The novel image encryption scheme based on three-dimentional coupled chaotic system

Xudong Ren\textsuperscript{1,a}, Wanbo Yu\textsuperscript{2,b,*}

\textsuperscript{1}School of Information Engineering, Dalian University, Dalian, Liaoning Province, China
\textsuperscript{2}School of Information Engineering, Dalian University, Dalian, Liaoning Province, China
\textsuperscript{a}email: 767152581@qq.com
\textsuperscript{b}Corresponding author’s e-mail: yuwanbo@dlu.edu.cn

Abstract. In order to improve the complexity of chaotic mapping and the security of image encryption algorithms, this paper proposes a new coupled three-dimensional chaotic system based on sine mapping and Lorenz mapping. Based on this chaotic system, a new color image encryption algorithm is proposed, which performs index position scrambling and Arnold scrambling on the bit plane of the plaintext image, and then performs an XOR diffusion operation on the scrambled ciphertext to obtain the final ciphertext image. Simulation experiments show that the algorithm has a large key space, a small image correlation coefficient, an information entropy value of 7.9921, and a good encryption effect.

1. Introduction

In modern society, information security has received great attention from people, and the research on image encryption has important practical significance\cite{1}. The traditional IDEA\cite{2}, DES\cite{3} and AES\cite{4} encryption algorithms are aimed at binary data and text data, and are easy to decrypt. Therefore, it is necessary to study encryption algorithms with better performance. Chaos phenomenon is a kind of inherent random process performance of nonlinear system. The chaotic sequence generated by chaotic system has the characteristics of noise-like, complex structure and extremely sensitive to initial conditions. Therefore, it is widely used in encryption system design\cite{5-8}. The chaotic characteristics of chaotic systems have an important impact on the security of image encryption. For example, Sine mapping and Logistic mapping of one-dimensional chaotic mapping. Although the encryption speed is fast, the variable parameters are less, the structure is relatively simple, the probability density distribution is uneven, and the encryption security is low \cite{9}. However, high-dimensional chaos has a larger key space, and its behavior trajectory is very complex and difficult to predict, so it is more suitable for image encryption\cite{10}. In the research of the color image encryption algorithm of the chaotic system, if a one-dimensional chaotic system is used, then it needs to be improved. For example, the parameter coupling of multiple one-dimensional maps, or the coupling between a one-dimensional map and a high-dimensional chaotic map. In order to solve the problem of low-dimensional chaotic characteristics, the problem of low security of traditional encryption algorithms, the problem of the encryption space, and the connection between the three primary colors of the image is relatively large, this paper proposes an encryption algorithm based on a new coupled three-dimensional chaotic system. The scrambling operation is performed on the bit level first, and then the pixel level is encrypted for...
the second time. Finally, experiments are carried out based on real images, and the results show that this method has high security, robustness and anti-attack characteristics.

2. Chaotic System

In order to solve the problem of the periodic window and low security of the Sine mapping system and the weaker chaotic characteristics of the Lorenz mapping system, this paper combines the Sine mapping and the Lorenz mapping through the coupling method to construct a new type of 3D-SL Chaotic system, the simulation experiment shows that the system has good chaotic characteristics. The expression of the 3D-SL chaotic system is shown in equation (1):

\[
\begin{align*}
X_i + 1 &= \mu \ast \sin(p1 \ast x_i) + a \ast (\sin(p2 \ast y_i) - \sin(p1 \ast x_i)) \ast k \\
Y_i + 1 &= \mu \ast \sin(p2 \ast y_i) + (\sin(p1 \ast x_i) \ast (c - \sin(p3 \ast z_i)) - \sin(p2 \ast y_i)) \ast k \\
Z_i + 1 &= \mu \ast \sin(p3 \ast z_i) + (\sin(p1 \ast x_i) \ast \sin(p2 \ast y_i) - b \ast \sin(p3 \ast z_i)) \ast k
\end{align*}
\]

(1)

