HOSTED BY

ELSEVIER

Contents lists available at ScienceDirect

Journal of King Saud University - Computer and Information Sciences

journal homepage: www.sciencedirect.com

Full length article

Exploring the future application of UAVs: Face image privacy protection scheme based on chaos and DNA cryptography

Heping Wen[a,b,*], Zhiyu Xie[a,b], Zhuxi Wu[a,b], Yiting Lin[a,b], Wei Feng[c]

[a] University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan, 528402, China
[b] University of Electronic Science and Technology of China, Chengdu, 611731, China
[c] School of Mathematics and Computer Science, Panzhihua University, Panzhihua 617000, China

ARTICLE INFO

Keywords:
Chaos
Image encryption
Privacy-preserving
DNA encoding

ABSTRACT

In the application and promotion of UAV in the future, remote sensing image information is transmitted frequently, and its security issues will not be ignored. Aiming at the privacy security problem of portrait information in remote sensing images, this paper proposes a face privacy protection technology scheme based on chaos and DNA cryptography. Firstly, the edge recognition face detection technology is used to identify the face information, and the corresponding matrix is selected as the object of selective encryption. Then, the hash eigenvalues of the selected encrypted object are extracted, and the plaintext-associated chaotic sequences are generated for RGB permutation and zigzag interleaved scrambling in turn. Then, the three channels of RGB are encrypted by dynamic chain DNA encoding in turn. Finally, the cipher-image is obtained after performing discontinuous diffusion and lightweight bit-level confusion. In this paper, chaotic pseudo-random sequences with plaintext correlation and dynamic DNA chain encryption are used to effectively improve the ability of encryption system to resist cryptographic attacks. At the same time, selective encryption can effectively reduce the encryption complexity and performance overhead. Experimental results and security analysis show that the privacy protection scheme has excellent security and efficiency performance. Therefore, the face privacy protection technology scheme reported in this paper has excellent performance and has broad application prospects in UAV and remote sensing communication.

1. Introduction

Currently, UAV technology is developing rapidly. With the unprecedented capabilities of aerial equipment in capturing photographs, the ability to capture images is constantly improving, resulting in more diverse and rich image information. However, along with the benefits of this technology, the associated challenges in information security have increasingly attracted attention, such as the issue of privacy protection for facial information in digital images. Therefore, privacy protection technology is an indispensable key element for the captured digital images in future UAV applications. Encrypting the images captured by UAVs will be an important technical approach to protect important sensitive information from potential leaks during network communication. Currently, various encryption methods have been proposed to ensure the security of image data, such as quantum cryptographic (Chai et al., 2023; Li and Yang, 2022; Singh et al., 2021) thumbnail storage encryption (Chai et al., 2022b; Zhao et al., 2023; Zhang et al., 2022b,a), biometric encoding (Chai et al., 2022b; Zhao et al., 2023; Zhang et al., 2022b,a), discrete wavelet transform (Wen et al., 2022a; Araghi and Manaf, 2019; Wen et al., 2023b), discrete cosine transform (Wang et al., 2021; Ariatmanto and Ernawan, 2022; Sisaudia and Vishwakarma, 2022), bit-level encryption (Wei et al., 2023; K.U. and Mohamed, 2020; Wang et al., 2020), fourier transform (Wen et al., 2023d; Xie et al., 2023; Melman and Evsutin, 2023), chaos theory (Li et al., 2022, 2019; Banerjee et al., 2023) and so on (Wen et al., 2023a; Lu et al., 2023; Ma et al., 2020). Furthermore, the utilization of chaotic system in image encryption algorithms (Wen and Lin, 2024, 2023; Wen et al., 2023c)

[*] Corresponding author at: University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan, 528402, China.
E-mail addresses: wenheping@uestc.edu.cn (H. Wen), ZhiyuXie@ieee.org (Z. Xie), ZhuxiWu@stu.zsc.edu.cn (Z. Wu), YitingLin@stu.zsc.edu.cn (Y. Lin), fengwei@pzhu.edu.cn (W. Feng).

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.101871
Received 14 October 2023; Received in revised form 30 November 2023; Accepted 6 December 2023
Available online 7 December 2023

have gained immense popularity due to its inherent characteristics of unpredictability, pseudo-randomness and sensitivity to initial values. These properties make chaos not only highly effective but also exceptionally suitable for ensuring the security and confidentiality of image data. By leveraging the unpredictable and sensitive nature of chaos, image encryption algorithms can provide robust protection against potential attacks or unauthorized access, making them a preferred choice in the field of image security.

Throughout the international status, many scholars have achieved a series of important theoretical (Lai et al., 2023a; Chai et al., 2022a; Yu et al., 2021) and applied results (Zhou et al., 2014; Vikas and Parhi, 2023; Xiang et al., 2021; Chai et al., 2022c) in using chaotic system for image encryption. In 2023, Ref. (Gao et al., 2023) introduces a new facial image encryption method. This method encrypts only the facial region in the face image with high computational efficiency. Firstly, facial recognition technology is used to extract and recognize the features of the facial image. Then, the facial image is input into the encryption algorithm to generate cipher-images using methods like permutation and diffusion. The proposed algorithm is evaluated on a dataset and achieves good performance. In the same year, a comprehensive survey on security, privacy issues and emerging defence technologies for UAV (Hadi et al., 2023) was proposed. This study presents perspectives and insights on the threats and vulnerabilities associated with drones, extensively examines their privacy and security issues and summarizes key lessons learned in drone security and privacy. Finally, recommendations for future research directions are provided. It can be seen from these studies that most of the UAV security communication algorithms have achieved satisfactory results, which has greatly promoted the development of information security technology. Unfortunately, in the era of rapid development of the Internet and digital technology, most of the achievements have limitations of the times: (1) The existing biological coding has the problem of decipherable coding and single operation rules. (2) The existing encryption algorithm structure is too simple or unreasonable. If the plaintext association or ciphertext feedback is not used, the algorithm is vulnerable to known-plaintext attack or chosen-plaintext attack. (3) Global encryption or full encryption makes a lot of redundant information encrypted, which wastes the performance and communication bandwidth.

This paper presents a scheme for protecting the privacy of portrait information in remote sensing images by using chaos and DNA cryptography. The proposed technology includes several steps: First, the face detection technology based on edge recognition is employed to identify the face information. Next, the hash eigenvalues of the selected encrypted object are extracted, and a plaintext-associated chaotic sequences are generated. The sequences is then used to perform RGB permutation and zigzag interleaved scrambling. Afterward, each channel of RGB is encrypted using dynamic chain DNA encoding. Finally, the encrypted image is obtained by applying discontinuous diffusion and lightweight bit-level confusion. Additionally, local encryption can effectively reduce encryption complexity and performance overhead.

The main innovations and contributions of this paper are as follows.

(i) Most existing image encryption schemes primarily focus on encrypting the entire image. When processing facial images, researchers often encrypt the entire image without considering the need to protect redundant information. In order to enhance the security and efficiency of encryption systems, it is necessary to perform local encryption on facial images.

(ii) In comparison to pixel-level encryption, DNA encoding provides finer security for images. The DNA-based encryption method used in this algorithm is a more complex and efficient approach. It re-encodes the pixels in the image based on DNA sequences to achieve a higher level of encryption. Additionally, this algorithm employs multiple DNA manipulation rules to make the encryption and decryption processes more complex and secure. Experimental results demonstrate that this algorithm effectively enhances the security of image encryption.

Table 1
DNA coding rules.

Rules	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

(iii) Existing encryption schemes utilize encoding methods that are easy to crack and have single operation rules. In contrast to previous encryption schemes, this secure image encryption algorithm combines multiple encryption techniques, including RGB Permutation, Zigzag Interleaved Scrambling, DNA domain encryption, Discontinuous Diffusion, and Bit-level Confusion. This combination enhances the security and robustness of the encryption algorithm, making it more resistant to attacks and ensuring the confidentiality of transmitted images.

(iv) Many existing encryption algorithm structures are unreasonable. Without the presence of related plaintext or ciphertext feedback, they are vulnerable to known-plaintext or chosen-plaintext attacks. This secure image encryption scheme utilizes dynamic feedback mechanism to update the encryption key based on encrypted data. This feedback mechanism enhances the security and resistance against attacks such as chosen-plaintext and chosen-ciphertext attacks.

The remaining part of this paper is organized as follows. Section 2 provides relative theory. Section 3 discusses face detection. Section 4 presents results and analysis. The final part is the conclusion of the paper.

2. Related theories

2.1. DNA cryptography

In 1994, Ref. (Adleman, 1994) proposed DNA cryptography. Early research focused on using the physical and chemical properties of DNA molecules to design encryption algorithms. Because of its highly reliable information storage capacity and complex biological characteristics, DNA is considered to be a potential cryptographic tool. With the continuous development and progress of DNA technology, researchers have begun to explore DNA as a new encryption method in cryptography (Wen et al., 2022b).

