Image Encryption and Decryption Algorithm Based on DNA Sequence: Performance Analysis of Channel Fusion Processing

Weijie Gao[1], Qiang Liu[2(✉)], and Kun Yang[3]

[1] University of Electronic Science and Technology of China, Sichuan, China
202322011011@std.uestc.edu.cn
[2] Yangtze Delta Region Institute (Quzhou), University of Electronic Science and Technology of China, Quzhou, Zhejiang, China
liuqiang@uestc.edu.cn
[3] University of Essex, Colchester, Essex, UK
kunyang@essex.ac.uk

Abstract. To address the challenges of image encryption and decryption in the field of information security, this paper proposes a multi-channel fusion image encryption and decryption algorithm based on DNA sequences. Initially, a random key is generated using the Chen chaotic system. This key is then combined with eight DNA mapping methods that comply with the Watson-Crick rule to encode the original image data and a disordered matrix, resulting in corresponding base sequences. Boolean operations are performed on these base sequences, and the results are decoded using the DNA mapping methods to obtain the encrypted image. Finally, the encrypted image undergoes analysis for information entropy and gray value correlation. Simulation results demonstrate that transforming the three-dimensional matrix of a color image into a two-dimensional matrix for data processing significantly enhances encryption performance.

Keywords: Image encryption · DNA sequence · Chen chaotic system · Channel fusion · Encryption performance

1 Introduction

In modern society, protecting the security of image data is crucial for personal privacy, business secrets, and national security, so the secure transmission and storage of images is increasingly becoming a focus of attention [1]. In such a context, emerging technologies based on molecular communication provide

Supported by the National Natural Science Foundation of China under Grant No.62071101 and the Municipal Government of Quzhou under Grant No.2022D019 and Grant No. 2023D008.

Y. Chen et al. (Eds.): BICT 2024, LNICST 592, pp. 130–142, 2025.
https://doi.org/10.1007/978-3-031-81599-7_13

solutions. As a new communication mode, molecular communication integrates the mechanism of molecules transferring information in living organisms, and uses molecules as information carriers, which has the advantages of ultra-high density, ultra-low power consumption, and anti-jamming, etc. [2], and DNA sequences, as one of the important carriers of molecular communication, which provides a new way of thinking and methods for image encryption and decryption.

In this paper, a multi-channel fusion image encryption and decryption algorithm based on DNA sequences is proposed, which utilizes a chaotic system to generate a random key [3–5], maps the image and the permutation matrix under the Watson-Crick rule, and then uses Boolean operations on the mapping results of the image and the matrix. If the input is a color image, the Boolean operation will result in a three-dimensional matrix, and the multichannel fusion proposed in this paper is to change this three-dimensional matrix into a two-dimensional matrix.

In this paper, the basic theory related to the proposed algorithm is first introduced, then the algorithm implementation of multi-channel fusion encryption and decryption is described in detail, and simulation experiments are carried out together with single-channel processing and multi-channel processing (without fusion), and finally the information entropy and grayscale value correlation are analyzed for the simulation results.

2 Basic Theory of Proposed Algorithm

2.1 DNA Coding Rules

A DNA strand contains four nucleotides: A (adenine), T (thymine), G (guanine), and C (cytosine). These nucleotides can combine into a long strand where A pairs with T and G pairs with C. The grayscale value of each image pixel ranges from 0 to 255 and can be converted into an eight-bit binary number. This binary number can be split into two four-bit segments, each of which is encoded as a DNA base.

There are 24 possible encoding schemes, but only 8 schemes meet the Watson-Crick pairing rule [6]. Table 1 shows these schemes. Using the encoding scheme where A is 00, T is 11, G is 10, and C is 01, a binary sequence like 00111001 becomes ATGC. Thus, a pixel value can be represented by its corresponding DNA sequence, e.g., 57 is ATGC.

