entropy

MDPI

Article

Breaking an Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos

Heping Wen [1,*], **Simin Yu** [1] **and Jinhu Lü** [2]

[1] School of Automation, Guangdong University of Technology, Guangzhou 510006, China; siminyu@163.com
[2] School of Automation Science and Electrical Engineering, State Key Laboratory of Software Development Environment, and Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing 100191, China; jhlu@iss.ac.cn
* Correspondence: hepingwen@yeah.net

Received: 3 February 2019; Accepted: 26 February 2019; Published: 5 March 2019

Abstract: Recently, an image encryption algorithm based on DNA encoding and spatiotemporal chaos (IEA-DESC) was proposed. In IEA-DESC, pixel diffusion, DNA encoding, DNA-base permutation and DNA decoding are performed successively to generate cipher-images from the plain-images. Some security analyses and simulation results are given to prove that it can withstand various common attacks. However, in this paper, it is found that IEA-DESC has some inherent security defects as follows: (1) the pixel diffusion is invalid for attackers from the perspective of cryptanalysis; (2) the combination of DNA encoding and DNA decoding is equivalent to bitwise complement; (3) the DNA-base permutation is actually a fixed position shuffling operation for quaternary elements, which has been proved to be insecure. In summary, IEA-DESC is essentially a combination of a fixed DNA-base position permutation and bitwise complement. Therefore, IEA-DESC can be equivalently represented as simplified form, and its security solely depends on the equivalent secret key. So the equivalent secret key of IEA-DESC can be recovered using chosen-plaintext attack and chosen-ciphertext attack, respectively. Theoretical analysis and experimental results show that the two attack methods are both effective and efficient.

Keywords: image encryption; DNA encoding; chaotic cryptography; cryptanalysis; image privacy

1. Introduction

With the rapid development of information technologies such as mobile Internet, cloud computing, social networking, and Big Data, the security of multimedia data such as image and video has attracted more and more attention [1–3]. Image is an important part of multimedia data, and its encryption protection techniques are particularly interesting [4,5]. In the past three decades, many novel image encryption schemes based on various methodologies were proposed, such as chaos theory [6], DNA computing [7], cellular automaton [8,9], and quantum information [9,10]. Among them, chaos is the most popular one because it has the unique characteristics of sensitivity to initial values and parameters, ergodicity, and deterministic inherent randomness [11–16], which correspond to the confusion and diffusion properties of encryption [17]. Moreover, DNA computing has the characteristics of high parallelism, large storage capacity, and low energy consumption [7]. Hence, researches on image encryption schemes combined with chaos theory and DNA computing have become a hot topic in recent years [18–20]. Nevertheless, many encryption schemes are actually insecure as a result of their various security defects [21,22]. Therefore, performing cryptanalysis on these existing encryption algorithms is indispensable [21,23,24].

In recent years, with the security analysis and breaking of some existing chaotic image algorithms combining DNA computing and chaos theory [25–30], research interest in cryptanalysis has become increasingly stimulated [31–34]. In 2010, Zhang et al. [25] created an image encryption method using DNA addition combined with chaotic maps. However, in 2014, Hermassi et al. [26] pointed out that the algorithm in Reference [25] was irreversible and was vulnerable to the chosen-plaintext attack and the known-plaintext attack. In 2015, Zhen et al. [27] proposed an image encryption scheme combining DNA coding and entropy. Nonetheless, in 2016, Su et al. [28] pointed out that the algorithm of Reference [27] was insecure and could be broken using the chosen-plaintext attack. In 2016, Jain et al. [29] proposed a robust DNA chaotic image encryption scheme based on Reference [25] and Reference [26]. Whereas, in 2017, Dou et al. [30] used the chosen-plaintext attack method to break the algorithm proposed in Reference [29]. In addition, Özkaynak et al. [33] and Zhang et al. [34] further concluded that an encryption algorithm may lead to the existence of an equivalent secret key if only a single DNA encoding and operation rule is employed.

Generally speaking, cryptanalysis becomes more difficult as the level of encryption design increases [35]. However, there are still some existing algorithms that can be broken owing to their inherent defects [36]. Moreover, since each encryption algorithm has natural features, the corresponding attack method may also be different. Therefore, it makes sense, even if a similar attack method is used, to reveal the intrinsic characteristics of the different encryption algorithms.

In 2015, an image encryption algorithm based on DNA encoding and spatiotemporal chaos (IEA-DESC) was proposed [37]. In IEA-DESC, pixel diffusion, DNA encoding, DNA-base permutation, and DNA decoding are adopted successively to obtain cipher-images from plain-images. Some security analyses and simulation results are given to prove that it can withstand various common attacks. Despite this, according to the basic criteria of cryptanalysis, some findings in IEA-DESC can be given as follows:

(1) Its pixel diffusion is invalid for attackers.

In IEA-DESC, there is no external secret key during the pixel diffusion phase. According to the cryptographic principle proposed by Kerckhoffs [38], the algorithm is public for attackers. Therefore, its pixel diffusion is essentially useless.

(2) The combination of DNA encoding and DNA decoding can be equivalently simplified.

Although the DNA encoding rule is related to the plain-image, there is a certain relationship between its decoding rule and its encoding rule. This leads to the fact that for any binary bit, the output is the complement of the input after DNA encoding and DNA decoding. Hence, DNA encoding and DNA decoding are a complementary process on the whole.

(3) The sequences for DNA-base permutation are fixed for different plain-images.

During IEA-DESC's DNA-base permutation, the chaos-based sequences for encryption are neither associated with plain-image nor cipher-image. Thus, on the basis of the basic rules of cryptanalysis, under the condition of a given secret key, the encryption sequences are fixed for different plain-images. Once the attackers obtain these sequences, i.e., an equivalent secret key, the DNA-base permutation is deciphered.

On the basis of the above properties, IEA-DESC's pixel diffusion is invalid, and therefore, its security depends only on the DNA domain encryption. Unfortunately, an equivalent secret key exists in the overall DNA domain encryption phase. More specifically, the DNA-based encryption algorithm is essentially a permutation-only process of a quaternary element. Yet, permutation-only encryption algorithms have been analyzed to be insecure [39,40]. Therefore, in this paper, two attack methods for breaking IEA-DESC using the chosen-plaintext attack and chosen-ciphertext attack are proposed, respectively.

The rest of the paper is organized as follows. Section 2 concisely describes IEA-DESC. Section 3 proposes two different attack methods on IEA-DESC. Section 4 presents the experimental simulation results. Section 5 gives some improvement suggestions for the security of chaos-based encryption algorithms. The last section concludes the paper.

2. The Encryption Algorithm under Study

In this section, the DNA coding rules and spatiotemporal chaos used in Reference [37] are introduced, and then the specific steps of IEA-DESC are detailed.

2.1. DNA Coding Rules

A DNA sequence includes four kinds of nucleic acid bases: 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 pairs. More precisely, A and T are complementary to each other, as are C and G. Table 1 shows the eight DNA coding rules.

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
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

2.2. Spatiotemporal Chaos

Two discrete chaotic maps are used in IEA-DESC [37], one is the logistic map and the other is a spatiotemporal chaos map based on the so-called new chaotic algorithm (NCA) given in Reference [41]. The iterative equation of the Logistic map is represented as

$$x_{n+1} = \mu x_n(1 - x_n), \tag{1}$$

where the state variable $x \in (0,1)$ and the control parameter $\mu \in (3.57, 4)$. The structure of the functional graph of the Logistic map in a digital computer is quantitatively analyzed in Reference [16].

The spatiotemporal chaos is a dynamic system using discrete time and space, in which the coupled map lattice (CML) is its most common model. The iterative equation of NCA-based CML is modeled by

$$\begin{cases} x_{n+1}(i) = (1-\varepsilon) f(x_n(i)) + \varepsilon \left\{ f\left[x_n(i-1)\right] + f\left[x_n(i+1)\right] \right\} / 2, \\ f(x) = (1-\beta^{-4}) \cdot \mathrm{ctg}(\alpha/(1+\beta)) \cdot (1+1/\beta)^{\beta} \cdot \mathrm{tg}(\alpha x_n) \cdot (1-x)^{\beta}, \end{cases} \tag{2}$$

where the spatial lattice index $i = 1, 2, \cdots, L$, the time grid index $n = 1, 2, \cdots$, the coupling strength $\varepsilon \in (0,1)$, the state variable $x_n(i) \in (0,1)$, and the periodic boundary condition is $x_n(0) = x_n(L)$. The second equation of Equation (2) is the so-called NCA, which is actually an improved logistic map. Given the parameters $\alpha = 1.57, \beta = 3.5, \varepsilon = 0.3$, and $L = 1024$, the system is chaotic, and its attractor is shown in Figure 1.

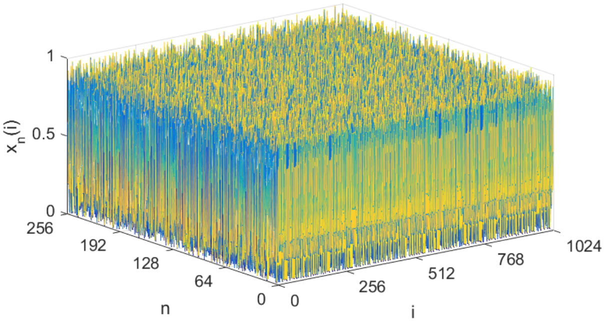


Figure 1. The attractor of the new chaotic algorithm (NCA)-based coupled map lattice (CML).

