Multimedia Tools and Applications (2019) 78:14823–14835
https://doi.org/10.1007/s11042-018-6758-y

A new color image encryption algorithm based on DNA and spatial chaotic map

Ping Liu[1] · Tongxun Zhang[2] · Xiang Li[3]

Received: 25 January 2018 / Revised: 31 August 2018 / Accepted: 4 October 2018 /
Published online: 17 November 2018

Abstract

In this paper, a color image encryption algorithm based on DNA encoding combined with logistic map and spatial map is proposed. Firstly, the algorithm carries out scrambling by logistic map for R, G, B channels. Then, XOR is operated between channels pixel and sequence matrix controlled by spatial map. After that, realizes the addition of R, G, B by DNA addition after DNA encoding and carries out complement operation by using the DNA sequence matrix controlled by spatial map. What is more, R G B channel images are got after DNA decoding. Finally, gets the encrypted R, G, B images by reconstructing R, G, B components. The results of several experimental, statistical analysis and key sensitivity tests show that the proposed image encryption algorithm provides an efficient and secure way for real-time image encryption and transmission.

Keywords Image encryption · Spatial chaotic · Information security · DNA coding

1 Introduction

As the Internet increasingly becomes the preferred channel of communication worldwide, more and more information such as images, videos and other forms of data are transmitted over the internet, but convenient access to the network brings lots of concerns about information security such as copyrights pirating and threats to safety of online personal properties. It is extremely urgent to develop some more reliable and effective cryptographic techniques to protect the information [20]. Therefore, many encryption algorithms are designed to protect information security. Ref. [16] proposed a new privacy-preserving patient-centric clinical decision support system, the system can efficiently calculate patient's disease risk with high accuracy in a privacy-preserving way. Ref. [27] proposed a new fingerprint encryption scheme which utilizes the high-dimension space projection. Ref. [28] proposed a

✉ Xiang Li
lixiang@sdau.edu.cn

[1] College of Mechanical and Electronic Engineering, Shandong Agricultural University, Taian 271018, China

[2] Shandong Agricultural University, Taian 271018, China

[3] College of Life Sciences, Shandong Agricultural University, Taian 271018, China

privacy-preserving face recognition protocol with outsourced computation to protects individuals privacy.

Unlike text files, digital image has some intrinsic features such as bulk data capacities, strong correlation between the adjacent pixels and high redundancy, previous algorithm such as AES and DES [15, 19, 21, 22] are not efficient for proper encryption. Therefore, several methods have been proposed by scientists. The characteristics of chaotic system determine that it can be applied to image encryption [2, 9, 18], Ref. [13] proposed a color image encryption based on one-time keys and robust chaotic maps which has good shear resistance. Ref. [17] proposed a new image encryption scheme based on double chaotic system to complete scrambling and replacement of images. Ref. [12] proposed an adaptive parameter image encryption algorithm based on chaotic theory, result shows that it has good performance.

Image encryption based on DNA computing is an important content of the intersection for computer science and biological science. It is a new developing trend with the successful completion of the human genome project. In 1994, Dr. Adleman [1] of University of Southern California implemented the Directed Hamilton path problem by using the complementary pairing principle of DNA molecules. The birth of DNA computing symbolizes the emergence of a new computing model, breaks original computing model and opens up a new path for solving various complex problems. Image encryption based on DNA computing has been well developed [29]. Ref. [10] proposed a pseudo DNA cryptography method which has better effect. The combination of DNA computation and cat mapping improve the security intensity. Image scrambling after Chebyshev mapping and DNA encoding has good effect on gray scale images [3, 30].

The rest of this paper is organized as follows: Section 2 introduces basic theories of proposed algorithm. Section 3 describes the implementation of algorithm in detail. Section 4 shows simulation experiments results. Section 5 provides security analysis. Conclusions are drawn in Section 6.

