RESEARCH ARTICLE

New insights into the existing image encryption algorithms based on DNA coding

Xianglian Xue[1,2]*, **Dongsheng Zhou**[3], **Changjun Zhou**[4]

1 Section of Computer Teaching and Research, Shaanxi University of Chinese Medicine, Xianyang, China, **2** Laboratory of Network Computer and Security Technology in Shaanxi Province, Xi'an University of Technology, Xi'an, China, **3** Key Laboratory of Advanced Design and Intelligent Computing, Ministry of Education, Dalian University, Dalian, China, **4** College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua, China

* xuexianglian0419@126.com

OPEN ACCESS

Citation: Xue X, Zhou D, Zhou C (2020) New insights into the existing image encryption algorithms based on DNA coding. PLoS ONE 15 (10): e0241184. https://doi.org/10.1371/journal.pone.0241184

Editor: Jun Ma, Lanzhou University of Technology, CHINA

Received: April 21, 2020

Accepted: October 10, 2020

Published: October 23, 2020

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: Changjun Zhou 61672121 the National Natural Science Foundation of China Yes Dongsheng Zhou in part by program for the Liaoning Distinguished Professor, the Science and Technology Innovation Fund of Dalian (No.2018J12GX036). Yes There was no additional external funding received for this study.

Competing interests: The authors have declared that no competing interests exist.

Abstract

Because a DNA nucleotide sequence has the characteristics of large storage capacity, high parallelism, and low energy consumption, DNA cryptography is favored by information security researchers. Image encryption algorithms based on DNA coding have become a research hotspot in the field of image encryption and security. In this study, based on a comprehensive review of the existing studies and their results, we present new insights into the existing image encryption algorithms based on DNA coding. First, the existing algorithms were summarized and classified into five types, depending on the type of DNA coding: DNA fixed coding, DNA dynamic coding, different types of base complement operation, different DNA sequence algebraic operations, and combinations of multiple DNA operations. Second, we analyzed and studied each classification algorithm using simulation and obtained their advantages and disadvantages. Third, the DNA coding mechanisms, DNA algebraic operations, and DNA algebraic combination operations were compared and discussed. Then, a new scheme was proposed by combining the optimal coding mechanism with the optimal DNA coding operation. Finally, we revealed the shortcomings of the existing studies and the future direction for improving image encryption methods based on DNA coding.

1 Introduction

Since Dr. Adleman of the United States used DNA molecular biological computing to solve the directed path problem of seven nodes [1] in 1994, DNA computing has attracted the attention of researchers across the world [2–5]. In DNA computing, DNA nucleotide bases A, C, G, and T coding sequences are used as carriers of information; it has great advantages in dealing with large storage capacity, parallelism, and energy consumption of information [6–9]. DNA computing essentially uses biochemical experiments to address practical problems. However, because of the limitations of biochemical reaction conditions, such as expensive experimental equipment, environmental requirements, difficulty in extracting DNA sequence, and difficulties in controlling the concentration, temperature, and PH of the reactant, studying DNA computing is difficult. Regarding image encryption in DNA computing, researchers ignore the complex experimental links of DNA, only use DNA coding to carry image information, and design a reasonable and effective encryption algorithm by combining chaotic mapping with different DNA coding algorithms. This idea gives rise to new perspectives in the research on image encryption.

From 2009 to 2014, Zhang et al. innovatively used DNA coding methods for image encryption, and proposed many image encryption algorithms based on DNA coding [10–17]; this created new ideas in DNA cryptography. Their main encryption ideas involve the following four steps. First, the original image is encoded using the DNA encoding rule. Then, the position of the DNA-encoded matrix is scrambled by the chaotic sequences generated by the one-dimensional chaotic system [14], combination of several low-dimensional chaotic systems [10–12], and hyper chaotic system [13, 15] or the combination of several hyper chaotic systems [16, 17]. Subsequently, the values of the image pixels are changed by various operations, namely, DNA addition and subtraction [10, 12, 13], XOR [15], DNA subsequence [16], DNA complement [11], or the combination of these operations [14, 17] under the control of chaotic sequences. Finally, the encrypted image is obtained by DNA decoding and regrouping. The image encryption technology based on DNA coding proposed by Zhang et al. combined DNA coding and image encryption effectively. Consequently, the application of DNA cryptography in image encryption garnered the attention of many researchers both home and abroad. However, in recent years, researchers have highlighted many shortcomings in the methods proposed by Zhang et al. For example, [18, 19] observed that the method of Zhang [12] combined DNA addition with chaotic mapping to encrypt an image. Nevertheless, the addition operation of this method is non-invertible; therefore, the decrypted image cannot be obtained. Belazi [20], Liu [21], and Wang [22] used an RGB image encryption algorithm based on DNA coding and chaotic mapping proposed by Liu and Zhang [14], to restore original images using chosen-plaintext attack (CPA). Wang indicated that the main drawback of this algorithm is that the key used for the encryption is independent of the original image. Furthermore, changing a base in DNA can only affect the base in one position; moreover, the diffusion ability of the base is poor, resulting in poor diffusion ability of the image pixels. Similarly, an image fusion encryption algorithm based on the DNA sequence operation and hyper chaotic system proposed by Zhang and Guo et al. [15] was broken by choosing different sizes of plain images in [23–26]. Li [27] analyzed some image encryption algorithms based on the DNA subsequence operation and chaotic system proposed by Zhang [16] using CPA to obtain original images. In summary, although the methods proposed by Zhang et al. are effective, their security is very poor.

Since 2015, some researchers have applied a combination of multiple simple chaos, more complex, or more secure chaotic systems to encrypt images, for enhancing the security. For instance, Wu [28] used three one-dimensional chaotic systems combined with the DNA addition and subtraction, and XOR operations. Zhang [29] and Mondal [30] used a mixed linear–nonlinear coupled map lattices (MLNCML) system embedded logistic, and Zhang [31] used a fractional-order piecewise-linear (PWL) hyperchaotic map combined with DNA addition and subtraction, to realize image encryption. Li [32] used fractional-order hyper chaotic mapping Lorenz (FOHCL) to determine the rules of DNA addition and subtraction as well as DNA XOR. Color images are encrypted using a logistic system in combination with DNA addition and subtraction, and XOR [33]. Similarly, Zhang [34] used a logistic system combined with DNA addition, subtraction, and complementation. The DNA coding method used in the above-mentioned algorithms is the same as that in the method of Zhang et al., which adopts fixed DNA coding, and gives DNA coding operation rules (DNA addition and subtraction, DNA XOR, and DNA complementation). The security of the above-mentioned encryption algorithms is guaranteed by a chaotic system. Without a chaotic system, the image encryption based on DNA would only be a binary bit computation. If the security is greatly threatened, it is difficult to resist the brute-force attack, known plaintext attack (KPA), and CPA. For instance, Dou [35] used brute-force attack and CPA to analyze Ref. [30], and restored the plaintext image. In addition, Kumar [36] used DNA encoding and elliptic curve Diffie–Hellman cryptography without a chaotic system to realize RGB image encryption. However, this method was less-secure, and was broken by Akhavan [37] via CPA.

For these reasons, dynamic DNA coding and more complex DNA coding algorithms have been proposed in recent years. Kalpana [38], Zhang [39], Zhen [40], Cai [41], Rehman [42], and many others proposed various dynamic DNA coding algorithms. They first defined different DNA coding rules, and used chaotic sequences to select DNA coding rules dynamically to encode images. Further, [39, 43, 44] proposed replacing the conventional single-base complement operation with a complement operation based on the principle of base complementation, to increase the complexity of DNA operation. These encryption algorithms achieved better encryption results. Belazi [45] proposed a novel medical image encryption scheme based on chaos and DNA encoding, and realized two encryption rounds using different coding rules and complement, and XOR operation under chaotic control. This method achieves good encryption, and could resist all types of attacks. Furthermore, a new image encryption scheme based on CML and DNA sequences was proposed by Wang [46], which also performs good encryption. Nevertheless, because fixed DNA coding was selected in their coding process, and the security could be improved. Dagadu [47] proposed a medical image encryption scheme based on multiple chaos and DNA coding, different DNA coding rules, and XOR operation combined with chaotic map to realize image encryption. Although the scrambling degree in their method was high, it could not resist CPA and KPA.

This literature review reveals that researchers generally improve the performance of the encryption algorithms by changing the DNA coding methods and operations. The existing studies simply use a DNA coding method, DNA coding operation (addition, subtraction, complement, XOR, etc.), or a combination of multiple coding operations to realize image encryption, without comprehensively comparing or analyzing the methods or operations. Put differently, in any existing study, the reasons for selecting a specific DNA coding (fixed or dynamic coding) method, DNA coding operation, or a combination of multiple coding operations to realize image encryption are unclear.

Therefore, this study provides new insights into the existing image encryption algorithms based on DNA coding. We categorized the existing image encryption algorithms based on DNA coding into five types, depending on the type of DNA coding: fixed DNA coding, dynamic DNA coding, different types of DNA base complement operations, different DNA sequence algebraic operations, and combinations of multiple DNA operations. Then, a more detailed classification is performed according to the characteristics of the different algorithms. Furthermore, we comprehensively compared and analyzed all these methods, and revealed their advantages and disadvantages. Further, the DNA coding mechanism, DNA algebraic operation, and DNA algebraic combination operation are compared, and the newly proposed scheme is discussed. Finally, the study highlights the shortcomings and indicates the future research direction for improving image encryption based on DNA coding.

The remainder of this manuscript is structured as follows. In the second section, the theoretical basis of this study is introduced. In the third section, we categorize the existing DNA coding-based image encryption methods, and discuss their advantages and disadvantages by a comprehensive comparison and analysis, and on the basis of above discussion a new method is proposed. Finally, the last section discusses the shortcomings and the future research direction for improving image encryption based on DNA coding.

2 Theoretical basis of this study

2.1 DNA coding

A DNA sequence is composed of four nucleic acid bases, namely, adenine (A), cytosine(C), guanine (G), and thymine (T), wherein A and T, and G and C are complements. Researchers use the binary values 00, 01, 10, and 11 to denote these four bases. A total of 24 types of coding can be listed; however, according to the complementary relation between 0 and 1 in binary, it can be deduced that 00 and 11 are complements, and that 01 and 10 complement each other. Therefore, 8 out of the 24 coding rules are selected to satisfy the base complementary criterion shown in Table 1. The pixel value of an image lies between [0, 255], and consists of eight-bit binary numbers; therefore, a single pixel value may consist of four-bit DNA bases. For example, for a pixel value of 175, the corresponding binary bit is "10101111," the DNA sequence generated by the R1 rule presented in Table 1 is "GGTT," and decoding is performed with the same rule or with the other seven different rules. The existing image encryption algorithms based on DNA coding are almost inseparable from this coding rule or deforming based on this coding rule.

2.2 DNA complement rules

Two methods are available for image encryption based on DNA sequence complement: (1) single base direct complement method, and (2) the method that uses the principle of single base and double base complementary pairing in biotechnology to perform the complement operation. A single base direct complement is defined as follows:

$$\begin{cases} T = complement(A) \\ A = complement(T) \\ G = complement(C) \\ C = complement(G) \end{cases} \quad (1)$$

where complement (.) is the function of the complement. The complement of base A is T, and that of base C is G. The corresponding binary complement is satisfied when both the complement of 00 is 11 and that of 01 is 10, and vice versa.

The complement rule is defined based on a double helix structure; a nucleoside is paired according to the double helix structure. Supposing the complementary transformation is D, every nucleoside x_i satisfies the following equation:

$$\begin{cases} x_i \neq D(x_i) \neq D(D(x_i)) \neq D(D(D(x_i))) \\ x_i = D(D(D(D(x_i)))) \end{cases} \quad (2)$$

where x_i and $D(x_i)$ are complementary, i.e., x_i and $D(x_i)$ are a pair of base pairs. These base

Table 1. Eight types of DNA coding rules.

Binary	R1	R2	R3	R4	R5	R6	R7	R8
00	A	A	C	C	G	G	T	T
01	C	G	A	T	A	T	C	G
10	G	C	T	A	T	A	G	C
11	T	T	G	G	C	C	A	A

https://doi.org/10.1371/journal.pone.0241184.t001

Table 2. Complement operation for base complementary principle.

Rules	Complement operation			
R1	(AT)	(TC)	(CG)	(GA)
R2	(AT)	(TG)	(GC)	(CA)
R3	(AC)	(CG)	(GT)	(TA)
R4	(AC)	(CT)	(TG)	(GA)
R5	(AG)	(GC)	(CT)	(TA)
R6	(AG)	(GT)	(TC)	(CA)

https://doi.org/10.1371/journal.pone.0241184.t002

pairs must satisfy the condition of single-shot mapping. Based on the above equation, the base pairs satisfying single-shot mappings are listed in Table 2 [48].

2.3 DNA addition, subtraction, and XOR algebra operations

Because encoding and decoding processes are implemented in binary, the algebraic operation of the DNA sequence (addition or subtraction) follows the binary operation rule. The coding of eight different rules corresponds to eight different operations (addition or subtraction). In the processes of encryption and decryption, the addition and subtraction operations are reciprocal. Furthermore, the inverse operation of XOR remains an XOR operation. Therefore, we only list the addition and XOR operations, and Table 3 is based on the addition and XOR operations of R1 in Table 1.