2.3. Description of IEA-DESC

2.3.1. Secret Key

The secret key of IEA-DESC consists of $x_0, \mu, K_0, N_0, \alpha, \beta, \varepsilon$, and L, where x_0, μ, K_0, and N_0 are the parameters of the logistic map, $\alpha, \beta, \varepsilon$, and L are the parameters of NCA-based CML, and N_0 is the length of discarded sequence for eliminating harmful transient effects.

2.3.2. Encryption Process

The encryption objects of IEA-DESC are 8-bit grayscale images of size $H \times W$ (height × width). For convenience, the symbolic representation is different without changing the original algorithm. A block diagram of IEA-DESC is shown in Figure 2, where $\boldsymbol{P}$, $\boldsymbol{P}'$, and $\boldsymbol{C}$ are the plain-image, the diffused image, and the cipher-image, respectively. As can be seen from Figure 2, the encryption process of IEA-DESC includes four phases: pixel diffusion, DNA encoding, DNA-base permutation, and DNA decoding.

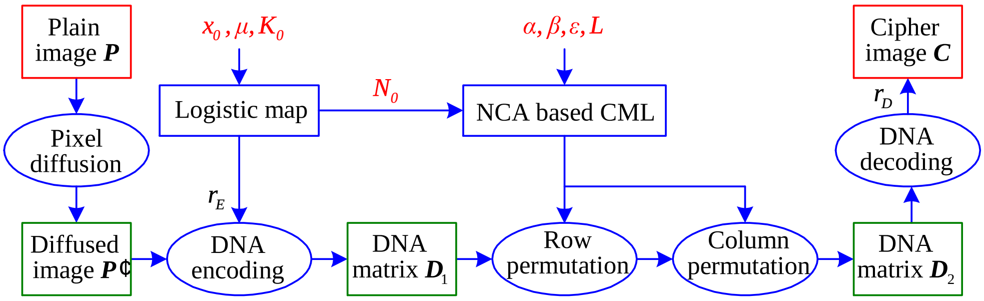


Figure 2. Block diagram of the image encryption algorithm based on DNA encoding and spatiotemporal chaos (IEA-DESC).

The specific descriptions of IEA-DESC are given as follows:

- **Phase 1.** Pixel Diffusion:

  By converting the plain-image $\boldsymbol{P}$ into the corresponding sequence $\{p_1, p_2, \ldots, p_{H\times W}\}$ in raster scanning order, the pixel diffusion equation is defined as

$$\begin{cases} p'_1 = p_1 \oplus p_{H\times W}, \\ p'_{i+1} = p_i \oplus p'_i, \end{cases} \tag{3}$$

  where $i = 1, 2, \ldots, H \times W - 1$, and $\oplus$ represents the bitwise XOR operation. Thus, the diffused image $\boldsymbol{P}'$ of size $H \times W$ is obtained from the diffused sequence $\{p'_1, p'_2, \ldots, p'_{H\times W}\}$.

- **Phase 2.** DNA Encoding:

  Calculating the sum of the plain-image pixels, the K_0-th iteration value x_{K_0} is obtained by Equation (1) under the initial value x_0 and the control parameter μ. The DNA encoding rule r_E, as in Table 1, is further determined by

$$r_E = \lfloor x_{K_0} \times 8 \rfloor + 1, \tag{4}$$

  where $r_E \in [1, 8]$, and $\lfloor a \rfloor$ rounds the element a to the nearest integer toward minus infinity. Then, by the r_E-th encoding rule in Table 1, the diffused image $\boldsymbol{P}'$ of size $H \times W$ is firstly converted into the corresponding binary matrix of size $H \times 8W$, and then encoded as the DNA matrix $\boldsymbol{D}_1$ of size $H \times 4W$.

- **Phase 3.** DNA-Base Permutation:

First, by iterating Equation (1) $N_0 + 4W$ times and then discarding the front N_0 elements under the initial value x_0 and the control parameter μ, a sequence $\{a_1, a_2, \ldots, a_{4W}\}$ of length $4W$ is obtained. Here, the sequence $\{a_1, a_2, \ldots, a_{4W}\}$ is taken as an initial value of the spatiotemporal chaos called NCA-based CML. Thus, by iterating Equation (2) H times under the parameters $\alpha, \beta, \varepsilon$, and L, a real matrix $\boldsymbol{X}$ of size $H \times 4W$ is achieved.

Then, by sorting each row's elements of $\boldsymbol{X}$ in ascending order, the corresponding H row position index sequences are obtained as $\boldsymbol{RI}_i$. Using $\boldsymbol{RI}_i$ to perform permutation for each row on the DNA matrix $\boldsymbol{D}_1$, the corresponding row permuted DNA matrix $\boldsymbol{D}_1'$ is obtained, given by

$$[\boldsymbol{D}_1']_{i,k} = [\boldsymbol{D}_1]_{i,\boldsymbol{RI}_i(k)}, \tag{5}$$

where $i = 1, 2, \ldots, H$, $k = 1, 2, \ldots, 4W$, $\boldsymbol{RI}_i(k)$ indicates a position index of the k-th element in the i-th row, and $\boldsymbol{RI}_i(k) \in \{1, 2, \ldots, 4W\}$. Similarly, by sorting each column's elements of $\boldsymbol{X}$ in ascending order, the corresponding $4W$ column position index sequences are obtained as $\boldsymbol{CI}_j$. Using $\boldsymbol{CI}_j$ to perform permutation for each column on the DNA matrix $\boldsymbol{D}_1'$, the corresponding column permuted DNA matrix $\boldsymbol{D}_2$ is obtained, represented as

$$[\boldsymbol{D}_2]_{k,j} = [\boldsymbol{D}_1']_{\boldsymbol{CI}_j(k),j}, \tag{6}$$

where $j = 1, 2, \ldots, 4W$, $k = 1, 2, \ldots, H$, $\boldsymbol{CI}_j(k)$ indicates a position index of the k-th element in the j-th column, and $\boldsymbol{CI}_j(k) \in \{1, 2, \ldots, H\}$.

- **Phase 4.** DNA Decoding:

  Corresponding to Equation (4), the DNA decoding rule r_D is determined as

  $$r_D = 9 - r_E, \tag{7}$$

  where $r_D \in [1, 8]$. Thus, by the r_D-th decoding rule in Table 1, the DNA matrix $\boldsymbol{D}_2$ of size $H \times 4W$ is firstly decoded as the corresponding binary matrix of size $H \times 8W$, and then converted into the cipher-image $\boldsymbol{C}$ of size $H \times W$.

2.3.3. Decryption Process

Decryption is the inverse of encryption. First, the cipher-image $\boldsymbol{C}$ is converted into the DNA matrix $\boldsymbol{D}_2$ by the r_D-th encoding rule. Then, the DNA matrix $\boldsymbol{D}_1$ is exacted from the DNA matrix $\boldsymbol{D}_2$ after the anti-permutation. Next, the DNA matrix $\boldsymbol{D}_1$ is decoded as the diffused image $\boldsymbol{P}'$ with the r_E-th decoding rule. Finally, the plain-image $\boldsymbol{P}$ is recovered by anti-diffusion decryption from Equation (3).

3. Cryptanalysis of IEA-DESC

3.1. Preliminary Analysis of IEA-DESC

According to modern cryptography principles, encryption algorithms are public and only the secret keys are unknown to attackers [42,43]. More precisely, the security of an algorithm solely depends on its secret key. Four common attack methods for cryptanalysis are shown in Table 2. A secure cryptosystem should be able to resist all types of attacks in Table 2. If a cryptosystem cannot resist anyone of these attacks, one can conclude that the cryptosystem is insecure.

By observing Figure 2, one can divide the encryption process of IEA-DESC into two parts, one is pixel diffusion, and the other is DNA domain encryption. For the pixel diffusion part, there is no secret key involved. Since the algorithm is open from the perspective of cryptanalysis, the diffusion phase of IEA-DESC is essentially invalid for the attacker.

Table 2. Four common attack methods for cryptanalysis.

Attack Methods	Available Resources for Cryptanalysis
Ciphertext-only attack	The attacker only knows the ciphertext.
Known-plaintext attack	The attacker knows any given plaintext, and also knows the corresponding ciphertext.
Chosen-plaintext attack	The attacker can choose the plaintext that would be useful for deciphering, and also knows the corresponding ciphertext.
Chosen-ciphertext attack	The attacker can choose the ciphertext that is useful for deciphering, and also knows the corresponding plaintext.

For this reason, only the DNA domain encryption part is worthy of further discussion here. Following Equations (4) and (7), one knows that there is a definite one-to-one correspondence between DNA encoding rule r_E and DNA decoding rule r_D. Hence, one can list all possible pairs of DNA codec rules, given as

$$(r_E, r_D) \in \{(1,8),(2,7),(3,6),(4,5),(5,4),(6,3),(7,2),(8,1)\}\,. \tag{8}$$

Accordingly, given the eight pairs of DNA codec rules, within the binary bits before and after DNA coding, there appears a certain regularity [34]. Table 3 shows any 2-bit input and its 2-bit output with the eight pairs of DNA codec rules. As can be seen from Table 3, given any 2-bit input, no matter which DNA encoding rule is taken, the corresponding 2-bit output is the same because $r_E + r_D = 9$ holds. Put explicitly, the 2-bit input and the corresponding 2-bit output are complementary.

