mathematics

MDPI

Article

Dynamic RNA Coding Color Image Cipher Based on Chain Feedback Structure

Heping Wen [1,2,*], Shenghao Kang [1], Zhuxi Wu [1], Yiting Lin [1,2,*] and Yiming Huang [1]

[1] School of Electronic Information, University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan 528402, China
[2] School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
* Correspondence: wenheping@uestc.edu.cn (H.W.); dr.yitinglin@gmail.com (Y.L.)

Abstract: This paper proposes a dynamic RNA-encoded color image encryption scheme based on a chain feedback structure. Firstly, the color pure image is decomposed into red, green, and blue components, and then a chaotic sequence based on plaintext association is introduced to encrypt the red component. Secondly, the intermediate ciphertext is obtained by diffusion after encryption by bit-level permutation, RNA dynamic encoding, RNA dynamic operation rules, and RNA dynamic decoding. Finally, to enhance the security of the image cryptosystem, the green and blue components of the image are repeatedly encrypted using the chain encryption mechanism associated with the intermediate ciphertext to obtain the color cryptographic image. In this paper, a 2D-SFHM chaotic system is used to provide pseudo-random chaotic sequences, and its initial key is calculated by combining the hash function and external parameters of the image, and the one-time ciphertext encryption strategy causes the proposed encryption to effectively resist cryptographic attacks. Experimental results and security analysis show that our encryption algorithm has excellent encryption effects and security performance against various typical attacks.

Keywords: dynamic RNA encoding; image encryption; chaotic encryption; chain encryption

MSC: 68W50; 34C28; 68P25

Citation: Wen, H.; Kang, S.; Wu, Z.; Lin, Y.; Huang, Y. Dynamic RNA Coding Color Image Cipher Based on Chain Feedback Structure. *Mathematics* **2023**, *11*, 3133. https://doi.org/10.3390/math11143133

Academic Editor: Konstantin Kozlov

Received: 29 May 2023
Revised: 10 July 2023
Accepted: 14 July 2023
Published: 16 July 2023

1. Introduction

With the rapid development of computer communication technology and network technology in recent years, various forms of data and information can be disseminated more frequently, more widely, and more rapidly through the network. Various types of data on information exchange have put forward new demands for a more secure transmission environment. As one of the most visual and common types of data in information transmission, images include a large amount of sensitive information. Therefore, the utilization of image encryption techniques can effectively prevent important data from being leaked during transmission. Many encryption methods have been proposed, such as quantum cipher [1–3], thumbnail-preserving encryption [4–7], biological coding [8–10], discrete wavelet transform [11–13], discrete cosine transform [14–16], bit-level encryption [17–19], Fourier transform [20–22], chaos theory [23–25], and so on [26–28]. Moreover, the unpredictability, pseudo-randomness, and high sensitivity to initial values of chaos make it the most effective and widely used approach for image encryption algorithms.

With international status, many scholars have achieved a series of important theoretical [29–31] and applied results [32–35] in using chaotic systems for image encryption. In 2022, article [9] proposed a color image encryption scheme combining a non-degenerate discrete hyperchaotic system with dynamic coding of deoxyribonucleic acid (DNA). This paper proposes a sequence based on a non-degenerate hyperchaotic

system to perform binary bit-level alignment, DNA encoding encryption, and bit-level confusion for image encryption. The experimental results show that this encryption algorithm can resist various common cryptographic attacks and has strong resistance to interference. A color image encryption scheme based on a two-dimensional hyperchaotic enhanced Henon map and cross-diffusion [36] was proposed in 2023. In this paper, an enhanced version of the Henon map is proposed, while image diffusion is performed after scrambling the three channels of the color image using the Arnold map to obtain the final ciphertext. It was experimentally verified that this encryption algorithm has the features of high efficiency and security. In the same year, a cross-channel color image encryption algorithm based on a 2D hyperchaotic map [37] was proposed. This algorithm newly proposed a cross-channel color image encryption algorithm combined with peripheral-pixel expansion technique, and the resultant experimental analysis illustrates that this algorithm encrypts well against various cryptographic attacks. In the existing research on chaotic image encryption, the performance of chaos and algorithms has a great impact on the security and efficiency of cryptosystems. It is significantly important and an urgent need to explore an image encryption algorithm that uses chaotic mapping constructs to resist various illegal attacks.

In this paper, we propose a cross-channel chaotic color image encryption algorithm based on 2D-SFHM and RNA coding for plaintext association and ciphertext data feedback. The algorithm uses a chaotic encryption sequence associated with the plaintext image for encrypting the first channel of the color image and then uses a chaotic sequence associated with the intermediate ciphertext for encrypting the last two channels of the color image and proposes a color image encryption scheme consisting of bit-level permutation, RNA dynamic encoding, and row and column diffusion. The experimental results demonstrate that the algorithm achieves excellent encryption effectiveness and good encryption efficiency, and the proposed image encryption algorithm can be safe against various illegal attacks.

The main innovations and contributions of this paper are as follows.

- Existing biological coding possesses easy-to-break encoding and a single operation rule. This color image encryption algorithm differs from the previous static RNA encoding by using dynamic RNA encoding and dynamic operation rules to improve the encryption effect and resistance to illegal attacks.
- Existing encryption algorithms have unreasonable structures. If plaintext correlation or ciphertext feedback is not used, an algorithm is vulnerable to attacks, such as a known plaintext attack or a chosen plaintext attack. This color image encryption algorithm uses plaintext correlation to generate the dynamic chaotic key and intermediate ciphertext correlation to generate dynamic chaotic keys, which greatly improves the ability to resist cryptographic attacks.
- Existing encryption schemes are based on pixel-level encryption, which has insufficient encryption granularity, and pixel-level scrambling has security risks. The present color image encryption algorithm uses bit-level permutation and chain RNA dynamic encoding with two-bit-level diffusion in its RNA dynamic encoding. It is experimentally verified that this algorithm effectively improves security.
- Existing low-dimensional chaotic systems have difficulty in passing the National Institute of Standards and Technology (NIST) test due to their insufficient security, and the chaotic sequences have the risk of being estimated or identified. The current color image encryption algorithm, employing the 2D-SFHM chaotic system, offers faster generation of random sequences, exhibits more intricate dynamic behavior, and delivers superior performance compared to mainstream mappings. Furthermore, it incorporates multiple parameters that facilitate the design of more secure and sensitive keys without introducing data redundancy.

The rest of this paper is organized as follows. Section 2 briefly describes the 2D-SFHM chaotic system and the RNA rules for encoding and RNA operation. Section 3 introduces the encryption algorithm developed in this paper. Section 4 presents the experimental results and simulation results. The last section is the conclusion of the paper.

2. Related Theories

2.1. 2D-SFHM Chaotic System

Chaotic systems are extensively utilized in image encryption algorithms because of their high initial value sensitivity and their non-divergence, non-convergence, and non-periodicity characteristics, and the resulting sequences are strongly random. This paper uses a 2D-SFHM chaotic system, 2D-SFHM, consisting of an inversely proportional function and a 1D sine map. The specific equation is expressed as follows:

$$\begin{cases} x_{n+1} = \sin \frac{a\pi^2}{x_n y_n} \\ y_{n+1} = \sin(b\pi^2 x_n (1 - y_n)) \end{cases} \tag{1}$$

where a and b are recursive parameters and the variables x_{n+1} and y_{n+1} are generated by iterating over the initial variables x_n and y_n.

2.2. RNA Coding and Operation Rules

RNA (ribonucleic acid) is a vital biological macromolecule in biological systems, serving as a conduit for the transmission of genetic information. RNA is a long-chain molecule composed of ribonucleotides linked together by phosphodiester bonds. It consists of four bases: adenine (A), guanine (G), cytosine (C), and uracil (U), where A and U are complementary pairs and C and G are complementary pairs. Comply with the principle of complementary pairing, namely A–U and C–G. There are eight coding rules specified in Table 1.

Table 1. RNA coding rules.

Rule	1	2	3	4	5	6	7	8
00	A	A	U	U	C	C	G	G
01	C	G	C	G	A	U	A	U
10	G	C	G	C	U	A	U	A
11	U	U	A	A	G	G	C	C

In addition, RNA has six types of operations: addition, subtraction, addition-complement, subtraction-complement, exclusive OR (XOR), and exclusive NOR (XNOR), like the binary system. The specific operation rules are shown in Tables 2 and 3.