2.4 Correlation equation of this study

For a comprehensive comparison, we use the logistic chaotic sequence under the same parameter to act on the operation of the DNA sequence. Additionally, histogram, information entropy [49], rate of base distribution, hamming distance [50], fixed point ratio [51], histogram variance [52], correlation coefficient, and the number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used as the evaluation indexes. The relevant theories of these evaluation indexes are given by the following Eqs (3)–(16).

1. Logistic map

A logistic map is an excellent chaotic map. A logistic map is used in this study for experimental simulation, and is described as follows:

$$x_{n+1} = \mu x_n(1 - x_n) \tag{3}$$

where $\mu \in [0, 4]$, $x_n \in (0, 1)$, $n = 0, 1, 2. . .,$. The study result showed that the system is in a chaotic state under the condition $3.569945 < \mu \leq 4$.

2. Global information entropy and local information entropy

Table 3. DNA sequence of addition and XOR operations.

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

https://doi.org/10.1371/journal.pone.0241184.t003

The global information entropy is defined below.

$$H(m) = -\sum_{i=0}^{L} P(m_i) log_2 P(m_i) \tag{4}$$

where m_i denotes the *ith* grey value for the L level grey image, and $P(m_i)$ represents the emergence probability of m_i. The information entropy of an ideal random image is eight.

The local information entropy is defined below.

In a test image S, we select the non-overlapping image blocks S_1, S_2, S_3. . .S_k randomly, and calculate the information entropy of each image block using Eq (4). Here, the intensity scale of the test image is L; generally, L = 256. Finally, the following equation is used to calculate the average value of the information entropy of the image blocks.

$$H(S)_{local} = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{5}$$

where $H(S)_{local}$ denotes the local information entropy of the image blocks, and i = 1,2,3. . .k.

3. Rate of base distribution

The rate of base distribution is defined below.

$$AP = count(A) \div (M \times N \times 4) \times 100\% \tag{6}$$

where count (A) denotes the number of bases "A" in the entire image coding matrix; M ×N denotes the size of the image (a pixel can be represented by four bases; therefore, M×N×4 is the total number of bases); and AP denotes the percentage of base "A" in the entire coding matrix (the distribution of other bases is similar). Because DNA coding consists of four different bases (A, C, G, and T), the distribution rate of the DNA bases in an ideal random image should be 25%.

4. Hamming distance

The hamming distance is used to calculate the total number of different bases at the same location for two sequences of equal length, and is given by,

$$\begin{cases} D(M, N) = \sum_{i=0}^{L} d(m_i, n_i) \\ d(m_i, n_i) = \begin{cases} 0, & if \;\; m_i = n_i \\ 1, & if \;\; m_i \neq n_i \end{cases} \end{cases} \tag{7}$$

where m_i and n_i denote the *ith* base of the DNA sequence M and N, respectively, and D(M,N) denotes the hamming distance of M and N; the greater the hamming distance, the greater the difference between the bases in the two sequences.

5. Fixed point ratio

Let $O = (O_{i,j})_{M\times N}$ and $N = (N_{i,j})_{M\times N}$ represent the original and encrypted images, respectively, where $M \times N$ defines their sizes. If the pixel position (i,j) in an image O does not change its gray value after scrambling (i.e., $o_{ij} = n_{ij}$), the pixel is a fixed point. We use the following equation to represent the fixed point ratio:

$$FP(O, N) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} f(i, j)}{M \times N} \times 100\% \tag{8}$$

If $o_{ij} = n_{ij}$, $f(i, j) = 1$, and if $o_{ij} \neq n_{ij}$, $f(i, j) = 0$; clearly, the smaller the fixed point ratio of the two images, the greater the difference between the encrypted image and the original image and the better the scrambling effect.

6. Histogram variance

In addition to visual analysis to determine the distribution of image histograms, the histogram variance can be used for quantitative analysis. It is known that visual analysis is often unreliable. The histogram variance is defined below.

$$Var(M) = \frac{1}{n^2} \times \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(m_i - m_j)^2 \tag{9}$$

where $M = m_0, m_1, \ldots, m_{255}$ denotes the vector of the histogram value, m_i and m_j denote the numbers of pixels whose gray values are given by i and j, respectively, and n is the greyness level. Clearly, the smaller the histogram variance, the more uniform the histogram distribution of the image.

7. Correlation coefficient

The correlation of the adjacent pixels in an original image is very high. Therefore, the better the encryption, the smaller the correlation coefficient (close to 0). In this study, we randomly select 8000 pairs (horizontal, vertical, and diagonal) of adjacent pixels from the original and encrypted images. Then, we use the following equations [53] to calculate the correlation coefficient:

$$E(x) = \frac{1}{N} \times \sum_{i=1}^{N} x_i \tag{10}$$

$$D(x) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x)^2) \tag{11}$$

$$cov(x) = \frac{1}{N} \times \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{12}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{13}$$

where x and y denote the grey value of two adjacent pixels in the image.

8. Analysis of differences between two images

The NPCR and UACI are used in this study to analyze the differences between two images. They are defined as follows [54]:

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} D(i,j)}{M \times N} \times 100\% \tag{14}$$

$$D(i,j) = \begin{cases} 0, & if \;\; E(i,j) = E^{'}(i,j) \\ 1, & if \;\; E(i,j) \neq E^{'}(i,j) \end{cases} \tag{15}$$

$$UACI = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} \frac{|E(i,j) - E^{'}(i,j)|}{255}}{M \times N} \times 100\% \tag{16}$$

3 Analysis and comparison of the existing DNA coding-based image encryption methods

The existing image encryption algorithms based on DNA coding involve four basic processes: (1) scrambling the pixel position of the image by using a chaotic sequence; (2) encoding the scrambled image matrix to the DNA sequence; (3) disturbing the DNA sequence matrix by using a chaotic sequence combined with addition, subtraction, XOR, or complement operation, or a combination of these operations; (4) obtaining the encrypted image by DNA decoding and recombination. The block diagram of these processes is shown in Fig 1. As discussed already, a DNA chain consists of four bases (A, C, G, and T), which are used as the carriers of information. The process of converting the information into a DNA nucleotide chain is known as encoding. The opposite process of converting a DNA nucleotide into information is known as decoding. These processes are depicted in Fig 1. DNA encoding and decoding are the key problems in image encryption based on DNA coding. As discussed already, a DNA operation includes addition, subtraction, XOR, and complement. Apparently, different types of encoding, operations, and decoding can produce different encryption results. Therefore, researchers use different methods of DNA encoding and decoding, and different DNA operations, to achieve safer and more effective image encryption.

Now, the existing image encryption algorithms based on DNA coding are categorized into five, depending on the type of DNA coding: fixed DNA coding, dynamic DNA coding, different types of base complement operations, different DNA sequence algebra operations, and combinations of multiple DNA operations. Dynamic DNA coding is further classified into three categories: image block or row-column dynamic coding (row-by-row), pixel dynamic coding (pixel-by-pixel), and binary bit dynamic coding. The image encryption based on different types of base complement operations is categorized into two: single base direct complement method and base complementary method based on the principle of base complement (static regular base complement and dynamic regular base complement). Further, addition and subtraction operations and the XOR operation based on different DNA sequence algebra operations are available. We not only analyzed and compared all the five methods independently, but also compared and studied the DNA coding mechanism, DNA coding operation, and DNA combination operation intensively. The specific classification scheme is shown in Fig 2.

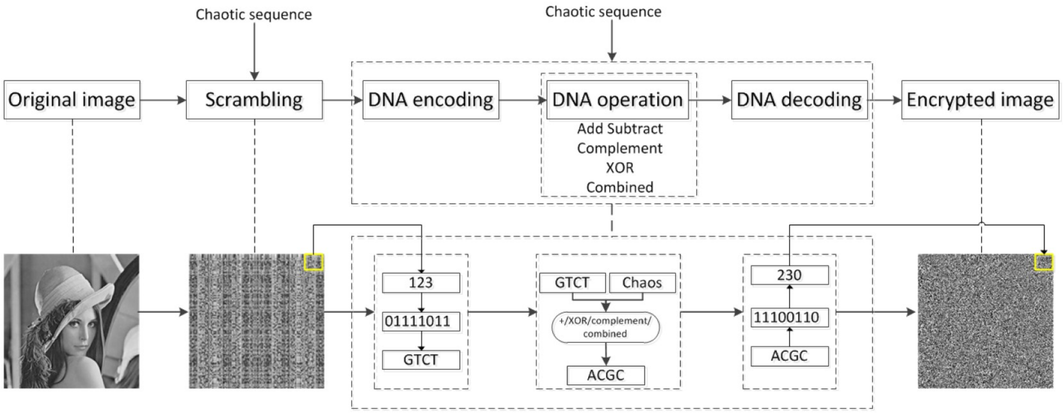


Fig 1. Block diagram of image encryption based on DNA coding.

https://doi.org/10.1371/journal.pone.0241184.g001

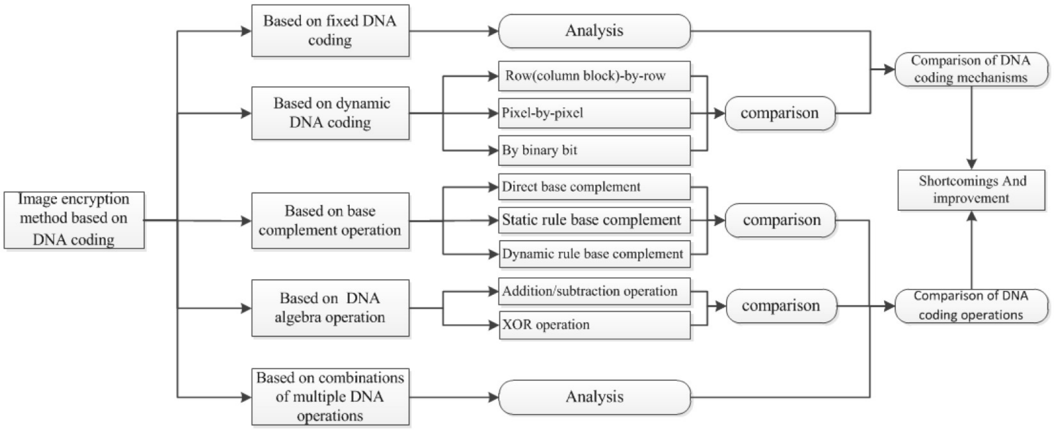


Image encryption method based on DNA coding
Based on fixed DNA coding
Based on dynamic DNA coding
Based on base complement operation
Based on DNA algebra operation
Based on combinations of multiple DNA operations
Analysis
Row(column block)-by-row
Pixel-by-pixel
By binary bit
Direct base complement
Static rule base complement
Dynamic rule base complement
Addition/subtraction operation
XOR operation
Analysis
comparison
comparison
comparison
Comparison of DNA coding mechanisms
Shortcomings And improvement
Comparison of DNA coding operations

Fig 2. The framework of this research.

https://doi.org/10.1371/journal.pone.0241184.g002

3.1 Image encryption based on fixed DNA coding

Researchers typically use a DNA coding rule listed in Table 1 for encoding; after performing some DNA operations, the DNA sequence is decoded using the same encoding rule or other encoding rules listed in Table 1. We refer to the way of coding as the fixed DNA coding method in this study. The previous studies [55–58] adopted a specific coding rule for encoding, and used the same rule for decoding. For example, for the pixel value of 175, the corresponding binary bit is "10101111," the DNA sequence generated using the R1 rule defined in Table 1 is "GGTT," and decoding is performed using the same rule. Apparently, multi-step encryption operations must be performed before decoding. However, [10–14, 16, 17] randomly selected one of the eight coding rules for encoding, and selected other rules for decoding using seed key1 and key2. For instance, the pixel value of 175 was encoded with the R1 rule to generate the DNA sequence "GGTT," and "GGTT" was decoded using the R5 rule to obtain the binary bit "00001010"; the corresponding decimal number is 10. Apparently, the pixel values are changed in this manner.

To further analyze and study the image encryption algorithm based on DNA fixed coding, we conducted two experiments.

Experiment 1: A "lena" image whose size is 256×256 was first encoded using the R1 rule defined in Table 1. Then, the encrypted image was obtained by decoding using the other seven rules. The results are shown in Fig 3.

Experiment 2: Eqs (4), (6) and (8) are used to calculate the base distribution, information entropy, and histogram variance of the eight different coding. Then, the time complexity of the algorithm and the maximum distance between the base distribution and 25% are calculated. The results are presented in Table 4.