Table 3. Any 2-bit input and its 2-bit output with the eight pairs of DNA codec rules.

2-Bit Input	DNA-Base with Encoding Rule r_E								2-Bit Output with Decoding Rule r_D
	1	2	3	4	5	6	7	8	
00	A	A	G	C	G	C	T	T	11
01	G	C	A	A	T	T	C	G	10
10	C	G	T	T	A	A	G	C	01
11	T	T	C	G	C	G	A	A	00

Furthermore, one can see that the chaos-based sequences for DNA-base permutation are fixed for different plain-images under the premise of a given secret key. Indeed, it means that an equivalent secret key exists in IEA-DESC.

On this basis, it is found that IEA-DESC is essentially a combination process of a fixed DNA-base position permutation and bitwise complement. Therefore, a simplified block diagram of IEA-DESC can be illustrated, as is shown in Figure 3, where EK_P is the equivalent secret key. Once EK_P is obtained, IEA-DESC will be broken. Note that the eight different pairs of DNA encoding and decoding, as in Table 3, are equivalent. For simplicity, one sets $r_E = 1$ and $r_D = 8$, i.e., the first DNA encoding rule and the eighth DNA decoding rule are adopted below.

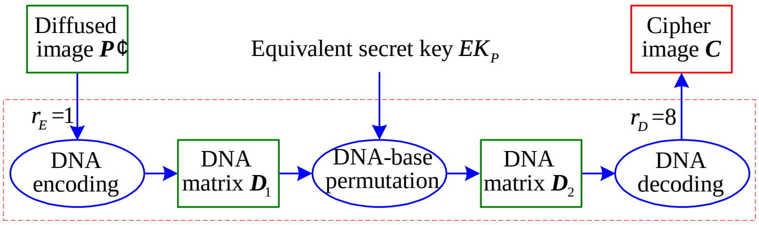


Figure 3. Simplified block diagram of IEA-DESC.

3.2. Analysis of DNA-Base Permutation

To obtain the equivalent secret key EK_P, performing analysis on the DNA-base permutation is significant. Since DNA only has four different bases, the essence of DNA-base permutation is a position shuffling procedure for a quaternary matrix of size $H \times 4W$.

Supposing that one has an input matrix $\boldsymbol{PV}$ of size $H \times 4W$ which satisfies that each element is unequal, and its corresponding one-dimensional sequence in the raster scanning order is $\{0, 1, 2, \ldots, 4HW - 1\}$. Letting $\mathbb{Z}_m$ denote a set $\{0, 1, \cdots, m-1\}$, one has $\boldsymbol{PV} \in \mathbb{Z}_{4HW}$. Obviously, after a position permutation, the output matrix $\boldsymbol{CV}$ corresponding to the input matrix $\boldsymbol{PV}$ also has the feature that all elements are not equal to each other. According to the assumption of the chosen-plaintext attack in Table 2, one can know both $\boldsymbol{PV}$ and $\boldsymbol{CV}$. Thus, the equivalent secret key can be determined by comparing the elements before and after the permutation.

However, since each DNA-base only takes four values, A, G, C, and T, such an input matrix $\boldsymbol{PV}$ does not exist. To cope with the problem, an appropriate transformation is inevitable. Therefore, the specific analysis steps to determine the equivalent secret key EK_P, as in Figure 3, are detailed as follows:

Step 1. Decompose the virtual matrix $\boldsymbol{PV}$ of size $H \times 4W$ into some quaternary matrices of the same size.

The virtual matrix $\boldsymbol{PV}$ is firstly decomposed into the N_C corresponding quaternary matrices $\boldsymbol{PQ}_n (n = 1, 2, \ldots, N_C)$, defined by

$$\boldsymbol{PV} = \sum_{n=1}^{N_C} 4^{n-1} \boldsymbol{PQ}_n = \boldsymbol{PQ}_1 + 4\boldsymbol{PQ}_2 + 4^2\boldsymbol{PQ}_3 + \ldots + 4^{N_C - 1}\boldsymbol{PQ}_{N_C}, \tag{9}$$

where $\boldsymbol{PV} \in \mathbb{Z}_{4HW}$, $\boldsymbol{PQ}_n \in \mathbb{Z}_4$, and N_C is the minimum amount required to ensure this decomposition method. Referring to Reference [39], generally one has

$$\begin{aligned} N_C &= \lceil \log_4(H \times 4W) \rceil \\ &= 1 + \lceil \log_4(HW) \rceil , \end{aligned} \tag{10}$$

where $\lceil a \rceil$ rounds the element a to the nearest integer toward positive infinity.

Step 2. Transform these quaternary matrices into the 8-bit images of size $H \times W$, respectively.

The quaternary matrices $\boldsymbol{PQ}_n (n = 1, 2, \ldots, N_C)$ are transformed into the corresponding decimal matrices using the method whereby every four quaternary elements are combined into a decimal one in order from low to high. For instance, given four quaternary elements are 0, 1, 2, and 3, one gets the corresponding decimal result as 228 because of its combination procedure: $0 \times 1 + 1 \times 4 + 2 \times 4^2 + 3 \times 4^3$. In fact, these decimal matrices are the resulting 8-bit images $\boldsymbol{PI}_n (n = 1, 2, \ldots, N_C)$ of size $H \times W$.

Step 3. Temporarily use the encryption machine to obtain the N_C corresponding cipher-images.

Following Figure 3, the diffused image $\boldsymbol{P}'$ is deemed as an input plain-image. As for the chosen-plaintext attack in Table 2, the input plain-images can be arbitrarily chosen, and the encryption machine can be temporarily used. Therefore, one gets the N_C cipher-images $\boldsymbol{CI}_n (n = 1, 2, \ldots, N_C)$ corresponding to the input plain-images $\boldsymbol{PI}_n (n = 1, 2, \ldots, N_C)$, respectively, after the encryption. Obviously, one has $\boldsymbol{PI}_n \in \mathbb{Z}_{256}$ and $\boldsymbol{CI}_n \in \mathbb{Z}_{256}$.

As shown in Figure 3, it takes three phases from $\boldsymbol{PI}_n$ to $\boldsymbol{CI}_n$: DNA encoding, DNA-base permutation, and DNA decoding. First, the N_C plain-images $\boldsymbol{PI}_n$ are encoded as the corresponding DNA matrices with the first DNA encoding rule of Table 1. Then, the permuted DNA matrices are further obtained after a DNA-base permutation. Finally, the N_C corresponding cipher-images $\boldsymbol{CI}_n$ are decoded from the permuted DNA matrices with the eighth DNA decoding rule.

Step 4. Convert these 8-bit cipher-images into the quaternary matrices of size $H \times 4W$, respectively.

Note that the eighth DNA decoding rule corresponds to the first DNA encoding rule, and the combination process of DNA encoding and DNA decoding is bitwise complement analyzed as in Table 3. Therefore, the complement operation cannot be ignored.

First, similar to the method in Step 2, the N_C 8-bit cipher-images $\boldsymbol{CI}_n(n = 1, 2, \ldots, N_C)$ of size $H \times W$ are converted to the corresponding quaternary matrices $\boldsymbol{CQ}_n(n = 1, 2, \ldots, N_C)$ of size $H \times 4W$. Then, the corresponding complementary quaternary matrices $\overline{\boldsymbol{CQ}}_n(n = 1, 2, \ldots, N_C)$ can be obtained from these quaternary matrices $\boldsymbol{CQ}_n(n = 1, 2, \ldots, N_C)$, respectively. Here, the quaternary complement operation is defined as being subtracted by 3. Specifically, the complements of 0, 1, 2, and 3 are 3, 2, 1, and 0, respectively.

Step 5. Compose the N_C complementary quaternary matrices into a virtual matrix of size $H \times 4W$.

Corresponding to Equation (9), the virtual matrix $\boldsymbol{CV}$ is composed from the N_C complementary quaternary matrices $\overline{\boldsymbol{CQ}}_n(n = 1, 2, \ldots, N_C)$, given as

$$\boldsymbol{CV} = \sum_{n=1}^{N_C} 4^{n-1}\overline{\boldsymbol{CQ}}_n = \overline{\boldsymbol{CQ}}_1 + 4\overline{\boldsymbol{CQ}}_2 + 4^2\overline{\boldsymbol{CQ}}_3 + \ldots + 4^{N_C-1}\overline{\boldsymbol{CQ}}_{N_C}, \tag{11}$$

where $\boldsymbol{CV} \in \mathbb{Z}_{4HW}$, and $\overline{\boldsymbol{CQ}}_n \in \mathbb{Z}_4$.

Step 6. Obtain the equivalent secret key EK_P.

Finally, EK_P is obtained by comparing all the different elements of $\boldsymbol{PV}$ and $\boldsymbol{CV}$.

