Journal of King Saud University – Computer and Information Sciences 35 (2023) 101612

HOSTED BY

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

Cryptanalyzing an image cipher using multiple chaos and DNA operations

Heping Wen *, Yiting Lin

School of Electronic and Information Engineering, 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

Article history:
Received 12 April 2023
Revised 10 May 2023
Accepted 3 June 2023
Available online 14 June 2023

Keywords:
Image encryption
Chaos
DNA coding
Cryptanalysis

ABSTRACT

Recently, an improved color image cipher (ICIC-DNA) based on multiple deoxyribonucleic acid (DNA) sequence operations with DNA synthetic image and chaos was proposed. ICIC-DNA features the use of multiple chaotic systems and diverse DNA operations. However, after our careful cryptanalysis, we found that ICIC-DNA has several fatal security flaws. First, despite the use of multiple chaotic systems, the corresponding encryption sequences are independent of the plaintext, such that equivalent keys exist. Second, the diverse DNA operation is essentially a 2-bit data substitution process, and thus can be equivalently simplified. Third, ICIC-DNA includes substitution and permutation of DNA domains, and based on the equivalent simplification operation, the substitution and permutation can be attacked separately. Based on these, we propose a chosen-plaintext attack method to attack ICIC-DNA. Differential analysis is firstly adopted to break the DNA-base permutation process, and then the DNA domain encryption is eliminated, and finally the equivalent key is used to achieve complete cracking. Theoretical analysis and experimental results show that the proposed attack method is effective and has low computational complexity and data complexity.

1. Introduction

Nowadays, with the popularity of social platforms such as Facebook, Twitter and Wechat, multimedia digital information, especially images, are used more and more frequently in people's daily life and work. Correspondingly, the privacy protection of images becomes particularly important. Due to the unique features of the image, such as the high correlation of adjacent pixels, the encryption protection using the traditional text encryption algorithm cannot meet the efficiency requirements. To fulfill this challenge, many methodologies (Li et al., 2022; Liu et al., 2020; Chai et al., 2022; Hua et al., 2022; Wen et al., 2022; Hua et al., 2021) have been introduced for designing more promising image ciphers. Among them, image encryption technology based on chaos theory and deoxyribonucleic acid (DNA) coding is a hot topic in recent years. Many such image encryption algorithms (Wen et al., 2022; Wang and Su, 2021) have been proposed. However, current research (Chai et al., 2021; Bao et al., 2019; Ali and Ali, 2022; Wu et al., 2021; Wen et al., 2021; Wen et al., 2023) focuses more on chaotic cryptographic algorithm design only, neglecting the corresponding cryptanalysis. This has also led to some algorithms (Liu et al., 2022; Wen et al., 2021; Chen et al., 2021; Shi et al., 2022) having security flaws that are not resistant to cryptanalysis attacks. From the perspective of practical security, cryptanalysis of the designed algorithm is more important than cryptographic algorithm design.

In the last decade, the design and security analysis of a class image ciphers based on DNA and chaos are discussed enthusiastically (Wang and Zhao, 2021; Cun et al., 2021; Farah et al., 2020). In 2010, the earliest research articles (Zhang et al., 2010) introduced DNA encoding for the first time in chain image encryption and further created an image cipher using DNA addition and substitution. Yet, in 2013, Ref. (Hermassi et al., 2014) pointed out that the

* Corresponding author at: School of Electronic and Information Engineering, 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).

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2023.101612
1319-1578/

cipher presented in Ref. (Zhang et al., 2010) has design defects and is insecure against chosen-plaintext attacks. As summarized in Ref. (Zhang et al., 2019; Liu et al., 2014), these decipherable ciphers share a number of common characteristics, including (1) a single DNA encoding and manipulation rule; (2) a small number of chaos-based key streams for encryption.

To address the problem of inadequate security performance of such cryptographic systems, various security enhancement mechanisms have been introduced and discussed. In 2015, Ref. (Song and Qiao, 2015) proposed an image encryption algorithm based on DNA coding and spatiotemporal chaos, traversing eight rules of DNA coding to enhance security. Unfortunate, after our preliminary cryptology research in 2019, we found that this algorithm is secure (Wen et al., 2019). Moreover, this cipher is not able to resist either chosen-plaintext or chosen-ciphertext attacks, and the complexity required for the attack is very low. In fact, the results of cryptanalysis for similar chaotic image ciphers show that many of them currently still lack provable security (Wen et al., 2021). These studies and reports above foreshadow that even the latest DNA and chaos-based image encryption algorithms have security performance pitfalls. Therefore, the security mechanism of such image encryption algorithms still needs to be studied more systematically and deeply.

In this paper, we performed a rigorous and detailed cryptanalysis on a recently proposed (Kalpana and Murali, 2015) improved color image cipher named ICIC-DNA. In 2015, J Kalpana et al. proposed an improved color image cipher in Ref. (Kalpana and Murali, 2015), which is based on multiple DNA sequence operations with DNA synthetic image and chaos. Compared with Ref. (Liu et al., 2012; Zhang et al., 2019; Zhang and Wei, 2019), it enhances security in two aspects: (1) using diverse DNA operations to enhance the complex nature of the encoding; (2) introducing multiple chaotic systems to generate more key-streams for encryption. However, after our careful cryptanalysis, we found that ICIC-DNA has several fatal security flaws. First, despite the use of multiple chaotic systems, the corresponding encryption sequences are independent of the plaintext, such that equivalent keys exist. Second, the diverse DNA operation is essentially a 2-bit data substitution process, and thus can be equivalently simplified. Third, ICIC-DNA includes substitution and permutation of DNA domains, and based on the equivalent simplification operation, the substitution and permutation can be attacked separately. Based on these, we propose a chosen-plaintext attack method to attack ICIC-DNA. Differential analysis is firstly adopted to break the DNA-base permutation process, and then the DNA domain encryption is eliminated, and finally the equivalent key is used to achieve complete cracking.