From the analysis of the test results of Experiment 1, the results of encoding by R1 and decoding by the other seven rules are shown in Fig 3. In fact, Fig 3(a) can be regarded as an image encoded by R1 and decoded by R1. The results shown in Fig 3(a), 3(b), 3(d), 3(e), 3(c), 3(f), 3(g) and 3(h) are similar based on visual observations. Therefore, it can be concluded that among the eight types of coding mechanisms, only four are effective. The contour of the original image can be observed in all the encrypted images. Table 4, which presents the results of Experiment 2, shows that the base distributions of the eight coding rules are not uniform. The maximum distance between the base distribution and 25% is 10.6%, and the base distributions of R1 and R2, R3 and R4, R5 and R6, and R7 and R8 are very similar. Their information

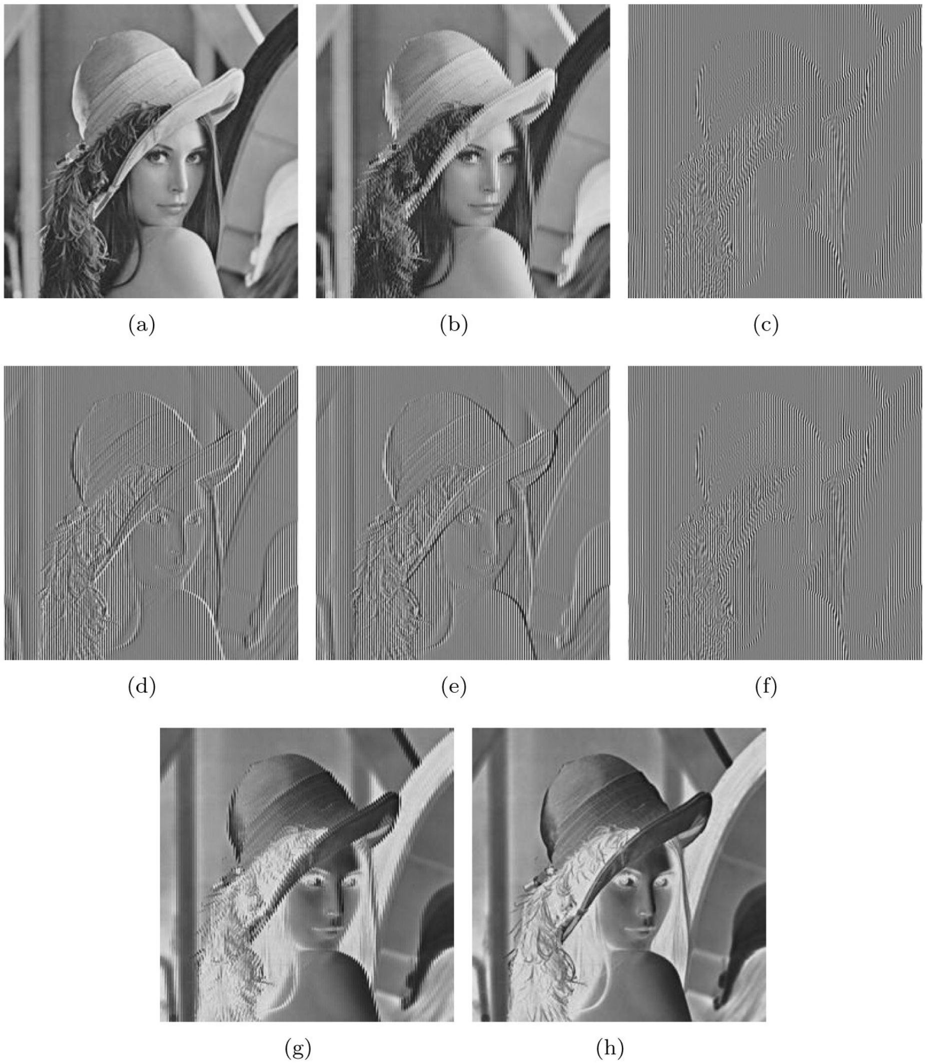


Fig 3. Encoding of original image using the R1 rule and decoding it using the remaining seven rules to obtain the encrypted image: (a)Original image. (b) Encoding with R1 and decoding with R2. (c) Encoding with R1 and decoding with R3. (d) Encoding with R1 and decoding with R4. (e) Encoding with R1 and decoding with R5. (f) Encoding with R1 and decoding with R6. (g) Encoding with R1 and decoding with R7. (h) Encoding with R1 and decoding with R8.

https://doi.org/10.1371/journal.pone.0241184.g003

Table 4. Comparison of the characteristics of the eight different fixed coding.

Comparative characteristic	R1	R2	R3	R4	R5	R6	R7	R8
AP	35.60%	35.60%	15.24%	15.31%	15.24%	15.31%	33.85%	33.85%
TP	33.85%	33.85%	15.31%	15.24%	15.31%	15.24%	35.60%	35.60%
CP	15.24%	15.31%	35.60%	35.60%	33.85%	33.85%	15.24%	15.31%
GP	15.31%	15.24%	33.85%	33.85%	35.60%	33.60%	15.31%	15.24%
Information entropy	7.4603	7.4603	7.4894	7.4894	7.4894	7.4894	7.4603	7.4603
Histogram variance	40068	40068	36189	36189	36189	36189	40068	40068
Complexity order	$O(8MN)$	$O(8MN)$	$O(8MN)$	$O(8MN)$	$O(8MN)$	$O(8MN)$	$O(8MN)$	$O(8MN)$
The max distance of base distribution and 25%				10.6%				

https://doi.org/10.1371/journal.pone.0241184.t004

entropy is not close to eight, and the histogram variance is very large. However, the complexity order is only $O(8MN)$ (M, N denotes the size of the image).

Therefore, the following conclusions can be drawn: fixed DNA coding rules are simple to implement, have high computational efficiency, and one can even disturb a pixel value by selecting decoding rules that are different from the encoding rules. However, because there are only eight coding combinations, effective results are obtained only for four kinds. Further, the encryption is poor, ability to resist exhaustion is poor, bit distribution of the bases is not uniform, and the degree of scrambling is low. Therefore, it is difficult to encrypt an image, especially a single-pixel image such as a medical image. To our knowledge, most existing image encryption algorithms based on DNA coding adopt fixed coding; therefore, their security is apparently under threat.

3.2 Image encryption based on dynamic DNA coding

In dynamic DNA coding of images, the DNA sequence is obtained using different rules (the eight rules listed in Table 1) to encode each row, each column, each pixel, or each binary bit of the whole image. Selecting encoding patterns for different encoding objects randomly makes the coding system more complex, renders decoding more difficult, and enhances the image encryption security.

In this study, the existing dynamic coding methods are categorized into three, as follows. (1) Dynamic coding according to image block or row–column (row(column/block)-by-row). For example, Zhen [40] encoded each row of the original image differently using different rules that were controlled by a logistic chaotic sequence, and obtained the encrypted image by decoding with one of the rules. (2) Dynamic coding according to pixel (pixel-by-pixel). For instance, Kalpana [38], Wang [48], and Dagadu et al. [47] chose different encoding rules to encode each pixel in the image under the action of chaotic sequences. (3) Dynamic coding according to binary bit (bit-by-bit), wherein a single pixel can be converted to 8-bit binary bits, and every two binary bits can be encoded into one base using different rules that are controlled by the chaotic sequence; this method was used by [39]. The decoding process of all the above three methods is simply the opposite of the encoding process, and is thus not discussed here.

Now, the three dynamic DNA coding methods are comprehensively analyzed.

We assume that the chaotic sequences of the control encoding and decoding rules are E = {7,3,8,6. . .6} and D = {5,4,5,1. . .5}, respectively. Fig 4 presents a detailed description of the three dynamic encoding methods. Fig 4(a) depicts dynamic DNA encoding and decoding by row; because the first elements in E and D are 7 and 5, respectively, the first row of pixels for the "lena" image is encoded with R7 and decoded with R5. Similarly, the second row is encoded with R3 and decoded with R4. Fig 4(b) depicts dynamic DNA encoding and decoding by pixels. Each pixel in the first row of the "lena" image is encoded with R7, R3, R8, and R6. . .R6, and decoded with R5, R4, R5, and R1. . .R5. Fig 4(c) depicts dynamic DNA encoding and decoding by binary bit. Take the first pixel value (162) of the "lena" image as an example; the corresponding binary bit is "01010000." In this case, R7, R3, R8, and R6 are used to encode every two binary bits, and R5, R4, R5, and R1 are used for decoding; finally, a pixel value of 24 was obtained.

Experiment 3: By using the logistic map described in Eq (3), the initial values x0 = 0.35, u1 = 3.95, y0 = 0.38, and u2 = 3.92 are chosen to generate two chaotic sequences of 1×256, and map them to the integer interval [1, 8] to obtain the encoding rule E and decoding rule D. Then, we implement the three dynamic DNA coding methods using E and D to encode and decode "lena" gray scale images, respectively. The encrypted images are shown in Fig 5(a)–5(c).

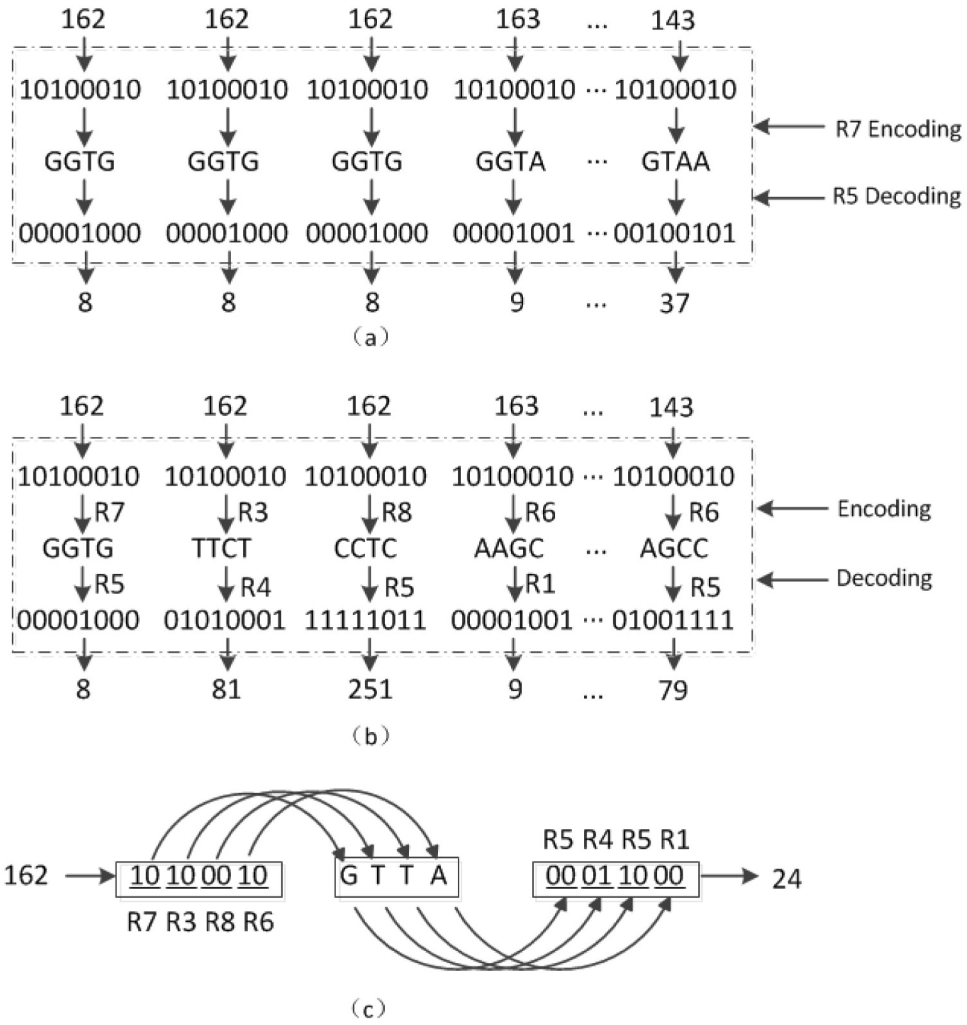


Fig 4. Decomposition diagram of dynamic coding (a) by row, (b) by pixel, and (c) by binary bit.

https://doi.org/10.1371/journal.pone.0241184.g004

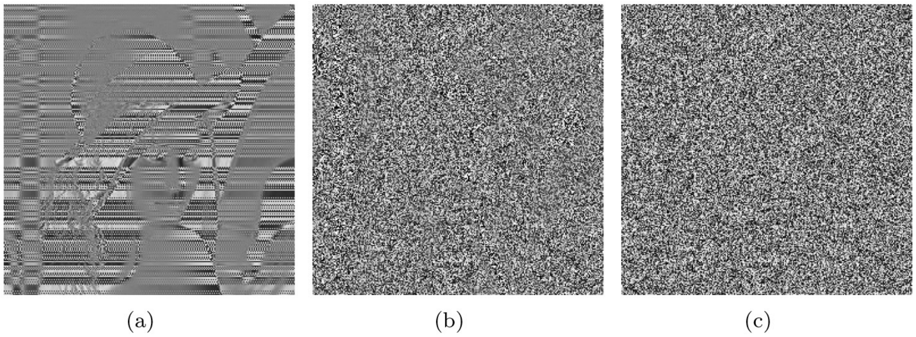


Fig 5. Three types of DNA dynamic encoding and decoding images for "lena". Encrypted images using dynamic coding (a) by row, (b) by pixel, and (c) by binary bit.

https://doi.org/10.1371/journal.pone.0241184.g005

Experiment 4: Eqs (4), (6) and (8) are used to calculate the base distribution, information entropy, and histogram variance of Fig 5(a)–5(c) obtained in Experiment 3. Further, the time complexity of the algorithm and the maximum distance between the base distribution and 25% are calculated. The results of this experiment are presented in Table 5.