3. Encryption Algorithm

In a digital image, the pixel value of a grayscale image ranges from 0 to 255, and the conversion to binary is 8 bits. The grayscale image is expanded according to the binary system. The numbers in the same bit form a plane, so a grayscale image has 8 bit planes. In a color image, there are 8 bit planes for each of the R, G, and B components. By decomposing the bit plane of the Lena image, it can be seen that the higher the bit plane, the more information it contains. The upper four bits contain the main image information, while the lower four bits change very randomly. Therefore, the high four-bit plane and the low four-bit plane are scrambled separately, then perform a diffusion operation on the scrambled bit plane.

| Bit plane | Amount of information/% |
|-----------|-------------------------|
| P1        | 0.39                    |
| P2        | 0.78                    |
| P3        | 1.57                    |
| P4        | 3.14                    |
| P5        | 6.28                    |
| P6        | 12.55                   |
| P7        | 25.10                   |
| P8        | 50.20                   |

The encryption algorithm structure used in this article is a scrambling-diffusion structure. Taking the encryption process of the R layer as an example, the encryption flowchart is shown in ‘figure 1’. The specific process is as follows:

![Figure 1. R-layer encryption flowchart.](image-url)
Step 1: The R layer is decomposed into 8 bit planes, the lower five bit planes are denoted as Rpic (i=1, 2, ..., 5), the upper three bit planes are denoted as Rp6, Rp7, Rp8. The image size of each bit plane is M×N (M and N are both integers), R(i,j) represents the size of the pixel value at the i-th row and j-th column of the plaintext image R layer.

Step 2: Set the chaos control parameters as a, b, c, u, p1x, p2, p3, k, Initial value x₀, y₀, z₀, iterate m + M×N times, in order to eliminate the influence brought by the transient process, discard the first m sequences, and obtain 3 chaotic sequences of length M×N.

\[ x_i = [x_{m+1}, x_{m+2}, ..., x_{m+MN}], y_i = [y_{m+1}, y_{m+2}, ..., y_{m+MN}], z_i = [z_{m+1}, z_{m+2}, ..., z_{m+MN}], \]
\[ x'_i = [x'_{m+1}, x'_{m+2}, ..., x'_{m+MN}], y'_i = [y'_{m+1}, y'_{m+2}, ..., y'_{m+MN}], z'_i = [z'_{m+1}, z'_{m+2}, ..., z'_{m+3}] \]

Sort these three sequences in descending order, and get the sequence as \( x'_1, y'_1, z'_1 \) in the original sequence of these three sequences, write down the corresponding conversion position matrix \( T_{x_i} = [T_{x_1}, T_{x_2}, ..., T_{x_{MN}}], T_{y_i} = [T_{y_1}, T_{y_2}, ..., T_{y_{3}}] \).

Step 3: According to the conversion position matrix \( T_{x_i}, T_{y_i} \) and \( T_{z_i} \) rearrange each high-order vector Rpn (n=6, 7, 8) to obtain three scrambled vectors Rpn’.

Step 4: Expand the image of the lower five-bit plane into a one-dimensional vector P, denoted as A, with a size of 5×M×N, perform an improved Arnold transformation on any coordinate position (1, j) to obtain a new coordinate position (p, q). Use formula (2) to scramble the plain text image to get the scrambled cipher text image.

\[ w_i = \text{mod} \left( \left( \text{floor} \left( \frac{x_i + y_i + z_i}{3} \right) \times 10^{14} \right), 256 \right) \] (2)

Expand the image pixel values of the 8 planes after scrambling into a one-dimensional sequence \( O(i=1, 2, ..., 8) \), perform forward and reverse XOR diffusion operations on the scrambled cipher text according to equations (3) and (4). After the above two operations, the encrypted binary image Rpinc’ (i=1, 2, ..., 8) is obtained, and the 8 binary images are combined to obtain the encrypted image R’.

\[ C_i = C_{i-1} \oplus S_i \oplus O_i \] (3)
\[ C_i = C_{i+1} \oplus S_i \oplus O_i \] (4)

Step 6: Encrypt the G and B components in the same way to obtain the encrypted image G’, B’, and arrange the three image matrices horizontally to obtain the encrypted ciphertext image P1.

