Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding

Qiuyu Zhang | Jitian Han | Yutong Ye

School of Computer and communication, Lanzhou University of Technology, Gansu, Lanzhou 730050, People’s Republic of China

Correspondence
Qiuyu Zhang, School of Computer and communication, Lanzhou University of Technology, Gansu, Lanzhou 730050, People’s Republic of China. Email: zhangqylz@163.com

Abstract
Problems such as large data volumes, slow transmission rates and low security often occur when transmitting multiple digital images over the internet. In order to protect the content security of multiple images and improve the speed of internet transmission, a multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding is proposed in this study. First, the proposed algorithm merges several grey images and image hashing algorithm is used to generate the initial key for chaotic mapping. Second, the random sequence generated by the improved three-dimensional chaotic map is used to decompose the bit plane of the merged image and the bit-plane matrix is substituted numerically. Finally, the random sequence generated by the four-dimensional hyperchaotic system is used to perform dynamic DNA coding and calculation on the image and the final multiple ciphertext images are generated by decomposition of the pixel matrix. The experimental results show that the proposed algorithm has large key space, strong key sensitivity, strong security and robustness, and can resist various conventional attacks such as statistical analysis, differential attack, exhaustive attack, cropping and noise attack.

1 | INTRODUCTION
Digital images in the internet environment carry a lot of private information and play an irreplaceable role in many fields (such as military detection, natural disaster monitoring, medical and health, traffic monitoring, e-government and personal affairs) [1–3]. However, image data is often seriously threatened in public network transmission. In order to ensure the security of private data transmission, scholars have proposed many encryption algorithms for a single image. With the continuous increase in the amount of data on the internet and the advent of the era of big data, and in order to increase the speed of transmission on the internet and protect the content security of multiple images, multi-image data encryption has received extensive attention from many scholars and different application areas [4, 5].

Multi-image encryption (MIE) is a new multimedia security and privacy protection technology. Traditional encryption algorithms such as the data encryption standard, advanced encryption standard, Rivest–Shamir–Adleman) are no longer suitable for the hidden transmission of existing images. Chaotic systems are widely used in MIE because of their excellent characteristics such as strong sensitivity and high pseudo-randomness [6–11].

Zhang et al. [6] proposed an MIE algorithm based on piecewise linear chaotic map that has a small key space and needs to be improved to resist brute-force attacks. Zarebina et al. [7] proposed an MIE algorithm combining chaotic system, operation of xor (XOR) operation and cyclic shift. Yu et al. [8] proposed a four-image encryption scheme based on quaternion Fresnel transform, computer hologram and two-dimensional logistic-adjusted-sine map. The pixel correlation of ciphertext images of this algorithm needs to be improved to resist statistical attacks. Kumar et al. [10] proposed an asymmetric double-image encryption algorithm combining two-dimensional non-separable linear canonical transform and iterative phase retrieval algorithm. Bisht et al. [11] proposed an MIE algorithm based on chaotic system and bit plane, but the information entropy of the algorithm was low and it was difficult to resist the information entropy attack. As a new biological technology, DNA has become the object of concern of many researchers and many DNA-based MIE algorithms have been proposed [12–14]. Nematzadeh et al. [12] proposed a symmetric MIE method based on DNA and binary search tree that has low key...
space and needs to be improved to resist exhaustive attacks. Enayatifar et al. [13] proposed an MIE algorithm based on DNA coding and cellular automata technology. Zhang et al. [14] proposed an MIE algorithm based on DNA coding and chaotic system. The pixel replacement and diffusion were performed on a three-dimensional (3D) DNA matrix. In addition, many image encryption algorithms based on frequency domain transformation [15–17], cellular automata [18], optical technology [19–21] and compressed sensing [22, 23] have been proposed.

From what has been discussed above, the existing MIE algorithms often have the defects of large data volume, slow transmission efficiency and vulnerability to various conventional attacks. Therefore, a new MIE algorithm based on chaos mapping, image hashing, bit-plane decomposition and dynamic DNA coding is proposed in this study. The main contribution of this study is listed as follows: (i) Image hashing technology is used to strengthen the connection between the initial key and plaintext image that can effectively resist plaintext statistical attacks; (ii) the improved 3D chaotic mapping and four-dimensional (4D) hyperchaotic system not only make the chaotic sequence more random but also increase the key space; (iii) using a combination of bit-plane decomposition and chaotic sequences that makes multiple images more chaotic and combines pixel displacement and diffusion; (iv) the dynamic DNA encryption algorithm is designed to further enhance the image diffusion and improve the robustness of the MIE algorithm.

The rest of the paper is organised as follows. Section 2 describes the theoretical principle. Section 3 presents the proposed encryption and decryption scheme and its phases. Section 4 provides detailed simulation results and security analysis of the proposed algorithm. Finally, we conclude our study in Section 5.

## 2 RELATED THEORETICAL PRINCIPLE

### 2.1 Improved 3D chaotic mapping

As a deterministic non-linear system, chaos is widely used in image encryption because of its strong pseudo-randomicity and ergodicity. The mathematical expression of the improved 3D chaotic map is as follows:

\[
\begin{align*}
    x_{n+1} &= \text{mod}(a \times x_n \times (1 - y_n) - (4 - b \sin(\pi \times z_n) \times (2^{12} - 1)), 1) \\
    y_{n+1} &= \text{mod}(a \times y_n \times (1 - z_n) - (4 - b \sin(\pi \times x_n) \times (2^{12} - 1)), 1) \\
    z_{n+1} &= \text{mod}(a \times z_n \times (1 - x_n) - (4 - b \sin(\pi \times y_n) \times (2^{12} - 1)), 1)
\end{align*}
\]

where \(a\) and \(b\) are system parameters and \(x_0, y_0, z_0 \in (0, 1)\) are initial parameters.