Fig 4 indicates that the correlation of the image pixel cannot be reduced by converting (162,162,162,. . .) to (8,8,8. . .) after the encoding and decoding operations using dynamic coding by row. However, dynamic coding by pixel and binary bit can reduce the correlation of the image pixels. In Fig 5, the contour of the original image is clearly seen in the image processed using dynamic encoding and decoding by row, but completely invisible in the images processed using dynamic encoding and decoding by pixel and binary bit. Table 5 shows that the base distributions of all these three methods are close to 25%. Moreover, the base distribution of dynamic coding by binary bits is much closer to 25% compared with that of the other two methods. The maximum distance between the base distribution and 25% is 0.04% for this method; additionally, the information entropy of its encrypted image is 7.9976, which is very close to eight. Furthermore, its histogram variance is the least, but the complexity order is highest.

In summary, the implementation of dynamic coding by binary bit is more complex than that of the other two methods. Nevertheless, dynamic coding by binary bit performs better encryption, has higher degree of scrambling, and can resist exhaustive attacks.

3.3 Image encryption based on different types of base complement operations

The complement operation of a DNA sequence under chaotic sequence control is a common encryption tool for changing the pixel values of an image. According to the principle of base complementary in Table 2, two methods are available for base diffusion. The first method selects one of the six rules randomly, and then uses Eqs (2) and (17) to select the corresponding complementary bases [39, 43]; this method is called the static regular base complement method in this study. The other diffusion method [48] involves two steps: (a) selecting the complement rule for each base by chaotic sequence (i.e., to randomly select a rule from among R1 to R6 from Table 2), and (b) selecting the corresponding complement base using Eqs (2) and (17); this method is called the dynamic regular base complement method in this study. Moreover, [16] adopted a single base direct complement method (for details, see Section 2.2). Therefore, we classified the existing image encryption algorithms based on DNA complement into three: (1) single base direct complement method, (2) static regular base complement method, and (3) dynamic regular base complement method. The selection of the complement rule is expressed in the equation below:

$$x_i = \begin{cases} x_i, & if\ \ L(i) = 0 \\ D(x_i), & if\ \ L(i) = 1 \\ D(D(x_i)), & if\ \ L(i) = 2 \\ D(D(D(x_i))), & if\ \ L(i) = 3 \end{cases} \tag{17}$$

where L(i) is a chaotic sequence mapped to the integer region [0, 3], and x_i and $D(x_i)$ are the same as those in Eq (2). For the complement rule R1, if the base of the current position is $x_i = A$, and $ifL(i) = 3$, the complementary base of x_i is $D(D(D(x_i)))$. We can obtain the base as G (Table 2); in other words, the complement of A is G.

Table 5. Comparative characteristics of different dynamic coding methods.

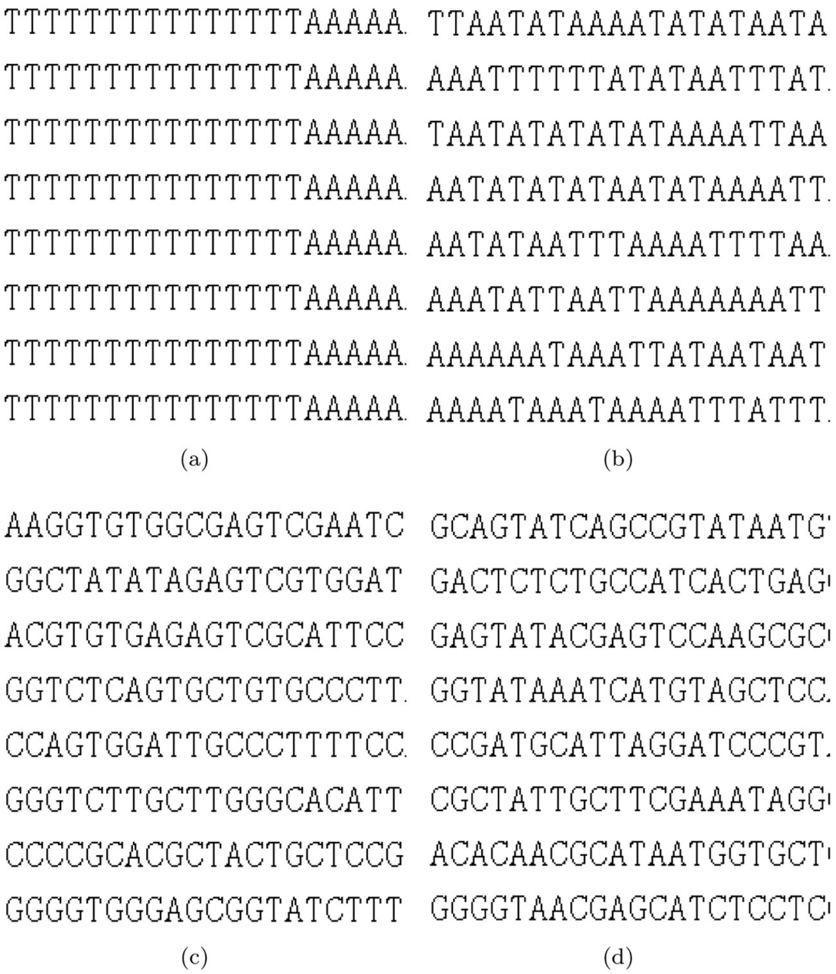
Comparative characteristic	Coding by row Dynamic coding	By pixel Dynamic coding	By binary bit
AP	24.50%	24.90%	24.98%
TP	24.65%	24.90%	25.04%
CP	25.42%	25.33%	24.97%
GP	25.43%	24.87%	25.01%
Information entropy	7.4895	7.8846	7.9976
Histogram variance	36177	11159	217.008
Complexity order	$O(8MN + 2M)$	$O(10MN)$	$O(16MN)$
The max distance of base distribution and 25%	0.50%	0.33%	0.04%

https://doi.org/10.1371/journal.pone.0241184.t005

To comprehensively compare the above two categories involved in the three complementary methods, in the simulation of the above three methods, we use the logistic chaotic sequence generated by the same initial value to control the position of the complementary base. In addition, to avoid the interference of dynamic coding, we use R1 from Table 1 for encoding and decoding.

Experiment 5: The methods of Zhang [16] and Jian [44] were applied to the single base direct complement and the static regular base complement operation for the "lena" gray scale image of 256×256, using the logistic system with the initial values x0 = 0.38 and u1 = 3.95. Similarly, using the logistic system, the initial values x0 = 0.35, u1 = 3.95, y0 = 0.38, and u2 = 3.92 were taken to perform the dynamic regular base complement operation on the "lena" gray scale image of 256×256, based on the ideas from [48]. Fig 6 shows the "lena" partial base sequence and complemented base sequence obtained by the three methods. Fig 7 shows the encrypted images and the histograms obtained by the three methods. Table 6 compares the three methods in terms of information entropy, the hamming distance of the corresponding position base, and histogram variance. We use "DBCO," "SRCO," and "DRCO" to denote the single base direct complement, static regular base complement, and dynamic regular base complement methods, respectively, in Table 6, Figs 6 and 7.

From Fig 6, it is seen that the base diffusion of the corresponding position with static regular base complement operation or dynamic base complement operation is better than that of the direct base complement operation. Visual observation of Fig 7(a), 7(c), 7(e), 7(g), 7(i), 7(k), 7(m) and 7(o) shows that the encrypted images of the static regular base complement and the dynamic regular base complement methods are completely different from the original image, whereas the contour of the original image is seen in the image encrypted by the direct base complement method. Analyzing the histograms of Fig 7(b), 7(d), 7(f), 7(h), 7(j), 7(l), 7(n), and 7(p) shows that the histogram distributions for direct base complement and dynamic regular base complement are more uniform. The six histograms of the static regular base complement method showed three forms. The histograms of R1 and R2, R3 and R5, R4 and R6 have similar shapes, and the other four regular distributions are not uniform, except the histograms of R4 and R6. Here, R1–R6 were obtained from Table 2. A comparison of the information entropy and hamming distance of the three methods indicates that the information entropy of the dynamic regular base complement method is the largest, and the static regular base complement is not very stable. The hamming distance of the static regular base complement and dynamic regular base complement methods is the same and larger than that of the direct base complement method, because the chaotic sequence of the control complement operation is the same. The smaller the histogram variance, the better the encryption. Further, the variance value of the dynamic regular base complement method is the least of all methods.



TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA
TTTTTTTTTTTTTTTAAAAA

(a)

TTAATATAAAATATATAATA
AAATTTTTATATAATTTAT
TAATATATATATAAAATTAA
AATATATATAATATAAAATT
AATATAATTTAAAATTTTAA
AAATATTAATTAAAAAAATT
AAAAAATAAATTATAATAAT
AAAATAAATAAAATTTATTT

(b)

AAGGTGTGGCGAGTCGAATC
GGCTATATAGAGTCGTGGAT
ACGTGTGAGAGTCGCATTCC
GGTCTCAGTGCTGTGCCCTT
CCAGTGGATTGCCCTTTTCC
GGGTCTTGCTTGGGCACATT
CCCCGCACGCTACTGCTCCG
GGGGTGGGAGCGGTATCTTT

(c)

GCAGTATCAGCCGTATAATG
GACTCTCTGCCATCACTGAG
GAGTATACGAGTCCAAGCGC
GGTATAAATCATGTAGCTCC
CCGATGCATTAGGATCCCGT
CGCTATTGCTTCGAAATAGG
ACACAACGCATAATGGTGCT
GGGGTAACGAGCATCTCCTC

(d)

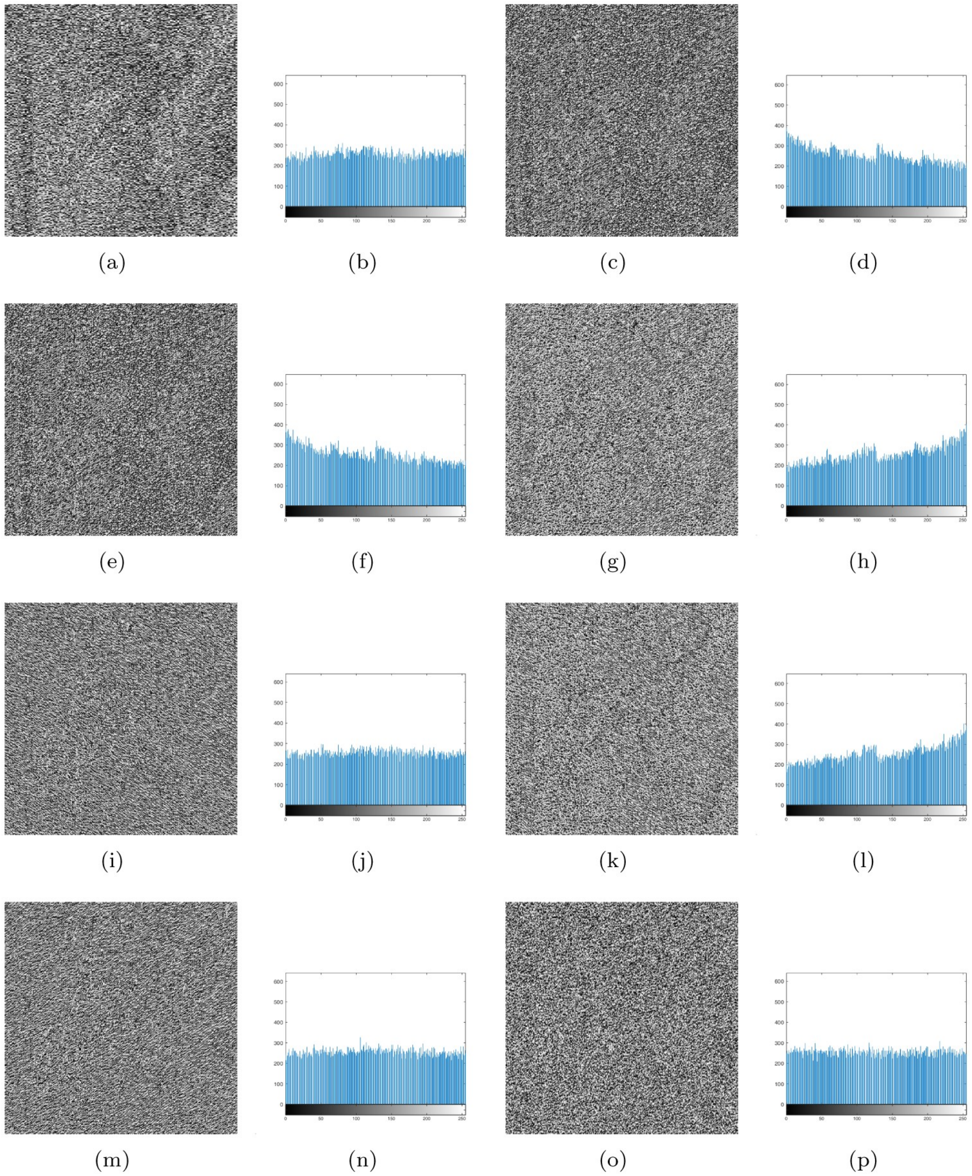
Fig 6. Variation of the partial bases in the first row of the"lena" image for the three complementary methods. (a) Variation of partial bases in the first row of the "lena" image, (b) variation of DBCO, (c) variation of SRCO, (d) variation of DRCO.

https://doi.org/10.1371/journal.pone.0241184.g006

In summary, the dynamic regular base complement operation performs better encryption, and has higher diffusion degree of pixels. Moreover, the complexity of this algorithm makes it robust to image encryption attacks.

