*electronics*

MDPI

*Article*

# One-Dimensional Quadratic Chaotic System and Splicing Model for Image Encryption

**Chen Chen [1], Donglin Zhu [2], Xiao Wang [3,*] and Lijun Zeng [1]**

[1] Nanhang Jincheng College, Nanjing 211156, China
[2] College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, China
[3] Xingzhi College, Zhejiang Normal University, Jinhua 321000, China
* Correspondence: tianzhu213@zjnu.cn

**Abstract:** Digital image transmission plays a very significant role in information transmission, so it is very important to protect the security of image transmission. Based on the analysis of existing image encryption algorithms, this article proposes a new digital image encryption algorithm based on the splicing model and 1D secondary chaotic system. Step one is the algorithm of this article divides the plain image into four sub-parts by using quaternary coding, and these four sub-parts can be coded separately. Only by acquiring all the sub-parts at one time can the attacker recover the useful plain image. Therefore, the algorithm has high security. Additionally, the image encryption scheme in this article used a 1D quadratic chaotic system, which makes the key space big enough to resist exhaustive attacks. The experimental data show that the image encryption algorithm has high security and a good encryption effect.

**Keywords:** 1D quadratic chaotic system; image encryption; splicing model; DNA coding



**Citation:** Chen, C.; Zhu, D.; Wang, X.; Zeng, L. One-Dimensional Quadratic Chaotic System and Splicing Model for Image Encryption. *Electronics* **2023**, *12*, 1325. https://doi.org/10.3390/electronics12061325

Academic Editor: Gwanggil Jeon

Received: 13 February 2023
Revised: 1 March 2023
Accepted: 9 March 2023
Published: 10 March 2023



## 1. Introduction

With the development of technologies such as artificial intelligence and 5G and the internet of things, we have entered the times of big data information. However, due to the sharing and openness of computer networks, information security is facing great challenges. Most of the information in the network is carried by images, so it is very necessary to protect information security. Meanwhile, researchers have adopted a series of digital image encryption schemes [1–5]. Some researchers put forward the image encryption algorithm based on DNA computing and chaotic system, which protects its safe transmission of images in the network to some extent [6–14]. Reference [1] put forward an image encryption algorithm based on a one-dimensional composite chaotic mapping system, which is composed of logistic mapping and tent mapping. The algorithm has high complexity and insufficient key space. Reference [2] put forward an image encryption method based on diffusion (JPD) and joint permutation, which determines which pixels will be permuted and diffused by hyperchaotic sequence. Reference [7] put forward an image encryption algorithm based on one-dimensional fractional chaotic mapping, which uses chaotic mapping to design parallel DNA coding to encrypt images. The algorithm has a greater key space. References [15,16] put forward image encryption algorithms based on a logistic chaotic system and a sine mapping system, respectively. Although its scheme is simple, it adopts a low-dimensional logical chaotic system, and the number of parameters is small, which leads to less key space. In addition, the mapping is easy to predict, and the ability to resist exhaustive attacks is poor. The author of reference [17] proposed an encryption algorithm based on quaternary separation of the original image and hyperchaotic system, which has a good anti-attack ability, but the calculation speed is not fast enough, and the key space is not large enough. Reference [18] encrypts the image by generating chaotic sequence and bit cross-diffusion through iterative logical mapping, which has a larger key space. Therefore, the choice of a chaotic system is very significant, which will affect the whole image encryption scheme.

In order to ensure that its key space is exceptionally large and the calculation time is appropriate, the paper uses 1D quadratic chaotic mapping to encrypt digital images. Because 1D quadratic mapping has three adjustable parameters, it will obtain a larger key space, and its calculation speed is faster than that of a high-dimensional chaotic system.

According to different digital image encryption methods, encryption technologies of the image are roughly split into image encryption technology based on matrix transformation, chaos, frequency domain, SCAN language and DNA computing, etc. At present, the most popular encryption technology is based on DNA computing, which has the characteristics of low embodied energy, high concurrency, and high storage density and can meet the space and speed requirements of DNA sequences. Therefore, encryption methods are widely used in the field of information hiding, which is based on DNA computing [8–12]. Reference [8] put forward an encryption algorithm of DNA coding and sequence based on constructing short DNA chains and long DNA chains. Reference [18] put forward a way to modify the pixels of original images by DNA encoding. Reference [9] put forward a novel image encryption algorithm, which is based on an intertwining logistic map and DNA coding. However, these experiments only use DNA bases as operating objects and require harsh laboratory environments and expensive experimental equipment. At present, the laboratory cannot always meet such requirements. Therefore, the image encryption methods which combine DNA computing with a chaotic system were introduced by countless researchers. In recent years, some researchers have abandoned the disadvantages of traditional DNA encryption algorithms using complex biological operations and used the idea of DNA subsequence operations to scramble and spread pixel values. However, there is no perfect encryption algorithm for image information encryption, which has its advantages and disadvantages. Decryption technology is also constantly improving, so digital image encryption needs further research.

According to the existing digital image encryption algorithm, this paper puts forward the following improvement measures:

1. Based on the quaternary coding theory, the plaintext image is edited into four subparts, and each sub-part can be coded by different coding rules, which makes it more difficult for attackers to crack the original image.
2. There are three key parameters of a 1D quadratic chaotic map, which are significantly expanded compared with the traditional 1D chaotic map in parameter space. This algorithm uses a 1D quadratic chaotic map to encrypt the original image. Large key space makes the encryption algorithm more robust.
3. Using DNA sequence XOR operation to diffuse the pixel value of the digital image. In the process of digital image encryption, the mosaic model is introduced, which makes it difficult for image attackers to recover the original image.

## 2. Relevant Knowledge

### *2.1. D Quadratic Chaotic Map*

The general 1D quadratic chaotic formula is defined as follows $f(x) = mx^2 + nx + k$ when $m \neq 0$ and

$$k = \frac{2a - a^2 + n^2 - 2n}{4m} \tag{1}$$

where $a \in (3.5699, 4]$ this map will be chaotic. Equation (1) can be solved in reverse, and its solution is:

$$\begin{cases} a_1 = 1 - \sqrt{(n-1)^2 - 4mk} \\ a_2 = 1 + \sqrt{(n-1)^2 - 4mk} \end{cases} \tag{2}$$

For $a_2$, we should make:

$$3.5699 < a_2 \leq 4 \tag{3}$$

By Equation (3), can obtain:

$$6.6 < (n-1)^2 - 4mk \leq 9 \tag{4}$$

If $(n-1)^2 - 4mk = 9$, map $p$ will be full. $p(x) = mx^2 + nx + k$ is chaotic when condition (4) holds; the 1D quadratic function is chaotic because it is topologically conjugate with logical chaotic mapping [19]. The 1D quadratic function is chaotic because it is topologically conjugate with logical chaotic mapping [19]. The values of three adjustable parameters $k$, $n$ and $m$ of a 1D quadratic chaotic map need to meet the limitations of Equation (4). In the implementation of the encryption algorithm, we usually determine the values of $n$ and $k$ at random first and then determine the value range of the third parameter, $m$, by Formula (4).