DNA consists of four types of nucleobases: Adenine (A), Thymine (T), Cytosine (C) and Guanine (G). According to the principles of permutation and combination, these four nucleobases can be arranged in 24 different ways. However, in DNA computation, we need to follow the rule of complementarity, where A complements T and C complements G. Therefore, as shown in Table 1, there are eight encoding rules for DNA sequences to satisfy the complementary rules. In DNA computation, there are mainly six basic operations: Addition, Subtraction, XOR (exclusive OR), Add complement, Sub-complement, and XNOR (exclusive NOR). The specific operation rules are shown in Table 2.

Different encoding rules in DNA computation may lead to different representations of the same sequence. For example, the binary form of 54 is '00110110'. When using the first encoding rule, its DNA sequence representation is 'ATGC'; when using the sixth encoding rule, its DNA sequence representation is 'CGTA'. Similarly, different decoding rules can also yield different results in information recovery. For instance, if we take the string 'ATCG' and apply the first decoding rule, the resulting sequence is '00111001', corresponding to the value 57. However, using the fourth decoding rule would result in a different sequence, '01100011', corresponding to the value 99. Obviously, the application of different rules in image encryption can achieve the purpose of encryption.

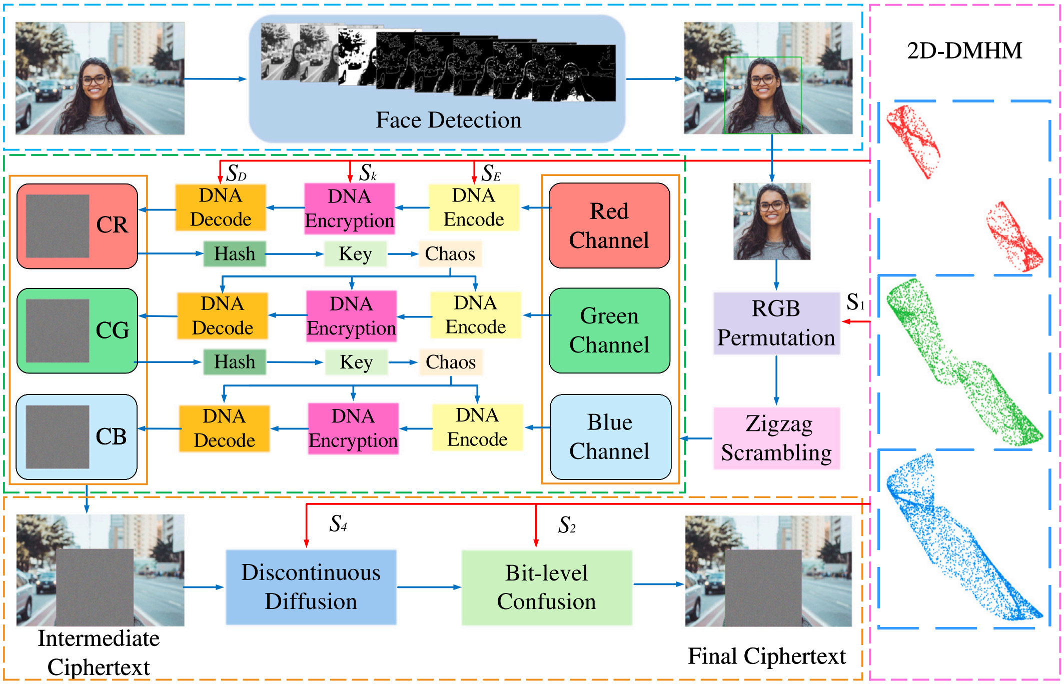


Fig. 1. The flowchart of encryption process.

Table 2
DNA operations.

	Addition				Subtraction				XOR			
	A	G	C	T	A	G	C	T	A	G	C	T
A	A	G	C	T	A	T	C	G	A	T	C	G
G	G	C	T	A	G	A	T	C	G	C	T	A
C	C	T	A	G	C	G	A	T	C	G	A	T
T	T	A	G	C	T	C	G	A	T	A	G	C

	Add-Complement				**Sub-complement**				**XNOR**			
	A	**G**	**C**	**T**	**A**	**G**	**C**	**T**	**A**	**G**	**C**	**T**
A	T	C	G	A	T	A	G	C	T	C	G	A
G	C	G	A	T	C	T	A	G	C	T	A	G
C	G	A	T	C	G	C	T	A	G	A	T	C
T	A	T	C	G	A	G	C	T	A	G	C	T

2.2. The adopted chaotic map

The chaotic system used in this paper is 2D-discrete memristive hyperchaotic map, abbreviated as 2D-DMHM. The chaotic system is a complex mathematical model that combines a coupled improved Logistic diagram with a discrete memristor (Lai et al., 2023b). The model of chaotic system is described as follows:

$$\begin{cases} x_{n+1} = ux_n \sin(a(1-x_n)) + k\sin(y_n)x_n \\ y_{n+1} = x_n + y_n \end{cases} \tag{1}$$

where the chaotic parameters are $a = 0.1$, $k = 1.72$ and $u \in [-2.4, 4]$. At the same time, when $u \in [-2, -0.1]$, the system is in a hyperchaotic state.

3. The proposed face image privacy protection scheme

In contrast to traditional algorithms, this paper incorporates the plaintext correlation mechanism and utilizes the MD5 hash function to dynamically update the key together with the encrypted data. The key is generated using a sequence derived from 2D-DMHM chaos. This sequence is employed for RGB permutation, DNA domain encryption, discontinuous diffusion, and lightweight bit-level confusion on the image. Furthermore, the ciphertext feedback method is innovatively utilized to perform a two-round encryption process, enhancing the computational complexity of the algorithm and offering resistance against chosen-plaintext attacks and chosen-ciphertext attacks. Fig. 1 illustrates the overall block diagram of the algorithm design.

3.1. Face detection

Firstly, the image undergoes mean filtering to reduce fine details, followed by binarization for subsequent morphological processing. The algorithm employs morphological boundary extraction to identify and separate facial regions. This approach effectively addresses the issue of smaller connected regions that may arise after image binarization due to darker skin colors, thereby minimizing errors in face detection. Next, a closure operation is performed using a vertically elongated strip of structuring elements to eliminate interference from the captured person's face, hair, and clothing, ensuring that the facial region remains intact during the morphological boundary extraction process. Subsequently, lateral erosion operations segment the large connected domains of the body parts and remove background clutter, thereby further refining the image. Finally, the largest filtered connected domain that satisfies the necessary facial feature requirements in terms of size and shape is selected for face acquisition. Fig. 2 presents the overall block diagram, illustrating the steps of the face recognition algorithm.

3.2. Initialization of encryption

Taking the image P of size $H \times W \times 3$ as an example, the eigenvalues of the image are read, and the MD5 hash function is used to generate

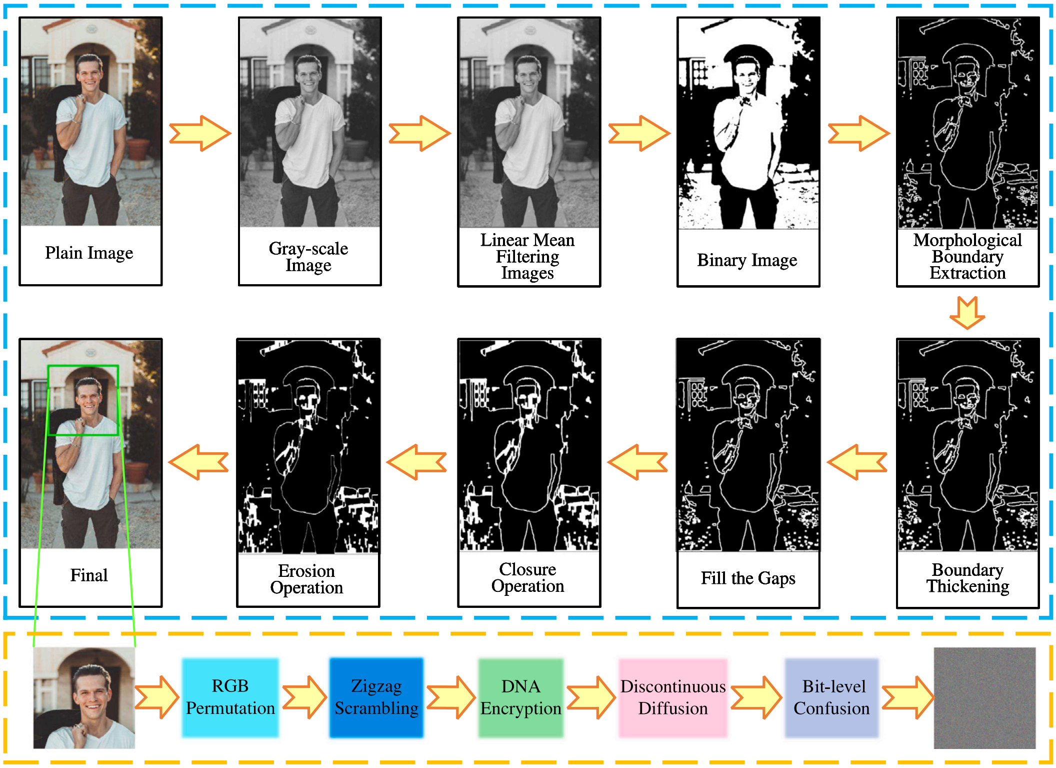


Fig. 2. The flowchart of face detection and encryption process.