Table 1. DNA coding rules

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

To further elaborate, let's break down the process of how an image's pixel values are converted to DNA sequences:

1. Each pixel in a grayscale image has a value between 0 and 255. This value is first converted into an 8-bit binary number. For example, a pixel value of 57 is 00111001 in binary. The 8-bit binary number is then split into two four-bit segments: 0011 and 1001.
2. Using our encoding scheme, 00 is A, 11 is T, 10 is G, and 01 is C. Thus, 0011 translates to AT (A for 00, T for 11) and 1001 translates to GC (G for 10, C for 01). Therefore, 00111001 is represented as ATGC in the DNA sequence.
3. Due to Watson-Crick pairing rules, A pairs with T and G pairs with C. This ensures the robustness of the encoding scheme by allowing the complementary DNA strand to be deduced accurately.
4. Consequently, the grayscale value of 57 can be uniquely represented by the DNA sequence ATGC. This transformation ensures that each pixel's grayscale value is translated into a corresponding DNA sequence, preserving the image information in a biologically meaningful format.

2.2 Chen Chaotic Systems

Chen chaotic system is widely used in the field of encryption to generate random keys [6]. The system is based on a set of nonlinear equations, as shown in (1), these three nonlinear ordinary differential equations describe the rate of change of x, y, and z over time, respectively. The values of a,b,c can affect the behavior of the system so that it exhibits different dynamic properties such as periodic, quasi-periodic, or chaotic behavior. A common parameter setting is: a=35,b=3,c=28, under this parameter setting, Chen chaotic systems usually exhibit typical chaotic behavior.Chaotic sequences of high complexity and unpredictable nature can be generated by setting the system parameters and initial conditions, which are used in this paper to select a certain DNA coding rule to enhance the security of encryption.

$$\begin{aligned} x' &= a(y - x) \\ y' &= (c - a)x - xz + cy \\ z' &= xy - bz \end{aligned} \tag{1}$$

The process of generating the key stream by Chen chaotic system is as follows: first, the initial conditions and system parameters of Chen chaotic system are set, and then numerical integration using Euler's method is carried out, and iterative computation is performed to obtain the value of the system state at each time step. The generated chaotic sequence is converted into a key stream suitable for encryption operation after modulo operation and discretization. To ensure the uniformity and randomness of the key stream, an initial segment of the sequence is discarded.

The final generated keystream is used in different steps of image encryption, ensuring the complexity and security of the encryption process, making the encrypted image difficult to be decrypted by unauthorized third parties.

3 Proposed Algorithm

3.1 Boolean Rule Design

In the process of image encryption, after encoding the DNA rules, we obtain two DNA sequences representing the image data and the permutation matrix. These two DNA sequences are then compared and manipulated bit by bit to further encrypt the image data. This involves Boolean arithmetic [6], where logical operations on each base in the DNA sequence generate a new sequence, ensuring information confusion and concealment. During decryption, Boolean operations allow us to decode the encrypted data back into the original image information using the DNA sequence and the permutation matrix.

In this paper, three different Boolean operation rules are proposed, as shown in Table 2 to Table 4, and the encryption and decryption of a single channel is taken as an example, as shown in Fig. 1, to demonstrate the encryption and decryption effects of these three rules and their effects on image confidentiality and information integrity.

Table 2. Boolean rule 1

Encryption																
DNA1	A	A	A	A	T	T	T	T	G	G	G	G	C	C	C	C
DNA2	A	T	G	C	A	T	G	C	A	T	G	C	A	T	G	C
Result	T	G	C	G	C	A	G	C	G	T	A	T	C	G	T	A
Decryption																
DNA1	A	A	A	A	T	T	T	T	G	G	G	G	C	C	C	C
DNA2	A	T	G	C	A	T	G	C	A	T	G	C	A	T	G	C
Result	/	T	G	C	A	G	A/C	G	G	C	T	A	T/C	/	A	T

