A color image encryption algorithm based on DNA computation and Chen system

Liyan Liu 1,3, Yingqian Zhang2 and Hengzhi Zhang1

1 City Institute, Dalian University of Technology, Dalian, China
2 School of Information Science & Technology, Xiamen University Tan Kah Kee College, Zhangzhou, China
3 E-mail: liuliyan81@sina.com

Abstract. To improve the security performance of color images encrypted, a new color image encryption algorithm based on DNA computation and Chen system is proposed. In the proposed algorithm, the chaotic sequences generated by Chen system are applied to the permutation and confusion phase of image encryption. And the mean value of image pixel of each component of a color image is used as the part of the initial conditions of Chen system, which makes that different original images have different secret keys. Besides, the proposed DNA operations can break the bit planes of the plaintext image entirely. Simulation results show that the proposed algorithm is suitable for color image encryption. Therefore, the proposed algorithm can enhance the sensitivity to the plaintext image and resist differential attack, brute-force attack, and statistical attack.

1. Introduction
Transmitting images through internet and storing them on various platforms have become more and more frequent with the rapid development of the networks. However, people have taken more and more attention to the security and confidentiality of digital images transmitted over the public and shared networks. Traditional encryption algorithms like AES (advanced encryption standard) and IDEA (international data encryption algorithm) [1] have been designed for encrypting text data. But many researchers have found that they might be vulnerable for encrypting images in some circumstances, due to the intrinsic properties of images such as bulk data volume, high pixel correlation between adjacent pixels and high redundancy. In recent years, some researchers have proposed many new image encryption algorithms. Wei et al. [2] proposed a novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, and the algorithm had good encryption effect. Zhang et al. [3] proposed RGB Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation, and the method had strong sensibility, high security, and good ability of resisting statistic attack. In [4], a RGB image encryption algorithm based on DNA encoding and chaos map was proposed. In [5], a novel chaos-based image encryption algorithm using DNA sequence operations was proposed. However, from the point of view of cryptanalysis, a lot of encryption algorithms have the weaker ability to resist chosen plaintext attack and chosen ciphertext attack. Ercan [6] and Chen [7] use chosen plaintext attack method to crack the encryption algorithms proposed by Xiang [8] and Masuda [9]. Zhang et al. [10] analyze the encryption algorithm proposed by Zhu [11], and crack a round of the encryption algorithm through the method of chosen plaintext attack and chosen ciphertext attack.
In this paper, Chen system is combined with DNA addition, subtraction and permutation operation to implement color image encryption. The mean value of image pixel of each component of a color image is used as the part of the initial conditions of Chen system, which makes that different original images have different secret keys. Due to better security performance, especially, performance of sensitivity to the plaintext image, the proposed algorithm is more suitable for color image encryption. Furthermore, the experimental results show that the proposed image encryption algorithm is effective.

2. Preliminary materials

2.1. Chen system

In 1999, Chen [12] has found a new chaotic attractor-Chen attractor, which is produced by the following three dimensional chaotic system:

\[
\begin{align*}
\frac{dx}{dt} &= a(y - x) \\
\frac{dy}{dt} &= -xz + (c - a)x + cy \\
\frac{dz}{dt} &= xy - bz
\end{align*}
\]

(1)

where \(a\), \(b\) and \(c\) are the parameters of the system. When \(a = 35\), \(b = 3\) and \(c = 28\), the system turns into the best chaotic state. Compared with Lorenz system, Chen system has the more complex topology structure and dynamic behavior.

2.2. DNA encoding and decoding rules

A DNA sequence is composed of four nucleic acid bases: A (adenine), C (cytosine), G (guanine), T (thymine), where A and T are complementary, G and C are complementary. Because 0 and 1 are complementary in the binary, so 00 and 11 are complementary, 01 and 10 are also complementary. By using four bases A, C, G and T to encode 00, 01, 10 and 11, there are 24 kinds of encoding rules. But there are only 8 kinds of encoding rules satisfying the Watson – Crick complement rule [13], as listed in table 1. DNA decoding rules are the reverse of DNA encoding rules.