Generally, the low-dimensional chaotic map having a lesser key space will lead to difficulty in resisting exhaustive attacks, while 1D quadratic map contains three adjustable parameters, so the encryption algorithm using the 1D quadratic map has a larger key space.

### *2.2. The Splicing Model*

The splicing model was proposed by Tom Head [20]. The basic theory of splicing model details as below:

Suppose there is an abstract alphabet M and two strings $x = x_1k_1k_2x_2$, $y = y_1k_3k_4y_2$, which is composed of symbols of M. The primary splicing operation refers to the conversion of ($x_1k_1k_2x_2$,$y_1k_3k_4y_2$) to ($x_1k_1k_4y_2$,$y_1k_3k_2x_2$) under the premise of rule $r = k_1\#k_2\$k_3\#k_4$. Figure 1 shows the conversion process.

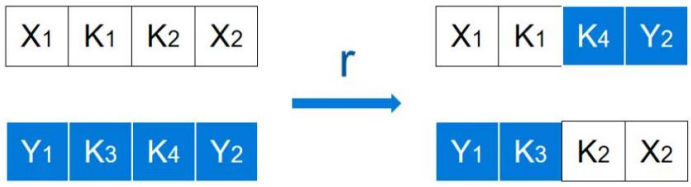



**Figure 1.** The splicing operation.

### *2.3. DNA Computing*

#### 2.3.1. DNA Encoding and Decoding

In the realm of number theory, a positive integer $W$ can be replaced by $H$ integers smaller than it. Defined as follows:

$$\begin{cases} m_1 = W \bmod h; \\ m_2 = (W/h) \bmod h; \\ m_3 = (W/h^2) \bmod h; \\ \cdots \\ m_N = (W/h^{H-1}) \bmod h \end{cases} \tag{5}$$

where h is a positive integer smaller than $W$. These performed calculations are reversible, and the value of $W$ can be found according to Equation (6).

$$W = ((((W/h^H) \times h + m_H) \times h + m_{H-1}) \ldots) \times h + m_1 \tag{6}$$

We divide the plaintext image into four sub-parts by using the quaternary principle; each sub-part is coded separately, and each sub-part is transformed independently on the internet, so the encrypted image of no sub-part is incomplete. Therefore, the information interceptor cannot obtain the original image without any DNA sequence matrix, which increases the difficulty for attackers to crack the original image information and improves the security of the original image information.

For example, let us assume that the first $W$ of the original image, according to Formula (6), is 125, and we choose $h = 4$. In this way, after four modular operations, the value of $W$ is zero. Four position integers $m_1 = 1$, $m_2 = 3$, $m_3 = 3$, $m_4 = 1$ are the results of expression (5), so the value of each sub-section is $m_1, m_2, m_3, m_4$ individually, and the value of $W$ can be found in reverse according to Formula (6) that $W = 125 = (((0 \times 4 + 1) \times 4 + 3) \times 4 + 3) \times 4 + 1$.

Through the calculation of Formula (5), a grayscale image can get four sub-segments with pixel values of 0, 1, 2 and 3. These four sub-fragments can be expressed by four nucleic acid bases, which are adenine, cytosine, guanine, and thymine, respectively. Among them, adenine is represented by A, cytosine by C, guanine by G and thymine by T. In this paper, Table 1 provides 24 coding schemes. Therefore, by using quaternary and DNA coding, the plaintext image can be divided into four sub-parts, and the grayscale image can be turned into four DNA sequence matrices. These four DNA sequence matrices are got by DNA coding using DNA coding rules. Therefore, using the quaternary image encryption method changes the statistical characteristic of the plain image information.

**Table 1.** Maping rules.

| | **0** | **1** | **2** | **3** |
|---|---|---|---|---|
| (1) | C | G | T | A |
| (2) | C | T | G | A |
| (3) | G | C | T | A |
| (4) | G | T | C | A |
| (5) | T | G | C | A |
| (6) | T | C | G | A |
| (7) | A | G | T | C |
| (8) | T | G | A | C |
| (9) | G | T | A | C |
| (10) | G | A | T | C |
| (11) | T | A | G | C |
| (12) | A | T | G | C |
| (13) | C | T | A | G |
| (14) | C | A | T | G |
| (15) | T | A | C | G |
| (16) | A | C | T | G |
| (17) | A | T | C | G |
| (18) | T | C | A | G |
| (19) | G | A | C | T |
| (20) | G | C | A | T |
| (21) | C | G | A | T |
| (22) | C | A | G | T |
| (23) | A | C | G | T |
| (24) | A | G | C | T |

Figure 2 shows the DNA coding. The DNA coding process is as follows:

A sub-image with a size of $5 \times 5$ is obtained from the pixel values of the plaintext image from (208.1) to (212.5).

The second step is to perform four modulo-4 operations on the pixel values, respectively, with the result of the first operation as the pixel value of the first sub-image, the result of the second operation as the pixel value of the second sub-image, and so on until all four sub-images are generated. Finally, according to the coding method, the four sub-image matrices are coded to obtain four DNA sequence matrices. Similarly, the gray values of other parts of the original image can be coded in the same way [17].

In the process of encryption, four DNA sequence matrices are encoded by different rules, so in the process of decoding, four DNA matrices should be decoded by specific rules. Therefore, in order to obtain the original image information, the attacker needs to have four matrix sequences at the same time, all of which are indispensable.