Table 2. RNA base Addition, Subtraction, and XOR operation.

Base	Addition $+$	AGCU Subtraction $-$	XOR $\oplus$
A	A G C U	A U C G	A G C U
G	G C U A	G A U C	G A U C
C	C U A G	C G A U	C U A G
U	U A G C	U C G A	U C G A

Table 3. RNA base Add-Complement, Sub-Complement, and XNOR operation.

Base	Add-Complement $+'$	AGCU Sub-Complement $-'$	XNOR $\odot$
A	U C G A	U A G C	U C G A
G	C G A U	C U A G	C U A G
C	G A U C	G C U A	G A U C
U	A U C G	A G C U	A G C U

3. The Proposed Encryption Algorithm

In this paper, we propose a chained feedback structure with plaintext correlation and ciphertext data feedback and design a digital image encryption scheme based on RNA dynamic coding and 2D chaotic system. The scheme consists of five steps: dynamic key generation, bit-level permutation, RNA dynamic encryption, row and column diffusion, and ciphertext data feedback. The overall design block diagram of the encryption scheme is shown in Figure 1.

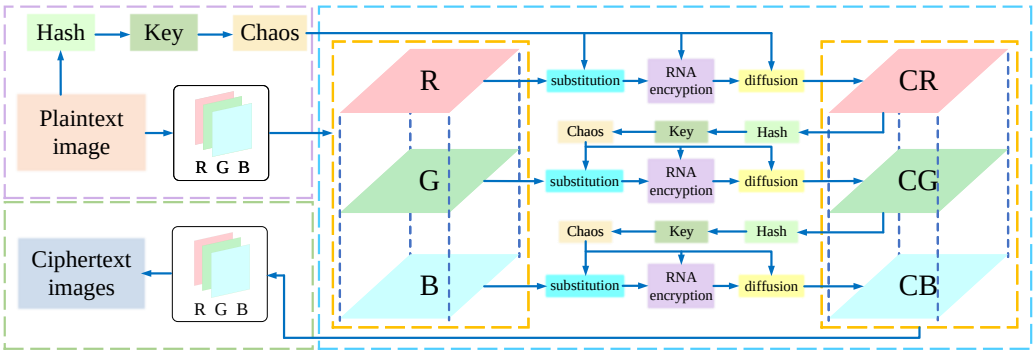

Figure 1. Block diagram of the overall design of the encryption scheme.

Take the matrix as an example to encrypt a single channel, and the specific encryption process is shown in Figure 2.

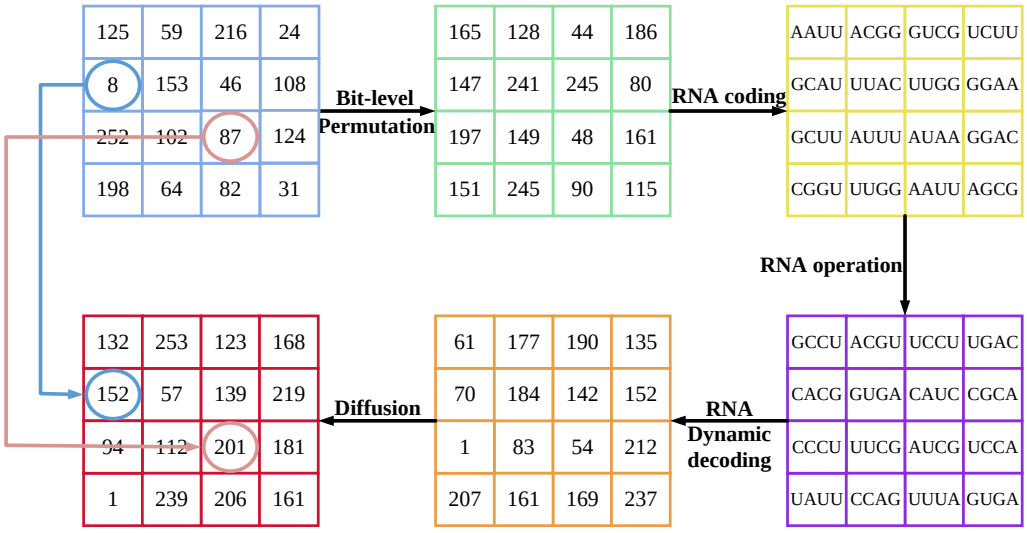

Figure 2. Single-channel encryption example.

3.1. Encryption Process

3.1.1. Dynamic Key Generation

Input a color plaintext image P of size $H \times W \times 3$, and divided into three channels by R, G, B as P_R, P_G, P_B. In this paper, the ciphertext data feedback structure is used to encrypt the layered image first, and the specific process is as follows:

Step 1: Obtain image feature values.

Firstly, after inputting the plaintext image and using the hash table to obtain the MD5 hash of the plaintext image, a 32-bit hexadecimal number of fixed bit lengths can be obtained. Then, further processed to a decimal number, each bit is represented as $h(x)$ and $h(x) \in \{0, 1, 2, \ldots, 14, 15\}$, where $x = [1, 2, 3, \ldots, 31, 32]$.

Step 2: Scrambled initial values.

After obtaining the hash values, the initial values of the chaotic mapping are perturbed so that different images correspond to different obtained key sequences to improve their ability to resist differential attacks, as shown in Equation (2).

$$\begin{cases} key_1 = h(1) + h(5) + h(9) + h(13) + h(17) + h(21) + h(25) + h(29) mod 100 \\ key_2 = h(2) + h(6) + h(10) + h(14) + h(18) + h(22) + h(26) + h(30) mod 100 \\ key_3 = 0.1 + (h(3) + h(7) + h(11) + h(15) + h(19) + h(23) + h(27) + h(31))/10000 \\ key_4 = 0.1 + (h(4) + h(8) + h(12) + h(16) + h(20) + h(24) + h(28) + h(32))/10000 \end{cases} \tag{2}$$

where $mod(.)$ is the modulo function, key_1, key_2 denotes the plaintext-based key parameter, and key_3, key_4 denotes the scrambled initial value of the sequence.

Step 3: Sequence processing.

The key_1, key_2, key_3, key_4 is substituted into the 2D-SFHM chaotic system to obtain four pseudo-random sequences w_1, w_2, w_3, w_4 and processed according to the range of values required by the encryption module as follows:

$$\begin{cases} s_1 = (|w_1| \times 10^{15} - |\lfloor w_1 \rfloor| \times 10^{15}) \\ s_2 = (|w_2| \times 10^{15} - |\lfloor w_2 \rfloor| \times 10^{15}) mod 8 \\ s_3 = (|w_3| \times 10^{15} - |\lfloor w_3 \rfloor| \times 10^{15}) mod 6 \\ s_4 = (|w_4| \times 10^{15} - |\lfloor w_4 \rfloor| \times 10^{15}) mod 8 \\ s_5 = (|w_4| \times 10^{15} - |\lfloor w_4 \rfloor| \times 10^{15}) \end{cases} \tag{3}$$

where $\lfloor \cdot \rfloor$ denotes downward rounding, $mod(.)$ is the modulo function, s_1, s_2, s_3, s_4, s_5 is the processed random sequences.

3.1.2. Bit-level Permutation

At the same time, the pseudo-random sequence s_1 is sorted to obtain two sorted sequences $rowK, colK$. Next, the image P_R is expanded by bit-level; the image size is adjusted to $H \times 8W$. Finally, the hierarchical image is permuted in bit level by the sorted sequence. The specific operation is as follows:

$$\begin{cases} [v_1, rowK] = sort(s_1(1:H)) \\ [v_2, colK] = sort(s_1(H+1, 8W)) \\ C_{R1}(i,j) = P_R(rowK(i), rowK(j)) \end{cases} \tag{4}$$

where the $sort(\cdot)$ function sorts each bit of the input sequence from lowest to highest. v_1, v_2 denotes the result of reordering the sequence. C_{R1} denotes the image after bit-level permutation, i, j denotes the sorting index, $i = 1, 2, 3, \ldots, H$, $j = 1, 2, 3, \ldots, 8W$.

3.1.3. RNA Dynamic Encryption

RNA encryption is performed on the permuted image C_{R1}. Through the three steps of RNA dynamic encoding, RNA dynamic operation, and RNA dynamic decoding, the effect of multiple iterations of encryption is achieved, thus enhancing the security and randomness of the algorithm. The specific encryption steps are shown in Figure 3.

Step 1: RNA dynamic encoding.