The rest of this paper is organized as follows. Section 2 briefly describes the ICIC-DNA. Section 3 presents a cryptanalysis of the ICIC-DNA. Section 4 presents the results of experimental simulations. Section 5 presents suggestions for improvement of ICIC-DNA. Section 6 concludes the paper.

2. The image cipher under study

2.1. DNA coding rules and sequence operations

A DNA sequence includes four kinds of nucleic acid bas- es: A, T, C and G. With respect to these four bases, the total number of coding combinations is 4! = 24. However, there are only eight kinds of coding combinations because these four bases satisfy the principle of complementary base pair. More precisely, A and T are complementary with each other, so are C and G. Table 1 shows the eight DNA coding rules. Tables 2 and 3 show the addition and subtraction rules for DNA coding, respectively.

Table 1
Eight kinds of DNA coding 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.

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 3
DNA subtraction operation.

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

2.2. The adopted chaotic systems

In the image cipher, five chaotic systems are adopted. They are introduced as follows:

- **Lorenz system** is mathematically modeled by

$$\begin{cases} \dot{x} = a(x-y) \\ \dot{y} = -xz + bx - y \\ \dot{z} = xy - cz \end{cases} \tag{1}$$

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. (1) is chaotic.

- **Chen's hyper-chaos system** is defined as

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = -xz + dx + cy - q \\ \dot{z} = xy - bz \\ \dot{w} = x + k \end{cases} \tag{2}$$

where a, b, c, d, k are system parameters. When (a, b, c, d) = (35, 8/3, 55, 1.3) and $k \in [-7, 7]$, Eq. (2) is hyper-chaotic.

- **Sine map** is defined as

$$x_{i+1} = \mu \cdot sin(\pi \cdot x_i) \tag{3}$$

where $x \in [0, 1]$ is the state variable and $\mu = 0.99$ is the control parameter respectively.

- **Cubic map** is defined as

$$x_{i+1} = \mu \cdot x_i \cdot (1 - x_i^2) \tag{4}$$

where the control parameter $\mu = 0.99$.

- **Logistic map** is defined as

$$x_{i+1} = \mu \cdot x_i \cdot (1 - x_i) \tag{5}$$

where the state variable $x \in (0, 1)$ and the control parameter $\mu \in (3.57, 4)$.

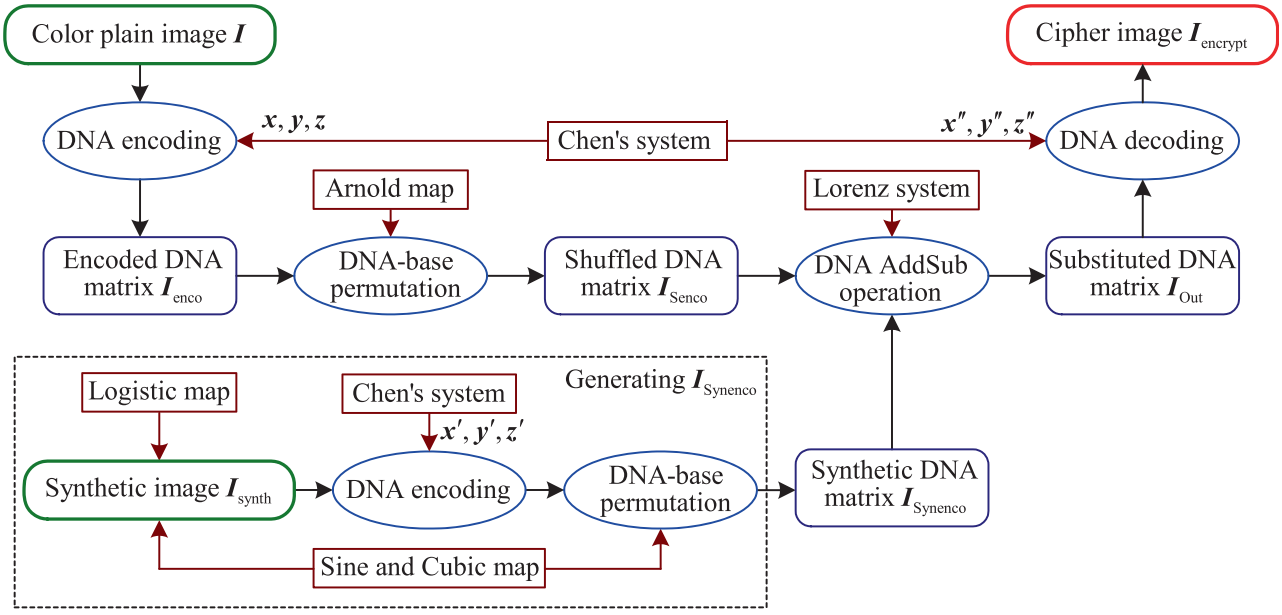

Fig. 1. The overall block diagram of ICIC-DNA.

- **Arnold cat map** is defined as

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 1 = A \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 1 \tag{6}$$

where p and q are the control parameters.

2.3. Description of ICIC-DNA

2.3.1. The secret key

As mentioned in (Kalpana and Murali, 2015), ICIC-DNA includes 27 secret keys. Among them, the four initial values (x_0, y_0, z_0, w_0) of Chen's hyper-chaos system are used three times, the initial value and control parameter of Sine and Cubic maps are both served twice. Besides, the three initial values (x_0, y_0, z_0) of Lorenz system, the control parameters (p, q) of Arnold map, and the initial value and control parameter (μ, x_0) of Logistic map are all used once.