Table 3. Boolean rule 2

Encryption																
DNA1	A	A	A	A	T	T	T	T	G	G	G	G	C	C	C	C
DNA2	A	T	G	C	A	T	G	C	A	T	G	C	A	T	G	C
Result	A	G	T	C	G	A	C	T	T	C	A	G	C	T	G	A
Decryption																
DNA1	A	A	A	A	T	T	T	T	G	G	G	G	C	C	C	C
DNA2	A	T	G	C	A	T	G	C	A	T	G	C	A	T	G	C
Result	A	T	G	C	G	C	A	T	T	A	C	G	C	G	T	A

Table 4. Boolean rule 3

Encryption															
DNA1	A	A	A	A	T	T	T	T	G	G	G	G	C	C	C
DNA2	A	T	G	C	A	T	G	C	A	T	G	C	A	T	G	C
Result	A	T	G	C	T	A	C	G	G	C	A	T	C	G	T	A
Decryption															
DNA1	A	A	A	A	T	T	T	T	G	G	G	G	C	C	C	C
DNA2	A	T	G	C	A	T	G	C	A	T	G	C	A	T	G	C
Result	A	T	G	C	T	A	C	G	G	C	A	T	C	G	T	A

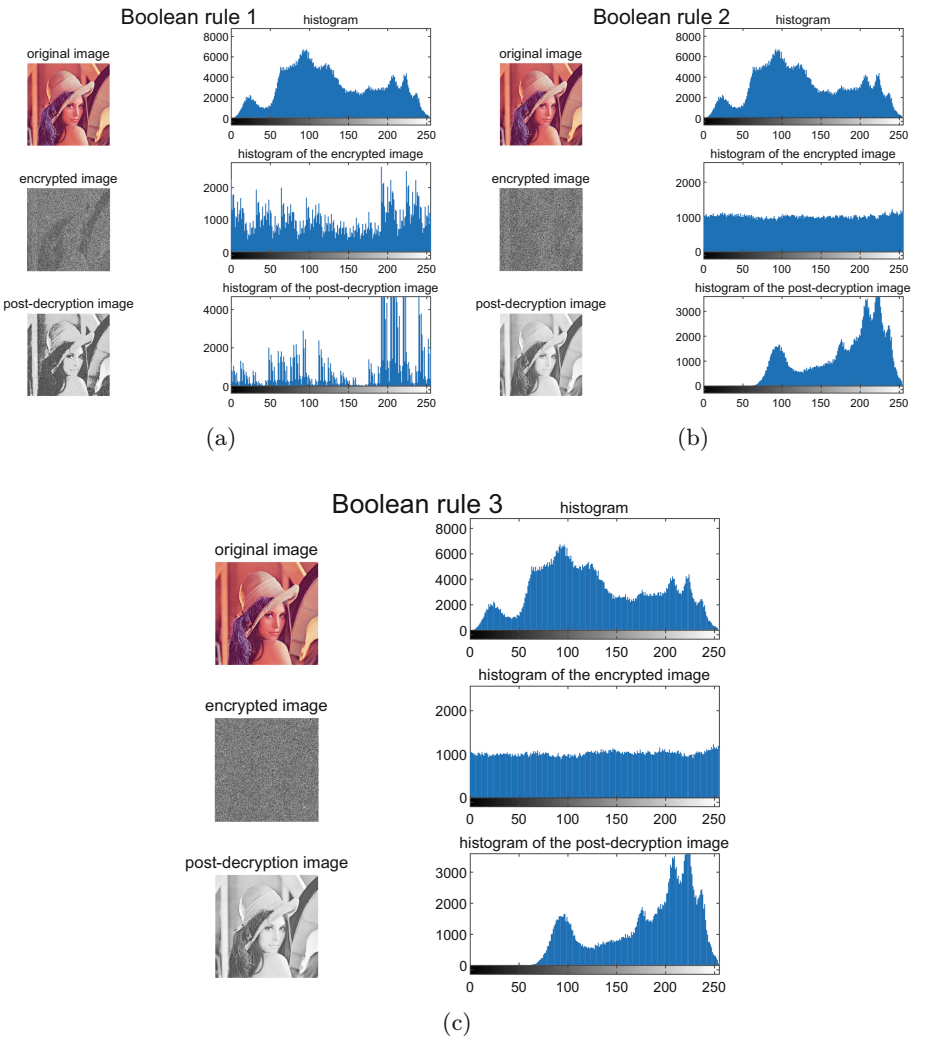

Fig. 1. Implementation of grayscale images under three Boolean operation rules.

