Hindawi
Advances in Multimedia
Volume 2023, Article ID 9821201, 1 page
https://doi.org/10.1155/2023/9821201

Retraction

Retracted: Multimedia Image Encryption Analysis Based on High-Dimensional Chaos Algorithm

Advances in Multimedia

Received 15 August 2023; Accepted 15 August 2023; Published 16 August 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Zhang, "Multimedia Image Encryption Analysis Based on High-Dimensional Chaos Algorithm," *Advances in Multimedia*, vol. 2021, Article ID 7384170, 8 pages, 2021.

Hindawi
Advances in Multimedia
Volume 2021, Article ID 7384170, 8 pages
https://doi.org/10.1155/2021/7384170

Research Article

Multimedia Image Encryption Analysis Based on High-Dimensional Chaos Algorithm

Xing Zhang

Nanyang Medical College, Nanyang 473000, Henan, China

Correspondence should be addressed to Xing Zhang; 20130939@stu.nun.edu.cn

Received 22 July 2021; Accepted 12 October 2021; Published 20 December 2021

Academic Editor: Zhendong Mu

With the development of network and multimedia technology, multimedia communication has attracted the attention of researchers. Image encryption has become an urgent need for secure multimedia communication. Compared with the traditional encryption system, encryption algorithms based on chaos are easier to implement, which makes them more suitable for large-scale data encryption. The calculation method of image encryption proposed in this paper is a combination of high-dimensional chaotic systems. This algorithm is mainly used for graph mapping and used the Lorenz system to expand and replace them one by one. Studies have shown that this calculation method causes mixed pixel values, good diffusion performance, and strong key performance with strong resistance. The pixel of the encrypted picture is distributed relatively random, and the characteristics of similar loudness are not relevant. It is proved through experiments that the above calculation methods have strong safety performance.

1. Introduction

With the development of science and technology and Internet technology, network digital communication has become more and more frequent, the security of digital image storage and transmission has become more and more important, and multimedia digital products have also been widely used in all walks of life. For multimedia information, especially image and sound information, the traditional encryption technology encrypts it as an ordinary data stream, regardless of the characteristics of the multimedia data, so it has certain limitations. In order to improve its security, high-dimensional chaotic algorithms are widely used in the field of image encryption. High-dimensional chaotic algorithms have gradually become a research hotspot due to their large key space and high security. At present, the more widely used high-dimensional chaotic algorithms include Lorenz and Rossler and Chua system. In order to ensure that the dissemination and use of multimedia data information gradually expose many security problems, digital pictures are characterized by large data and high correlation between data. The traditional encryption method used for multimedia encryption in the past has the disadvantage of low efficiency [1]. The development of a new type of the chaotic system, which enables multimedia image encryption with high efficiency and high security performance, is a research boom in recent years. The high-dimensional chaotic algorithm is a new image encryption analysis algorithm that has gradually emerged in recent years [2]. This algorithm can be used for the processing and analysis of multimedia image data encryption. Multiple encryption operations are performed on the image with the same algorithm or under different conditions, and the appropriate method is selected to encrypt and optimize the data to obtain the best result. There are many types of multimedia image data encryption. Due to the high dimensions, multimedia image encryption leads to unsatisfactory results. The multigranularity algorithm of multimedia image data should not be applied to the fusion of high-order data clusters because multimedia image data cannot be encrypted to the hypotenuse boundary [3]. In literature [4], a weighted encryption algorithm for multimedia image data encryption is proposed. There is a big error in the encryption result. In literature [5], due to the

dispersiveness of the algorithm in the use process, a multimedia image data encryption analysis based on a priori information is proposed.

With regard to multimedia, especially image and sound information, the previous encryption technology used to encrypt normal data does not show the characteristics of multimedia data and has limitations. In recent years, many researchers have suggested an image scrambling encryption algorithm for chaotic systems. The previous multimedia image encryption calculation methods cannot solve the problem of key space. The structure of the unified high-dimensional chaotic system is simple, and it has the advantage of shorter time sequence, but the key capacity is smaller, and the resistance to exhaustive attack is weak. Therefore, it is necessary to study the encryption calculation method of multimedia pictures on high-dimensional chaotic systems or even super-dimensional chaotic systems. It adopts the advantages of generalized mapping, Lorenz high-dimensional chaotic system, large output, and large key space. The multimedia image encryption method of high-order chaotic computing is studied in this paper. It has strong resistance to exhaustive supply and system analysis attacks, with high computational efficiency and high security performance.