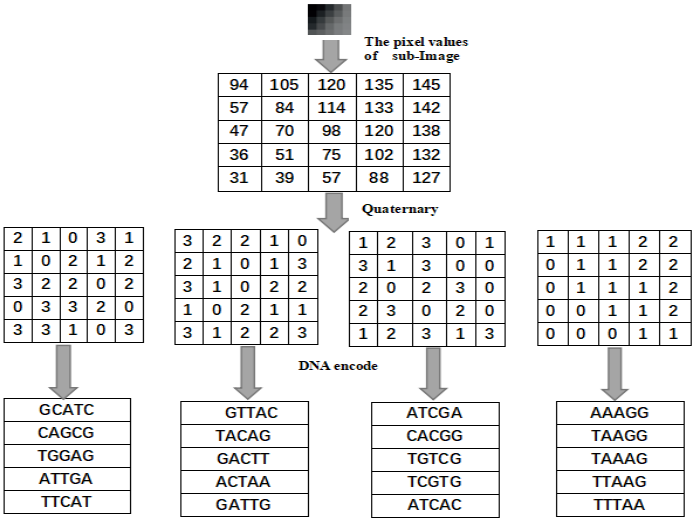



**Figure 2.** DNA encoding.

#### 2.3.2. XOR Operation for DNA Sequence

Traditional digital calculation methods cannot meet the requirements of calculation. Researchers have put forward some biological calculation methods, such as DNA sequence XOR operation, DNA sequence subtraction operation, and DNA sequence addition operation. The exclusive-or operation of DNA sequence is adopted, which is put forward on the basis of traditional modulo-two operation. In Table 2, the operation rules of DNA sequence XOR operation are listed.

**Table 2.** XOR rules.

| XOR | G | T | C | A |
|---|---|---|---|---|
| G | C | A | G | T |
| C | G | T | C | A |
| T | A | C | T | G |
| A | T | G | A | C |

## 3. Image Encryption Scheme

There are three stages in the encryption process: (1) transforming a plaintext image into four DNA sequence matrices; (2) generating a 1D quadratic chaotic sequence and diffusing four matrix pixel values through DNA XOR operation; and (3) a mosaic model is introduced and the four matrices are combined into an image matrix.

### *3.1. The Basic Theory Introduction*

This subsection will introduce the concrete flow of the image encryption scheme based on a 1D quadratic chaotic system and splicing model. First of all, the plain image is encoded into four sub-regions with pixel values of 0, 1, 2, and 3 by using quaternary. Then, the replaced four sub-images are coded into four DNA sequence matrices by DNA coding rules. During the second step, we use the XOR operation of DNA sequences and chaotic sequences produced by the 1D secondary chaotic system to diffuse pixel values. Ultimately, the pixel values are diffused again through the splicing model, these matrices are combined into one image matrix by using the quaternary system, and in the final stages of the image encryption scheme, the encrypted digital holograph is obtained. Figure 3 displays the process and steps of the encryption scheme described above.

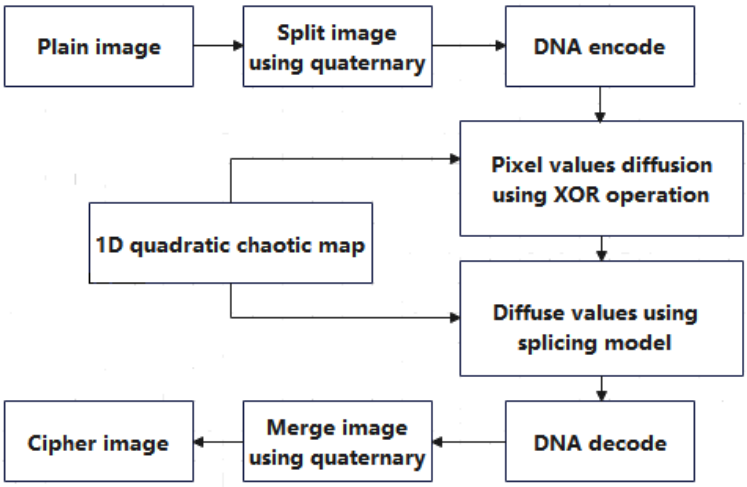



**Figure 3.** Encryption Process.

### *3.2. The Generation of Secret Key*

By the following operations, the key can be obtained:

1. Read the original image M, which size is M × H.
2. The statistical data can be obtained by the following calculation:

$$p = 10 \times \sum_{i=1}^{M} \sum_{j=1}^{H} a_{ij}/MH \bmod 1 \tag{7}$$

3. Set $k = -9/8, n = 1$, and assign values to four parameters $m_1$, $m_2$, $m_3$, and $m_4$. Randomly select the parameters $m_1$, $m_2$, and $m_3$ in the chaotic region, and $m_4 = (m_1 + m_2 + m_3 + m_4')/4$ in which $m_4'$ is randomly picked out in the chaotic region.
4. Additionally, four chaotic sequences are generated $\{x_i\}$, $\{y_i\}$, $\{s_i\}$, and $\{t_i\}$, according to

$$x_{i+1} = f(x_i) = m{x_i}^2 + x_i - 9/8 \tag{8}$$

through using four initial conditions and four sets of parameters $x_0 + p/10$, $y_0 + p/10$, $s_0 + p/10$, and $(x_0 + y_0 + s_0 + t_0)/4 + p/10$, where $x_0$, $y_0$, $s_0$, and $t_0$ all these parameters are randomly selected in the chaotic region.

We selected the parameters $m_1$, $m_2$, $m_3$, and $m_4'$, initial keys $x_0$, $y_0$, $s_0$, and $t_0$ as the secret keys.

### *3.3. Encryption Process*

From Figure 3 above, the specific encryption algorithm process is as follows:

1. Divide the plain image M(m, h) into four sub-images according to the operation Formula (5), and convert them into four sub-matrices $HA, HB, HC, HD$ of size (m, h).
2. According to the coding rules of DNA sequence rules (2), (8), (13), and (19) in Table 1, encode the matrices $HA, HB, HC, HD$ into four DNA sequence matrices $FA, FB, FC, FD$, respectively.
3. Generate four chaotic sequences $\{x_i\}$, $\{y_i\}$, $\{s_i\}$, and $\{t_i\}$, which are the consequences of the 1D quadratic chaotic system under the condition that initial values are $x_0 + p/10$, $y_0 + p/10$, $s_0 + p/10$, and $(x_0 + y_0 + s_0 + t_0)/4 + p/10$.
4. Scrambling the DNA sequence matrices $FA, FB, FC, FD$ is based on the following formula:

$$\begin{aligned} FA(v,k) &= FA(fx(v), fy(k)); \\ FB(v,k) &= FB(fy(v), fz(k)); \\ FC(v,k) &= FC(fz(v), fq(k)); \\ FD(v,k) &= FD(fq(v), fx(k)); \end{aligned} \tag{9}$$

In which $v = 1, 2, \ldots m$, $k = 1, 2, \ldots h$, $FA(v,k)$, $FB(v,k)$, $FC(v,k)$, and $FD(v,k)$ are DNA sequence matrices. The values at the $(v,k)$ positions of $FA, FB, FC, FD$ can be scrambled to obtain a new DNA sequence matrix $NA, NB, NC, ND$.