3.4 Image encryption based on different DNA sequence algebra operations

Based on the discussion in Section 2.1, image pixels can be represented as DNA sequences by encoding. These DNA sequences can be changed by using different DNA sequence algebra operations. When the DNA sequence is changed, the pixel values of the image are disrupted. Thus, the addition, subtraction, and XOR algebra operations of the DNA sequences are widely used in image encryption. Table 3 shows that the rows and column bases corresponding to A and G of the addition and XOR operations are the same, and that the two operations are very similar. The main difference is that the addition operation is irreversible, whereas the XOR operation is reversible. Zhang et al. [12] used chaotic mapping and the DNA addition operations to perform image encryption. [18, 19] indicated that the encrypted image in [12] cannot be restored back to the original image. [59] also has the problem of irreversibility of the



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

(e) (f) (g) (h)

(i) (j) (k) (l)

(m) (n) (o) (p)

Fig 7. Encrypted images and histograms of "lena" for the three complementary methods. Encrypted images and histograms obtained by (a) and (b) DBCO, (c)—(n) SRCO (static rule is R1–R6 in Table 4), and (o)—(p) DRCO.

https://doi.org/10.1371/journal.pone.0241184.g007

addition operation. To overcome this disadvantage, the DNA sequence matrix of the original grayscale image is usually added to that generated by the chaotic sequence [29, 30, 34, 60]. In case of a color image, the image is divided into three channel matrices (R, G, and B), and the channel matrix is transformed into DNA sequences, which are then added [14, 38]. The XOR

Table 6. Comparison of the three complementary methods.

complementary methods	DBCO	SRCO						DRCO
		R1	R2	R3	R4	R5	R6	
Information entropy	7.9955	7.9852	7.9824	7.9794	7.9967	7.9803	7.9966	7.9969
Hamming distance	158812	204683	204683	204683	204683	204683	204683	204683
Histogram variance	405.2422	1619.6	1637.7	1927	296.0078	1840.7	312.1875	279.3750

https://doi.org/10.1371/journal.pone.0241184.t006

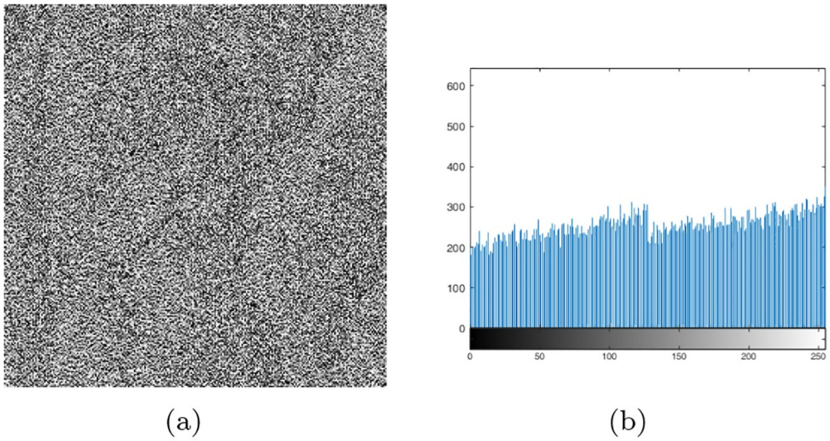


Fig 8. Encrypted image and histogram of addition operation. (a)Encrypted image of 'lena'. (b) Histogram of encrypted image.

https://doi.org/10.1371/journal.pone.0241184.g008

operation also mainly follows the above two ideas. For example, the DNA sequence matrix of the original image and the DNA matrix which is generated by the chaotic system are carried out using the XOR operation [61–63]. Reference [64] implemented the XOR operation between the three channel DNA matrices in the color image. To compare the encryption performance of the addition and XOR operations, we do not scramble the original gray image. We use R1 in Table 1 to encode the original image, and then perform the addition and XOR operations using the DNA matrix produced by the chaotic sequence. The experimental procedure is as follows.

Experiment 6: The initial values x0 = 0.38 and u1 = 3.95 are chosen to generate the chaotic sequences of $X_{256\times256\times8}$ using the logistic system. If x(i) > = 0.5, x(i) = 1, and if x(i) < 0.5, x(i) = 0; here, x(i) is an element of X. Then, the X sequence is encoded according to the fixed coding rule R1 in Table 1 to obtain the DNA matrix L, whose size is 256,256×4. The original "lena" image is also encoded into a DNA matrix P according to the fixed coding rule R1 in Table 1. We performed P+L and P XOR L operations by using the addition and XOR rules defined in Table 3. Finally, we obtained the encrypted image after decoding and reconstructing (Figs 8 and 9). To our knowledge, these methods have been adopted in [29, 30, 61–63].

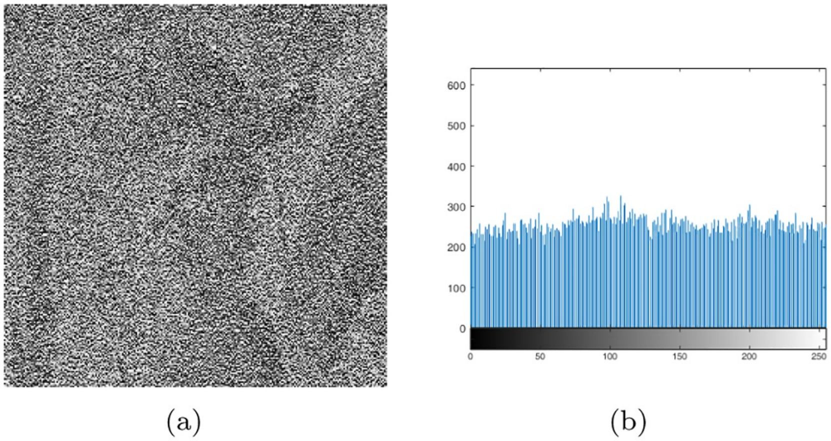


Fig 9. Encrypted image and histogram of XOR operation. (a) Encrypted image of "lena." (b) Histogram of the encrypted image.

https://doi.org/10.1371/journal.pone.0241184.g009

Table 7. Comparison of addition and XOR operations.

DNA algebra operations	Original image	Addition operation	XOR operation
Information entropy	7.4895	7.9897	7.9953
Hamming distance	/	221592	221592
Fixed point ratio	/	0.14%	0.05%
histogram variance	40068	934.7500	424.3594

https://doi.org/10.1371/journal.pone.0241184.t007

In Figs 8(a) and 9(a), the contours of the original "lena" image can be seen, because the original image was not scrambled before the addition and XOR operations. A comparison of Figs 8(b) and 9(b) show that the histogram distribution of the encrypted images obtained by the XOR operation is more uniform. Table 7 indicates that the information entropy of the XOR operation is closer to eight. Because the two methods use the same chaotic mapping with the same parameters, they have the same hamming distance, and approximately 85% of their bases have changed (221592/(256×256×4)×100% = 85%).

The smaller fixed point ratio and histogram variance indicate a better degree of disturbance. Clearly, the fixed point ratio and the histogram variance of the XOR operation are smaller as observed from Table 7. This indicates that the encryption of the DNA XOR operations is better than that of DNA addition.

3.5 Image encryption based on combinations of multiple DNA operations

Recently, combining DNA coding mechanisms and different DNA algebraic operations (such as addition and subtraction, and XOR and complement) to perform image encryption based on DNA coding has attracted the attention of scholars. Chai [65] used 2D logistic mapping to dynamically encode a plaintext image by pixels, and then used a cyclic displacement scrambling DNA matrix. Then, the addition and XOR operations were performed on the scrambled DNA matrix and the DNA matrix generated by the chaotic system under the new key updated by the hamming distance of the plaintext image. Finally, the encrypted image was obtained by decoding and recombining. Zhang [39] used Lorenz to generate chaotic sequences, and obtained a, b, and c after deforming. Then, Chen chaotic map was used to generate chaotic sequences, and A, B, C, and D were obtained after deformation. Further, the plain images were scrambled to obtain E1 using a and b, and E1 and C were dynamically encoded by binary bit using A and B, respectively, after that obtained E2 and E3. Addition operation was performed on E2 and E3 under c sequence, and E4 was obtained using D to perform the direct complement operation on E3 which is the result of addition, to finally obtain the encrypted image.

These methods perform good encryption, are highly secure, and can resist common attacks. However, most combination encryption methods are not secure, because most of them use the fixed coding rule, or the base is directly complemented, which was proven to be unsafe in Sections 3.1 and 3.3. Furthermore, some methods cannot restore the plaintext image, and cannot resist CPA and KPA. A detailed analysis is presented in Table 8.

3.6 Further analysis and comparison of methods

The previous sections independently discussed the advantages and disadvantages of the methods. In this section, all the proposed methods are compared comprehensively. Image encryption based on DNA coding involves two main aspects: DNA coding mechanisms and DNA coding operation. We compare these two aspects individually.

Table 8. Analysis of image encryption based on combinations of multiple DNA operations.

Reference	Chaotic system	DNA Coding	Combination of DNA operations	Shortcomings
Zhang [12]	2D Logistic Logistic	Fixed coding	Addition Subtraction DBCO	The addition is irreversible
Liu [14]	Logistic	Fixed coding	Addition Subtraction DBCO XOR	Unable to resist the chosen plaintext attack, attacked by Belazi [20]
Zhang [17]	Lorenz Logistic	Fixed coding	XOR DBCO	Similar to the reference [14], the security is low and cannot resist the chosen plaintext attack
Wang [58]	CML Logistic	Fixed coding	Addition Subtraction SRCO	The security can be further improved
Jain [44]	Logistic 2D Logistic	Fixed coding	Addition Subtraction SRCO	The security can be further improved
Li [32]	Fractional-Order hyper chaotic system	Dynamic coding by binary bit	Addition Subtraction XOR	The algorithm has high complexity and cannotresist the chosen plaintext attack
Zhang [66]	Chen	Dynamic encoding by pixel decoding by fixed rule	Addition Subtraction XOR	Cannot resist the chosen plaintext attack, information entropy is lower
Suryadi [33]	Logistic	Fixed coding	Addition Subtraction DBCO XOR	Cannot resist the chosen plaintext attack, similar to the reference [14], the security is low
Zhang [34]	Logistic	Fixed coding	Addition Subtraction DBCO	Cannot resist the chosen plaintext attack
Dagadu [47]	Logistic Tent map	Dynamic coding by pixel	Addition Subtraction XOR	Cannot resist the chosen plaintext attack
Ahadpour [67]	Coupled chaotic maps lattices	Fixed coding	Addition Subtraction XOR DBCO	Similar to the reference [14], cannot resist the chosen plaintext attack

https://doi.org/10.1371/journal.pone.0241184.t008

3.6.1 Comparison of DNA coding mechanisms. DNA coding (encoding and decoding) is the interface between image pixels and DNA sequences. Different DNA coding mechanisms yield different encryption performances. Therefore, choosing a better DNA coding method is a key step in the DNA image encryption process. The existing DNA coding methods are compared in Tables 4 and 5. The performance of the three dynamic DNA coding methods is better than that of fixed DNA coding. Among all the dynamic DNA coding methods, the dynamic coding by binary bit has the best performance; the information entropy is 7.9976, which is very close to 8. Further, its histogram variance is the least, suggesting that the histogram distribution of the encrypted image is the most uniform for this method than for the other methods. It has the least maximum distance between the base distribution rate and 25%, indicating that the base distribution is the most uniform for this method than for the other methods. However, due to calculation by binary bit, this algorithm is more complex than the others. We believe that the current speed of the computer is totally affordable for this method.

3.6.2 Comparison of DNA coding operations. The existing DNA encoding operations include individual DNA operations and the combination of multiple operations. We compared them based on information entropy, histogram variance, correlation coefficient, and time complexity (Tables 9 and 10). Table 9 indicates that the information entropy of DRCO is much closer to 8 than that of the other DNA coding operations. Further, its histogram variance and correlation coefficient (very close to 0) are the least. However, it has the highest complexity order. The order of superiority of the other DNA coding operations is as follows: SRCO (Rule 4 and Rule 6 from Table 6) >DBCO>XOR>addition. This order can be used to determine if a specific DNA operation is reasonable. Because DRCO exhibits the best performance of all the base complement methods, the combination of DRCO with other DNA operations attracts our attention. All DNA operations in this section used the same experimental data and environment as those in the previous sections. Table 10 shows that DRCO + Addition is better

Table 9. Comparison of the performance of DNA coding operations.

DNA coding operation		Information entropy	Histogram variance	Correlation coefficient			Complexity order
				Horizontal	Vertical	Diagonal	
Base complement	DBCO	7.9955	405.2422	0.4117	-0.1642	-0.0685	$O(16MN)$
	SRCO	7.9967(max)	296.008(max)	-0.0412	-0.3457	-0.0435	$O(16MN)$
	DRCO	7.9969	279.3750	-0.0317	0.0010	0.0629	$O(32MN)$
Algebra operations	Addition	7.9897	934.7500	-0.0383	-0.1260	-0.0153	$O(24MN)$
	XOR	7.9953	424.3594	0.0238	-0.1646	-0.0018	$O(24MN)$

https://doi.org/10.1371/journal.pone.0241184.t009

than Addition + DRCO, DRCO + XOR is better than XOR + DRCO, and XOR + Addition is better than Addition + XOR. Table 9 shows that DRCO>Addition, DRCO>XOR, and XOR>Addition.