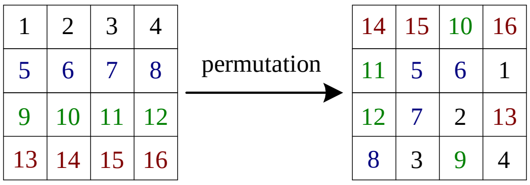
To better illustrate this analysis process, a simple example is taken. Let a input virtual matrix $\boldsymbol{PV}$ of size 4 × 4 be

$$\boldsymbol{PV} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{bmatrix}.$$

First, following Steps 1 and 2, one gets two quaternary matrices $\boldsymbol{PQ}_1$ and $\boldsymbol{PQ}_2$, the two 8-bit images $\boldsymbol{PI}_1$ and $\boldsymbol{PI}_2$, and their corresponding DNA matrices as below:

$$\boldsymbol{PQ}_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{bmatrix} \rightarrow \boldsymbol{PI}_1 = \begin{bmatrix} 228 \\ 228 \\ 228 \\ 228 \end{bmatrix} \xrightarrow{r_E=1} \begin{bmatrix} A & G & C & T \\ A & G & C & T \\ A & G & C & T \\ A & G & C & T \end{bmatrix},$$

$$\boldsymbol{PQ}_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \end{bmatrix} \rightarrow \boldsymbol{PI}_2 = \begin{bmatrix} 0 \\ 85 \\ 170 \\ 255 \end{bmatrix} \xrightarrow{r_E=1} \begin{bmatrix} A & A & A & A \\ G & G & G & G \\ C & C & C & C \\ T & T & T & T \end{bmatrix}.$$



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

14	15	10	16
11	5	6	1
12	7	2	13
8	3	9	4

Figure 4. The illustration diagram of a position shuffling for matrices of size 4 × 4.

Then, as in Steps 3 and 4, supposing that the procedure of DNA-base permutation is given in Figure 4, one obtains the two cipher-images $\boldsymbol{CI}_1$ and $\boldsymbol{CI}_2$, their corresponding DNA matrices, and the two quaternary ones $\boldsymbol{CQ}_1$ and $\boldsymbol{CQ}_2$ via

$$\boldsymbol{CQ}_1 = \begin{bmatrix} 2 & 1 & 2 & 0 \\ 1 & 3 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ 0 & 1 & 3 & 0 \end{bmatrix} \leftarrow \boldsymbol{CI}_1 = \begin{bmatrix} 38 \\ 237 \\ 228 \\ 52 \end{bmatrix} \xrightarrow{r_D=8} \begin{bmatrix} G & C & G & T \\ C & A & G & A \\ T & C & G & A \\ T & C & A & T \end{bmatrix},$$

$$\boldsymbol{CQ}_2 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 1 & 3 \end{bmatrix} \leftarrow \boldsymbol{CI}_2 = \begin{bmatrix} 16 \\ 233 \\ 57 \\ 222 \end{bmatrix} \xrightarrow{r_D=8} \begin{bmatrix} T & T & C & T \\ C & G & G & A \\ C & G & A & T \\ G & A & C & A \end{bmatrix}.$$

Correspondingly, one gets the two complementary quaternary matrices $\overline{\boldsymbol{CQ}}_1$ and $\overline{\boldsymbol{CQ}}_2$ as

$$\overline{\boldsymbol{CQ}}_1 = \begin{bmatrix} 1 & 2 & 1 & 3 \\ 2 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 \\ 3 & 2 & 0 & 3 \end{bmatrix}, \overline{\boldsymbol{CQ}}_2 = \begin{bmatrix} 3 & 3 & 2 & 3 \\ 2 & 1 & 1 & 0 \\ 2 & 1 & 0 & 3 \\ 1 & 0 & 2 & 0 \end{bmatrix}.$$

Next, as in Step 5, one obtains the corresponding output virtual matrix as

$$\boldsymbol{CV} = \begin{bmatrix} 13 & 14 & 9 & 15 \\ 10 & 4 & 5 & 0 \\ 11 & 6 & 1 & 12 \\ 7 & 2 & 8 & 3 \end{bmatrix}.$$

Finally, the equivalent secret key EK_P is achieved with Step 6.

On the basis of the above discussion, one can conclude that the encryption algorithm given in Figure 3 can be broken just with the equivalent secret key EK_P without knowing any secret key parameter.

3.3. Breaking IEA-DESC Using the Chosen-Plaintext Attack

Following Section 3.2, the diffused image $\boldsymbol{P}'$ is considered as the input of the cryptosystem. However, as shown in Figure 2, the actual input of IEA-DESC is the plain-image $\boldsymbol{P}$ rather than the diffused image $\boldsymbol{P}'$. To accommodate to this change, the input chosen plain-image should be adjusted accordingly.

According to the analysis in Section 3.1, the pixel diffusion part of IEA-DESC is actually useless for attackers. Under the premise that the algorithm is known, there is a certain one-to-one correspondence between the diffused image and the plain-image. Therefore, for 8-bit grayscale images of size $H \times W$, the specific analysis steps for the chosen-plaintext attack are given as follows:

Step 1. Choose some special plain-images.

The N_C 8-bit images $\boldsymbol{PI}_n(n = 1, 2, \ldots, N_C)$ constructed in Section 3.2 are presented as the diffused images $\boldsymbol{P}'_n(n = 1, 2, \ldots, N_C)$, respectively, and then their one-to-one corresponding plain-images $\boldsymbol{P}_n(n = 1, 2, \ldots, N_C)$ are obtained using anti-diffusion decryption, which is defined from Equation (3) as

$$\begin{cases} p_i = p'_{i+1} \oplus p'_i, \\ p_{H\times W} = p_1 \oplus p'_1, \end{cases} \tag{12}$$

where $i = 1, 2, \ldots, H \times W - 1$, $\{p_1, p_2, \ldots, p_{H\times W}\}$ and $\{p'_1, p'_2, \ldots, p'_{H\times W}\}$ are the sequences transformed by the plain-image $\boldsymbol{P}$ and the diffused image $\boldsymbol{P}'$ in the raster scanning order, respectively.

Step 2. Temporarily use the encryption machine to get the corresponding cipher-images.

On the basis of the condition of the chosen-plaintext attack, the corresponding N_C cipher-images $\boldsymbol{C}_n(n = 1, 2, \ldots, N_C)$ are obtained from the N_C plain-images $\boldsymbol{P}_n(n = 1, 2, \ldots, N_C)$ by temporarily using the encryption machine.

Step 3. Achieve the equivalent DNA-base permutation secret key.

By substituting $\boldsymbol{PI}_n(n = 1, 2, \ldots, N_C)$ and $\boldsymbol{CI}_n(n = 1, 2, \ldots, N_C)$ in Section 3.2 with the diffused images $\boldsymbol{P}'_n(n = 1, 2, \ldots, N_C)$ and the cipher-images $\boldsymbol{C}_n(n = 1, 2, \ldots, N_C)$, respectively, one gets the equivalent DNA-base permutation secret key EK_P with the same method as in Section 3.2.

Step 4. Recover the images with the equivalent secret key.

First, using the equivalent secret key EK_P, the corresponding diffused image can be obtained from a cipher-image. Then, the recovered plain-image is obtained from the diffused images with Equation (12).

Therefore, the chosen-plaintext attack is effective to break IEA-DESC, and its data complexity is $\boldsymbol{O}(N_C) = \boldsymbol{O}(1 + \lceil \log_4(HW) \rceil)$.

3.4. Breaking IEA-DESC Using the Chosen-Ciphertext Attack

Since the encryption structure of Figure 3 is symmetrical, the chosen-ciphertext attack is also available. The specific analysis steps based on the chosen-ciphertext attack are detailed below:

Step 1. Choose some specific cipher-images and temporarily use the decryption machine to get the corresponding plain-images.

Here, the N_C images $\{\boldsymbol{PI}_n\}_{n=1}^{N_C}$ in Secction 3.2 are served as the chosen cipher-images $\{\boldsymbol{C}_n\}_{n=1}^{N_C}$ respectively, and then temporarily use the decryption machine to get the corresponding plain-images $\{\boldsymbol{P}_n\}_{n=1}^{N_C}$.

Step 2. Get the corresponding diffused images.

The one-to-one corresponding N_C diffused images $\boldsymbol{P}'_n$ $(n = 1, 2, \ldots, N_C)$ are obtained from these plain-images $\boldsymbol{P}_n(n = 1, 2, \ldots, N_C)$ using Equation (3).

Step 3. Achieve the equivalent secret key.

The equivalent DNA-base permutation secret key is achieved by using the same method as Step 3 in Section 3.3.

Step 4. Recover images with the equivalent secret key:

This step is also the same as Step 4 in Section 3.3, so it is omitted.