2.3.2. Encryption process

ICIC-DNA's encryption objects are color images of size $H \times W$ (height $\times$ width). Block diagram of ICIC-DNA is illustrated as Fig. 1, where $\boldsymbol{I}$ and $\boldsymbol{I}_{encrpyt}$ are the plain-image and the cipher-image respectively. As can be seen from Fig. 1, the encryption process of IEA-DESC includes five stages: DNA encoding, DNA-base permutation, generating synthetic DNA matrix, DNA diffusion operation and DNA decoding. Its specific steps are given as follows:

- **Stage 1.** DNA encoding:
  - *Step 1.* Get the three channels $\boldsymbol{I}_R, \boldsymbol{I}_G, \boldsymbol{I}_B$ of size $H \times W$ from the color plain image $\boldsymbol{I}$, and transform $\boldsymbol{I}_R, \boldsymbol{I}_G, \boldsymbol{I}_B$ into their bit forms with size $H \times 8W$;
  - *Step 2.* Use Chen's hyper-chaos system for the first time, and get three integer matrices $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ of size $H \times W$, where $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z} \in [1, 8]$;
  - *Step 3.* Encode the color image's three channels by the three encoding rules matrices $\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z}$ respectively, then get the three corresponding encoded DNA matrices of size $H \times 4W$, given as $\boldsymbol{I}_{enco} = (\boldsymbol{R}_{enco}, \boldsymbol{G}_{enco}, \boldsymbol{B}_{enco})$.
- **Stage 2.** DNA-base permutation:
  Use Arnold map to perform permutation on the three DNA matrices $\boldsymbol{R}_{enco}, \boldsymbol{G}_{enco}, \boldsymbol{B}_{enco}$, and get the corresponding shuffled DNA matrices, represented as $\boldsymbol{I}_{Senco} = (\boldsymbol{R}_{Senco}, \boldsymbol{G}_{Senco}, \boldsymbol{B}_{Senco})$.
- **Stage 3.** Synthesizing a DNA image:
  - *Step 1.* Synthesize a gray-scale image $\boldsymbol{I}_{synth}$ of size $H \times W$ by mixing Sine, Cubic and Logistic maps;
  - *Step 2.* Use Chen's hyper-chaos system for the second time, and get an integer matrix $\boldsymbol{x}'$ of size $H \times W$, where $\boldsymbol{x}' \in [1, 8]$;
  - *Step 3.* Encode the gray-scale image $\boldsymbol{I}_{synth}$ by the encoding rules matrix $\boldsymbol{x}'$, then get the corresponding DNA matrix $\boldsymbol{I}_{Synenco}$ of size $H \times 4W$;
  - *Step 4.* Use Sine and Cubic maps to perform permutation on the DNA matrix $\boldsymbol{I}_{Synenco}$, and get the corresponding shuffled DNA matrix as $\boldsymbol{I}_{Synenco}$.
- **Stage 4.** DNA diffusion operation:
  Unlike the basic DNA operations such as addition or subtraction adopted in (Wei et al., 2012), an improved operation was proposed during the DNA diffusion stage in (Kalpana and Murali, 2015).
  - *Step 1.* Use the Lorenz system to generate three binary matrices $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_3$ of size $H \times 4W$, where $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_3 \in [0, 1]$;
  - *Step 2.* Perform the outcomes of the Stage 2 and 3 by the three binary matrices $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_3$, and then get the diffused matrices, exactly given as

$$\begin{cases} \boldsymbol{R}_{out} = DNA_{add,subtract}(\boldsymbol{R}_{Senco}, \boldsymbol{I}_{Synenco}, \boldsymbol{q}_1) \\ \boldsymbol{G}_{out} = DNA_{add,subtract}(\boldsymbol{G}_{Senco}, \boldsymbol{I}_{Synenco}, \boldsymbol{q}_2) \\ \boldsymbol{B}_{out} = DNA_{add,subtract}(\boldsymbol{B}_{Senco}, \boldsymbol{I}_{Synenco}, \boldsymbol{q}_3) \end{cases} \tag{7}$$

  where $DNA_{add,subtract}$ is the improved operation function. When the element of the three control matrices $\boldsymbol{q}_1, \boldsymbol{q}_2, \boldsymbol{q}_3$ is equal to 0, addition operation is adopted, otherwise subtraction is used.
  - *Step 3.* Get the diffused DNA matrix $\boldsymbol{I}_{out}$, given by $\boldsymbol{I}_{out} = (\boldsymbol{R}_{out}, \boldsymbol{G}_{out}, \boldsymbol{B}_{out})$.
- **Stage 5.** DNA decoding:
  - *Step 1.* Use Chen's hyper-chaos system for the third time, and get three integer matrices $\boldsymbol{x}'', \boldsymbol{y}'', \boldsymbol{z}''$ of size $H \times W$, where $\boldsymbol{x}'', \boldsymbol{y}'', \boldsymbol{z}'' \in [1, 8]$;

- *Step 2.* Decode the three DNA matrices $\boldsymbol{R}_{out}, \boldsymbol{G}_{out}, \boldsymbol{B}_{out}$ by the three decoding rules matrices $\boldsymbol{x}'', \boldsymbol{y}'', \boldsymbol{z}''$ respectively, then get the three channels of the color cipher image $\boldsymbol{I}_{encrypt}$ of size $H \times W$, given as $\boldsymbol{I}_{encrypt} = (\boldsymbol{R}_{encrypt}, \boldsymbol{G}_{encrypt}, \boldsymbol{B}_{encrypt})$.

2.3.3. Decryption process

Decryption is the inverse of encryption. Firstly, the cipher image $\boldsymbol{I}_{encrypt}$ is encoded as the DNA matrix $\boldsymbol{I}_{out}$; Then, the shuffled DNA matrix $\boldsymbol{I}_{Senco}$ is obtained from $\boldsymbol{I}_{out}$ and the synthetic DNA matrix $\boldsymbol{I}_{Synenco}$; Next, the encoded DNA image $\boldsymbol{I}_{enco}$ is achieved after the anti-permutation; Finally, the color plain image $\boldsymbol{I}$ is recovered by DNA decoding.

3. Cryptanalysis of ICIC-DNA by chosen-plaintext attack

3.1. Preliminary Analysis of ICIC-DNA

Chosen-plaintext attack is a common cryptanalysis method in conventional cryptography. It suppose that the attackers can arbitrarily choose the plaintext that would be useful for deciphering, and also know the corresponding ciphertext. Moreover, referring to the basic assumption of modern cryptography, ciphers are public and their security solely depend on the unknown secret keys.