Figure 1 shows the bifurcation diagram and Lyapunov exponential (LE) diagram of the improved 3D chaotic map. As shown in Figure 1, the improved 3D chaotic map has obvious chaotic characteristics and stronger pseudo-randomicity.

### 2.2 Four-dimensional hyperchaotic system

The expression definition of the 4D hyperchaotic system [24] is as follows:

\[
\begin{align*}
    \dot{x} &= a(x - y) - yz + w \\
    \dot{y} &= xy - by + w \\
    \dot{z} &= xy - cz \\
    \dot{w} &= -x
\end{align*}
\]

where \(x, y, z, w\) are state variables, \(a, b, c\) are system parameters.

Figure 2 shows the bifurcation diagram and LE diagram of the 4D hyperchaotic map. Through a large number of experimental tests, the Lyapunov index of the 4D hyperchaotic system reaching the chaotic state are \(L_1 = 2.2703\), \(L_2 = 0.0794\), \(L_3 = 0\), \(L_4 = -34.5747\) when system parameters \(a = 7\), \(b = 30\), \(c = 10\).

As shown in Figure 2, the 4D hyperchaotic system has high system unpredictability and randomness that is more suitable for image encryption.

### 2.3 Bit-plane decomposition

As an important attribute of digital image, bit plane is widely used in the image encryption algorithm, image information hiding and image recognition [11]. The binary pixel values at the same bit position in the grey image are combined to obtain a binary value image that is called a bit plane of the grey image and the process is called bit-plane decomposition. Figure 3 shows the schematic diagram of bit-plane decomposition of the Lena image.

As shown in Figure 3, the feature information of the image gradually decreases with the decrease of the position. The feature information contained in the high 4 bits accounts for more than 94% of the original image, which has the greatest impact on the quality of the image.

### 2.4 DNA coding rules and operations

The DNA sequence has four nucleic acid bases: Adenine (A), cytosine (C), guanine (G) and thymine (T) in which A, T and G
FIGURE 1  The bifurcation and Lyapunov exponential (LE) diagram of improved three-dimensional (3D) chaotic map (a) x-y-z bifurcation diagram, (b) LE diagram

FIGURE 2  The bifurcation and LE diagram of four-dimensional (4D) hyperchaotic map (a) x-y bifurcation diagram, (b) y-z bifurcation diagram, (c) x-y-w bifurcation diagram, (d) LE diagram

FIGURE 3  Bit-plane decomposition of the Lena image (a) 1st–4th plane of lower 4 bits, (b) 5th–8th plane of higher 4 bits
and C are complementary, and 0 and 1 in binary are complementary. Thus 00, 01, 10, 11 can be encoded using A, C, G, T. There are 24 encoding rules in this encoding method, but only eight rules comply with the Watson–Crick pairing rules. The encoding method is shown in Table 1.

A certain encoding method is selected to encode the pixel DNA and different DNA decoding operations are used to change the pixel value in this paper. The binary operation rules are used to calculate the encoded pixel DNA, which makes the DNA coding more secure.

3 | PROPOSED ALGORITHM

The encryption scheme mainly combines image hash, bit-plane decomposition and dynamic DNA coding to encrypt several grey images in this study. The encryption steps are mainly divided into three main parts: Key generation, bit-plane decomposition and merger, and dynamic DNA coding. The process flowchart of the MIE algorithm is shown in Figure 4.

3.1 | Key generation

The initial key is mainly generated by the image hash algorithm that can strengthen the relationship between the key and multiple plaintext images and achieve the effect of one secret at a time in this study. The generation steps of the initial key are as follows:

Step 1: Pretreatment. Let the number of multiple images to be encrypted be \( n \). If \( n \) is even, half of it is \( n/2 \). If \( n \) is an odd number, any image is randomly added so that half of it is \( k = (n+1)/2 \). Then, the input of \( n \) grey images with the size of \( M \times N \) and the combination, namely, \( I_1(i, j), I_2(i, j), \ldots, I_{2k}(i, j) \), is done. According to the odd and even number of the image to make the corresponding addition, the combination is divided into \( I_1, I_3, \ldots, I_{2k-1} \) odd combination and \( I_2, I_4, \ldots, I_{2k} \) even combination. The odd combinations are combined into the matrix \( A(i, j) \) and even combinations into the matrix \( B(i, j) \).

Step 2: Hash construction. First, the matrix \( A \) and \( B \) are scaled to transform them into matrices \( A' \) and \( B' \) with sizes of \( M/4 \times k \) and \( N/4 \times k \). Then, the pixel matrix is transformed and multiplied, that is, \( P(i, j) = A'(i, j) \times B'(i, j) \). Finally, the obtained \( P(i, j) \) is subjected to binary hash construction to generate a hash sequence \( p_{bh}(x) \) where the matrix \( P(i, j) \) is matrix converted to \( p(x) \), that is, \( p(x) = P(i, j) \).

The binary hash construction method is as follows:

Subtract the average value from each value in the same combination. The odd combinations are combined into a single pixel DNA, which makes the DNA coding more secure.

The average value of \( p(x) \) is named as \( p'(x) \):

\[
P_{bh}(x) = \begin{cases} 
1 & p(x) > p'(x), \quad i = 1, 2, \ldots, n \\
0 & p(x) \leq p'(x)
\end{cases}
\]

where \( p_{bh}(x) \) is the constructed binary hash sequence.