5. Diffuse the pixel values via chaotic sequences and DNA sequence XOR operation. In addition, we obtain $SA, SB, SC, SD$, which are the DNA sequence matrices.
6. Taking a column of DNA sequence matrix $SA, SB, SC, SD$ as a subsequence, four one-dimensional arrays $QA, QB, QC, QD$ can be obtained, and then the arrays $QA, QB, QC, QD$ are scrambled by using the idea of the splicing model, following these steps:

   If $x(v) + y(v) < 1$, implement the following formula:

$$QA\{v\} \leftrightarrow QB\{v\} \tag{10}$$

   If $z(v) + q(v) < 1$, implement the following formula:

$$QC\{v\} \leftrightarrow QD\{v\} \tag{11}$$

   The value range of $v$ is an integer from 1 to m; the value of k is an integer from 1 to $n$.
7. Decoding the DNA sequence matrices $QA, QB, QC, QD$ according to the second DNA decoding rule (6), (11), (18), and (24) in Table 1 can obtain four matrices $OA, OB, OC, OD$.
8. The matrices of these values are reorganized using Equation (6). Lastly, we got the encrypted digital holograph.

The procedure of decrypt image is the reserve order of encrypt image. In the other words, the encrypted image is complemented as the contrary operations of encryption algorithm, and the only change is that the secret image is used in Step 2 among the decryption algorithm.

## 4. Experiment and Analysis

### *4.1. Exhaustive Attacks*

#### 4.1.1. Analysis of Key Space

It is very significant for the robustness of the image encryption scheme that the capacity of key space. If the capacity of the key space is small, it cannot resist the exhaustive attack. The key space represents the total number of selectable keys in the image password. In the image encryption algorithm, eight adjustable parameters, including the parameters $m_1, m_2, m_3, m_4'$ and initial key $x_0, y_0, s_0, t_0$ are chosen as secret keys. Presume that the maximum calculation accuracy is $10^{-x}$. According to the value ranges of the eight adjustable parameters, the image encryption algorithm's key space is calculated as follows $(10^{x-1} \times 0.53)^4 \times (10^{x-1} \times 0.85)^4 = 10^{8x-10} \times 4.12$. If the operational precision $x = 14$, the capacity of the key space is $4.12 \times 10^{102} \approx 2^{340}$. The calculation results turn out that the key space of the scheme is big enough to effectively resist exhaustive attacks. In Table 3, the key space size of our scheme is compared with that of other documents.

**Table 3.** Key space.

| | **Our Method** | **In Ref. [1]** | **In Ref. [17]** | **In Ref. [19]** | **In Ref. [21]** |
|---|---|---|---|---|---|
| Key space | $2^{340}$ | $2^{209}$ | $2^{100}$ | $2^{340}$ | $2^{261}$ |

#### 4.1.2. Key Sensitivity

Obviously, the encryption method using a 1D quadratic chaotic system put forward in the dissertation is sensitive to all initial keys, under the condition that we cannot obtain the plain image result from a small modification to input conditions. Figure 4 demonstrates the conclusions of the key sensitivity test, and decrypted digital holography under only $10^{-14}$ inappreciable difference in its secret keys $m_1, m_2, m_3, m_4'$, $s_0$, $t_0 x_0$, and $y_0$, respectively.

We can sum up that the original image information can be extracted only if the secret keys are consistent. The decrypted digital holograph cannot reflect the true information of the plaintext image if any small change in the primary key values. Therefore, our scheme has a greater level of security and can withstand exhaustive attack efficiency.

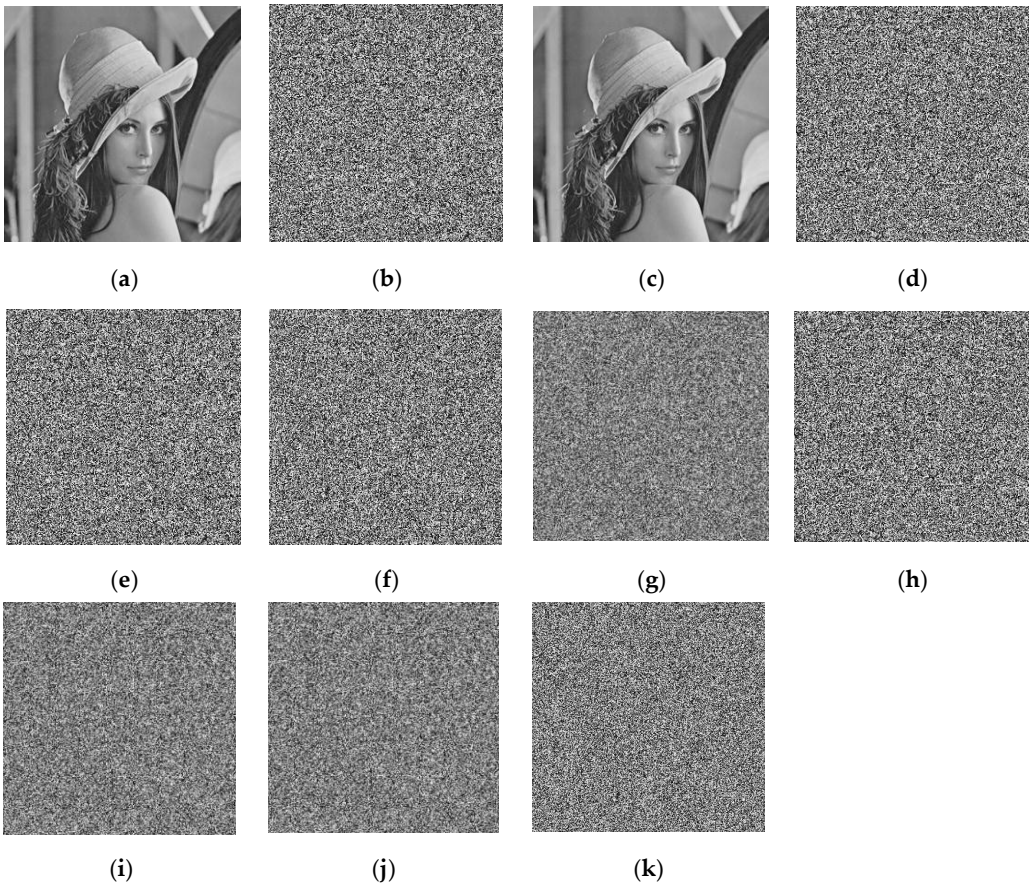
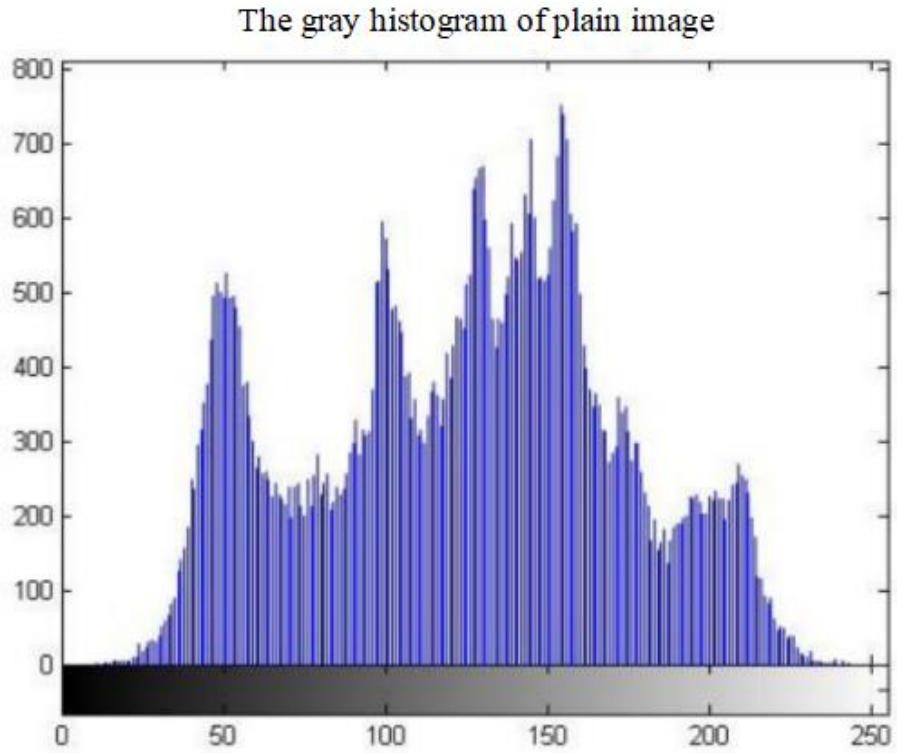



