Research on Chaotic Digital Image Encryption Algorithm

Ye Jia1, Zheng Yu-fu1, Yang Zi-wei1
1School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China
e-mail:1527049813@qq.com

Abstract. In view of the problems of pseudo-randomness, complexity, short period and limited precision of traditional digital image encryption technology, this paper improves the traditional chaotic digital image encryption technology. Firstly, a random sequence is generated from the chaotic map according to the definition, and then the design process is improved according to the encryption algorithm, and finally the simulation experiment is performed. The improved algorithm uses the Henon-mapped chaotic sequence to generate the shuffle control parameters, and replaces the gray value with the improved two-dimensional Logistic map sequence, shuffles the array using the Henon map, and changes the image pixels using the improved two-dimensional Logistic map. Grayscale values, these algorithms are highly secure against exhaustive attacks, statistical attacks, and plain-text attacks. Even if the attacker knows the algorithm, it does not know the parameters of the algorithm and cannot obtain image information. The improved encryption algorithm can increase the key space and improve the security performance of the encryption algorithm. The image viewing effect is also very good, and the time is greatly shortened, which can fully meet the real-time requirements.

1. Introduction
With the rapid development of multimedia technology, video communication has gradually become an important means of communication, and its information security has received more and more attention[1-2]. The research of image encryption technology is also a research field that people pay attention to. For the traditional digital image encryption technology, there is a detention in the numerical simulation stage, and there is no theoretical proof, and the operation precision is limited, which is easy to cause major problems such as the cycle sequence[3]. At present, most of the digital image encryption is based on the spatial domain encryption exchange method of pixel coordinate points, and its security performance is reduced. The Arnold mapping algorithm is proposed in [4]. The literature [3, 4] applies it to digital image encryption, and proposes an Arnold mapping encryption algorithm, although the Arnold mapping can perform digital images between pixel coordinate points of images. Encryption, but this has the obvious disadvantage of not being able to exchange the original image.

2. Improved digital image encryption algorithm
In view of the above deficiencies, this paper proposes a new image encryption method: based on improved chaotic digital image encryption. The advantage of this method is that it can be combined with other watermarking schemes to make these schemes more secure; another advantage is that it allows the user to select different parameters and even use pseudo-random numbers to control the implementation of the algorithm, which means potential attackers. There are great difficulties in restoring the original image. Even if the attacker knows the algorithm, the image cannot be restored without knowing the parameters of the algorithm.
Below we extend the three-dimensional chaotic map by introducing four control parameters a, b, c and d:

\[
\begin{bmatrix}
    x \\
    y \\
    z
\end{bmatrix} =
\begin{bmatrix}
    1 & a & 0 \\
    b & ab+1 & 0 \\
    c & d & 0
\end{bmatrix} \bullet
\begin{bmatrix}
    x \\
    y \\
    z
\end{bmatrix} \mod N = R
\begin{bmatrix}
    x \\
    y \\
    z
\end{bmatrix} \mod N
\]

Where a and b are two positive integers, and c and d are two integers. Then, using matrix theory, the eigenvalue of R can be:

\[
\lambda_1 = ab + 1 > 1, \quad \lambda_2 = \lambda_3 = 1, \quad \text{when } \sigma_1 = \ln \lambda_1 > 0, \quad \text{and } \sigma_2 = \sigma_3 = 0.
\]

According to the knowledge of chaos theory, the three-dimensional cat map is chaotic, so it can be used for chaotic digital image encryption.

In the scheme presented in this paper, x, y and x', y' in mapping (1) are considered to be image positions before and after mapping, and z and z' are considered as grays of images before and after mapping. Degree value, in which case we change z to p and convert (1) to the following mapping form:

\[
\begin{bmatrix}
    x' \\
    y'
\end{bmatrix} =
\begin{bmatrix}
    1 & a \\
    b & ab+1
\end{bmatrix} \bullet
\begin{bmatrix}
    x \\
    y
\end{bmatrix} \mod N
\]

\[
p' = (cx + dy + p) \mod M
\]

Here, N is the width and height of the image, M is the color level (for 256 grayscale images, M = 256), and the 3D cat map proposed in equation (2) can achieve double encryption, that is, shuffling and replacement. First, the 3D cat map can use the 2D cat map to change the position of the pixel. After n(n>1) iterations, the correlation between adjacent pixels can be completely disturbed. In addition, the 3D cat map can be based on the pixel. The position and the original gray value are used instead of the gray value. After the pure image is transformed as described above, the password image is completely unrecognizable, and the distribution of the gray value is uniform.