the scrambling values $h(x)$, and $x \in [1, 32]$, which are processed by the following equation to generate the key parameters:

$$\begin{cases} \theta = 0.1 + (h(1) + h(4) + h(7) + h(10) + h(13) + \\ h(16) + h(19) + h(22) + h(25) + h(28)) \bmod 0.21 \\ a(0) = (h(2) + h(5) + h(8) + h(11) + h(14) + h(17) + \\ h(20) + h(23) + h(26) + h(29) + h(31)) \bmod 1.5 \\ b(0) = (h(3) + h(6) + h(9) + h(12) + h(15) + h(18) + \\ h(21) + h(24) + h(27) + h(30) + h(32)) \bmod 2.4 \end{cases} \tag{2}$$

where θ is the key parameter, $a(0)$ and $b(0)$ are the initial values of the chaotic system.

The keys θ, $a(0)$, and $b(0)$ obtained from the plain-image are substituted into the 2D-DMHM chaotic system to generate two chaotic sequences, denoted as S_1 and S_2. These sequences are then processed using Eq. (3) to ensure their suitability for the algorithm's requirements. The specific equation is as follows:

$$\begin{cases} S_{RGB} = floor(S_1(H \times W) \times 10^{15}) \bmod 6 \\ S_{bit} = floor(S_2 \times 10^{15}) \bmod 256 \end{cases} \tag{3}$$

where $floor(\cdot)$ is the downward integer function and $\bmod (\cdot)$ is the modulo operation function. S_{RGB} and S_{bit} are chaotic sequences required for RGB permutation and lightweight bit-level confusion.

3.3. Encryption process

- *RGB permutation*

The RGB permutation of the plain-image P is performed using the chaotic sequence S_{RGB}. Firstly, the plain-image P is decomposed into its RGB channels, and the resulting images are extended into 1D vectors P_R, P_G and P_B, each with length of $H \times W$. The RGB permutation rules are determined by the chaotic sequence $S_{RGB}(i)$. For example, the first pixel value is replaced as follows: the value of the R channel is replaced with the value of the B channel, the value of the G channel is replaced with the value of the R channel, and the value of the B channel is replaced with the value of the G channel. The permutation rules are shown in Table 3. Finally, the image C_1 is obtained after the RGB permutation.

Table 3
RGB permutation rules.

$S_{RGB}(i) = 0$	$R \to R$	$G \to G$	$B \to B$
$S_{RGB}(i) = 1$	$R \to R$	$G \to B$	$B \to G$
$S_{RGB}(i) = 2$	$R \to G$	$G \to R$	$B \to B$
$S_{RGB}(i) = 3$	$R \to B$	$G \to R$	$B \to G$
$S_{RGB}(i) = 4$	$R \to G$	$G \to B$	$B \to R$
$S_{RGB}(i) = 5$	$R \to B$	$G \to G$	$B \to R$

- *Zigzag interleaved scrambling*

The preprocessed image C_1 undergoes zigzag interleaved scrambling. The scanning process starts with the first element in the upper left corner of the original image, which has a size of $H \times W$. The scanning continues until $(H \times W)/2$ elements have been scanned, and each scanned element is added to the array V_1. Similarly, the lower half of the image is scanned, starting from the first element in the lower right corner, and each scanned element is added to the array V_2. V_1 and V_2 are then interleaved to create V_3, which is reconstructed into a larger image. The resulting scrambled image C_2 from these two operations is used for the subsequent encryption operation, as depicted in Fig. 3.

- *DNA domain encryption*

Step 1: Preprocessing of chaotic sequences

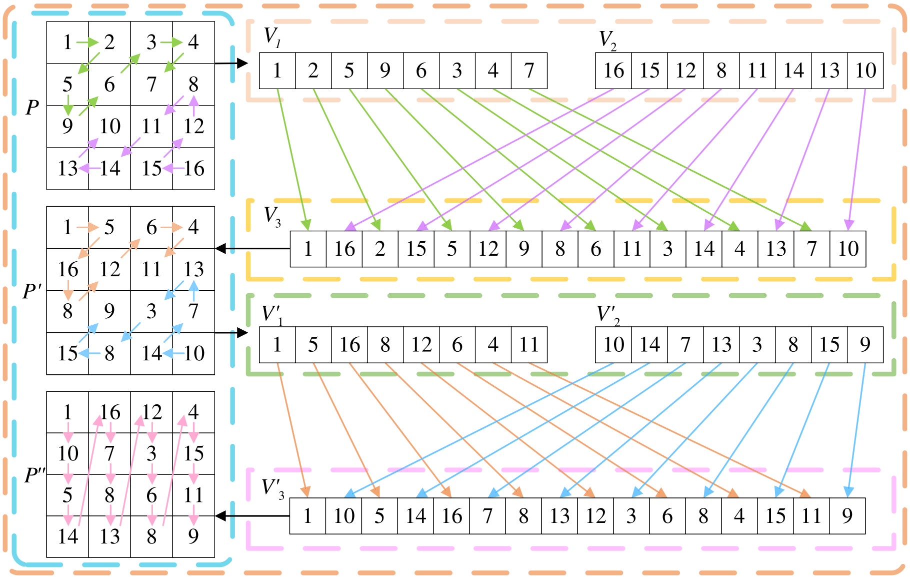


Fig. 3. Interleaved scrambling process of zigzag.

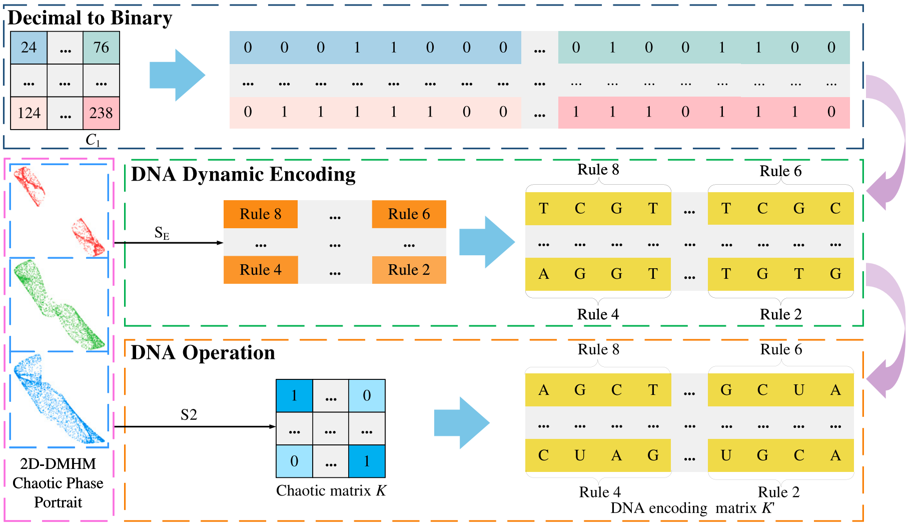


Fig. 4. DNA dynamic coding example diagram.