2. Two-Dimensional Generalized Mapping and Image Scrambling

Generalizing the mapping, the following generalized mapping formula is obtained:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \mathrm{mod} N. \tag{1}$$

From formula (1), there is a fixed point (0, 0) in this mapping. That is to say, the point (0, 0) will not change after n repeated mappings. The value of the coordinate point is changed to {1, 2, N} to avoid the occurrence of a fixed point... {1,...2,..., N}, and the mapping equation is converted to a format containing two independent parameters:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix}^n \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \mathrm{mod} N + 1. \tag{2}$$

In formula (2), after n times of repeated operations of the pattern N from the initial value point (x_0, y_0), the result is expressed as 1 as the transformed coordinate (x_n, y_n).

As for multimedia image encryption analysis, the diversity and accuracy are used for definition, to comprehensively evaluate for completing the multimedia image encryption selectivity. During the multimedia image encryption analysis, the multimedia image encryption composition is formed by the particle swarm in the search space, and the characteristic vector χ_i of corresponding multimedia image encryption data is expressed as follows:

$$l_\varepsilon(g) = (1-\rho) l_\varepsilon(g-1) + \gamma f(\chi_i(g)). \tag{3}$$

In the above expression, f represents the corresponding adaptive function of the feature vector χ_i of the multimedia image encryption feature data and $\gamma\chi_i(g)$ represents the multimedia image encryption analysis corresponding to the ε-th encryption in the actual application process.

The expression of encryption π_p in multimedia image encryption II is as follows:

$$\mathrm{Acu}(\pi_p) = \mathrm{NMI}(\pi_p, \pi^*). \tag{4}$$

In formula (4),π_p and π_q represent the encryption of multimedia image encryption. If there is less information shared with the multimedia image encryption basic cluster, the accuracy of the basic cluster is low; otherwise, vice versa.

Based on the accuracy and diversity characteristics clusters based on multimedia image encryption, the comprehensive evaluation criteria for defining clusters based on multimedia image encryption include the following:

$$\mathrm{Eval}(\pi_p) = \lambda \mathrm{Acu}(\pi_p) + (1-\lambda)\mathrm{Div}(\pi_p). \tag{5}$$

In the formula $\lambda \in [0, 1]$, the correctness of multimedia image encryption is an important dimension in the evaluation standard.

Formula (6) is based on the diversity $\mathrm{Div}(\pi_p)$ of multimedia image encryption basic encryption and calculates the probability of selecting each multimedia image encryption basic encryption algorithm as the optimized basic encryption $\mathrm{pro}(\pi_p)$. The calculation formula is as follows:

$$\mathrm{pro}(\pi_p) = \frac{\mathrm{Div}(\pi_p)}{\sum_{p=1}^{B} \mathrm{Div}(\pi_p)}. \tag{6}$$

The calculation result is used to randomly select multimedia image encryption based on roulette and obtain multimedia image encryption analysis.

3. Three-Dimensional Unified Chaotic System and Image Replacement

Scramble is to rearrange the pixel positions of the image and only change the correlation between adjacent pixels of each basic color image instead of the histogram of each basic color image [6–8]. Alternatively, by transforming the pixel value of each basic color image, the histogram distribution characteristics of the entire basic color image can be changed. Therefore, if the pixel value is replaced and converted after scrambling, better encryption security can be obtained.

A new three-dimensional chaotic system is put forward in this paper, which connects the Lorenz system and the Chen system, but the Liu system is only a special example of it, and it is called a unified chaotic system.

$$\begin{cases} \dfrac{dx}{dt} = (25\alpha + 10)(y - x), \\ \dfrac{dy}{dt} = (28 - 35\alpha)x - xz + (29\alpha - 1)y, \\ \dfrac{dz}{dt} = xy - \dfrac{(8+\alpha)z}{3}. \end{cases} \tag{7}$$

In the formula, the system united by the system parameter $\alpha \in [0, 1]$ within this range has the entire chaotic characteristics. In this paper, the chaotic sequence generated by the unified chaotic system equation (7) is used to construct the key of image pixel substitution transformation. Here, the x, y, and z sequences of the unified chaotic system are used to replace and encrypt the pixels of the three primary colors point by point. For each pixel, use a certain 3 digits after the decimal point in a chaotic real number sequence value to construct the key (here, we take the 3 digits 5, 6, and 7 after the decimal point to construct the key). Assuming that the image size is $N \times N$, the subsequences of length $N \times N$ from the generated 3 chaotic sequences are used to construct the key. For any point (i, j) of a primary color image after scrambling (the pixel value is represented as $A_1(i, j, k)$, where $k = 1,2,3$ corresponds to the red, green, and blue primary colors, respectively), select the K value in the X and Y variables or the sequence value in the Z variable as the encryption key of the data. Suppose the current real-valued chaotic sequence value selected from the chaotic sequence is r, then the 3 digits 5, 6, and 7 after the decimal point of r form a positive integer Intky. After the positive integer is modulo 256, 1 word will be obtained. Then, the 1-byte unsigned integer is used as the encryption key of the pixel; the encryption adopts a binary exclusive OR operation between the key and the pixel value.

