information entropy of an image denotes the randomness of its pixel distribution. The information entropy H of image S can be calculated by the following formula:

$$H(S) = -\sum_{i=1}^{N} P(S_i) \log_2 \left[P(S_i) \right] \tag{10}$$

where $P(S_i)$ represents the probability of pixel value S_i appearing in the image. For an ideal completely random image, $H(S) = 8$. Table 4 provides the information entropy of three standard test diagrams (Lena, Peppers, and Baboon) with different methods. It can be seen from the table that the ciphertext information entropy of the three standard test graphs with the new method is close to 8. Moreover, compared with other image encryption methods, the presented algorithm has more advantages in precision, which indicates that the proposed algorithm has stronger randomness in terms of the ciphertext pixel distribution.

Table 4 Information entropy

Method	*Lena*	*Peppers*	*Baboon*
GSAPSO-MQC	7.9964	7.9969	7.9961
NLCC	7.9971	7.9966	7.9965
CDDM	7.9969	0.9968	7.9968
SNNPST	7.9974	7.9975	7.9972
Proposed	7.9978	7.9978	7.9976

4.5 Sensitivity analysis

The sensitivity of ciphertext determines the ability of the algorithm to resist differential attack. To measure the sensitivity of encryption algorithm, the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) are commonly used to evaluate the effectiveness of the proposed algorithm. When the value of NPCR represents a grey value change in the digital image, the ratio of grey value change in the corresponding ciphertext image is calculated according to formulas (11) and (12).

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} R(i, j) \times 100\% \tag{11}$$

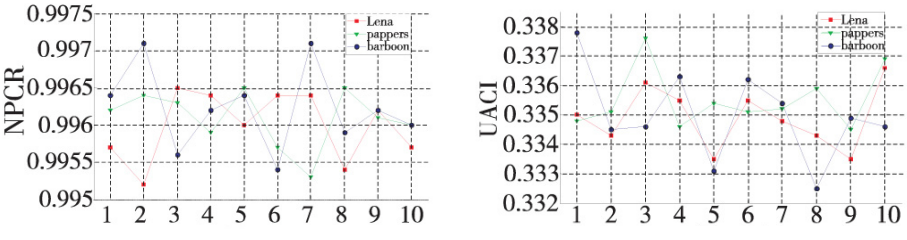
$$R(i, j) = \begin{cases} 1 & C_1(i, j) \neq C_2(i, j) \\ 0 & C_1(i, j) = C_2(i, j) \end{cases} \tag{12}$$

UACI value represents the average change intensity of image pixel value, which is calculated according to equation (13).

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\% \tag{13}$$

where M and N are the width and height of the image. $C_1(i, j)$ is the pixel value at (i, j) of the ciphertext image obtained from the original plaintext encryption. $C_2(i, j)$ is the pixel value at (i, j) of the ciphertext image obtained from the changed plaintext encryption.

Figure 8 (a) NPCR and (b) UACI value (see online version for colours)



(a) (b)

For greyscale images with greyscale $L = 8$, the ideal values for NPCR and UACI are 0.9961 and 0.3346, respectively. To verify the sensitivity of this algorithm, Lena, Peppers and Baboon are selected to randomly change a pixel value respectively. 10 NPCR and UACI values are randomly tested, the results are shown in Figure 8, which shows that both NPCR and UACI values are very close to the ideal value, it indicates that ciphertext is highly sensitive to plaintext.

The sensitivity of ciphertext to the key is also a measurement to resist differential attacks. The key is modified as (256, 256, 7, K_i, Q_m, i, 3), where K_i is unchanged and Q_m is randomly changed. Then, the values of NPCR and UACI between the two ciphertext images before and after the change of the test key are carried out for the three standard test images respectively. The results are shown in tables 5 and 6. It can be seen that ciphertext is extremely sensitive to the initial key, and the proposed algorithm has more advantages than other methods.

Table 5 NPCR value

Image	*Proposed*	*GSAPSO-MQC*	*NLCC*	*CDDM*	*SNNPST*
Lena	0.9961	0.9956	0.9963	0.9968	0.9969
Peppers	0.9959	0.9958	0.9964	0.9966	0.9971
Baboon	0.9963	0.9961	0.9962	0.9958	0.9957

Table 6 UACI value

Image	*Proposed*	*GSAPSO-MQC*	*NLCC*	*CDDM*	*SNNPST*
Lena	0.3336	0.3334	0.3371	0.3375	0.3378
Peppers	0.3347	0.3335	0.3370	0.3372	0.3375
Baboon	0.3364	0.3333	0.3375	0.3376	0.3378

4.6 Efficiency analysis

The experiments are conducted on Intel CoreTM i7-4712mq CPU @ 2.30 GHz 2.29 GHz, 8 GB memory, 500 GB hard disk hardware environment and Windows 10, MATLAB 2017a software environment. The encryption experiment is carried out for Lena, Peppers, Baboon images with 256×256 pixels. The results are shown in Table 7.

Table 7 Time (s)

Image	*Proposed*	*GSAPSO-MQC*	*NLCC*	*CDDM*	*SNNPST*
Lena	0.761	0.824	0.853	0.917	1.102
Peppers	0.685	0.699	0.758	0.793	0.826
Baboon	0.674	0.718	0.776	0.896	0.913

The total time of the whole process is about 0.761s with the proposed method for Lena. The GSAPSO-MQC is tested in the same environment, and the whole process encryption time is 0.824 s. The results show that the efficiency of the proposed algorithm is better than that of other methods, the overall efficiency is good.