Prior to commencing DNA encryption, the intermediate cipher-image C_2 undergoes a hashing process, as demonstrated in Eq. (2), to derive new chaotic parameters and generate a new chaotic sequence S_3. The processing method of chaotic sequence S_3 is as follows:

$$\begin{cases} S_k = floor(S_3(H \times W) \times 10^{15}) \bmod 256 \\ S_4 = S_3(H \times W + 19 \times H \times W) \\ S_E = floor(S_4(14 \times H \times W) \times 10^{15}) \bmod 8 + 1 \\ S_D = floor(S_4(4 \times H \times W + 18 \times H \times W) \times 10^{15}) \bmod 8 + 1 \end{cases} \tag{4}$$

Step 2: DNA dynamic encoding

Firstly, the preprocessed sequence S_k is used to reconstruct the key matrix K. Following that, DNA coding is conducted utilizing the coding sequence S_E. The image C_2 and the key matrix K are extended at the bit-level, and DNA coding is then applied sequentially from left to right and top to bottom. The coding rules are updated every 8-bits to enhance coding complexity and algorithm security. The specific process of DNA dynamic coding is outlined in Eq. (5), while an example of DNA dynamic coding is presented in Fig. 4. By the end of the process, a DNA matrix with a height of H and a width of $4 \times W$ is generated.

$$\begin{cases} C_2{}'(4(i-1)+1(4(i-1)+4)) = \\ Encode(C_2(8(i-1)+1(8(i-1)+8), S_E(i))) \\ K'(4(i-1)+1(4(i-1)+4)) = \\ Encode(K(8(i-1)+1(8(i-1)+8), S_E(i))) \end{cases} \tag{5}$$

Step 3: DNA dynamic operations

In order to enhance the resistance of the encryption algorithm to differential attacks, the DNA domain uses ciphertext feedback encryption operation, which helps to increase the complexity of the relationship between plaintext, key and ciphertext. The dynamic operation of DNA is represented as follows:

$$\begin{cases} C_d(i,j) = sub(C_2{}'(i,j), K(i,j)) \\ C'_d(i,j) = xor(C_d(i,j), K(i,j)) \\ C'_2(i,j) = add(C'_d(i,j)), C_2{}'(i-1,n) \end{cases} \tag{6}$$

where $i = 2 \times H$ and $j = 14 \times W$, C_d and C'_d represent the intermediate ciphertext, K represents the encoded chaotic matrix, $add(\cdot)$ represents

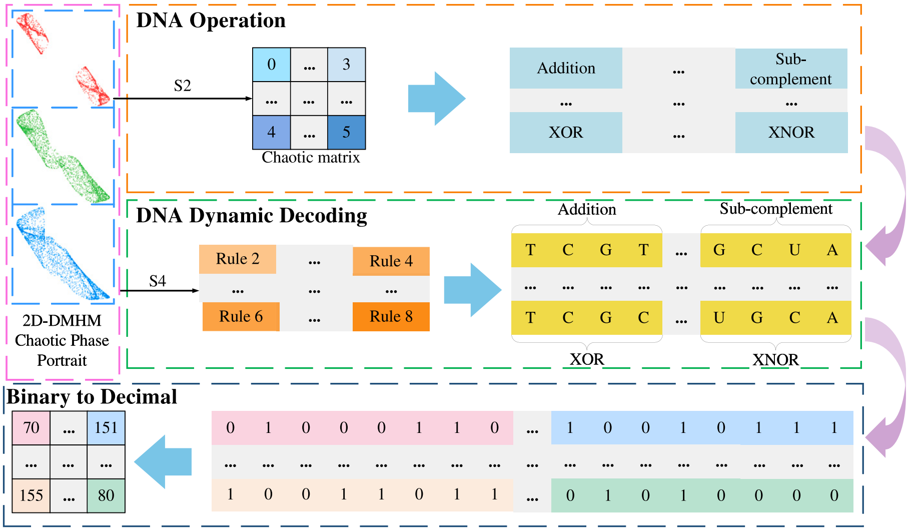


Fig. 5. DNA dynamic encoding example diagram.

DNA addition operation, $xor(\cdot)$ represents DNA XOR operation and $sub(\cdot)$ represents DNA subtraction operation.

By analyzing the Eq. (6), it becomes evident that the previous position of the DNA matrix is utilized to encrypt the subsequent position. To achieve chain encryption, this paper adopts the approach of using the last digit of the DNA encoding in the lower right corner of the R layer to encrypt the first digit in the R layer. Similarly, the last digit of the encrypted R layer in the lower right corner is utilized to encrypt the first digit in the G layer, and the last digit of the encrypted G layer in the lower right corner is employed to encrypt the B layer. This approach ensures the continuity and effectiveness of the encryption process. The resulting ciphertext after the DNA operations is denoted as C_3.

Step 4: DNA dynamic decoding

The process of DNA decoding resembles the encoding process. However, it is important to note that the decoding sequence undergoes processing using the sequence denoted as S_D. This distinguishes it from the encoding sequence, rendering it not a simple reverse process, but rather an additional encryption transformation. An example of dynamic DNA decoding is illustrated in Fig. 5. The DNA decoding process can be represented as follows:

$$\begin{aligned} &C_3'(24(i-1)+1(24(i-1)+24)) \\ &\quad = Decode(C_3(12(i-1)+1(12(i-1)+12), S_D(i))) \end{aligned} \tag{7}$$

where C_3' is the image after DNA dynamic decoding.

- *Discontinuous diffusion*

To achieve the diffusion characteristics of encryption algorithms, many image encryption algorithms employ the method of altering the current pixel based on the previous pixel. However, utilizing a fixed order of pixel processing may lead to reduced encryption performance and provide attackers with a significant amount of information. To address this concern, we have implemented a non-sequential encryption algorithm that utilizes random and secret access mechanisms for pixel processing. The specific operational process is illustrated in Fig. 6.

As depicted in Fig. 6, the processing order is determined by the generated chaotic sequence. Consequently, a pixel may be influenced not only by pixels within the same plane but also by any pixel from a different color plane. The encryption and decryption operations are as follows:

$$C_{i,j,k} = \begin{cases} (S_{i,j,k} + S_{M,N,3} + A_{i,j,k}) \bmod F & if \quad i=1, j=1, k=1 \\ (S_{i,j,k} + C_{M,N,k-1} + A_{i,j,k}) \bmod F & if \quad i=1, j=1, k \neq 1 \\ (S_{i,j,k} + C_{M,j-1,k} + A_{i,j,k}) \bmod F & if \quad i=1, j \neq 1 \\ (S_{i,j,k} + C_{i-1,N,k} + A_{i,j,k}) \bmod F & if \quad i \neq 1 \end{cases} \tag{8}$$

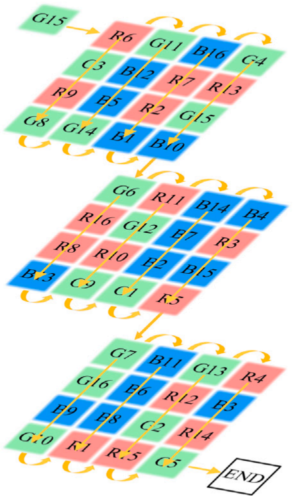


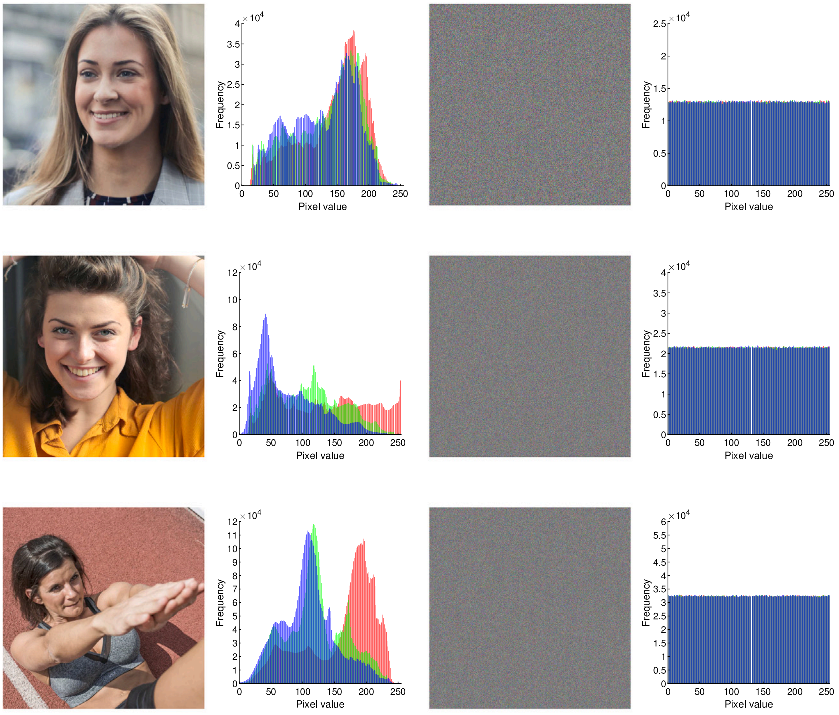
Fig. 6. Schematic diagram of discontinuous diffusion.

$$S_{i,j,k} = \begin{cases} (C_{i,j,k} - S_{M,N,3} - A_{i,j,k}) \bmod F & if \quad i=1, j=1, k=1 \\ (C_{i,j,k} - C_{M,N,k-1} - A_{i,j,k}) \bmod F & if \quad i=1, j=1, k \neq 1 \\ (C_{i,j,k} - C_{M,j-1,k} - A_{i,j,k}) \bmod F & if \quad i=1, j \neq 1 \\ (C_{i,j,k} - C_{i-1,N,k} - A_{i,j,k}) \bmod F & if \quad i \neq 1 \end{cases} \tag{9}$$

where mod(·) denotes the modulo operation, C_3' is the input color image, A is the chaos matrix generated from the chaotic sequences S_4 and F denote the number of pixel values in each color image C_3'. The ciphertext C_4 is finally obtained.