Firstly, the RNA encoding is performed on the permuted matrix P_{R1} presented in sequential order from left to right and from top to bottom, and one encoding rule, i.e., 4 RNA characters, is dynamically updated every 8 bits, thus enhancing the encoding complexity to improve the security of the algorithm. Next, the pseudo-random sequence s_2 is reconstructed as the key image K, with size of $H \times W$, expanded by bits and adjusted to a bit matrix of dimension size of $H \times 8W$. Finally, the permuted image C_{R1} and the key matrix K are dynamically encoded to obtain the encoded image C_{R2} and the key matrix K'. The particular mechanism of RNA dynamic encoding is depicted as follows:

$$\begin{cases} C_{R2}(4(i-1)+1)(4(i-1)+4) = RNA\_encode(C_{R1}(8(i-1))+1:(8(i-1)+8), s_2) \\ K'(4(i-1)+1)(4(i-1)+4) = RNA\_encode(K(8(i-1))+1:(8(i-1)+8), s_2) \end{cases} \quad (5)$$

where $i = 1, 2, 3, \ldots, H$, RNA_encode is the RNA dynamic coding rules, and the operation is shown in Figure 3. The coding method is dynamically controlled by chaotic sequences s_2 to improve the security of the algorithm.

Step 2: RNA dynamic operation.

To make the encryption algorithm more resistant to differential attacks, a pseudo-random sequence s_3 is used to perform RNA dynamic operation on the image C_{R2} and the key matrix K' to make the encryption algorithm more randomized. The RNA dynamic operation process is expressed as follows:

$$\begin{cases} C_{R3} = C_{R2} + K' & if \quad s_3 = 0 \\ C_{R3} = C_{R2} - K' & if \quad s_3 = 1 \\ C_{R3} = C_{R2} +' K' & if \quad s_3 = 2 \\ C_{R3} = C_{R2} -' K' & if \quad s_3 = 3 \\ C_{R3} = C_{R2} \oplus K' & if \quad s_3 = 4 \\ C_{R3} = C_{R2} \odot K' & if \quad s_3 = 5 \end{cases} \quad (6)$$

where C_{R3} is the intermediate ciphertext image after the RNA dynamic operation.

Step 3: RNA dynamic decoding.

RNA dynamic decoding is the reverse process of RNA dynamic coding. However, it is worth pointing out that the chaotic sequences for decoding are different from encoding, so it is not a straightforward inverse process but rather equivalent to a dual encryption transformation. The RNA dynamic decoding process is represented as

$$C_{R4}(8(i-1)+1)(8(i-1)+8) = RNA\_decode(C_{R3}(4(i-1))+1:(4(i-1)+4), s_4) \quad (7)$$

where RNA_decode is the RNA dynamic decoding rules, and the operation is shown in Figure 3. The decoding method is dynamically controlled by chaotic sequences s_4 to achieve the secondary encryption effect and improve the algorithm's security.

3.1.4. Row and Column Diffusion

The input pseudo-random sequence s_5 is processed and converted into a pseudo-random sequence R_1, R_2, R_3, R_4 suitable for row and column diffusion. The four generated sequences are reconstructed into matrices of the same size as the decoded image C_{R5}, which are R_1, R_2, R_3, R_4, respectively. Then, these four matrices are used to perform two rounds of row and column modulo operation and diffusion on the disordered image, respectively, and the diffusion result is expressed as C_R. The basic type of this diffusion is expressed as

$$C_{R(i)} = \begin{cases} (C_{R5(1)} + C_{R5(T)} + \lfloor (R_{(1)} \times 2^{10}) \rfloor) modF & if \quad i = 1 \\ (C_{R(i-1)} + C_{R5(i)} + C_{R5(i+1)} + \lfloor (R_{(i)} \times 2^{10}) \rfloor) modF & if \quad i = [2, T-1] \\ (C_{R(T-1)} + C_{R5(T)} + \lfloor (R_{(T)} \times 2^{10}) \rfloor) modF & if \quad i = T \end{cases} \quad (8)$$

where $floor(.)$ is the downward rounding function, $mod(.)$ is the modulo function, and F is the pixel level of the image. For row diffusion, T is the number of rows. C_{R5}, C_R and R represent the i-th row sequence of decoded image, diffused image, and chaotic real matrix, respectively. For column diffusion, T is the number of columns. C_{R5}, C_R and R represent the i-th column sequence of decoded image, diffused image, and chaotic real matrix, respectively. The specific flow of single-round row diffusion is shown in Figure 4.

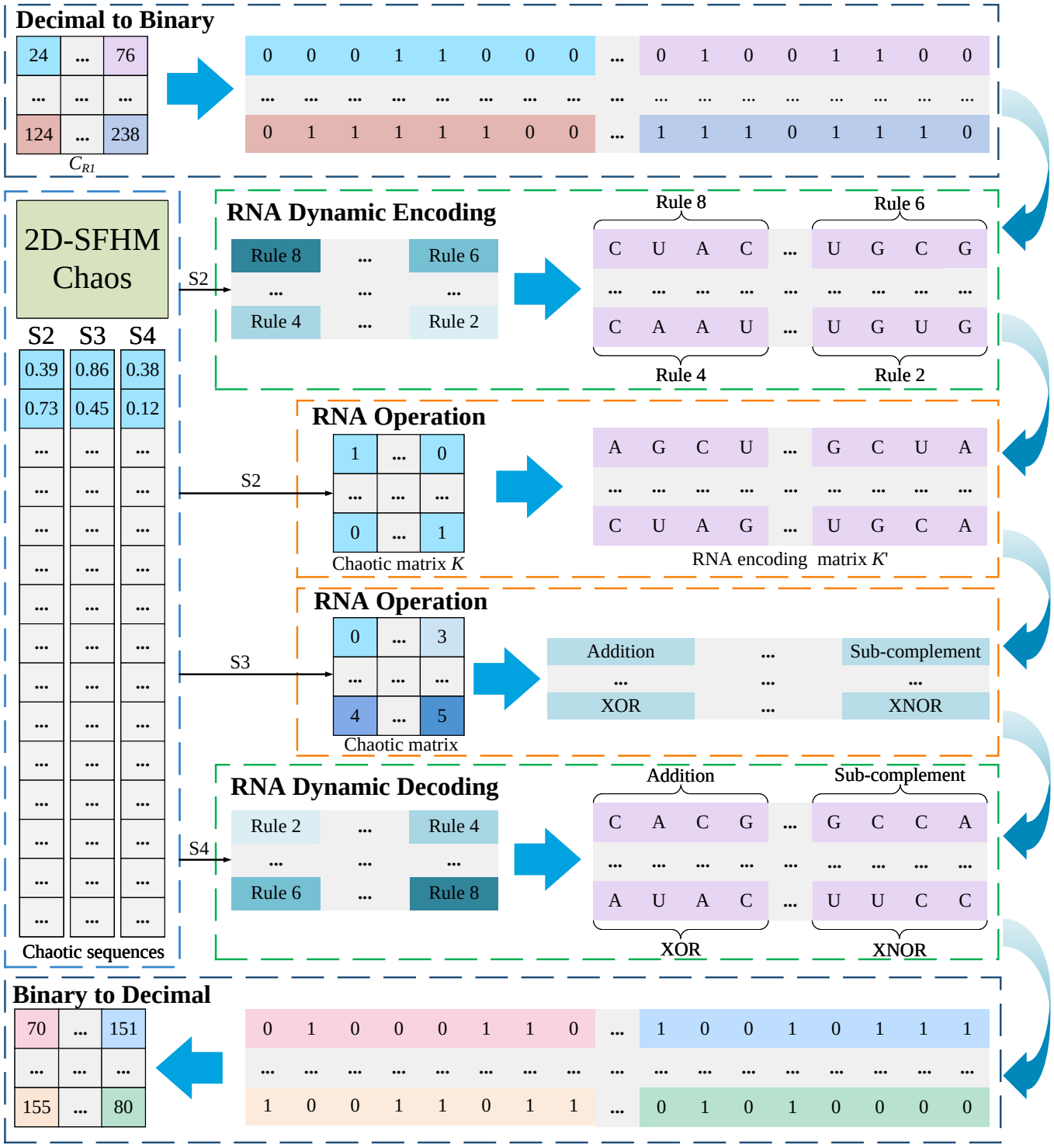

Figure 3. RNA dynamic encryption example.