4. Experiment And Analysis Of The Encryption Scheme

4.1. Experimental simulation

The computer used in the experiment is configured with 16G memory, WINDOW10 operating system, and the simulation software is MATLAB R2016a. In the simulation experiment, the Lena image is selected as the plaintext image, the image size is 512×512, and the initial values of the three-dimensional coupled chaotic system \( x_0=2.156, y_0=1.456, z_0=4.668, \mu=3.3 \) are used as the key. Set the internal parameters \( a=10, b=8/3, c=28, p_1=13.1, p_2=11.4, p_3=8.5 \), after experimental testing, the ciphertext image is shown in ‘figure 2’.

![Figure 2. Experimental results.](image-url)
4.2. Statistical analysis of histogram

Histogram analysis is the most common method used to analyze image encryption. You can intuitively see the proportion of image pixel size. If the distribution of the ciphertext histogram is relatively uniform, useful image information cannot be obtained from it. The histograms corresponding to the plaintext image and the ciphertext image are shown in ‘figure 3’. It can be concluded that the encrypted ciphertext image cannot obtain any plaintext image information and can resist statistical analysis attacks.

![Figure 3. Plaintext and ciphertext histogram.](image)

4.3. Correlation analysis of adjacent pixels

Correlation analysis of adjacent pixels is used to reflect the degree of diffusion of pixels. Generally, the pixels of the image are highly correlated in the horizontal, vertical, and diagonal directions. The correlation of the ciphertext image obtained after the algorithm is encrypted will be reduced. Generally speaking, the stronger the encryption algorithm performance, the lower the correlation of adjacent pixels. This paper randomly selects 4000 pixels for calculation. The correlation coefficient of adjacent pixels can be calculated by formula (5), where x, y are the adjacent pixel pairs randomly selected in the image, K is the number of pixel pairs, \(\text{cov}(x,y)\), \(\text{D}(x)\), \(\text{E}(x)\) Represents the covariance, variance and average value respectively.

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

\[
\text{cov}(x, y) = \frac{1}{K} \times \sum_{i=1}^{K} (x_i - \text{E}(x)) \times (y_i - \text{E}(y))
\]

\[
\text{D}(x) = \frac{1}{K} \times \sum_{i=1}^{K} (x_i - \text{E}(x))^2
\]

\[
\text{E}(x) = \frac{1}{K} \times \sum_{i=1}^{K} x_i
\]

The analysis results are shown in Table 2, ‘figure 4’, and ‘figure 5’. It can be seen that the adjacent points of the ciphertext image in all directions have almost no relationship.
4.4. Information entropy analysis

Information entropy is used to describe the uncertainty of information and reflects the gray distribution in the image. When the probability of each gray value in the image is equal, the information entropy of the image is the largest, and the information entropy of the gray image is ideally 8. The formula for calculating the information entropy is shown in (9).

\[
H = - \sum_{n=0}^{255} p(n) \log_2 p(n)
\]  

(9)

In the formula, p(n) is the probability of the appearance of the image gray level n. According to formula (9), the encrypted image information entropy is 7.9921, and the original image information entropy is 7.6735. It can be seen that the information encrypted by the algorithm in this paper Entropy is very close to 8, so it can better resist statistical attacks.

4.5. Analysis of anti-differential attack ability

Differential attack is a selective plaintext attack. In order to resist the differential attack, the encryption algorithm must be highly sensitive to the plaintext image. Even if the pixel value of the plaintext image is slightly modified, it can produce a completely different ciphertext image. NPCR pixel change rate and UACI average change intensity are important indicators for judging the ability of image encryption algorithm to resist differential attacks. The corresponding calculation formula is as follows.
Two images with significant differences, the ideal values of NP CR and UACI are 99.6045% and 33.4635% \textsuperscript{[11]}. Randomly select and change a pixel value in "lena" for testing, and the results are shown in Table 3. It can be seen that compared with literature \textsuperscript{[12]} and literature \textsuperscript{[13]}, the test values of NPCR and UACI in this article are both close. The theoretical expectation value shows that the algorithm can effectively resist differential attacks.