- *Lightweight bit-level confusion*

To improve the encryption performance of the algorithm, this paper incorporates bit-level confusion to enhance the granularity of data processing. Initially, the key matrix K_h is reconstructed using the chaotic sequence S_{bit}. Subsequently, the image C_4 is compared with the key matrix K_h using a bitwise XOR operation. Finally, the resulting post-image C_4' undergoes a bit-level right shift by s-bits, where $s \in [1, 1000]$.



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

Fig. 7. Images before and after encryption (a) Original images; (b) Histogram of (a); (c) Encrypted images; (d) Histogram of (c).

The detailed process is outlined as follows:

$$\begin{cases} C_4{}' = bitxor(C_4, K_h) \\ C_5(i+s) = C_4{}'(i) & i+s \le 24 \times H \times W \\ C_5((i+s) - 24 \times H \times W) = C_4{}'(i) & i+s > 24 \times H \times W \end{cases} \tag{10}$$

where C_5 is the image after bit-level confusion. The encryption process is hereby completed.

3.4. Decryption process

The decryption process is the inverse process of the encryption process. It first anti-lightweight bit-level confusion on the cipher-image, and then inverse discontinuous diffusion. Subsequently, the DNA domain is decrypted. After performing zigzag inverse scrambling, reverse RGB permutation is performed to restore the original plain-image.

4. Results and analysis

4.1. Experimental environment

The proposed algorithm was validated on a computer equipped with MATLAB R2023a experimental software. The computer is equipped with an i7-11800H CPU and has 32 GB of RAM. The image data selected for the experiments are from the standardized test image database USC-SIPI and the open-source image website gratisography.com.

4.2. Statistical analysis

4.2.1. Histogram analysis

Image encryption algorithms need to be adaptable to various application scenarios, ensuring that different types of images can be encrypted into unrecognizable cipher images. The original image can only be fully recovered with the correct key, and without it, no useful information about the original image can be obtained. In this paper, the encryption process is simulated using test images of different colors, and their pixel histograms are displayed in Fig. 7. Analyzing the histogram of an image provides valuable information. Furthermore, Fig. 8 illustrates the 3D histograms of both the original image and the corresponding encrypted image. Observing these histograms highlights that the encrypted image exhibits an even distribution of pixels on the red, green, and blue planes. This demonstrates the algorithm's effectiveness in encrypting natural images into high-performance cipher images.

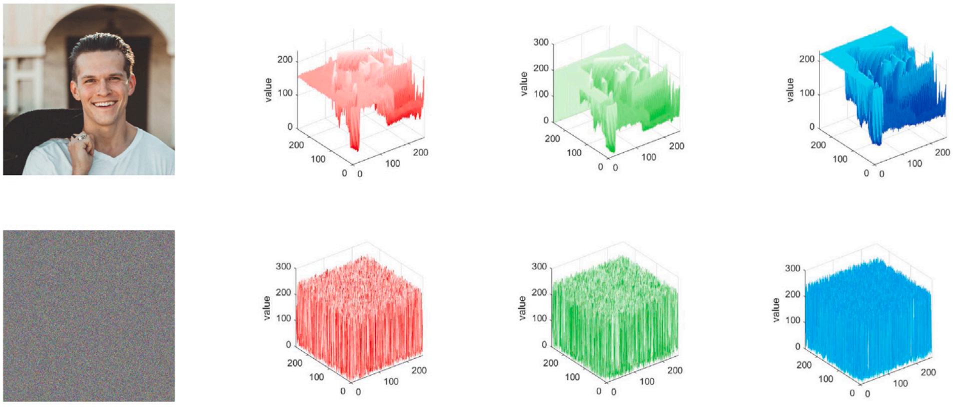
4.2.2. The coefficient of adjacent pixels

The original image has small differences in values between adjacent pixels and is highly correlated in the horizontal, vertical, diagonal and anti-diagonal directions. By using a good image encryption algorithm, the correlation between adjacent pixels in the image can be effectively broken, making it impossible to decipher the encrypted image through statistical analysis. The correlation coefficient between adjacent pixels can be represented as:

$$\begin{cases} r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ \mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \end{cases} \tag{11}$$

where x_i and y_i constitute the ith pair of horizontal/ vertical/ diagonal/ anti-diagonal neighboring pixels, N is the total number of horizontal/ vertical/ diagonal/ anti-diagonal neighboring pixels, $cov(x,y)$ is the covariance between pixel values x and y, $D(x)$ and $D(y)$ are the pixel value x and pixel value y mean-square error, $E(x)$ and $E(y)$ are the expected values of pixel value x and pixel value y, respectively. And r_{xy} is the correlation coefficient of pixel values x and y.

One of the key tasks of an image encryption algorithm is to disturb the correlation between pixels to effectively resist attackers' decryption



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

Fig. 8. 3D visualization histogram of plain-image and cipher-image (**a**)Images before and after encryption; (**b**) R channel; (**c**) G channel; (**d**) B channel.

Table 4
The comparison results of the correlation coefficients of adjacent pixels.

Component	Direction	Original image	Proposed
R channel	Horizontal	0.8752	0.0162
	Vertical	0.8802	0.0218
	Diagonal	0.8482	0.0071
	Anti-diagonal	0.8009	0.0067
G channel	Horizontal	0.8676	0.0079
	Vertical	0.8794	−0.0051
	Diagonal	0.8609	−0.0058
	Anti-diagonal	0.8054	0.0101
B channel	Horizontal	0.8569	−0.0286
	Vertical	0.8746	−0.0267
	Diagonal	0.8542	−0.0005
	Anti-diagonal	0.8017	−0.0213

attempts based on pixel correlations. In this paper, taking the 'Pepper' image as an example, 3000 pairs of adjacent pixels are randomly selected from the plaintext and ciphertext, and the correlation coefficients of the adjacent pixels in the horizontal, vertical, diagonal and anti-diagonal directions are calculated and the related scatter plots are drawn, as shown in Fig. 9. The results of the correlation analysis are shown in Table 4. The experiment demonstrates that our encryption algorithm successfully weakens the correlation between pixels, and there is almost no discernible correlation in the ciphertext. This strongly indicates that our proposed encryption algorithm possesses excellent security.

4.2.3. Differential statistical analysis

Using the values of the Number of Pixel Changes Rate (NPCR) and the Unified Average Changing Intensity (UACI) is a common method to evaluate the permutation and diffusion properties of image encryption algorithms. This approach is widely used to assess the performance of image encryption algorithms against differential attacks. In mathematical terms, the NPCR and UACI between two images can be defined as:

$$\begin{cases} NPCR = \frac{1}{H}\times W\times \sum_{i=1}^{H}\sum_{j=1}^{w} D(i,j)\times 100\% \\ UACI = \frac{1}{H}\times W\times \sum_{i=1}^{H}\sum_{j=1}^{w}\frac{|v_1(i,j)-v_2(i,j)|}{255}\times 100\% \end{cases} \tag{12}$$

where $H\times W$ is the size of the image, v_1 and v_2 are the cipher-image before and after the plain-image is changed by one pixel respectively. D can be defined by the following equation.

$$D = \begin{cases} 0 & if \quad v_1(i,j) = v_2(i,j) \\ 1 & if \quad v_1(i,j) \neq v_2(i,j) \end{cases} \tag{13}$$

The ideal values for NPCR and UACI are 99.6094% and 33.4635%, respectively. According to Eq. (12), this study selected some open-source images for NPCR testing and collected data for the RGB channels as shown in Table 5. The experimental data indicates that the encryption results of this algorithm are very close to the theoretical values.

Table 5
Test of NPCR values.