2.1 Design of Chaotic Digital Image Encryption Algorithm

In the cat diagram given by equation (2), the effect of shuffling is determined by parameters a, b and n, and the operation of the replacement is determined by parameters c and d. In order to resist the periodic attack of the two-dimensional Arnold cat mapping and to make the chaos and permutation operations sensitive to the key, the control parameters in equation (2) are generated by the pseudo-random sequence of the chaotic system. This not only improves the security of encryption, but also enhances the chaos of the extended 3D cat map. Since the one-dimensional chaotic system can be easily decrypted, and the three-dimensional Lorenz chaotic system and the Chen chaotic system are continuous dynamic systems, the two-dimensional Henon map is used to generate the shuffling and improved control parameters, and more random two-dimensional Logistic is used. Map to generate alternate parameters.

2.1.1 Generation of chaotic digital image control parameters

Generation of chaotic digital image control parameters...

\[
\begin{align*}
    x_{i+1} &= 1 - px_i^2 + y_i \\
    y_{i+1} &= qx_i
\end{align*}
\]

Among them, when 1.025<p<1.4, q=0.3, the system is in a chaotic state, and a chaotic sequence (-1.3, 1.3) can be generated in the region, and 10000 points are generated by selecting the initial value (x0, y0). Among them, 6000 points, assuming that the acquired sequence is S={(xi, yi)|i=1, 2...6000}, select the rth point from the sequence S, and then generate the values of parameters a and b, as follows:

As shown in the formula:
Starting from the \((r+1)\)th point, the value of the parameter \(n\) is generated by selecting \(t\) points from the sequence \(S\) as follows:

\[
\begin{align*}
    a &= x_r \times 10^{12} \mod k_1 + 1 \\
    b &= y_r \times 10^{12} \mod k_1 + 1 \\
\end{align*}
\]

\((0 < r < 6000)\) \hspace{1cm} (4)

Where \(k_2\) represents the half period of the two-dimensional Arnold map. Since \(r, t, k_1\) determine the values of the control parameters \(a, b\) and \(n\), they can be used as keys other than the initial values \(x_0\) and \(y_0\), thus, three control parameters is sensitive to the initial value of the Henon map. Furthermore, no password is built, and the attacker cannot use the periodicity of the Arnold map to obtain a clear image.

### 2.1.2 Generation of chaotic digital image substitution parameters

In the process of replacing the gray value by formula (2), no matter which one gray value is substituted, a pair of values are selected from the chaotic sequence as parameters \(c\) and \(d\) to obtain higher randomness and unpredictability of the chaotic system. As follows:

\[
\begin{align*}
    x_{i+1} &= \mu_1 x_i (1-x_i) + \gamma_1 y_i^2 \\
    y_{i+1} &= \mu_2 y_i (1-y_i) + \gamma_2 (x_i^2 + x_i y_i) \\
\end{align*}
\]

\((6)\)

In equation (6), three quadratic coupling terms are added, mainly to enhance the complexity of the system.

In the formula (6), when \(2.75 < \mu_1 < 3.4, 2.7 < \mu_2 < 3.45, 0.15 < \gamma_1 < 0.21, 0.13 < \gamma_2 < 0.15\), the system is in a chaotic state, and a region \((0, 1)\) can be generated. In order to make the generated chaotic sequence more and more random, the random sequence \(S' = \{(x_i, y_i) | i = 1, 2,...\}\) generated by formula (6) is transformed as follows:

\[
X_i = 10^4 X_i - \text{round}(10^4 X_i)
\]

\((7)\)

Among them, \(X_i\) can be represented by \(x_i\) or \(y_i\), and round is the operator closest to the integer. After processing, the chaotic sequence is in the \((-0.5, 0.5)\) region, after further conversion:

\[
X_i = \begin{cases} 
    X_i, & X_i > 0 \\
    1 + X_i, & X_i \leq 0 
\end{cases}
\]

\((8)\)

In this way, the range of the chaotic sequence is returned to the region \((0, 1)\). At the same time, compared with the sequence directly generated by the formula (6), the scrambling sequence has better randomness and its distribution is more colorful.

