information

Article

Block Image Encryption Algorithm Based on Novel Chaos and DNA Encoding

Jianfeng Zhao [1], Shuying Wang [2,*] and Litao Zhang [3]

[1] Information Center, Henan Polytechnic, Urumqi 450046, China
[2] School of Astronautics, Xi'an Jiaotong University, Urumqi 710049, China
[3] College of Science, Zhengzhou University of Aeronautics, Urumqi 450015, China
* Correspondence: wangsy@stu.xjtyu.edu.cn

Abstract: To solve the problem of the low secret space and security of some image schemes, a novel 4D chaotic system is derived in this paper. Compared with other similar chaotic systems, the new system only has one equilibrium point and can exhibit hyperchaotic characteristics, under some parameter space. The system has better dynamic characters represented by calculation of the Lyapunov exponents, phase planes, and visual 0–1 test diagram. In this study, a novel image encryption algorithm is employed based on the new dynamic system, Zigzag transform, and DNA operation. Based on the improved Zigzag transformation, the plain image is block-scrambled, and DNA encoded with the treated chaotic sequences. The transformation efficiency is improved by combining multiple images at the same time. Numerical analysis has been carried out; the results show that our algorithm achieves much better performance in security, i.e., with enhanced pseudo-randomness, higher key sensitivity, weak correlation, fairly large key space, higher security, and a stronger ability to resist various attacks. Through visual analysis, the algorithm is deemed safe and effective for digital images.

Keywords: image encryption; novel chaos; Zigzag transform; DNA

Citation: Zhao, J.; Wang, S.; Zhang, L. Block Image Encryption Algorithm Based on Novel Chaos and DNA Encoding. *Information* **2023**, *14*, 150. https://doi.org/10.3390/info14030150

Academic Editor: Marco Baldi

Received: 25 January 2023
Revised: 22 February 2023
Accepted: 24 February 2023
Published: 26 February 2023

1. Introduction

With the rapid development of computer network communication technology, digital images are being widely used in numerous fields of society. On the other hand, digital images can be employed in the Behoove Pennon Carter process of information expression in multimedia information systems. At present, a variety of mobile devices, such as digital cameras, smart phones, and tablet computers, are increasingly popular. Using these mobile devices, people can conveniently realize the collection and transmission of digital image information. The privacy protection of digital images has attracted high attention from all walks of life. It is also a research hotspot in the field of information security. Traditional data encryption algorithms are not secure enough to encrypt digital images, which have high redundancy and a high pixel correlation. The chaotic system has many excellent characteristics; for instance, its sensitivity depends on the initial conditions and system parameters, ergodicity, and mixed diffusion properties (stretching and folding) of states [1–3]. Chaotic and hyperchaotic systems are an ideal choice for constructing cipher systems [4–8].

In recent years, many cryptographic algorithms based on discrete chaotic systems have been proposed by scholars [9,10]. However, multiple chaotic cryptosystems only use one-dimensional discrete chaotic maps, which have the following shortcomings: the secret key space is too small, which makes the capacity of resisting exhaustive attacks weak; and they are vulnerable to phase space identification attacks. With the wide application of image encryption in secure communication, color image encryption requires a large amount of calculation space and long encryption times. Belazi proposed a novel image

encryption scheme based on a permutation substitution network and chaotic systems [11]. Some new chaotic maps have been proposed, and the designed encryption approach has high security [12–14]. The beneficial characteristics of DNA computing have recently been discovered [15–18], including large computing parallelism, huge storage space and small energy loss. Great progress has been made in information encryption using complementary DNA rules [19,20]. Some encryption algorithms pass several statistical and randomness tests, but they are not secure enough in actually [21–23]. Recently, Erkan et al. designed an improved novel better image encryption scheme, which designs better key generation using deep CNN [24].

Özkaynak proposed a checklist to further test the security of different encryption algorithms [25]. In addition to encryption efficiency, the security of the encryption algorithm is another essential metric. In view of some shortcomings existing in the field of chaotic image encryption, such as the orbit of low-dimensional chaotic systems being relatively simple and easy to estimate, the construction and analysis of chaotic systems with new characteristics will still be an important direction in the field of chaos research for a long time. Complex image encryption schemes based on chaotic systems and other methods have potential applications in information security, secure communication, and other fields, and they all have been widely concerned. In this paper, the plain image is block scrambled using Zigzag transformation. To obtain higher randomness and overcome the limitations of DNA calculation, this paper randomly selects DNA rules for image blocks diffusion. With larger key space, weak dependence, better pseudo-randomness, and higher security, the designed algorithm has a strong ability to resist various attacks.

The rest of the paper is organized as follows: Section 2 introduces some related works. The proposed image cryptosystem is explained in Section 3. Section 4 conducts numerical experiments and shows the representative simulation results. The conclusion is given in the last section.

2. Image Encryption Scheme

2.1. Proposed 4D Chaotic System

In this paper, we propose a new four-dimensional chaotic system. The mathematical expression of this system is shown in Equation (1):

$$\begin{cases} \dot{x} = a_1 x + yz + a_2 w^2 + a_3 \\ \dot{y} = a_4 y - xz + w|y| \\ \dot{z} = xy + a_5 z \\ \dot{w} = w + a_6 z \end{cases} \tag{1}$$

Let the right side of Equation (1) of system take 0 to obtain:

$$\begin{cases} a_1 x + yz + a_2 w^2 + a_3 = 0 \\ a_4 y - xz + w|y| = 0 \\ xy + a_5 z = 0 \\ w + a_6 z = 0 \end{cases} \tag{2}$$

In this study, the parameters are set as $a_1 = -12$, $a_2 = 0.05$, $a_3 = -0.4$, $a_4 = 8$, $a_5 = -45$, $a_6 = -10$, and the initial value of the system is (0.02, 0.01, 0.03, 0.04). By solving this equation, the three equilibrium points $O(-\frac{1}{30}, 0, 0, 0)$ can be obtained. The system is linearized at the equilibrium point, and the Jacobian matrix is obtained as follows:

$$J(X)|_O = \begin{bmatrix} a_1 & z & y & 2a_2 w \\ -z & a_4 + w\mathrm{sgn}(y) & -x & |y| \\ y & x & a_5 & 0 \\ 0 & 0 & a_6 & 1 \end{bmatrix}\Bigg|_O = \begin{bmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_4 & \frac{1}{30} & 0 \\ 0 & -\frac{1}{30} & a_5 & 0 \\ 0 & 0 & a_6 & 1 \end{bmatrix} \tag{3}$$

Therefore, the characteristic equation of the Jacobian matrix J_O is:

$$\det(J|_O - \lambda I) = (a_1 - \lambda)(1 - \lambda)(\lambda^2 - (a_4 + a_5)\lambda + a_4 a_5 + \frac{1}{900}) = 0 \quad (4)$$

where λ and I are the eigenvalue and unit matrix, respectively. Four eigenvalues can be obtained as: $\lambda_1 = 0$, $\lambda_2 = 1$, $\lambda_3 = -12$, and $\lambda_4 = -37$. Given the one positive and two negative eigenvalues, the equilibrium point O is an unstable saddle point and is marked with a red square in Figure 1.

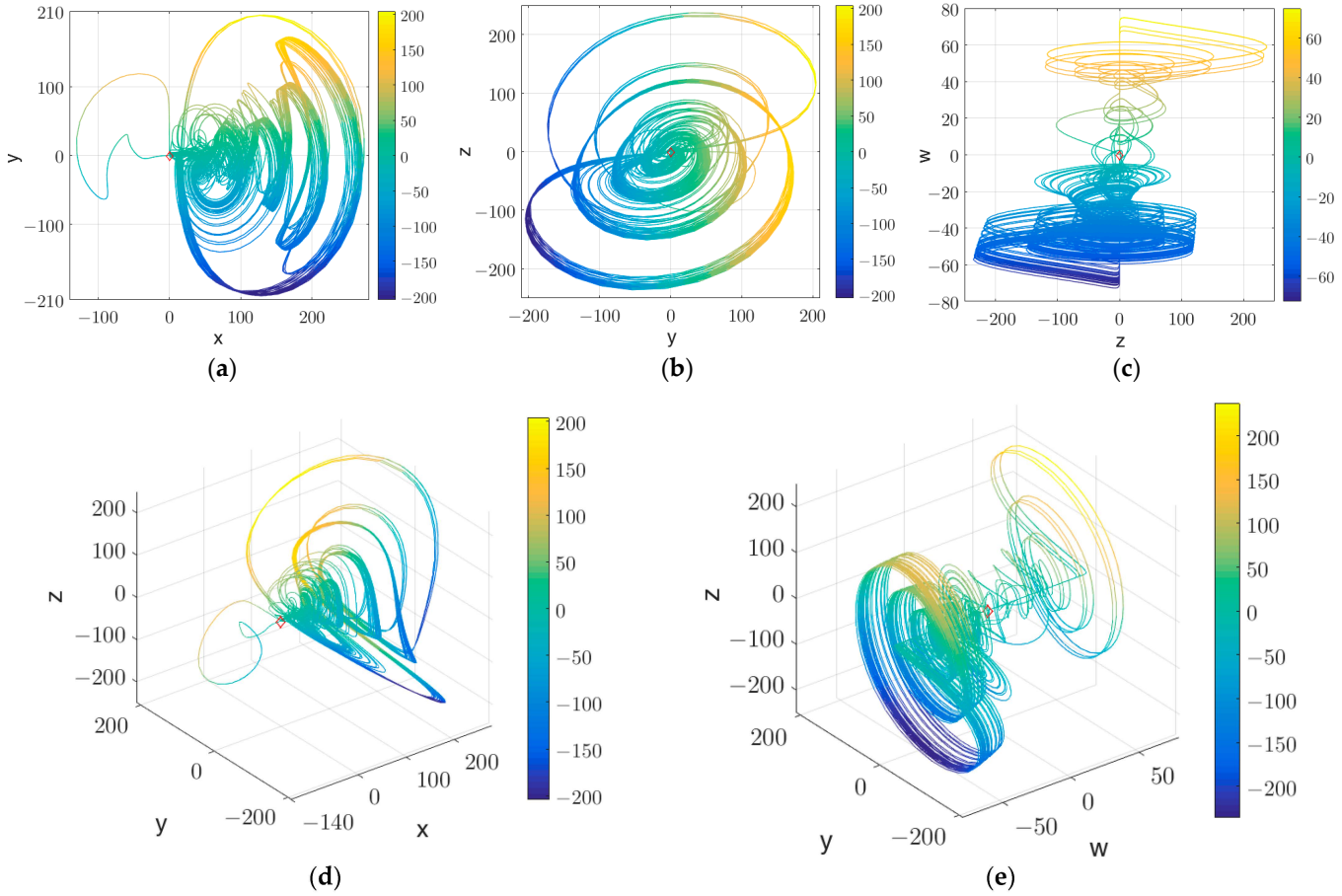


Figure 1. The chaotic behavior of system (1): (**a**) x–y plane; (**b**) y–z plane; (**c**) z–w plane; (**d**) x–y–z plane, (**e**) w–x–y plane.

