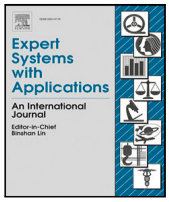
Expert Systems With Applications 237 (2024) 121514

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa



Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding

Heping Wen *, Yiting Lin

University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

ARTICLE INFO

Keywords:
Image encryption
Quantum chaotic map
Chaotic encryption
Cryptanalysis
DNA coding

ABSTRACT

Recently, an image encryption algorithm using Quantum Chaotic Map and DNA Coding (QCMDC-IEA) has been reported. It consists of two main components: pixel-level permutation and DNA domain substitution. To support its ability to withstand various attacks, several security analyses and experimental simulations were presented. However, after careful cryptanalysis, we found that QCMDC-IEA has inherent fatal security problems. Although formally using complex chaos and DNA encoding, the chaos-based sequences used for encryption in QCMDC-IEA are independent of a plain image such that it suffers from the defect of the existence of an equivalent key. Moreover, the lack of confusion and diffusion in DNA domain encryption makes it vulnerable to cryptographic attacks. DNA domain encryption is then essentially a 2-bit data substitution process, so it can be equivalently simplified. On this basis, we propose an attack method to crack QCMDC-IEA, which first obtains an equivalent permutation key by differential cryptanalysis, and then eliminates the DNA domain substitution based on a chosen-plaintext attack using only four special plain images and their corresponding cipher images, and finally recovers the original plain images. Our attack method takes full advantage of the security defects in QCMDC-IEA and achieves complete decipherment with low complexity, thus better revealing its intrinsic security mechanism. To improve the security performance, some security enhancement suggestions are recommended for similar cryptosystems. Both theoretical analysis and experimental simulation results show that the proposed cryptographic attack method is effective and feasible for QCMDC-IEA with low attack complexity. Therefore, the cryptanalysis work in this paper can provide some theoretical hints for improving the security of a class of image encryption algorithms based on DNA coding and chaos.

1. Introduction

In the 21st century, with the popularity of social media such as Facebook, Twitter and WeChat, people increasingly rely on online communication to obtain information and communicate with others. As an important information carrier, the use frequency of digital images in online communication is also increasing (Jiang et al., 2020; Liang et al., 2023; Luo et al., 2023; Wu et al., 2023). Therefore, it is particularly critical to encrypt and protect sensitive digital images in network transmission (Chai et al., 2022; Liu et al., 2023a; Lu et al., 2023b; Zhang et al., 2021). In view of the inherent unique characteristics of the image (Bao et al., 2023; Cao et al., 2022; Ding et al., 2023; Liu et al., 2023b), such as the high redundancy of information, the increase of correlation between adjacent pixels and the large amount of data involved, the traditional text encryption algorithm is difficult to meet the performance requirements of today's secure transmission. In order to cope with this challenge, various new image encryption algorithms have been reported (Hu et al., 2022; Man et al., 2021, 2023; Teng et al., 2021). Among them, the introduction of DNA coding method (Chen et al., 2022, 2023; Zou et al., 2022) to enhance the security of image encryption technology is an important research direction. The main reason is that DNA computing has the advantages of built-in parallelism, minimum power consumption and huge storage capacity (Wen et al., 2023c, 2022b; Zou et al., 2022). In addition, chaos has attracted much attention due to its good pseudo-randomness, ergodicity and long-term unpredictability of orbits, which have many similarities with confusion, diffusion and avalanche effect in cryptography (Hua et al., 2023; Lai et al., 2022; Tang et al., 2023; Ye et al., 2023). Therefore, the design of image encryption algorithm combining DNA coding and chaos theory has attracted the attention of key experts and scholars, and has developed into an academic research hotspot (Chai et al., 2023; Gao et al., 2022; Jiang & Ding, 2023; Su et al., 2023; Zhang et al., 2022) today.

* 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), Dr.YitingLin@gmail.com (Y. Lin).

https://doi.org/10.1016/j.eswa.2023.121514
Received 4 June 2023; Received in revised form 3 September 2023; Accepted 7 September 2023
Available online 11 September 2023

In recent years, many new image encryption algorithms based on DNA coding and chaotic systems have been continuously reported (Wang & Zhao, 2021; Wen et al., 2023c, 2022b). In 2021, Wang and Zhao (2021) proposed a chaotic image encryption scheme that combines block permutation and DNA coding. This scheme utilizes SHA-512 hash function and plaintext image to generate initial values and parameters, employing sequences generated by the Chen hyperchaotic system for image permutation and diffusion. Experiments demonstrated the algorithm's robust encryption effectiveness and its ability to withstand various common attacks. In 2022, addressing security concerns in chaotic image encryption for Optical Access Networks, a color image encryption scheme (Wen et al., 2022b) is presented, combining non-degenerate discrete hyperchaotic systems and dynamic DNA encoding. A novel non-degenerate hyperchaotic system is introduced, generating a dynamic secret key through plaintext correlation. This key is then used for binary bit-planes permutation and subsequent DNA encoding, obfuscation, and decoding, resulting in a robust ciphertext. The algorithm successfully passes tests, resists common attacks, and demonstrates feasibility for secure communication technology in optical access networks. In 2023, a novel dynamic RNA-encoded color image encryption method (Wen et al., 2023c) is introduced, utilizing a chain feedback structure. RNA encoding is a variant of DNA encoding. This approach employs chaotic sequences for encryption, involving color component decomposition, RNA dynamic encoding, and chained encryption mechanisms, effectively countering cryptographic attacks as confirmed by experiments and security analysis. The proposed scheme demonstrates strong encryption capabilities and resistance against typical attacks. It can be seen that chaotic encryption based on this kind of biological genetic information coding has strong operability and timeliness, and the algorithm of biological genetic information coding has broad application prospects in cryptography (Li et al., 2021, 2023; Lu et al., 2023b).

Throughout the current digital image encryption algorithms combining DNA coding and chaotic systems, the commonly used technical path is to first use a more complex chaotic system to generate a sufficient number of chaotic encryption sequences, and use more dynamic and abundant DNA coding (Wang & Zhao, 2021; Wen et al., 2023c, 2022b). Finally, the numerical statistical results are used to prove its security. However, the security analysis results based on numerical statistics are only necessary conditions for the security algorithm, rather than sufficient conditions (Liu et al., 2022; Lu et al., 2023a; Wen et al., 2023a). In fact, some digital image encryption algorithms with excellent numerical statistics have been pointed out by cryptanalysis researchers as being unable to withstand selective plaintext attacks (Chen et al., 2020; Feng et al., 2021; Ma et al., 2020). In cryptography, cryptanalysis and cryptographic design are two complementary modules. Cryptographic design (Wen et al., 2023b; Zhou et al., 2023a, 2023b) is usually about proposing new cryptographic algorithms for certain problems and combining them with practical scenarios. While cryptanalysis (Lai et al., 2023; Wen et al., 2022a, 2023d) reveals the security problems in it from the attacker's perspective. Both of them motivate each other and promote the development of cryptography together. Therefore, it is especially necessary to implement systematic cryptanalysis for reported algorithms.

In this paper, we implement a cryptanalysis of the target algorithm (Zhang & Huo, 2019) named QCMDC-IEA. The target QCMDC-IEA is an image encryption algorithm that combines DNA coding and quantum chaotic mapping, which consists of two major modules: pixel-level permutation and DNA domain substitution. Compared with the same type of image ciphers, QCMDC-IEA mainly uses the following measures to improve security: First, differentiating from the single-rule encoding mechanism, it supports the dynamic selection of eight DNA coding and decoding and arithmetic rules, which improves the algorithmic complexity; Second, it employs two complex chaotic systems, which generates seven chaos-based encrypted sequences, thus enhancing security. However, from the cryptanalytic point of view, QCMDC-IEA is still insecure because of its inherent security flaws in terms of cryptographic structure. On the one hand, all chaos-based pseudo-random number sequences (PRNS) are independent of the plain image, leading to the existence of equivalent keys. On the other hand, pixel-level permutation and DNA-domain substitution can be used to obtain the corresponding equivalent keys through differential cryptanalysis and chosen-plaintext attacks, respectively. Thus, this paper proposes a cryptanalysis idea combining differential analysis and chosen-plaintext attack, which can achieve complete decipherment of QCMDC-IEA with low computational complexity.