The purpose of the image restoration network module is to ensure that the color and spatial position of each reconstructed pixel can restore the original color and texture of the image to the greatest extent. The total loss function Linp of the image restoration network module is defined as shown in equation (8), consisted of the repair loss of the unmasked area, the repair loss of the masked area, the perception loss, the style loss, the confrontation loss, and the total variation loss:

$$L_{\text{total}}^{\text{inp}} = 2L_{\text{valid}} + 12L_{\text{hole}} + 0.04L_{\text{per}} + 100\left(L_{\text{style}}^{1} + L_{\text{style}}^{2}\right) + 100L_{\text{adv}} + 0.3L_{\text{var}}. \tag{8}$$

The weight of each loss item is determined after analyzing the results of 50 independent experiments.

The definition of the repair loss in the unmasked area is shown in equation (9), using the Manhattan distance between the repaired image and the unmasked area of the real image as the repair loss, where Idam represents the damaged image, M represents the irregular binary mask (the corresponding area to be repaired in the mask is 0, and the others are 1), Iinp represents the repair result image, and Ireal represents the real undamaged image [9–11]. The repair loss function of the masked area is shown in equation (6):

$$L_{\text{valid}} = \left\| M \times \left(I_{\text{inp}} - I_{\text{dam}}\right) \right\|_1, \tag{9}$$

$$L_{\text{hole}} = \left\| (1 - M) \times \left(I_{\text{inp}} - I_{\text{dam}}\right) \right\|_1. \tag{10}$$

In this paper, different convolutional feature layers of multiple pretrained networks are used to obtain the feature perception loss between the repaired result image and the real image, and the perception loss of the area to be repaired is enhanced. In formula (11), Icom represents the realistic image in the nonmissing area plus the predicted image of the missing area, as shown in equation (11), m represents the number of pretraining networks used, n represents the number of convolutional feature layers used, Ψ_j^i means the j-th layer convolution feature of i-th pretraining network, and ω_i is the weight of the perception loss of the i-th pretraining network. In this paper, after 50 independent experiment comparisons, we use the output characteristic graph of vgg16's pool1, pool2, and pool3 layers and density net's conv1, pool2, and pool3 layers as the perception layer of the generated network, which is used to calculate the perception loss. The parameters of the pretraining network are not involved in the training but only used to calculate the loss value. The weighted sum of the perception losses obtained by the two pretraining networks is used as the final perception loss.

The weight setting used in the experiment in this paper is shown in equation (12).

$$L_{\text{per}}^{*} = \sum_{i=0}^{m-1} \omega_i \left(\sum_{j=0}^{n-1} \left\| \psi_j^i\left(I_{\text{inp}}\right) - \psi_j^i\left(I_{\text{real}}\right) \right\|_1 + \sum_{j=0}^{n-1} \left\| \psi_j^i\left(I_{\text{com}}\right) - \psi_j^i\left(I_{\text{real}}\right) \right\|_1 \right), \tag{11}$$

$$I_{\text{com}} = M \times I_{\text{real}} + (1 - M) \times I_{\text{inp}}, \tag{12}$$

$$L_{\text{per}} = L_{\text{per}}^{\text{VGG-16}} + 30L_{\text{per}}^{\text{DenseNet}}. \tag{13}$$

4. Image Pixel Value Replacement Transformation of Lorenz System

The Lorenz system is a classic three-dimensional chaotic system and has three advantages to generate the encrypted chaotic sequence in the Lorenz system [12–14]. The encrypted chaotic sequence can process the real chaotic sequence output by the system and generate a combination of univariate or multivariate, and the encrypted sequence can be designed very flexibly. The three initial values and three parameters of the three systems can be used as seed keys to generate encrypted chaotic sequences, and when some control variables are added during design, the key space of the encryption algorithm is much higher than that of the low-dimensional chaotic system. The dynamic equation of the Lorenz system is as follows:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y - x), \\ \frac{dy}{dt} &= rx - zx - y, \\ \frac{dz}{dt} &= xy - bz. \end{aligned} \tag{14}$$

After a few days, σ, r, and b are system parameters, and the typical values are $b = 11$, $r = 30$, and $b = 9/4$. Keeping σ unchanged, the Lorenz system enters a chaotic state.