3.1.5. Ciphertext Data Feedback

The MD5 hash of the diffused image C_R is obtained using a hash table, and the pseudo-random sequence is obtained by substituting the key into the chaotic system. Following the above encryption process, ciphertext image C_G is obtained, and ciphertext image C_G is used in the same way to obtain ciphertext image C_B. This process constitutes a chained ciphertext data feedback structure, which improves the performance and efficiency of the encryption algorithm.

Finally, ciphertext image C_R, C_G, C_B is synthesized into the final ciphertext C .

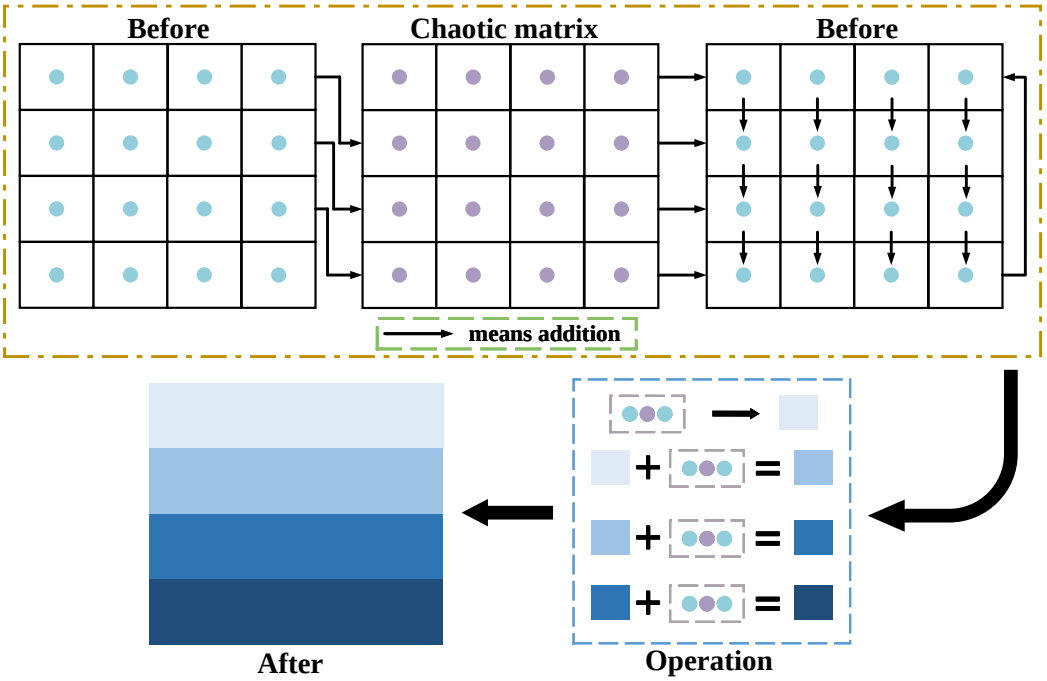

Figure 4. Example of single-round row diffusion visualization.

3.2. Decryption Process

Decryption is the inverse process of encryption. First, the ciphertext C is divided into three channels RGB, divided into C_R, C_G, C_B, and the hash value of ciphertext C_G is used to decrypt the ciphertext C_B through inverse row and column diffusion, RNA dynamic encoding, RNA dynamic operation, RNA dynamic decoding, and inverse permutation to obtain the decrypted image I_B . Then, in the same way, the decrypted image I_B is obtained by using the image I_G, I_R in turn. Finally, the images I_R, I_G, I_B are synthesized into the final decrypted image I. The single-channel decryption flow is shown in Figure 5.

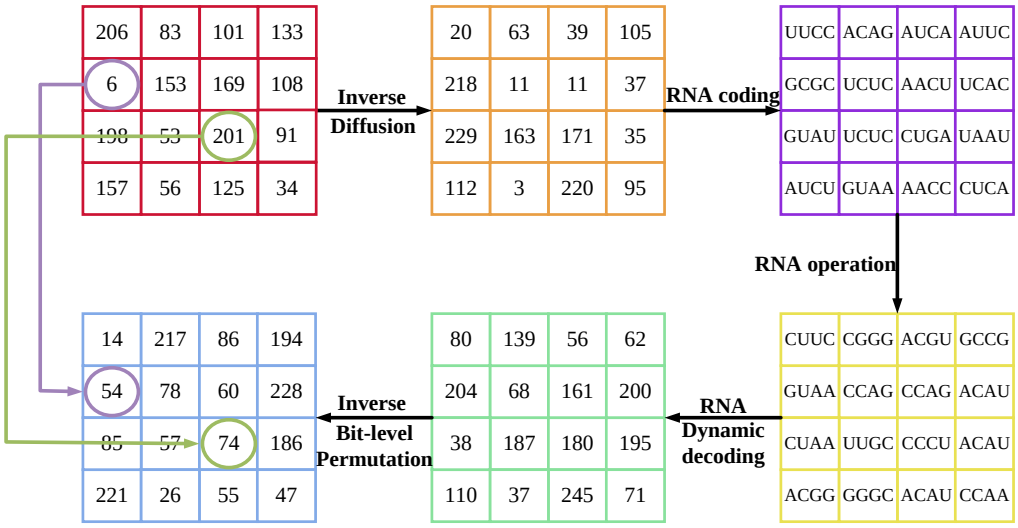

Figure 5. Single-channel decryption example.

4. Experimental Results, Analysis, and Discussion

4.1. Experimental Environment

For the experimental platform, we used a personal computer (PC) host with MATLAB R2022a experimental software installed. The processor of the PC is AMD Ryzen™ 9 5950X

CPU with 3.88 GHz, the memory size is 16 GB, the hard disk size is 1 TB, and the operating system is Windows 10. The image data selected for the experiment is also USC-SIPI.

4.2. Experimental Results and Analysis

4.2.1. Statistics Histogram

The histogram visually portrays the distribution of grayscale levels and their respective frequencies within the image. Generally, the histogram of a plaintext image shows a certain statistical pattern, while the statistical characteristics of the encrypted image histogram show a noise-like distribution, so a good encryption algorithm can process the image into the form of a noise-like distribution and thus mask the main information of the image. We select seven plaintext images of different sizes, as illustrated in Figure 6a, and obtain the corresponding ciphertext images by encryption, as presented in Figure 6c. The respective histograms before and after encryption are shown in Figure 6b,d. It can be seen that the encrypted image well masks the main information of the plaintext image, thus eliminating the possibility of an attacker using image statistical analysis to decipher the ciphertext image.

4.2.2. The Coefficient of Adjacent Pixels

Usually, the plaintext image contains a large number of pixels with high neighborhood correlation, while the ciphertext image encrypted by a good encryption algorithm will not correlate any pixel and its neighboring pixels. Therefore, a robust encryption scheme aims to generate a ciphertext image wherein neighboring pixels exhibit negligible correlation.

To calculate and compare the correlation of adjacent pixels in the plaintext and ciphertext images, we used the Pearson correlation coefficient equation for calculation. Firstly, we randomly select 3000 pairs of neighboring pixel points from the plaintext image and ciphertext image and then calculate the correlation coefficients of neighboring pixels in horizontal, vertical, diagonal, and anti-diagonal directions, respectively, according to Equation (9). The correlation coefficients are calculated as follows:

$$\begin{cases} r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ \mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \\ E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \end{cases} \tag{9}$$

where x_i and y_i constitute the i-th pair of horizontal/vertical/diagonal/anti-diagonal neighboring pixels, N is the total number of horizontal/vertical/diagonal/anti-diagonal neighboring pixels, $cov(x,y)$ is the covariance between pixel values x and y, $D(x)$ and $D(y)$ are the pixel value x and pixel value y mean-square error, $E(x)$ and $E(y)$ are the expected values of pixel value x and pixel value y, respectively. r_{xy} is the correlation coefficient of pixel values x and y. The adjacent pixel correlation data of the encrypted images are shown in Figure 7, which shows the correlation between two horizontal, vertical, diagonal, and anti-diagonal neighboring pixels in the normal image and encrypted image of "Lena", respectively. And, from the experimental data in Table 4, it is evident that the correlation coefficient of ordinary images approaches 1, while the correlation coefficient of encrypted images is approximately equal to 0. This signifies that the proposed encryption scheme generates images with de-correlated neighboring pixels. Therefore, the proposed scheme in this paper can protect against statistical attacks.