5 Conclusions

This paper makes full use of 3D Arnold mapping, elementary cellular automata and quadtree decomposition in digital image encryption, and proposes an efficient and secure image encryption algorithm. The quadtree decomposition can reduce the number of iterations in the phase of image scrambling and confusion. The ideal encryption effect can be achieved with fewer iterations. Experimental results and security analysis show that the proposed algorithm has good cryptographic performance, including large key space, strong randomness of ciphertext image pixel value distribution, very low correlation between adjacent pixels, and extremely sensitive ciphertext to plaintext and key. In addition, the time efficiency of the encryption algorithm can meet the real-time requirements in most applications. Therefore, the algorithm in this paper has a good application value for the encryption processing of image in secure communication.

Acknowledgements

This paper was supported by Key research Project of higher education institutions in Henan Province (Project Name: A Study on Students' concentration in Class Based on Deep Multi-task Learning Framework; Project No. 23B413004) and the Science and Technology Project No. 222102310222.

References

Belazi, A., El-Latif, A.A.A. and Belghith, S. (2016) 'A novel image encryption scheme based on substitution-permutation network and chaos', *Signal Processing*, November, Vol. 128, pp.155–170, https://doi.org/10.1016/j.sigpro.2016.03.021.

Cao, G-H., Hu, K. and Tong, W. (2011) 'Image scrambling based on logistic uniform distribution', *Acta Physica Sinica*, Vol. 60, No. 11, p.110508, DOI: 10.7498/aps.60.110508.

Chai, X., Gan, Z., Yang, K. et al. (2017) 'An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations', *Signal Processing Image Communication*, Vol. 52, pp.6–19, https://doi.org/10.1016/j.image.2016.12.007.

Enayatifar, R., Sadaei, H.J., Abdullah, A.H. et al. (2015) 'A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata', *Optics and Lasers in Engineering*, August, Vol. 71, pp.33–41, https://doi.org/10.1016/j.optlaseng.2015.03.007.

Feizi-Derakhsh, M.R. and Kadhim, E.A. (2022) 'An improved binary cuckoo search algorithm for feature selection using filter method and chaotic map', *Journal of Applied Science and Engineering*, Vol. 26, No. 6, pp.897–903.

Hosseini, S.A., Mohammadi, I. and Kamel, S.R. (2014) 'A parallel image encryption based on elementary cellular automata using two processors', *2014 International Congress on Technology, Communication and Knowledge (ICTCK)*, IEEE.

Hou, W., Li, S., He, J. et al. (2020) 'A novel image-encryption scheme based on a non-linear cross-coupled hyperchaotic system with the dynamic correlation of plaintext pixels', *Entropy*, Vol. 22, No. 7, p.779.

Karim, S., Tong, G., Li, J., Qadir, A., Farooq, U. and Yu, Y. (2022) 'Current advances and future perspectives of image fusion: a comprehensive review', *Information Fusion*, Vol. 90, pp.185–217, https://doi.org/10.1016/j.inffus.2022.09.019.

Li, J., Hao, J., Tong, G., Karim, S., Sun, X. and Yu, Y. (2022) 'Unsupervised demosaicking network using the recurrent renovation and the pixel-wise guidance', *Optics Letters*, Vol. 47, No. 16, pp.4008–4011.

Ma, S., Zhang, Y., Yang, Z. et al. (2019) 'A new plaintext-related image encryption scheme based on chaotic sequence', *IEEE Access*, Vol. 7, pp.30344–30360 [online] https://ieeexplore.ieee.org/abstract/document/8651453.

Song, C.Y., Qiao, Y.L. and Zhang, X.Z. (2013) 'An image encryption scheme based on new spatiotemporal chaos', *Optik – International Journal for Light and Electron Optics*, Vol. 124, No. 18, pp.3329–3334.

Tan, X., Xiang, C., Cao, J., Xu, W., Wen, G. and Rutkowski, L. (2022) 'Synchronization of neural networks via periodic self-triggered impulsive control and its application in image encryption', *IEEE Transactions on Cybernetics*, Vol. 52, No. 8, pp.8246–8257, DOI: 10.1109 /TCYB.2021.3049858.

Teng, L., Li, H., Yin, S. and Sun, Y. (2019) 'A new chi-square distribution de-noising method for image encryption', *International Journal of Network Security*, Vol. 21, No. 5, pp.804–811.

Wacker, S. (2019) 'Cellular automata on group sets and the uniform Curtis-Hedlund-Lyndon theorem', *Natural Computing*, Vol. 18, Nos. 1–3, pp.459–487.

Wang, X. and Luan, D. (2013) 'A novel image encryption algorithm using chaos and reversible cellular automata', *Communications in Nonlinear Science and Numerical Simulation*, Vol. 18, No. 11, pp.3075–3085.

Yin, S. and Li, H. (2020) 'GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system', *Evolutionary Intelligence*, DOI: 10.1007/s12065-020-00440-6.

Zhang, X., Zhang, H. and Xu, C. (2016) 'Reverse iterative image encryption scheme using 8-layer cellular automata', *KSII Transactions on Internet & Information Systems*, Vol. 10, No. 7, pp.3397–3413.

Zhao, H. (2022) 'Research on construction of educational management model based on data mining technology', *Journal of Applied Science and Engineering*, Vol. 26, No. 5, pp.613–621.

Zheng, C., Raabe, D. and Li, D. (2012) 'Prediction of post-dynamic austenite-to-ferrite transformation and reverse transformation in a low-carbon steel by cellular automaton modeling', *Acta Materialia*, Vol. 60, No. 12, pp.4768–4779.