Definition 1. Set $k(\mu)$ in a one-dimensional arrangement $\mu = 1, 2, \ldots, M{\times}N$, where $M{\times}N$ is the image size:

$$k(\mu) = (x, y, z), \tag{15}$$

where x is the transformed address of the pixel of the image, y is the converted address of the pixel range of the image, z is the converted address of the pixel bit block of the image given as follows:

$$\begin{cases} x = \mathrm{mod}(w + i, N) + 1, \\ y = \mathrm{mod}(q + i, N) + 1, \\ z = \mathrm{mod}\left(r + i, M \times \dfrac{N}{8}\right) + 1. \end{cases} \tag{16}$$

As can be seen from Formula 16, A is set as an image with a size of $M{\times}N$ and B is the image obtained after A is encrypted by the original algorithm, denoted as follows:

$$B = F(k(\mu), A); i = 1, 2, \cdots, M \times N. \tag{17}$$

As can be seen from Formula 18, $I_A(i, j)$ and $I_B(i, j)$ are set as the pixel value of each point of image A and B, where $i = 1, 2, \ldots, \mathrm{M}$ and $j = 1, 2, \ldots, N$. Then,

$$I_B(i, j) = F(k(\mu), I_A(i, j)); \mu = 1, 2, \cdots, M \times N. \tag{18}$$

The first and second steps in Formula (16) shall be performed when encrypting in case of the equivalent encryption algorithm.

In Step 3, 285 pixels are selected × 285 images for encryption process research samples. The following conversion is started.

(1) Transform in the direction of the x1 axis. If $\mathrm{b1}(i) = 1$, then let $\mathrm{i'} = \mathrm{mod}(q + i, N){+}1$; if $b_1(i') = 1$, let $i\text{“} = \mathrm{mod}(q + i, \mathrm{N}) + 1$, ...until $b_1(i^n) = 0$, mark $x(i^n) = i^n$.

(2) Transform in the direction of the x2 axis. If $\mathrm{b2}(i) = 1$, then set $j = \mathrm{mod}(q + j, N){+}1$; if $b_2(j') = 1$, then set $j\text{“} = \mathrm{mod}(q + j, \mathrm{N}) + 1$, ...until $b_2(j^n) = 0$, mark $y(j^n) = j^n$.

(3) Transform in the direction of the x3 axis. If $\mathrm{b3}(i) = 1$, set $\mathrm{u'} = \mathrm{mod}(r + i, M{\times}N/8){+}1$; if $b_3(u') = 1$, set $u\text{“} = \mathrm{mod}(r + i, M{\times}N/8){+}1$, ...until $b_3(u^n) = 0$, mark $z(u^n) = u^n$.

According to formula (4), $x(i)$, $y(j)$, and $z(u)$ are recorded into kg, and the position displacement series is obtained.

The encryption map can be obtained from Step 4 formulas (5) and (6).

Experiments have proved that the encryption result of this algorithm is the same as that of high-dimensional chaotic multimedia image encryption.

The image before and after encryption is used as a known condition to solve the above multimedia image encryption algorithm. Assuming that the image A is already known, after encrypting it according to the algorithm description, the encryption drawing B is obtained and processed.

Based on the center offset distribution characteristics of the encrypted image of the actual world image sequence, the tracking range of the feature is limited, and the search window with the size of the center area of the current frame set to $M{\times}M$ is the tracking range. When each feature is displayed with $r(i,j)$, the encrypted feature matrix formed is expressed as follows:

$$R_{\mathrm{Matrix}} = \begin{bmatrix} r(0,0) & \cdots & r(0, M-1) \\ \vdots & & \vdots \\ r(M-1, 0) & \cdots & r(M-1, M-1) \end{bmatrix}. \tag{19}$$

The purpose of cryptographic analysis is to find the location of certain features of the current frame that meet the following criteria (least absolute error) (i, j):

$$d = \min_{i,j} |r - r(i, j)|, \tag{20}$$

where r is the encrypted feature generated in the reference frame and $r(i, j)$ is the encrypted feature generated in the current frame. The features of the reference frame are compared with the features of the current frame for calculation, and the absolute difference sum matrix of the MXM size is formed.

$$S_{\mathrm{MAD}} = |r(i, j)| = \sum_{n=0}^{N} |P[i, j, n] - P[n]|. \tag{21}$$

The feature $r(i, j)$ that minimizes the high-dimensional chaotic algorithm is the required feature, and then the coordinate difference of the two features of r and $r(i, j)$ is calculated to get the best encrypted image required. According to the feature filtering criteria, each time the high-dimensional chaos algorithm subtracted from the elements of the two feature arrays is calculated; it will be judged whether it is greater than the current min value. If it is greater, computing the high-dimensional chaotic algorithm shall be stopped immediately. Then, this feature is excluded. If it is less, the high-dimensional chaotic algorithm shall be calculated continuously.

