New color image encryption algorithm based on double chaos system

Qi Qi Cun, Xiaojun Tong*

Computer Science and Technology, Harbin Institute of Technology, Weihai, 264200, China

*corresponding author.
E-mail address: tong_xiaojun@hit.edu.cn, cunqiqi @163.com

Abstract. Due to the specific characteristics of a chaotic system described by a set of nonlinear deterministic dynamic equations, encryption based on chaos has high security. Therefore, this paper proposes a very safe and effective new color image encryption algorithm based on double chaos system. First, a true color image is divided into three channels, and under the operation of the control signal, different pseudo-random sequences generated by the Chirikov standard image are selected for XOR operation with the image pixels of a certain channel. Secondly, this paper provides a process of generating replacement boxes using one-dimensional attacks and entropy-based attacks. Therefore, the algorithm has a good encryption effect and has broad application prospects in the field of image encryption.

1. Introduction
In today's society, digital images have become one of the most valuable assets in human life. Therefore, the need to protect the information contained in the image is particularly urgent. Many scholars at home and abroad consider applying chaos theory to image encryption. For example: Pak C [1] proposed an image encryption algorithm based on one-dimensional Logistic chaotic system. Elazzaby F [2] uses two-dimensional chaos to encrypt images. Chen [3] proposed a color image encryption algorithm based on two-dimensional CIMM chaotic mapping. Ying [4] proposed to use the Zig-Zag scanning method to scan the random laser speckle and Logistic chaotic mapping to encrypt the image. Ying [5] proposed an improved chaotic image encryption algorithm. Xiao [6] proposed an encryption method that uses different chaos and different structures to perform multiple rounds of diffusion on the three primary color components of a color image.

However, these algorithms generally have some problems. One is that low-dimensional chaotic maps are well known. If these chaotic maps are simply used, the cracker may use a high-performance computer to calculate the key with sufficient accuracy when the number of plaintext and ciphertext is small. The second is for color images. They only encrypt the three layers of RGB separately. If the cracker decrypts one layer, he can know the complete image information without knowing the plaintext of the other two layers.

Therefore, this paper proposes a new color image encryption algorithm based on double chaos system. The algorithm divides a true-color image into three channels, and generates a control signal by analyzing the plaintext of one of the channels, thereby selecting different pseudo-random sequences for XOR operation, and then performing pixel replacement, confusion, and diffusion, and outputting the secret. The text is fed back to the input of the next round of encryption and used as the key for
another channel. Since the chaotic system used in the encryption process of this method is not only related to the initial value, but also related to the ciphertext of another channel, each encryption process is safe and random. Moreover, the encryption of the three channels of the color image is interrelated, so it is basically impossible for a decryptor to decrypt through past experience.

2. Design of Encryption Algorithm based on Double Chaotic System

2.1. Research on Classical Chaotic System

1) Logistic graph [7] is a one-dimensional classical chaotic graph, and its mathematical form is defined as (1).

\[ x_{n+1} = \lambda x_n (1 - x_n) \]  

Among them, \( x_n \in (0, 1) \), \( n = 1, 2, 3 \ldots \), \( \lambda \in (0, 4) \), when \( \lambda \in \left[3.5699456, 4\right) \), the system is in a chaotic state.

2) The Chirikov standard graph [8] is a two-dimensional chaotic model, and its dynamic equation is (2) and (3).

\[ x_n = x_{n-1} + \alpha \sin(y_{n-1}) \text{ mod } (2\pi) \]  
\[ y_n = y_{n-1} + x_n \text{ mod } (2\pi) \]  

When \( \alpha > 5 \), a better distribution is obtained.

2.2. Color Image Encryption Algorithm based on Double Chaos System

The encryption process involves four main steps. Using plaintext to generate control signals is the first step, using Chirikov standard graphs and logistic graphs to generate chaotic sequences is the second step, pixel replacement, confusion and diffusion are the third step, and ciphertext feedback is the last step. Here, we assume that the size of the image \( I \) is \( M \times N \times 3 \).