Under different Boolean rules, the encryption performance of the image shows obvious differences, as can be seen in Fig. 1, the image encrypted by Boolean Rule 1 can respond to some of the information of the original image, and the image obtained by decryption does not respond well to the information of the original image. This is because the encryption and decryption process of Boolean Rule 1 has two problems: in the decryption process, AA and CT cannot correspond to any single base. This means that these pairs cannot be correctly restored during the decryption process, resulting in loss of information; TG and CA correspond to the same result during the decryption process. This situation triggers ambiguity in decryption because we cannot determine which base pair the original encrypted message is.

Although the ambiguity of Boolean Rule 1 in the decryption process limits its application in high-precision encryption and decryption, it can still be useful in specific domains or under specific conditions. Therefore, in practical applications, appropriate Boolean rules should be selected according to specific needs and tolerance to ensure the security and reliability of data.

In contrast, the other two Boolean operation rules can realize the mapping of each base pair, which avoids the problems of conflict and loss, and the encryption and decryption performance of images under these rules is significantly improved. Among these two rules, the encryption and decryption rules of Boolean operation Rule 3 are identical, thus reducing the complexity of the code while ensuring performance. The next Boolean operation used in this paper is Rule 3.

3.2 An Image Encryption And Decryption Algorithm Using Multi-channel Fusion

The encryption and decryption of grayscale images only need to deal with one color channel, while color images need to deal with three color channels, and the multi-channel fusion is to convert the three-dimensional matrix representing the color image into a two-dimensional matrix as shown in (2), and the following will describe its implementation process in detail. First of all, the three channels of the image and the disorder matrix are mapped with DNA coding; then a cell array of length 3 is created, each cell is used to store the DNA coding data of a color channel; then under the Boolean operation rules, the three cell arrays are operated with the disorder matrix to obtain a 1×3 cell array, and the size of each array is 512×512; Then the cell array is decoded to map the DNA sequence into decimal data; finally, the cell array is traversed, and the character array in the cell is converted to uint8 and appended to the result array dat_enc, which is a multi-channel fusion; finally, a 512×1536 encrypted image is obtained.

$$I_{MN\times C} = \mathrm{vec}(I_{M\times N\times C}) \tag{2}$$

The specific implementation process is shown in Fig. 2. The key of the whole process is how to convert the gray value of the image to DNA base sequence for operation. Its mainly through the bitand function of matlab, the image by bit with the operation. In matlab, bitand function can receive any decimal number

as input, and regard them as binary number for operation; bitand function will compare the two binary numbers corresponding to the bit, if both positions are 1, then the corresponding position of the result is also 1, or else the corresponding bit in the result is 0. This paper adopts the bitand function as shown in (3). The following gray value 216 as an example, calculate the value of a1, 216 corresponds to the binary of 11011000, 192 corresponds to the binary of 11000000, the two are operated, the first two binary digits are obtained. Finally, the four two-digit binary numbers corresponding to the grayscale values are put into matrix A for calculation. Using the DNA mapping rules defined above, the matrix A is traversed and transformed into a DNA sequence.