The main contributions of this paper can be categorized as follows:

(1) To the best of our knowledge, this is the first report of a cryptographic attack on QCMDC-IEA that has resulted in a complete crack. In fact, it is quite difficult to be broken. Especially, the block diagram shown in Fig. 1 contains seven chaotic encrypted sequences or matrices $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, $\boldsymbol{d}$, $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$, which is difficult to be effective against using those attack methods presented in the available (Chen et al., 2020; Feng et al., 2021).

(2) After our cryptanalysis, we found that QCMDC-IEA suffers from two fatal security defects: the existence of an equivalent key, and the fact that the DNA domain encryption contains neither confusion nor diffusion. Purposefully, we propose an attack method that combines chosen-plaintext attack and differential analysis to achieve complete cracking with low complexity. Thus, the secure working mechanism of QCMDC-IEA is revealed at a deeper level.

(3) Based on the cryptanalysis in this paper, combined with the research foundation of cryptanalysis (Wen et al., 2023a; Wen & Lin, 2023), we give some recommendations for security enhancement. Therefore, the work in this paper can provide a theoretical reference basis for the security enhancement of a class of digital image encryption algorithms based on DNA coding and chaotic systems.

The rest of the paper is organized as follows: Section 2 briefly introduces the QCMDC-IEA; Section 3 gives the cryptanalysis of QCMDC-IEA; Section 4 gives the experimental simulation results; Section 5 presents suggestions for improvement of QCMDC-IEA; Section 6 concludes the paper.

2. Description of QCMDC-IEA

2.1. The adopted two chaotic systems

Zhang and Huo (2019) used two chaotic systems. One is the so-called quantum chaotic map, given as

$$\begin{cases} x_{n+1} = r(x_n - |x_n|^2) - ry_n \\ y_{n+1} = -y_n e^{-2\beta} + e^{-\beta} r\left[(2 - x_n - x_n^*)y_n - x_n z_n^* - x_n^* z_n\right] \\ z_{n+1} = -z_n e^{-2\beta} + e^{-\beta} r\left[2(1 - x_n^*)z_n - 2x_n y_n - x_n\right] \end{cases} \tag{1}$$

where x, y, z are the state variables and r, β are the control parameters. x^* and z^* are complex conjugates of x and z, respectively. The range of the parameters is $x \in (0,1), y \in (0,0.1), z \in (0,0.2)$, $x^* = x, z^* = z$, $\beta \in [6, +\infty)$ and $r \in [0,4]$. And the other is the classical chaotic system Lorenz, modeled by

$$\begin{cases} \dot{x} = a(x - y) \\ \dot{y} = -xz + bx - y \\ \dot{z} = xy - cz \end{cases} \tag{2}$$

where x, y, z are the state variables, and a, b, c are the control parameters respectively. When $(a, b, c) = (10, 28, 8/3)$, Eq. (2) is chaotic.

2.2. Basic principles of DNA coding

A DNA sequence consists of four distinguishable nucleic acid bases: A, T, C and G. With four bases to choose from, the total number of possible coding combinations is $4! = 24$. However, due to the principle of complementary base pairing, which states that A pairs with T and

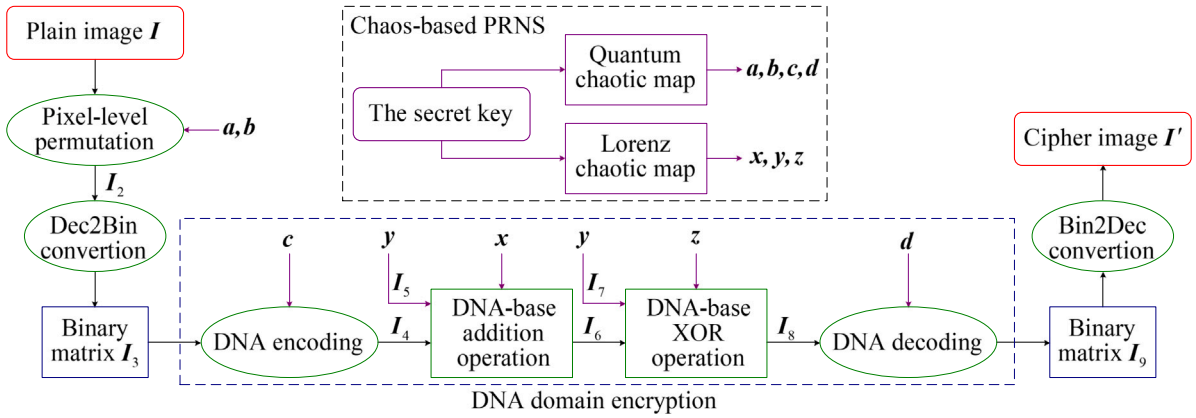


Fig. 1. The overall block diagram of QCMDC-IEA.

Table 1
DNA coding states under 8 rules.

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

Table 2
DNA addition operation by rule 1.

+	A	G	C	T
A	00	00	01	01
G	11	11	10	10
C	01	10	00	11
T	10	01	11	00

Table 3
DNA subtraction operation by rule 1.

−	A	G	C	T
A	00	00	01	01
G	11	11	10	10
C	01	10	00	11
T	10	01	11	00

Table 4
DNA XOR operation by rule 1.

XOR	A	G	C	T
A	00	00	01	01
G	11	11	10	10
C	01	10	00	11
T	10	01	11	00

C pairs with G, there are only eight possible coding combinations for DNA sequences (Wang & Zhao, 2021; Wen et al., 2023c, 2022b). The DNA encoding states under these eight rules are shown in Table 1. For the same decimal number, the result is different according to different encoding rules. For example, the binary form of an image pixel value of 156 is "10011100", and if rule 1 is selected, the DNA encoding result is "TCGA", while if rule 6 is followed, the result is "AGCT". In addition, common DNA coding operations include addition, subtraction, and XOR, and the operation states by rule 1 of Table 1 are shown in Tables 2, 3, and 4, respectively.

2.3. Description of QCMDC-IEA

Without loss of generality, the encryption objects are images of size $H \times W$ (height × width). Block diagram of QCMDC-IEA is illustrated as Fig. 1.

- **The secret key**
  As mentioned in Zhang and Huo (2019), QCMDC-IEA includes 17 key parameters. From the perspective of chaotic systems, the key parameters include the following two parts:
  - *Quantum chaotic map.* It consists of 14 key parameters. Specially the two control parameters (r, β), and four groups of initial values (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) and (x_4, y_4, z_4) of Eq. (1);
  - *Lorenz system.* It includes 3 key parameters, exactly the three initial values (x_0, y_0, z_0) of Eq. (2).

- **Chaos-based PRNS**
  Corresponding to the two chaotic systems, two PRNS sets are generated as follows.
  - *PRNS based on Quantum chaotic map.*

$$\begin{cases} \boldsymbol{a} = mod(fix(a_i \times 10_6), W) + 1, i = 1 \sim H \times 2 \\ \boldsymbol{b} = mod(fix(b_i \times 10_6), H) + 1, i = 1 \sim W \times 2 \\ \boldsymbol{c} = mod(fix(c_i \times 10_8), 8) + 1, i = 1 \sim H \times W \times 4 \\ \boldsymbol{d} = mod(fix(d_i \times 10_8), 8) + 1, i = 1 \sim H \times W \times 4 \end{cases} \tag{3}$$

  where $mod(.)$ is the modulo function, $fix(.)$ is a rounding function to zero. The four chaotic sequences $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, and $\boldsymbol{d}$ are generated by quantum chaotic map, and a_i, b_i, c_i and d_i are the elements of $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, and $\boldsymbol{d}$, respectively. Here, H and W are the height and width of the image, respectively.

  - *PRNS based on Lorenz system.* It includes 3 key parameters, exactly the three initial values (x_0, y_0, z_0) of Eq. (4).

$$\begin{cases} \boldsymbol{x} = mod(fix([abs(x) - fix(abs(x))] \times 10^{10}), 8) + 1 \\ \boldsymbol{y} = mod(fix([abs(y) - fix(abs(y))] \times 10^{10}), 2) + 1 \\ \boldsymbol{z} = mod(fix([abs(z) - fix(abs(z))] \times 10^{10}), 8) + 1 \end{cases} \tag{4}$$

  where $abs(.)$ is used to obtain the absolute value. Based on these operations, the contents of the sequences $x = \{x_1, x_2, \ldots, x_{H \times W \times 4}\}$ and $z = \{z_1, z_2, \ldots, z_{H \times W \times 4}\}$ are transformed into random numbers within 1 to 8. According to the value of the two sequences, the DNA addition and XOR rules are selected. The content of the sequence $y = \{y_1, y_2, \ldots, y_{H \times W \times 16}\}$ is transformed into random values that are equal to either 0 or 1 and are used to generate the natural DNA matrix.