Step 3: Key generation. The hash sequence is processed by matrix transformation and summation and 16 initial values are obtained finally. Six of them are randomly selected as the initial values and system parameters of the chaotic map. The key generation method is shown in (4).

\[
k(i) = \text{Mean}(\text{reshape}(p_{bh}(x), [k^2 \times MN/16^2, 16]))
\]

where \( \text{reshape}() \) can realise grouping, \( \text{Mean}() \) can realise summation.
3.2 Image encryption algorithm

Step 1: The matrices $A(i,j)$ and $B(i,j)$ are decomposed into bit planes. The 8-bit planes after decomposition are $A_1$, $A_2$, ..., $A_8$ and $B_1$, $B_2$, ..., $B_8$.

Step 2: The initial key is used as the initial values $x_0, y_0, z_0$ of the improved 3D chaotic map and the control parameters $a$ and $b$ are obtained in Equations (5) and (6). The improved 3D chaotic mapping in Section 2.1 was used to generate a 3D random sequence with the length of $10000 \times 8 \times k \times M \times N$. In order to obtain better randomness, the first 1000 terms of the random sequence are removed and the random sequences $X$, $Y$ and $Z$ are obtained finally:

$$a = \frac{\sum_{i=1}^{M \times 2} \sum_{j=1}^{N} A(i,j)}{255 \times M \times 2 \times N}$$

$$b = \frac{\sum_{i=1}^{M \times 2} \sum_{j=1}^{N} B(i,j)}{255 \times M \times 2 \times N}$$

Step 3: Items $8 \times M \times N$ of random sequence $X$ are intercepted and divided into eight parts of the length of $k \times M \times N$, which are $X_1, X_2, ..., X_8$. Subsequently, the 8-bit planes $A_1, A_2, ... , A_8$ are subjected to matrix transformation and the position replacement is performed according to the position relationship corresponding to $P_x(i)$ in order to obtain new replacement matrices $A_1', A_2', ... , A_8'$.

Step 4: Random sequence $Y$ is used to perform matrix transformation on the bit planes $B_1, B_2, ... , B_8$ according to the rules of step 3, and new permutation matrices $B_1', B_2', ... , B_8'$ are obtained finally.

Step 5: Combining the bit planes $A_1', A_2', A_3', A_4', A_5'$ and $B_1', B_2', B_3', B_4', B_5', B_6', B_7', B_8'$, then the ciphertext image $C$ is obtained where $C \leftarrow \text{bitset}(A_1,3,5,6', B_2,4,6,8')$. Combining the bit planes $B_1', B_2', B_3', B_4', B_5', B_6', B_7', B_8'$ and $A_2', A_3', A_4', A_5', A_6'$, then the ciphertext image $D$ is obtained where $D \leftarrow \text{bitset}(A_1,3,5,6', B_2,4,6,8')$.

Step 6: Items $k \times M \times N$ of random sequence $Z$ are selected to perform integer conversion according to Equation (7). Then the sequence is converted into a 2D matrix $E$ with the size of $k \times M$ and $k \times N$:

$$z_i \leftarrow \text{mod}(\text{ceil}(z_i \times 10^3), 256)$$

Step 7: The images $C$ and $D$ encrypted by the bit plane into a matrix $F$ are combined. The matrices $E$ and $F$ are divided into $k \times t$ squares where $t$ is the size of the squares.

Step 8: Equation (2) is used to generate 4D random sequences $\{x'_i\}, \{y'_i\}, \{z'_i\}$ and $\{b'_i\}$. The initial values $x_1$, $y_1$, $z_1$ and $b_1$ are obtained in Section 3.1, which is handled in a manner similar to step 2.

Step 9: The matrices $E$ and $F$ are DNA-encoded according to the chaotic sequences $\{x'_i\}$ and $\{y'_i\}$, respectively, and the random matrix $E'$ and pixel matrix $F'$ are generated finally. The encoding method adopts the DNA encoding rules of Table 1 and the processing method of the random sequence is shown in Equations (8) and (9):

$$x_i \leftarrow \text{mod}(\text{floor}(x_i \times 10^3), 8) + 1$$

$$y_i \leftarrow \text{mod}(\text{floor}(y_i \times 10^3), 8) + 1$$

where $x_i$ and $y_i$ are encoded by DNA from left to right and from top to bottom, respectively.

Step 10: DNA calculation is performed on the random matrix $E$ and the pixel matrix $F$ according to the operation rules of the chaotic sequence $\{z'_i\}$. The calculation rule is shown in Equation (10).

$$z'_i \leftarrow \text{mod}(\text{floor}(z'_i \times 10^3), 3)$$

In Equation (10), random sequence $\{z'_i\}$ produces three values 0, 1 and 2, respectively. When $z'_i = 0$, the encryption calculation is performed; when $z'_i = 1$, the subtraction calculation is performed; when $z'_i = 2$, the XOR calculation is performed.

Step 11: In order to make the diffusion effect more significant, the following operations need to be performed on the evenly divided images: Setting $z'_i = 0$, then

$$m_i = m_{i-1} + E'_i + F'_i$$

Step 12: The random matrix $E$ and pixel matrix $F$ are decoded according to the rules of chaotic sequence $\{b'_i\}$ and the DNA decoding operation is similar to step 9. After the DNA-decoded image in binary format is converted to decimal, the final ciphertext image $Q$ is obtained. Then, the ciphertext image $Q$ is separated as $Q_1(i,j), Q_2(i,j), ..., Q_{2k}(i,j), Q_{2k+1}(i,j), Q_{2k+2}(i,j)$ in which the number of ciphertext images is $2k$. If $n$ is an even number, it means $n = 2k$, and if $n$ is an odd number, it means $n+1 = 2k$.