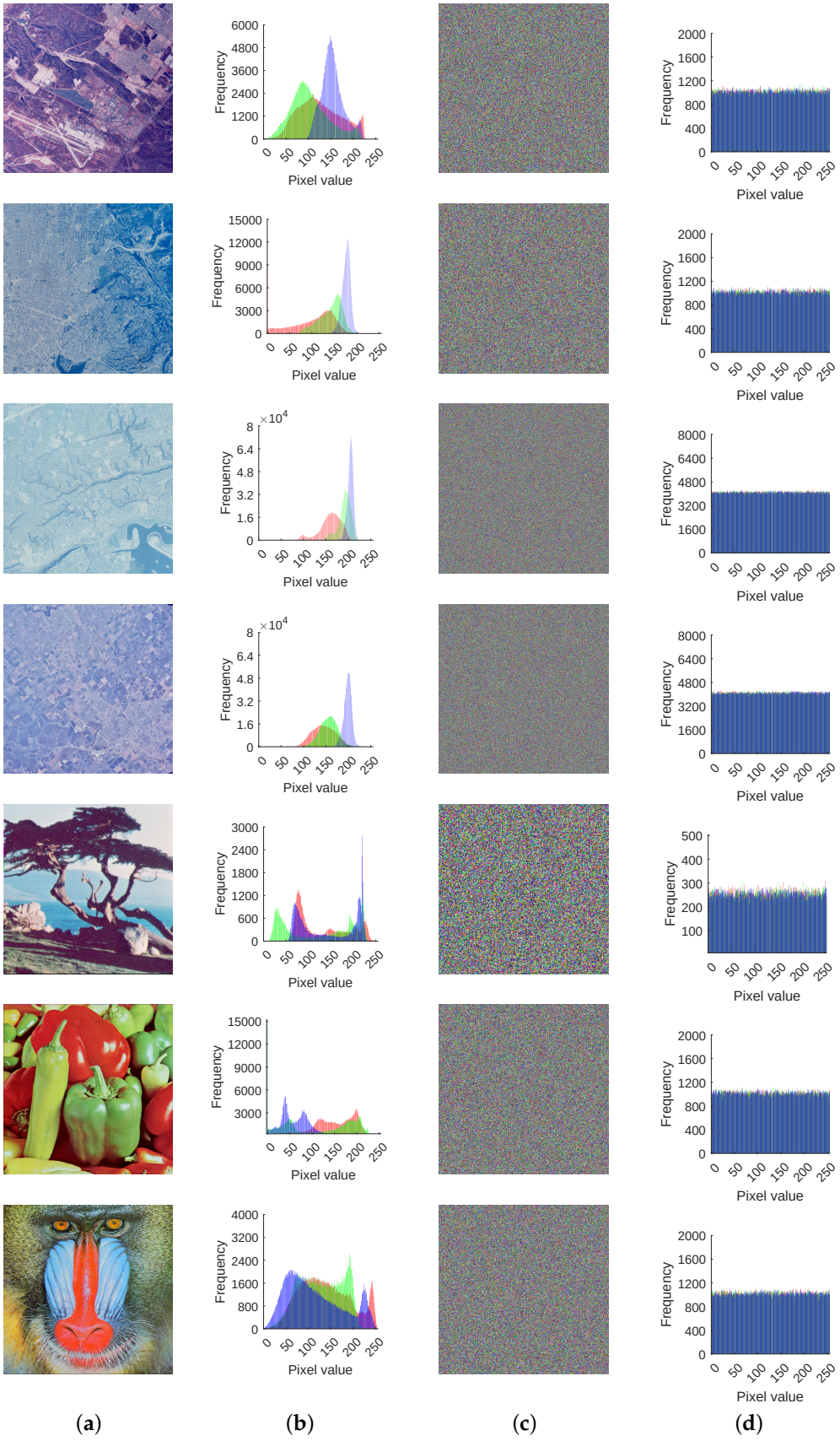

Figure 6. Images prior to and following encryption: (**a**) original images; (**b**) histogram of (**a**); (**c**) encrypted images; (**d**) histogram of (**c**).

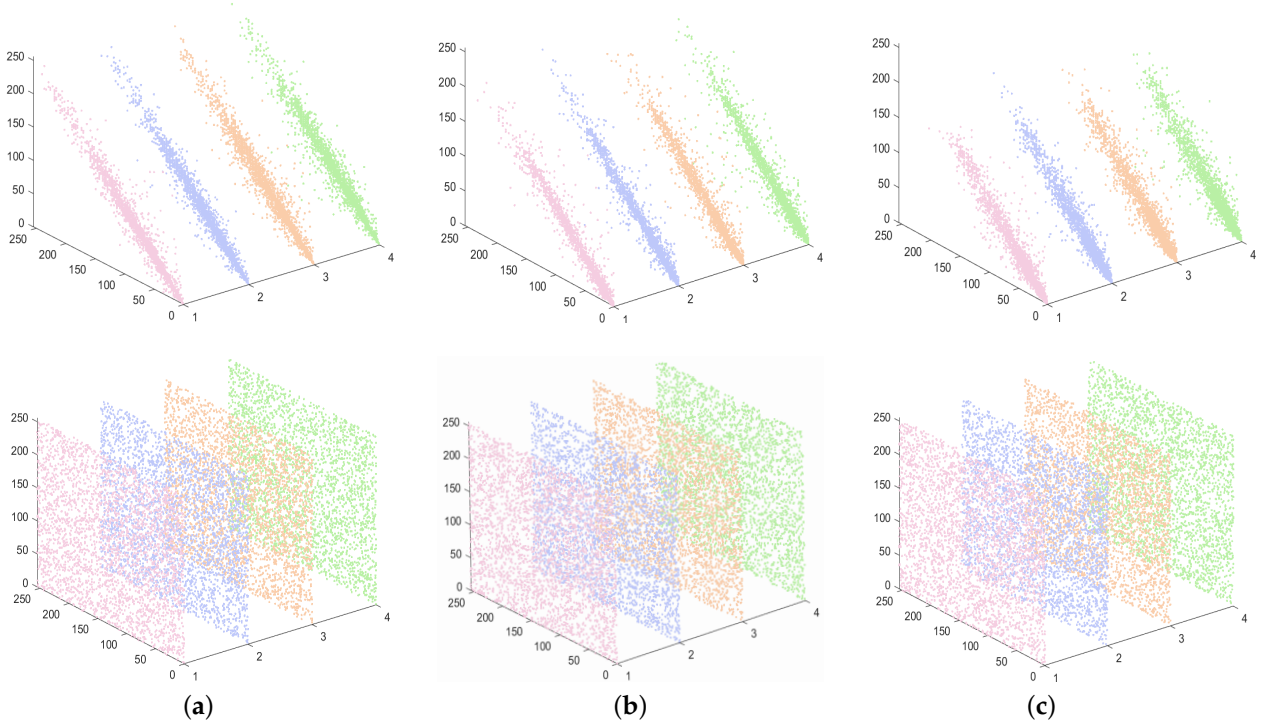

Figure 7. The correlation between horizontal/vertical/diagonal/anti-diagonal pixels of video plaintext and ciphertext images: (**a**) R channel; (**b**) G channel; (**c**) B channel.

Table 4. Contrast results of correlation coefficients of adjacent pixels.