From the perspective of cryptanalysis, ICIC-DNA shown in Fig. 1 has the two following features:

- *Feature 1.* During the whole encryption process, *all key-streams are not related to plain images*. Thus, under the premise of a given key, these key-streams keep unchanged for different encrypted images with the same size and type. This leads to the existence of an equivalent key, which is also the fatal defect of ICIC-DNA.
- *Feature 2. The basic unit of operation is 2-bit*. According to Table 1, DNA encoding and decoding are performed by a 2-bit form. Thus, all DNA operations are based on this paradigm, the only difference is the coding form. Therefore, an image of size $H \times W$ can be regarded as a matrix of size $H \times 4W$, where the unit is 2-bit.
- *Feature 3.* The entire encryption process includes two types of operations: permutation and substitution for 2-bit unit. DNA encoding, DNA AddSub operation, and DNA decoding are essentially substitution operation.

3.2. Differential analysis on the DNA-base permutation

Similar to other substitution and permutation network type ciphers, the common analytical thinking is to break them one by one with the idea of divide and conquer. In order to analyze the DNA-base permutation, the following Property 1 is first given.

Property 1. *In ICIC-DNA, for each 2-bit input of plain image, it only affects the 2-bit output of the cipher image after an encryption process.*

Proof. Following ICIC-DNA illustrated in Section 2.3 and Fig. 1, there is no interaction between the DNA bases of other encryption processes except for DNA-base permutation. Moreover, DNA-base permutation only alters the position of bases without changing their values.

Based on Property 1, by choosing two plain images with only one 2-bit different values, one can get the two corresponding cipher images with the same feature, exactly with only one 2-bit different values. Thus, one can determine the secret permutation of a DNA-base. Similarly, using this method to traverse all the different positions, the secret permutation matrix of size $H \times 4W$ can be obtained. Based on the differential cryptanalysis, one can get the secret permutation matrix as follows:

- *Step 1.* Choose the all-zero plain image and get the corresponding cipher image.
- *Step 2.* Choose a plain image with only one 2-bit non-zero (01, 10 or 11) and traverse all the different positions, and then get the corresponding $4HW$ cipher images respectively.
- *Step 3.* Compare the $4HW$ cipher images with the all-zero cipher image respectively, then get the secret permutation matrix of size $H \times 4W$.

Therefore, $4HW + 1$ chosen plain images are sufficient to break the DNA-base permutation.

3.3. Eliminating the DNA domain encryption

Once the replacement is deciphered, only the DNA replacement process will be unknown. For further simplification, give the Property 2 below.

Property 2. *For any 2-bit matrix of size $H \times 4W$, DNA encoding and DNA-base permutation satisfy the exchange law in ICIC-DNA.*

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

Case 1. First DNA encoding and then DNA-base permutation:

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

Case 2. First DNA-base permutation and then DNA encoding:

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

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

Thus, an equivalent simplified block diagram is shown in Fig. 2. Note that $\boldsymbol{P}_{2-bit}$ and $\boldsymbol{C}_{2-bit}$ are both in size $H \times 4W$, which are the 2-bit forms of $\boldsymbol{I}$ and $\boldsymbol{I}_{encrypt}$ with size $H \times W$ in Fig. 1 respectively. Observing Fig. 2, one can see that input and output of dotted boxes are 2-bit data, specially 00, 01, 10 and 11. To facilitate further cryptanalysis, the following Property 3 is derived.

Property 3. *In Fig. 2, there is a fixed correspondence between the 2-bit input and output at any position during the DNA domain encryption (dotted box).*

Proof. Based on Feature 1 of Section 3.1, all the chaos-based key-streams are not related to plain images. Thus, the synthetic image and the rules of DNA encoding, decoding and operation are all fixed under a given key. Moreover, in the doctted box of Fig. 2, there is no interaction between the DNA bases. Therefore, for any 2-bit input at any position, its corresponding 2-bit output is fixed.

Following Property 3, one can break the DNA domain encryption by obtaining the correspondence between 2-bit input and output at all positions. Instead of asking for many unknown variables, this will greatly simplify the complexity of the cryptanalysis.

Thus, the specific steps for recovering the original images are detailed below:

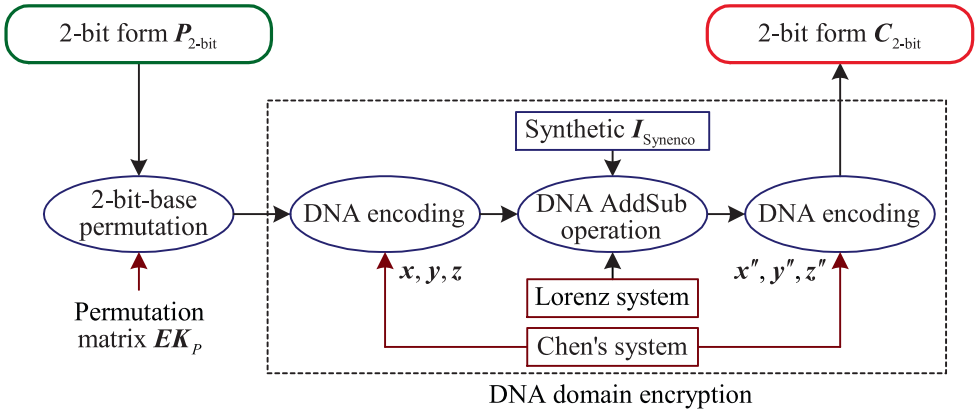

Fig. 2. The simplified block diagram of IEIE-DNA.