- **Encryption steps**
  Fig. 1 illustrates the five primary stages involved in the encryption process of QCMDC-IEA, which are as follows: pixel-level permutation, DNA encoding, DNA addition operation, DNA XOR operation, and DNA decoding.

– **Stage 1.** Pixel-level permutation:
Use the sequences $\boldsymbol{a}$ and $\boldsymbol{b}$ to perform row and column permutation on a plain image $\boldsymbol{I}$, respectively, and then obtain the permuted image $\boldsymbol{I}_2$.
– **Stage 2.** DNA encoding:
Step 1. Convert the permuted image $\boldsymbol{I}_2$ of size $H \times W$ to the corresponding binary matrix $\boldsymbol{I}_3$ with size $H \times W \times 8$;
Step 2. Dynamically selects the DNA encoding rules by the sequence $\boldsymbol{c}$, and encode the binary matrix $\boldsymbol{I}_3$ as the DNA matrix $\boldsymbol{I}_4$ in size $H \times W \times 4$.
– **Stage 3.** DNA addition operation:
Step 1. Similar as Step 2 of Stage 2, encode the left half of sequence $\boldsymbol{y}$ into the DNA matrix $\boldsymbol{I}_5$;
Step 2. Dynamically selects the DNA addition rules by the sequence $\boldsymbol{x}$, and perform DNA-base addition operation on the two DNA matrices $\boldsymbol{I}_4$ and $\boldsymbol{I}_5$ to get the DNA matrix $\boldsymbol{I}_6$.
– **Stage 4.** DNA XOR operation:
Step 1. Similar as Step 1 of Stage 3, encode the right half of sequence $\boldsymbol{y}$ into the DNA matrix $\boldsymbol{I}_7$;
Step 2. Dynamically selects the DNA XOR rules by the sequence $\boldsymbol{z}$, and perform DNA-base XOR operation on the two DNA matrices $\boldsymbol{I}_6$ and $\boldsymbol{I}_7$ to get the DNA matrix $\boldsymbol{I}_8$.
– **Stage 5.** DNA decoding:
Step 1. Dynamically selects the DNA decoding rules by the sequence $\boldsymbol{d}$, and decode the DNA matrix $\boldsymbol{I}_8$ into the binary matrix $\boldsymbol{I}_9$;
Step 2. Convert the binary matrix $\boldsymbol{I}_9$ into the corresponding cipher image $\boldsymbol{I}'$.

3. Cryptanalysis of QCMDC-IEA

3.1. Common attack methods of cryptanalysis

In the field of cryptography, the well-recognized Kerckhoff hypothesis holds that the encryption algorithm of a secure cryptosystem is open to attackers, and only the key is unknown (Kerckhoffs, 1883). The four commonly used cryptanalysis methods from weak to strong are given as follows (Wen et al., 2023a; Wen & Lin, 2023):

- **Ciphertext-only attack**
Assuming that the attacker only obtains some ciphertext, by analyzing the statistical properties of the ciphertext, the attacker's goal is to determine the plaintext or key.
- **Known-plaintext attack**
Assuming that the attacker has partial plaintext and corresponding ciphertext, their goal is to solve or crack the corresponding key and encryption algorithm.
- **Chosen-plaintext attack**
It is assumed that the attacker can temporarily use the encryption machine, choose the plaintext that is conducive to deciphering, and obtain the corresponding ciphertext, thereby attacking the target algorithm.
- **Chosen-ciphertext attack**
It is assumed that the attacker can temporarily use the decryption machine, choose the ciphertext that is conducive to deciphering, and obtain the corresponding plaintext, thereby attacking the target algorithm.

3.2. Preliminary analysis of QCMDC-IEA

From Section 2 and Fig. 1, QCMDC-IEA includes two main parts, pixel-level permutation and DNA domain substitution. It belongs to a modification of the classical permutation-substitution structure, except that the substitution is based on the DNA domain. From the perspective of cryptanalysis, QCMDC-IEA has the following two security defects in the terms of cipher algorithm:

- **Security defect 1.** *The existence of an equivalent key*:
Observing Fig. 1, QCMDC-IEA has 7 chaotic sequences for encryption: $(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d})$ and $(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$. Obviously, they are independent of a plain image. In the event of a specified key, chaotic PRNS generated using chaos-based techniques remain identical even when used for different plain images with a similar size and type. As a consequence, PRNS based on chaos can be considered as equivalent and interchangeable keys. Once the attacker obtains these equivalent keys, the original algorithm can be deciphered without knowing the actual key.
- **Security defect 2.** *For a 2-bit-base matrix during the DNA domain encryption, neither confusion nor diffusion are performed between 2-bit-bases*:
DNA domain encryption part consists of DNA encoding, DNA-base addition operation, DNA XOR operation and DNA decoding. Its input and output and the binary matrix $\boldsymbol{I}_3$ and the binary matrix $\boldsymbol{I}_9$ with the same size $H \times W \times 8$. According to Table 1, DNA coding is based on 2-bit as the smallest unit. Thus, the encrypted object of the DNA domain encryption can be deemed as a 2-bit-base matrix of size $H \times W \times 4$. More precisely, the set of 2-bit-base elements for input and output is $00, 01, 10, 11$. Since there is no confusion mechanism, the encryption process between the elements of the 2-bit-base matrix is independent of each other. This also provides an important premise for the divide and conquer attack.

First of all, based on Security defect 1, one only needs to obtain the equivalent key to decipher QCMDC-IEA without knowing its actual secret key. Then, with Security defect 2, one can further obtain the equivalent keys by the divide-and-conquer attack strategy of the two main parts: pixel-level permutation and DNA domain substitution. Exactly, this paper firstly obtains the permutation matrix by differential analysis, and then eliminates the DNA domain encryption by chosen-plaintext attack.

3.3. Obtaining the permutation matrix by differential analysis

Following Security defect 2, QCMDC-IEA is obviously not sensitive to plain images. For two 2-bit-base plain matrices with only one element different, the corresponding two 2-bit-base ciphertext matrices have the same property, that is, only one element is different. Thus, if the attacker selects two plain images, only one 2-bit element at the same location is different, then the resulting two ciphertext images also have a 2-bit element with only one location. Moreover, this pair of positional relationships is actually an element of the permutation matrix. Based on this idea, the steps to obtain the permutation matrix using differential analysis are given as follows:

- **Step 1.** Select the all-zero plain image $\boldsymbol{P}_0$, and derive the corresponding cipher image $\boldsymbol{C}_0$;
- **Step 2.** Select HW special plain images $\boldsymbol{P}_n (n = 1, 2, \ldots, HW)$ and obtain their corresponding cipher images $\boldsymbol{C}_n (n = 1, 2, \ldots, HW)$, respectively;
- **Step 3.** Calculate the differences between $\boldsymbol{P}_n$ and $\boldsymbol{P}_0$ and the differences between $\boldsymbol{C}_n$ and $\boldsymbol{C}_0$, give by

$$\begin{cases} \Delta \boldsymbol{P}_n = (\boldsymbol{P}_n - \boldsymbol{P}_0) \bmod 256 \\ \Delta \boldsymbol{C}_n = (\boldsymbol{C}_n - \boldsymbol{C}_0) \bmod 256. \end{cases} \tag{5}$$

- **Step 4.** Determine the permutation matrix of size $H \times W$ by the results of these differences.

To better illustrate this process, let us take a simple example. In this example, we define $\boldsymbol{P}$ as plaintext and $\boldsymbol{C}$ as ciphertext. According to Fig. 1, we can see that I_3 and I_9 are intermediate ciphertexts through different encryption modules.