2 Basic theory of proposed algorithm

2.1 Logistic maps

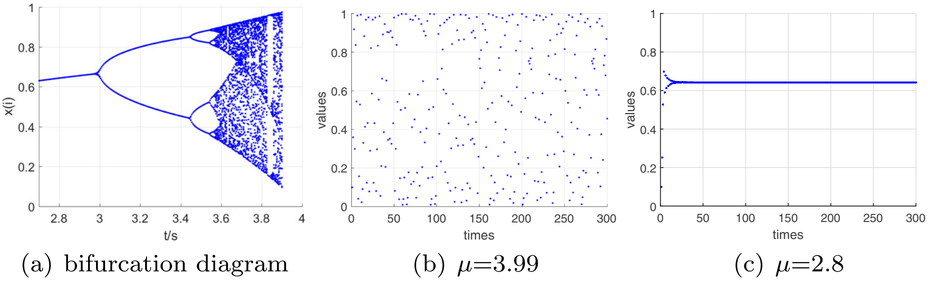
Logistic map is strongly sensitive to initial parameter values [8], slight alteration will cause huge changes, the function is described by (1).

$$X_{n+1} = \mu * X * (1 - X_n) \qquad \mu \in [0, 4], X \in [0, 1], \tag{1}$$

Figure 1a shows bifurcation diagram when μ ∈[3.56,4.0], especially μ near to 4. Figure 1b shows values distribution when $\mu = 3.99$. Figure 1c shows when μ ∉[3.56,4.0], the result tend to a specific value.

2.2 Deoxyribonucleic acid sequence

Nowadays, DNA computing has permeated the domain of cryptography. DNA cryptogram utilizes DNA as information carrier and takes advantage of biological technology to achieve encryption. DNA consists of four types deoxyribonucleic acid: A, G, C, T. A and T, G and C are complementary bases. There are 24 encoding schemes to represent a case by two bits, 8 of them conform to Watson-Crick [11] complementary based pairing rules shown in Table 1. We use 4 bits DNA sequences to represent pixel values. For example, the pixel value is 231,



(a) bifurcation diagram (b) μ=3.99 (c) μ=2.8

Fig. 1 The characteristics of Logistic system

it's binary array is [1 1 1 0 0 1 1 1], the DNA sequence is [T C G T] coded by first coding rule.

2.3 Spatial chaotic system

Chaotic encryption was first proposed by Halle and Hasler [6, 7] in 1993. Spatial chaotic system is a deterministic random processes in nonlinear dynamics system with m and n two variables in the space of chaotic mapping. Spatial chaotic sequences than 2D (a variable m) is more complex, more randomness, more difficult to predict chaotic sequences [4, 5, 23, 24]. Based on the properties of chaotic system, we use spatial chaotic system in encrypting image. The differential form of the two-dimensional system for spatial generalization is shown in (2).

$$X_{m+1,n} + \omega X_{m,n+1} = 1 - (\beta(1+\omega) \times X_{m,n})^2, \tag{2}$$

where $m, n, X_{m,n}$ is geometric coordinates of 3D space, β is real parameter, ω is real number. Research shows that when $\beta \in$ [1.55, 2.0], $\omega \in$ (-1,1), system presents chaotic state, as is shown in Fig. 2.

3 Algorithm description

The detailed description of proposed algorithm is shown in Fig. 3. The algorithm involves dynamic index image scrambling scheme and a new spatial chaotic based diffusion scheme. In the encryption procedure, The logistic map is used to scramble image pixels, and we proposed a new spatial chaotic sequence for diffusion. In addition, DNA coding and XOR are introduced to enhance encryption effect and improve the complexity of algorithm. The encryption process is divided into 6 steps and the detailed description of proposed algorithm is shown in Fig. 3.