- *Step 1.* Choose the four special plain images with the same values $0, 85, 170, 255$, defined as $\boldsymbol{P}_0, \boldsymbol{P}_{85}, \boldsymbol{P}_{170}, P_{255}$, and get the corresponding cipher images $\boldsymbol{C}_0, \boldsymbol{C}_{85}, C_{170}, \boldsymbol{C}_{255}$ respectively. The reason for choosing such the images is that the corresponding 2-bit forms have the characteristics of all the same elements.
- *Step 2.* Use these four cipher images $\boldsymbol{C}_0, \boldsymbol{C}_{85}, \boldsymbol{C}_{170}, C_{255}$ to eliminate the DNA domain encryption process. The specific method is as shown in Algorithm 1.

Algorithm 1. Eliminating DNA domain encryption process.

Input: Given cipher image C_{2-bit}, and the four cipher images $\boldsymbol{C}^0_{2-bit}, \boldsymbol{C}^{85}_{2-bit}, \boldsymbol{C}^{170}_{2-bit}, \boldsymbol{C}^{255}_{2-bit}$
Output: Recovered permuted image $\boldsymbol{P}'_{2-bit}$
for $i \leftarrow 1$ *to* $4HW$ **do**
  if $C_{2-bit}(i) = C^0_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 00$;
  else if $C_{2-bit}(i) = C^{85}_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 01$;
  else if $C_{2-bit}(i) = C^{170}_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 10$;
  else if $C_{2-bit}(i) = C^{255}_{2-bit}(i)$ **then**
    $P'_{2-bit}(i) \leftarrow 11$;

- *Step 3.* Perform anti-permutation on the permuted image $\boldsymbol{P}'_{2-bit}$ with the DNA permutation matrix $\boldsymbol{EK_P}$ to obtain $\boldsymbol{P}_{2-bit}$, and then transform into the original plain image $\boldsymbol{P}$.

Therefore, 4 chosen plain images are enough to eliminate the DNA domain encryption. And total data complexity of the chosen-plaintext attack is $\boldsymbol{O}(4HW + 5)$.

4. Experimental simulations for breaking ICIC-DNA

In order to verify the validity of our security analysis and the feasibility of the proposed attack method, we conducted an experimental validation without changing the target algorithm idea. The image data selected for the decipherment experiment is the same as the original (Kalpana and Murali, 2015), which is also USC-SIPI "Miscellaneous".

In this experiment, we first select the color "lena" and color "baboon" images with the size of 256×256×3 as the target objects, and their corresponding ciphertext images are shown in Fig. 4a) and and Fig. 4(c), respectively. The reason for selecting these two images is to maintain consistency with the objects analyzed in the original literature.

According to the cryptanalysis steps in Section 3.3, first, four special plaintext images, which are solid color images with all pixel values of 0, 85, 170, and 255, are selected according to the conditions of the chosen-plaintext attack, and their corresponding ciphertext images are obtained by temporarily using a cryptograph on them. These four selected plaintext images are shown in Fig. 3(a)-(d), and their corresponding histograms are shown in Fig. 3(e). The corresponding ciphertext images are shown in Fig. 3(f)-(i), and their corresponding histograms are shown in Fig. 3(j).

Then, the corresponding four ciphertext images as shown in Fig. 3(f)-(i) are obtained using the chosen-plaintext attack, and the DNA domain encryption module can be cracked to obtain the replacement-only intermediate ciphertext image according to Algorithm 1 in Section 3.3. For the target ciphertext as in Fig. 4 (a), the intermediate ciphertext image as in Fig. 4(e) can be recovered. As shown in Fig. 4(e), some features of the original image can be obtained visually, and the features presented in its corresponding histogram Fig. 4(f) effectively verify this. The same experimental method and steps can be used to reduce another target ciphertext, as shown in Fig. 4(c), to its corresponding replacement-only intermediate ciphertext, as shown in Fig. 4(g).

Finally, the obtained permutation-only intermediate ciphertext image can be restored to the original plaintext image using the permutation matrix obtained by the difference analysis method. For the intermediate ciphertext image shown in Fig. 4(e), the recovered original plaintext image and its histograms are shown in Fig. 5a) and and Fig. 5(b), which can be seen to be exactly the same as the original image information. Similarly, we can recover its corresponding original plaintext image from Fig. 4(g), as shown in Fig. 5(c). After verifying that Fig. 5(a) and and Fig. 5(c) deciphered by this experiment are consistent with the original image given plaintext, the feasibility of the attack method proposed in this paper is verified.

In addition, in order not to lose generality, three main types of images were selected from this image dataset, specifically color images, grayscale images, and binary images, which are "Airport", "San Diego", and "Pixel ruler". The ciphertexts of the above images were selected, and the plaintexts were decrypted, and the experimental results are shown in Fig. 6.

By analogy, it is known that this attack method has general effectiveness under the condition of chosen-plaintext attack. The statistics of the effectiveness of the chosen-plaintext attack