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

2.3. DNA addition and subtraction rules

Corresponding to 8 kinds of DNA encoding rules, there also exist 8 kinds of DNA addition rules and 8 kinds of DNA subtraction rules. For example, according to DNA encoding Rule 1, the DNA addition Rule 1 and DNA subtraction Rule 1 are shown in table 2 and table 3, respectively.
3. Image encryption and decryption scheme

The proposed encryption algorithm can be presented as follows:

Step 1. The original color image is denoted as I, which has R, G and B three components. The initial values \( x(0), y(0), z(0) \) of Chen system can be calculated as follows:

\[
\begin{align*}
\Delta x &= \text{mod}(\sum_{i=1}^{N} \sum_{j=1}^{M} I(i, j, 1), 256) \\
\Delta y &= \text{mod}(\sum_{i=1}^{N} \sum_{j=1}^{M} I(i, j, 2), 256) \\
\Delta z &= \text{mod}(\sum_{i=1}^{N} \sum_{j=1}^{M} I(i, j, 3), 256)
\end{align*}
\]

\[\begin{align*}
x(0) &= 1 + \frac{\Delta x}{1000} \\
y(0) &= 1 + \frac{\Delta y}{1000} \\
z(0) &= 1 + \frac{\Delta z}{1000}
\end{align*}\]  

(2)

(3)

Where \( I(i, j, k) \) is the value of the image pixel of the \( k \)th color component in \((i, j)\) pixel position, \( i \in [1, N], j \in [1, M], k \in [1, 3] \), and \( N \times M \) is the size of color image \( I \).

Step 2. Generate the following three chaotic sequences \( x, y, z \), by solving equation (1) with the initial values \( a, b, c, x(0), y(0) \) and \( z(0) \):

\[
\begin{align*}
x &= \text{uint8}(\text{mod}(x \times 1000, 256)) \\
y &= \text{uint8}(\text{mod}(y \times 1000, 256)) \\
z &= \text{uint8}(\text{mod}(z \times 1000, 256))
\end{align*}
\]

(4)

Step 3. Iterate \( N \times M \) times for the following operation to implement the first exclusive or operation for \( R, G \) and \( B \) components of the color image \( I \) and \( y \) sequence:

\[
I(i, j, k) = \text{bitxor}(y(n), I(i, j, k))
\]

(5)

where \( n \in [1, N \times M] \). Iterate \( N \times M \) times for the following operation to implement the second exclusive or operation:

\[
I(i, j, k) = \text{bitxor}(h, I(i, j, k)) \quad ,
\]

(6)

\[
h = \begin{cases} 100, & i = 1 \text{ and } j = 1 \\ I(i - 1, M, \text{mod}(k + 1, 3)), & i \neq 1 \text{ and } j = 1 \\ I(i, j - 1, \text{mod}(k + 1, 3)), & \text{otherwise} \end{cases}
\]

(7)
Step 4. Transform \( R, G \) and \( B \) components of the color image \( I \) and \( y, z \) sequences into binary sequences noted as \( A_1, A_2, A_3 \) and \( A_4, A_5 \). Encode \( A_1, A_2, A_3 \) and \( A_4, A_5 \) by a kind of DNA encoding rule in Table 1 and transform them into DNA sequences noted as \( D_1, D_2, D_3 \) and \( D_4, D_5 \).

Step 5. Carry out permutation for DNA sequence \( D_k \), the length of sequence \( D_k \) is denoted as \( V \), where \( V = N \times M \times 4 \). The \( p \)th element of \( D_k \) is exchanged with the \( q \)th element of \( D_k \), where \( p = [1, V-1] \), \( q = \text{uint16(mod(list(p),V-p))+p} \) and \( \text{list} = [x, y, z, x] \).

Step 6. Calculate the DNA sequence \( D'_k \) as follows:

\[
D'_k = \begin{cases} 
D_{ij} + D_{ij}, & l = 1 \\
D_{ij} - D_{ij}, & l = 0 
\end{cases}
\]  

where \( l = [1, V] \), “+” and “−” are respectively the DNA addition operation and DNA subtraction operation in the proposed algorithm. The indexes of the used DNA addition rule and DNA subtraction rule serve as secret keys.

Step 7. Decode \( D'_1, D'_2 \) and \( D'_3 \) by a kind of DNA decoding rule to obtain decimal sequences noted as \( Z_1, Z_2 \) and \( Z_3 \). The \( N \times M \)-th elements of \( Z_1, Z_2 \) and \( Z_3 \) are assigned with the values of \( \Delta x, \Delta y \) and \( \Delta z \) correspondingly. \( Z_1, Z_2 \) and \( Z_3 \) are transformed into three \( N \times M \) matrices denoted as \( H_1, H_2 \) and \( H_3 \) correspondingly. The ciphered image \( C \) is obtained, and \( H_1, H_2 \) and \( H_3 \) are the corresponding \( R, \ G \) and \( B \) components of \( C \). The encryption process finishes.

The decryption algorithm is the reverse process of encryption algorithm.

In figure 1, the encryption and decryption of Lena, Peppers and Baboon are shown. From the figures, we can see that there is no relationship between the original image and the encrypted image, and the decrypted image looks like the original image. It is shown that the proposed image encryption scheme has good encryption and decryption effect.