According to the numerical calculation, the three-dimensional phase planes, and two-dimensional phase planes of the chaotic system in Equation (1) are shown in Figure 1. Figure 2a depicts the time sequence y of system (1), and the corresponding simple visual 0–1 test algorithm can be used to describe the dynamic behavior of system (1) in the p-s plane shown in Figure 2b. It can be clearly seen that the time series has periodic and pseudo-random characteristics. The behavior of the system is like Brownian motion, which indicates that the system has a hidden chaotic property.

Within parameter $a_2 \in [0.4, 0.7]$, the system (1) presents hyperchaotic state in a larger range. It can be verified from Figure 2c that two LE exponents are greater than 0, and the corresponding fractional dimension of the system is shown with blue pentagram in Figure 2d. The green pentagrams represent chaos state of the system (1). When parameter $a_2 = 0.0503$, the four Lyapunov exponents of the system are calculated as 1.598184, 0.498311,

-5.592705, and -41.243868. In this case, the fractional dimension of the system (1) is calculated by

$$D_L = j + \frac{1}{|L_{j+1}|}\sum_{i=1}^{j} L_i = 2 + \frac{1.5982 + 0.4983}{|-5.5927|} \approx 2.3749.$$

The maximum dimension is labeled with red pentagram in Figure 2d. With higher fractal dimensions, the chaotic system has more complex dynamic characteristics, and its chaotic sequence has higher quasi-randomness. Compared with low-dimensional chaotic systems, the system has resistance to brute-force attacks and a large key space.

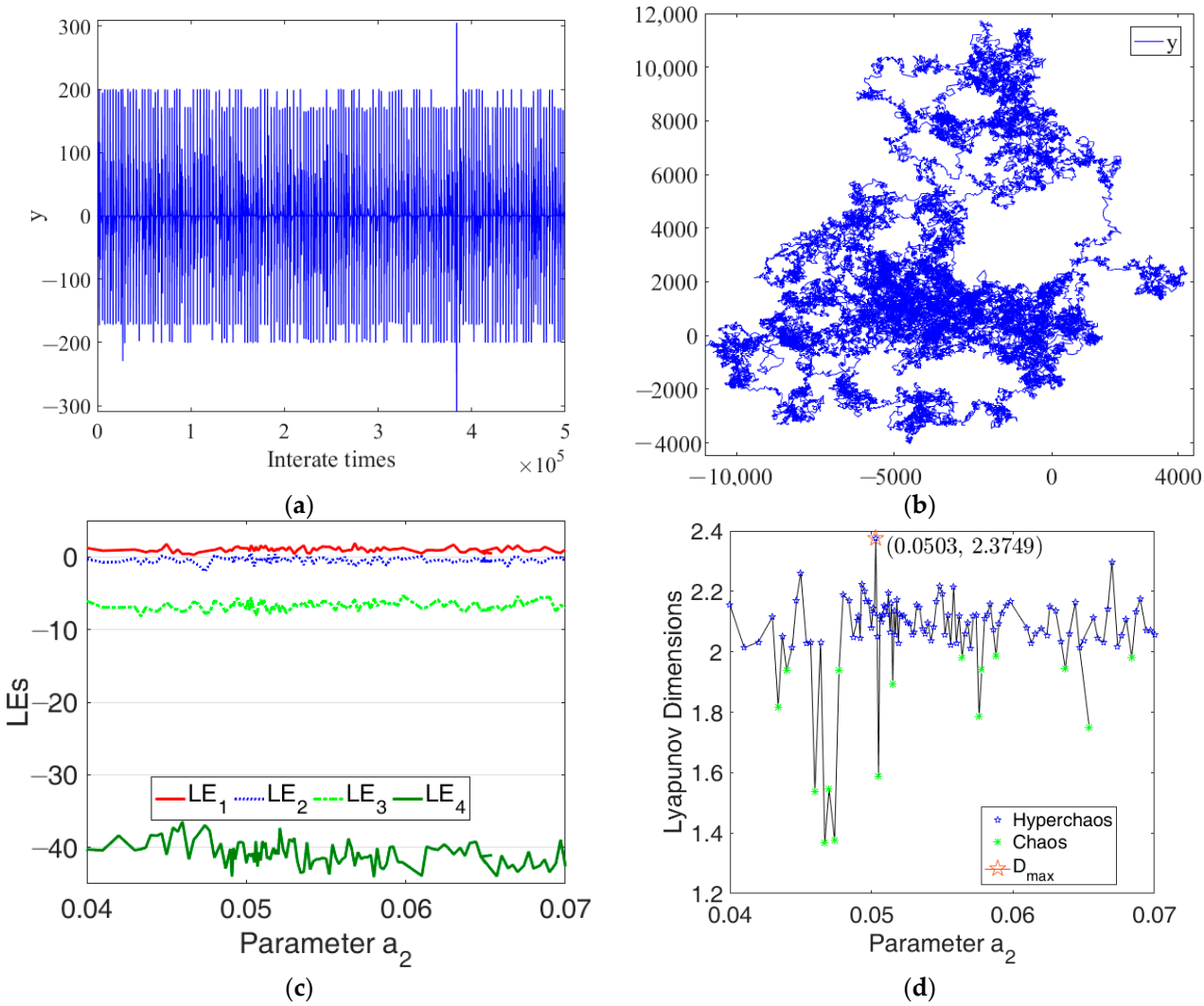
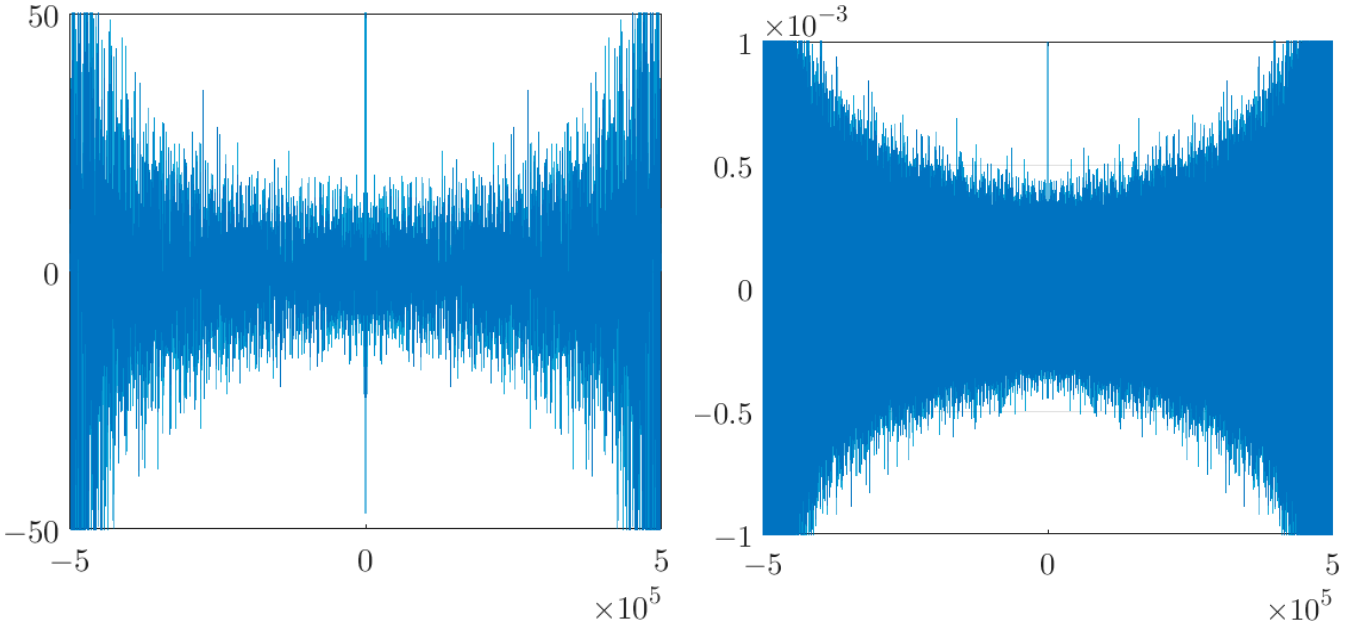


Figure 2. Nonlinear dynamical characters of the variable y: (**a**) time sequence; (**b**) p-s plane; (**c**) Lyapunov exponents; (**d**) Lyapunov dimensions of system (1).