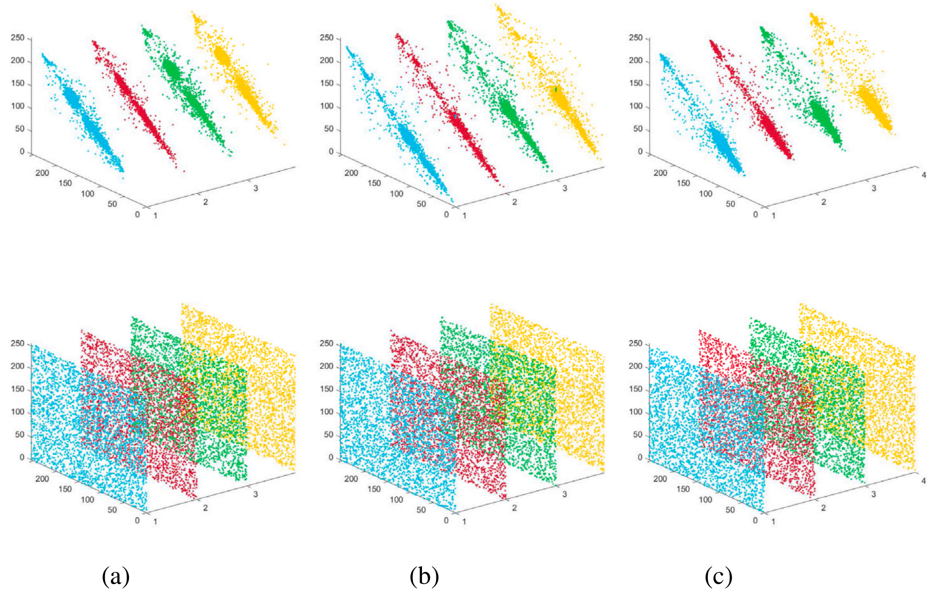
Image	Size	R channel	G channel	B channel
2.1.01	512 × 512 × 3	99.5655	99.6010	99.6319
2.1.02	512 × 512 × 3	99.6040	99.5895	99.5930
2.1.03	512 × 512 × 3	99.6136	99.5857	99.3771
2.1.04	512 × 512 × 3	99.6445	99.6239	99.5758
2.1.05	512 × 512 × 3	99.5998	99.6025	99.6216
2.1.06	512 × 512 × 3	99.6170	99.5991	99.6040
2.1.07	512 × 512 × 3	99.5934	99.5609	99.5907
2.1.08	512 × 512 × 3	99.5857	99.5075	99.4598
2.1.09	512 × 512 × 3	99.6193	99.5430	99.5998
2.1.10	512 × 512 × 3	99.6212	99.5621	99.5949
2.1.11	512 × 512 × 3	99.6750	99.5995	99.6452
2.1.12	512 × 512 × 3	99.5945	99.6227	99.6090
2.2.01	1024 × 1024 × 3	99.6042	99.6239	99.6039
2.2.02	1024 × 1024 × 3	99.6022	99.6129	99.6100
2.2.03	1024 × 1024 × 3	99.6058	99.5354	99.6035
2.2.04	1024 × 1024 × 3	99.6167	99.5682	99.5619
2.2.05	1024 × 1024 × 3	99.5947	99.6044	99.6158
2.2.06	1024 × 1024 × 3	99.5589	99.6395	99.6222
2.2.07	1024 × 1024 × 3	99.6101	99.5380	99.6106
2.2.08	1024 × 1024 × 3	99.6071	99.6115	99.5922
2.2.09	1024 × 1024 × 3	99.6151	99.4625	99.5982
2.2.10	1024 × 1024 × 3	99.6119	99.5266	99.6530
2.2.11	1024 × 1024 × 3	99.6129	99.6374	99.6088
2.2.12	1024 × 1024 × 3	99.6127	99.5353	99.6116
2.2.13	1024 × 1024 × 3	99.6165	99.6260	99.6110
2.2.14	1024 × 1024 × 3	99.5976	99.6762	99.6158
2.2.15	1024 × 1024 × 3	99.6108	99.6097	99.6122
2.2.16	1024 × 1024 × 3	99.6605	99.6774	99.6154
2.2.17	1024 × 1024 × 3	99.6124	99.6222	99.6130
2.2.18	1024 × 1024 × 3	99.6156	99.5960	99.6098

4.3. Information entropy

Another key metric for evaluating the distribution of grayscale values in an image and measuring the randomness of image information is information entropy, which can be expressed as:

$$H(m) = -\sum_{i=1}^{L} p(m_i)\log_2 p(m_i) \tag{14}$$

where L is the total number of symbols $m(i) \in m$ and $p(m_i)$ denotes the probability of the symbols. The experimental results are shown in Table 6. HI represents the plain-image information entropy, and HC represents the cipher-image information entropy. We can see that the



(a) (b) (c)

Fig. 9. The correlation of adjacent pixels in different directions between plain-image and cipher-image (**a**) R channel; (**b**) G channel; (**c**) B channel.

experimental results are close to the ideal value of 8, so the proposed algorithm has good information entropy properties.

4.4. *Image quality analysis*

Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) are commonly used as a tool to weigh the quality of encryption in the image processing field. Mean Square Error (MSE) is a part of PSNR which is defined as:

$$\begin{cases} \mathrm{MSE} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(X(i,j)-Y(i,j))^2 \\ \mathrm{PSNR} = 10\times\log_{10}\left(\frac{Q^2}{MSE}\right) \end{cases} \tag{15}$$

where MSE denotes the mean square error of the plain-image X and the cipher-image Y. The height and width of the image are denoted by H and W, respectively. And Q denotes the pixel level of the image. SSIM is a measure of the similarity of two images, defined as:

$$\mathrm{SSIM}(X,Y) = \frac{(2\mu_X\mu_Y + (0.01L)^2)(2\sigma_{XY} + (0.03L)^2)}{(\mu_X^2+\mu_Y^2+(0.01L)^2)(\sigma_X^2+\sigma_Y^2+(0.03L)^2)} \tag{16}$$

where μ_X and μ_Y denote the mean values of image X and Y, respectively, the standard deviation of image X and Y, respectively, and L denotes the dynamic range of pixel values. The values of PSNR and SSIM are calculated by using Eqs. (15) and (16). At the same time, in order not to lose generality, we also selected many images to test our encryption module, and its results are shown in Table 6. The PSNR value of the encrypted image should be less than 10db, and the range of SSIM value should be close to 0. The experimental results show that our encryption algorithm has good encryption effect.

Table 6
Information entropy, MSE, PSNR and SSIM values of different images.

Image	Size	HI	HC	MSE	PSNR	SSIM
2.1.01	512 × 512x3	7.4705	7.9953	21 926.0000	4.7213	0.0105
2.1.02	512 × 512x3	7.3311	7.9997	25 482.0000	4.0685	0.0111
2.1.03	512 × 512x3	6.8709	7.9606	28 957.0000	3.5133	0.0061
2.1.04	512 × 512x3	7.0728	7.9798	23 283.0000	4.4604	0.0083
2.1.05	512 × 512x3	7.5787	7.9932	24 190.0000	4.2945	0.0095
2.1.06	512 × 512x3	7.3983	7.9975	22 977.0000	4.5179	0.0092
2.1.07	512 × 512x3	6.7943	7.9856	26 620.0000	3.8787	0.0100
2.1.08	512 × 512x3	6.3833	7.8112	25 787.0000	4.0167	0.0135
2.1.09	512 × 512x3	6.8026	7.9848	26 092.0000	3.9657	0.0099
2.1.10	512 × 512x3	6.9127	7.9406	25 214.0000	4.1144	0.0128
2.1.11	512 × 512x3	7.3511	7.9898	23 249.0000	4.4667	0.0100
2.1.12	512 × 512x3	6.5674	7.9863	27 301.0000	3.7690	0.0114
2.2.01	1024 × 1024x3	7.6133	7.9946	27 439.0000	3.7472	0.0088
2.2.02	1024 × 1024x3	6.5786	7.9999	26 251.0000	3.9393	0.0106
2.2.03	1024 × 1024x3	6.3301	7.9802	27 628.0000	3.7173	0.0102
2.2.04	1024 × 1024x3	6.9188	7.9571	25 841.0000	4.0078	0.0105
2.2.05	1024 × 1024x3	7.4349	7.9982	22 079.0000	4.6909	0.0106
2.2.06	1024 × 1024x3	6.4133	7.9275	24 622.0000	4.2175	0.0123
2.2.07	1024 × 1024x3	6.4492	7.9914	27 740.0000	3.6997	0.0107
2.2.08	1024 × 1024x3	7.6470	7.9978	27 168.0000	3.7902	0.0079
2.2.09	1024 × 1024x3	6.8672	7.9781	27 060.0000	3.8075	0.0106
2.2.10	1024 × 1024x3	6.7117	7.8332	24 682.0000	4.2070	0.0116
2.2.11	1024 × 1024x3	6.7947	7.9953	23 642.0000	4.3940	0.0105
2.2.12	1024 × 1024x3	6.9619	7.9880	21 839.0000	4.7384	0.0107
2.2.13	1024 × 1024x3	7.3534	7.9903	24 011.0000	4.3267	0.0087
2.2.14	1024 × 1024x3	7.0507	7.9946	22 007.0000	4.7051	0.0104
2.2.15	1024 × 1024x3	6.7776	7.9999	23 054.0000	4.5033	0.0110
2.2.16	1024 × 1024x3	7.1279	7.9705	22 202.0000	4.6669	0.0098
2.2.17	1024 × 1024x3	7.1177	7.9961	22 804.0000	4.5508	0.0105
2.2.18	1024 × 1024x3	6.9236	7.9935	23 236.0000	4.4691	0.0105

4.5. *Key space analysis*

The key space refers to the set of all possible keys that can be used to generate a key, and the size of the key space depends on the length of the security key, which is one of the most important characteristics that determine the strength of a cryptosystem. The image encryption algorithm designed in this paper uses a 2D-DMHM chaotic system, whose key space can be expressed as $S \in \{a, k, u, MD5\}$, where a, k, u are the key parameter with the precision of 10^{-16} and $MD5$ is the hash value introduced to enhance the key space, which can generate 128 bits hash value. After calculation, the key space size of this encryption scheme is about $10^{3\times 16} \times 2^{128} \approx 2^{287}$ and the key length reaches 287 bits in this paper. Usually, the larger the key space is, the more computational resources and time are required to break the encryption algorithm. Therefore, the key space generated by the encryption algorithm in this paper is large enough to resist any form of brute force attack. The key space comparison is shown in Table 7.