Firstly, one can get $\boldsymbol{P}_0$ and $\boldsymbol{C}_0$ by Step 1:

$$\boldsymbol{P}_0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \xrightarrow{Permutation} \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\xrightarrow{Dec2Bin} \boldsymbol{I}_3 = \begin{bmatrix} 00000000 & 00000000 \\ 00000000 & 00000000 \end{bmatrix}$$

$$\xrightarrow{Substitution} \boldsymbol{I}_9 = \begin{bmatrix} 00110001 & 11110110 \\ 00111100 & 01011011 \end{bmatrix}$$

$$\xrightarrow{Bin2Dec} \boldsymbol{C}_0 = \begin{bmatrix} 49 & 246 \\ 60 & 91 \end{bmatrix}.$$

Secondly, following Step 2, one obtains $\boldsymbol{P}_n$ and $\boldsymbol{C}_n$ for $1 \sim 4$, respectively:

$$\boldsymbol{P}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \xrightarrow{Permutation} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$$\xrightarrow{Dec2Bin} \boldsymbol{I}_3 = \begin{bmatrix} 00000000 & 00000000 \\ 00000001 & 00000000 \end{bmatrix}$$

$$\xrightarrow{Substitution} \boldsymbol{I}_9 = \begin{bmatrix} 00110001 & 11110110 \\ 00111110 & 01011011 \end{bmatrix}$$

$$\xrightarrow{Bin2Dec} \boldsymbol{C}_1 = \begin{bmatrix} 49 & 246 \\ 62 & 91 \end{bmatrix},$$

$$\boldsymbol{P}_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \xrightarrow{Permutation} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\xrightarrow{Dec2Bin} \boldsymbol{I}_3 = \begin{bmatrix} 00000000 & 00000000 \\ 00000000 & 00000001 \end{bmatrix}$$

$$\xrightarrow{Substitution} \boldsymbol{I}_9 = \begin{bmatrix} 00110001 & 11110110 \\ 00111100 & 01011001 \end{bmatrix}$$

$$\xrightarrow{Bin2Dec} \boldsymbol{C}_2 = \begin{bmatrix} 49 & 246 \\ 60 & 89 \end{bmatrix},$$

$$\boldsymbol{P}_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \xrightarrow{Permutation} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\xrightarrow{Dec2Bin} \boldsymbol{I}_3 = \begin{bmatrix} 00000001 & 00000000 \\ 00000000 & 00000000 \end{bmatrix}$$

$$\xrightarrow{Substitution} \boldsymbol{I}_9 = \begin{bmatrix} 00110011 & 11110110 \\ 00111100 & 01011011 \end{bmatrix}$$

$$\xrightarrow{Bin2Dec} \boldsymbol{C}_3 = \begin{bmatrix} 51 & 246 \\ 60 & 91 \end{bmatrix},$$

$$\boldsymbol{P}_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \xrightarrow{Permutation} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\xrightarrow{Dec2Bin} \boldsymbol{I}_3 = \begin{bmatrix} 00000000 & 00000001 \\ 00000000 & 00000000 \end{bmatrix}$$

$$\xrightarrow{Substitution} \boldsymbol{I}_9 = \begin{bmatrix} 00110001 & 11110100 \\ 00111100 & 01011011 \end{bmatrix}$$

$$\xrightarrow{Bin2Dec} \boldsymbol{C}_4 = \begin{bmatrix} 49 & 244 \\ 60 & 91 \end{bmatrix}.$$

Thirdly, get the corresponding difference results by Eq. (5) as below:

$$\Delta\boldsymbol{P}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \Delta\boldsymbol{P}_2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix},$$

$$\Delta\boldsymbol{P}_3 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \Delta\boldsymbol{P}_4 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

$$\Delta\boldsymbol{C}_1 = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, \Delta\boldsymbol{C}_2 = \begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix},$$

$$\Delta\boldsymbol{C}_3 = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}, \Delta\boldsymbol{C}_4 = \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}.$$

Based on the above results, by comparing the corresponding plaintext–ciphertext pairs, we can analyze the pixel-level permutation process. For example, by comparing $\Delta\boldsymbol{P}_1$ and $\Delta\boldsymbol{C}_1$, it is seen that the plaintext coordinates are (1, 1), and after permutation, the coordinates in the ciphertext are (2, 1). Similarly, for $\Delta\boldsymbol{P}_3$ and $\Delta\boldsymbol{C}_3$, the plaintext coordinates are (2, 1), and after permutation, the coordinates in the ciphertext are (1, 2). Therefore, we can find a matrix $\boldsymbol{w}$ for deciphering the pixel-level permutation as:

$$\boldsymbol{w} = \begin{bmatrix} (2,1) & (2,2) \\ (1,1) & (1,2) \end{bmatrix}.$$

3.4. Eliminating the DNA domain encryption by chosen-plaintext attack

Once the permutation matrix is obtained, QCMDC-IEA degenerates to a DNA domain-only encryption process. Subsequently, we will proceed to a discussion of the DNA domain encryption process. The DNA domain encryption process of the original algorithm is shown in the dashed line in Fig. 1. If we follow the common cryptanalysis method, we need to find all the used sequences $\boldsymbol{c}, \boldsymbol{d}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$. However, in the case of a large number of unknowns, this attack method may be very complicated or even impossible to obtain. To solve this problem, a new attack method is discussed in this paper, and for further simplification, Property 1 is given below.

Property 1. *For any 2-bit matrix of size $H \times 4$ W, the encryption of a DNA domain is performed in such a way that the DNA encoding and permutation operations satisfy the exchange law.*

Proof. For a simple instance, the two cases are shown below.

Case 1. First DNA encoding and then pixel-level permutation:

$$\begin{bmatrix} 00 & 01 \\ 10 & 11 \end{bmatrix} \xrightarrow{encoding} \begin{bmatrix} A & G \\ C & T \end{bmatrix} \xrightarrow{permutation} \begin{bmatrix} T & C \\ G & A \end{bmatrix}$$

Case 2. First pixel-level permutation and then DNA encoding:

$$\begin{bmatrix} 00 & 01 \\ 10 & 11 \end{bmatrix} \xrightarrow{permutation} \begin{bmatrix} 11 & 10 \\ 01 & 00 \end{bmatrix} \xrightarrow{encoding} \begin{bmatrix} T & C \\ G & A \end{bmatrix}$$

Obviously, the outputs of the two cases are exactly the same. Similarly, this rule applies to any other 2-bit matrix. □

Property 2. *During DNA domain encryption, there is a fixed correspondence between the 2-bit input and output at any position. Exactly speaking, it is a one-to-one corresponding value substitution relationship.*

Proof. Based on the security flaw 1 of QCMDC-IEA analyzed in Section 3.2, it can be seen that all chaotic sequences contained in the encryption phase are independent of the plain image. Thus, when employing a designated chaotic initial value key, the DNA domain encryption process enforces fixed rules, with no interaction between the elements of the 2-bit matrix encryption. As a result, the resulting output remains fixed for a specific input image. □

According to Property 2, DNA domain encryption can be broken by obtaining the correspondence between 2-bit input and output at all positions. This will greatly simplify the complexity of cryptanalysis without finding all chaotic sequences or keys.

3.5. The overall cryptanalysis for QCMDC-IEA

Based on the above analysis, we can obtain the equivalent matrix $\boldsymbol{w}$ for deciphering pixel-level permutation according to the method in Section 3.3, and eliminate the DNA domain encryption process by the method in Section 3.4. Therefore, we can obtain the overall cryptographic analysis block diagram for QCMDC-IEA, as shown in Fig. 2, and the specific steps of the cryptanalysis are given as below:

- **Step 1.** Choose four special plain images with pixel values of 0, 85, 170 and 255, and get the corresponding cipher images. The reason for selecting these four special images is that their corresponding binary are 00000000, 01010101, 101010101 and 11111111, respectively. Thus, they satisfy Properties 1 and 2 when converted;
- **Step 2.** Use Algorithm 1 to eliminate the DNA domain encryption. For a given cipher image $\boldsymbol{I}'$, after conversion into a binary matrix, the DNA domain substitution can be eliminated by Algorithm 1 proposed in Section 3.4.

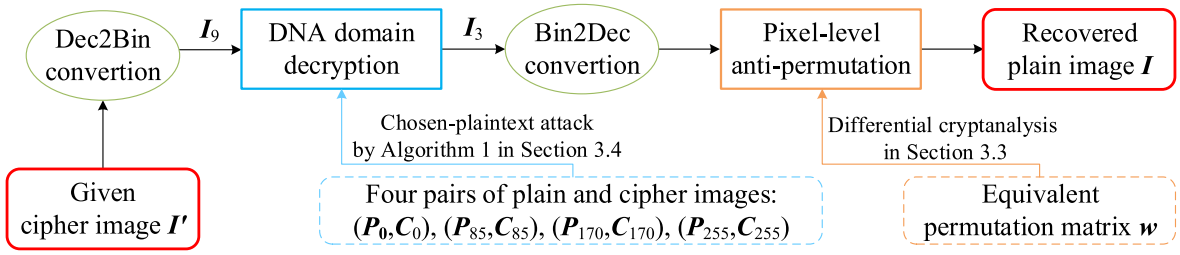


Fig. 2. The overall cryptographic analysis block diagram of QCMDC-IEA.