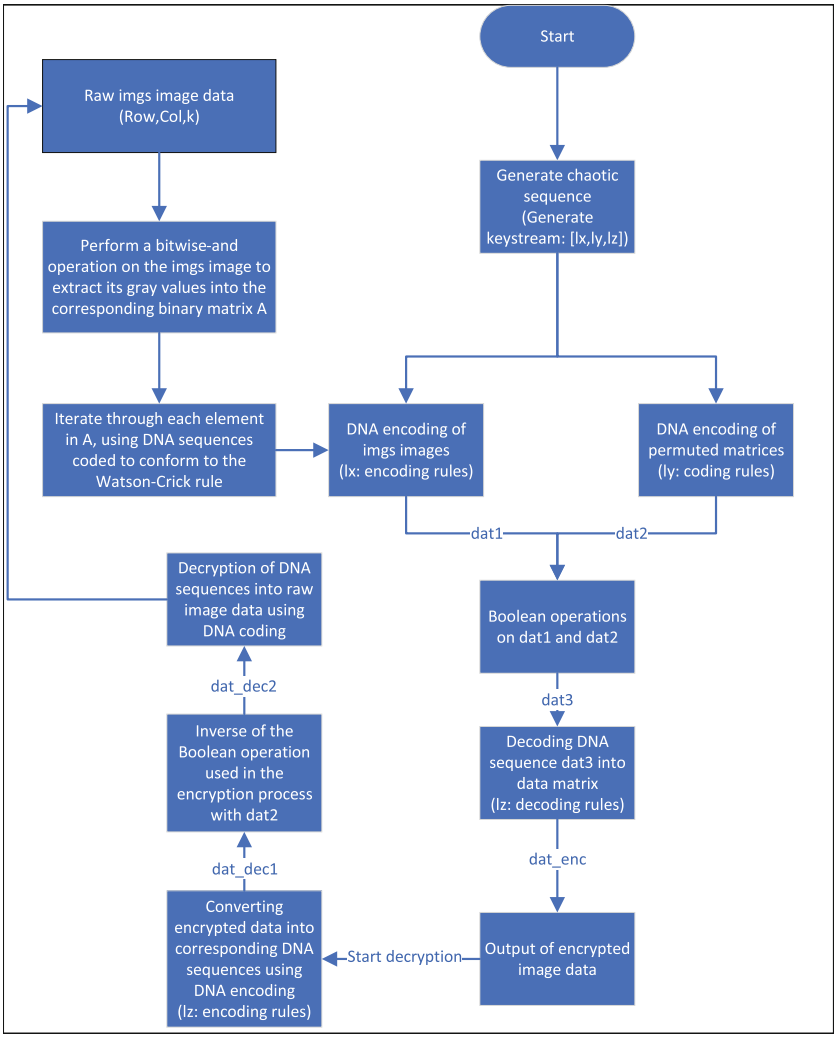

Fig. 2. Algorithm implementation flow.

$$\begin{aligned} a1 &= bitand(img, 192)/64; \\ a2 &= bitand(img, 48)/16; \\ a3 &= bitand(img, 12)/4; \\ a4 &= bitand(img, 3); \\ A &= [a1, a2, a3, a4]; \end{aligned} \tag{3}$$

The decryption process of the image simply follows the reverse order of the encryption process to restore the original image. It will not be elaborated in detail here. It should be noted that the same key [7] must be used when performing the inverse operation of the same operation as in the encryption process, otherwise the original image data will not be restored correctly.

4 Simulation Experiment and Result Analysis

In this section, simulation experiments are carried out on an image encryption and decryption algorithm using multi-channel fusion and comparative simulations are carried out along with single-channel processing and multi-channel processing (without fusion), the simulation results are shown in Fig. 3, and finally, the simulation results are analyzed in terms of information entropy and gray value correlation.