3.3 Image decryption algorithm

Symmetric encryption and decryption algorithm is used in this study. In the decryption process, the dynamic DNA coding and decoding rules correspond to the DNA decoding and encoding rules in the encryption process, while the dynamic DNA addition and subtraction rules correspond to the DNA subtraction and addition rules in the encryption process. The multi-image decryption algorithm flowchart is shown in Figure 5.

Step 1: System parameters $a, b$ and initial values $x_0, y_0, z_0$ and $x_1, y_1, z_1, b_1$ are used to obtain random sequences $X^+, Y^+, Z^+$ and $\{x'_i\}, \{y'_i\}, \{z'_i\}, \{b'_i\}$ through 3D and 4D chaotic mapping. The system parameters and
initial values are obtained in the same way as the encryption algorithm.

Step 2: Items $k^2 \times M \times N$ of random sequence $Z'$ are selected and integer conversion is carried out. After matrix transformation, a 2D matrix $J$ with the size of $k \times M$ and $k \times N$ is formed.

Step 3: $Q_1, Q_2, \ldots, Q_{k^2}, L$ is inputted and merged into a new ciphertext image $L$. Then, $L$ is divided and the random matrix $J$ are evenly divided into $N \times t$ squares in which $t$ is the size of the squares.

Step 4: Random matrix $J$ and ciphertext image $L$ are encoded by DNA according to chaotic sequences $\{x'_i\}$ and $\{b'_i\}$, respectively. Random matrix $J$ and pixel matrix $L'$ are generated in which the encoding method adopts the DNA coding rules in Table 1, and the processing method of random sequences is shown in Equations (12) and (13):

$$x'_i \leftarrow \text{mod} \left( \text{floor} \left( x'_i \times 10^4 \right), 8 \right) + 1$$  \hspace{1cm} (12)

$$b'_i \leftarrow \text{mod} \left( \text{floor} \left( b'_i \times 10^4 \right), 8 \right) + 1$$  \hspace{1cm} (13)

where $\{x'_i\}$ and $\{b'_i\}$ perform DNA coding in the order from left to right and top to bottom, respectively.

Step 5: The random matrix $J$ and pixel matrix $L'$ are calculated according to the operation rules of chaotic sequence $\{z'_i\}$. The calculation rules are shown in Equation (14):

$$z'_i \leftarrow \text{mod} \left( \text{floor} \left( z'_i \times 10^4 \right), 3 \right)$$  \hspace{1cm} (14)

Random sequences $\{z'_i\}$ produces three values 0, 1 and 2, respectively, in Equation (14). When $z'_i = 0$, subtraction calculation is performed; when $z'_i = 1$, addition calculation is performed; when $z'_i = 2$, XOR calculation is performed.

Step 6: In order to make the diffusion effect more significant, the following operations need to be performed on the evenly divided images: Setting $z'_i = 0$, then

$$m_{i-1}' = m_i' + f_{i-1}' + k_{i-1}'$$  \hspace{1cm} (15)

Step 7: Random matrix $J$ and pixel matrix $L'$ are decoded according to the rules of chaotic sequence $\{y'_i\}$ and DNA decoding operation is similar to step 4. After the DNA decoding image in binary format is converted to decimal, the DNA-decoded image $L''$ is obtained.

Step 8: The DNA-decoded image $L''$ is separated into two-pixel matrices $A^R$ and $B^R$. After the decomposition of the bit plane, there are 8-bit planes $A_1, A_2, \ldots, A_8$ and $B_1, B_2, \ldots, B_8$.

Step 9: $8 \times M \times N$ of random sequence $X'$ are intercepted and divided into eight sequences with the length of $k \times M \times N$, namely, $X_1^R, X_2^R, \ldots, X_8^R$. The random sequence is arranged in ascending order to obtain $X_1^R, X_2^R, \ldots, X_8^R$, and the permutation sequence $P_{x'}(i)$ is formed according to the index relationship of the elements in $X'$ corresponding to $X$. Then, the 8-bit planes $A_1^R, A_2^R, \ldots, A_8^R$ are matrix-transformed in order to perform position transformation according to the position relationship corresponding to $P_{x'}(i)$. The new permutation matrices $A_1, A_2, \ldots, A_8$ are obtained.

Step 10: Using random sequence $Y$ according to the transformation bit plane $B_1, B_2, \ldots, B_8$, a new permutation matrix $B_1, B_2, \ldots, B_8$ is obtained finally.

Step 11: The bit planes $A_1^R, A_2^R, A_8^R$ and $B_1^R, B_2^R, B_6^R, B_8^R$ are merged into decryption Image $C$ where $C \leftarrow \text{bitset}(A_1, A_3, A_5, A_7, B_1, B_3, B_5, B_7)$. The bit planes $B_1^R, B_3^R, B_5^R$ and $A_2^R, A_4^R, A_6^R, A_8^R$ are merged into decryption image $D$ where $D \leftarrow \text{bitset}(B_1, A_3, A_5, A_7, B_1, B_3, B_5, B_7)$.

Step 12: $C$ and $D'$ are separated to obtain $2k$ ciphertext images $I_1, I_2, \ldots, I_{2k-1}, I_{2k}$ where $n$ is an even number, which means that $n = 2k$, and if $n$ is odd numbers, it represents $n+1 = 2k$.