Algorithm 1: Eliminating DNA domain encryption process.

Input: Given cipher image C_{2-bit}, and the four cipher images $C^0_{2-bit}, C^{85}_{2-bit}, C^{170}_{2-bit}, C^{255}_{2-bit}$
Output: Recovered permuted image P'_{2-bit}

for $i \leftarrow 1$ *to* $4HW$ **do**
  if $C_{2-bit}(i) = C^0_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 00$;
  end
  else if $C_{2-bit}(i) = C^{85}_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 01$;
  end
  else if $C_{2-bit}(i) = C^{170}_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 10$;
  end
  else if $C_{2-bit}(i) = C^{255}_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 11$;
  end
end

- **Step 3.** The original plain image can be recovered by using the equivalent permutation matrix $\boldsymbol{w}$ determined in Section 3.3. Here, we solve for $\boldsymbol{w}$ requiring $HW+1$ selected plain images, where the all-0 images overlap with Step 1.

In summary, for an image of size HW, the number of selected plain images required by this cryptanalysis method is $HW+4$. Moreover, for any given cipher image, it can recover a version that is identical to the corresponding original plain image.

4. Experimental simulations for breaking QCMDC-IEA

To verify the effectiveness of our security analysis and the practicality of the proposed attack method, we performed experimental verification without altering the intended algorithm. Our experimental setup employed a PC host installed with MATLAB R2022a experimental software. The CPU deployed in the PC was an AMD Ryzen 9 5950X with a main frequency of 3.88 GHz and 64 GB of memory. The system's hard disk had a capacity of 8TB, and Windows 10 was selected as the operating system. The image data selected in the deciphering experiment is the same as the original paper (Zhang & Huo, 2019), which is also USC-SIPI.

4.1. Breaking experiment of the image used in original paper

In this experiment, in order to strictly simulate and restore the experimental process of Zhang and Huo (2019), we first select the grayscale "Lena" image and "Peppers" image with a size of 256 × 256 as the experimental target object, and use the QCMDC-IEA encryption machine to encrypt the above two plain images. The corresponding ciphertext images are shown in Fig. 3(c) and (g), and the corresponding histograms are shown in Fig. 3(d) and (h). The reason for selecting these two images is to maintain consistency with the objects analyzed in the original paper.

With the divide-and-conquer strategy, the operation process of the DNA domain in the QCMDC-IEA algorithm can be equivalent. Four special plain images $\boldsymbol{P}_0, \boldsymbol{P}_{85}, \boldsymbol{P}_{170}, \boldsymbol{P}_{255}$ with pixel value 0, pixel value 85, pixel value 170 and pixel value 255 are selected, as shown in Fig. 4(a)–(d). After encryption, four corresponding cipher images $\boldsymbol{C}_0, \boldsymbol{C}_{85}, \boldsymbol{C}_{170}, \boldsymbol{C}_{255}$ are obtained, as shown in Fig. 4(f)–(i), and the histograms of the four plaintext and four ciphertexts are shown in Fig. 4(e) and (j), respectively. According to the Algorithm 1 proposed in Section 3.4, the intermediate ciphertext replacement image can be obtained by operating on the cipher image Fig. 3(c). The result is shown in Fig. 5(a), and the corresponding histogram is shown in Fig. 5(b). The same method is applied to another ciphertext image Fig. 3(g), and the obtained intermediate ciphertext image and its corresponding histogram are shown in Fig. 5(c) and (d) respectively. After this step, it can be seen from the histogram that the pixel value of the obtained replacement image has returned to normal, and only the position of the original image pixels is disturbed, which indicates that the attack method used in Section 3.4 is effective.

Finally, we use the difference method proposed in Section 3.3 to generate the permutation matrix, and the restored plain image can be obtained. After the permutation matrix is obtained, because the encryption process in the algorithm is not associated with the plain image, the permutation process is determined only by the sequence generated by the pre-set chaotic initial values. Therefore, the same permutation matrix is used to operate the permutation image Fig. 5(a) and (c), and the corresponding decryption images can be obtained respectively. The results are shown in Fig. 6(a) and (c). Comparing the deciphered results with the original image, it can be confirmed that the cryptanalysis method proposed in this paper is reliable.

4.2. Algorithm deciphering experiment of general image

This section is concerned with selecting three distinct images of varying sizes to verify the efficiency and versatility of the cryptanalysis method proposed in this study. The first image is a binary image with dimensions of 256 × 256, followed by a pixel-valued gradient image of 512 × 512 and a person image of 1024 × 1024 dimensions. The intent behind utilizing these images is to assess the general applicability of the proposed cryptanalysis method. The QCMDC-IEA ciphertext images are shown in Fig. 7(a), (d), and (g), respectively. The DNA domain decryption images of QCMDC-IEA are shown in Fig. 7(b), (e), and (h), respectively. The recovered plain images of QCMDC-IEA are as shown in Fig. 7(c), (f), and (i), respectively. The experimental results show that the proposed cryptanalysis method is effective for any general image.

In addition, from the perspective of data complexity, given an 8-bit grayscale image with a size of H×W, the data complexity of the attack method required to destroy QCMDC-IEA is $\boldsymbol{O}(HW+4)$. Specifically, for 256 × 256 images, the data complexity is $\boldsymbol{O}(256 \times 256 + 4) = \boldsymbol{O}(65540)$. For images with size of 512 × 512, the data complexity is $\boldsymbol{O}(512 \times 512 + 4) = \boldsymbol{O}(262148)$. For images with size of 1024 × 1024, the data complexity is $\boldsymbol{O}(1024 \times 1024 + 4) = \boldsymbol{O}(1048580)$. All decoding times in this paper are shown in Table 5. Obviously, the required data

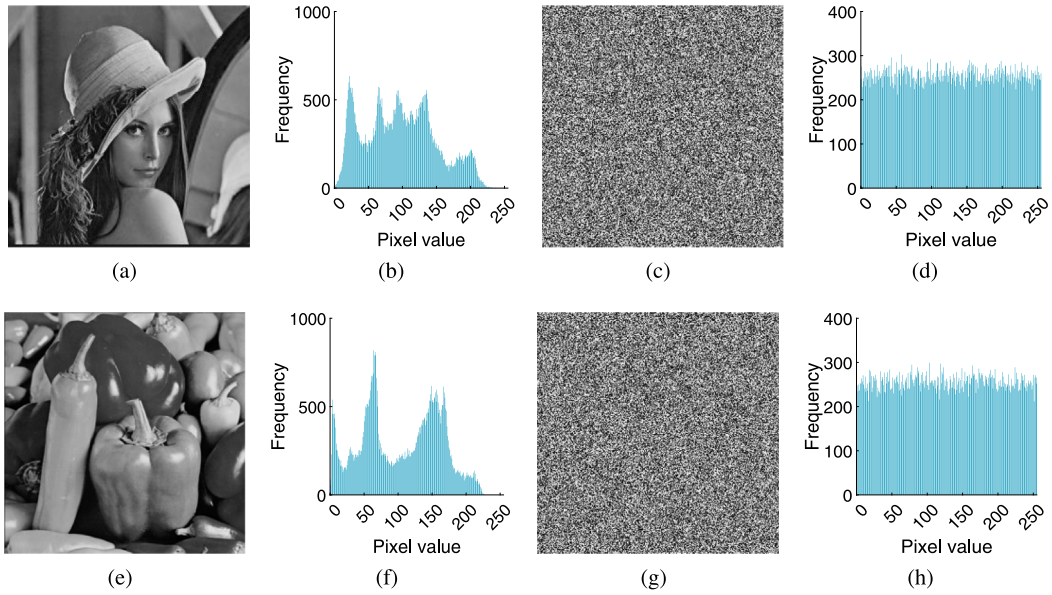


Fig. 3. This includes the plain image, the cipher image, and their respective histograms: (a) Plain image "Lena"; (b) Histogram of (a); (c) Cipher image of (a); (d) Histogram of (c); (e) Plain image "Peppers"; (f) Histogram of (e); (g) Cipher image of (e); (h) Histogram of (g).