Component	Direction	Original Image	This Paper	Ref. [38]	Ref. [39]	Ref. [40]
R	Horizontal	0.9593	0.0030	−0.0063	0.0076	0.0023
	Vertical	0.9747	−0.0022	−0.0016	0.0017	−0.0130
	Diagonal	0.9507	0.0006	0.0156	0.0110	−0.0061
G	Horizontal	0.9678	−0.0091	−0.0032	−0.0048	−0.0236
	Vertical	0.9720	−0.0129	0.0335	0.0274	0.0308
	Diagonal	0.9526	0.0043	−0.0095	0.0342	−0.0179
B	Horizontal	0.9487	−0.0113	−0.0044	−0.0056	−0.0266
	Vertical	0.9598	−0.0038	−0.0079	0.0150	−0.0057
	Diagonal	0.9331	−0.0164	0.0034	−0.0115	0.0378

4.2.3. Differential Statistical Analysis

In the field of image encryption, NPCR (number of pixel change rate) and UACI (uniform average change intensity) are important metrics to quantify the disparity between two images and can also serve as a metric to evaluate the resistance of encryption algorithms against differential attacks. Usually, an attacker will make minor changes to the plaintext image data and then encrypt the plaintext image before and after the changes separately using the proposed algorithm and derive the relationship between the plaintext image and the ciphertext image by comparison, i.e., the differential attack. To resist the differential attack, it is necessary to make a huge change in the ciphertext image data when a pixel change occurs in the plaintext image. The ideal values of NPCR and UACI are 99.6094% and 33.4635%, respectively. when the results of the algorithm's NPCR and UACI calculations

are closer to the ideal values; this implies that the algorithm exhibits enhanced resistance against differential attacks. The formulas for calculating NPCR and UACI are as follows:

$$\begin{cases} NPCR = \frac{1}{H} \times \frac{1}{W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} D(i,j) \times 100\% \\ UACI = \frac{1}{H} \times \frac{1}{W} \times \sum_{i=1}^{H} \sum_{j=1}^{W} \frac{|v_1(i,j) - v_2(i,j)|}{255} \times 100\% \end{cases} \tag{10}$$

where $H \times W$ is the size of the image, and v_1,v_2 are the ciphertext images before and after changing one pixel of the plaintext image, respectively. D can be defined by the following equation:

$$D = \begin{cases} 0 & if \quad v_1(i,j) = v_2(i,j) \\ 1 & if \quad v_1(i,j) \neq v_2(i,j) \end{cases} \tag{11}$$

Table 5 shows the results of the algorithm calculated according to Equation (10). Using Table 5, we find that both NPCR and UACI are close to their ideal values of 99.6094% and 33.4635%. These results show that even a slight difference in the plaintext image in using the encryption scheme proposed in this paper can lead to results that are not even close to ideal. In conclusion, the encryption scheme presented in this paper demonstrates robust resistance to differential attacks.

Table 5. NPCR and UACI values.

Images	NPCR (%)	UACI (%)
2.1.01	99.6116	33.4181
2.1.03	99.6048	33.4052
2.1.04	99.6212	33.4429
2.1.06	99.6155	33.4488
2.2.03	99.6113	33.4849
2.2.05	99.6058	33.4567
2.2.08	99.6252	33.4905
2.2.11	99.6089	33.4774
4.1.01	99.5972	33.4714
4.1.04	99.6124	33.3961
4.1.06	99.6120	33.4099
4.1.08	99.6143	33.3263
4.2.03	99.6208	33.4181
4.2.07	99.6117	33.5582

4.3. Information Entropy

Information entropy, being a crucial metric in image encryption, signifies the level of uncertainty associated with image information and is usually used to evaluate the degree of randomness in the system. A higher value of information entropy indicates greater uncertainty and reduced visibility of image information, signifying improved encryption performance of the algorithm. Thus, a comparison was conducted between the information entropy of the original and encrypted images, with the experimental results presented in Table 6, and, for the information source m, the information entropy $H(m)$ is provided by the following equation:

$$H(m) = -\sum_{i=1}^{L} p(m_i) \log_2 p(m_i) \tag{12}$$

where L is the total number of symbols $m(i) \in m$ and $p(m_i)$ denotes the probability of the symbols.

Assuming that the source sends 256 symbols and that we can obtain the theoretical value by Equation (12), the closer to 8, the less likely the attacker will decode the cipher image. Table 6 shows the comparison of information entropy of plaintext and ciphertext.

From Table 6, we can see that the experimental results are close to 8, so the proposed algorithm has good information entropy properties.

Table 6. The entropy of the plain and cipher images.

Images	Plain Image	Cipher Image
2.1.01	7.4705	7.9997
2.1.03	6.8709	7.9998
2.1.04	7.0728	7.9997
2.1.06	7.3983	7.9998
2.2.03	6.3301	7.9999
2.2.05	7.4349	7.9999
2.2.08	7.6470	7.9999
2.2.11	6.7947	7.9999
4.1.01	6.8981	7.9990
4.1.04	7.4270	7.9991
4.1.06	7.5371	7.9991
4.1.08	6.8527	7.9989
4.2.03	7.7624	7.9998
4.2.07	7.6698	7.9997

4.4. Key Space Analysis

The key space denotes the collection of all potential keys that can be employed to generate a cryptographic key, and the size of the key space is contingent on the length of the security key. This attribute plays a pivotal role in determining the robustness of a cryptosystem. The image encryption algorithm proposed in this study employs a 2D-SFHM chaotic system, whose key space can be expressed as $S \in \{x, y, a, b, MD5\}$, where x, y, a, b are the key parameter with the precision of 10^{-16} and $MD5$ is the hash value introduced to enhance the key space, which can generate a 128-bit hash value. After calculation, the key space size of this encryption scheme is about $10^{4\times16} \times 2^{128} \approx 2^{340}$ and the key length reaches 340 bits in this paper. Usually, the larger the key space is, the more computational resources and time are required to break the encryption algorithm. Therefore, the key space generated by the encryption algorithm in this paper is large enough to resist any form of brute force attack. The key space comparison is shown in Table 7.

Table 7. Key space comparison.

This Paper	Ref. [41]	Ref. [42]	Ref. [43]	Ref. [44]
340	166	128	154	224

4.5. Speed Analysis

The running speed of encryption and decryption directly reflects the efficiency of the design scheme. In this section, we have used four sets of images with sizes 64×64, 128×128, 256×256, and 512×512 to test the average running time and rate of the encryption and decryption operations, as shown in Table 8. From Table 8, it can be observed that the proposed encryption algorithm performs well in terms of encryption and decryption time.

Table 8. Execution speed test.

Image Size	64×64	128×128	256×256	512×512
Encryption time(s)	0.02160	0.05621	0.27413	1.01921
Decryption time(s)	0.01854	0.05433	0.25423	0.94582

4.6. Sensitivity Analysis

In this section, the performance metrics of the algorithm are assessed based on the sensitivity to both the encryption key and plaintext. This highlights the critical requirement for high sensitivity in a security algorithm, whereby even a minor alteration in the key or plaintext image information during the encryption or decryption process can significantly affect the outcome of subsequent encryption.

4.6.1. Analysis of Sensitivity to the Key

Key sensitivity is analyzed by analyzing the ciphertext obtained when encrypting the same image using two slightly different keys. In this section, we encrypt the plaintext image by using the original key, which defined as key, and the scrambling key, which is defined as $key + 10^{-14}$, respectively. Then, compare the difference between the encrypted ciphertexts by calculating the NPCR and UACI, where NPCR and UACI are defined as shown in Equation (10). The results are shown in Figures 8 and 9, and we can find that the difference between the two ciphertext images is very large when the scrambling is added to the key, and their NPCR and UACI values are very close to the ideal values of 99.6094% and 33.4635%.

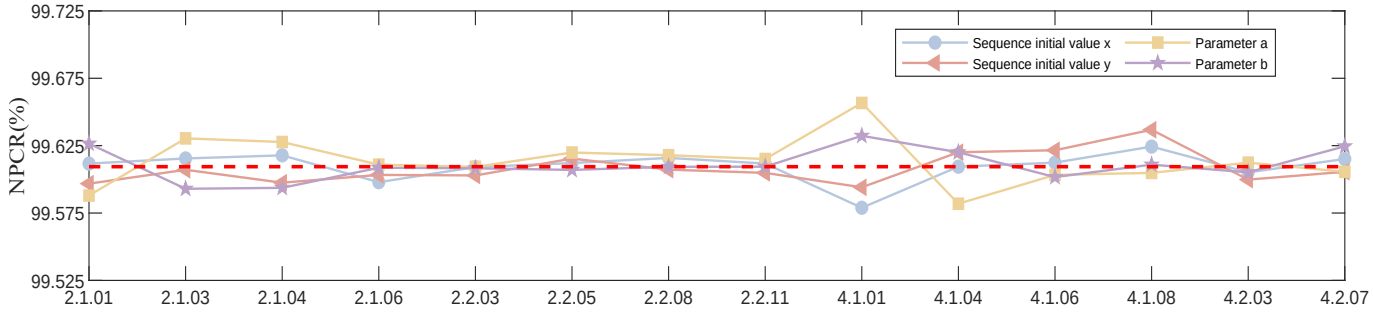

Figure 8. Test values of NPCR after different keys are perturbed.