4 | EXPERIMENTAL RESULTS AND ANALYSIS

The experimental hardware environment is Intel(R) Core(TM) i5-230 m CPU @ 2.60ghz, 4G RAM, Win7(64-bit) operating system and the software environment is MATLAB R2016a in this study. Four standard grey images of Lena, peppers, baboon
and aeroplane with the size of 512 × 512 were selected as test images. Figure 6 shows the experimental results of four plaintext images, ciphertext images and decrypted images.

It can be seen from Figure 6 that the encrypted ciphertext image cannot be recognised by the human eye and no original information is leaked. The decrypted image and the plaintext image have the same visual effect.

4.1 Statistical analysis

4.1.1 Histogram analysis

Histogram reflects the pixel value distribution of a grayscale image that defines the frequency of each grayscale distribution in the whole image, and it is an important feature to evaluate the image encryption algorithm [13]. In order to resist statistical analysis effectively, the histogram of ciphertext images should be uniform. Figure 7 is a histogram of the plaintext image and the decrypted image of Lena, peppers, baboon, aeroplane, respectively.

It can be seen from Figure 7, the grey value distribution of the histogram of the plaintext image is uneven and has certain rules. The histogram of the ciphertext image has a uniform distribution of grey value, so the statistical characteristics of grey image cannot be identified successfully. The experimental results show that the distribution law of the pixel value of the plaintext image is successfully hidden and has good diffusion characteristics, which can effectively resist the statistical attack.

4.1.2 Correlation analysis

The plaintext images have a strong correlation in horizontal, vertical and diagonal directions, so a good encryption algorithm must reduce this correlation characteristic of images [7]. Equations (16)–(19) are used to calculate the correlation coefficients of the pixels from the three directions of horizontal, vertical and diagonal directions. Figure 8 shows the result of the correlation calculation of the Lena image:

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i$$  \hspace{1cm} (16)

$$D(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))^2$$  \hspace{1cm} (17)

$$\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))$$  \hspace{1cm} (18)

$$r_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$  \hspace{1cm} (19)

where $x$ and $y$ represent the grey values of two adjacent pixels, $N$ is the total, $E(x)$ and $D(x)$ represent the expectation and variance of variable $x$, $E(y)$ and $D(y)$ represent the expectation and variance of variable $y$, $\text{cov}(x,y)$ and $r_{xy}$ represent the covariance of variable $x$ and $y$. $r_{xy}$ represents the correlation coefficient between two adjacent pixels.

As shown in Figure 8, the distribution of pixels in each direction of the plaintext image of the Lena image is concentrated, which shows a left-right distribution trend according to the linear relationship of $y = x$. However, the distribution of adjacent pixels in the ciphertext image is random and uniform.
Figure 8  Horizontal, vertical, and diagonal correlations of pixel correlation between Lena plaintext and ciphertext images (a) plaintext images, (b) ciphertext images

Table 2  Correlation analysis between plaintext and ciphertext images

| Image          | Direction | Lean   | Peppers | Baboon | Aeroplane | Merge images |
|----------------|-----------|--------|---------|--------|-----------|--------------|
| Plaintext image| Horizontal| 0.97737| 0.98039 | 0.86554| 0.9686    | 0.96848      |
|                | Vertical  | 0.98777| 0.98352 | 0.76481| 0.9643    | 0.9547       |
|                | Diagonal  | 0.96376| 0.9704  | 0.73129| 0.94008   | 0.94136      |
| Ciphertext image| Horizontal| −9.9589×10⁻⁷| 6.7496×10⁻⁷| 6.0838×10⁻⁷| −6.9019×10⁻⁷| −3.4549×10⁻⁷|
|                | Vertical  | 1.3504×10⁻⁶| −8.6322×10⁻⁸| −1.7255×10⁻⁷| −6.7341×10⁻⁷| 1.6199×10⁻⁶  |
|                | Diagonal  | −2.3986×10⁻⁷| −1.2514×10⁻⁶| 6.6758×10⁻⁷| −5.8825×10⁻⁸| −1.6843×10⁻⁷|

Table 2 shows correlation coefficients and comparative analysis results of Lena, peppers, baboon and aeroplane test images.

The higher the correlation coefficient, the stronger the correlation of adjacent pixels. It can be seen from Table 2 that the pixel correlation coefficient of the plaintext image is close to 1 and the pixel correlation of the ciphertext image is almost close to 0.

Table 3 shows the results of the image pixel correlation coefficient comparison between this algorithm and other existing encryption algorithms.

The correlation between adjacent pixels of the algorithm is significantly better than that in the literature [12, 14, 18] and the test value of the correlation coefficient is closer to 0 in Table 3. According to the experimental results, this algorithm effectively reduces the statistical characteristics of pixels that have high-enough security to resist statistical attack analysis.