The self-correlations of chaotic sequence y before and after treatment are shown in Figure 3. Figure 3b displays the local amplification and longitudinal amplification, and most of the data are concentrated in intervals $[-50, 50]$ and $[-0.001, 0.001]$ before and after treatment. Thus, the randomness of the hyperchaotic sequence is clearly improved, and the sequence is more suitable for cryptography.

The quality evaluation of the chaotic pseudo-random sequence is shown in Table 1 according to the FIPS 140-2 standard [26]. Accordingly, the random properties of the chaotic sequences meet the requirements of the encryption algorithm.



(**a**) (**b**)

Figure 3. Self-correlation comparison results of random sequences generated before and after sequence transformation: (**a**) primitive chaos sequence; (**b**) improved chaos sequence.

Table 1. Test Result of FIPS 140-2 Random Properties of chaotic sequence y.

Test Value	Monobit Test	Poker Test	Runs Test						Long Run Test
			Run Length						
			1	2	3	4	5	6	
Bit 0	9988	25.6832	2628	1232	600	310	161	152	0
Bit 1	10,012		2575	1317	512	321	142	156	0
Theory Value	9925~10,725	2.16~46.17	2315~2685	1114~1386	527~723	240~384	103~209	103~209	0
Result	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

2.2. Zigzag Transform

Zigzag transform is a scanning scrambling method [27,28], that stores all the scanned elements in a one-dimensional array in turn and then transforms the array into a scrambling matrix that is the same size as the original matrix by storing them in rows. This paper uses the Zigzag transform to scramble the blocked image. Figure 4a gives the classical scan table for a 5×5 matrix, and the obtained scrambled table is shown in Figure 4b. The Zigzag scanning process of the 8×8 Lena matrix is shown in Figure 4c–e. Accordingly, the matrix can be restored by using the Zigzag inverse transform for inverse scrambling. Zigzag transform is simple to implement and has low time complexity. In the practical application, performing only one Zigzag scramble for the image is not enough. We can perform multiple rounds of Zigzag scrambling to ensure the scrambling effect.

2.3. DNA Information

The concept of deoxyribonucleic acid (DNA) is taken from biology and represents the genetic information of biological characteristics with a double helix structure. It contains four types of nitrogenous bases, namely, adenine (A), thymine (T), cytosine (C), and guanine (G). T is connected in complementary base pairs with A, G, and C are complementary [29]. In connecting binary coding with DNA coding, assuming that the binaries 00 and 01, and 10 and 11, are complementary, then we can infer eight DNA encoding and decoding rules,

as listed in Table 1. The pixels of the gray image are converted to 8 bits. For example, the pixel value is 202, representing an 8-bit binary code 11001010. If rule 1 (A-00, G-10, C-01, T-11) in Table 2 is used for encoding, the binary sequence can be converted to encoding TAGG. If the DNA sequence is decrypted according to rule 4, the corresponding value is 54. DNA operations of rule 1 including addition, subtraction, and XOR operations are given in Table 3.

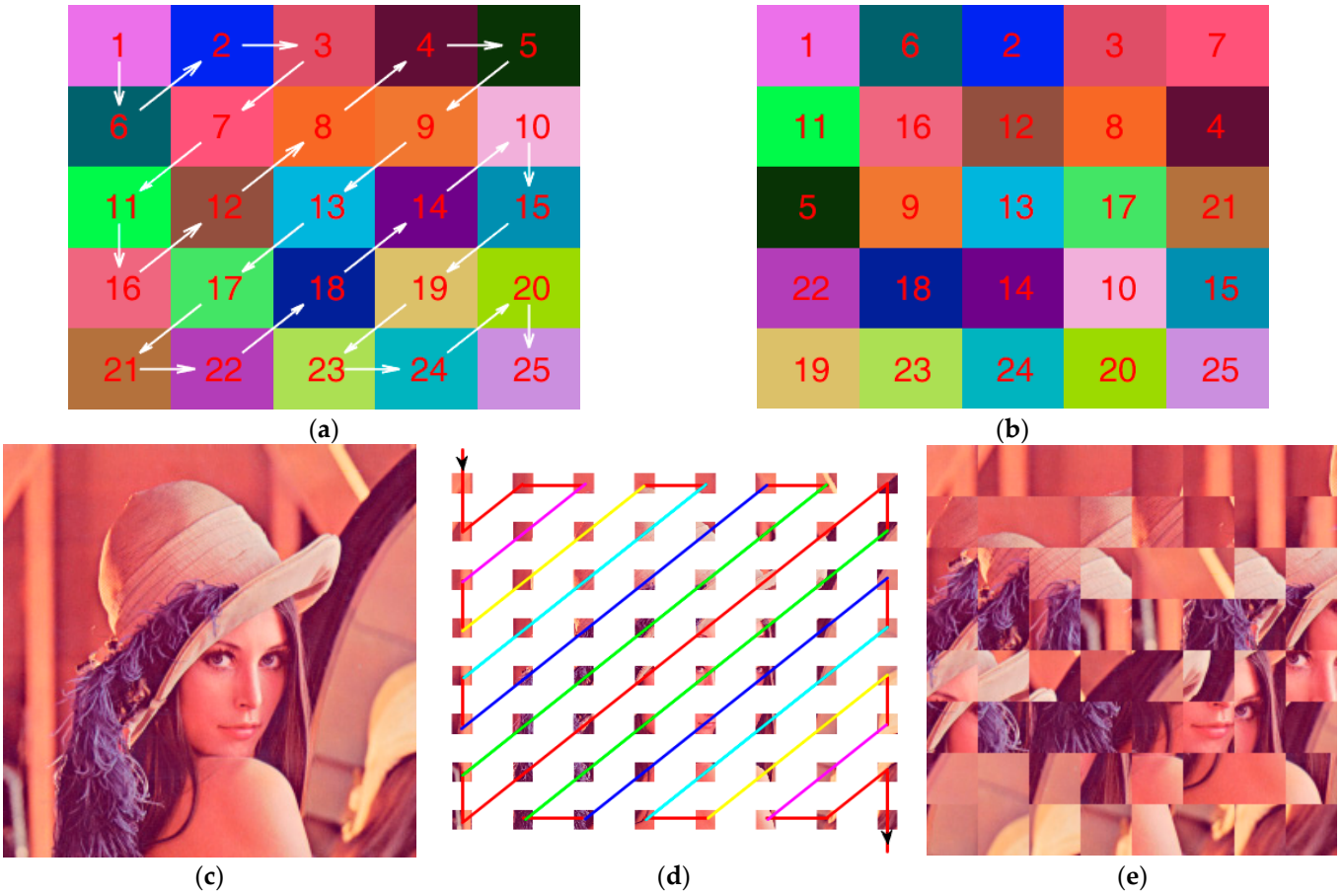


Figure 4. Zigzag scanning process. For a 5 × 5 matrix: (**a**) Zigzag transformation diagram; (**b**) the transformed matrix. For 8 × 8 block Lena color image: (**c**) plain image; (**d**) process of Zigzag transform; (**e**) scrambled Lena image.

Table 2. DNA coding rules.

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

Table 3. DNA base addition, subtraction, and XOR operation.

Base	Addition/Subtraction				XOR			
A	A/A	T/T	C/C	G/G	A	T	C	G
T	T/A	A/A	G/T	C/C	T	A	G	C
C	C/T	G/G	A/A	T/T	C	G	A	T
G	G/C	C/C	T/G	A/A	G	C	T	A

3. Structure of the Algorithm

The flowchart of the designed image encryption algorithm is illustrated in Figure 5, and the main steps of the encryption algorithm are described in detail here.

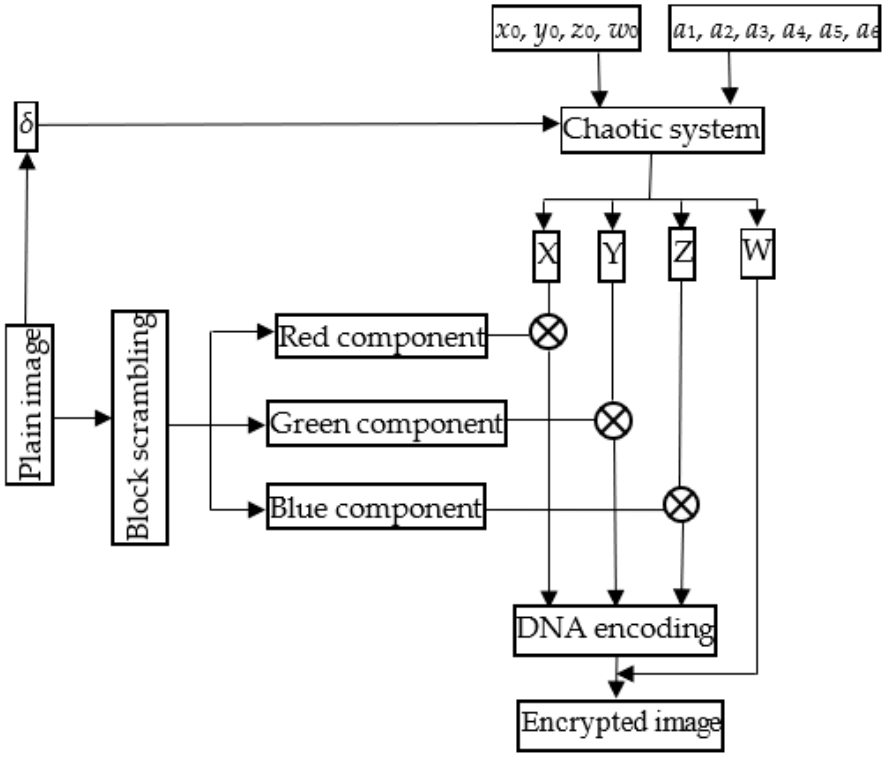


Figure 5. The flowchart of the cryptosystem.