4.1 Histogram Analysis

Histogram analysis [8] is a method used to count the distribution pattern of pixel gray values in an image, whose horizontal axis represents the gray level (0 255) and vertical axis represents the number of pixels corresponding to the gray level. When the gray value distribution is more uniform, the image is more random and the ideal encryption effect is achieved. From the simulation results in Fig. 3, it can be seen that under the three encryption methods (a), (b), and (c), the number of pixels corresponding to the gray value of the histogram is uniformly distributed around 1000, 3000, and 3000, respectively, and thus (a), (b), and (c) have effectively encrypted the original image, which suggests that the attacker cannot decrypt the original image by analyzing the pattern of distribution of the pixel gray values in the image to break the original information of the original image.

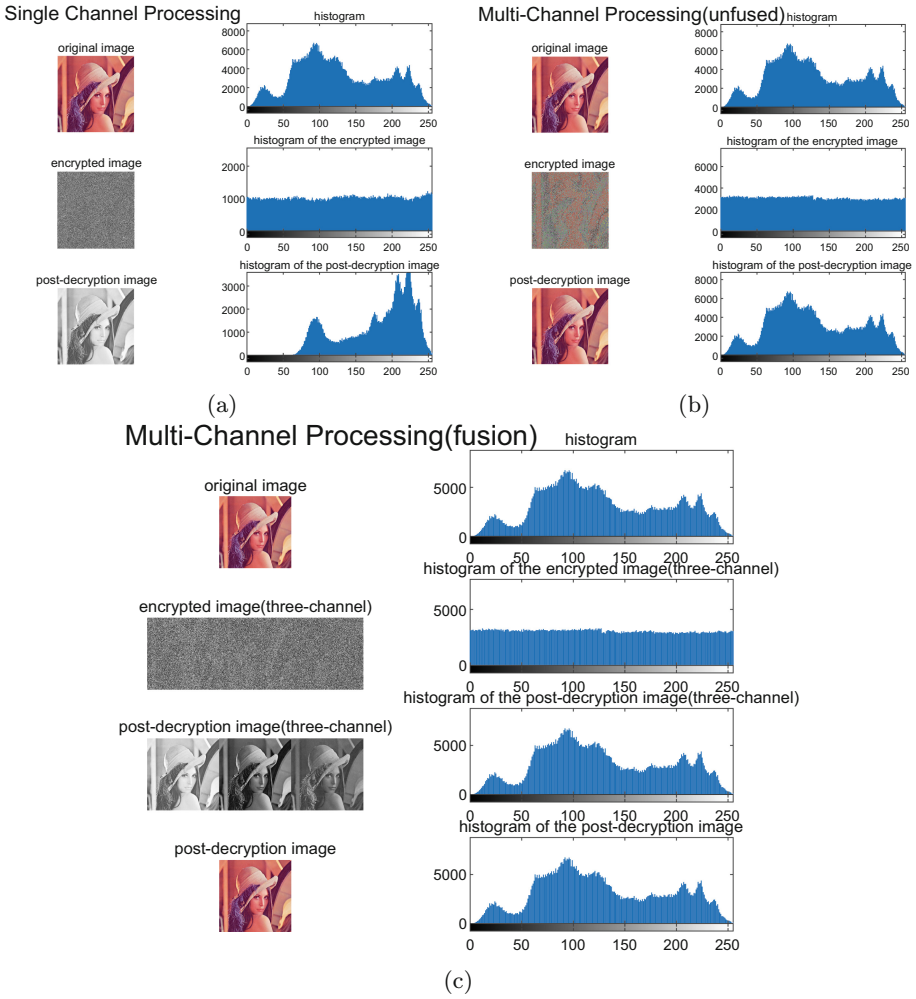

Fig. 3. Simulation results with three different treatments.

4.2 Information Entropy Analysis

Information entropy is a key metric for evaluating the randomness of the information source [9], and its increase improves the security of the cipher image.

The following is the process of calculating the information entropy. First of all, if the input image is a color image, we use the built-in `rgb2gray` function of MATLAB to convert it to a grayscale image. The `rgb2gray` function achieves this conversion by weighting the average RGB channel values (i.e., adding the red, green, and blue channel values according to the weights of 0.2989, 0.5870, and 0.1140, respectively), which better reflects the human eye's perception of brightness. Next, the `imhist` function built into MATLAB is used to calculate the gray level histogram of the image to obtain the frequency distribution of each gray level.