![Figure 1](image1.png)

Figure 1. Encryption and decryption of Lena. (a) Original image of Lena, (b) Encrypted image of Lena, (c) Decrypted image of Lena, (d) Original image of Peppers, (e) Encrypted image of Peppers, (f) Decrypted image of Peppers, (g) Original image of Baboon, (h) Encrypted image of Baboon, (i) Decrypted image of Baboon.
4. Simulation results

4.1. Differential attack analysis
An attacker often makes a slight change to the original image, and observes the change of encryption results. Then, the attacker may find out a meaningful relationship between two ciphered images and the original image. It is called differential attack. NPCR (number of pixels change rate) and UACI (unified average changing intensity) usually are used to examine the performance of resisting differential attack, which is defined in equation (9) and equation (10):

\[
D(i, j) = \begin{cases} 
1, & c_1(i, j) \neq c_2(i, j) \\
0, & \text{otherwise}
\end{cases}
\]

\[
\text{NPCR} = \frac{\sum_{D(i, j)} 1}{M \times N} \times 100% 
\]

\[
\text{UACI} = \frac{1}{M \times N} \left[ \sum_{ij} \frac{|c_1(i, j) - c_2(i, j)|}{255} \right] \times 100% 
\]

where \( M \) and \( N \) are the height and width of an image, \( c_1(i, j) \) and \( c_2(i, j) \) denote the two different cipher images in which their plaintext images have only one pixel difference from each other. Considering two random images, the maximum expected value of NPCR is found to be 99.61\%, while the maximum expected value of UACI is 33.46\% [14]. As shown in table 4, NPCR and UACI values for the proposed algorithm are computed. It can be found that NPCR and UACI values are very close to the above expected values. Thus, it can be concluded that the proposed encryption algorithm ensures the required strength against any type of differential cryptanalysis.

| Test images | R layer | G layer | B layer |
|-------------|---------|---------|---------|
| Lena        | NPCR    | 0.9960  | 0.9959  |
|             | UACI    | 0.3351  | 0.3349  |
| Baboon      | NPCR    | 0.9958  | 0.9960  |
|             | UACI    | 0.3348  | 0.3349  |
| Peppers     | NPCR    | 0.9959  | 0.9960  |
|             | UACI    | 0.3350  | 0.3350  |

4.2. Correlation analysis
It is known that adjacent image pixels of the original image are highly correlated. An effective encryption scheme can reduce the correlation between adjacent pixels. To test the correlation of adjacent pixels, 3000 pairs of two adjacent pixels from the plaintext image and the encrypted image are randomly selected. Then, the correlation coefficients of adjacent pixels in vertical, horizontal and diagonal directions are evaluated using the following formulas:

\[
r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} ,
\]

\[
E(x) = \frac{1}{S} \sum_{i=1}^{S} x_i ,
\]

\[
D(x) = \frac{1}{S} \sum_{i=ref}^{S} (x_i - E(x))^2 ,
\]

where
\[
\text{cov}(x, y) = \frac{1}{S} \sum_{i=1}^{S} (x_i - E(x))(y_i - E(y)), \quad (14)
\]

where \( x \) and \( y \) are two adjacent pixels and \( S \) is the total number of duplets \((x, y)\) obtained from the image. \( E(x) \) is the expectation and \( D(x) \) is the variance.

As Table 5 shows, the correlation coefficients of the encrypted image are close to 0 no matter in horizontal, vertical and diagonal directions, but for the original image, the correlation coefficients are always high and are very close to 1. So, it can be concluded that using the proposed encryption algorithm, it is very hard to reveal some information about the original image from the corresponding cipher image.

**Table 5. Correlation coefficients of the adjacent pixels.**

| Test images | Directions | Original images | Cipher images |
|-------------|------------|-----------------|---------------|
| Lena        | horizontal | 0.977407        | 0.000893      |
|             | vertical   | 0.976693        | -0.000663     |
|             | diagonal   | 0.972571        | -0.000284     |
| Baboon      | vertical   | 0.914697        | -0.000429     |
|             | diagonal   | 0.920951        | -0.000857     |
|             | horizontal | 0.907963        | -0.000793     |
| Peppers     | vertical   | 0.968743        | -0.009040     |
|             | diagonal   | 0.965487        | 0.004678      |

4.3. Information entropy analysis

The information entropy can be used to express uncertainty in the image information, and to measure the distribution of gray values in the image. The information entropy is defined as follows:

\[
H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \left( \frac{1}{p(m_i)} \right),
\]

where \( m_i \) is the information source, \( p(m_i) \) is the probability of symbol \( m_i \). The minimum entropy is zero while the maximum entropy is eight. For an ideal random image, the information entropy is eight. An effective encryption scheme should make the information entropy close to 8. As shown in Table 6, the values of information entropy are very close to the maximal theoretical value of 8. It means that the information leakage in the encryption process is negligible. So, it can be concluded that the proposed encryption algorithm is secure upon the entropy attack.