Step 1. The number of transmitted images is judged. If multiple images are transmitted at the same time, we combine images to improve encryption efficiency. If only one image is transmitted, the encryption operation can be directly performed. That is to say, the plain image is a single image, or a combined image composed of several images.

Step 2. An interrupt parameter is generated based on plain image with a size of $L = M \times N$ by calculation formula: $\delta = \frac{\text{mean}(P(:))}{M \times N + \text{sum}(P(:))}$. Parameters and initial state vector are $(x_0 + \delta, y_0 + \delta, z_0 + \delta, w_0 + \delta)$ and $(a_1 + \delta, a_2 + \delta, a_3 + \delta, a_4 + \delta, a_5 + \delta, a_6 + \delta)$, respectively.

Step 3. The plain image is divided into several sub-blocks: $P_1, P_2, \cdots, P_{L/V^2}$, the size of every block is $V \times V$, thus the total number of sub-blocks is L/v^2. In this paper, the Zigzag transform is used to scramble the 8×8 sub-block images.

Step 4. In the proposed encryption scheme, as part of the secret key, parameter δ is combined with another part of the secret key to generate the initial input of the novel four-dimensional chaotic system. Based on the two parts of the secret key, the novel four-dimensional chaos generates four chaotic sequences: $X = \varphi(x)$, $Y = \varphi(y)$, $Z = \varphi(z)$, and $W = \varphi(w)$. The function φ is defined as $\varphi(t) = \text{mod}\left(floor\left(10^{15}|t| - floor\left(10^{15}|t|\right)\right), 256\right)$.

Step 5. The Red, Green, and Blue components of the scrambled image are labeled with S_r, S_g, S_b, and they are subjected to the XOR operation with sequences X, Y, and Z and to generate sequences S'_r, S'_g, and S'_b, respectively. The main calculation formulas are $S'_r = S_r \otimes X$, $S'_g = S_g \otimes Y$, and $S'_b = S_b \otimes Z$.

Step 6. Using rule 2 in Table 2, the processed fourth chaotic sequence is subjected to the DNA encoding and XOR operations with S'_r, S'_g, S'_b.

In the designed symmetric algorithm, decryption and encryption are reciprocal operations.

4. Numerical Experiment and Discussion

The numerical simulation of the encryption algorithm is running in a Windows 8 environment. We selected MATLAB R2016b as the programming language in the experiment. The system CPU was Core i5-5, the running memory is 16G, and the storage space is 2T.

4.1. Statistical Histogram Analysis

The gray histogram of each original image fluctuates greatly and shows certain statistical characteristics, as demonstrated in Figures 6b, 7b and 8b. In Figure 7, the combined image of the size 1024 × 1024 is composed of sixteen images (size: 256 × 256). Images in the first row: 4.1.01, 4.1.02, 4.1.07, and 4.1.04. Images in the second row: 4.1.05, 4.1.02, 4.1.07, and 4.2.03. Images in the third row: 4.2.01, 4.1.08, 4.1.03, and 4.2.06. Images in the fourth row: Babara, Peppers, House, and Lena. Except for the Lena standard image, the other tested images are from the USC-SIPI open-source database. The histograms of the R, G, and B components are indicated using a red line, a green line, and a blue line, respectively. To resist statistical attacks, the histogram of the encrypted image must be completely different from the histogram of the plain image. As shown in Figures 6d, 7d and 8d, the occurrence probability of each gray pixel in the encrypted image has no statistical characteristics, which indicates that the encrypted algorithm yielding uniform histograms can resist statistical attacks.

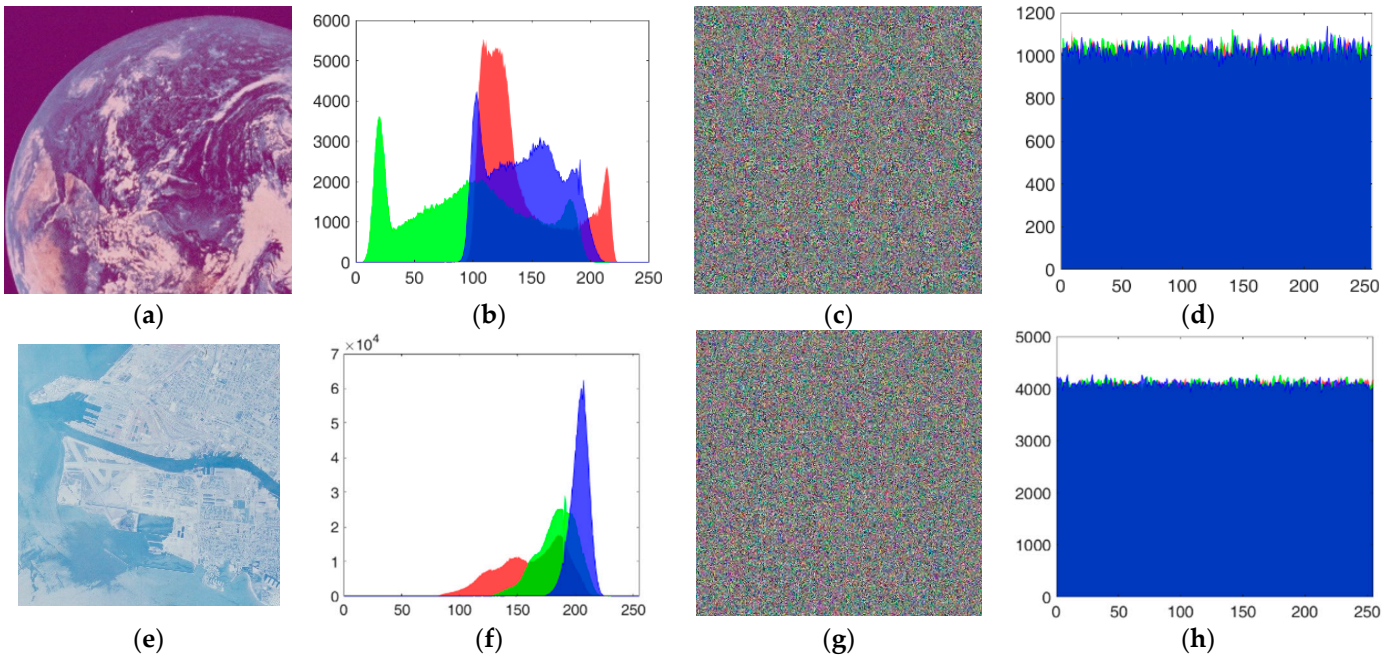


Figure 6. Encryption results for gray image: (**a**) Earth image; (**b**) histogram of (**a**); (**c**) encrypted Clock image; (**d**) histogram of (**c**); (**e**) Oakland image; (**f**) histogram of (**e**); (**g**) encrypted Pentagon image; (**h**) histogram of (**g**).

4.2. Correlation of Adjacent Pixels

Generally speaking, adjacent pixel correlation in the encrypted image should be close to 0. Here, we select 10,000 pixels randomly from the plain images and their encrypted images, respectively. The correlation coefficients between adjacent pixels in four directions (horizontal, vertical, diagonal, and counter-diagonal directions) are calculated via

$$R_{xy} = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})} \cdot \sqrt{\sum_{i=1}^{n}(y_i - \overline{y})}}, \quad (5)$$

where $\overline{x} = \frac{1}{n}\sum_{i=1}^{n} x_i, \overline{y} = \frac{1}{n}\sum_{i=1}^{n} y_i$, and the total number in selected pixels of the image is n. The correlation diagrams of adjacent pixels of the three channels in plain images are shown in Figure 7. The pixel points of the plain image are mostly distributed around the diagonal line shown in the first, third, and fifth line of Figure 7, which indicates that the image has strong correlation before encryption. The pixels with a certain tendency to aggregate are evenly distributed in space after the encryption, which shows that the encryption scheme achieves good de-correlation.

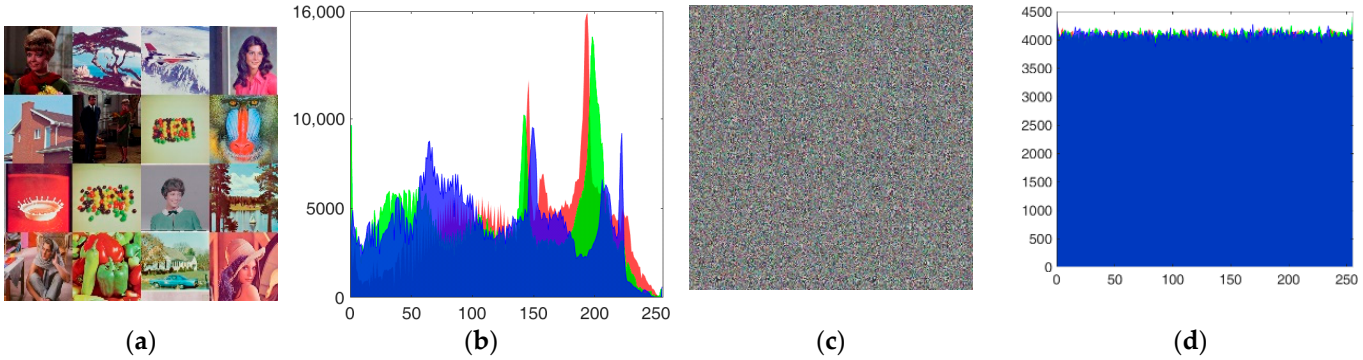


Figure 7. Encryption results for Combined image: (**a**) Combined image; (**b**) histogram of (**a**); (**c**) encrypted Combined image; (**d**) histogram of encrypted Combined image.