4.2  Information entropy analysis

Information entropy is an important indicator to reflect the distribution state of pixel grey value. The more uniform distribution of pixel grey values, the greater the information entropy [14]. The grey level of the grey image is 256, so the theoretical value of the information entropy is 8. The calculation formula of information entropy is shown in Equation (20). Table 4 shows the test results of information entropy of different

Table 3  Comparative analysis of pixel correlation in ciphertext image

| Image  | Direction | Proposed        | [12]  | [14]  | [18]  |
|--------|-----------|-----------------|-------|-------|-------|
| Lena   | Horizontal| −9.9589×10⁻⁷    | 0.0017| −0.0019| 0.0063|
|        | Vertical  | 1.3504×10⁻⁶     | 0.0007| −0.0066| 0.0011|
|        | Diagonal  | −2.3986×10⁻⁷    | 0.0008| 0.0031 | −0.0151|
| Peppers| Horizontal| 6.7496×10⁻⁷     | 0.0059| −0.0030| −0.0014|
|        | Vertical  | −8.6322×10⁻⁸    | 0.0029| −0.0019| 0.0202 |
|        | Diagonal  | −1.2514×10⁻⁶    | 0.0018| 0.0016 | −0.0057|
| Baboon | Horizontal| 6.0838×10⁻⁷     | 0.0026| −0.0012| 0.0095 |
|        | Vertical  | −1.7255×10⁻⁷    | 0.0009| −0.0026| −0.0110|
|        | Diagonal  | 6.6758×10⁻⁷     | 0.0006| −0.0001| 0.0005 |
| Aeroplane| Horizontal| −6.9019×10⁻⁷   | 0.0019| −         | −0.0086|
|        | Vertical  | −6.7341×10⁻⁷    | 0.0015| −         | −0.0058|
|        | Diagonal  | −5.8825×10⁻⁸    | 0.0050| −         | −0.0001|
**4.3 Differential attack analysis**

People usually make small transformations to the plaintext image and verify the encryption algorithm’s ability to resist differential attacks when other conditions remain unchanged [6]. Therefore, an excellent encryption algorithm should have the desirable property of spreading the influence of slight change to the plaintext over as much to the ciphertext as possible that proves the algorithm’s excellent resistance to differential attacks. The number pixels change rate (NPCR) and the unified average changing intensity (UACI) are important indexes for evaluating differential attack and their expressions are shown in Equations (21) and (22). Under the condition that other conditions remain unchanged, the random selection of any position of the test image, adding 1 to the pixel value of the position and testing the NPCR and UACI values of the ciphertext image was performed. The experiment was repeated 200 times with different pixel positions and the mean values of NPCR and UACI were obtained. Table 5 is a comparative analysis of the differential attack performance of this algorithm and other existing algorithms:

\[
NPCR = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=0}^{N} \text{Sign}(i, j) \times 100\% \quad (21)
\]

where \( \text{Sign}(x) = \begin{cases} 0 & \text{if } c_1(i, j) = c_2(i, j) \\ 1 & \text{if } c_1(i, j) \neq c_2(i, j) \end{cases} \)

\[
UACI = \frac{1}{M \times N} \sum_{i=0}^{M} \sum_{j=0}^{N} \left| c_1(i, j) - c_2(i, j) \right| \div 255 \times 100\% \quad (22)
\]

where \( M \) and \( N \) represent the length and width of the image, respectively, and \( c_1(i, j) \) and \( c_2(i, j) \) represent the pixel values of the ciphertext image before and after the change of the plaintext.

The theoretical expectations of NPCR and UACI for grayscale images were 255/256 \( \approx 99.6094\% \) and 257/256 \( \approx 99.6058\% \), respectively. According to Table 5, the average values of NPCR and UACI in the test images of the proposed algorithm are 99.60655\% and 33.4630\%, which are closer to the theoretical values than those in the literature [12, 24]. It shows that the proposed algorithm has strong sensitivity and stability to plaintext images, which is enough to resist differential attacks.

**4.4 Exhaustive attack analysis**

**4.4.1 Key-space analysis**

Key space is an important indicator to prove the encryption performance of image encryption algorithm. The larger the key space, the stronger ability to resist exhaustive attacks [18]. According to the basic theory of cryptography, when the key space is less than \( 2^{100} \approx 10^{30} \), the encryption algorithm is not secure. The key of the encryption algorithm is mainly composed of the control parameters and initial values of the improved 3D chaotic map and 4D hyperchaotic map in this study. There are the control parameters \( a, b \) and the initial parameters \( x_0, y_0, z_0, x_1, y_1, z_1 \) and \( b_1 \). It can be known that the key space of the algorithm is \( 10^{16} \times 10^{16} \times 10^{15} \times 10^{15} \times 10^{15} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} = 10^{141} \), which are through a large number of key sensitivity tests. Table 6 shows the key-space comparison results between this algorithm and other existing algorithms.

---

**TABLE 4** Comparative analysis of information entropy

| Image    | Lean | Peppers | Baboon | Aeroplane | Merge images |
|----------|------|---------|--------|-----------|--------------|
| Plaintext | 7.3722 | 7.5715  | 7.3579 | 6.6776    | 7.7038       |
| Ciphertext | 7.9993 | 7.9993  | 7.9992 | 7.9991    | 7.9998       |

**TABLE 5** Comparative analysis of number pixels change rate (NPCR) and unified average changing intensity (UACI) test values of ciphertext images (100%)

| Image | Test | [12] | [14] | Proposed |
|-------|------|------|------|----------|
| Lena  | NPCR | 99.6289 | 99.61 | 99.6096 |
|       | UACI | 33.5420 | 33.45 | 33.4645 |
| Peppers | NPCR | 99.6047 | 99.63 | 99.6102 |
|       | UACI | 33.3447 | 33.46 | 33.4632 |
| Baboon | NPCR | 99.3665 | 99.62 | 99.6007 |
|       | UACI | 33.5084 | 33.43 | 33.4545 |
| Aeroplane | NPCR | 99.4036 | –    | 99.6057 |
|       | UACI | 33.3682 | –    | 33.4591 |
| Average value | NPCR | 99.50925 | 99.62 | 99.60655 |
|       | UACI | 33.440825 | 33.447 | 33.4603 |

**TABLE 6** Key space comparison analysis

| Method | [6] | [8] | [12] | [14] | [18] | Proposed |
|--------|-----|-----|------|------|------|----------|
| Key space | \(10^{60}\) | \(2^{201}\) | \(2^{72}\) | \(10^{56}\) | \(10^{187}\) | \(10^{141}\) |
4.4.2 Key-sensitivity analysis

An efficient encryption algorithm should be highly sensitive to any small change in the encryption or decryption key [12]. In order to test the sensitivity of the encryption algorithm, a small change is made to the value of an initial key and other parameters remain unchanged. The plaintext image, ciphertext image and the decrypted image are shown in Figure 6.