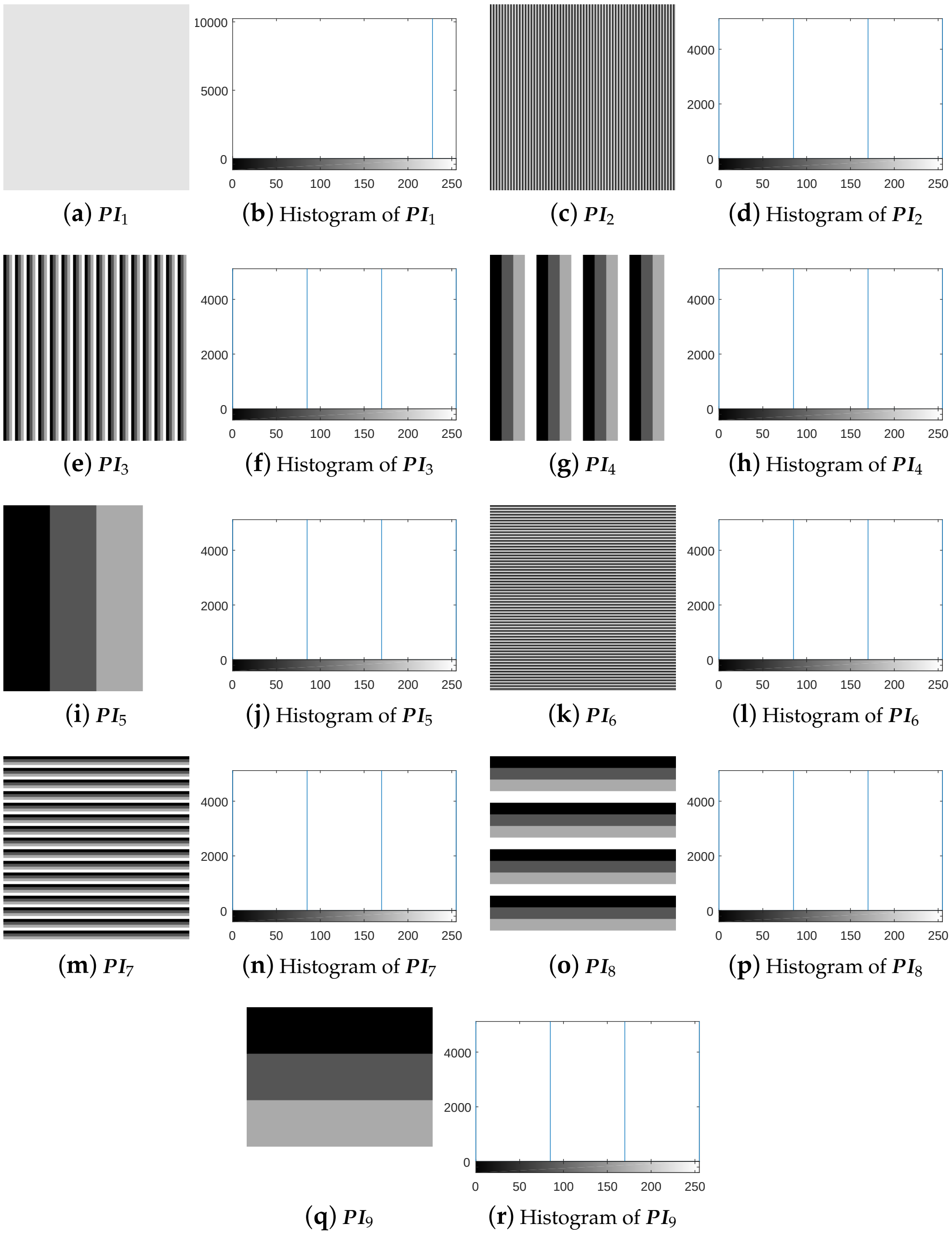
Therefore, the chosen-ciphertext attack is also valid for breaking IEA-DESC, and its data complexity is also $\boldsymbol{O}(1 + \lceil \log_4(HW) \rceil)$.

4. The Experiments for Breaking IEA-DESC

To verify the feasibility of the two proposed attack methods, some experimental simulations were performed based on a personal computer with Matlab R2016a. Similar to those in Reference [37], our experimental images are 8-bit grayscale images "Lenna" and "Peppers" of size 256 × 256.

4.1. Breaking IEA-DESC by Chosen-Plaintext Attack

The experiment for breaking IEA-DESC was firstly carried out by the chosen-plaintext attack method proposed in Section 3.3. Given $H = 256$ and $W = 256$, one gets $N_C = 1 + \lceil \log_4(H \times W) \rceil = 9$ from Equation (10). Correspondingly, the nine 8-bit images $\boldsymbol{PI}_n$ $(n = 1, 2, \ldots, 9)$ constructed using the method in Section 3.2 are shown in Figure 5a–r.



(**a**) $\boldsymbol{PI}_1$ (**b**) Histogram of $\boldsymbol{PI}_1$ (**c**) $\boldsymbol{PI}_2$ (**d**) Histogram of $\boldsymbol{PI}_2$

(**e**) $\boldsymbol{PI}_3$ (**f**) Histogram of $\boldsymbol{PI}_3$ (**g**) $\boldsymbol{PI}_4$ (**h**) Histogram of $\boldsymbol{PI}_4$

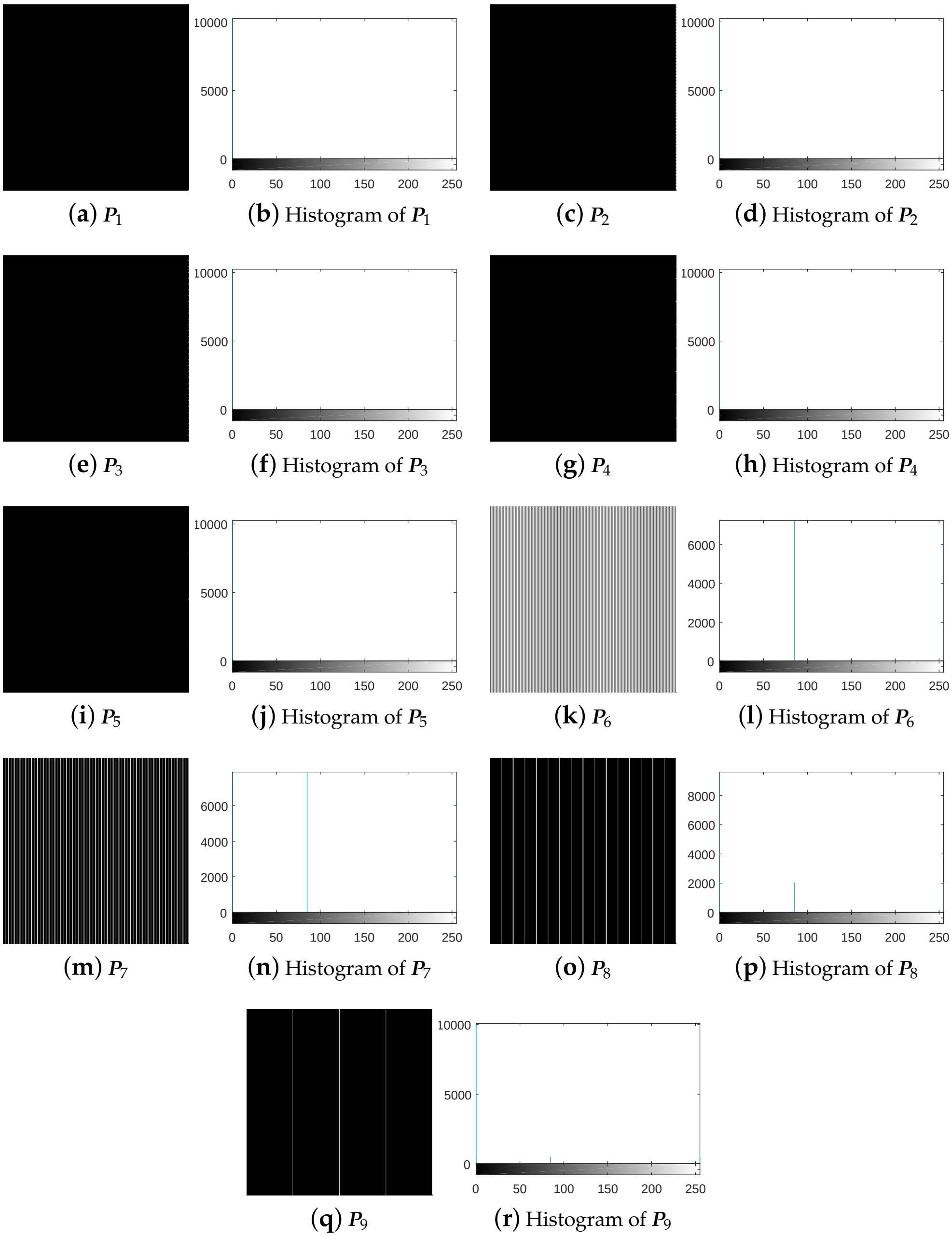
(**i**) $\boldsymbol{PI}_5$ (**j**) Histogram of $\boldsymbol{PI}_5$ (**k**) $\boldsymbol{PI}_6$ (**l**) Histogram of $\boldsymbol{PI}_6$

(**m**) $\boldsymbol{PI}_7$ (**n**) Histogram of $\boldsymbol{PI}_7$ (**o**) $\boldsymbol{PI}_8$ (**p**) Histogram of $\boldsymbol{PI}_8$

(**q**) $\boldsymbol{PI}_9$ (**r**) Histogram of $\boldsymbol{PI}_9$

Figure 5. The nine 8-bit special images and their corresponding histograms.

First, following Step 1 in Section 3.3, the nine special images shown in Figure 5 are selected as the diffused images $\boldsymbol{P}'_n(n = 1, 2, \ldots, 9)$, respectively, and then their corresponding plain-images $\boldsymbol{P}_n(n = 1, 2, \ldots, 9)$ are obtained, as shown in Figure 6a–r. Then, according to Step 2 in Section 3.3, the nine corresponding cipher-images $\boldsymbol{C}_n(n = 1, 2, \ldots, 9)$ and their histograms are obtained as shown in Figure 7a–r. Next, using the method in Step 3 in Section 3.3, the equivalent secret key EK_P is obtained using the nine chosen diffused images shown in Figure 5a–r and the nine corresponding cipher-images shown in Figure 7a–r. Finally, the images are recovered using the equivalent secret key EK_P. The attacking results on IEA-DESC with the 8-bit images "Lenna" and "Peppers" are shown in Figures 8a–d and 9a–d, respectively.