4.6. *Sensitivity analysis*

In this section, the performance metrics of the algorithm are analyzed in terms of both key and plaintext sensitivity, respectively. The

Table 7
Key space comparison.

Proposed	(Liu et al., 2012)	(Murillo-Escobar et al., 2015)	(Mansouri and Wang, 2021)
287	166	128	154

Table 8
Key sensitivity test of NPCR and UACI.

	10^{-12}		10^{-13}		10^{-14}		10^{-15}	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
2.1.01	99.6223	33.1931	99.6292	33.4353	99.6063	33.4516	99.6243	33.2291
2.1.02	99.5911	33.4634	99.6197	33.4377	99.6094	33.4568	99.6101	33.4320
2.1.03	99.6143	33.7490	99.6170	33.6342	99.6136	33.4259	99.6178	33.8541
2.1.04	99.6105	33.4514	99.5903	33.4250	99.6162	33.4680	99.5953	33.4913
2.1.05	99.6204	33.4392	99.5941	33.4225	99.5914	33.4162	99.6159	33.3825
2.1.06	99.6185	33.4480	99.6185	33.4481	99.6220	33.4402	99.6159	33.2623
2.1.07	99.6162	33.4450	99.6082	33.3830	99.6052	32.9092	99.6086	33.4498
2.1.08	99.6326	32.0282	99.5872	32.1361	99.6174	32.1761	99.6223	32.0470
2.1.09	99.6265	33.4976	99.6029	32.9537	99.6132	33.4448	99.6204	33.4402
2.1.10	99.6201	33.3965	99.6357	33.4968	99.6147	32.4546	99.6033	33.4828
2.1.11	99.6059	33.4872	99.6006	33.4574	99.5865	33.4843	99.5987	33.5233
2.1.12	99.5953	33.4915	99.6071	32.6136	99.6201	33.4117	99.6181	33.4236
2.2.01	99.6024	33.4725	99.6148	33.4502	99.6126	33.4165	99.6082	33.4633
2.2.02	99.6163	33.4726	99.6103	33.4480	99.6165	33.4605	99.6154	33.4658
2.2.03	99.5984	33.4534	99.6156	33.4685	99.6104	33.4486	99.6078	33.4269
2.2.04	99.6103	32.5604	99.6175	33.4497	99.6049	32.5970	99.6091	33.4323
2.2.05	99.6589	33.1605	99.6160	33.5138	99.6103	33.4572	99.6116	33.4414
2.2.06	99.6179	33.4714	99.6021	33.4792	99.6091	33.4621	99.6155	33.4429
2.2.07	99.6024	33.4570	99.6028	33.7393	99.6171	33.4625	99.6063	33.4631
2.2.08	99.6063	33.4376	99.6158	33.3392	99.5974	33.3495	99.6127	33.3181

Table 9
The plaintext sensitivity test of NPCR and UACI.

	(H/4,W/4)		(H/4,W/2)		(H/2,W/4)		(H/2,W/2)	
	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
2.1.01	99.6067	33.4432	99.6151	33.4552	99.5922	33.1569	99.6178	33.3942
2.1.02	99.6124	33.3608	99.6094	33.2856	99.6037	33.3244	99.6174	33.4769
2.1.03	99.5991	33.4842	99.6071	33.4814	99.6002	33.8384	99.6174	33.4620
2.1.04	91.5630	33.4259	99.6063	33.4303	99.5945	34.0275	99.6105	33.4091
2.1.05	99.6170	33.4075	99.6220	33.4450	99.5819	33.4762	99.6052	33.4360
2.1.06	99.6120	33.3806	99.6014	33.2898	99.6136	33.3536	99.6353	33.4303
2.1.07	99.6037	33.4300	99.6155	33.5428	99.6075	33.4501	99.6017	33.4236
2.1.09	99.6109	33.4085	99.6136	33.4369	99.6185	33.5017	91.3654	33.4964
2.1.11	99.6132	33.4285	99.6365	33.4243	99.6235	33.4982	99.6029	33.5198
2.1.12	99.6113	33.4545	99.5975	33.4603	99.5998	33.4481	99.6050	33.4219
2.2.01	99.6037	33.1558	99.6123	33.5075	99.6072	33.4151	99.6082	33.1508
2.2.02	99.5995	33.4535	99.6078	33.4754	99.6222	33.4520	99.6045	33.4989
2.2.03	99.6165	33.4501	99.6117	33.4380	99.6040	32.3599	99.6094	33.4693
2.2.04	99.6012	32.5897	99.6185	33.4440	99.6007	33.4532	99.6108	32.6028
2.2.05	99.6098	33.4643	99.6037	33.1194	99.6105	33.4506	99.6110	33.4417
2.2.06	99.6011	33.4561	99.6127	33.4680	99.6164	32.6058	99.6119	33.4718
2.2.07	99.6084	33.3969	99.6050	33.4752	99.6046	33.4423	99.6169	32.6862
2.2.08	99.6121	33.3636	99.6013	33.4908	99.6079	33.3273	99.6078	33.4151
2.2.09	99.6268	33.4808	99.6086	33.4612	95.3673	33.7231	99.6178	33.4562
2.2.11	99.5997	33.5541	99.6061	32.4152	99.6091	33.4969	99.6140	33.4283

security algorithm should be highly sensitive, which means that if there is a slight change in the key or plain-image information during encryption or decryption, it will have a huge impact on the result of the subsequent encryption.

4.6.1. Analysis of key sensitivity

Key sensitivity is analyzed ciphertext obtained when encrypting the same image using two slightly different keys. In this section, we encrypt the plain-image by using the original key, which defined as key, and the scrambling key, which defined as $key + 10^{-12}$, $key + 10^{-13}$, $key + 10^{-14}$, $key + 10^{-15}$, respectively. Then, compare the difference between the encrypted ciphertexts by calculating the NPCR and UACI, defined as shown in Eq. (12). The results are shown in Table 8, and we can find that the difference between the two cipher-images is very large when the scrambling is added to the key, and their NPCR and UACI values are very close to the ideal values of 99.6094% and 33.4635%.

4.6.2. Analysis of plaintext sensitivity

The plaintext sensitivity is the degree of change in the corresponding ciphertext when changing the pixels of the plaintext. If the algorithm lacks plaintext sensitivity, an attacker is likely to decipher the algorithm by analyzing the difference between the plaintext and ciphertext pairs. Therefore, the algorithm's plaintext sensitivity is the key to its resistance to plaintext attacks. In this section, we analyze the sensitivity of the proposed algorithm to the plain-image by adding 1 to the pixel values of the plain-image at $(H/4, W/4)$, $(H/4, W/2)$, $(H/2, W/4)$ and $(H/2, W/2)$. The results can be obtained by comparing the NPCR and UACI values. The results are shown in Table 9. From the experimental results, it can be seen that the NPCR between the ciphertext and the original ciphertext is very close to the ideal value of 99.6094%, and the UACI is also very close to the ideal value of 33.4635%. This indicates that the cipher-image has undergone significant changes, making it impossible for the attacker to crack the algorithm by comparing the differences between the ciphertexts. Therefore, the algorithm proposed in this paper is sufficient to resist plaintext attacks.

5. Conclusions

Aiming at the problem of information security of UAV remote sensing images in the future, this paper proposes a face privacy protection technology scheme based on 2D-DMHM chaotic system and DNA coding. Different from the complete encryption of the whole image, this paper uses face detection technology to extract the face part matrix including sensitive information as the object of selective encryption, so as to improve the efficiency of privacy protection. The encryption scheme performs RGB permutation and zigzag interleaved scrambling, DNA encoding encryption, discontinuous diffusion and lightweight bit-level confusion in turn. At the same time, the chaotic sequences adopted in these encryption modules all realize plaintext association or intermediate ciphertext association, so they can effectively resist the chosen-plaintext attack. The experimental results and theoretical analysis show that the face image encryption algorithm has excellent characteristics in histogram, adjacent pixel correlation, information entropy, encrypted image quality, etc., and has a large key space and can effectively resist various attacks. Therefore, the face detection and encryption algorithm reported in this paper is the preferred technical scheme in the future UAV remote sensing communication. In the future work, based on the existing simulation analysis results, we will further consider the technical implementation and experimental verification of the actual scene of remote sensing communication.