### 2.1.3 Chaotic digital image encryption process

Based on the above digital image encryption algorithm design, the image encryption process is shown in Figure 1:
The following is a detailed description of image encryption:

Input. Suppose the image to be encrypted is I;

Randomly place the pixels. Select several passwords \((x_0, y_0)\), and generate chaotic discrete sequence \(S\) according to equation (3). Then, according to equation (4) and equation (5), select key \(r, t, k_1\) to generate control parameters \(a, b, \), \(n\), for the position \((x, y, z)\) of each pixel in the image, the formula (1) is performed \(n\) times, then the shuffle image \(I_1\) can be obtained;

Replace the gray value of the pixel. Select another pair of keys \((x_0, y_0)\), generate another discrete chaotic sequence \(S'\) according to equation (6), and further process equations (7) and (8) for each position \((x, y)\) in image \(I_1\). And corresponding gray value \(p\), continuously select a sequence point \((x_i, y_i)\) from \(S'\), according to equation (2), by setting \(c=x_i\), \(d=y_i\), and changing \((x, y)\), in processing after all the pixels in image \(I_1\), the final password image \(I_2\) can be obtained\(^{[5-7]}\).

2.1.4 Chaotic digital image decryption process

The decryption process of a digital image is similar to an encryption process with a sequence of reverse operations. First, the gray value of the ciphertext image is replaced with the gray value of the original image, that is, for each position \((x, y)\) of the ciphertext image \(I_2\) and the corresponding gray value \(p\), then the original image gray value is calculated. As follows:

\[
p = (2M + p' - cx - dy) \mod M
\]  \(\text{(9)}\)

After all the pixels have returned to the original gray value, we can get the shuffle image \(I_1\), which iterates \(n\) times with the two-dimensional Arnold transform. If the image \(I_1\) continues to transform \(n\) times, the original image will be obtained\(^{[8-10]}\). Therefore, our decryption algorithm introduces an anti-Arnold transform to decrypt the shuffle image by performing the following inverse mapping for each position \((x, y)\) in image \(I_1\):

\[
\begin{bmatrix}
x \\
y
\end{bmatrix} = \begin{bmatrix}
ab + 1 & -a \\
-b & 1
\end{bmatrix} \cdot \begin{bmatrix}
x' \\
y'
\end{bmatrix} \mod N
\]  \(\text{(10)}\)

After following the above steps, the original image \(I\) can be restored and the decryption process ends. As can be seen from the above process, if the key or encryption process is kept secret, the attacker will encounter some difficulties in getting the correct result.

3. Simulation environment and analysis

In order to verify the reliability of the algorithm, the simulation software environment used is MATLAB2018a, the hardware environment is win10 system, the processor is i5, the memory is 4GB,
and the hard disk is 500G laptop. The above simulation environment was used to simulate and decrypt
the image encryption and decryption.

The experimental results show that the algorithm achieves good results in encrypting general
grayscale images and document images, and there is almost no continuous gray region in grayscale.
After multiple shuffling and replacing with highly random chaotic sequences, the ciphertext image
will become completely blurred regardless of the image encrypted, and the algorithm also has high
security. As shown in Figure 2, Figure 3, Figure 4:

![Figure 2 original image](image1)
![Figure 3 scrambled image](image2)
![Figure 4 Encrypted image](image3)

3.1 Correlation coefficient analysis
There is a large correlation between the pixels of the plaintext image, but the encrypted ciphertext
image should have as little correlation as possible. The correlation coefficient is calculated according
to (11)(12)(13):

\[
E(X) = \frac{1}{S} \sum_{i=1}^{S} X_i 
\]

(11)

\[
D(X) = \frac{1}{S} \sum_{i=1}^{S} [X_i - E(X)]^2 
\]

(12)

\[
r_{x,y} = \frac{E[(X - E(X))(Y - E(Y))]}{\sqrt{D(X)D(Y)}} 
\]

(13)

Where: \(X, Y\) represents the gray value of two adjacent pixels; \(E(X)\) and \(D(X)\) respectively represent
the expectation and variance of the gray value of the corresponding pixel. The adjacent pairs of pixels
distributed in the horizontal, vertical, and diagonal directions are respectively selected, and their
correlation coefficients are compared. The results are shown in FIG. 5, FIG. 6, and FIG.7.