**Figure 4.** (**a**) "Lena" image; (**b**) cipher image (initial encryption key); (**c**) decrypted image (initial encryption key); (**d**) $m_1 + 10^{-14}$; (**e**) $m_2 + 10^{-14}$; (**f**) $m_3 + 10^{-14}$; (**g**) $m'_4 + 10^{-14}$; (**h**) $x_0 + 10^{-14}$; (**i**) $y_0 + 10^{-14}$; (**j**) $s_0 + 10^{-14}$; (**k**) $t_0 + 10^{-14}$. Key sensitivity test: (**d**–**k**) Decrypted image with the wrong key.

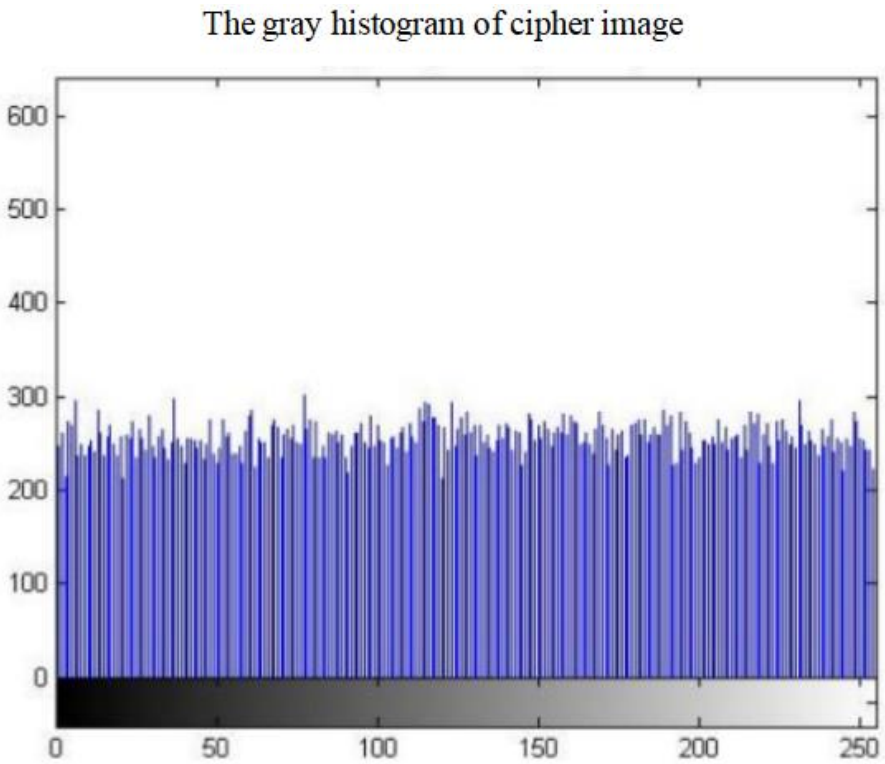
### *4.2. Statistical Attacks*

#### 4.2.1. Gray Histogram

A gray histogram describes each pixel value's frequency in a gray image. Typically, original image pixel values are concentrated on some specific gray values, and encrypted pixel values of the image are evenly distributed on all gray values. The gray histogram of the original image and encrypted digital holograph are demonstrated in Figure 5. From the figure, the distribution of pixel values in the original image is uneven, mainly concentrated on several gray values. However, the pixel values of the encrypted digital holograph are relatively evenly distributed on all gray values. The image encryption system has influenced and changed the distribution of pixel values. The algorithm with a high sense of resisting statistical attacks, which ensures the security of images in the process of transmission.




(**a**) The gray histogram (original image)




(**b**) The gray histogram (encrypted holograph)

**Figure 5.** Gray histogram analysis.

4.2.2. Correlation Coefficient Analysis

The quality of scrambling and diffusion of the image encryption system can be expressed by calculating the relationship between adjacent pixels of the encrypted digital holograph. The greater the degree of encryption scrambling and diffusion, the smaller the correlation coefficient of the neighboring pixels of the encrypted digital holograph, indicating that the relationship of the adjacent pixels of the encrypted digital holograph is weaker. If the calculated values of neighboring pixels in the original image show a linear distribution, the correlation between neighboring pixels will be strong. The distribution of neighboring pixel values of the encrypted image should be irregular, and the correlation between neighboring pixels should be weak. When the correlation coefficient of the encrypted digital holograph is close to zero, it shows that the encryption scheme has good robustness.