Table 1 Eight of pairing rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

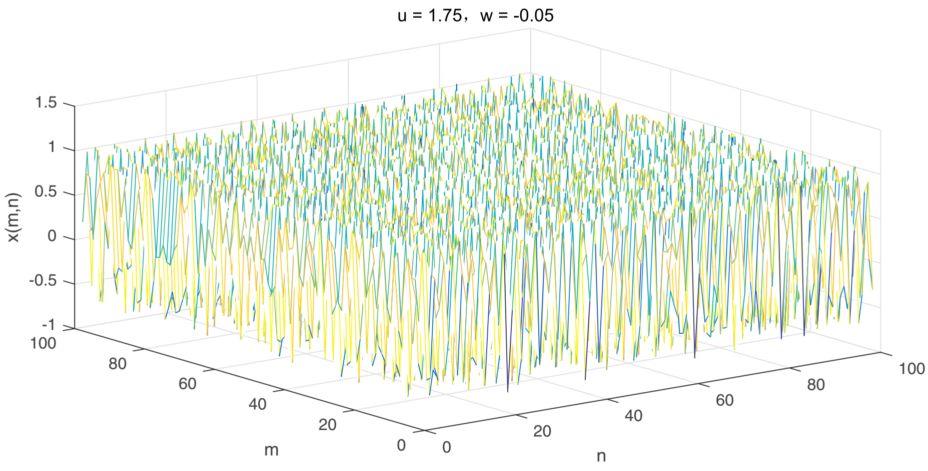


Fig. 2 Chaotic behavior of spatial chaos system

Step1: The color image A(m,n,3) is converted into three matrices R(m,n), G(m,n) and B(m,n) and then calculate pixel average L_1, L_2 and L_3 of each channel.

Step2: Scrambling the R(m,n), G(m,n) and B(m,n), the detail steps are described as follows:

Firstly, define initial parameters L_1, L_2, L_3, offset=3000, $\mu = 3.99$. According to (1), we can get $X1$, $X2$ and $X3$.

Secondly, select an array of the same size as the original matrix.

Thirdly, sort the sequences $X1$, $X2$ and $X3$, as (3) shows.

$$\begin{cases} [Sort\_StdX1, Flag1] = sort(X1) \\ [Sort\_StdX2, Flag2] = sort(X2) \\ [Sort\_StdX3, Flag3] = sort(X3) \end{cases} \tag{3}$$

where $[StdXi, Flagi] = sort(Xi)$ is the sequencing index function, $Flag1$, $Flag2$, and $Flag3$ are the index sequences of $L1$, $L2$ and $L3$.

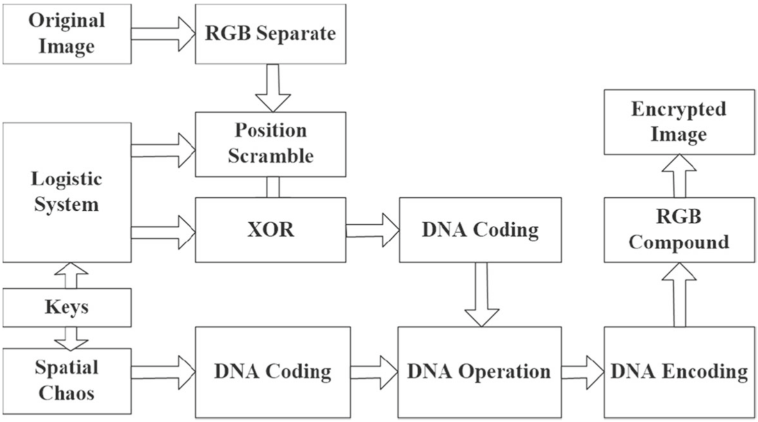


Fig. 3 Specific steps of algorithm

Table 2 Addition operation

	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Finally, sort the index sequences and get the final sorted matrices based on (4).

$$\begin{cases} Rscr(:,1) = Sort\_StdL1(Flag1(:,1),:) \\ Gscr(:,2) = Sort\_StdL2(Flag2(:,1),:) \\ Bscr(:,3) = Sort\_StdL3(Flag3(:,1),:) \end{cases} \tag{4}$$

Step3: The pixel values are changed by XOR operation between scrambled sequences and the random sequences Ch(i) generated by (7). After that, we can get a new image matrix $R'(m,n)$, $G'(m,n)$ and $B'(m,n)$ as follows:

$$\begin{cases} R(i,1)XORCh1 \rightarrow R'(i,1) \\ G(i,1)XORCh2 \rightarrow G'(i,1) \\ B(i,1)XORCh3 \rightarrow B'(i,1) \end{cases} \tag{5}$$

$$\begin{cases} Ch1 = uint8(fix(mod(StdL1 * 10^{12}, 256))) \\ Ch2 = uint8(fix(mod(StdL2 * 10^{12}, 256))) \\ Ch3 = uint8(fix(mod(StdL3 * 10^{12}, 256))) \end{cases} \tag{6}$$

where i=1,2, $\cdots$ 65536.