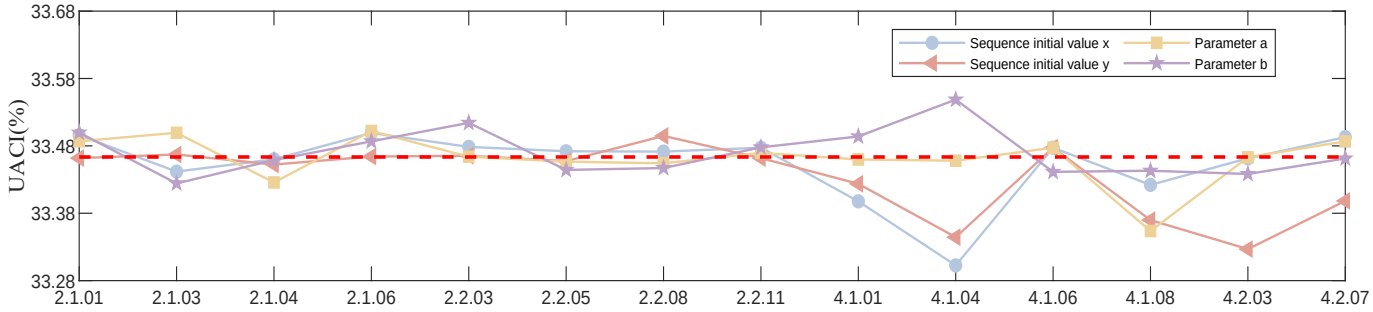

Figure 9. Test values of UACI after different keys are perturbed.

4.6.2. Analysis of Plaintext Sensitivity

Plaintext sensitivity refers to the extent of variation in the resulting ciphertext when the pixels of the plaintext are modified. Insufficient plaintext sensitivity in an algorithm increases vulnerability to attacks as attackers can potentially decrypt the algorithm by analyzing the discrepancies between the plaintext and ciphertext pairs. Therefore, the algorithm's plaintext sensitivity is vital for its resilience against plaintext attacks. In this section, we evaluate the sensitivity of the proposed algorithm to the plaintext image by adding 1 to the pixel value of the plaintext image at (H/3, W/3), (H/3, 2×W/3), (2×H/3, W/3), and (2×H/3, 2×W/3), and the results can be obtained by comparing its NPCR and UACI values. The results are shown in Figures 10 and 11. From the experimental results, it can be seen that the NPCR between the ciphertext and the original ciphertext is very close to the ideal value of 99.6094% and the UACI is also very close to the ideal value of 33.4635% when the change in the pixel values at the selected locations is 1. This observation

demonstrates a significant alteration in the ciphertext image, rendering it infeasible for an attacker to exploit the algorithm by analyzing the discrepancies between ciphertexts. Hence, the algorithm proposed in this study exhibits sufficient resistance against plaintext attacks.

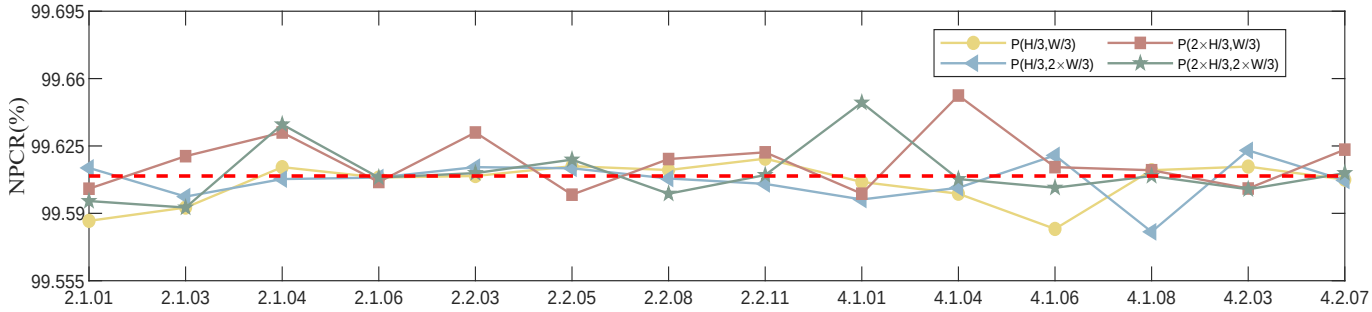

Figure 10. Test values of NPCR after being perturbed at different locations.

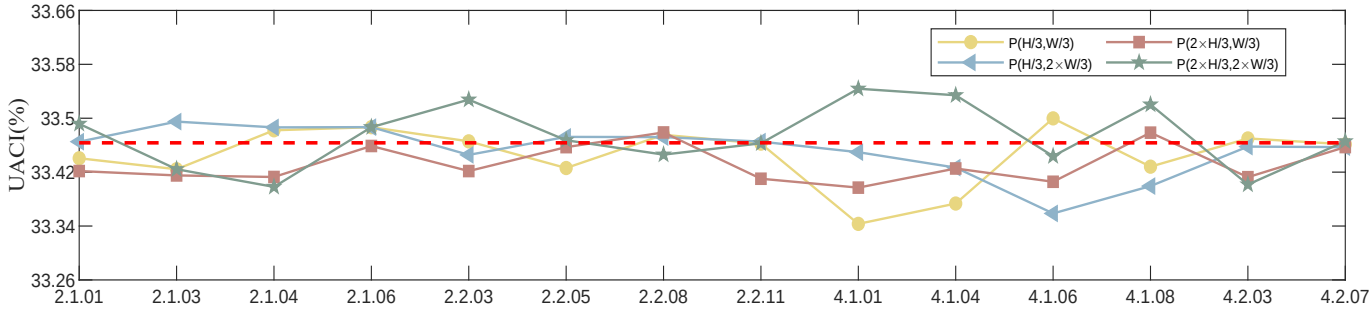

Figure 11. Test values of UACI after being perturbed at different locations.

5. Conclusions

To conclude, in this paper, we have proposed a novel dynamic RNA-encoded color image encryption scheme based on a chain feedback structure. The encryption algorithm employs various encryption techniques, such as chaotic sequences, bit-level permutation, RNA dynamic encoding, RNA dynamic operation rules, and RNA dynamic decoding, to encrypt color images. The proposed algorithm has been evaluated using various experimental results and security analysis, which demonstrate that it provides good encryption performance and effective security against a variety of typical attacks. In the future, we plan to extend our work to improve the efficiency of the encryption algorithm while maintaining its high security. Additionally, we will explore the possibility of extending this algorithm to other domains beyond image encryption, such as video, audio, and other types of data. We believe that the proposed algorithm has significant potential for real-world application and can be used as an effective tool for securely transmitting sensitive data.

Author Contributions: Conceptualization, H.W. and Y.L.; methodology, Y.L.; software, Y.L. and S.K.; validation, S.K. and Z.W.; formal analysis, S.K. and Y.L.; investigation, Z.W., S.K. and Y.H.; resources, H.W. and Y.L.; data curation, Z.W. and S.K.; writing—original draft preparation, H.W., Y.L. and S.K.; writing—review and editing, Y.L., S.K. and H.W.; visualization, Z.W. and S.K.; supervision, H.W.; project administration, H.W.; funding acquisition, H.W. All authors have read and agreed to the published version of the manuscript.

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

Data Availability Statement: Data sharing not applicable to this article as no datasets were generated during the current study.