The correlation coefficient $r_{st}$ of neighboring pixels of the image may be calculated by the subsequent formula.

$$P(s) = \frac{1}{H}\sum_{k=1}^{H} s_k \tag{12}$$

$$Q(s) = \frac{1}{H}\sum_{k=1}^{H} (s_k - E(s))^2 \tag{13}$$

$$\mathrm{cov}(s,t) = \frac{1}{H}\sum_{k=1}^{H} (s_k - E(s))(t_k - E(t)) \tag{14}$$

$$r_{st} = \frac{\mathrm{cov}(s,t)}{\sqrt{Q(s) \times Q(t)}} \tag{15}$$

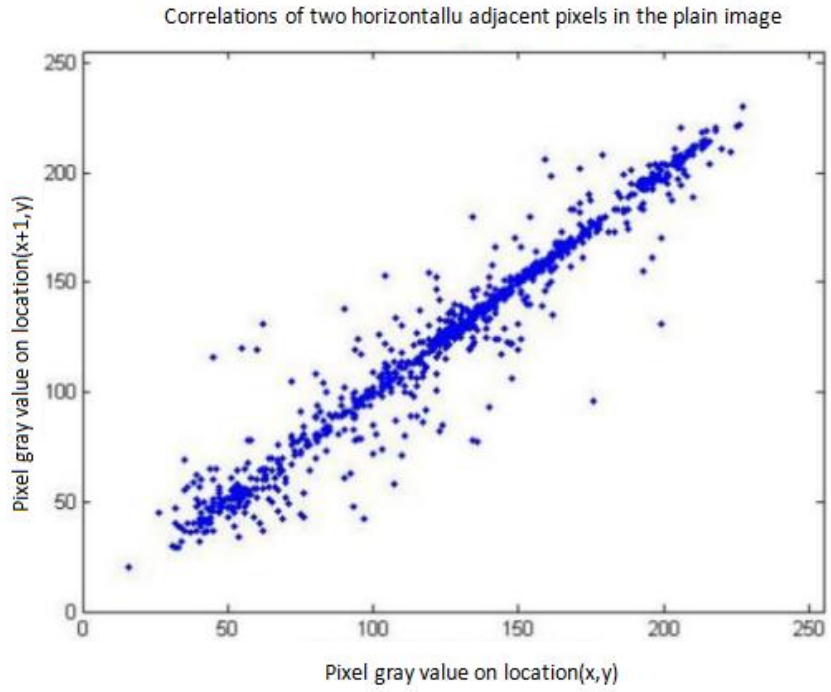
The pixel values of two adjacent pixels in the image are denoted by $s$ and $t$, respectively, and $\mathrm{cov}(s,t)$ is covariance, $P(s)$ is mean, $Q(s)$ is variance.

First, 1000 pairs of adjacent pixels were selected from the original image, and the correlation was calculated in horizontal, vertical, and diagonal directions. Similarly, 1000 pairs of adjacent pixels were selected in the same position in the encrypted image, and the correlation was calculated in horizontal, vertical, and diagonal directions again. Figure 6 correlation coefficient analysis demonstrates the relationship between the two horizontally adjacent pixels in the original image and in the encrypted digital holograph is very different. From Figure 6a, the pertinence of two horizontally adjacent pixels is strong. From Figure 6b, the pertinence of two horizontally adjacent pixels is weak.

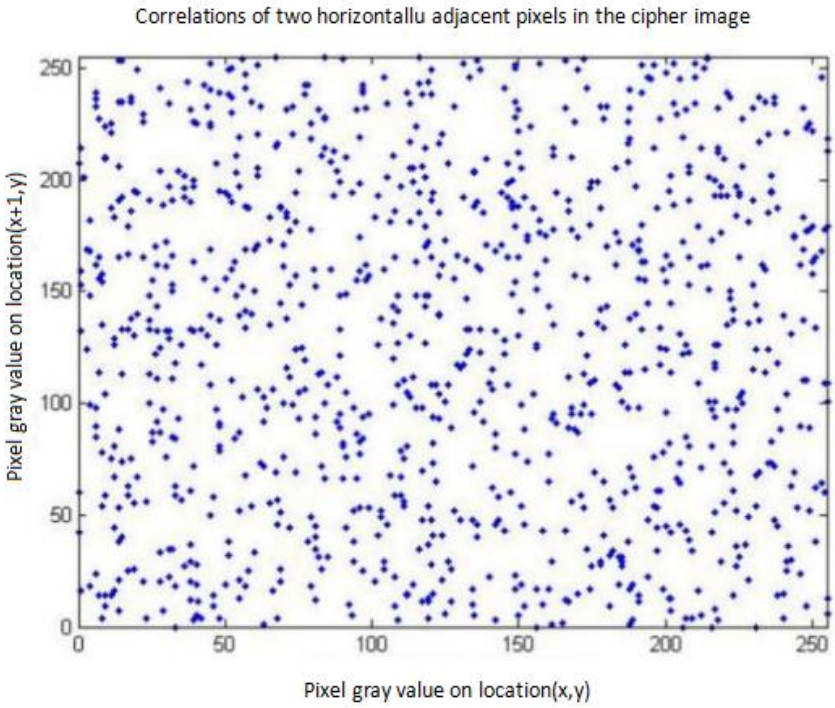
From Table 4 below, it can be concluded that the correlation coefficient between two neighboring pixels of the encrypted image with the original image of "lenna.bmp" is close to 0, and the relationship between neighboring pixels of the image is weak. By comparing the correlation between neighboring pixels of the original image and the encrypted image, the following conclusions can be drawn. In the encryption algorithm, a 1D quadratic chaotic system was used to generate the key and scramble the image, and the mosaic model was introduced to participate in scrambling the image. The correlation between adjacent pixel values of the scrambled image was very low. It showed that the encryption algorithm can effectively resist statistical attacks.