Step4: According to the DNA coding rule proposed in Table 1, the matrices can be encoded.

Step5: Define initial parameters of spatial system ω=-0.05, β=1.75, A(1,1)=0.27, A(1,2)=0.83, A(2,1)=-0.45 and substituting initial parameters into (2), we can get a submatrix B. Do the following operation for B to get a submatrix Ch which has same size with the sorted component matrices.

$$Ch = fix(mod(B \times 10^{12}, 4)) \tag{7}$$

Step6: In order to increase the complexity of the algorithm, we define an addition operation, as shown in Table 2. Using another DNA rule to decrypt the DNA matrices and changing the binary matrices into decimal matrices. Through the above steps, we can

Table 3 Scrambling scheme description

```
Input: the original image Lena with the size of 256×256
separate original image to obtain R G B channel;
set each channel averages as logistic system initial values;
generate logistic sequences using (1);
sort logistic sequence to get index sequence using (3);
for ecah image pixel do
    sort index sequence to confuse image pixel using (4);
end for
Output: confused image.
```

Table 4 diffusion scheme description

```
Input: confused image Lena with the size of $256\times256$
XOR between Ch(i) and confused image sequence by diffusion scheme;
DNA coding using Table 2;
Spatial chaotic sequence Ch using (2) and (7);
code Ch using Table 2;
for Ch and DNA sequence do
    Ch + DNA sequence;
end for
Output: encrypted image.
```

obtain an encrypted image. Table 3 illustrates the scrambling scheme by pseudo code. Similarly diffusion scheme is described in Table 4.

It is worth mentioning that the reverse process of encryption is decryption, Fig. 4 shows the concrete steps of the decryption process.

4 Simulation results

We use Matlab R2014a to run the encryption and decryption process in computer with 2.30 GHz CPU, 8 GB memory and Microsoft Windows 10 operation system. The initial image we choose is Lena.bmp of size 256×256, the keys we select are ω=-0.05, β=1.75, A(1,1)=0.27, A(1,2)=0.83, A(2,1)=-0.45. In Fig. 5, we show the results of encryption and decryption.

5 The security analysis

This section reports the simulation results and performance analysis for the proposed algorithm. A good encryption system should resist to all kinds of known attacks and the corresponding security analyses have been performed on the proposed algorithm, including gray histogram analysis, key space analysis, sensitivity analysis, information entropy analysis, correlation coefficient analysis and statistical analysis, noise interference analysis.

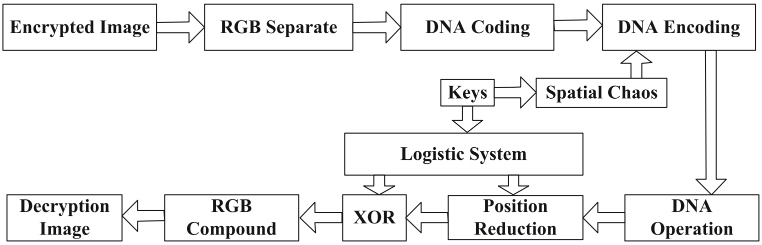
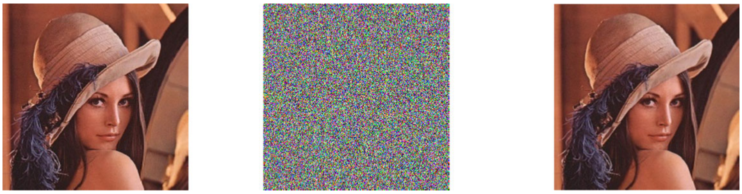