These results show that when performing combinatorial DNA operations, better encryption performance can be obtained by placing the better operation before other operations. Table 10 indicates that DRCO + XOR is the best encryption method of all combinatorial operations, because DRCO and XOR operations occupy superior positions in the order DRCO>XOR>addition. If time complexity permits, the superposition of the operation with better performance will result in better encryption; for instance, DRCO + XOR + Addition>DRCO + XOR. This would indicate the direction for implementing DNA combinatorial operation encryption later.

3.7 Proposed DNA coding encryption scheme

Section 3.6.1 revealed that the dynamic DNA coding by binary bit is the best DNA coding method; Section 3.6.2 revealed that DRCO + XOR + Addition is the best DNA coding operation. Now, we attempt to develop a new encryption scheme by combining the optimal DNA coding and optimal DNA operation defined above. First, the original image is encoded by binary bit dynamically; then, DRCO + XOR + Addition operation is performed on the coding matrix. Finally, the encrypted image is obtained by decoding the DNA coding matrix to the binary sequence dynamically. The encryption process is the same as the decomposition process mentioned above, and is thus not discussed again. However, as described by Eqs (18) and (19), the key is treated as follows to make the proposed scheme more secure.

$$a_0 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} A(i,j)}{10 \times M \times N} \tag{18}$$

$$x_{terminal} = a_0 + x_{initial}(k) \tag{19}$$

Table 10. Comparing the performance of combinatorial DNA operations.

Combination of DNA operation	Information entropy	Histogram variance	Correlation coefficient			Complexity order
			Horizontal	Vertical	Diagonal	
Addtion+DRCO	7.9967	297.1640	0.0158	-0.0159	-0.0147	$O(48MN)$
DRCO+Addtion	7.9969	279.0156	0.0156	-0.0094	0.0195	$O(48MN)$
XOR + DRCO	7.9970	273.2500	0.0086	-0.0051	0.0025	$O(48MN)$
DRCO+ XOR	7.9974	233.2500	-0.0033	0.0012	0.0022	$O(48MN)$
Addition+XOR	7.9969	281.2813	-0.0069	0.0248	0.0042	$O(40MN)$
XOR +Addition	7.9971	260.1094	-0.0081	0.0051	0.0019	$O(40MN)$
DRCO+XOR+Addition	7.9975	225.3203	-0.0031	0.0007	-0.0011	$O(64MN)$

https://doi.org/10.1371/journal.pone.0241184.t010

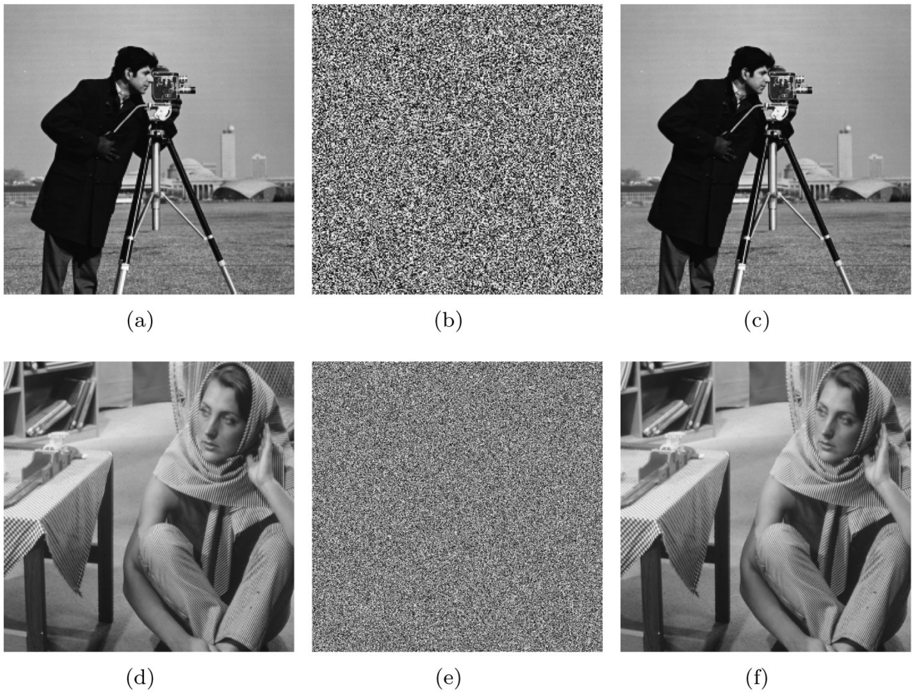


Fig 10. Encrypted image and decrypted image produced by the proposed scheme. (a) Original image of "Cameraman," (b) Encrypted image of "Cameraman," (c) Decrypted image of (b); (d) Original image of "Woman," (e) Encrypted image of "Woman," and (f)Decrypted image of (e).

https://doi.org/10.1371/journal.pone.0241184.g010

We apply the proposed algorithm to ten standard gray-scale images, of which seven are 256×256 and three are 512×512. The encrypted images of "Cameraman" and "Woman" are shown in Fig 10. Apparently, the encrypted images are difficult to be recognized, but only from a visual perspective. Next, we evaluate the proposed algorithm in terms of information entropy, resistance to exhaustive attacks, resistance to statistical attacks, and resistance to differential attacks, and conduct a NIST randomness test.

3.7.1 Analysis of global and local information entropy. To analyze the information entropy more accurately, we calculate both the global information entropy and local information entropy of different scales. This is because the local information entropy can effectively overcome the weaknesses of the global information entropy, such as inaccuracy, inconsistency, and low efficiency. Table 11 shows that the global information entropy and local information

Table 11. Global and local information entropy of the encrypted images.

Image	size	Global entropy	Local entropy 16×16	Local entropy 32×32
lena	256×256	7.9979	7.1790	7.8064
Airplane	256×256	7.9974	7.1767	7.8028
Cameraman	256×256	7.9973	7.1867	7.8014
Sailboat	256×256	7.9974	7.1730	7.8021
Parrot	256×256	7.9973	7.1750	7.8024
Monarch	256×256	7.9973	7.1702	7.8049
starfish	256×256	7.9971	7.1765	7.8034
couple	512×512	7.9994	7.1754	7.8046
woman	512×512	7.9993	7.1790	7.8029
Man	512×512	7.9993	7.1742	7.8022

https://doi.org/10.1371/journal.pone.0241184.t011

Table 12. Comparison of information entropy of the proposed and the existing methods.

Scheme	size	Entropy	Scheme	size	Entropy
Proposed	256×256	7.9974	Proposed	512×512	7.9993
Ref [69]	256×256	7.9970	Ref [70]	512×512	7.9588
Ref [71]-Ahmad's	256×256	7.9801	Ref [69]	512×512	7.9990
Ref [71]-Niu's	256×256	7.9888	Ref [72]	512×512	7.9985
Ref [71]	256×256	7.9972	Ref [73]	512×512	7.9993
Ref [74]	256×256	7.99615	Ref [75]	512×512	7.9986

https://doi.org/10.1371/journal.pone.0241184.t012

entropy of each block are 16×16 and 32×32, respectively (here, k = 30 and L = 256). Further, all global information entropy are very close to 8, and the average local entropy of 16×16 and 32×32 is 7.1766 and 7.8033, respectively; these values are close to 7.1749 and 7.8087, which are the local information entropy of the random images in [68]. Table 12 compares the developed encryption scheme with the existing encryption schemes. The comparison indicates that the information entropy obtained by our scheme is higher, and the encrypted image is similar to the ideal random image.

3.7.2 Key sensitivity analysis (resistance to exhaustive attacks). The key is determined to be sensitive or insensitive depending on whether the encryption scheme can resist exhaustive attacks. We use NPCR and UACI to analyze the difference between two encrypted images with a key (x0) difference of 10^{-14}. Table 13 lists the NPCR and UACI values of the encrypted images before and after minor changes to the key. NPCR = 99% and UACI = 33% are the benchmark values [53]. Table 13 reveals that all the NPCR and UACI values of our method are larger than the benchmark values. Table 14 compares our algorithm with the existing algorithms, and reveals that the NPCR and UACI values of our algorithm are larger than those of the existing methods. Therefore, our algorithm has high key sensitivity and is robust against exhaustive attacks.

Table 13. Results of key sensitivity analysis.

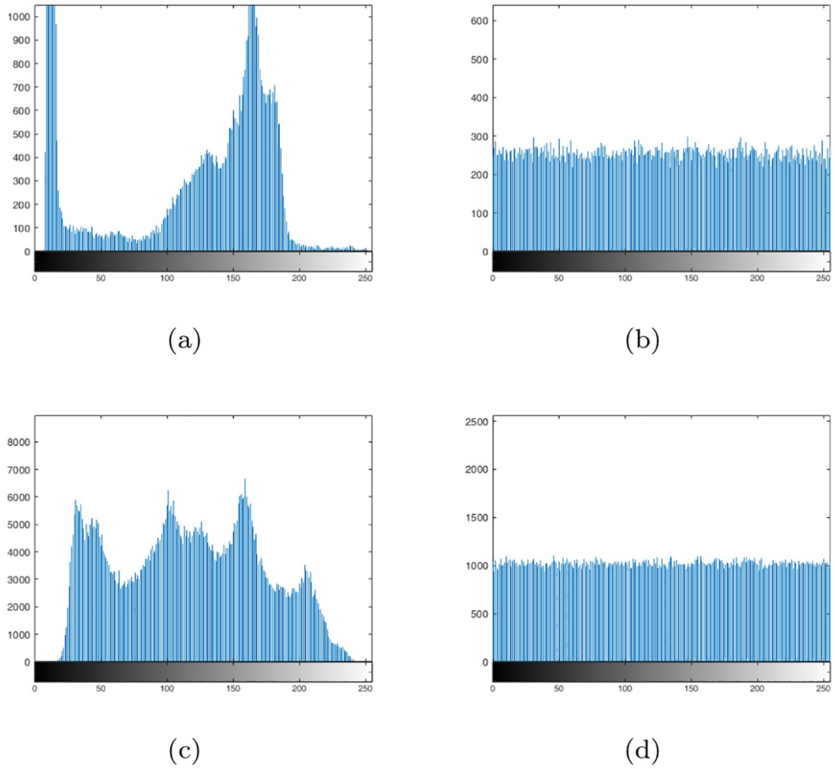
image	NPCR(%)	UACI(%)
lena	99.61	33.60
Cameraman	99.60	33.60
Parrot	99.60	33.59
woman	99.60	33.48
Man	99.59	33.45
Average	99.60	33.54

https://doi.org/10.1371/journal.pone.0241184.t013

Table 14. Comparison of key sensitivities of the proposed and the existing methods.

Scheme	NPCR(%)	UACI(%)
Proposed	99.60	33.54
Ref [76](average)	99.60	33.46
Ref [77]	99.64	33.31
Ref [71]	99.57	33.49
Ref [78]	99.58	33.37

https://doi.org/10.1371/journal.pone.0241184.t014



(a)

(b)

(c)

(d)

Fig 11. Histograms of the original and the encrypted images. (a)Histograms of "Cameraman," (b) Histograms of encrypted image of "Cameraman," (c))Histograms of "Woman," (d) Histograms of encrypted image of "Woman."

https://doi.org/10.1371/journal.pone.0241184.g011

3.7.3 Resistance to statistical attacks.

Here, we discuss the effectiveness of the proposed algorithm in resisting statistical attacks. Cryptoanalysts generally use the distribution of histograms and the correlation between adjacent pixels to count important information in order to find information related to plaintext images [79, 80]. Therefore, the histograms of "Cameraman" and "Woman" are shown in Fig 11, and the histogram variances of all 10 standard original and encrypted images are listed in Table 15. Further, we use Eqs (10)–(13) to calculate the correlation coefficients of 10 standard gray-scale images and the corresponding encrypted images (Table 16).

Table 15. Histogram variances of the original and encrypted images.

Image	size	Original	encrypted
lena	256×256	40068	192.3438
Airplane	256×256	177300	236.6328
Cameraman	256×256	110970	244.6875
Sailboat	256×256	68597.5	232.1094
Parrot	256×256	26464.5	241.9922
Monarch	256×256	40207	246.9297
starfish	256×256	16292	260.6642
couple	512×512	1387200	881.4033
woman	512×512	382200	1015.1
Man	512×512	1201300	1011.4

https://doi.org/10.1371/journal.pone.0241184.t015

Table 16. Correlation coefficients of the original and encrypted images.

Image	size	Original image			Encrypted image		
		H	V	D	H	V	D
Lena	256 × 256	0.9421	0.9718	0.9160	0.0010	-6.8640×10^{-5}	-0.0014
Airplane	256 × 256	0.8337	0.8950	0.9029	0.0014	0.0011	-7.0240×10^{-4}
Cameraman	256 × 256	0.9306	0.9609	0.9080	1.0600×10^{-4}	-0.0021	0.0019
Sailboat	256 × 256	0.8652	0.9162	0.8156	0.0016	-0.0013	7.8222×10^{-4}
Parrot	256 × 256	0.9581	0.9389	0.9100	0.0013	0.0011	8.7092×10^{-4}
Monarch	256 × 256	0.9354	0.9265	0.9060	0.0029	8.9210×10^{-4}	-5.6692×10^{-5}
starfish	256 × 256	0.9598	0.9611	0.9360	5.6808×10^{-4}	-0.0026	-1.4678×10^{-4}
couple	512 × 512	0.9456	0.9554	0.9115	-1.5336×10^{-4}	-8.0640×10^{-4}	0.0015
woman	512 × 512	0.8969	0.9576	0.8827	-4.3208×10^{-4}	0.0017	-1.4784×10^{-4}
Man	512 × 512	0.9632	0.9684	0.9385	0.0031	-0.0015	9.4602×10^{-4}

https://doi.org/10.1371/journal.pone.0241184.t016

Apparently, the distributions of the histograms for encrypted images are very uniform, and the histogram variance of all encrypted images is much lower than that of the original image. The correlation coefficients in the horizontal, vertical, and diagonal directions of the encrypted images are very close to 0, suggesting that the correlation between adjacent pixels is very low. Therefore, the proposed scheme can resist statistical attacks very well.