**Table 6. The information entropy of encrypted image.**

| Cipher images | Entropy     |
|---------------|-------------|
| Lena          | 7.999236    |
| G             | 7.999378    |
| B             | 7.999304    |
| R             | 7.999101    |
| Baboon        | 7.999244    |
| G             | 7.999221    |
| B             | 7.999303    |
| R             | 7.999303    |
| Peppers       | 7.999267    |
| G             | 7.999438    |
| B             |              |
4.4. Key space analysis
In the proposed algorithm there are six secret keys: the initial values \(x(0), y(0), z(0)\) and system parameters \(a, b, c\). If the precision is \(10^{-14}\), the key space size is \(10^{84}\). Except the secret key the index of the used DNA encoding rule, the index of the used DNA decoding rule, the key space is large enough to resist brute-force attack.

4.5. Key sensitivity analysis
It is time consuming to examine the sensitivity of secret keys by enumerating all the possible combinations of secret key parts. Peppers image is used to testing the key sensitivity when the secret keys part is randomly changed a little bit, which is shown in figure 2.

![Figure 2. Key sensitivity.](image)

4.6. Differential attack analysis
Figure 3 is the histograms of \(R\), \(G\) and \(B\) three components of three original images and their ciphered images. From figure 3, it can be found that the image pixels values of the original image are concentrated on some values, but the histograms of ciphered image are fairly uniform and are significantly different from that of the plaintext image, which makes statistical attacks difficult.
Figure 3. Histograms for R, G and B three components of the original images and ciphered images. 
(a) Histograms for R, G and B three components of Lena. (b) Histograms for R, G and B three components of the ciphered image of Lena. (c) Histograms for R, G and B three components of Peppers. (d) Histograms for R, G and B three components of the ciphered image of Peppers. (e) Histograms for R, G and B three components of Baboon. (f) Histograms for R, G and B three components of the ciphered image of Baboon.
5. Conclusions
In this paper, a color image encryption algorithm based on DNA computation and Chen system is proposed. In the proposed encryption algorithm, the chaotic sequences generated by Chen system are applied to the permutation and confusion phase of image encryption. DNA permutation and addition/subtraction operations can break the bit planes of the plaintext image entirely. In addition, the proposed encryption algorithm is sensitive to the plaintext image. Different tests are applied to the proposed encryption algorithm, including differential attack, correlation coefficient, information entropy, key space, key sensitivity and histogram analysis. Simulations results show that the proposed encryption algorithm is effective and suitable for color image encryption.

References
[1] Stinson D R 1995 Cryptography: theory and practice (Boca Raton: CRC Press)
[2] Wang X L 2012 A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system J. Syst. Software. 85 290-9
[3] Zhang Q and Wei X 2013 RGB Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation Iete Tech. Rev. 30 404-9
[4] Liu L L, Zhang Q and Wei X 2012 A RGB image encryption algorithm based on DNA encoding and chaos map Comput. Electr. Eng. 38 1240-8
[5] Chai X, Chen Y and Broyle L 2017 A novel chaos-based image encryption algorithm using DNA sequence operations Opt. Laser. Eng. 88 197-213
[6] Solak E and Cokal C 2011 Algebraic break of image ciphers based on discretized chaotic map lattices Inform. Sciences 181 227-33
[7] Chen Y, Liao X and Wong K W 2006 Chosen plaintext attack on a cryptosystem with discretized skew tent map IEEE Trans. Circuits Syst. II, Exp. Briefs 53 527-9
[8] Xiang T, Wong K W and Liao X 2007 Selective image encryption using a spatiotemporal chaotic system Chaos 17 415-27
[9] Masuda N and Aihara K 2002 Cryptosystems with discretized chaotic maps IEEE Trans. Circuits Syst. I, Fundam. Theory Appl. 49 28-40
[10] Jiang Y Q and Wang X Y 2014 Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation Nonlinear Dyn. 77 687-98
[11] Zhu Z L, Zhang W, Wong K W and Yu H 2011 A chaos-based symmetric image encryption scheme using a bit-level permutation Inform. Sciences 181 1171-86
[12] Chen Y and Ueta T 1999 Yet another chaotic attractor Int. J. Bifurcat. Chaos 9 1465 - 6
[13] Watson J D and Crick F H 1953 Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid Nature 171 737-8
[14] Kwok H S and Tang W K S 2007 A fast image encryption system based on chaotic maps with finite precision representation Chaos Soliton. Fract. 32 1518-29