**Step1:** Convert the input 3-dimensional true color image into three 2-dimensional channels.

\[
\begin{align*}
R &= I(:, :, 1) \\
G &= I(:, :, 2) \\
B &= I(:, :, 3)
\end{align*}
\]  

**Step2:** Use channel R, channel G, and channel B to generate control signals \( C_r, C_g, C_b \) respectively. Take the R channel as an example.

\[
\sum_{0 \leq i < M-1} R(i, j) / M \times N
\]  

**Step3:** Channel R uses (2) and (3) to generate chaotic sequences \( R_x_i = \{R_{x_1}, R_{x_2}, \ldots, R_{x_{M*N-1}}\} \) and \( R_y_i = \{R_{y_1}, R_{y_2}, \ldots, R_{y_{M*N-1}}\} \). Then use (1) to generate a chaotic sequence \( R_z_i = \{R_{z_1}, R_{z_2}, \ldots, R_{z_{M*N-1}}\} \), and convert it into a two-dimensional array \( R_x(i, j), R_y(i, j), \text{ and } R_z(i, j) \). Use (6), the value of the chaotic sequence is limited between 0 and 255.

\[
\begin{align*}
Rx(i, j) &= \text{mod}(\text{floor}(Rx(i, j) \times 10^9), 256) \\
Ry(i, j) &= \text{mod}(\text{floor}(Ry(i, j) \times 10^9), 256) \\
Rz(i, j) &= \text{mod}(\text{floor}(Rz(i, j) \times 10^9), 256)
\end{align*}
\]
Step4: Determine the control signal $C_r$, and then perform bitwise XOR operation on channel R and chaotic sequence $R_x(i, j)$ or $R_y(i, j)$.

\[
\begin{align*}
Rx1(i, j) &= R(i, j) \text{ XOR } R_x(i, j), \text{mod} (Cr, 2) = 0 \\
Rx1(i, j) &= R(i, j) \text{ XOR } R_y(i, j), \text{mod} (Cr, 2) \neq 0
\end{align*}
\]  

Step5: Use the chaotic sequence $R_x(i, j)$ to generate an S-box to confuse the pixel values of $Rx1(i, j)$.

Step6: Use chaotic sequence $R_x(i, j)$ to perform diffusion operation on the result of Step5, and the result is $Rx2$.

Step7: The result of $Rx2$ is fed back to R next round of encryption, as the chaotic initial value of the next round of encryption, and as the initial key of the next channel G. See Fig. 1 for the R channel encryption process.

3. Simulation Experiment and Analysis

3.1. Simulation
In this paper, two true color images are selected for simulation experiments. The experimental results are shown in Fig. 2.

![Simulation experiment](image-url)
3.2. Histogram
Fig. 3 shows the original image histogram and the encrypted histogram of the Lena image. It can be seen from the result that the encrypted image is randomly distributed, and the histogram is evenly distributed. This shows that the algorithm has good encryption performance.

![Histogram of Lena image](image1)

3.3. Correlation Analysis
The correlation coefficient between adjacent pixels is one of the most important parameters of cryptanalysis. In order to check the correlation of adjacent pixels after encryption, this paper graphically shows the position pixel values before and after encryption in Figure 4, and lists the correlation coefficients in Tab. 1. After observation, it is found that the correlation coefficient is close to 0, indicating that the algorithm proposed in this paper has higher security.

![Correlation coefficient of Lena image](image2)

3.4. Information Entropy
Entropy is a measure of the uncertainty of random variables in information theory. The calculation formula is shown in (8).

\[
H(m) = \sum_{i=1}^{n} P_i \log P_i
\]  

(8)
In an image with a sample space size of 256, the maximum value of entropy is 8. As shown in Table 2, comparing with the entropy in other algorithms, it is proved that the algorithm proposed in this article has higher information entropy, so the algorithm in this article is more secure against entropy-based attacks.

### Table 1. Correlation coefficient analysis

| Images                        | Horizontal | Vertical | Diagonal |
|-------------------------------|------------|----------|----------|
| Original Lena image           | 0.9890     | 0.9809   | 0.9699   |
| Lena image after encryption   | -0.0150    | 0.0029   | 0.0081   |
| Original Baboon image         | 0.8699     | 0.9180   | 0.8278   |
| Baboon image after encryption | 0.0078     | 0.0029   | 0.0072   |

### Table 2. Comparison of information entropy

| Information entropy          |
|-------------------------------|
| proposed algorithm            | 7.9920     |
| Ref. [9]                      | 7.9564     |
| Ref. [10]                     | 7.9595     |
| Ref. [11]                     | 7.977      |

### 3.5. Differential Attack

To quantify the difference between images, two measurement methods are usually used: Net Pixel Change Rate and Unified Average Changing Intensity. The definitions of NPCR and UACI are shown in (9-11).