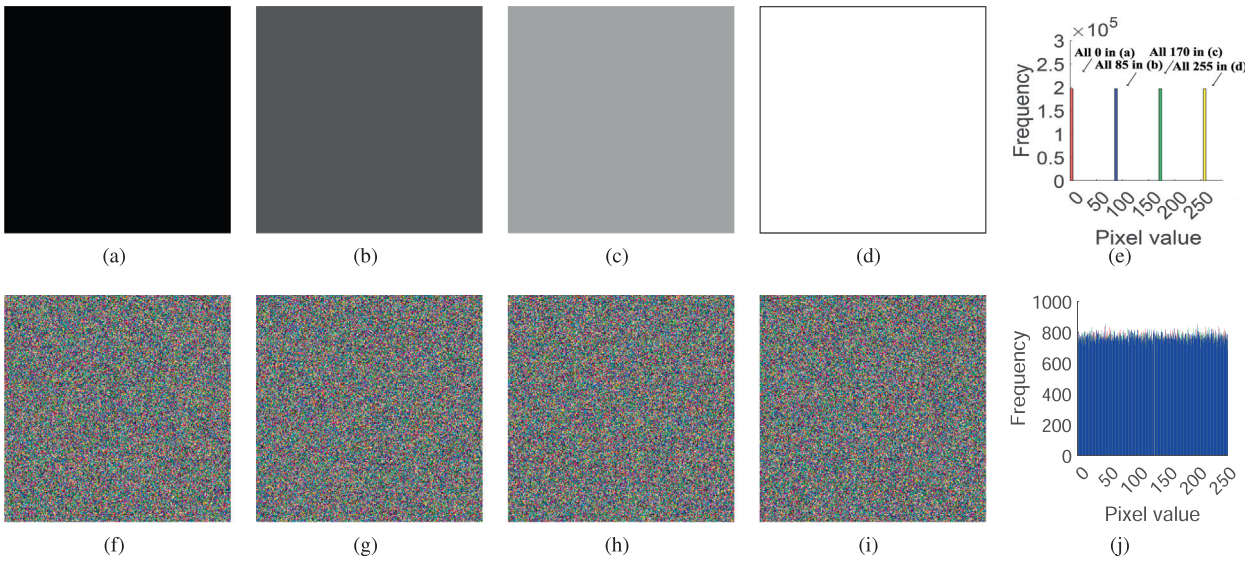

Fig. 3. Chosen-plaintext images, their ciphertext images, and their histograms: (a) M_0; (b) M_{85}; (c) M_{170}; (d) M_{255}; (e) Histogram of M; (f) C_0; (g) C_{85}; (h) C_{170}; (i) C_{255}; (j) Histogram of C.

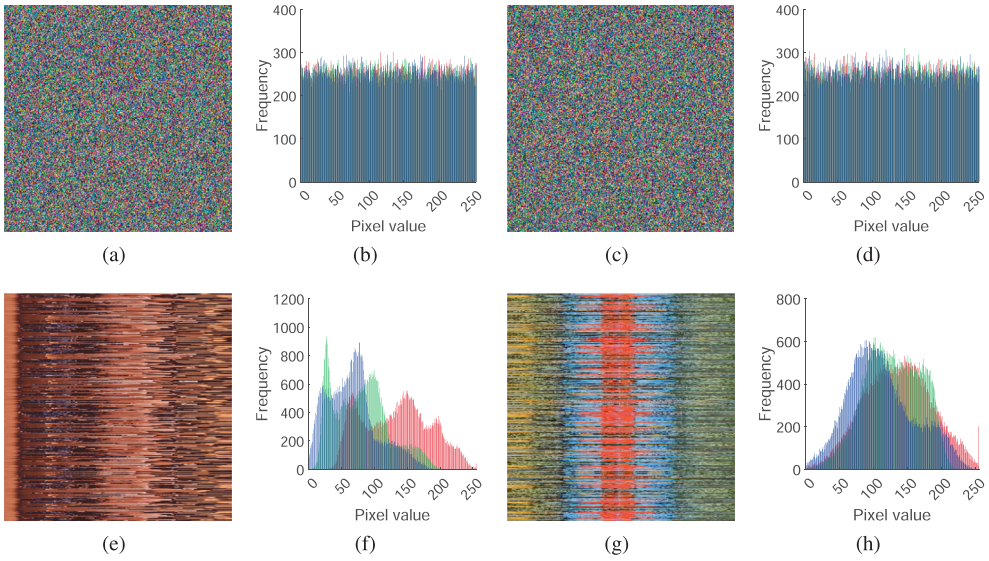

Fig. 4. Given ciphertext images, their recovered permutation images, and their histograms: (a) C_1; (b) Histogram of C_1; (c) C_2; (d) Histogram of C_2; (e) P'^1_{2-bit}; (f) Histogram of P'^1_{2-bit}; (g) P'^2_{2-bit}; (h) Histogram of P'^2_{2-bit}.

method are shown in Table 4. Meanwhile, the experiments also test the efficiency of this attack method under different types and sizes, and it can be seen from Fig. 7 that the proposed attack method only requires a lower time and can achieve the algorithm decipherment of ICIC-DNA. The experimental results show that the attack method proposed in this paper is effective for various experimental images.

5. Suggestions for improvement

According to the above analysis, ICIC-DNA is insecure and cannot resist chosen-plaintext attacks. In fact, some existing chaotic cryptosystems based on DNA encoding methods also have similar security vulnerabilities or flaws. To enhance the security of such algorithms, we give the following suggestions for improvement:

(1) Avoiding the presence of equivalent keys. After the analysis in Section 3, the ICIC-DNA algorithm has equivalent keys. Although the process of its encryption algorithm is more complicated, the inherent defect of purely in the equivalent key makes the algorithm eventually insecure. Therefore, the correlation between the key stream and the plaintext should be considered, and a dynamic encryption mechanism should be introduced to increase the security of the algorithm.

(2) Assessing the security contribution of DNA coding from a cryptanalytic perspective. The DNA encoding used in this paper is essentially a quadratic algebraic transformation. In this target algorithm, although the cross-fertilization of bioinformatics theory, the security contribution is actually insufficient. For this reason, the essential security should be assessed from a cryptanalytic perspective rather than formal security.

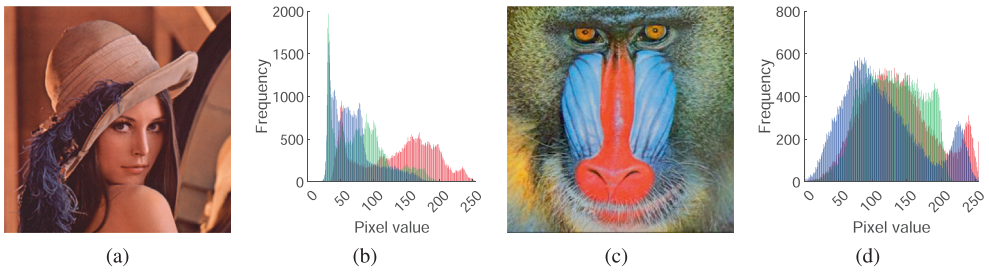

Fig. 5. The recovered ciphertext image and their histogram: (a) P_1; (b) Histogram of P_1; (c) P_2; (d) Histogram of P_2.