(**a**) P_1 (**b**) Histogram of P_1 (**c**) P_2 (**d**) Histogram of P_2

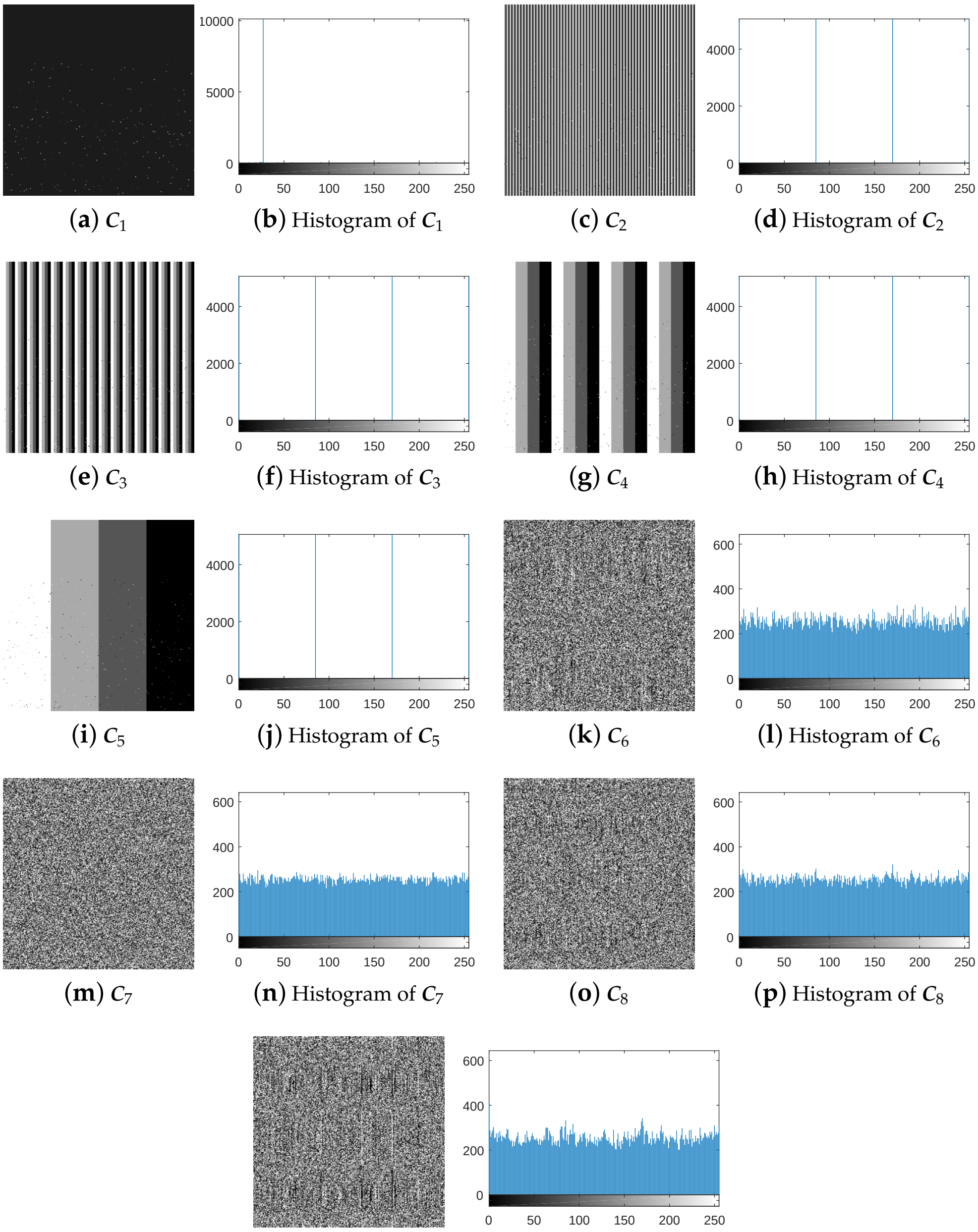
(**e**) P_3 (**f**) Histogram of P_3 (**g**) P_4 (**h**) Histogram of P_4

(**i**) P_5 (**j**) Histogram of P_5 (**k**) P_6 (**l**) Histogram of P_6

(**m**) P_7 (**n**) Histogram of P_7 (**o**) P_8 (**p**) Histogram of P_8

(**q**) P_9 (**r**) Histogram of P_9

Figure 6. The nine plain-images under chosen-plaintext attack.



(**a**) C_1 (**b**) Histogram of C_1 (**c**) C_2 (**d**) Histogram of C_2

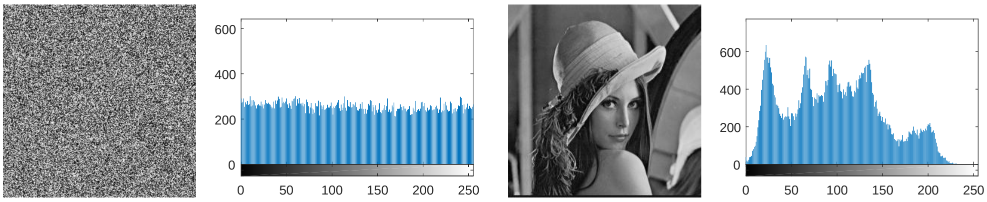
(**e**) C_3 (**f**) Histogram of C_3 (**g**) C_4 (**h**) Histogram of C_4

(**i**) C_5 (**j**) Histogram of C_5 (**k**) C_6 (**l**) Histogram of C_6

(**m**) C_7 (**n**) Histogram of C_7 (**o**) C_8 (**p**) Histogram of C_8

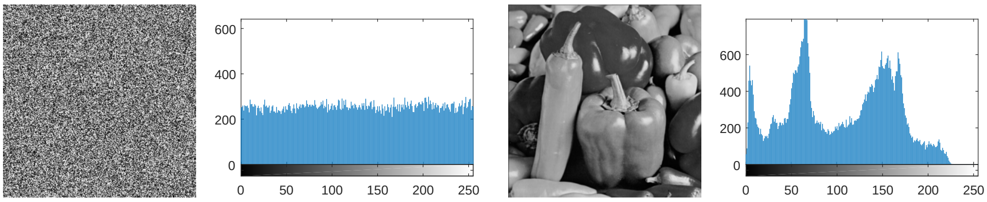
(**q**) C_9 (**r**) Histogram of C_9

Figure 7. The nine corresponding output cipher-images under chosen-plaintext attack.



(**a**) Cipher-image (**b**) Histogram (**c**) Recovered image (**d**) Histogram

Figure 8. Attacking result on IEA-DESC with the 8-bit image "Lenna".