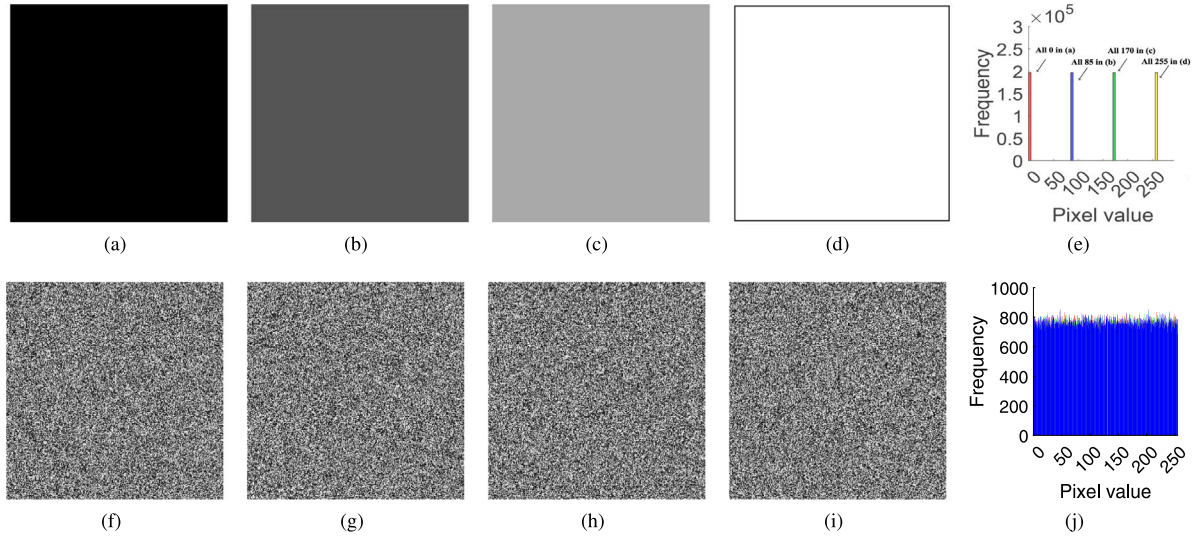


Fig. 4. This comprises chosen-plaintext images, their corresponding ciphertext images, and their respective histograms: (a) P_0; (b) P_{85}; (c) P_{170};(d) P_{255}; (e) Histogram of P;(f) C_0; (g) C_{85}; (h) C_{170}; (i) C_{255}; (j) Histogram of C.

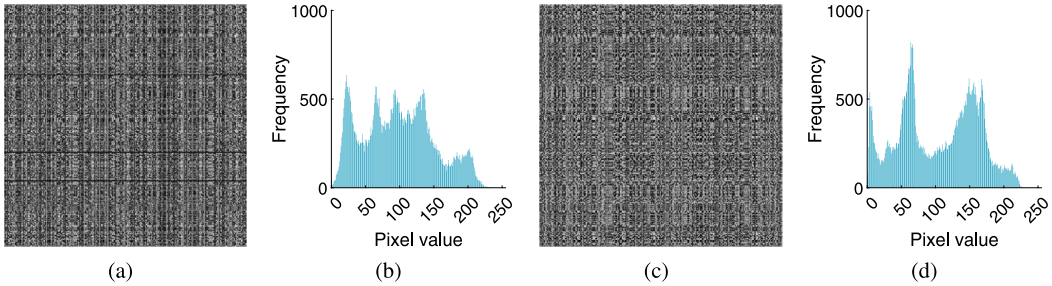


Fig. 5. Image after eliminating the DNA domain: (a) Permuted image of "Lena"; (b) Histogram of (a); (c) Permuted image of "Peppers"; (d) Histogram of (c).

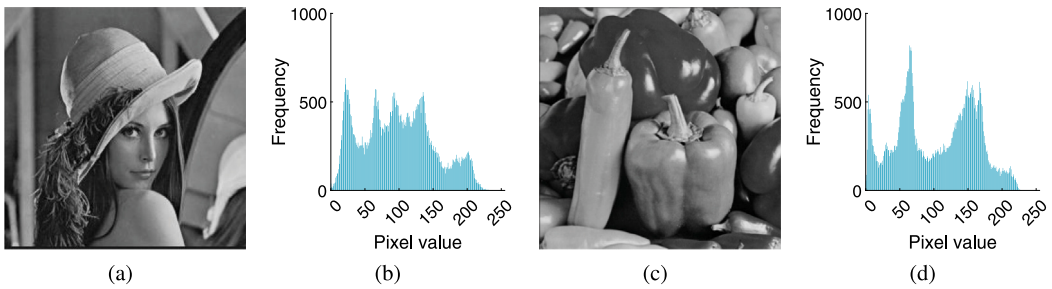


Fig. 6. Recovered plain image: (a) Recovered image of "Lena"; (b) Histogram of (a); (c) Recovered image of "Peppers"; (d) Histogram of (c).

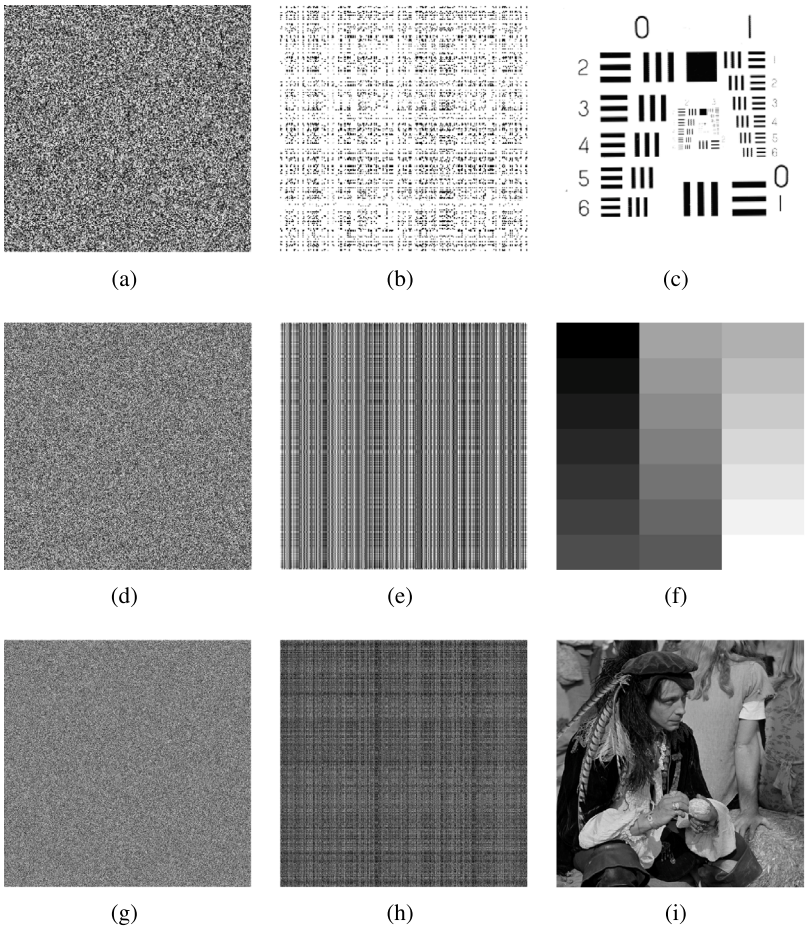


Fig. 7. Breaking results for three different size images: (a) Cipher image of size 256 × 256; (b) DNA domain breaking image of (a); (c) Recovered result of a; (d) Cipher image of size 512 × 512; (e) DNA domain breaking image of (d); (f) Recovered result of (d); (g) Cipher image of size 1024 × 1024; (h) DNA domain breaking image of (g); (i) Recovered result of (g).

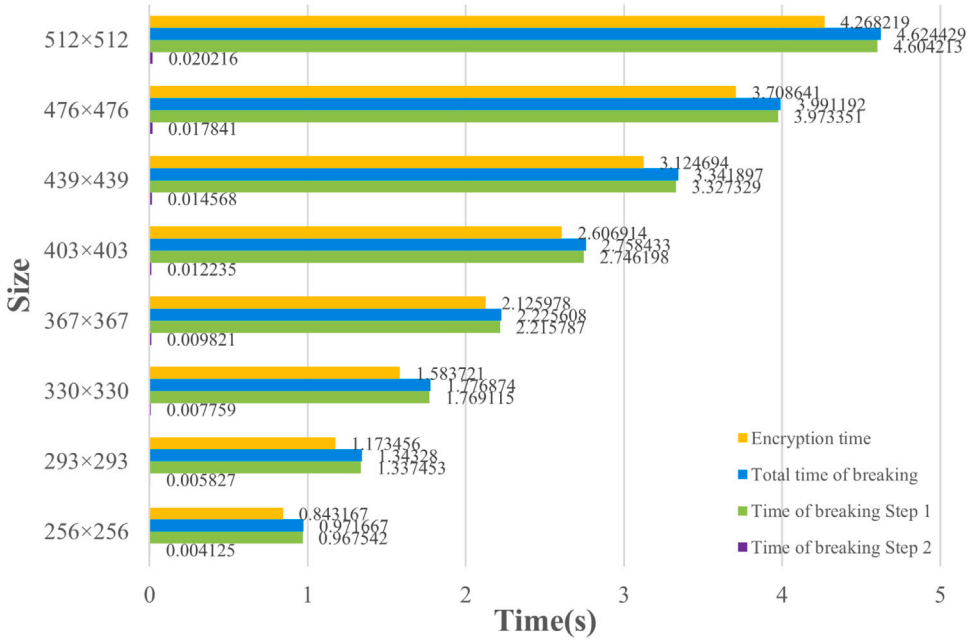
Table 5
Results of time statistics for breaking QCMDC-IEA.