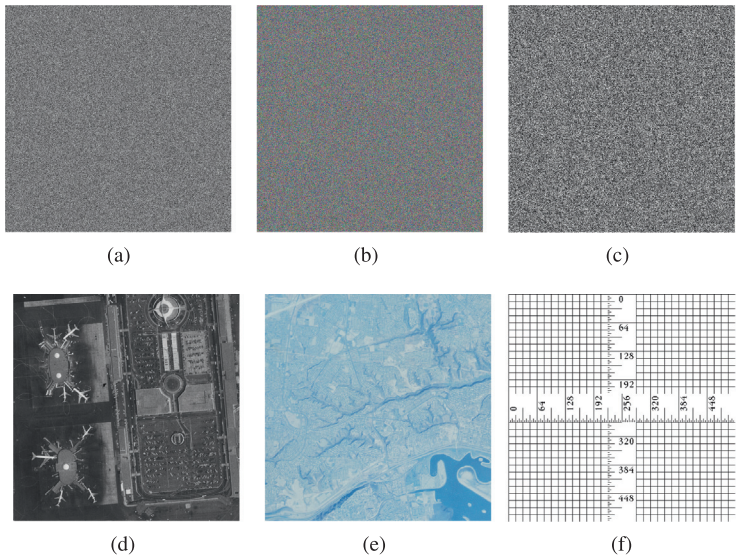

Fig. 6. Supplementary experiment: (a) Ciphertext of grayscale image "5.3.02"; (b) Ciphertext of Color image "2.2.03"; (c) Ciphertext of binary image "2.2.03"; (d) Grayscale image "5.3.02"; (e) Color image "2.2.03"; (f) Binary image "2.2.03".

Table 4
Attacking results for breaking ICIC-DNA.

The image type	The file name	Image description	size	Encryption time(s)	Decipher time(s)
Gray image	5.1.10	Aerial	256×256	0.9120	0.6858
	5.2.08	Couple	512×512	3.8503	2.7441
	5.3.02	Airport	1024×1024	17.7700	11.4434
Color image	lena	lena	256×256×3	2.7672	2.0804
	baboon	baboon	256×256×3	2.5236	1.8215
	4.1.06	Tree	256×256×3	2.7526	2.0731
	2.1.11	Earth from space	512×512×3	9.7001	6.9954
	2.2.03	San Diego	1024×1024×3	44.4720	29.1729
Gradient image	Gradient image	Gradient image	256×256	1.6109	1.2451
Binary image	ruler.512	Pixel ruler	512×512	2.4374	1.8350

(3) Considering the organic interconnectedness of the modules of the DNA-based code. DNA encoding, substitution, and diffusion are the basic modules, but many cryptographic substitutions and diffusions are breakable by divide-and-conquer strategies such that they are insecure. Therefore, it should be more organically combined to make the confusion and diffusion properties of ciphers more significant.

(4) Testing the chaotic encryption sequence for random characteristics. Chaos has properties such as high sensitivity to initial values and parameters, which is an important reason why chaotic cryptography has become a hot research topic today. However, even if the chosen chaotic system is complex enough, the randomness of the resulting chaotic sequence is not necessarily good enough. Therefore, the substantial contribution of chaotic systems to the security of cryptosystems should be examined from the perspective of cryptography.

6. Conclusion

In this paper, the security analysis of an improved color image cipher based on DNA encoding named ICIC-DNA was performed in detail. From the perspective of cryptanalysis, it is found that ICIC-DNA has several fatal security flaws. First, there is an equivalent key for ICIC-DNA, since multiple chaotic sequences are all independent of the plaintext. Second, the diverse DNA operation is essentially a 2-bit data substitution process, and thus can be

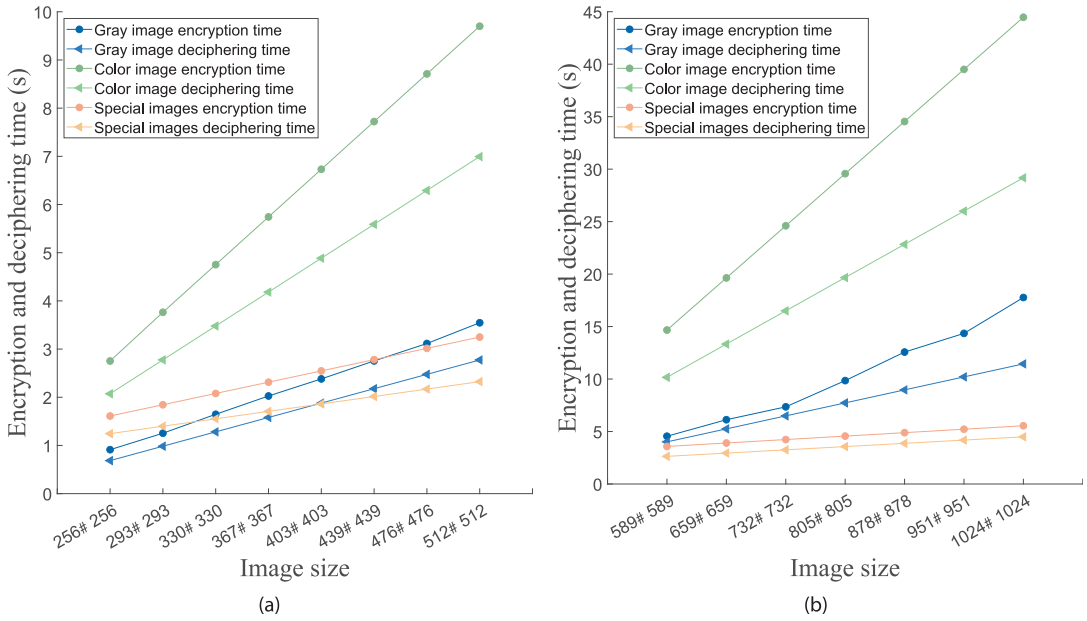

Fig. 7. Attacking results for breaking ICIC-DNA: (a) Encryption and deciphering of smaller size images; (b) Encryption and deciphering of larger size images.

equivalently simplified. Third, based on the equivalent simplification, ICIC-DNA can be attacked by divide-and-conquer strategy. Based on the above, we propose a chosen-plaintext attack method to attack ICIC-DNA. Differential analysis is firstly adopted to break the DNA-base permutation process, and then the DNA domain encryption is eliminated, and finally the equivalent key is used to achieve complete cracking. The theoretical analysis and experimental simulations were provided to support performances of the attack method. This cryptanalysis work can provide some reference for improving the security of image ciphers based on chaos theory and DNA encoding.