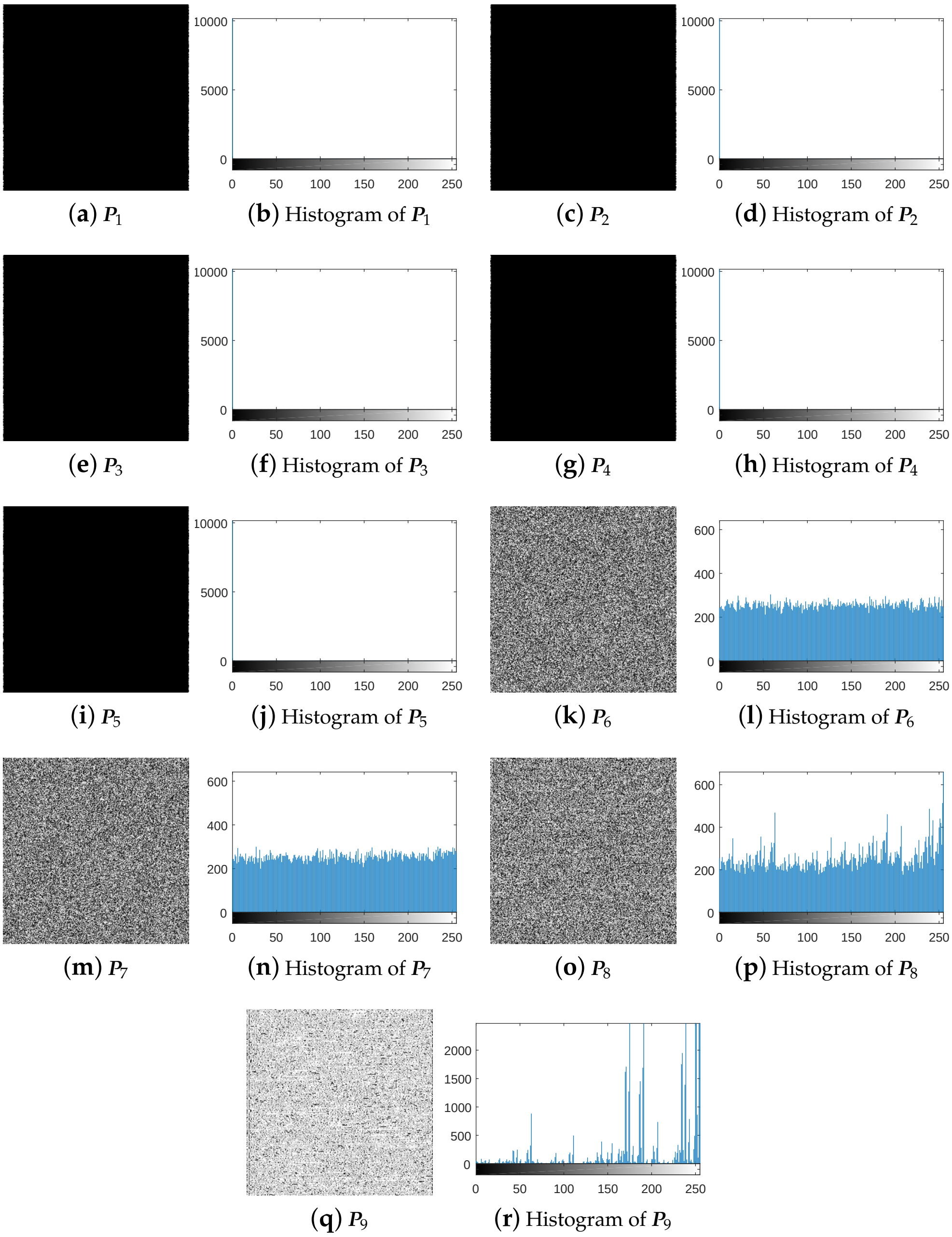


(**a**) Cipher-image (**b**) Histogram (**c**) Recovered image (**d**) Histogram

Figure 9. Attacking result on IEA-DESC with the 8-bit image "Peppers".

4.2. Breaking IEA-DESC Using the Chosen-Ciphertext Attack

Accordingly, the experiment for breaking IEA-DESC is accomplished using the chosen-ciphertext attack method proposed in Section 3.4.



(**a**) P_1 (**b**) Histogram of P_1 (**c**) P_2 (**d**) Histogram of P_2

(**e**) P_3 (**f**) Histogram of P_3 (**g**) P_4 (**h**) Histogram of P_4

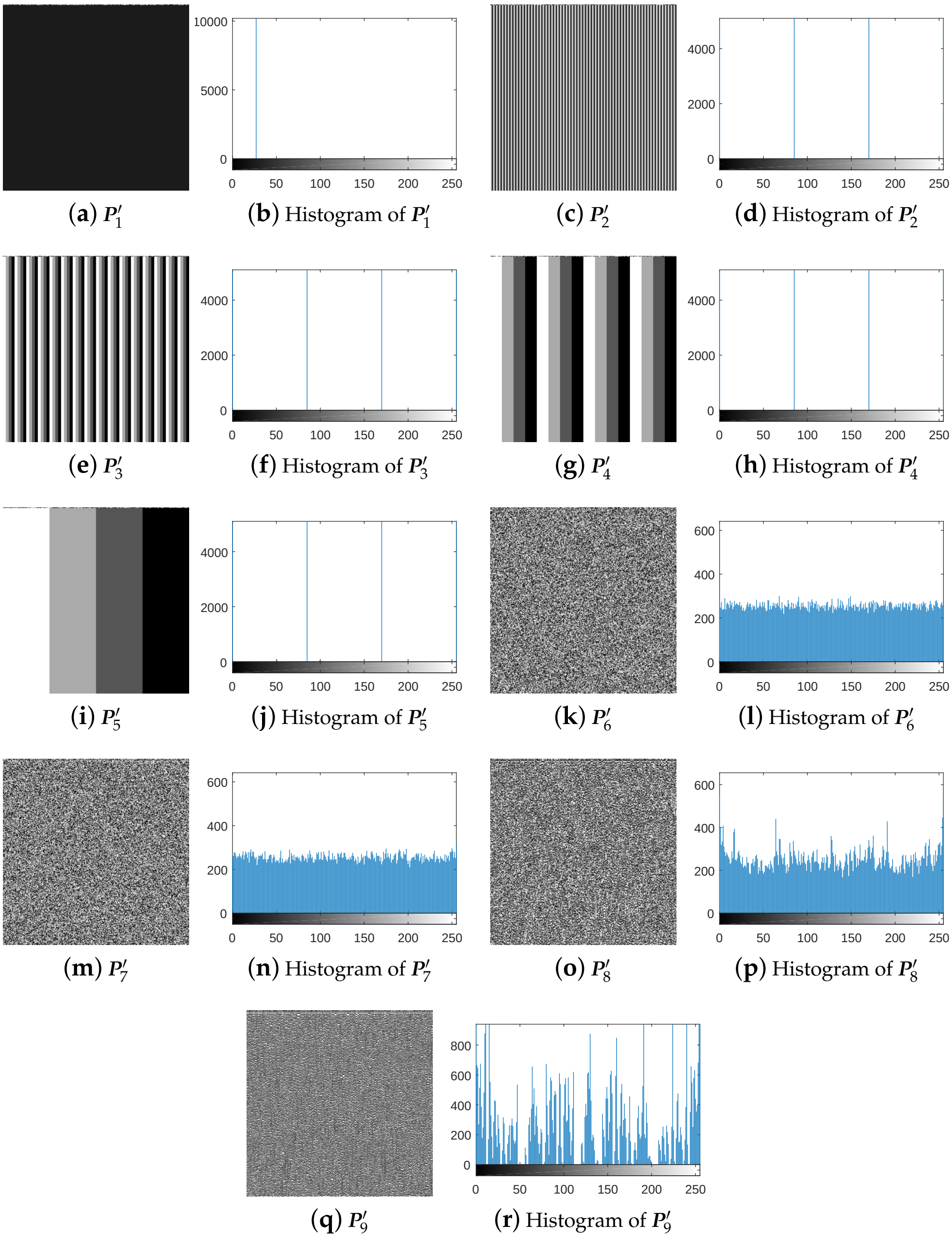
(**i**) P_5 (**j**) Histogram of P_5 (**k**) P_6 (**l**) Histogram of P_6

(**m**) P_7 (**n**) Histogram of P_7 (**o**) P_8 (**p**) Histogram of P_8

(**q**) P_9 (**r**) Histogram of P_9

Figure 10. The nine corresponding output plain-images under chosen-ciphertext attack.

First, following Step 1 in Section 3.4, the nine special images shown in Figure 5 are used as the cipher-images $\boldsymbol{C}_n(n = 1, 2, \ldots, 9)$ respectively, and then their corresponding plain-images $\boldsymbol{P}_n(n = 1, 2, \ldots, 9)$ are obtained, as shown in Figure 10a–r. Then, according to Step 2 in Section 3.4, the nine corresponding diffused images $\boldsymbol{P}'_n(n = 1, 2, \ldots, 9)$ and their histograms are obtained as shown in Figure 11a–r, respectively. Next, using the method in Step 3 in Section 3.4, the equivalent secret key EK_P is obtained using the nine chosen cipher-images shown in Figure 5a–r and the nine corresponding diffused images shown in Figure 11a–r. Finally, the images are recovered using the equivalent secret key EK_P. The attacking results on IEA-DESC with the 8-bit images "Lenna" and "Peppers" are also shown in Figures 8a–d and 9a–d, respectively.



(**a**) $\boldsymbol{P}'_1$ (**b**) Histogram of $\boldsymbol{P}'_1$ (**c**) $\boldsymbol{P}'_2$ (**d**) Histogram of $\boldsymbol{P}'_2$

(**e**) $\boldsymbol{P}'_3$ (**f**) Histogram of $\boldsymbol{P}'_3$ (**g**) $\boldsymbol{P}'_4$ (**h**) Histogram of $\boldsymbol{P}'_4$

(**i**) $\boldsymbol{P}'_5$ (**j**) Histogram of $\boldsymbol{P}'_5$ (**k**) $\boldsymbol{P}'_6$ (**l**) Histogram of $\boldsymbol{P}'_6$

(**m**) $\boldsymbol{P}'_7$ (**n**) Histogram of $\boldsymbol{P}'_7$ (**o**) $\boldsymbol{P}'_8$ (**p**) Histogram of $\boldsymbol{P}'_8$

(**q**) $\boldsymbol{P}'_9$ (**r**) Histogram of $\boldsymbol{P}'_9$

Figure 11. The nine corresponding diffused images under chosen-ciphertext attack.

4.3. Attack Complexity

In terms of attack complexity, the running times of the chosen-plaintext attack method and the chosen-ciphertext attack method are about 2.1165 s and 2.0785 s, respectively. Moreover, given 8-bit images of size 256 × 256, the data complexity of the two attack methods required for breaking IEA-DESC are both $\boldsymbol{O}(9)$. Therefore, the experimental results verify that the two attack methods are both effective and efficient.

5. Suggestions for Improvement

On the basis of the analysis above, IDE-DESC can neither resist against chosen-plaintext attacks nor chosen-ciphertext attacks because of its inherent security defects. In fact, some other chaos-based ciphers also have similar vulnerabilities as mentioned in Reference [36]. To deal with these problems, some suggestions for improvement to enhance the security are given below:

(1) Checking the validity of each encryption component is significant.

The diffusion part of IEA-DESC is invalid for the attacker because it does not involve any secret key parameter. In fact, it does not contribute to security, but increases the computational complexity of the algorithm. Therefore, the designed algorithms should be scrutinized from the perspective of cryptanalysis to ensure the validity of each encryption component.

(2) Exploiting some novel permutation mechanisms to enhance the security.