**Table 4.** Correlations coefficients.

| Direction | Lenna | Cipher Image | In Ref. [1] | In Ref. [5] | In Ref. [13] | In Ref. [17] |
|---|---|---|---|---|---|---|
| Horizontal | 0.9277 | 0.0015 | −0.0062 | −0.0020 | −0.0119 | 0.0015 |
| Vertical | 0.9168 | −0.0021 | −0.0001 | −0.0065 | −0.0087 | 0.0018 |
| Diagonal | 0.8871 | −0.0020 | 0.0018 | 0.0087 | −0.0045 | 0.0018 |




(**a**) lenna.bmp




(**b**) Cipher image

**Figure 6.** Correlation coefficient analysis.

### *4.3. Differential Attacks*

The calculation results of the following formula can measure the ability of the encryption algorithm to resist differential cryptanalysis. The change rate of image pixel number (the number of pixels change rate, NPCR) is calculated by the Formula (16), and the even average change intensity of the image (the unified average changing intensity, UACI) is calculated by the Formula (17). The magnitude of these values reflects the ability of the

encryption algorithm to resist differential cryptanalysis. The larger these two values are, the more sensitive the image encryption algorithm is to small changes in gray images.

$$NPCR = \frac{\sum_{s=1}^{H}\sum_{t=1}^{U} C(s,t)}{H \times U} \times 100\% \tag{16}$$

$$UACI = \frac{\sum_{s=1}^{H}\sum_{t=1}^{U} |T_1(s,t) - T_2(s,t)|}{H \times U \times 255} \times 100\% \tag{17}$$

where $H, U$ are the size of cipher image, $T_1(s,t)$ represents the pixel value of one ciphertext image at (*s*,*t*) position, and $T_2(s,t)$ represents the pixel value of another ciphertext image at the same position. $C(s,t)$ is determined as

$$C(s,t) = \begin{cases} 0, & if \quad T_1(s,t) = T_2(s,t); \\ 1, & if \quad T_1(s,t) \neq T_2(s,t); \end{cases} \tag{18}$$

NPCR and UACI analysis of the 256 × 256 Lena image and Baboon image were carried out by existing methods. The values in Table 5 show the approximate theoretical values. It can be concluded that the image encryption algorithm based on the 1D quadratic chaotic system and splicing model excellent in resisting differential cryptanalysis.

**Table 5.** UACI and NPCR of our innovate algorithm and other algorithms.

| | **UACI** | **NPCR** |
|---|---|---|
| Lena | 33.4685% | 99.6092% |
| Baboon | 33.4687% | 99.6089% |
| In Ref. [1] (Lena) | 33.48% | 99.61% |
| In Ref. [5] (Lena) | 33.4477% | 99.6063% |
| In Ref. [14] (Lena) | 33.4645% | 99.6096% |
| In Ref. [17] (Lena) | 33.505% | 99.571% |
| In Ref. [21] (Lena) | 34.61% | 99.65% |

### *4.4. Information Entropy*

In information theory, information entropy refers to the average amount of information received, and it can also represent the unpredictability and uncertainty of image information. Information entropy is also an index to measure the quality of the image encryption scheme. If the information entropy is close to 8, it indicates that the image encryption algorithm is excellent. If the entropy of an image encryption algorithm is far less than 8, the encryption scheme has certain security problems. The information entropy of an encrypted digital hologram can be calculated according to the Formula (19).

$$P(X) = -\sum_{i=0}^{m} Q(x_i) \log_2 Q(x_i) \tag{19}$$

$x_i$ is the value of the ith position of the grayscale image, the $Q(x_i)$ is the frequency of $x_i$'s appearance, and m is the size of the grayscale [22]. The following Table 6 shows the information entropy values of the encrypted digital holograph in this thesis and those of encrypted images under other algorithms.

**Table 6.** The entropy analysis.

| Images | In Ref. [1] | In Ref. [8] | In Ref. [17] | In Ref. [21] | Our Method |
|---|---|---|---|---|---|
| Lena | 7.9978 | 7.9971 | 7.9971 | 7.9975 | 7.9994 |
| Baboon | 7.9974 | 7.9973 | / | / | 7.9991 |

By comparing the values in Table 6, indicated that the encryption algorithm proposed in this thesis is very competitive. According to our encryption algorithm, the information entropy of encrypted digital holography is 7.9994 and 7.9991, respectively, which shows that the algorithm is excellent because the value is infinite and close to the theoretical value of 8.

### *4.5. Encryption Speed Test*

In the proposed algorithm, the plaintext image is divided into four matrices, which can be encrypted at the same time, and four cycles are parallel, so the total number of cycles is $1/4(M+N)$, and this algorithm's time complexity is chiefly expressed as $O(1/4(M+N))$. The number of cycles of the traditional image encryption algorithm with a single pixel as the processing unit is equal to the number of pixels, and the number of cycles is $(M \times N)$. Therefore, the time complexity of this kind of encryption algorithm is $O(M \times N)$. This algorithm significantly improves the encryption speed compared with the encryption algorithm in references. In this thesis, the experimental diagram Lena was decrypted in the experimental environment, and its running time is shown in Table 7. The actual running efficiency of the encryption algorithm was influenced by many factors, such as running environment and programming skills, so the specific running time of the algorithm was not compared, but the time complexity of the algorithm was compared.

**Table 7.** Encryption speed test.

| | In Ref. [2] | In Ref. [14] | Our Method |
|---|---|---|---|
| Time complexity | $O(6N^2)$ | $O(M \times N)$ | $O(1/4(M+N))$ |

## 5. Conclusions

This article presents the digital image encryption system based on a 1D quadratic chaotic system and splicing model. Firstly, the plaintext image was divided into four sub-parts by using the quaternary principle, and each sub-part was coded separately. If an attacker wants to obtain the original image, he must have all the sub-parts at the same time, which increases the difficulty for the attacker to crack the image. In addition, the encryption system encrypted the image using 1D quadratic chaotic mapping, which not only increased the key space of the algorithm but also improved the randomness. Finally, the mosaic model was introduced in the process of digital image encryption to ensure the security of the algorithm. Security analysis and experimental results show that the encryption scheme is not only highly secure, but also resistant to various attacks from the outside world, for instance, statistical attacks, exhaustive attacks, and score-checking attacks and has good robustness.

**Author Contributions:** Data curation, formal analysis, C.C.; software, validation, C.C. and L.Z.; supervision, D.Z.; writing—review and editing, C.C. and X.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported in part by the National Natural Science Foundation of China under Grant numbers 62272418 and 62002046.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Dataset used in this study may be available on demand.