Image selection	Image size	Encryption time (s)	Breaking time (s)		
			Step 1	Step 2	Total
Fig. 2(a)	256 × 256	0.865062	0.938043	0.003974	0.942017
Fig. 2(e)	256 × 256	0.892052	0.886710	0.003898	0.890608
Fig. 6(a)	256 × 256	0.864963	0.862339	0.003497	0.865836
Fig. 6(d)	512 × 512	4.271325	4.594403	0.020452	4.614855
Fig. 6(g)	1024 × 1024	23.362997	24.560158	0.445286	25.005444

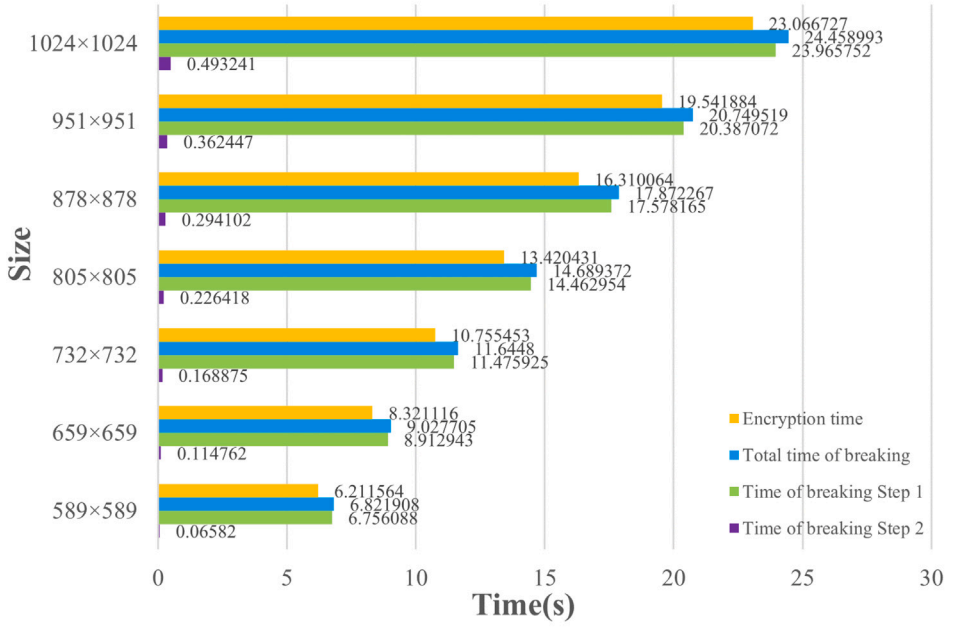
complexity is linear with the image size. The larger the image size, the higher the complexity, and vice versa. At the same time, in order not to lose generality, we randomly selected 100 grayscale images of different sizes, and carried out encryption and break experiments. The average encryption time and breaking time are shown in Fig. 8.

5. Suggestions for improvement

Based on the above analysis, it can be seen that QCMDC-IEA does not have the ability to resist the chosen-plaintext attack. Moreover, it is able to achieve complete decipherment with low complexity. In



(a)



(b)

Fig. 8. Statistical results of time to break QCMDC-IEA for different image sizes: (a) smaller size image; (b) larger size image.

fact, some other image encryption algorithms based on DNA coding and chaos suffer from similar security flaws (Wen et al., 2023a; Wen & Lin, 2023). To improve the security performance, the following security enhancement suggestions are recommended:

(1) Eliminating the existence of equivalent key.

Based on the cryptanalysis in this paper, it can be seen that one of the key reasons why QCMDC-IEA is completely decipherable is the existence of an equivalent key. As a result, the attacker does not need to solve the real key, but can realize the attack cracking only by obtaining the equivalent key. In order to solve this problem, it is suggested to consider enhancing the obfuscation and diffusion properties of cryptosystems so as to eliminate static dynamic keys.

(2) Performing a systematic cryptanalysis on DNA encoding.

DNA encoding is a widely adopted technique for digital image encryption in recent years, and although this approach incorporates bioinformatics theory, its practical contribution to security remains insufficient. The important reason lies in the defective research on the security mechanism of DNA encoding encryption algorithm, which

leads to its vulnerability to attacks. For this reason, it is recommended to conduct systematic fundamental research on DNA-encoded modules to reveal the extent of their security contribution to encryption algorithms.

(3) Improving the substantial contribution of complex chaotic systems to cryptography.

In QCMDC-IEA, complex chaos and a sufficient number of chaotic sequences are used for encryption. However, from the cryptanalysis results, it is not secure. In fact, the key reason why QCMDC-IEA can be cracked is not the chaos itself but the poor design of the algorithm. Therefore, it is recommended to pay more attention to the cryptographic security contribution of chaotic systems to the corresponding algorithms. Specifically, the degree of security contribution of chaos to cryptographic algorithms should be assessed from a cryptographic perspective, especially considering the perspective of a cryptographic attacker.

6. Conclusion

In this paper, an image cipher named QCMDC-IEA is cryptanalyzed comprehensively. QCMDC-IEA combines quantum chaotic maps and DNA coding, and is a symmetric cipher based on the permutation-substitution structure. However, due to its inherent security defects, the pixel permutation and DNA substitution of QCMDC-IEA can be broken respectively. We perform differential cryptanalysis to acquire an equivalent permutation key and use a chosen-plaintext attack method to equivalently eliminate DNA domain substitution via four pairs of special plain and cipher images. With low computational complexity, the original plain image can be recovered from a given cipher image. Through theoretical analysis and experimental simulation, we verify the feasibility and feasibility of the proposed attack method. Consequently, the cryptanalysis work presented in this study can serve as a valuable reference for designers seeking to enhance the security of image encryption technology through chaotic encryption. In the end, to avoid the security defects similar to the target algorithm in this paper, we give some suggestions on security enhancement for this kind of image encryption algorithm based on DNA coding and chaos. We hope that the work of this paper can provide some theoretical and practical reference for the design of secure image encryption algorithms.

CRediT authorship contribution statement

Heping Wen: Supervision, Project administration, Funding acquisition, Resources, Writing – original draft, Writing – review & editing. **Yiting Lin:** Conceptualization, Methodology, Software, Formal analysis, Writing – original draft, Writing – review & editing.

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.

Data availability

Data will be made available on request.

Acknowledgments

This work was supported in part by Guangdong Basic and Applied Basic Research Foundation, China under Grant 2023A1515011717, and in part by Project for Zhongshan Science and Technology, China under Grant 2021B2062.

References

Bao, B., Wang, Z., Hua, Z., Chen, M., & Bao, H. (2023). Regime transition and multi-scroll hyperchaos in a discrete neuron model. *Nonlinear Dynamics*, *111*(14), 13499–13512.

Cao, C., Cen, Z., Feng, X., Wang, Z., & Zhu, Y. (2022). Straightforward guess and determine analysis based on genetic algorithm. *Journal of Systems Science and Complexity*, *35*(5), 1988–2003.

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 of Things Journal*, *10*(8), 7380–7392.

Chai, X., Wang, Y., Chen, X., Gan, Z., & Zhang, Y. (2022). TPE-GAN: Thumbnail preserving encryption based on GAN with key. *IEEE Signal Processing Letters*, *29*, 972–976.

Chen, J., Chen, L., & Zhou, Y. (2020). Cryptanalysis of a DNA-based image encryption scheme. *Information Sciences*, *520*, 130–141.

Chen, L., Li, C., & Li, C. (2022). Security measurement of a medical communication scheme based on chaos and DNA coding. *Journal of Visual Communication and Image Representation*, *83*, Article 103424.