Here \( c \) and \( c' \) are images of size \( M \times N \). This experiment randomly changed a pixel of the plaintext, compared the difference between the ciphertext image corresponding to the plaintext image and the ciphertext image corresponding to the plaintext image by 1 pixel bit change, and calculated its NPCR and UACI. The results are shown in Table 3. The experimental results show that a small change in the plaintext image can make a huge change in the ciphertext image. Therefore, the algorithm is not affected by differential attacks.

### Table 3. Differential Attack Test

|                  | UACI (%) | NPCR (%) |
|------------------|----------|----------|
| proposed algorithm| 33.4828  | 99.61    |
| Ref. [9]          | 33.46    | 99.61    |
| Ref. [12]         | 33.3     | 99.5     |
| Ref. [13]         | 33.41    | 99.59    |

\[
D(i, j) = \begin{cases} 
0, & c(i, j) = c'(i, j) \\
1, & c(i, j) \neq c'(i, j)
\end{cases}
\]

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

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

### 4. Conclusion

The encryption algorithm proposed in this article involves four main steps. Using plaintext to generate control signals is the first step, using Chirikov standard graphs and Logistic graphs to generate chaotic sequences is the second step, pixel replacement, confusion and diffusion are the third step, and ciphertext feedback is the last step. Through experimental analysis of its histogram, correlation.
coefficients between adjacent pixels, information entropy, NPCR and UACI, the results show that the algorithm has a large key space enough to resist exhaustive attacks, and the analysis shows that the algorithm can effectively resist differential attacks and entropy-based attacks. Therefore, the algorithm has a good encryption effect and has broad application prospects in the field of image encryption.

Acknowledgments
This work was supported by the following projects and foundations: project ZR2019MF054 supported by Shandong Provincial Natural Science Foundation, the National Natural Science Foundation of China (No.61902091, 61702139) and Innovation Research Foundation of Harbin Institute of Technology (HIT.NSRIF.2020009), the Foundation of Science and Technology on Information Assurance Laboratory (No.KJ-17-004), 2017 Weihai University Co-construction Project.

References
[1] Pak C , Huang L . A new color image encryption using combination of the 1D chaotic map. Signal Processing, 2017, 138(SEP.):129-137.
[2] Elazzaby F , Akkad N E , Kabbaj S . Advanced encryption of image based on S-box and chaos 2D (LSMCL)[C]// 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET). 2020.
[3] Cengfei Chen,Kehui Sun,Qiaoyun Xu.A Color Image Encryption Algorithm Based on 2D-CIMM Chaotic Map. China Communications,2020,17(05):12-20.Wu Fangbai, Liu Biao,et al. Analysis of the interlocking effect of the combined interface in a new type of composites floor[J]. Journal of Hunan University, 2014,41(2):1-7(in Chinese).
[4] Jiao Ying,Feng Tao He,Hong Xi Wang. Color image encryption based on the combination of Zig-Zag scanning laser speckle and chaos. Laser magazine,2018,39(03):85-88.
[5] Xi Ying,Wei Qing Huang. Research on Color QR Code Watermarking Technology Based on Chaos Theory. Journal of Communications,2018,39(07):50-58.
[6] Feng Xiao,Li Li Zhang,Fei Feng. Parallel multi-channel color image encryption for hybrid chaotic system. Microelectronics and Computer,2016,33(08):76-81.
[7] Sui L,Duan K,Liang J. Double-image encryption based on discrete multiple-parameter fractional angular transform and two-coupled logistic maps. Optics Communications, 2015, 343:140-149.
[8] Narcis Miguel, Carles Simó, Arturo Vieiro. From the Hénon conservative map to the Chirikov standard map for large parameter values.2013,18(5):469-489.
[9] Avuolu, Ünal, Kaar S , Zengin A. A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics,2018,92(4):1745-1759.
[10] Shah AA, Parah SA, Rashid M. Efficient image encryption scheme based on generalized logistic map for real-time image processing. Journal of Real-Time Image Processing,2020(5).
[11] Aashiq BS, Noorul NA, Harini M. Implementation of Image Encryption based on Chaos-IWT–An Image security// 2020 International Conference on Computer Communication and Informatics (ICCCI).2020.
[12] Norouzi B, Seyedzadeh SM, Mirzakuchaki S. A novel image encryption based on hash function with only two-round diffusion process. Multimedia Systems,2014,20(1):45-64.
[13] Chai X, Chen Y, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Optics & Lasers in Engineering,2017,88(Complete):197-213.