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

References

1. Luo, Y.; Tang, S.; Liu, J.; Cao, L.; Qiu, S. Image encryption scheme by combining the hyper-chaotic system with quantum coding. *Opt. Lasers Eng.* **2020**, *124*, 105836. [CrossRef]
2. Li, C.; Yang, X. An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos. *Optik* **2022**, *260*, 169042. [CrossRef]
3. Singh, R.K.; Kumar, B.; Shaw, D.K.; Khan, D.A. Level by level image compression-encryption algorithm based on quantum chaos map. *J. King Saud Univ.-Comput. Inf. Sci.* **2021**, *33*, 844–851. [CrossRef]
4. Chai, X.; Wang, Y.; Chen, X.; Gan, Z.; Zhang, Y. TPE-GAN: Thumbnail Preserving Encryption Based on GAN With Key. *IEEE Signal Process. Lett.* **2022**, *29*, 972–976. [CrossRef]
5. Zhao, R.; Zhang, Y.; Wen, W.; Lan, R.; Xiang, Y. E-TPE: Efficient Thumbnail-Preserving Encryption for Privacy Protection in Visual Sensor Networks. *ACM Trans. Sen. Netw.* **2023**. [CrossRef]
6. Zhang, Y.; Zhou, W.; Zhao, R.; Zhang, X.; Cao, X. F-TPE: Flexible Thumbnail-Preserving Encryption Based on Multi-Pixel Sum-Preserving Encryption. *IEEE Trans. Multimed.* **2022**, 1–15. [CrossRef]
7. Zhang, Y.; Zhao, R.; Xiao, X.; Lan, R.; Liu, Z.; Zhang, X. HF-TPE: High-Fidelity Thumbnail- Preserving Encryption. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 947–961. [CrossRef]
8. Zhang, X.; Yan, X. Adaptive Chaotic Image Encryption Algorithm Based on RNA and Pixel Depth. *Electronics* **2021**, *10*, 1770. [CrossRef]
9. Wen, H.; Liu, Z.; Lai, H.; Zhang, C.; Liu, L.; Yang, J.; Lin, Y.; Li, Y.; Liao, Y.; Ma, L.; et al. Secure DNA-Coding Image Optical Communication Using Non-Degenerate Hyperchaos and Dynamic Secret-Key. *Mathematics* **2022**, *10*, 3180. [CrossRef]
10. Zhang, D.; Wen, X.; Yan, C.; Li, T. An image encryption algorithm based on joint RNA-level permutation and substitution. *Multimed. Tools Appl.* **2022**, *82*, 23401–23426. [CrossRef]
11. Wen, H.; Chen, Z.; Zheng, J.; Huang, Y.; Li, S.; Ma, L.; Lin, Y.; Liu, Z.; Li, R.; Liu, L.; et al. Design and Embedded Implementation of Secure Image Encryption Scheme Using DWT and 2D-LASM. *Entropy* **2022**, *24*, 1332. [CrossRef]
12. Araghi, T.K.; Manaf, A.A. An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Gener. Comput. Syst.* **2019**, *101*, 1223–1246. [CrossRef]
13. Lee, S.H. DWT based coding DNA watermarking for DNA copyright protection. *Inf. Sci.* **2014**, *273*, 263–286. [CrossRef]
14. Wang, X.; Liu, C.; Jiang, D. A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT. *Inf. Sci.* **2021**, *574*, 505–527. [CrossRef]
15. Ariatmanto, D.; Ernawan, F. Adaptive scaling factors based on the impact of selected DCT coefficients for image watermarking. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 605–614. [CrossRef]
16. Sisaudia, V.; Vishwakarma, V.P. A secure gray-scale image watermarking technique in fractional DCT domain using zig-zag scrambling. *J. Inf. Secur. Appl.* **2022**, *69*, 103296. [CrossRef]
17. Wei, D.; Jiang, M.; Deng, Y. A secure image encryption algorithm based on hyper-chaotic and bit-level permutation. *Expert Syst. Appl.* **2023**, *213*, 119074. [CrossRef]
18. Shahna, K.U.; Mohamed, A. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. *Appl. Soft Comput.* **2020**, *90*, 106162. [CrossRef]
19. Feng, W.; Zhao, X.; Zhang, J.; Qin, Z.; Zhang, J.; He, Y. Image Encryption Algorithm Based on Plane-Level Image Filtering and Discrete Logarithmic Transform. *Mathematics* **2022**, *10*, 2751. [CrossRef]
20. Wen, H.; Wu, J.; Ma, L.; Liu, Z.; Lin, Y.; Zhou, L.; Jian, H.; Lin, W.; Liu, L.; Zheng, T.; et al. Secure Optical Image Communication Using Double Random Transformation and Memristive Chaos. *IEEE Photonics J.* **2023**, *15*, 1–11. [CrossRef]
21. Xie, H.; Lu, J.; Han, J.; Zhang, Y.; Xiong, F.; Zhao, Z. Fourier coded aperture transform hyperspectral imaging system. *Opt. Lasers Eng.* **2023**, *163*, 107443. [CrossRef]
22. Melman, A.; Evsutin, O. Comparative study of metaheuristic optimization algorithms for image steganography based on discrete Fourier transform domain. *Appl. Soft Comput.* **2023**, *132*, 109847. [CrossRef]
23. Li, C.; Tan, K.; Feng, B.; Lv, J. The Graph Structure of the Generalized Discrete Arnold's Cat Map. *IEEE Trans. Comput.* **2022**, *71*, 364–377. [CrossRef]
24. Li, C.; Feng, B.; Li, S.; Kurths, J.; Chen, G. Dynamic Analysis of Digital Chaotic Maps via State-Mapping Networks. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 2322–2335. [CrossRef]
25. Banerjee, M.; Ghosh, S.; Manfredi, P.; d'Onofrio, A. Spatio-temporal chaos and clustering induced by nonlocal information and vaccine hesitancy in the SIR epidemic model. *Chaos Solitons Fractals* **2023**, *170*, 113339. [CrossRef]
26. Wen, H.; Chen, R.; Yang, J.; Zheng, T.; Wu, J.; Lin, W.; Jian, H.; Lin, Y.; Ma, L.; Liu, Z.; et al. Security analysis of a color image encryption based on bit-level and chaotic map. *Multimed. Tools Appl.* **2023**. [CrossRef]
27. Lu, X.; Xie, E.Y.; Li, C. Periodicity Analysis of Logistic Map over Ring $\mathbb{Z}_{3^n}$. *Int. J. Bifurc. Chaos* **2023**, *33*, 2350063. [CrossRef]
28. Wen, H.; Lin, Y. Cryptanalyzing an image cipher using multiple chaos and DNA operations. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101612. [CrossRef]
29. Chen, G. Pinning Control of Complex Dynamical Networks. *IEEE Trans. Consum. Electron.* **2022**, *68*, 336–343. [CrossRef]
30. Chen, G. Searching for Best Network Topologies with Optimal Synchronizability: A Brief Review. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 573–577. [CrossRef]

31. Yu, F.; Gong, X.; Li, H.; Wang, S. Differential cryptanalysis of image cipher using block-based scrambling and image filtering. *Inf. Sci.* **2021**, *554*, 145–156. [CrossRef]
32. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.* **2014**, *97*, 172–182. [CrossRef]
33. Vikas; Parhi, D.R. Chaos-based optimal path planning of humanoid robot using hybridized regression-gravity search algorithm in static and dynamic terrains. *Appl. Soft Comput.* **2023**, *140*, 110236. [CrossRef]
34. Xiang, Y.; Xiao, D.; Zhang, R.; Liang, J.; Liu, R. Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer. *Inf. Sci.* **2021**, *545*, 188–206. [CrossRef]
35. Mehra, I.; Rajput, S.K.; Nishchal, N.K. Cryptanalysis of an image encryption scheme based on joint transform correlator with amplitude- and phase- truncation approach. *Opt. Lasers Eng.* **2014**, *52*, 167–173. [CrossRef]
36. Hu, Y.; Wu, H.; Zhou, L. Color image encryption base on a 2D hyperchaotic enhanced Henon map and cross diffusion. *Alex. Eng. J.* **2023**, *73*, 385–402. [CrossRef]
37. Lai, Q.; Liu, Y. A cross-channel color image encryption algorithm using two-dimensional hyperchaotic map. *Expert Syst. Appl.* **2023**, *223*, 119923. [CrossRef]
38. Shafique, A.; Shahid, J. Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps. *Eur. Phys. J. Plus* **2018**, *133*, 331. [CrossRef]
39. Yin, Q.; Wang, C. A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850047. [CrossRef]
40. Xu, L.; Li, Z.; Li, J.; Hua, W. A novel bit-level image encryption algorithm based on chaotic maps. *Opt. Lasers Eng.* **2016**, *78*, 17–25. [CrossRef]
41. Liu, L.; Zhang, Q.; Wei, X. A RGB image encryption algorithm based on DNA encoding and chaos map. *Comput. Electr. Eng.* **2012**, *38*, 1240–1248. [CrossRef]
42. Murillo-Escobar, M.; Cruz-Hernández, C.; Abundiz-Pérez, F.; López-Gutiérrez, R.; Campo, O.A.D. A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Process.* **2015**, *109*, 119–131. [CrossRef]
43. Mansouri, A.; Wang, X. A novel block-based image encryption scheme using a new Sine powered chaotic map generator. *Multimed. Tools Appl.* **2021**, *80*, 21955–21978. [CrossRef]
44. Shafique, A.; Ahmed, F. Image Encryption Using Dynamic S-Box Substitution in the Wavelet Domain. *Wirel. Pers. Commun.* **2020**, *115*, 2243–2268. [CrossRef]