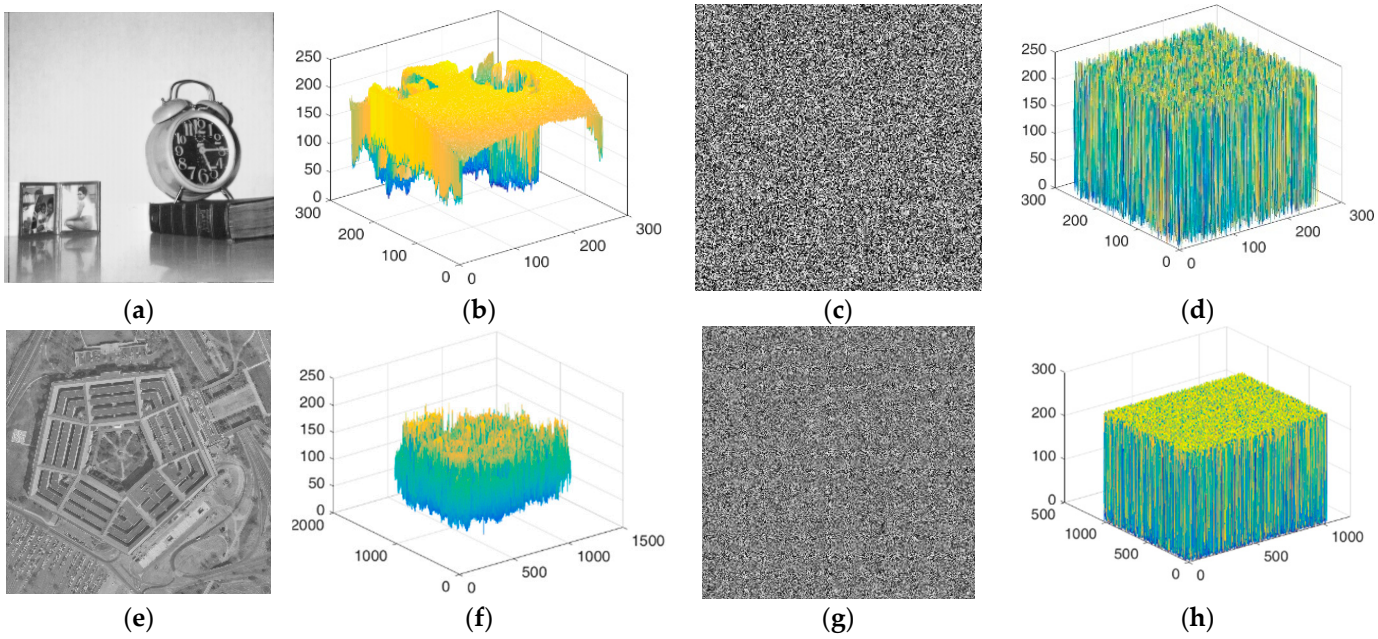


Figure 8. Encryption results for gray image: (**a**) Clock image; (**b**) Histogram of (**a**); (**c**) Encrypted Clock image; (**d**) histogram of (**c**); (**e**) Pentagon image; (**f**) histogram of (**e**); (**g**) encrypted Pentagon image; (**h**) histogram of (**g**).

The correlation coefficients of the plain images are close to 1, which means that the adjacent pixels of the original image have a strong correlation. The correlation coefficients of the encrypted images approach 0, as listed in Table 4, which means that the encrypted image has no correlation with the original image compared to the two other encryption algorithms [14,15], shown in Figure 9. As such, the attackers cannot compute any statistical information about the plain images from the encrypted images. According to the tests, the designed algorithm generates the highest values close to zero. Compared with some other state-of-the-art encryption techniques [30–34], the correlation coefficient of the designed

scheme is also lower than that of other schemes. We performed a comparison in Table 5, which shows that the encryption effect of this scheme is better.

Table 4. Correlation coefficients of test images.

Size	Image		Plain Image				Encrypted Image			
1024 × 1024	Earth	Red	0.9498	0.9461	0.9336	0.9440	-6.7918×10^{-4}	-2.3418×10^{-4}	-1.6835×10^{-4}	-6.0686×10^{-4}
		Green	0.9871	0.9859	0.9864	0.9476	-6.1831×10^{-4}	7.5871×10^{-4}	1.9887×10^{-4}	1.5069×10^{-6}
		Blue	0.9870	0.9859	0.9741	0.9863	9.2456×10^{-5}	-8.2715×10^{-5}	-3.4478×10^{-4}	-1.2586×10^{-5}
1024 × 1024	Oakland	Red	0.9144	0.9067	0.8868	0.8959	-3.0901×10^{-4}	4.7237×10^{-4}	5.7641×10^{-4}	-6.41116×10^{-4}
		Green	0.77241	0.7704	0.7253	0.7410	9.4721×10^{-4}	-6.8982×10^{-5}	-3.3608×10^{-4}	7.6725×10^{-5}
		Blue	0.4309	0.4357	0.3876	0.4042	-7.5263×10^{-4}	-2.8086×10^{-5}	1.2194×10^{-4}	-2.1374×10^{-4}
1024 × 1024	Combined image	Red	0.9723	0.9594	0.9442	0.9440	7.4802×10^{-4}	-2.3138×10^{-4}	4.2696×10^{-5}	5.1063×10^{-4}
		Green	0.9606	0.9522	0.9285	0.9220	-5.6293×10^{-4}	2.9770×10^{-4}	-1.0965×10^{-4}	5.2233×10^{-4}
		Blue	0.9314	0.9196	0.8874	0.8859	4.6697×10^{-4}	-3.5340×10^{-5}	0.0061	1.2482×10^{-5}
256 × 256	Gray Clock	Ref. [14]	0.9396	0.9672	0.9175	0.9266	8.0196×10^{-4}	6.7981×10^{-4}	2.7856×10^{-4}	0.0033
		Ref. [15]					0.022085	0.026092	−0.003475	
							0.0024	−0.0246	−0.0081	
1024 × 1024	Pentagon		0.7793	0.8405	06456	0.8179	-4.3352×10^{-5}	2.5509×10^{-5}	-2.1782×10^{-4}	3.0509×10^{-4}

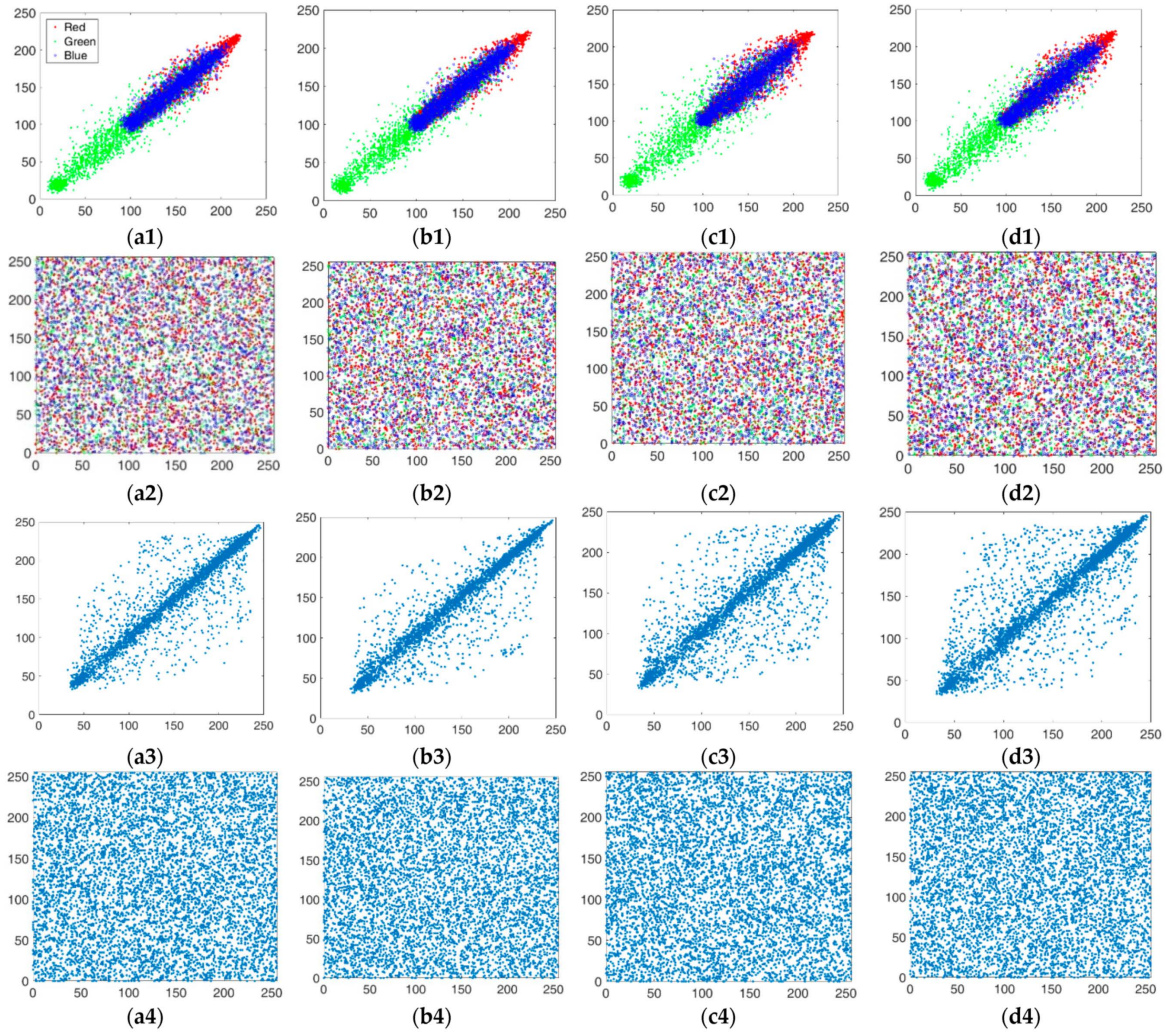


Figure 9. Correlation analysis in horizontal, vertical, Diagonal and Counter-Diagonal directions: (**a1**)–(**d1**) and (**a2**)–(**d2**) are the correlations of the Red channel, Green channel, and Blue channel of the Earth color image and the encrypted Earth image, respectively. (**a3**)–(**d3**) and (**a4**)–(**d4**) are the correlations of the Red channel, Green channel, and Blue channel of the Clock gray image and the encrypted Clock image, respectively.