If the high-dimensional chaos algorithm is greater than the current min when the sixth array element is calculated, $r(i, j)$ will be immediately excluded; otherwise, it will proceed. Generally speaking, when generating the feature matrix in the current frame, each element of the matrix is calculated according to the steps of generating the feature in the reference frame, but this is a large amount of calculation. Research has shown that there is a connection between the row spacing elements in each column of the matrix, and most of the data are the same [15]. For example, since the arrangement element corresponding to the third feature of a column and the first feature is different only in the last one, when the third feature is calculated, most of the element arrangements of the first feature can be used to calculate only the last arrangement element $p[x]$.

5. Experimental Results and Analysis

In this section, a Lena image with a size of 285 pixels is used as the encryption object image to verify the effectiveness of the algorithm. In the context of Matlab 7.1, the Lena image is encrypted according to the high-order chaotic multimedia image encryption algorithm, and the plaintext image and the ciphertext image are shown in Figure 1.

(a) (b) (c) (d)

Figure 1: Encryption effect diagram: (a) original image; (b) encryption image; (c) correctly decrypted image; (d) decrypted image with error 10^{-15}.

According to the solution algorithm introduced here, digital matrix A with the size of 285×285 is filled in the rows after the first column in the matrix in the order of 12 and 66849. Due to space limitations, the 7-column matrix block of the first 7 rows is shown as follows:

$$\begin{bmatrix} 1 & 257 & 513 & 769 & 1025 & 1281 & 1537 \\ 2 & 258 & 514 & 770 & 1026 & 1282 & 1538 \\ 3 & 259 & 515 & 771 & 1027 & 1283 & 1539 \\ 4 & 260 & 516 & 772 & 1028 & 1284 & 1540 \\ 5 & 261 & 517 & 773 & 1029 & 1285 & 1541 \\ 6 & 262 & 518 & 774 & 1030 & 1286 & 1542 \\ 7 & 263 & 519 & 775 & 1031 & 1287 & 1543 \end{bmatrix}. \quad (22)$$

The matrix is encrypted according to the high-dimensional chaotic multimedia image encryption algorithm, to obtain the encryption matrix E and record the corresponding position replacement sequence, and finally the part k (μ) is obtained as follows. This matrix is the equivalent key stream of the high-order chaotic multimedia image encryption algorithm. It converts the Lena image and the encrypted image to the initial state, with the main frequency of 1.95 GHz and the memory of 1 GB Windows Vista platform, and the calculation time of the algorithm of 245 s.

The initial values of the mapped chaotic system are as follows. $[(x_0, y_0) = [0, 1]$ two sequences with a length of 34000 are generated, and the two sequences obtained from the first 2485 points are deleted. $\{x(i), y(i), i = 1, 2, 32697\}$ are used to scramble and encrypt the pixel position of the image. The parameters of the Lorenz system are taken. $\sigma = 11$, $r = 30$, $b = 9/4$, initial value $x0 = 1.1838$, $y0 = 1.3558$, and $z0 = 1.22493$; 0.001 is taken as integration step, and the experimental results obtained are as follows.

According to Figure 1(b), the decoded image is all hidden, and the original face of the image is not known. The correctly decoded image (c) is exactly the same as the original image. The original image cannot be decoded when the initial error is 11.5–14.5. It is found that the encryption effect of the algorithm is good, and the initial value is strongly sensitive.

5.1. Histogram Analysis. As shown in Figure 2, the distribution of pixel values before encryption is not uniform, and the pixels after encryption are evenly distributed in the interval of [02, 55]. It can be seen that this algorithm has strong resistance to statistical analysis attacks.