Figure 9 is an image decrypted with an incorrect key.

As shown in Figure 9, the decrypted image obtained cannot be recognised when the initial key is slightly changed.

In order to further illustrate the difference between the decrypted images obtained by the wrong key and the correct key, mean squared error (MSE) and peak signal-to-noise ratio (PSNR) are used as important indicators to measure the effect of image encryption. The larger the value of MSE, the smaller the value of PSNR. It shows that the greater the difference between the images decrypted with the correct key and the wrong key, the better the sensitivity of the key. The mathematical expressions of MSE and PSNR are shown in Equations (23) and (24):

\[
MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [d(i,j) - d'(i,j)]^2 \tag{23}
\]

\[
PSNR = 10 \times \log_{10} \left( \frac{255^2}{MSE} \right) \tag{24}
\]

where \(M\) and \(N\) represent the length and width of the test image, \(d(i,j)\) and \(d'(i,j)\) represent the image decrypted with the correct key and the wrong key, respectively.

Selecting the initial value of a key and adding \(10^{-16}\) to the original value that guarantees other parameters will not change. The test results of key sensitivity are shown in Table 7.

From the actual test values of MSE and PSNR in Table 7, it can be seen that the decrypted images obtained by the slightly changed initial key are significantly different from the correct decrypted images. It shows that the proposed algorithm is sensitive to the key that can resist the exhaustive attack.

4.5 Robustness analysis

4.5.1 Cropping attack

In order to test the problem of information loss in covert transmission of ciphertext images, this study carries out local cropping attack on ciphertext images. The ciphertext image shown is cropped in four ways 1/16, 1/8, 1/4, 1/2 and the cropped portion is filled with a grey value of 255. The experimental test results are shown in Figure 10.

As shown in Figure 10, the decrypted image still retains most of the characteristic information of the plaintext image when the ciphertext image is attacked by cropping. This shows that the proposed encryption algorithm has good anti-crop performance, but the decrypted image quality is poor when the clipping size is too large.

4.5.2 Noise attack analysis

In nature, noise and channel losses are common problems that information faces during transmission. Therefore, it is necessary to test the recoverability of ciphertext images after being subjected to noise pollution [15]. Adding different intensity of
pepper and salt noises and Gaussian noise to the ciphertext image and the recovery effect of the decrypted image is shown in Figure 11.

It can be seen from Figure 11 that ciphertext images can still recover highly visible decrypted images after being subjected to different degrees of pepper and salt noise and Gaussian noise. With the increase of noise intensity, the recovery effect of the image becomes worse. But the image still retains the main feature information that can be recognised by the human eye. Because the effect of Gaussian noise on image quality is relatively serious, the recovery effect of post-ciphertext images subjected to pepper and salt noise is better than that of post-ciphertext images subjected to Gaussian noise.

From the experimental results of Figures 10 and 11, it can be seen that the ciphertext image can still recover the highly visible decrypted image after being subjected to cropping and noise attacks, so the proposed algorithm has strong robustness.

### 4.6 Discussion of tampering location analysis

Encrypted images are vulnerable to various kinds of attacks in the process of communication transmission. The proposed algorithm can use image hashing to conduct tamper location analysis of ciphertext images in this study. First, tamper authentication is set as

\[ F(x, y) = f(x, y) - f'(x, y) \]  

(25)

where \( f(x, y) \) is the hash matrix generated by the plain image, and \( f'(x, y) \) is the hash matrix generated by the decrypted image.

The image has not been tampered with, and the value of \( F(x, y) = 0 \); the image has been tampered with, and the value of \( F(x, y) \) does not equal 0. By setting \( F(x, y) \neq 0 \) to conduct tamper location analysis, we have

\[ F'(x, y) = f(x, y) \otimes f'(x, y) \]  

(26)

where \( f(x, y) \) and \( f'(x, y) \) are the hash matrices generated by the plain image and the decrypted image, respectively.

The value of the generated 2D matrix \( F'(x, y) \) is detected in the order from left to right and from top to bottom. When the value is 0, it means that this point pixel has not been tampered with; when the value is 1, it proves that this point pixel has been tampered with. A lot of experiments show that the proposed algorithm can tamper location analysis of decrypted images and even can be used in the application field of tampering recovery of the decrypted image.

### 4.7 Time complexity analysis

In order to analyse the time complexity of the encryption algorithm, the encryption speed needs to be tested. After a large number of experiments, the average time required to encrypt the four test images was measured as 19.1744 s in this study. In [12, 14] single-image and multi-image encryption algorithms are shown, respectively. Single-image encryption time in [12] is 3.009 s, and in [14], four-image encryption time is 43 s. Therefore, the encryption efficiency of the proposed algorithm is significantly better than that in [14] and slightly lower than that in [12], but after the above experimental analysis, its security is significantly better than that in [12, 14]. The proposed algorithm has high security, but the encryption efficiency needs to be further improved. DNA computing has the characteristics of massive parallelism, huge storage and ultra-low power consumption. With the development of DNA technology, the advantages of the new algorithm in the encryption speed will be improved.