Table 5. Correlation coefficients of encrypted Lena image in R, G, and B channels.

Planes	Directions	Plain Images	Proposed	Ref. [30]	Ref. [31]	Ref. [32]	Ref. [33]	Ref. [34]
Red	Horizontal	0.9475	0.000033	0.0064	−0.0067	−0.0217	−0.00076	0.0035
	Vertical	0.9727	−0.000295	0.0160	−0.0065	0.0654	0.01125	−0.0014
	Diagonal	0.9045	−0.000085	−0.0026	0.0006	−0.0381	−0.00255	0.0415
Green	Horizontal	0.9517	−0.000574	−0.0026	−0.0050	−0.0526	−0.00478	0.0029
	Vertical	0.9751	−0.000513	0.0034	0.0003	−0.0193	−0.01236	0.0040
	Diagonal	0.9159	0.000736	0.0125	0.7931	0.0364	0.00442	0.0031
Blue	Horizontal	0.9063	0.000390	0.0091	−0.0071	0.0219	0.00622	0.0029
	Vertical	0.9487	0.000301	−0.0045	0.0020	−0.4160	0.00950	0.0040
	Diagonal	0.8545	−0.000137	−0.0090	0.0015	−0.0567	0.00172	0.0031

4.3. Information Entropy Analysis

Information entropy is an important index used to evaluate the performance of encryption algorithms. The calculation of image source information entropy is performed as follows:

$$H(m) = -\sum_{i=1}^{2^n-1} p(m_i) \log_2 p(m_i) \tag{6}$$

where parameter n represents the length of the gray pixel value, and $p(m_i)$ is the probability of the random event m_i. For a random image with 256 gray level values, the probability of each gray level value is 1/256. The information entropy of the random image can be calculated as $H(m) = 8$. Therefore, the information entropy value of an ideal ciphertext image with an encrypted gray level of 256 is close to 8. The more uniform the encrypted gray value distribution is the lower the probability of information leakage.

The entropy values of plain images and encrypted images are listed in Table 6; all the values for the encrypted images are over 7.9, which is very close to the maximum entropy 8. This means that encrypted images are very close to random sources, and, thus, the proposed algorithm has a strong entropy analysis anti-attack capacity.

Table 6. Information entropy of plaintext and ciphertext images.

Test Images	Earth			Oakland			Combined Images			Clock	Pentagon
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue		
Plain image	6.5723	7.4511	6.7625	6.7458	6.0677	4.9460	7.7201	7.7389	7.7840	6.7056	6.7326
Encrypted image	7.9919	7.9916	7.9916	7.9921	7.9919	7.9918	7.9921	7.9872	7.9993	7.9985	7.9920

$S_1, S_2, \ldots,$ and S_k are k non-overlapping image blocks that are randomly selected from the image S. Every block has T_B pixels, and the calculation formula is defined as follows:

$$\overline{H_{(k,T_B)}(s)} = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{7}$$

where $H(S_i)$ is the global information entropy of S_i. In light of the suggestion of Ref. [35], we employ $k = 30$ and $T_B = 1936$ to test the encryption effect. For example, some image blocks of Clock are randomly selected to carry out the entropy calculation separately in Figure 10. The local information entropy value of the corresponding encrypted Clock gray image is 7.9027, which falls into the ideal interval, meaning that this encryption scheme approximately uniformly distributes the ciphertext pixels.

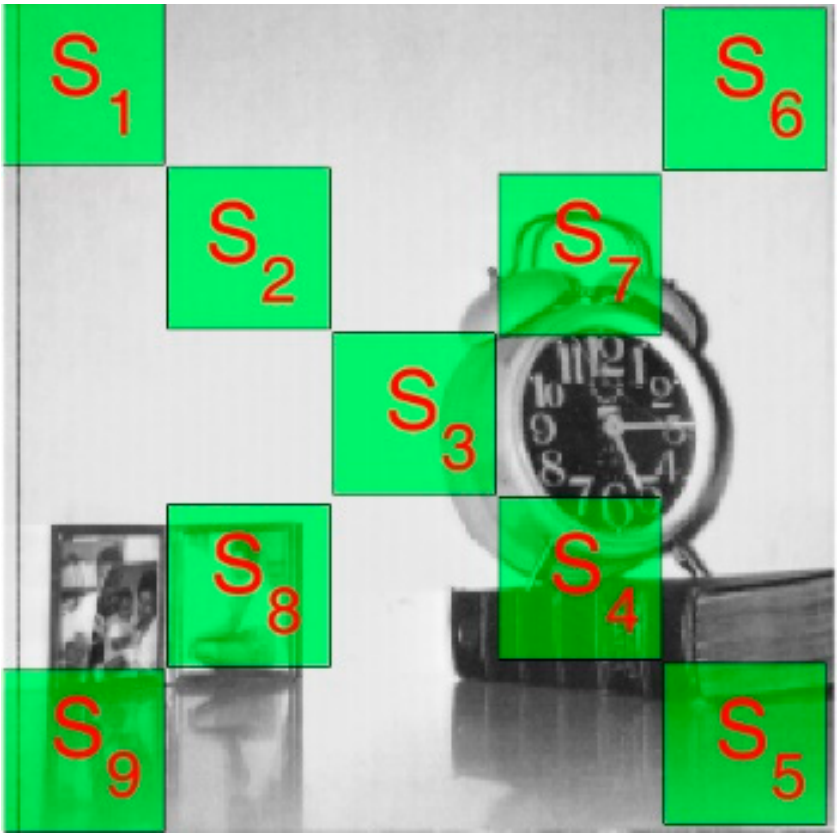


Figure 10. Partial non-overlapping image blocks of Clock image.

4.4. Differential Attack Analysis

The attacker can find the correlation between the plaintext and the ciphertext by observing the decryption change caused by the small change in plaintext. If a small change in the original image can cause a large change in the ciphertext, the effect of a differential attack is reduced. The Number of Pixel of Change Rate (NPCR) and Unified Average Changing Intensity (UACI) [36] are derived from

$$\begin{aligned} D'(i,j) &= \begin{cases} 0\,, C_1(i,j) = C_2(i,j), \\ 1\,, C_1(i,j) \neq C_2(i,j). \end{cases} \\ NPCR(C_1,C_2) &= \frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D'(i,j) \times 100\%, \\ UACI(C_1,C_2) &= \frac{1}{255\times M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N} |C_1(i,j) - C_2(i,j)| \times 100\%. \end{aligned} \tag{8}$$

where M and N are the width and height of the plain image, respectively. Moreover, $C_1(i, j)$ and $C_2(i, j)$ are the encrypted images of plain images before and after one-pixel modification at $P(20, 23)$, respectively. Average changing intensity is the difference between two images, obtained by evaluating changes in visual effects.

To test the ability of the proposed algorithm to resist a differential attack, we changed the one-pixel value of a plain image. Then, the same encryption algorithm and key are applied to encrypt it and derive its corresponding encryption image. Finally, NPCR and UACI are calculated by Equation (8). Table 7 gives the experimental results and comparison with other algorithms [37,38]. The data shows that the test results are close to the theoretical expected values of NPCR (99.6094%) and UACI (33.4635%), which indicates that the encrypted images are secure. The designed algorithm has strong differential anti-attack capacity when applied to color and grayscale images.

Table 7. Test results of NPCR and UACI.

Images	Earth			Combined Images			Clock		
	Red	**Green**	**Blue**	**Red**	**Green**	**Blue**	**Proposed**	**Ref. [37]**	**Ref. [38]**
Pixel value	102	25	99	226	137	113	197		
New pixel value	103	26	100	227	134	114	198		
NPCR (%)	99.6176	99.6280	99.5977	99.6504	99.5873	99.6117	99.5935	99.5703	49.8280
UACI (%)	33.4502	33.4412	33.4755	33.4131	33.4910	33.4655	33.4789	33.4302	17.0621

4.5. Key Sensitivity Analysis

Key sensitivity is one of the basic characteristics of cryptography and an important evaluation index of a cryptographic algorithm. To evaluate the key sensitivity of the algorithm, the author changes the first variable of the initial condition by adding 10^{-14} and selects the combined image to show the decryption results under different keys. Figure 11 shows the state space plots x–y with different values of x_0 = (0.02, 0.01, 0.03, 0.04) and x'_0 = (0.02 + 10^{-14}, 0.01, 0.03, 0.04). A tiny variation in the key can generate a completely different cipher image and recovered image, as shown in Figure 12. The key sensitivity of slight changes to an initial variable is calculated from the NPCR and UACI values, which are 99.6087, and 33.6451, respectively. The differences between the two decryption images are as follows: the decryption image is messy and unrecognizable; therefore, the experimental result shows that the proposed algorithm has a strong key sensitivity, and it can withstand the known ciphertext attacks and chosen ciphertext attacks.