5.2. Correlation Analysis. In order to confirm the correlation between the adjacent pixels of the plaintext image and the encrypted image, the adjacent pixel pairs in the horizontal direction, all the adjacent pixel pairs in the vertical direction, and the adjacent pixels in the partial diagonal direction are randomly selected from the image, and the correlation coefficient of adjacent pixels is quantitatively calculated by the following formula:

$$\begin{aligned} E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i, \\ D(x) &= \frac{1}{N}\sum_{i=1}^{N} \left[x_i - E(x)\right]^2, \\ \mathrm{Conv}(x, y) &= \frac{1}{N}\sum_{i=1}^{N} \left[x_i - E(x)\right]\left[y_i - E(y)\right], \\ \gamma_{xy} &= \frac{\mathrm{Conv}(x, y)}{y\sqrt{D(x)}\sqrt{D(y)}}. \end{aligned} \quad (23)$$

Here, y represents the pixel values of two adjacent pixels in the image and is quiet as a correlation coefficient of two adjacent pixels in the image. Table 1 shows the dependency numbers in the horizontal, vertical, and diagonal directions. Figure 3 shows the correlation between plaintext and plaintext adjacent pixels in the horizontal direction. It can be seen from the result that the neighboring pixels of the original plaintext image are highly correlated, and the correlation coefficient is close to 1. The correlation coefficient of the adjacent pixels of the encrypted image is close to 0, and the adjacent pixels are basically irrelevant, indicating that the statistical characteristics of the plaintext have been diffused into the random ciphertext, which can effectively resist statistical attacks.

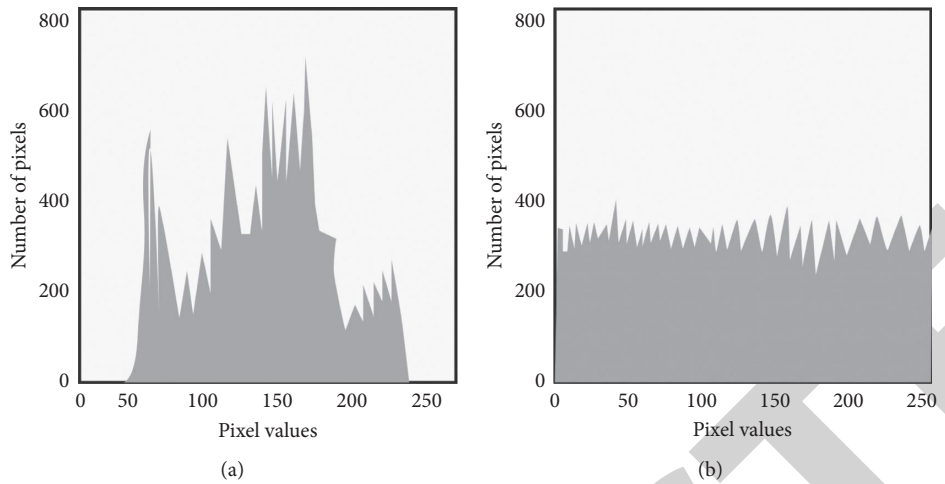

Figure 2: Histogram before and after encryption: (a) original image histogram; (b) image histogram after encryption.

Table 1: Correlation between adjacent pixels of plaintext and ciphertext.

Direction	Plaintext	Ciphertext
Horizontal	0.9655	–0.0051
Vertical	0.9664	–0.0026
Diagonal	0.9153	–0.0027

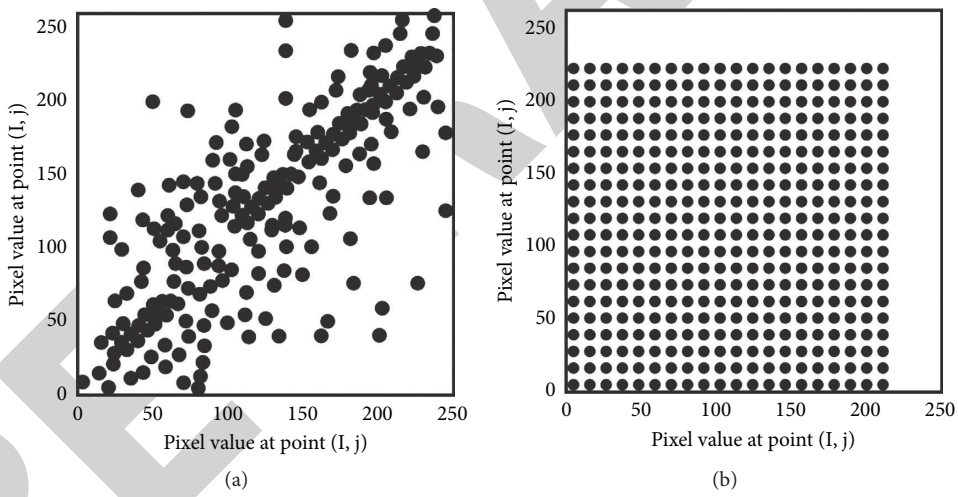

Figure 3: Correlation analysis before and after encryption: (a) original image correlation; (b) image correlation after encryption.