Then, these frequencies are normalized to a probability distribution, i.e., the frequency of each gray level is divided by the total number of pixels. In order to avoid invalid values (NaN) due to `log2(0)` in the calculation process, the parts with zero probability are removed. Finally, the information entropy is calculated using the normalized probability distribution according to Shannon's information entropy formula as shown in (4): where p_i denotes the probability of each gray level. This method effectively evaluates the complexity and information content of the image. Table 5 records the information entropy for the above three cases.

$$H = -\sum_{i} p_i \log_2(p_i) \tag{4}$$

Table 5. Information entropy

	(a)	(b)	(c)
original image	7.4451	7.4451	7.4451
encrypted image	7.9981	7.454	7.9989
post-decryption image	7.2531	7.4451	7.4451

It is known from literature [9] that the higher the information entropy, the higher the security of the image. Therefore, all three processing methods in (a)(b)(c) significantly improve the security of the ciphertext compared to the original image. However, in the case where a color image needs to be recovered, the method of color image processing with multi-channel fusion in (c) has a superior property, which has a higher value of information entropy than the method of unfused-channel processing in (b), which, in turn, represents a higher level of security. Alternatively, if image quality is not a primary consideration, we can also choose the single-channel processing method in (a), which encrypts and decrypts only one of the channels. This method not only has high security but also can save computational resources. In addition according to the literature [8], the ideal maximum value of the information entropy of a ciphertext image is 8, so both methods in (a)(c) have high security.

4.3 Neighboring Pixel Correlation Analysis

Neighboring pixel correlation reflects the degree of correlation of pixel values at adjacent locations in an image. A good image encryption algorithm reduces the adjacent pixel correlation. First, check whether the input image is a multi-channel image. If it is a multi-channel image, the function will calculate the adjacent pixel correlation of each channel separately, and finally find their mean value. The process is as follows: for each channel image, use the `circshift` function to circularly shift the image by 1 pixel in a column, then use the `corr2` function to calculate the correlation coefficients between the original channel image and the shifted image, and store the results in the `correlations` array. If

the input image is a single-channel image, it directly calculates the correlation between the image and its after-shift by 1 pixel in a circular column. The function `circshift` is used to circularly shift the image, while `corr2` is used to compute the 2D correlation coefficient between the two matrices.

In image encryption process, we expect smaller correlation of neighboring pixels [10], because smaller neighboring pixel correlation means less correlation between pixel values in the image, making the image more disordered. The more secure the image is in this case. Table 6 records the neighboring pixel correlation for the above three cases. Where in case of multi-channel images, we calculate the correlation for each channel separately and then the average value obtained is used as the correlation for the whole image.

Table 6. Neighboring pixel correlation

	(a)	(b)	(c)
original image	0.95802	0.95802	0.95802
encrypted image	−0.10842	0.075784	0.076751
post-decryption image	0.97749	0.95802	0.95802

From the results in the table, all three encryption methods (a)(b)(c) greatly reduce the correlation of the original image. However, both encryption methods (b)(c) are not as effective as (a).

Overall, among the three processing methods (a)(b)(c), (a) and (c) have better encryption performance. As shown in Fig. 4, the encrypted image of (a)(c) has a high information entropy, close to the ideal value of 8, while the (b) method, which has not been channel fusion, can only reach 7.45 with poor security. In Fig. 5, the correlation between the pixel values of the encrypted images of (a)(b)(c) are all low and the security is high.