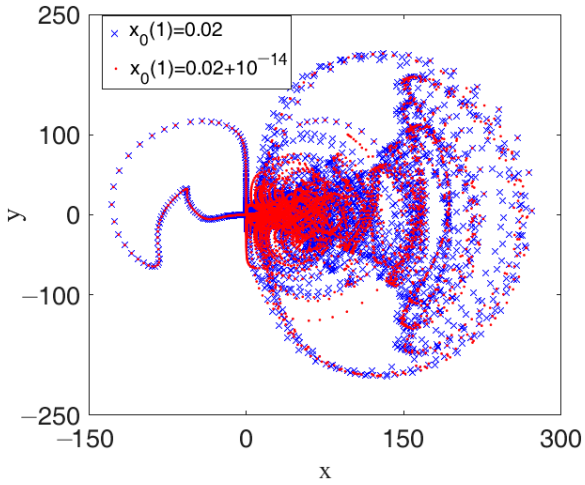


Figure 11. State space plots for different initial conditionals.

(**a**) (**b**) (**c**)

Figure 12. Key sensitivity analyses (**a**) encrypted image; (**b**) decrypted image with $x_0(1)$ = 0.02; (**c**) decrypted image with $x_0(1)$ = 0.02 + 10^{-14}.

4.6. Data Loss and Noise Attacks Analysis

The cropping attacks and noise attacks are used to disrupt the integrity of the ciphertext image, which would prevent the decryption or to obtain the correct decryption information. In the cropping attacks resistance experiment, the encrypted images at 1/16, 1/8, and 1/4 cropping degrees are decrypted, as shown in Figure 13. In the salt and pepper noise attacks resistance experiment, the encrypted images with noise strengths of 0.01, 0.05, and 0.1 are decrypted, as shown in Figure 14. The proposed cryptosystem can effectively resist cropping attacks and noise attacks. The algorithm can be used to encrypt identifiable plaintext images from ciphertext images that have been damaged to varying degrees.

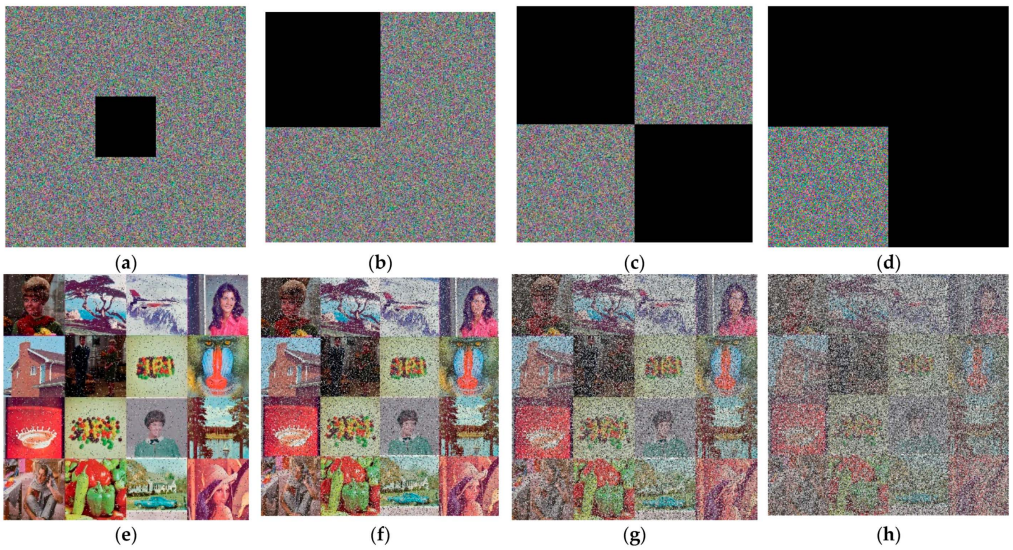


Figure 13. Decryption results of encrypted Combined image after cropping attacks: (**a**) 1/16 degree of cropping; (**b**) 1/4 degree of cropping; (**c**) 1/2 degree of cropping; (**d**) 3/4 degree of cropping; (**e**–**h**) decrypted images of (**a**–**d**).

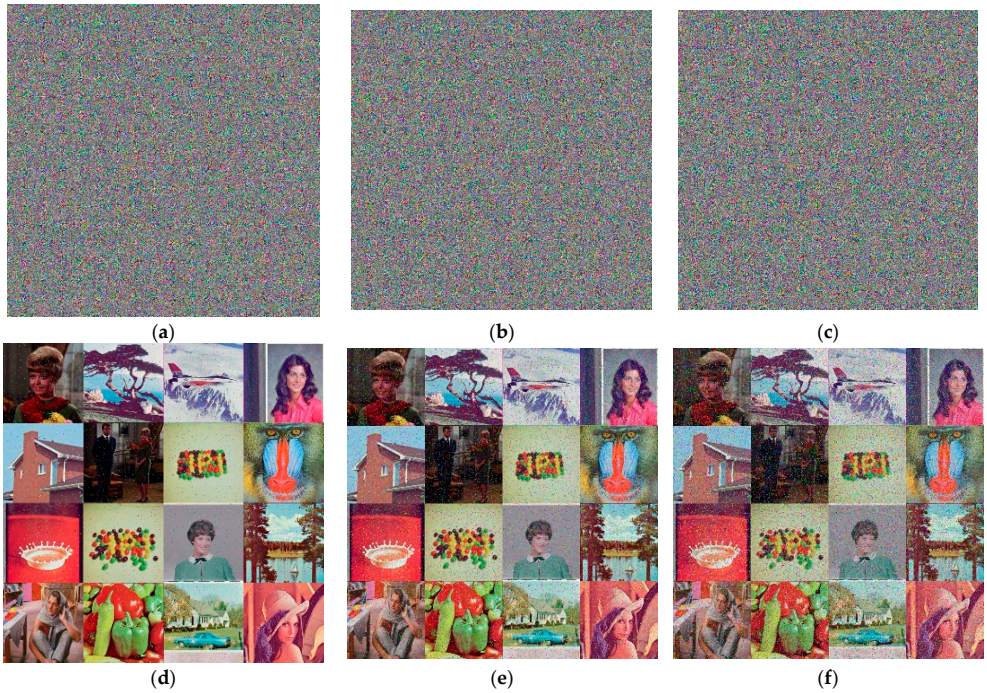


Figure 14. Decrypted Combined image after salt and pepper noise attacks: (**a**) with a noise strength of 0.01; (**b**) with a noise strength of 0.05; (**c**) with a noise strength of 0.1; (**d**–**f**) Decrypted images of (**a**–**c**).

4.7. Encryption Quality Analysis

The objective vertex that evaluates the quality of the image after compression and decryption is the PSNR (Peak Signal to Noise Ratio) value, and its mathematical definition is as follows:

$$PSNR = 10\log\left[\frac{(2^n-1)^2}{MSE}\right] \tag{9}$$

For a gray scale image, the bits per pixel n = 8. The MSE (Mean Square Error) is the mean squared error, defined as

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(P(i,j) - D(i,j))^2 \tag{10}$$

where $M \times N$ is the size of the original image, $P(i,j)$ is the original image, and $D(i,j)$ is the corresponding decrypted image that is cropped or has added noise.

Table 8 provides the PSNR and MSE values for the different attacks of the Combined color image in Section 4.5. The smaller the PSNR value, the more distorted the image is. When the data loss is 0.5, the decrypted image is still visible, thus the proposed encryption scheme satisfies the secure image transmission.

Table 8. PSNR and MSE for three channels of Combined image.

Attack		MSE				PSNR (dB)			
		Red	**Green**	**Blue**	**Mean**	**Red**	**Green**	**Blue**	**Mean**
Cropping ratio	1/16	6.1906	7.0087	6.5744	6.5912	38.9338	39.6744	39.9521	39.5201
	1/4	32.7330	27.4837	25.5995	28.6054	32.9809	33.7400	34.0484	33.5897
	1/2	65.6912	55.0312	51.5109	57.4111	29.9557	30.7247	31.0118	30.5641
	3/4	98.2682	82.2418	77.1118	85.8739	28.2066	28.9798	23.1080	26.7648
Pepper–salt noise densities	0.01	2.0369	23.4718	2.6262	9.3783	45.0409	44.2005	43.9374	44.3929
	0.05	10.1128	12.1453	12.7559	11.6713	38.0820	37.2867	37.0736	37.4807
	0.1	19.6899	23.6605	25.0473	22.7992	35.1883	34.3905	34.1431	34.5739

4.8. Time Complexity Analysis

Time complexity of the encryption algorithm depends on the highest value of all the steps of the encryption algorithm. It is assumed that the size of the plaintext image is M × N, and the time complexity of constructing four chaotic sequences is O(4 × M × N). Compared with image block scrambling, the time complexity of the XOR operation of image pixels O(M × N) is higher, and the time complexity of image DNA coding and decoding O(8 × M × N) is the highest. Therefore, the total time complexity of the proposed encryption scheme is O(8 × M × N).

4.9. Key Space Analysis

The entire key composition includes the external security key and the key generated by the encrypted object. As the initial value and parameter of the chaotic system, the main security key is the interrupt parameter δ, (x_0, y_0, z_0, w_0) and (a_1, a_2, a_3, a_4, a_5, a_6), which can be taken up to 15 decimal places. Then, the key space is $(10^{15})^{11} \approx 2^{548}$, that is, the key length is 548-bit, which is much larger than 100-bit, thus there is enough key space. If the disturbance parameter $\{r_i\}$ ($i = 1, 2 \ldots 64$) or DNA sequence generation rules and calculation methods are used, the key space will be larger. The key space of our algorithm is compared with those of existing encryption algorithms [30,32,39–42], and the comparison results are shown in Table 9. Thus, the encryption algorithm has larger key space to effectively resist exhaustive violent attacks.