Like other permutation-only encryption algorithms, DNA-base permutation only changes the position but does not change the value of each element. The only difference is that the element is quaternary. For permutation-only algorithms, many studies have proved that they are insecure [39,40,44]. To fulfil this demand, exploiting some novel permutation mechanisms is worthwhile.

(3) Avoiding the existence of an equivalent secret key in the algorithm.

The encryption process of the algorithm should be associated with the characteristics of the plain-image or cipher-image [2]. Otherwise, the encryption process for different input images is completely identical, which may lead to the existence of an equivalent secret key. Once the equivalent secret key is obtained by an attacker, the encryption algorithm is broken [36].

(4) Appropriately increasing the number of encryption rounds.

In a single-round encryption algorithm, the confusion and diffusion characteristics maybe insufficient [42]. Increasing the number of encryption rounds can effectively improve this problem. Of course, it also requires higher computational complexity [21]. Therefore, ways in which to balance safety and efficiency deserves more research.

6. Conclusions

In this paper, the security of a recent image encryption algorithm called IEA-DESC has been analyzed in detail. It was claimed that some merits of DNA encoding and spatiotemporal chaos are inherited in the algorithm. However, its algorithm structure has several inherent security pitfalls. It was found that IEA-DESC is actually a combined process of DNA-base permutation and bitwise complement from the perspective of cryptanalysis. Therefore, a chosen-plaintext attack and a chosen-ciphertext attack were proposed to recover the equivalent secret key of IEA-DESC, respectively. Both theoretical analysis and experimental results are provided to support effectiveness and efficiency of two attack methods for breaking IEA-DESC. The reported results would help the designers of DNA-based cryptography pay more attention to importance of the essential structure of an encryption scheme, instead of the elegance of the underlying theory.

Author Contributions: Methodology, H.W.; Software, H.W.; Validation, S.Y. and J.L.; Supervision, S.Y.; Project Administration, S.Y. and J.L.; Funding Acquisition, J.L.

Funding: This research was funded by the National Key Research and Development Program of China (No. 2016YFB0800401), and the National Natural Science Foundation of China (No. 61532020, 61671161).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Özkaynak, F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dyn.* **2018**, *92*, 305–313. [CrossRef]
2. Wen, H.; Yu, S.; Lü, J. Encryption algorithm based on hadoop and non-degenerate high-dimensional discrete hyperchaotic system. *Acta Phys. Sin.* **2017**, *66*, 230503. [CrossRef]
3. Chen, S.; Yu, S.; Lü, J.; Chen, G.; He, J. Design and FPGA-based realization of a chaotic secure video communication system. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 2359–2371. [CrossRef]
4. Fridrich, J. Symmetric ciphers based on two-dimensional chaotic maps. *Int. J. Bifurc. Chaos* **1998**, *8*, 1259–1284. [CrossRef]
5. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [CrossRef]
6. Lorenz, E.N. Deterministic nonperiodic flow. *J. Atmos. Sci.* **1963**, *20*, 130–141. [CrossRef]
7. Gehani, A.; LaBean, T.; Reif, J. DNA-based cryptography. In *Aspects of Molecular Computing*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2950, pp. 167–188.
8. Abdo, A.; Lian, S.; Ismail, I.; Amin, M.; Diab, H. A cryptosystem based on elementary cellular automata. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 136–147. [CrossRef]
9. Yang, Y.G.; Tian, J.; Lei, H.; Zhou, Y.H.; Shi, W.M. Novel quantum image encryption using one-dimensional quantum cellular automata. *Inf. Sci.* **2016**, *345*, 257–270. [CrossRef]
10. Akhshani, A.; Akhavan, A.; Lim, S.C.; Hassan, Z. An image encryption scheme based on quantum logistic map. *Commun. Nonlinear Sci. Numer. Simul.* **2012**, *17*, 4653–4661. [CrossRef]
11. Askar, S.S.; Karawia, A.; Al-Khedhairi, A.; Al-Ammar, F.S. An algorithm of image encryption using logistic and two-dimensional chaotic economic maps. *Entropy* **2019**, *21*, 44. [CrossRef]
12. Karawia, A. Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. *Entropy* **2018**, *20*, 801. [CrossRef]
13. Liu, H.; Wang, X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt. Commun.* **2011**, *284*, 3895–3903. [CrossRef]
14. He, S.; Sun, K.; Wang, H. Complexity analysis and DSP implementation of the fractional-order lorenz hyperchaotic system. *Entropy* **2015**, *17*, 8299–8311. [CrossRef]
15. Chen, C.; Sun, K.; Peng, Y.; Alamodi, A.O. A novel control method to counteract the dynamical degradation of a digital chaotic sequence. *Eur. Phys. J. Plus* **2019**, *134*. [CrossRef]
16. Li, C.; Feng, B.; Li, S.; Kurths, J.; Chen, G. Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*. [CrossRef]
17. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
18. Chai, X.; Gan, Z.; Yang, K.; Chen, Y.; Liu, X. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Process. Image Commun.* **2017**, *52*, 6–19. [CrossRef]
19. Zhang, L.; Sun, K.; Liu, W.; He, S. A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations. *Chin. Phys. B* **2017**, *26*, 100504. [CrossRef]
20. Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **2019**, *155*, 44–62. [CrossRef]
21. Li, C.; Lin, D.; Feng, B.; Lü, J.; Hao, F. Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *IEEE Access* **2018**, *6*, 75834–75842. doi:10.1109/ACCESS.2018.2883690. [CrossRef]
22. Lin, Z.; Yu, S.; Feng, X.; Lü, J. Cryptanalysis of a chaotic stream cipher and its improved scheme. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850086. [CrossRef]
23. Zhu, C.; Wang, G.; Sun, K. Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps. *Entropy* **2018**, *20*, 843. [CrossRef]

24. Li, C.; Liu, Y.; Zhang, L.Y.; Wong, K.W. Cryptanalyzing a class of image encryption schemes based on Chinese Remainder Theorem. *Signal Process. Image Commun.* **2014**, *29*, 914–920. [CrossRef]
25. Zhang, Q.; Guo, L.; Wei, X. Image encryption using DNA addition combining with chaotic maps. *Math. Comput. Model.* **2010**, *52*, 2028–2035. [CrossRef]
26. Hermassi, H.; Belazi, A.; Rhouma, R.; Belghith, S.M. Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. *Multimed. Tools Appl.* **2014**, *72*, 2211–2224. [CrossRef]
27. Zhen, P.; Zhao, G.; Min, L.; Jin, X. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimed. Tools Appl.* **2016**, *75*, 6303–6319. [CrossRef]
28. Su, X.; Li, W.; Hu, H. Cryptanalysis of a chaos-based image encryption scheme combining DNA coding and entropy. *Multimed. Tools Appl.* **2017**, *76*, 14021–14033. [CrossRef]
29. Jain, A.; Rajpal, N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimed. Tools Appl.* **2016**, *75*, 5455–5472. [CrossRef]
30. Dou, Y.; Liu, X.; Fan, H.; Li, M. Cryptanalysis of a DNA and chaos based image encryption algorithm. *Optik-Int. J. Light Electron Opt.* **2017**, *145*, 456–464. [CrossRef]
31. Sun, S. A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. *IEEE Photonics J.* **2018**, *10*, 1–14. [CrossRef]
32. Feng, W.; He, Y. Cryptanalysis and improvement of the hyper-chaotic image encryption scheme based on DNA encoding and scrambling. *IEEE Photonics J.* **2018**, *10*, 1–15. [CrossRef]
33. Özkaynak, F.; Yavuz, S. Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Nonlinear Dyn.* **2014**, *78*, 1311–1320. [CrossRef]
34. Zhang, Y.; Xiao, D.; Wen, W.; Wong, K.W. On the security of symmetric ciphers based on DNA coding. *Inf. Sci.* **2014**, *289*, 254–261. [CrossRef]
35. Li, C.; Lin, D.; Lü, J. Cryptanalyzing an Image-Scrambling Encryption Algorithm of Pixel Bits. *IEEE Multimed.* **2017**, *24*, 64–71. [CrossRef]
36. Li, C.; Lin, D.; Lü, J.; Hao, F. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. *IEEE Multimed.* **2018**, *25*, 46–56. [CrossRef]
37. Song, C.; Qiao, Y. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy* **2015**, *17*, 6954–6968. [CrossRef]
38. Schneier, B. *Applied Cryptography—Protocols, Algorithms, and Souce Code in C*, 2nd ed.; John Wiley & Sons, Inc.: New York, NY, USA, 1996.
39. Li, C.; Lo, K.T. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process.* **2011**, *91*, 949–954. [CrossRef]
40. Jolfaei, A.; Wu, X.W.; Muthukkumarasamy, V. On the security of permutation-only image encryption schemes. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 235–246. [CrossRef]
41. Gao, H.; Zhang, Y.; Liang, S.; Li, D. A new chaotic algorithm for image encryption. *Chaos Solitons Fractals* **2006**, *29*, 393–399. [CrossRef]
42. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurc. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
43. Xie, E.Y.; Li, C.; Yu, S.; Lü, J. On the cryptanalysis of Fridrich's chaotic image encryption scheme. *Signal Process.* **2017**, *132*, 150–154. [CrossRef]
44. Li, C. Cracking a hierarchical chaotic image encryption algorithm based on permutation. *Signal Process.* **2016**, *118*, 203–210. [CrossRef]