3.7.4 Resistance to differential attacks. To attack an encryption algorithm, a cryptographic attacker searches for loopholes by detecting the sensitivity of the keys to plaintext. If the keys are more sensitive to plaintext, it is difficult to perform a differential attack. Similar to that in Ref. [80, 81], we use NPCR and UACI to calculate the difference value after encrypting two plaintext images with very little differences. Table 17 lists the NPCR and UACI values for five standard grayscale images, and indicates that the averages of the NPCR and UACI values are higher than the corresponding benchmark values. Further, we compare our scheme with other existing methods in Table 18; Table 18 shows that our scheme is highly superior to the existing methods.

3.7.5 NIST randomness test. The SP800-22 test package of the National Institute of Standards and Technology (NIST) can detect the randomness of digital information, and is currently the most authoritative method for detecting the randomness of binary sequences [81, 84, 85]. Each value in this package is tested successfully only if it is greater than 0.01. Further, to preserve generality, we detect the randomness of both encrypted grayscale images and color images of three channels, and the results are presented in Table 19. Table 19 shows that all test values are greater than 0.01, and that the results are "success." This shows that our algorithm can obtain random sequences by encrypting grayscale and color images.

Table 17. NPCR and UACI values of two plaintext images with very little differences (1st pixel value+1).

image	NPCR(%)	UACI(%)
lena	99.62	33.44
Cameraman	99.61	33.43
Parrot	99.62	33.48
woman	99.60	33.50
Man	99.61	33.57
Average	99.61	33.48

https://doi.org/10.1371/journal.pone.0241184.t017

Table 18. Comparison of NPCR and UACI values of the proposed and the existing methods.

Scheme	NPCR(%)	UACI(%)
Proposed	99.61	33.48
Ref [82]	99.59	33.45
Ref [71]	99.59	32.46
Ref [74]	99.60	30.15
Ref [70]	99.52	33.51
Ref [83]	99.61	33.46

https://doi.org/10.1371/journal.pone.0241184.t018

Table 19. NIST randomness test of encrypted images.

Test	P values for different color layer of ciphered image				Results
	Gray	Red	Green	Blue	
Frequency	0.050840	0.093618	0.106726	0.343429	success
Block frequency	0.982411	0.935871	0.896638	0.739019	success
Rank	0.645533	0.032864	0.232596	0.109194	success
Run(M = 10000)	0.434548	0.025371	0.075586	0.475306	success
Long runs of ones	0.217490	0.492130	0.629059	0.577289	success
Linear complexity	0.334230	0.082060	0.776813	0.059248	success
Overlapping templates	0.234659	0.909920	0.490812	0.753541	success
Non overlapping templates	all P value>0.01	all P value >0.01	all P value >0.01	all P value >0.01	success
FFT	0.418761	0.463844	0.659148	0.423150	success
Approximate entropy	0.033674	0.786329	0.901310	0.279076	success
Universal	0.855914	0.563772	0.912692	0.232085	success
Serial P values 1	0.044550	0.163760	0.458336	0.533797	success
Serial P values 2	0.088164	0.367355	0.233775	0.686673	success
Cumulative sums forward	0.085808	0.183481	0.178746	0.442739	success
Cumulative sums reverse	0.024093	0.176673	0.088104	0.403578	success

https://doi.org/10.1371/journal.pone.0241184.t019

4 Shortcomings of existing methods and suggested improvements

4.1 Shortcomings

Section 3 indicates that the existing methods have some shortcomings. First, the existing DNA coding mechanisms are fragile. Although DNA coding is a crucial step in encryption, most of the existing coding methods use fixed coding. Section 3.1 proved that fixed coding yields poor encryption performance, has poor resistance to exhaustive attacks, and has non-uniform distribution of bases. Although some studies have used dynamic coding, most of them are row-by-row (image block) or pixel-by-pixel dynamic coding. These two methods are not as secure as dynamic coding by binary bit. Second, improper application of the DNA sequence addition operation, resulting in irreversibility of the image encryption method. The inverse operation of DNA sequence addition is the DNA sequence subtraction operation. Therefore, if addition is performed between the pixels of an original image, the DNA subtraction operation cannot be performed, and it would be difficult to decrypt an encrypted image. Third, the security of the DNA complement operations is poor. In recent years, various studies have widely used the method of DNA complement to diffuse the pixel values. However, most of them used the direct base complement or static regular base complement method. Section 3.3 showed that the static regular base complement method comprises three different encryption forms. Except for the fourth and the sixth rule, the information entropy of the other static regular complement methods is low, and the direct base complement method exhibits poor encryption performance. Fourth, because the combinatorial DNA operations are selected arbitrarily, image encryption based on combinations of multiple DNA operations is not highly secure. Fifth, the diffusion capacity of DNA bases is poor. Most studies only use the relevant theory of DNA coding to encrypt images and ignore the diffusion of bases, making their methods vulnerable to CPA and KPA. Sixth, the existing methods use chaotic systems combined with DNA coding to achieve image encryption, whose security (i.e., key space, key sensitivity, and degree of image scrambling) thus depends on the security of the chaotic system. Furthermore, parallelism and high storage of DNA computing were not applied to these image encryption methods.

4.2 Future direction for improvements

We propose the following improvements to alleviate the above shortcomings. The first suggestion is related to using the DNA dynamic coding mechanism to transform an original image into a DNA sequence matrix, for which dynamic coding by binary bit can be preferred. Table 5 shows that the information entropy of dynamic coding by binary bit reaches 7.9976, and its base distribution is very uniform, which are beneficial as good factors to the successfully begin the encryption process. Second, the DNA addition operation can be replaced with DNA XOR operation to perform image encryption. Table 3 indicates that the DNA XOR operation is very similar to the addition operation. Its main advantage is that it is reversible, and makes the algorithm simple. By comparing the relevant data, we can solve the problem of irreversible addition, and also obtain good encryption performance. Third, selecting the dynamic regular base complement method to improve the diffusion capacity of pixels is preferable. Fourth, choose a reasonable and effective DNA combination operation to change the pixel values of images based on Table 10. Fifth, use the information related to plaintext as a part of encryption key, such as combining the hamming distance of the DNA sequence from the plaintext image with the encryption key (chaotic initial value) to form the final key, or combining DNA dynamic coding with a chaotic system. This can improve the diffusion capacity of the DNA base, and effectively resist the CPA and KPA. Sixth, in addition to using more secure chaotic systems combined with DNA coding to perform image encryption, researchers should combine the DNA coding methods effectively to improve the security of the DNA coding encryption methods.

Future studies should emphasize the use of DNA computing parallelism and large storage in image encryption to quickly encrypt many images and even video files, while ensuring security.

5 Conclusion

This study first reviewed the existing DNA coding-based image encryption methods. Image encryption based on DNA coding was classified into five types, depending on the type of DNA coding: DNA fixed coding, DNA dynamic coding, different types of base complement operation, different DNA sequence algebraic operations, and combinations of multiple DNA operations. All these methods and other existing methods were compared and explained. Furthermore, we combined the optimal coding mechanism with the optimal DNA coding operation to develop a new encryption scheme, and demonstrated its effectiveness and security. Finally, the shortcomings of the existing image encryption methods and the future direction for improvement were discussed. In the future, we will study the advantages and disadvantages of image encryption methods based on different combinations of DNA coding and dynamic

DNA operations. We will also study the influence of different chaotic systems on DNA coding schemes.

Supporting information

S1 File.
(ZIP)

Author Contributions

Conceptualization: Xianglian Xue, Dongsheng Zhou.

Data curation: Xianglian Xue.

Formal analysis: Xianglian Xue, Dongsheng Zhou, Changjun Zhou.

Funding acquisition: Xianglian Xue, Changjun Zhou.

Investigation: Xianglian Xue.

Methodology: Xianglian Xue.

Project administration: Xianglian Xue.

Resources: Xianglian Xue.

Software: Xianglian Xue.

Validation: Xianglian Xue.

Visualization: Xianglian Xue.

Writing – original draft: Xianglian Xue.

Writing – review & editing: Xianglian Xue.

References

1. Adleman LM. Molecular computation of solutions to combinatorial problems. Science. 1994; 266:1021–1024. https://doi.org/10.1126/science.7973651 PMID: 7973651
2. Song T, Wang X, Li X, Zheng P. A programming triangular DNA origami for doxorubicin loading and delivering to target ovarian cancer cells. Oncotaget, 2017, Dec. https://doi.org/10.18632/oncotarget.23733
3. Shi XL, Chen CZ, Li X, Song T, Chen ZH, Zhang Z, et al. Size Controllable DNA Nanoribbons Assembled from Three Types of Reusable Brick Single-Strand DNA Tiles. Soft Matter. 2015; 11: 8484–8492. https://doi.org/10.1039/C5SM00796H PMID: 26367111
4. Li X, Hong L, Song T, Rodríguez-Patón A, Chen CZ, et al. Highly biocompatible drug-delivery systems based on DNA nanotechnology. Journal of Biomedical Nanotechnology. 2017; 13: 747–757. https://doi.org/10.1166/jbn.2017.2383
5. Shi XL, Wu XX, Song T, Li X. Construction of DNA Nanotubes with Controllable Diameters and Patterns by Using Hierarchical DNA Sub-tiles. Nanoscale. 2016 Aug; 8(31):14785–14792. https://doi.org/10.1039/C6NR02695H PMID: 27444699
6. Wang B, Zhang Q, Wei XP. Tabu Variable Neighborhood Search for Designing DNA Barcodes. IEEE Transactions on NanoBioscience. 2020; 19(1):127–131.
7. Li X, Wang B, Lv H, Yin Q, Zhang Q, Wei XP. Constraining DNA sequences with a triplet-bases unpaired. IEEE Transactions on NanoBioscience. https://doi.org/10.1109/TNB.2020.297164
8. Wang B, Zheng XD, Zhou SH, Zhou CJ, Wei XP, et al. Constructing DNA Barcode Sets based on Particle Swarm Optimization. IEEE/ACM Transactions on Computational Biology and Bioinformatics. 2018; 15(3):999–102. https://doi.org/10.1109/TCBB.2017.2679004 PMID: 28287980

9. Yin Q, Cao B, Li X, Wang B*, Zhang Q*, Wei XP. An intelligent optimization algorithm for constructing a DNA storage code: NOL-HHO. International Journal of Molecular Sciences. 2020; 21(6): 2191 https://doi.org/10.3390/ijms21062191

10. Xue XL, Zhang Q, Wei XP, Guo L, Wang Q, An Image Fusion Encryption Algorithm Based on DNA Sequence and Multi-Chaotic Maps. Journal of Computational and Theoretical Nanoscience. 2010; 7:397–403.

11. Xue XL, Zhang Q, Wei XP, Guo L, Wang Q. A digital image encryption algorithm based on DNA sequence and multi-chaotic maps. Neural Network World. 2010; 20,285–296.

12. Zhang Q, Guo L, Wei XP. Image encryption using DNA addition combining with chaotic maps. Mathematical and Computer Modelling. 2010; 52:2028–2035. https://doi.org/10.1016/j.mcm.2010.06.005

13. Wei XP, Guo L, Zhang Q, Zhang JX, Guo SL. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. The Journal of Systems and Software. 2012; 85:290–299. https://doi.org/10.1016/j.jss.2011.08.017

14. Liu LL, Zhang Q, Wei XP. A RGB image encryption algorithm based on DNA encoding and chaos map. Computers and Electrical Engineering. 2012; 38:1240–1248. https://doi.org/10.1016/j.compeleceng.2012.02.007

15. Zhang Q, Guo L, Wei XP. A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik—International Journal for Light and Electron Optics. 2013; 124:3596–3600. https://doi.org/10.1016/j.ijleo.2012.11.018

16. Zhang Q, Wei XP. A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik—International Journal for Light and Electron Optics. 2013; 124:6276–6281. https://doi.org/10.1016/j.ijleo.2013.05.009

17. Zhang Q, Wei XP. RGB Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation. IETE Technical Review. 2013; 30:404–409.

18. Zhu SQ, Li JQ, Wang WH. Security analysis of improved image encryption method based on DNA coding and chaotic map. Application Research of Computers. 2017; 34:3090–3093.