![Figure 5 Horizontal adjacent pixel distribution](image4)
![Figure 6 Dense map](image5)

(a) Bright map
(b) Dense map
3.2 Grayscale histogram

The gray histogram of the plaintext image is extremely uneven, and the gray histogram of the encrypted ciphertext image is relatively uniform. The ability to resist statistical attacks can be tested by the uniformity of the gray histogram of the ciphertext image. The test results are shown in Figure 8:

3.3 Key sensitivity analysis

Selecting only one different key to decrypt the ciphertext, the correct key can complete the normal decryption, and finally get the plaintext image, and the decrypted image obtained by the slightly different decryption key is very different from the original text, as shown in Figure 9. Show:
4. Conclusions
This paper presents an improved digital image encryption scheme. This scheme uses the Henon map to shuffle the position and transforms the gray value of the improved Logistic map image pixels to ensure the security of the scheme. According to the combination of algorithms, by setting different parameters, using pseudo-random numbers to control the implementation of the algorithm increases the difficulty for potential attackers to obtain image information. Even if the algorithm is known, the information of the image cannot be obtained without knowing the parameters of the algorithm. The experimental results show that the improved digital image encryption algorithm is superior to the traditional digital image encryption, both from the visual point of view and the position of the image. These improved digital images can improve the encryption efficiency in the space and time of the key.

Acknowledgments
This research was financially supported by Research on Network Selection and Cognitive Spectrum Allocation Joint Algorithm in National Natural Science Foundation of China-High-speed Rail Communication Environment (Grant NO. 61661026;Mission Book Number: 2017.01-2020.12).

References
[1] Wei Shuzhi,Zhu Qi.Video Communication Bandwidth Game Algorithm Based on Network Selection[J].Journal on Communications,2015,36(2):212-220.
[2] Hou Yonghong,Xu Jianming,Zhang Liang.Application Layer Forward Error Correction Technology in Video Communication[J].Journal of Tianjin Polytechnic University,2017,36(1):48-54.
[3] Qin Haiyu, Zhao Haiyan, Zhao He. Study on Digital Image Encryption Algorithm Based on Double Chaos[J]. Bulletin of Science and Technology,2016,32(12):169-173.
[4] Zhang Pengwei, Zhang Tao. Security Analysis of a Digital Image Encryption Algorithm[J]. Computer Engineering and Science,2015,37(09):1652-1655.
[5] Zheng Jiming, Tang Zhirui, Deng Jianxiu, Lin Yao. Digital Image Encryption Algorithm Based on Logistic Chaotic Map[J]. Technology and innovation, 2018(18):8-11.
[6] Li Bo. Arnold Transform and Pseudo-Round Cube Transform in Image Scrambling[J]. Wireless Interconnect Technology, 2018,15(16):141-144.
[7] Shen Chao, Du Juan. An Image Encryption Algorithm Based on Hybrid Hyperchaotic System[J]. Computer Knowledge and Technology,2018,14(20):186-189.
[8] Wang Xianfang, Wang Xiaolei, Wang Junmei, Li Ming. A Dynamic Cat Mapping Chaotic Image Encryption Algorithm[J]. Journal of Henan Normal University(Natural Science), 2018, 46(05): 110-117.
[9] Xu Xiao, Ma Jun, Zhao Fei, Chen Shouhong.Computed Holographic Multi-Image Synchronous Encryption of Arnold Transform and Chaotic Map[J]. Laser Journal,2018,39(06):57-60.
[10] Xu Yang, Huang Yingjiu, Li Hairong. Application of a Switched Lorenz Chaotic System in Image Encryption[J].Packaging Engineering,2018,39(05):179-184.