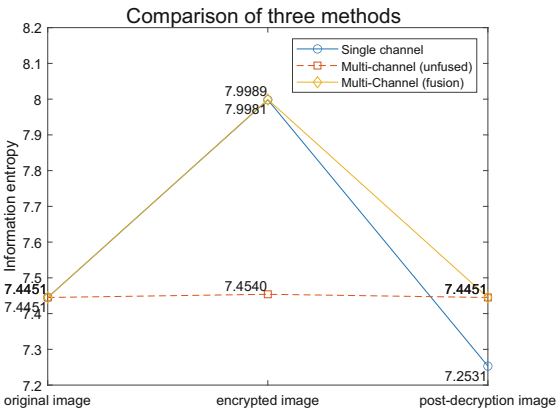

Fig. 4. Algorithm implementation flow.

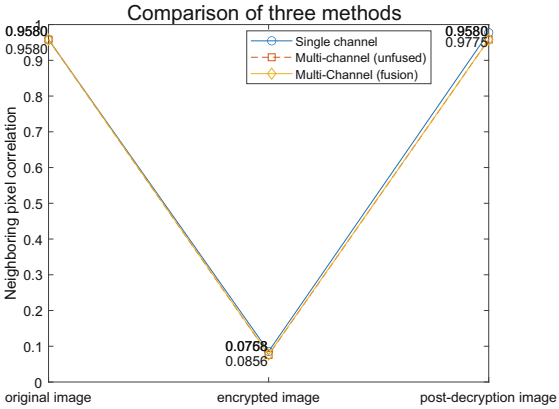

Fig. 5. Algorithm implementation flow.

5 Conclusion

To address the issue of image data security, this paper analyzes and compares three color image processing methods. If in the case of not pursuing image quality, it is recommended to use single-channel processing method, that is, only a certain channel of the color image processing. This method can restore the original image information to a certain extent with less computational resources. However, if color images need to be restored, multiple channels are fused, which has higher information entropy and therefore higher security. The experimental results also show that DNA-based computational storage has a wide range of applications and a great potential for development [11].

References

1. Sajitha, A.S., Rekh, A.S.: Review on various image encryption schemes. Mater. Today: Proc. **58**, 529–534 (2022)
2. Xue, X., Zhou, D., Zhou, C.: New insights into the existing image encryption algorithms based on DNA coding. PLoS ONE **15**(10), e0241184 (2020)
3. Samiullah, M., Aslam, W., Nazir, H., et al.: An image encryption scheme based on DNA computing and multiple chaotic systems. IEEE Access **8**, 25650–25663 (2020)
4. Iqbal, N., Hanif, M., Rehman, Z.U., et al.: On the novel image encryption based on chaotic system and DNA computing. Multimedia Tools Appl. **81**(6), 8107–8137 (2022)
5. Patro, K.A.K., Acharya, B., Nath, V.: Secure, lossless, and noise-resistive image encryption using chaos, hyper-chaos, and DNA sequence operation. IETE Tech. Rev. **37**(3), 223–245 (2020)
6. Sharkawy, N.H., Afify, Y.M., Gad, W., et al.: Gray-scale image encryption using DNA operations. IEEE Access **10**, 63004–63019 (2022)

7. Kaur, M., Singh, S., Kaur, M.: Computational image encryption techniques: a comprehensive review. Math. Probl. Eng. **2021**, 1–17 (2021)
8. Chen, F., Xu, J., Wang, J.: Research on color image encryption algorithms based on DNA coding and integer chaos. Shipboard Electron. Countermeasure **47**(01), 84–88 (2024). https://doi.org/10.16426/j.cnki.jcdzdk.2024.01.014
9. Fang, P., Huang, L., Lou, M., et al.: Image encryption algorithm based on two-dimensional logistic chaotic mapping and DNA sequence operation. China Sciencepaper **16**(03), 247–252 (2021)
10. Gasimov, V.A., Mammadov, J.I.: DNA-based image encryption algorithm. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing, vol. 734. no. 1, pp. 012162 (2020)
11. Zhang, Y., Ren, Y., Liu, Y., et al.: Preservation and encryption in DNA digital data storage. ChemPlusChem **87**(9), e202200183 (2022)