CRediT authorship contribution statement

Heping Wen: Software, Funding acquisition. **Zhiyu Xie:** Conceptualization, Methodology, Investigation, Data curation, Writing – original draft preparation, Writing – review and editing. **Zhuxi Wu:** Visualization. **Yiting Lin:** Investigation, Writing – original draft preparation, Writing – review and editing, Visualization, Supervision, Project administration. **Wei Feng:** Validation, Formal analysis, Resources.

Acknowledgment

This work was supported in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2023A1515011717, and in part by Project for Zhongshan Science and Technology under Grant 2021B2062, and in part by Special Projects for Key Fields of the Education Department of Guangdong Province under Grant 2023ZDZX1041.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Adleman, L.M., 1994. Molecular computation of solutions to combinatorial problems. Science 266 (5187), 1021–1024.

Araghi, T.K., Manaf, A.A., 2019. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. Future Gener. Comput. Syst. 101, 1223–1246.

Ariatmanto, D., Ernawan, F., 2022. Adaptive scaling factors based on the impact of selected dct coefficients for image watermarking. J. King Saud. Univ. Comput. Inf. Sci. 34 (3), 605–614.

Banerjee, M., Ghosh, S., Manfredi, P., d'Onofrio, A., 2023. Spatio-temporal chaos and clustering induced by nonlocal information and vaccine hesitancy in the SIR epidemic model. Chaos Solitons Fractals 170, 113339.

Chai, X., Fu, J., Gan, Z., Lu, Y., Zhang, Y., 2022a. An image encryption scheme based on multi-objective optimization and block compressed sensing. Nonlinear Dynam. 108 (3), 2671–2704.

Chai, X., Fu, J., Gan, Z., Lu, Y., Zhang, Y., Han, D., 2023. Exploiting semi-tensor product compressed sensing and hybrid cloud for secure medical image transmission. IEEE Internet Things J. 10 (8), 7380–7392.

Chai, X., Wang, Y., Chen, X., Gan, Z., Zhang, Y., 2022b. TPE-GAN: Thumbnail preserving encryption based on GAN with key. IEEE Signal Process. Lett. 29, 972–976.

Chai, X., Wang, Y., Gan, Z., Chen, X., Zhang, Y., 2022c. Preserving privacy while revealing thumbnail for content-based encrypted image retrieval in the cloud. Inform. Sci..

Gao, S., Wu, R., Wang, X., Liu, J., Li, Q., Tang, X., 2023. EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory. Inform. Sci. 621, 766–781.

Hadi, H.J., Cao, Y., Nisa, K.U., Jamil, A.M., Ni, Q., 2023. A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs. J. Netw. Comput. Appl. 213, 103607.

K.U., S., Mohamed, A., 2020. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Appl. Soft Comput. 90, 106162.

Lai, Q., Liu, Y., Yang, L., 2023a. Image encryption using memristive hyperchaos. Appl. Intell..

Lai, Q., Liu, Y., Yang, L., 2023b. Image encryption using memristive hyperchaos. Appl. Intell. 53 (19), 22863–22881.

Li, C., Feng, B., Li, S., Kurths, J., Chen, G., 2019. Dynamic analysis of digital chaotic maps via state-mapping networks. IEEE Trans. Circuits Syst. I. Regul. Pap. 66 (6), 2322–2335.

Li, C., Tan, K., Feng, B., Lv, J., 2022. The graph structure of the generalized discrete arnold's cat map. IEEE Trans. Comput. 71 (2), 364–377.

Li, C., Yang, X., 2022. An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. Optik 260, 169042.

Liu, L., Zhang, Q., Wei, X., 2012. A RGB image encryption algorithm based on DNA encoding and chaos map. Comput. Electr. Eng. 38 (5), 1240–1248, Special issue on Recent Advances in Security and Privacy in Distributed Communications and Image processing.

Lu, X., Xie, E.Y., Li, C., 2023. Periodicity analysis of logistic map over ring $\mathbb{Z}_{3^n}$. Int. J. Bifurcation Chaos 33 (05), 2350063.

Ma, Y., Li, C., Ou, B., 2020. Cryptanalysis of an image block encryption algorithm based on chaotic maps. J. Inf. Secur. Appl. 54, 102566.

Mansouri, A., Wang, X., 2021. A novel block-based image encryption scheme using a new Sine powered chaotic map generator. Multimedia Tools Appl. 80 (14), 21955–21978.

Melman, A., Evsutin, O., 2023. Comparative study of metaheuristic optimization algorithms for image steganography based on discrete Fourier transform domain. Appl. Soft Comput. 132, 109847.

Murillo-Escobar, M., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R., Acosta Del Campo, O., 2015. A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Process. 109, 119–131.

Singh, R.K., Kumar, B., Shaw, D.K., Khan, D.A., 2021. Level by level image compression-encryption algorithm based on quantum chaos map. J. King Saud. Univ. Comput. Inf. Sci. 33 (7), 844–851.

Sisaudia, V., Vishwakarma, V.P., 2022. A secure gray-scale image watermarking technique in fractional dct domain using zig-zag scrambling. J. Inf. Secur. Appl. 69, 103296.

Vikas, Parhi, D.R., 2023. Chaos-based optimal path planning of humanoid robot using hybridized regression-gravity search algorithm in static and dynamic terrains. Appl. Soft Comput. 140, 110236.

Wang, X., Liu, C., Jiang, D., 2021. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. Inform. Sci. 574, 505–527.

Wang, M., Wang, X., Wang, C., Xia, Z., Zhao, H., Gao, S., Zhou, S., Yao, N., 2020. Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption. Chaos Solitons Fractals 139, 110028.

Wei, D., Jiang, M., Deng, Y., 2023. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. Expert Syst. Appl. 213, 119074.

Wen, H., Chen, R., Yang, J., Zheng, T., Wu, J., Lin, W., Jian, H., Lin, Y., Ma, L., Liu, Z., Zhang, C., 2023a. Security analysis of a color image encryption based on bit-level and chaotic map. Multimedia Tools Appl..

Wen, H., Chen, Z., Zheng, J., Huang, Y., Li, S., Ma, L., Lin, Y., Liu, Z., Li, R., Liu, L., Lin, W., Yang, J., Zhang, C., Yang, H., 2022a. Design and embedded implementation of secure image encryption scheme using DWT and 2D-LASM. Entropy 24 (10).

Wen, H., Huang, Y., Lin, Y., 2023b. High-quality color image compression-encryption using chaos and block permutation. J. King Saud. Univ. - Comput. Inf. Sci. 101660.

Wen, H., Lin, Y., 2023. Cryptanalyzing an image cipher using multiple chaos and DNA operations. J. King Saud Univ. Comput. Inf. Sci. 35 (7), 101612.

Wen, H., Lin, Y., 2024. Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding. Expert Syst. Appl. 237, 121514.

Wen, H., Lin, Y., Xie, Z., Liu, T., 2023c. Chaos-based block permutation and dynamic sequence multiplexing for video encryption. Sci. Rep. 13 (1).

Wen, H., Liu, Z., Lai, H., Zhang, C., Liu, L., Yang, J., Lin, Y., Li, Y., Liao, Y., Ma, L., Chen, Z., Li, R., 2022b. Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. Mathematics 10 (17).

Wen, H., Wu, J., Ma, L., Liu, Z., Lin, Y., Zhou, L., Jian, H., Lin, W., Liu, L., Zheng, T., Zhang, C., 2023d. Secure optical image communication using double random transformation and memristive chaos. IEEE Photonics J. 15 (1), 1–11.

Xiang, Y., Xiao, D., Zhang, R., Liang, J., Liu, R., 2021. Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer. Inform. Sci. 545, 188–206.

Xie, H., Lu, J., Han, J., Zhang, Y., Xiong, F., Zhao, Z., 2023. Fourier coded aperture transform hyperspectral imaging system. Opt. Lasers Eng. 163, 107443.

Yu, F., Gong, X., Li, H., Wang, S., 2021. Differential cryptanalysis of image cipher using block-based scrambling and image filtering. Inform. Sci. 554, 145–156.

Zhang, Y., Zhao, R., Xiao, X., Lan, R., Liu, Z., Zhang, X., 2022a. HF-TPE: High-fidelity thumbnail- preserving encryption. IEEE Trans. Circuits Syst. Video Technol. 32 (3), 947–961.

Zhang, Y., Zhou, W., Zhao, R., Zhang, X., Cao, X., 2022b. F-TPE: Flexible thumbnail-preserving encryption based on multi-pixel sum-preserving encryption. IEEE Trans. Multimed. 1–15.

Zhao, R., Zhang, Y., Wen, W., Lan, R., Xiang, Y., 2023. E-TPE: Efficient thumbnail-preserving encryption for privacy protection in visual sensor networks. ACM Trans. Sen. Netw..

Zhou, Y., Bao, L., Chen, C.P., 2014. A new 1D chaotic system for image encryption. Signal Process. 97, 172–182.