Fig. 4 Decryption flow chart



(a) Initial image (b) Encrypted image (c) Decrypted image

Fig. 5 Algorithm implementation

5.1 Gray histogram analysis

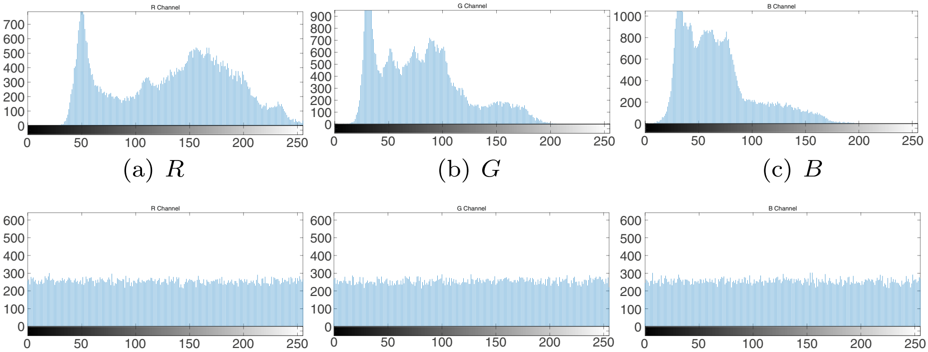
The histogram is one of the most statistical characteristics of an image, and represents the frequency of all the gray level values from all over the image. Figure 6a, b and c show the R G B component gray histogram of initial color image respectively, Fig. 6d, e and f show the R G B component gray histogram of decrypted color image respectively. From Fig. 6 we can see that the histogram of the ciphered image is fairly uniformly distributed, this is important in resisting statistical analysis attack.

5.2 Secret keys space analysis

A good image encryption system should be sensitive to cipher keys, and the key space needs to be large enough to make the brute-force impossible [26]. To our proposed encryption algorithm, the key consists of the initial values L_1, L_2, L_3 of logistic map, control parameter of logistic map μ, initial value and control parameter of spatial map A(1,1), A(1,2), A(2,1), β and ω. The precision is 10^{-15}, so the key space is larger than 10^{135}. So the key space is large enough to resist all kinds of brute-force attacks.

5.3 Sensitivity analysis

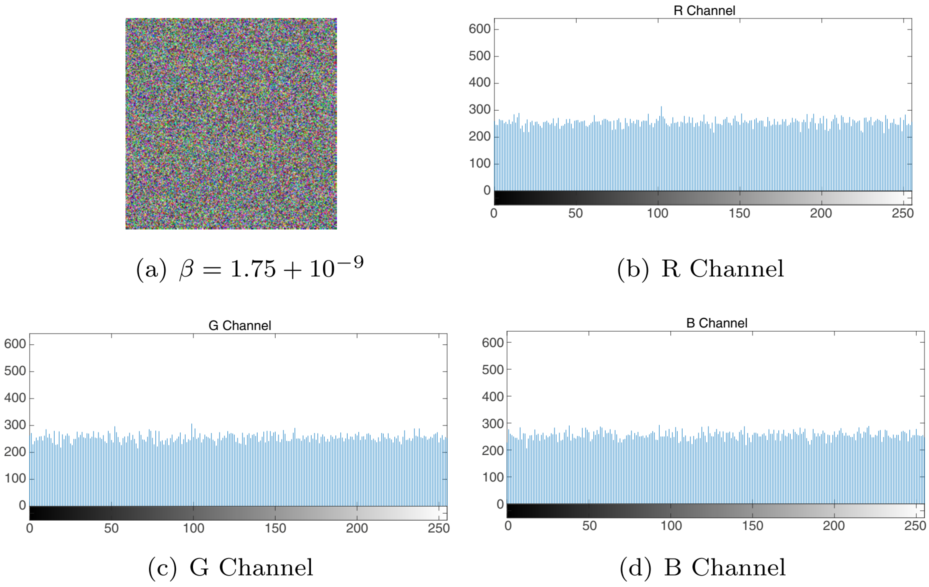
Chaotic sequences have high sensitivity to initial value and rapid diffusibility. In implementation of the algorithm, we decrypt the cipher image Fig. 5a using $\beta = 1.75 + 10^{-9}$ with



(a) R (b) G (c) B

(d) R (e) G (f) B

Fig. 6 Gray histograms of initial image and encrypted image



(a) $\beta = 1.75 + 10^{-9}$

(b) R Channel

(c) G Channel

(d) B Channel

Fig. 7 Sensitivity analysis

other keys the same. The decryption image and its corresponding histogram are shown in Fig. 7. From Fig. 7, we see that the decryption image is completely different from the original image and is nearly uniformly distributed, which means proposed encryption method provides a high key sensitivity.