### 5 CONCLUSIONS

A new MIE algorithm based on image hash, bit-plane decomposition and dynamic DNA coding is proposed. The proposed algorithm uses the image hash technology to generate the initial key that strengthens the connection between several grey images and the key, and it not only improves the key sensitivity but also can effectively resist the selected plaintext attack. The improved 3D chaotic mapping and 4D hyperchaotic system are used to generate more unpredictable chaotic sequences.
and increase the key space. The chaotic sequence is used to perform pixel replacement on the bit-plane-decomposed image so that the merged image realises synchronous operations of multiple image replacement and diffusion. In addition, the image encryption efficiency is improved by simultaneous encryption and decryption of multiple images. The experimental results show that compared with the existing MIE algorithm, the proposed algorithm proposes a novel key generation method that improves the security of multi-image transmission, making it not only resistant to various conventional attacks but also able to perform tamper-resistant images positioning analysis. The proposed algorithm has large-enough key space and strong key sensitivity and has excellent security and robustness against statistical analysis, differential attack, cropping and noise attack. The image hash technology lays a foundation for the next image tamper location and recovery.

The proposed algorithm has high security and can be used to locate and analyse tampered images, but it is too complex. Therefore, the next step of research is to improve the efficiency of encryption while ensuring security.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China (No. 61862041, 61363078). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

ORCID
Qiuyu Zhang https://orcid.org/0000-0003-1488-388X

REFERENCES

1. Chen, Q., et al.: Topological charge number multiplexing for JTC multi-image encryption. Opt. Commun. 412, 155–160 (2018)
2. Xi, S., et al.: Optical encryption method of multi-image based on δ modulation and computer generated hologram. Opt. Commun. 445, 19–23 (2019)
3. Zhang, L., et al.: Multi-image encryption based on double random phase encoding and compressive sensing by using a measurement array preprocessed with orthogonal-basis matrices. Opt. Laser Technol. 105, 162–170 (2018)
4. Karawia, A.A.: Encryption algorithm of multi-image using mixed image elements and two dimensional chaotic economic map. Entropy 20(10), 801 (2018)
5. Wang, H., et al.: Multiple-image encryption and authentication in interference-based scheme by aid of space multiplexing. Opt. Laser Technol. 95, 63–71 (2017)
6. Zhang, X., Wang, X.: Multi-image encryption algorithm based on mixed image element and permutation. Opt. Lasers Eng. 92, 6–16 (2017)
7. Zarchnia, M., Pakmanesh, H., Parvaz, R.: A fast multi-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik 179, 761–773 (2019)
8. Yu, C., et al.: Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimedia Tools Appl. 77(4), 4585–4608 (2018)
9. Kim, Y., et al.: Interference-based multi-image encryption using binary phase masks. Opt. Lasers Eng. 107, 281–287 (2018)
10. Kumar, R., Sheridan, J.T., Bhaduri, B.: Nonlinear double image encryption using 2D non-separable linear canonical transform and phase retrieval algorithm. Opt. Laser Technol. 107, 353–360 (2018)
11. Bisht, A., et al.: Symmetric multiple image encryption using multiple new one-dimensional chaotic functions and two-dimensional cat map. In: International Conference on Inventive Research in Computing Applications, Coimbatore, India, pp. 676–682 (2018)
12. Nematzadeh, H., et al.: Binary search tree image encryption with DNA. Optik 202, 163505 (2020)
13. Enayatifar, R., et al.: Index-based permutation-diffusion in multiple-image encryption using DNA sequence. Opt. Lasers Eng 115, 131–140 (2019)
14. Zhang, X., Wang, X.: Multi-image encryption algorithm based on DNA encoding and chaotic system. Multimedia Tools Appl. 78(6), 7841–7869 (2019)
15. Li, C.L., et al.: Multiple-image encryption by using robust chaotic map in wavelet transform domain. Optik 171, 277–286 (2018)
16. Xiong, Y., et al.: Multi-image encryption scheme based on pixel exchange operation and vector decomposition. Opt. Lasers Eng. 101, 113–121 (2018)
17. Yuan, X., et al.: Multi-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing. Appl. Phys. B 125(9), 174 (2019)
18. Zhou, N., et al.: Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. Quantum Inf. Process. 17(12), 338 (2018)
19. Liansheng, S., et al.: Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. Opt. Lasers Eng. 113, 29–37 (2019)
20. Yan, A., et al.: Multi-image encryption based on angular-multiplexing holography with quick response code and spiral phase keys. Appl. Opt. 58(34), 6–10 (2019)
21. Wu, J., et al.: Multi-image optical encryption based on phase retrieval algorithm and fractional Talbot effect. Opt. Express 27(24), 35096–35107 (2019)
22. Li, X., et al.: Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme. Opt. Lasers Eng. 102, 106–111 (2018)
23. Huo, D., et al.: Multiple-image encryption scheme via compressive sensing and orthogonal encoding based on double random phase encoding. J. Mod. Opt. 65(18), 2093–2102 (2018)
24. Chai, X.L., et al.: A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. Chinese Phys. B 25(10), 100503, 1–13 (2016)

How to cite this article: Zhang Q, Han J, Ye Y. Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding. IET Image Process 2021;15:885–896.
https://doi.org/10.1049/ipr2.12069