Table 2: Encryption and decryption schedule.

Image size (pixel)	Enciphering time (s)	Deciphering time (s)
136×136	0.121	0.121
285×285	0.212	0.211
512×512	1.082	1.083

5.3. Execution Efficiency Analysis. The Matlab 7.0, Intel Core 2 Duo E4600 CPU is adopted for algorithm if the algorithm is implemented on the 2.5 G memory, Windows XP operating system platform; the time it takes is shown in Table 2.

The defects of the new multimedia image encryption algorithm are mainly manifested in the following two aspects. (1) The pixel position of the image is only transformed, and the pixel value is not processed by any means. Therefore, the histogram of the image before and after encryption will not change. (2) Since the generated chaotic sequence is quantized as a binary chaotic sequence, that is, the key stream, the key stream has nothing to do with the

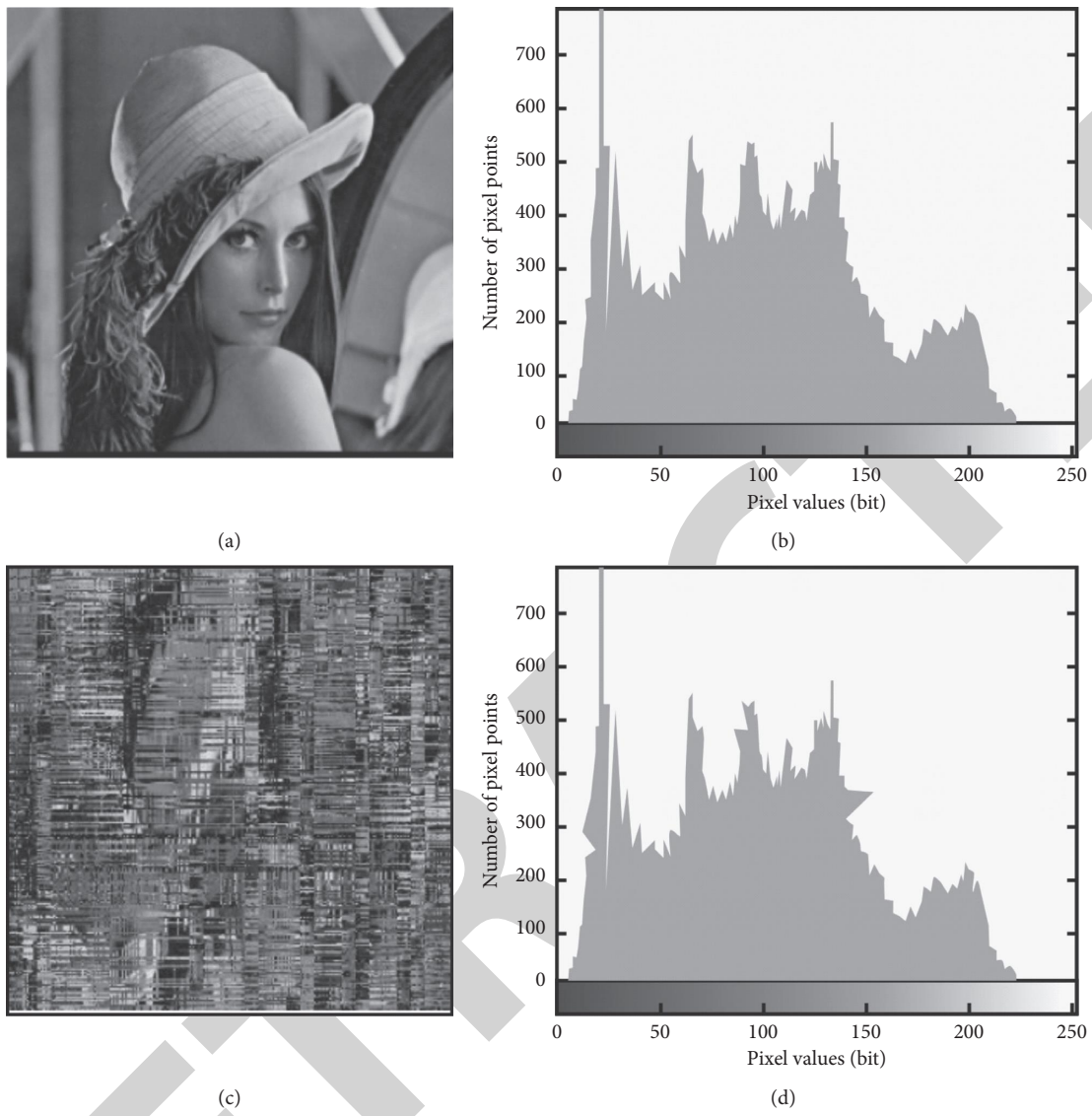

Figure 4: Comparison of histograms before and after encryption: (a) original image; (b) original image histogram; (c) encrypted image; (d) encrypted image histogram.

plaintext symbol during the execution of the algorithm. If the initial conditions do not change, the corresponding key stream will not change either, so the algorithm cannot resist known plaintext attacks well. The size of this article is 285×285, and the standard Lena image is set as an example. Figure 4 shows the histogram before and after SZC encryption.