Chen, X., Mou, J., Cao, Y., Yan, H., & Jahanshahi, H. (2023). A chaotic color image encryption scheme based on improved arnold scrambling and dynamic DNA encoding. *Multimedia Tools and Applications*.

Ding, Y., Liu, W., Wang, H., & Sun, K. (2023). A new class of discrete modular memristors and application in chaotic systems. *The European Physical Journal Plus*, *138*(7).

Feng, W., Qin, Z., Zhang, J., & Ahmad, M. (2021). Cryptanalysis and improvement of the image encryption scheme based on feistel network and dynamic DNA encoding. *IEEE Access*, *9*, 145459–145470.

Gao, Z., Wu, Q., Liao, L., Su, B., Gao, X., Fu, S., Li, Z., Wang, Y., & Qin, Y. (2022). Experimental demonstration of synchronous privacy enhanced chaotic temporal phase en/decryption for high speed secure optical communication. *Optics Express*, *30*(17), 31209.

Hu, M., Li, J., & Di, X. (2022). Quantum image encryption scheme based on 2D $Sine^2$ - logistic chaotic map. *Nonlinear Dynamics*, *111*(3), 2815–2839.

Hua, Z., Liu, X., Zheng, Y., Yi, S., & Zhang, Y. (2023). Reversible data hiding over encrypted images via preprocessing-free matrix secret sharing. *IEEE Transactions on Circuits and Systems for Video Technology*, 1.

Jiang, Z., & Ding, Q. (2023). Second-order side-channel analysis based on orthogonal transform nonlinear regression. *Entropy*, *25*(3), 505.

Jiang, N., Zhao, A., Liu, S., Zhang, Y., Peng, J., & Qiu, K. (2020). Injection-locking chaos synchronization and communication in closed-loop semiconductor lasers subject to phase-conjugate feedback. *Optics Express*, *28*(7), 9477.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*, *9*(4), 5–38.

Lai, Q., Hu, G., Erkan, U. g., & Toktas, A. (2023). A novel pixel-split image encryption scheme based on 2D salomon map. *Expert Systems with Applications*, *213*, Article 118845.

Lai, Q., Zhang, H., Kuate, P. D. K., Xu, G., & Zhao, X.-W. (2022). Analysis and implementation of no-equilibrium chaotic system with application in image encryption. *Applied Intelligence*, *52*(10), 11448–11471.

Li, M., Wang, P., Yue, Y., & Liu, Y. (2021). Cryptanalysis of a secure image encryption scheme based on a novel 2D sine–cosine cross–chaotic map. *Journal of Real-Time Image Processing*, *18*(6), 2135–2149.

Li, H., Yu, S., Feng, W., Chen, Y., Zhang, J., Qin, Z., Zhu, Z., & Wozniak, M. (2023). Exploiting dynamic vector-level operations and a 2D-enhanced logistic modular map for efficient chaotic image encryption. *Entropy*, *25*(8), 1147.

Liang, X., Zhang, C., Luo, Y., Wang, X., & Qiu, K. (2023). Secure encryption and key management for OFDM-PON based on chaotic Hilbert motion. *Journal of Lightwave Technology*, *41*(6), 1619–1625.

Liu, S., Li, C., & Hu, Q. (2022). Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE MultiMedia*, *29*(1), 74–84.

Liu, W., Sun, K., He, S., & Wang, H. (2023). The parallel chaotification map and its application. *IEEE Transactions on Circuits and Systems. I. Regular Papers*, 1–10.

Liu, X., Sun, K., Wang, H., & He, S. (2023). A class of novel discrete memristive chaotic map. *Chaos, Solitons & Fractals*, *174*, Article 113791.

Lu, D., Li, M., Liao, Y., Tao, G., & Cai, H. (2023). Verifiable privacy-preserving queries on multi-source dynamic DNA datasets. *IEEE Transactions on Cloud Computing*, *11*(2), 1927–1939.

Lu, X., Xie, E. Y., & Li, C. (2023). Periodicity analysis of the logistic map over ring Z3n. *International Journal of Bifurcation and Chaos*, *33*(5), Article 2350063. http://dx.doi.org/10.1038/s41598-023-41082-9.

Luo, Y., Zhang, C., Wang, X., Liang, X., & Qiu, K. (2023). Robust key update with controllable accuracy using support vector machine for secure OFDMA-PON. *Journal of Lightwave Technology*, *41*(14), 4663–4671.

Ma, Y., Li, C., & Ou, B. (2020). Cryptanalysis of an image block encryption algorithm based on chaotic maps. *Journal of Information Security and Applications*, *54*, Article 102566.

Man, Z., Li, J., Di, X., Sheng, Y., & Liu, Z. (2021). Double image encryption algorithm based on neural network and chaos. *Chaos, Solitons & Fractals*, *152*, Article 111318.

Man, Z., Li, J., Di, X., Zhang, R., Li, X., & Sun, X. (2023). Research on cloud data encryption algorithm based on bidirectional activation neural network. *Information Sciences*, *622*, 629–651.

Su, Y., Wang, X., Xu, M., Zou, C., & Liu, H. (2023). A three-dimensional (3D) space permutation and diffusion technique for chaotic image encryption using merkel tree and DNA code. *Sensing and Imaging*, *24*(1).

Tang, Z., Chai, X., Lu, Y., Wang, B., & Tan, Y. (2023). An end-to-end screen shooting resilient blind watermarking scheme for medical images. *Journal of Information Security and Applications*, *76*, Article 103547.

Teng, L., Wang, X., Yang, F., & Xian, Y. (2021). Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. *Nonlinear Dynamics*, *105*(2), 1859–1876.

Wang, X., & Zhao, M. (2021). An image encryption algorithm based on hyperchaotic system and DNA coding. *Optics and Laser Technology*, *143*, Article 107316.

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

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. (2022). Design and embedded implementation of secure image encryption scheme using DWT and 2D-LASM. *Entropy*, *24*(10), 1332.

Wen, H., Huang, Y., & Lin, Y. (2023). High-quality color image compression-encryption using chaos and block permutation. *Journal of King Saud University - Computer and Information Sciences*, *35*(8), Article 101660.

Wen, H., Kang, S., Wu, Z., Lin, Y., & Huang, Y. (2023). Dynamic RNA coding color image cipher based on chain feedback structure. *Mathematics*, *11*(14), 3133.

Wen, H., & Lin, Y. (2023). Cryptanalyzing an image cipher using multiple chaos and DNA operations. *Journal of King Saud University - Computer and Information Sciences*, *35*(7), Article 101612.

Wen, H., Liu, Z., Lai, H., Zhang, C., Liu, L., Yang, J., Lin, Y., Li, Y., Liao, Y., Ma, L., Chen, Z., & Li, R. (2022). Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. *Mathematics*, *10*(17), 3180.

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

Wu, T., Zeng, W., Liu, Y., Song, S., Zhao, L., Chen, C., Zhang, C., & Guo, L. (2023). Secure turbulence-resistant coherent free-space optical communications via chaotic region-optimized probabilistic constellation shaping. *Optics Letters*, *48*(3), 684–687.

Ye, G., Liu, M., Yap, W.-S., & Goi, B.-M. (2023). Reversible image hiding algorithm based on compressive sensing and deep learning. *Nonlinear Dynamics*, *111*(14), 13535–13560.

Zhang, Y.-Q., Huang, H.-F., Wang, X.-Y., & Huang, X.-H. (2021). A secure image encryption scheme based on genetic mutation and MLNCML chaotic system. *Multimedia Tools and Applications*, *80*(13), 19291–19305.

Zhang, J., & Huo, D. (2019). Image encryption algorithm based on quantum chaotic map and DNA coding. *Multimedia Tools and Applications*, *78*(11), 15605–15621.

Zhang, Y., Zhou, W., Zhao, R., Zhang, X., & Cao, X. (2022). F-TPE: Flexible thumbnail-preserving encryption based on multi-pixel sum-preserving encryption. *IEEE Transactions on Multimedia*, 1–15.

Zhou, S., Qiu, Y., Wang, X., & Zhang, Y. (2023). Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. *Nonlinear Dynamics*, *111*(10), 9571–9589.

Zhou, S., Wang, X., & Zhang, Y. (2023). Novel image encryption scheme based on chaotic signals with finite-precision error. *Information Sciences*, *621*, 782–798.

Zou, C., Wang, X., Zhou, C., Xu, S., & Huang, C. (2022). A novel image encryption algorithm based on DNA strand exchange and diffusion. *Applied Mathematics and Computation*, *430*, Article 127291.