19. Hermassi H, Belazi A, Rhouma R. Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. Multimedia Tools and Applications. 2014; 72:2211–2224. https://doi.org/10.1007/s11042-013-1533-6

20. Belazi A, Hermassi H, Rhouma R, Belghith S, Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. Nonlinear Dynamics. 2014; 76:1989–2004. https://doi.org/10.1007/s11071-014-1263-y

21. Liu YS, Tang J, Xie T. Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. Optics and Laser Technology. 2014; 60:111–115. https://doi.org/10.1016/j.optlastec.2014.01.015

22. Wang Y, Lei P, Yang HQ, Cao HY. Security analysis on a color image encryption based on DNA encoding and chaos map. Computers and Electrical Engineering. 2015; 46:433–446. https://doi.org/10.1016/j.compeleceng.2015.03.011

23. Xie T, Liu YS, Tang J. Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik—International Journal for Light and Electron Optics. 2014; 125:7166–7169. https://doi.org/10.1016/j.ijleo.2014.07.111

24. Özkaynak F, Yavuz S. Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik-International Journal for Light and Electron Optics. 2014; 125:1311–1320.

25. Zhang YS, Wen WY, Su MT, Li M. Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Nonlinear Dynamics. 2014; 125:1562–1564.

26. Zhang Y. Cryptanalysis of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik—International Journal for Light and Electron Optics. 2015; 126:223–229. https://doi.org/10.1016/j.ijleo.2014.08.129

27. Zeng L, Liu RR. Cryptanalyzing a novel couple images encryption algorithm based on DNA subsequence operation and chaotic system. Optik-International Journal for Light and Electron Optics. 2015; 126:5022–5025. https://doi.org/10.1016/j.ijleo.2015.09.219

28. Wu XJ, Kan HB, Kurths J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. Applied Soft Computing. 2015; 37:24–39. https://doi.org/10.1016/j.asoc.2015.08.008

29. Zhang YQ, Wang XY, Liu J, Chi ZL. An image encryption scheme based on the MLNCML system using DNA sequences. Optics and Lasers in Engineering. 2016; 82:95–103. https://doi.org/10.1016/j.optlaseng.2016.02.002

30. Mondal B, Mandal T. A light weight secure image encryption scheme based on chaos & DNA computing. Journal of King Saud University Computer and Information Sciences. 2017; 29:499–504. https://doi.org/10.1016/j.jksuci.2016.02.003

31. Zhang LM, Sun KH, Liu WH, He SB. A novel color image encryption scheme using fractional-order hyperchaotic system and DNA sequence operations. Chinese Physics B. 2017; 26:100504. https://doi.org/10.1088/1674-1056/26/10/100504

32. Li TY, Yang MG, Wu J, Jing X, Elsaid A. A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing. Complexity. 2017; 2017:1–13.

33. Suryadi M, Satria Y, Fauzi M. Implementation of digital image encryption algorithm using logistic function and DNA encoding. Journal of Physics: Conference Series.2018; 974: 1-8.

34. Zhang TT, Yan SJ, Gu CY, Ren R, Liao KX. Research on Image Encryption Based on DNA Sequence and Chaos Theory. Journal of Physics: Conference Series.2018; 1004: 1-6.

35. Dou YQ, Liu XM., Fan HJ, Li M. Cryptanalysis of a DNA and chaos based image encryption algorithm. Optik. 2017; 145: 456–464. https://doi.org/10.1016/j.ijleo.2017.08.050

36. Kumar M, Iqbal A, Kumar P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography. Signal Processing.2016; 125: 187-202.

37. Akhavan A, Samsudin A, Akhshani A. Cryptanalysis of an image encryption algorithm based on DNA encoding. Optics and Laser Technology. 2017; 95:94–99. https://doi.org/10.1016/j.optlastec.2017.04.022

38. Kalpana J, Murali P. An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos. Optik—International Journal for Light and Electron Optics. 2015; 126:5703–5709. https://doi.org/10.1016/j.ijleo.2015.09.091

39. Zhang J, Hou DZ, Ren HG, Islam N. Image Encryption Algorithm Based on Dynamic DNA Coding and Chen's Hyperchaotic System. Mathematical Problems in Engineering. 2016; 126:1–11.

40. Zhen P, Zhao G, Min LQ, Jin X. Chaos-based image encryption scheme combining DNA coding and entropy. Multimedia Tools and Applications. 2016; 75:1–17. https://doi.org/10.1007/s11042-015-2573-x

41. Chai XL, Gan ZH, Yang K, Chen YR, Liu XX. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operation. Signal Processing: Image Communication. 2017; 52:6–19.

42. Rehman A, Liao XF, Hahsmi MA, Haider R. An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. Optik—International Journal for Light and Electron Optics. 2018; 53:117–134. https://doi.org/10.1016/j.ijleo.2017.09.099

43. Zhang S, Gao TG. An image encryption scheme based on DNA coding and permutation of hyper-image. Multimedia Tools and Applications. 2016; 75:17157–14170. https://doi.org/10.1007/s11042-015-2982-x

44. Jain A, Rajpal N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimedia Tools and Applications. 2016; 75:5455–5472. https://doi.org/10.1007/s11042-015-2515-7

45. Belazi A, Talha M, Kharbech S, Xiang W. Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding. IEEE access. 2019; 7:36667–36681. https://doi.org/10.1109/ACCESS.2019.2906292

46. Wang XY, Hou YT, Wang SB, AND Li R. A New Image Encryption Algorithm Based on CML and DNA Sequence. IEEE access. 2018; 6:62272–62285. https://doi.org/10.1109/ACCESS.2018.2875676

47. Dagadu JC, Li JP, Aboagye EO and Deynu FK. Medical Image Encryption Scheme Based on Multiple Chaos and DNA Coding. International Journal of Network Security. 2019; 21: 83–90.

48. Wang XY, Wang Y, Zhu XQ, Luo C. A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. Optics and Lasers in Engineering. 2019;https://doi.org/10.1016/j.optlaseng.2019.105851.

49. Khan M, Hussain I, Jamal SS, Amin M. A Privacy Scheme for Digital Images based on Quantum Particles. International Journal of theoretical physics. 2019;. https://doi.org/10.1007/s10773-019-04301-6

50. Li X, Wang LY, Yan YF, Liu P. An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. Optik—International Journal for Light and Electron Optics. 2016; 127: 2558–2565. https://doi.org/10.1016/j.ijleo.2015.11.221

51. Zhou SH, Wang B, Zheng XD, Zhou CJ, Skokos C. An Image Encryption Scheme Based on DNA Computing and Cellular Automata. Computer Applications and Software. 2013; 30:318–322.

52. Chai XL, Fu XL, Gan ZH, Lu Y. A color image cryptosystem based on dynamic DNA encryption and Chaos. Signal Processing. 2019; 55:44–62. https://doi.org/10.1016/j.sigpro.2018.09.029

53. Khan M. A novel chaotic image encryption technique based on multiple discrete dynamical maps. Multimedia Tools and Applications. 2019; 78(18): 26203–26222. https://doi.org/10.1007/s11042-019-07818-4

54. Alghafis A, Waseem H., Khan M, Jamal SS, Amin M, Batool SI. A Novel Digital Contents Privacy Scheme Based on Quantum Harmonic Oscillator and Schrodinger Paradox. Wireless Networks. Wireless Netw (2020).

55. Huang XL, Ye GD. An image encryption algorithm based on hyper-chaos and DNA sequence. Multimedia Tools and Applications. 2014; 72:57–70. https://doi.org/10.1007/s11042-012-1331-6

56. Zhang J, Fang DX, Ren H, Miguel AF, San J. Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps. Mathematical Problems in Engineering. 2014; 60:111–115.

57. Enayatifar R, Abdullah AH, Isnin IF. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering. 2014; 56:83–93. https://doi.org/10.1016/j.optlaseng.2013.12.003

58. Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Optics and Lasers in Engineering. 2015; 73:53–61. https://doi.org/10.1016/j.optlaseng.2015.03.022

59. Xu GX, Guo XJ. DNA image encryption algorithm based on chaotic system. Journal of Computer Application. 2014; 34:3177–3179,3183.

60. Babaei M. A novel text and image encryption method based on chaos theory and DNA computing. Natural Computing. 2013; 12:101–107. https://doi.org/10.1007/s11047-012-9334-9

61. Rehman A, Liao XF, Ashraf R, Ullah S, Wang HW. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. Optik. 2018; 159: 348–367. https://doi.org/10.1016/j.ijleo.2018.01.064

62. Chen JX, Zhu ZL, Zhang LB, Zhang YS, Yang BQ. Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing. 2018; 142:340–353. https://doi.org/10.1016/j.sigpro.2017.07.034

63. Wu XJ, Wang KS, Wang XY, Kan HB, Kurths J. Color image DNA encryption using NCA map-based CML and one-time keys. Signal Processing. 2018; 148:272–287. https://doi.org/10.1016/j.sigpro.2018.02.028

64. Wu XJ, Kurths J, Kan HB. A robust and lossless DNA encryption scheme for color images. Multimedia Tools and Applications. 2018; 77:12349–12376. https://doi.org/10.1007/s11042-017-4885-5

65. Chai XL, Chen YR, Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in Engineering. 2017; 88: 197–213. https://doi.org/10.1016/j.optlaseng.2016.08.009

66. Zhang XC, Feng H, Niu Y. Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding. Computational intelligence and neuroscience. 2017; 2016: 1–11.

67. Ahadpour ZAS. Color image encryption based on DNA encoding and pair coupled chaotic maps. Multimedia Tools and Applications.2019; https://doi.org/10.1016/j.optlaseng.2019.105851.

68. Wu Y., Zhou Y.C., Saveriades G.,et al.,Local Shannon entropy measure with statistical tests for image randomness. Information Sciences. 2013; 222:323–342. https://doi.org/10.1016/j.ins.2012.07.049

69. Khan M, Masood F, Alghafis A. Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system. Neural Computing and Applications.2019.

70. Khan M, Munir N. A novel image encryption technique based on generalized advanced encryption standard based on field of any characteristic. Wireless and Personal Communication. 2019; 109(2):849–867. https://doi.org/10.1007/s11277-019-06594-6

71. Alghafis A, Firdousi F, Khan M., IramBatool S, Amin M. An efficient image encryption scheme based on chaotic and Deoxyribonucleic acid sequencing. Mathematics and Computers in Simulation. 2020; 177:441–466. https://doi.org/10.1016/j.matcom.2020.05.016

72. Alghafis A, Waseem HM, Khan M. A hybrid cryptosystem for digital contents confidentiality based on rotation of quantum spin states. Physica A: Statistical Mechanics and its Applications. 2019; 554:123908. https://doi.org/10.1016/j.physa.2019.123908

73. Alghafis A, Munir N, Khan M, Hussain I. An Encryption Scheme Based on Discrete Quantum Map and Continuous Chaotic System. International Journal of theoretical physics. 2020; 59:1227–1240. https://doi.org/10.1007/s10773-020-04402-7

74. Shah T, Ali A, Khan M, Farooq G, Andrade AA. Galois Ring GR(23,8) Dependent 24 × 24 S Box Design: An RGB Image Encryption Application. Wireless Personal Communications.

75. Waseem HM, Khan M, Alghafis A. An Efficient Public Key CryptosystemBased on Dihedral Group and Quantum Spin States, IEEE Access. 2020; 8: 71821–71832.

76. Munir N, Khan M, Wei ZC, Akgul A, Amin M, Hussain I. Circuit implementation of 3D chaotic self-exciting single-disk homopolar dynamo and its application in digital image confidentiality. Wireless Netw (2020). https://doi.org/10.1007/s11276-020-02361-9

77. Khan M, Masood F, Alghafis A, Amin M, Batool Naqvi SI. A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. PLoS ONE. 2019; 14(12): e0225031. https://doi.org/10.1371/journal.pone.0225031 PMID: 31856231

78. Rhouma R, Meherzi S, Belghith S. OCML-based colour image encryption. Chaos Soliton. Fract. 2009; 40:309–318 https://doi.org/10.1016/j.chaos.2007.07.083

79. Arshad U, Khan M, Shaukat S, Amin M, Shah T. An Efficient Image Privacy Scheme Based on Nonlinear Chaotic System and Linear Canonical Transformation. Physica A: Statistical Mechanics and its Applications. 2020; 546:123458. https://doi.org/10.1016/j.physa.2019.123458

80. Waseem HM, Khan M. A Novel Digital Contents Privacy Scheme Based on Kramer's Arbitrary Spin. International Journal of Theoritical Physics. 2019; 58(8):2720–2743. https://doi.org/10.1007/s10773-019-04162-z

81. Waseem HM, Khan M. A new approach to digital content privacy using quantum spin and finite-state machine. Journal of Applied Physics B. 2019; 125: 27. https://doi.org/10.1007/s00340-019-7142-y

82. Wang XY, Wang Y, Zhu XQ, Luo C. A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level. Optics and Lasers in Engineering. 2020; 125:105851. https://doi.org/10.1016/j.optlaseng.2019.105851

83. Yang YG, Guan BW, Li J, Li D, Zhou YH, Shi WM. Image compression-encryption scheme based on fractional order hyperchaotic systems combined with 2D compressed sensing and DNA encoding. Optics and Laser Technology. 2019; 119:105661. https://doi.org/10.1016/j.optlastec.2019.105661

84. Khawaja MA, Khan M. Application Based Construction and Optimization of Substitution Boxes Over 2D Mixed Chaotic Maps. International Journal of theoretical Physics. 2019; 58:3091–3117. https://doi.org/10.1007/s10773-019-04188-3

85. Khawaja MA, Khan M. A new construction of confusion component of block ciphers. Multimedia Tools and Applications. 2019; 78(22):32585–32604. https://doi.org/10.1007/s11042-019-07866-w