\begin{align}
NPCR &= \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \\
UACI &= \frac{1}{M \times N} \left[ \sum_{i} \sum_{j} \frac{|D_1(i,j) - D_2(i,j)|}{256} \right] \times 100\%
\end{align}

Table 3. NPCR and UACI values.

| Algorithm | Document \textsuperscript{[17]} Algorithm | Literature \textsuperscript{[18]} Algorithm |
|-----------|------------------------------------------|------------------------------------------|
| NPCR      | 99.64                                    | 99.72                                    |
| UACI      | 33.85                                    | 33.73                                    |

5. Conclusion
This paper proposes an image encryption algorithm that encrypts at the bit level. By coupling the sine chaotic map and the lorenz chaotic map, a 3D-SL high-dimensional chaotic system with excellent chaotic performance is constructed. The chaotic sequence generated by the 3D-SL chaotic system is used to scramble and diffuse the image, and the encryption is performed on the bit-level plane and the pixel-level plane respectively. The experimental results show that the algorithm has a large key space, strong key sensitivity, small correlation between adjacent pixels, and strong robustness. It can effectively resist external entropy attacks, differential attacks and brute force attacks, and has a good encryption effect.

Acknowledgments
Thank you for the support of the Dalian University Graduate Education and Teaching Reform Fund (2021)

References
[1] Jinyuan Liu, Jike Ge, Jitao Tang. A fast chaotic image encryption algorithm based on improved Sine map[J]. Journal of Chongqing University of Science and Technology (Natural Science Edition),2020,22(05):75-80+90.
[2] Xuejia Lai, MASSEY J L.A proposal for a new block encryption standard[C]. Proc of Workshop on the Theory and Application of Cryptographic Techniques, Heidelberg:Springer, 1990:389-404.
[3] FIPS PUB.46-3 Data encryption standard(DES) [EB/OL]. [1999-10-25].
[4] DAEMEN J, RIJMEN V.The design of rijndael:AES the advanced encryption standard[M]. Berlin: Springer Press, 2002.
[5] Fangzheng Zhao, Chenghai Li, Chen Liu, Yafei Song. Optimization and security analysis of hyperchaotic color image encryption algorithm[J]. Computer Science,2019,46(S2):483-487.
[6] Jinyuan Liu, Jike Ge, Jitao Tang. A fast chaotic image encryption algorithm based on improved Sine map[J]. Journal of Chongqing University of Science and Technology (Natural Science Edition),2020,22(05):75-80+90.
[7] Yun Tan, Chunhu Zhang, Jiaohua Qin, Xuyu Xiang. Image encryption algorithm based on exponential compound chaotic system[J]. Journal of Huazhong University of Science and Technology (Natural Science Edition),2021,49(02):121-126.
[8] Jiaqi Tian, Shucui Xie, Jianzhong Zhang. Color image encryption algorithm based on chaotic system [J]. Computer Engineering and Design, 2019, 40(07): 1816-1822.
[9] Li C, Lin D, Lü J et al. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography [J]. IEEE Multimedia, 2018 25(4):46-56.
[10] Qing Lin, Yangjiang WANG, Jun WANG. Image encryption algorithm based on hyperchaotic system [J]. Science in China: Science of Technology, 2016, 46(9): 910-918 (in Chinese).
[11] Feng Xiao, Lili Zhang, Fei Feng. Parallel Multi-channel Color Image Encryption Based on Hybrid Chaotic System [J]. Microelectronics & Computer, 2016, 33(08): 76-81.
[12] Qing Lin, Yanjiang Wang, Jun Wang. Image encryption algorithm based on hyperchaotic system [J]. Science in China: Technological Sciences, 2016, 46(09): 910-918.
[13] Cong Ma, Guodong Li. Color bit-level image encryption algorithm based on L-K double chaos system [J]. Computer Applications and Software, 2020, 37(03): 321-326.