5.4 Information entropy analysis

Information entropy is a concept used in the information theory to measure the amount of information. The more orderly a system is, the lower the entropy of information. Therefore, information entropy is also an evaluation criteria for the level of system confusion. The calculation formula is shown in (8).

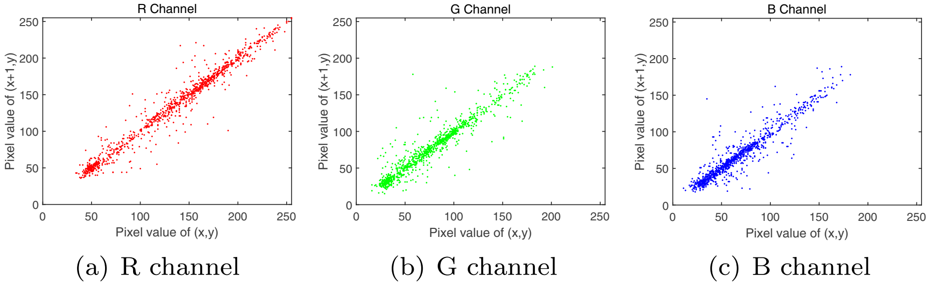
$$H = -\sum_{i=0}^{255} p_{(i)} \log_2 p_{(i)}, \tag{8}$$

where i is gray value of image, $P_{(i)}$ is emergence probability of i.

According to (8), we can get the ideal $H = 8$, which shows that the information is random. Hence the information entropy of the ciphered image should be close to 8 after encryption. The closer it gets to 8, the less possible for the cryptosystem to divulge information. Table 5 shows the information entropy of different algorithms.

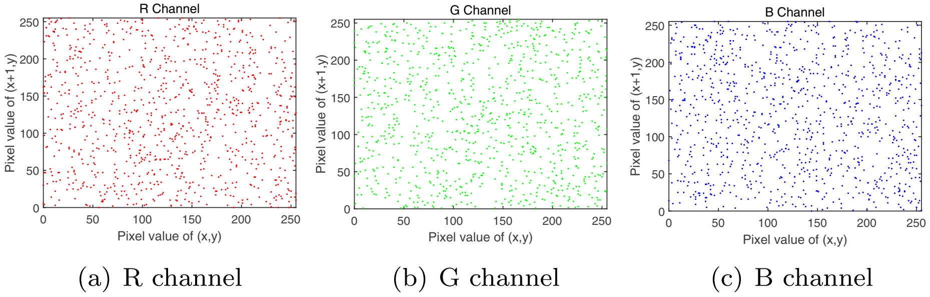
Table 5 Information entropy

References	Wang's [13]	Liu's [14]	Proposed algrithm
Information entropy	7.9832	7.9877	7.9913



(a) R channel (b) G channel (c) B channel

Fig. 8 Correlation of initial image



(a) R channel (b) G channel (c) B channel

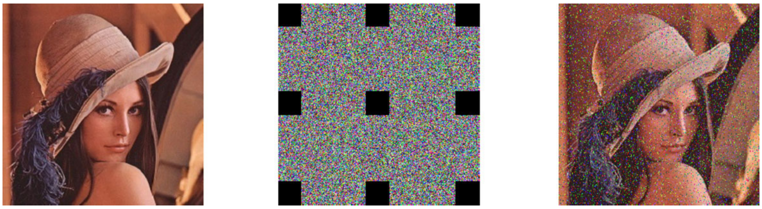
Fig. 9 Correlation of encrypted image

Table 6 Correlation coefficients of two adjacent pixels in three typical directions

Correlation	R	G	B
horizontal	0.0134/0.9663	0.0086/0.9458	−0.0013/0.9192
vertical	−0.0129/0.9780	−0.0004/0.9590	0.0054/0.9448
diagonal	−0.0009/0.9588	−0.0022/0.9251	−0.0018/0.9159

Table 7 Same position correlations between R, G, B components

Correlation	R, G channels	R, B channels	B, G channels
Initial image	0.9361	0.8067	0.9581
encrypted image	0.0022	−0.0084	−0.0080
wang’s [26]	−0.003803	−0.050968	0.012267



(a) Initial image (b) Noise interference (c) Decrypted image

Fig. 10 Noise interference analysis

5.5 Correlation coefficient analysis

An image generally has high data redundancy and thus its pixels have high correlations with their neighboring pixels. A good image encryption algorithm should have the ability of breaking these correlations. Mathematically, the correlation coefficients of the mentioned pixels in vertical, horizontal and diagonal direction are measured using (9).

$$\begin{cases} E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))) \\ r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)\times\sqrt{D(y)}}} \end{cases} \tag{9}$$

where x and y are gray-scale values of two adjacent pixels in image, N is the total number of pixels which are selected from image.