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

## References


1. Zhu, S.; Deng, X.; Zhang, W. A New One-Dimensional Compound Chaotic System and Its Application in High-Speed Image Encryption. *Appl. Sci.* **2021**, *11*, 11206. [CrossRef]
2. Li, T.Y.; Shi, J.Y.; Zhang, D.H. Color image encryption based on joint permutation and diffusion. *J. Electron. Imaging* **2021**, *30*, 013008. Available online: https://www.spiedigitallibrary.org/journals/journal-of-electronic-imaging/volume-30/issue-1/013008/Color-image-encryption-based-on-joint-permutation-and-diffusion/10.1117/1.JEI.30.1.013008.full?SSO=1 (accessed on 12 January 2022). [CrossRef]
3. Zhu, D.; Huang, Z.; Liao, S. Improved Bare Bones Particle Swarm Optimiztion for DNA Squence Dsign. *IEEE Trans. NanoBiosci.* **2022**, *35*. Available online: https://ieeexplore.ieee.org/document/9943286 (accessed on 9 December 2022).
4. Li, Z.; Peng, C.; Tan, W.; Li, L. A novel chaos-based color image encryption scheme using bit-level permutation. *Symmetry* **2020**, *12*, 1497. Available online: https://www.mdpi.com/2073-8994/12/9/1497 (accessed on 9 February 2022). [CrossRef]
5. Geng, S.T.; Tao, W.; Wang, S.D. A novel image encryption algorithm based on chaotic sequences and cross-diffusion of bits. *IEEE Photon.* **2021**, *13*, 6276–6281. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9291442 (accessed on 9 February 2022).
6. Li, T.; Yang, M.; Wu, J.; Jing, X. A Novel Image Encryption Algorithm Based on a Fractional-order Hyperchaotic Sysetem and DNA Computing. *Complexity* **2017**, *2017*, 9010251. Available online: https://www.hindawi.com/journals/complexity/2017/9010251/ (accessed on 13 February 2022).
7. Zhu, S.; Deng, X.; Zhang, W.; Zhu, C. Image Encryption Scheme Based on Newly Designed Chaotic Map and Parallel DNA Coding. *Mathematics* **2023**, *11*, 231. Available online: https://www.mdpi.com/2227-7390/11/1/231 (accessed on 1 February 2023). [CrossRef]
8. Zou, C.; Wang, X.; Zhou, C. A novel image encryption algorithm based on DNA strand exchange and diffusion. *Elsevier Appl. Math. Comput.* **2022**, *430*, 127291. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0096300322003654 (accessed on 13 December 2022). [CrossRef]
9. Dua, M.; Wesanekar, A.; Gupta, V. Differential evolution optimization of intertwining logistic map-DNA based image encryption technique. *J. Amb. Intell. Human. Comput.* **2020**, *11*, 3771–3786. Available online: http://link.springer.com/article/10.1007/12652-019-01580-z (accessed on 9 February 2022). [CrossRef]
10. Soni, R.; Johar, A.; Soni, V. An Encryption and Decryption Algorithm for Image Based on DNA. In Proceedings of the 2013 International Conference on Communication Systems and Network Technologies, Gwalior, India, 6–8 April 2013; Volume 12, pp. 478–481. Available online: https://ieeexplore.ieee.org/abstract/document/6524442 (accessed on 9 February 2022).
11. Gupta, S.; Jain, A. Efficient Image Encryption Algorithm Using DNA Approach. In Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development, INDIACom, New Delhi, India, 11–13 March 2015; Volume 8, pp. 726–731. Available online: https://ieeexplore.ieee.org/abstract/document/7100345 (accessed on 13 February 2022).
12. Som, S.; Kotal, A.; Chatterjee, A.; Dey, S.; Palit, S. A Colour Image Encryption Based on DNA Coding and Chaotic Sequences. *ICETACS* **2013**, *112*, 108–114. Available online: https://ieeexplore.ieee.org/document/6691405 (accessed on 13 February 2022).
13. Liu, Q.; Liu, L.F. Color image encryption algorithm based on DNA coding and double chaos system. *IEEE Access* **2020**, *35*, 3581–3596. Available online: https://ieeexplore.ieee.org/document/9082588 (accessed on 6 March 2022). [CrossRef]
14. Zhang, Q.Y.; Han, J.T.; Ye, Y.T. Multi-image encryption algorithm based on image hash, bit-plane decomposition and dynamic DNA coding. *IET Image Proc.* **2020**, *68*, 726–731. Available online: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ipr2.12069 (accessed on 6 March 2022). [CrossRef]
15. Matthews, R. On the derivation of a Chaotic encryption algorithm. *Cryptologia* **1989**, *13*, 29–42. Available online: https://www.tandfonline.com/doi/abs/10.1080/0161-11899186374 (accessed on 13 February 2022). [CrossRef]
16. Belazi, A.; El-Latif, A. A simple yet efficient S-box method based on chaotic sine map. *Optik* **2017**, *130*, 1438–1444. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0030402616314887 (accessed on 6 March 2022). [CrossRef]
17. Niu, H.; Zhou, C.; Wang, B.; Zheng, X.; Zhou, S. Splicing Model and Hyper- Chaotic System for Image Encryption. *J. Electr. Eng.* **2016**, *67*, 78–86. Available online: https://sciendo.com/article/10.1515/jee-2016-0012 (accessed on 13 February 2022). [CrossRef]
18. Zhu, X.S.; Liu, H.; Liang, Y.R. Image encryption based on Kronecker product over fifinite fifields and DNA operation. *Optik* **2020**, *224*, 164725. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0030402620305611 (accessed on 6 March 2022). [CrossRef]
19. Liu, L.F.; Wang, J. A cluster of 1D quadratic chaotic map and its applications in image Encryption. *Math. Comput. Simul.* **2022**, *204*, 89–114. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0378475422003329 (accessed on 6 March 2022). [CrossRef]
20. Tom, H. Splicing and Regularity. *Bull. Math. Biol.* **1987**, *49*, 737. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0092824087900188 (accessed on 13 February 2022). [CrossRef]

21. Zheng, J.; Hu, H.P. A symmetric image encryption scheme based on hybrid analog-digital chaotic system and parameter selection mechanism. *Multimed. Tools Appl.* **2021**, *27*, 176–191. Available online: https://link.springer.com/article/10.1007/s11042-021-10751-0 (accessed on 13 February 2022). [CrossRef]
22. Kamarposhti, M.S.; Mohammad, D.; Rahim, M.; Yaghobi, M.I. Using 3-cell chaotic map for image encryption based on biological operations. *Nonlinear Dyn.* **2014**, *7*, 407–416. Available online: https://link.springer.com/article/10.1007/s11071-013-0819-6 (accessed on 13 February 2022). [CrossRef]