CRediT authorship contribution statement

Heping Wen: Supervision, Project Administration, Conceptualization, 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.

Acknowledgement

This work was supported in part by the National Science Foundation of China under Grant 62071088, 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.

References

Ali, T.S., Ali, R., 2022. A novel color image encryption scheme based on a new dynamic compound chaotic map and s-box. Multimedia Tools Appl. 81, 20585–20609.
Bao, B., Luo, J., Bao, H., Chen, C., Wu, H., Xu, Q., 2019. A simple nonautonomous hidden chaotic system with a switchable stable node-focus. Int. J. Bifurcat. Chaos 29, 1950168.
Chai, X., Wu, H., Gan, Z., Han, D., Zhang, Y., Chen, Y., 2021. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. Inf. Sci. 556, 305–340.
Chai, X., Wang, Y., Chen, X., Gan, Z., Zhang, Y., 2022. TPE-GAN: Thumbnail Preserving Encryption Based on GAN With Key. IEEE Signal Process. Lett. 29, 972–976.
Chen, B., Yu, S., Li, D.D.-U., Lü, J., 2021. Cryptanalysis of some self-synchronous chaotic stream ciphers and their improved schemes. Int. J. Bifurcat. Chaos 31, 2150142.
Cun, Q., Tong, X., Wang, Z., Zhang, M., 2021. Selective image encryption method based on dynamic dna coding and new chaotic map. Optik 243, 167286.
Farah, M.B., Guesmi, R., Kachouri, A., Samet, M., 2020. A novel chaos based optical image encryption using fractional fourier transform and dna sequence operation. Opt. Laser Technol. 121, 105777.
Hermassi, H., Belazi, A., Rhouma, R., Belghith, S.M., 2014. Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimedia Tools Appl. 72, 2211–2224.
Hua, Z., Zhu, Z., Chen, Y., Li, Y., 2021. Color image encryption using orthogonal latin squares and a new 2D chaotic system. Nonlinear Dyn. 104, 4505–4522.
Hua, Z., Wang, Y., Yi, S., Zhou, Y., Jia, X., 2022. Reversible data hiding in encrypted images using cipher-feedback secret sharing. IEEE Trans. Circuits Syst. Video Technol. 32, 4968–4982.
Kalpana, J., Murali, P., 2015. An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos. Optik 126, 5703–5709.
Li, C., Tan, K., Feng, B., Lü, J., 2022. The graph structure of the generalized discrete Arnold's Cat Map. IEEE Trans. Comput. 71, 364–377.
Liu, L., Zhang, Q., Wei, X., 2012. A RGB image encryption algorithm based on DNA encoding and chaos map. Comput. Electr. Eng. 38, 1240–1248.
Liu, Y., Tang, J., Xie, T., 2014. Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Opt. Laser Technol. 60, 111–115.
Liu, H., Kadir, A., Xu, C., 2020. Color image encryption with cipher feedback and coupling chaotic map. Int. J. Bifurcat. Chaos 30, 2050173.
Liu, S., Li, C., Hu, Q., 2022. Cryptanalyzing two image encryption algorithms based on a First-Order Time-Delay system. IEEE MultiMedia 29, 74–84.
Shi, G., Yu, S., Wang, Q., 2022. Security analysis of the image encryption algorithm based on a two-dimensional infinite collapse map. Entropy 24, 1023.
Song, C.-Y., Qiao, Y.-L., 2015. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. Entropy 17, 6954–6968.
Wang, X., Su, Y., 2021. Image encryption based on compressed sensing and DNA encoding. Signal Process.: Image Commun. 95, 116246.
Wang, X., Zhao, M., 2021. An image encryption algorithm based on hyperchaotic system and dna coding. Opt. Laser Technol. 143, 107316.
Wei, X., Guo, L., Zhang, Q., Zhang, J., Lian, S., 2012. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J. Syst. Softw. 85, 290–299.
Wen, H., Yu, S., Lü, J., 2019. Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. Entropy 21, 246.
Wen, H., Xu, J., Liao, Y., Chen, R., Shen, D., Wen, L., Shi, Y., Lin, Q., Liang, Z., Zhang, S., Liu, Y., Huo, A., Li, T., Cai, C., Wen, J., Zhang, C., 2021. A security-enhanced image communication scheme using cellular neural network. Entropy 23, 1000.
Wen, H., Zhang, C., Huang, L., Ke, J., Xiong, D., 2021. Security Analysis of a Color Image Encryption Algorithm Using a Fractional-Order Chaos. Entropy 23, 258.

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, 1332.
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, 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 J. 15, 1–11.
Wu, T., Zhang, C., Chen, Y., Cui, M., Huang, H., Zhang, Z., Wen, H., Zhao, X., Qiu, K., 2021. Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission. Opt. Express 29, 3669–3684.
Zhang, Q., Wei, X., 2019. A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik 124, 6276–6281.
Zhang, Q., Guo, L., Wei, X., 2010. Image encryption using DNA addition combining with chaotic maps. Mathe. Comput. Modell. 52, 2028–2035.
Zhang, Y., Wen, W., Su, M., Li, M., 2019. Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik 125, 1562–1564.
Zhang, Q., Guo, L., Wei, X., 2019. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik - Int. J. Light Electron Opt. 124, 3596–3600.