6. Conclusions

By unifying the characteristics of the chaotic system and the generalized mapping, a calculation method for the high-dimensional nonlinear chaotic system to complete the pixel scramble and replacement encryption of multimedia pictures is researched. The three basic color components of multimedia images can be disarranged. Meanwhile, the adjacent pixels are not related, and the three elements of *R*, G, and B of each pixel are confused meanwhile, and the color change of the encrypted image achieves a higher security performance. The ciphertext is evenly distributed in space, and there is no relevance between adjacent pixels. Experimental analysis can prove that the safety performance of this method is high.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that there are no conflicts of interest.

References

[1] Y. Li, B. Song, R. Cao, Y. Zhang, and H. Qin, "Image encryption based on compressive sensing and scrambled index for secure multimedia transmission," *ACM Transactions on*

Multimedia Computing, Communications, and Applications, vol. 12, no. 4s, pp. 1–22, 2016.

[2] M. Jia, "Image encryption based on high-dimensional manifold computing and block dividing algorithm," *International Journal of Optics*, vol. 2020, no. 12, 11 pages, Article ID 8678527, 2020.

[3] Z. R. Kapach, A. Ulmer, D. Merrick, A. Alikhan, Y. H. Lu, and A. Mohan, "Cloud resource optimization for processing multiple streams of visual data," *IEEE Multimedia*, p. 1, 2018.

[4] X. Sun, Z. Shao, Y. Shang, M. Liang, and F. Yang, "Multiple-image encryption based on cascaded gyrator transforms and high-dimensional chaotic system," *Multimedia Tools and Applications*, no. 5, pp. 1–24, 2021.

[5] J.-F. Zhao, S.-Y. Wang, L.-T. Zhang, and X.-Y. Wang, "Image encryption algorithm based on a novel improper fractional-order attractor and a wavelet function map," *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 8672716, 10 pages, 2017.

[6] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2d-licm hyperchaotic map," *Signal Processing*, vol. 143, no. FEB, pp. 122–133, 2017.

[7] J. Zeng and C. Wang, "A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata," *Security and Communication Networks*, vol. 2021, no. 5, 15 pages, Article ID 6675565, 2021.

[8] Y. Naseer, T. Shah, and D. Shah, "A novel hybrid permutation substitution base colored image encryption scheme for multimedia data," *Journal of Information Security and Applications*, vol. 59, no. 4, pp. 554–557, 2021.

[9] G. Krishnan, D. Bouvier, and S. Naffziger, "Energy-efficient graphics and multimedia in 28-nm carrizo accelerated processing unit," *IEEE Micro*, vol. 36, no. 2, pp. 22–33, 2016.

[10] Z. H. Gan, X. L. Chai, D. J. Han, and Y. R. Chen, "A chaotic image encryption algorithm based on 3-d bit-plane permutation," *Neural Computing and Applications*, pp. 1–20, 2018.

[11] M. Li, H. Fan, Y. Xiang, Y. Li, and Y. Zhang, "Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system," *IEEE multimedia*, vol. 79, no. 2, pp. 1141–1149, 2018.

[12] J. Ferdush, M. Begum, and M. S. Uddin, "Chaotic lightweight cryptosystem for image encryption," *Advances in Multimedia*, vol. 2021, Article ID 5527295, 16 pages, 2021.

[13] S. Halagowda, S. K. Lakshminarayana, and S. Lakshminarayana, "Image encryption method based on hybrid fractal-chaos algorithm," *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 6, pp. 221–229, 2017.

[14] K. Ma, L. Teng, X. Wang, and J. Meng, "Color image encryption scheme based on the combination of the fisher-yates scrambling algorithm and chaos theory," *Multimedia Tools and Applications*, pp. 1–21, 2021.

[15] Y. Wan, S. Gu, and B. Du, "A new image encryption algorithm based on composite chaos and hyperchaos combined with dna coding," *Entropy*, vol. 22, no. 2, pp. 171–180, 2020.