Table 9. Comparison with other algorithms for key space.

Scheme	Proposed	Ref. [30]	Ref. [32]	Ref. [39]	Ref. [40]	Ref. [41]	Ref. [42]
key space	10^{150}	10^{35}	2^{512}	10^{56}	2^{449}	2^{312}	10^{94}

5. Conclusions

Based on a novel 4-D dynamic system, the improved Zigzag transform, and DNA encoding, we propose a better image encryption algorithm. Zigzag transform is used to break the position relationship of all sub-image blocks. Then, the RGB components of the scrambled image are diffused with the first three chaotic sequences. Lastly, three diffused image components are formed from the DNA operation with the fourth sequence. To improve the efficiency of multi-image transmission, sixteen images are combined into one image for data encryption transmission. The simulation results show that the algorithm has a quite large key space, high key sensitivity, weak correlation, enhanced pseudo-randomness, higher security, and a stronger ability to resist various attacks. The performance of the encrypted standard Lena image is compared with those of other state-of-the-art approaches, and we find that the proposed algorithm in this paper is closer to the ideal value in encryption performance and has better security. However, if the algorithm is applied to fast mobile devices, its efficiency needs to be further improved.

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

Funding: This work was supported by the National Natural Science Foundation of China (No. 11226337, 11501525), the Science and Technology Foundation of Henan Province of China (Grant No. 222102210250), the Research on Teaching Reform of Henan Polytechnic (Grant No. 2021J058), the Scientific Research of Henan Polytechnic (Grant No. 2022ZK49), the Basic Research Projects of Key Scientific Research Projects Plan in Henan Higher Education Institutions (20zx003), Henan Natural Science Foundation (222300420579), and the Teaching Reform and Practice Program of Vocational Education in Henan Province (Grant No. [2023] 03049).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

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

References

1. Baptista, M.S. Cryptography with chaos. *Phys. Lett. A* **1998**, *240*, 50–54. [CrossRef]
2. Alvarez, G.; Li, S. Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurcat. Chaos* **2006**, *16*, 2129–2151. [CrossRef]
3. Xu, Q.; Sun, K.; He, S.; Zhu, C. An effective image encryption algorithm based on compressive sensing and 2D-SLIM. *Opt. Lasers Eng.* **2020**, *134*, 106178. [CrossRef]
4. Hu, G.; Xiao, D.; Zhang, Y.; Xiang, T. An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy. *Nonlinear Dynam.* **2017**, *87*, 1359–1375. [CrossRef]
5. Ye, G.D.; Wong, K.W. An image encryption scheme based on time-delay and hyperchaotic system. *Nonlinear Dynam.* **2012**, *71*, 259–267. [CrossRef]
6. Wang, X.; Liu, L.; Zhang, Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Opt. Lasers Eng.* **2015**, *66*, 10–18. [CrossRef]
7. Riyahi, M.; Kuchaki Rafsanjani, M.; Motevalli, R. A novel image encryption scheme based on multi-directional diffusion technique and integrated chaotic map. *Neural Comput. Appl.* **2021**, *33*, 14311–14326. [CrossRef]
8. Erkan, U.; Toktas, A.; Lai, Q. 2D hyperchaotic system based on Schaffer function for image encryption. *Expert Syst. Appl.* **2003**, *213*, 119076. [CrossRef]

9. Chen, G.; Mao, Y.; Chui, C. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fract.* **2004**, *21*, 749–761. [CrossRef]
10. Hanis, S.; Amutha, R. Double image compression and encryption scheme using logistic mapped convolution and cellular automata. *Multimed. Tools Appl.* **2018**, *77*, 6897–6912. [CrossRef]
11. Belazi, A.; El-Latif, A.A.A.; Belghith, S. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process.* **2016**, *128*, 155–170. [CrossRef]
12. Erkan, U.; Toktas, A.; Toktas, F.; Alenezi, F. 2D eπ-map for image encryption. *Inf. Sci.* **2022**, *589*, 770–789. [CrossRef]
13. Lai, Q.; Hu, G.; Erkan, U.; Toktas, A. A novel pixel-split image encryption scheme based on 2D Salomon map. *Expert Syst. Appl.* **2003**, *213*, 118845. [CrossRef]
14. Farah, M.A.B.; Farah, A.; Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynam.* **2020**, *99*, 3041–3064. [CrossRef]
15. Wang, X.; Zhang, Y.; Bao, X. A novel chaotic image encryption scheme using DNA sequence operations. *Opt. Lasers Eng.* **2015**, *73*, 53–61. [CrossRef]
16. Chai, X.; Gan, Z.; Yang, K. An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Process. *Image Commun.* **2017**, *52*, 6–19.
17. Li, Z.; Peng, C.; Tan, W. A novel chaos-based image encryption scheme by using randomly DNA encode and plaintext related permutation. *Appl. Sci.* **2020**, *10*, 7469. [CrossRef]
18. Nematzadeh, H.; Enayatifar, R.; Yadollahi, M. Binary search tree image encryption with DNA. *Optik* **2020**, *202*, 163505. [CrossRef]
19. Dong, W.; Li, Q.; Tang, Y.; Zeng, M.H.R. A robust and multi chaotic DNA image encryption with pixel-value pseudorandom substitution scheme. *Opt. Commun.* **2021**, *15*, 127211. [CrossRef]
20. Yildirim, M. Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit. *Chaos Solitons Fract.* **2022**, *155*, 111631. [CrossRef]
21. Li, C.; Lin, D.; Lü, J. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multimed.* **2017**, *24*, 64–71. [CrossRef]
22. Chen, L.; Chen, J.; Ma, L.; Wang, S. Cryptanalysis of a chaotic image cipher based on plaintext-related permutation and lookup table. *Nonlinear Dynam.* **2020**, *100*, 3959–3978. [CrossRef]
23. Zhang, C.; Chen, J.; Chen, D. Cryptanalysis of an Image Encryption Algorithm Based on a 2D Hyperchaotic Map. *Entropy* **2022**, *24*, 1551. [CrossRef] [PubMed]
24. Erkan, U.; Toktas, A.; Enginoğlu, S.; Akbacak, E.; Thanh, N.H.D. An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimed. Tools Appl.* **2022**, *81*, 7365–7391. [CrossRef]
25. Özkaynak, F. Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynam.* **2018**, *92*, 305–313. [CrossRef]
26. Pareschi, F.; Rovatti, R.; Setti, G. On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Trans. Inf. Foren. Secur.* **2012**, *7*, 491–505. [CrossRef]
27. Gao, H.; Wang, X. Chaotic image encryption algorithm based on Zigzag transform with bidirectional crossover from random position. *IEEE Access* **2021**, *9*, 105627–105640. [CrossRef]
28. Ying, J.; He, F.; Wang, H. Color image encryption based on the combination of Zigzag scanning laser speckle and chaos. *Laser Mag.* **2018**, *39*, 85–88.
29. Guesmi, R.; Farah, M.A.B.; Kachouri, A.; Samet, M. A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. *Nonlinear Dyn.* **2016**, *83*, 1123–1136. [CrossRef]
30. Hosy, K.M.; Kamal, S.T.; Darwish, M.M. A color image encryption technique using block scrambling and chaos. *Multimed. Tools Appl.* **2022**, *81*, 505–525. [CrossRef]
31. Chen, L.; Yin, H.; Yuan, L.; Machado, A.T.; Wu, R.; Alam, Z. Double color image encryption based on fractional order discrete improved Henon map and Rubik's cube transform. Signal Process. *Image Commun.* **2021**, *97*, 116363.
32. Wang, Y.; Chen, L.; Yu, K.; Lu, T. Image encryption algorithm based on lattice hash function and privacy protection. *Multimed. Tools Appl.* **2022**, *81*, 18251–18277. [CrossRef]
33. Ge, F.; Qin, Z.; Chen, Y. Integrated time-fractional diffusion processes for fractional-order chaos-based image encryption. *Sensors* **2021**, *21*, 6838. [CrossRef]
34. Wu, J.; Liao, X.; Yang, B. Image encryption using 2D Henon sine map and DNA approach. *Signal Process.* **2018**, *153*, 11–23. [CrossRef]
35. Wu, Y.; Zhou, Y.; Saveriades, G.; Agaian, S.; Noonan, J.P.; Natarajan, P. Local Shannon entropy measure with statistical tests for image randomness. *Inf. Sci.* **2013**, *222*, 323–342. [CrossRef]
36. Wu, Y.; Noonan, J.; Again, S. NPCR and UACI randomness tests for image encryption. *Cyber J.* **2011**, *1*, 31–38.
37. Hua, Z.; Zhou, Y. Image encryption using 2D logistic-adjusted-sine map. *Inf. Sci.* **2016**, *339*, 237–253. [CrossRef]
38. Liao, X.; Lai, S.; Zhou, Q. A novel image encryption algorithm based on self-adaptive wave transmission. *Signal Process.* **2010**, *90*, 2714–2722. [CrossRef]
39. Zhang, Y.; He, Y.; Li, P.; Wang, X.-Y. A new color image encryption scheme based on 2DNLCML system and genetic operation. *Opt. Lasers Eng.* **2020**, *128*, 106040. [CrossRef]

40. Yang, F.; Mou, J.; Ma, C.; Cao, Y. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Opt. Lasers Eng.* **2020**, *129*, 106031. [CrossRef]
41. Hu, G.; Li, B. Coupling chaotic system based on unit transform and its applications in image encryption technique. *Signal Process.* **2018**, *178*, 107790. [CrossRef]
42. Rehman, A.U.; Liao, X.; Ashraf, R.; Ullah, S.; Wang, H. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik* **2018**, *159*, 348–367. [CrossRef]