We randomly select 1000 pairs of two adjacent pixels from initial image, Fig. 8a, b and c show R G B component correlation of initial image, Fig. 9a, b and c show encrypted image.

In the Table 6, we have given the correlation coefficients for the encrypted and initial images respectively which more irrelevant than the algorithm proposed by Ref. [4]. Table 7 shows same position correlations between R, G, B components, the result of the initial image are close to 1 while the encrypted image's result are closer to 0 than wang's algorithm [25]. These further verify that the encrypted image by proposed algorithm has extremely low correlation.

5.6 Noise interference analysis

It is easy to lose information in the process of image transmission. In order to verify the interference resistance of the algorithm, we selected nine parts from the Lena.jpg (the size is 256 × 256 × 3), each of part has size of 30 × 30 and then set the pixel value to 0 as the Fig. 10b shows. Then decrypt this incomplete image and get the result of in Fig. 10c. When the image lost 12% information, it can also get the primary information. Compared with Ref. [8] which lost 2% data, the proposed algorithm has stronger ability of resisting noise interference.

6 Conclusions

In this paper, a new way of color image encryption algorithm have been proposed which utilizes logistic maps, spatial maps and DNA coding. The initial conditions for both the logistic maps are derived using initial image. In the proposed encryption process, logistic maps is used for scrambling pixel, spatial maps is used for replacing pixel, DNA coding and ROX operations are used to enhance the complexity of the algorithm. To make the cipher more robust against any attack, the secret key is modified after DNA coding. We have carried out statistical analysis, key sensitivity analysis, key space analysis and etc to demonstrate the security of the new image encryption procedure. Finally, we conclude with the remark that the proposed method is expected to be useful for real time image encryption and transmission applications.

Acknowledgments The work was supported by the National Natural Science Foundation of China (Nos. 31700644), Postdoctoral Science Foundation of China (No. 2015M582122 240 and 2016T90644), the National Key Technology Support Program of China (No. 2015BAF13B02), Key research and development project of Shandong Province(No. 2016ZDJS02A07 and 2017GNC12105).

The Authors are sincerely thankful to the potential/anonymous reviewers for their critical comments and suggestions to improve the quality of the paper.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

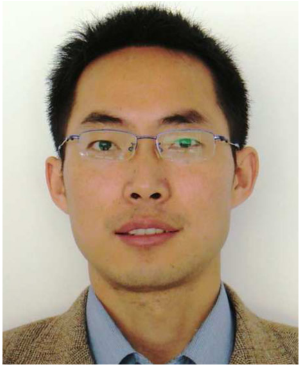
References

1. Adleman L (1994) Molecular computation of solutions to combinational problems. Science 226:1021–1024
2. Cao JQ, Xiao HR et al (2010) Chaotic encryption algorithm with double replacement of pixel location and pixel value. Computer engineering and Applications 46:192–195
3. Fang DX, Zhang J (2014) A image encryption scheme based on combination of DNA computation and cat mapping. Comput Eng 40:89–93
4. Gao TG, Chen ZQ (2008) A new image encryption algorithm based on hyper-chaos. Phys Lett A 372:394–400
5. Gu GS, Ling J (2014) A fast image encryption method by using chaotic 3D cat maps. Optik-International Journal Ior Light and Electron Optics 125:4700–4705
6. HALLE K et al (1993) Spread Spectrum communication through modulation of chaos. International Journal of Bifurcation and Chaos 03:469–477
7. Hasler M, Schimming T (2000) Chaos communication over noisy channels. Int J Bifurcation Chaos 10:719–735
8. Hua ZY, Zhou YC (2015) 2D Sine Logistic modulation map for image encryption. Information Sciences 297:80–94
9. Hua Z, Zhou Y (2016) Image encryption using 2D Logistic-adjusted-Sine map. Information Sciences 339:237–253
10. Kang N (2009) A pseudo DNA cryptography method. arXiv:0903.2693
11. Kimsey IJ, Petzold K et al (1953) Visualizing transient Watson-Crick like mispairs in DNA and RNA duplexes. Nature 519:315–320
12. Li CY (2016) An adaptive parameter image encryption algorithm based on chaos theory. scinece and technology information, pp 131-134
13. Liu HJ, Wang XY (2010) Color image encryption based on one-time keys and robust chaotic maps. Computers & Mathematics with Applications 59:3320–3327
14. Liu LL, Zhang Q, Wei XP (2012) A RGB image encryption algorithm based on DNA encoding and chaos map. Computers & Electrical Engineering 38:1240–1248
15. Liu DQ, Liu W, Xu J (2014) The application of DES encryption and decryption algorithm in the STS protocol. Applied Mechanics and Materials 644–650:2202–2205
16. Liu XM, Lu RX, Ma JF (2016) Privacy-Preserving Patient-Centric Clinical decision support system on naive bayesian classification. IEEE Journal of Biomedical and Health Informatics (IEEE J-BHI) 20:655–668
17. Lu HB, Zhang P (2012) A new image encryption scheme based on double chaotic system. Computer engineering and Applications 48:90–92

18. Mathews R, Goel A, Saxena P et al (2011) Image encryption based on explosive inter-pixel displacement of the RGB attributes of apixel.[C]. // Proceeding of the World Congress on Engineering and Computer Science, SanFrancisco, pp 19–21
19. Mathur N (2016) Rajeshbansode AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection. Procedia Computer Science 79:1036–1043
20. Peng C, Li Y (2013) A new algorithm for image encryption based on couple chaotic system and cellular automata. In: Proceedings 2013 International Conference on Mechatronic Sciences Electric Engineering and Computer (MEC), Shengyang
21. Rewagad P, Pawar Y (2013) Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing, international conference on communication systems and network technologies, Gwalior, pp 437–439
22. Singh G, Kinger S (2013) Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security. International Journal of Scientific & Engineering Research 4:2058–2062
23. Wang XY, Chen F, Wang T (2010) A new compound mode of confusion and diffusion for block encryption of image based on chaos. Commun Nonlinear Sci Numer Simul 15:2479–2485
24. Wang Y, Kwo-kwo W, Liao XF et al (2011) A new chaos-based fast image encryption algorithm. Appl Soft Comput 11:514–522
25. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Processing 92:1101–1108
26. Wang XY, Liu LT, Zhang YQ (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering 66:10–18
27. Wu ZD, Liang B (2016) High-dimension space projection-based biometric encryption for fingerprint with fuzzy minutia. Soft Comput 20(12):4907–4918
28. Xiang C, Tang C et al (2016) Privacy-preserving face recognition with outsourced computation. Soft Comput 20(9):3735–3744
29. Xiao G, Lu M, Qin L et al (2006) New field of cryptography: DNA Cryptography. Chinese Science Bulletin 51:1413–1420
30. Zhang J, Fang DX (2015) Application of chaotic mapping index and DNA encoding in image encryption. Computer Engineering and Design 36:613–618

Ping Liu received the B.E. degree from Dalian University, Dalian, China, the MA and the Ph.D. degree from the Shandong University, Jinan, China. She is currently an associate professor with the College of Mechanical and Electronic Engineering, Shandong Agriculture University. Professor Liu have published over 20 papers, including SCI and EI. Her current research interests include nonlinear dynamical systems, bifurcation and chaos, and cryptography.

Tongxun Zhang received the B.E. degree from Shandong Agriculture University, Taian, China. He is a graduate student at the Shandong Agricultural University. His current research direction is chaos and cryptography.



Xiang Li received the B.E. the MA and the Ph.D. degree from Shandong Agriculture University, Taian, China. He is senior experimentalist with the College of Life Sciences, Shandong Agriculture University. His current research interests genetics and molecular biology.