symmetry

MDPI

Article

Image Encryption Based on Local Fractional Derivative Complex Logistic Map

Hayder Natiq [1], Nadia M. G. Al-Saidi [2], Suzan J. Obaiys [3,*], Mohammed Najah Mahdi [4] and Alaa Kadhim Farhan [5]

1 Information Technology College, Imam Ja'afar Al-Sadiq University, Baghdad 10001, Iraq
2 Department of Applied Sciences, University of Technology, Baghdad 10066, Iraq
3 Department of Computer Systems and Technology, Faculty of Computer Science and Information Technology, University Malaya, Kuala Lumpur 50603, Malaysia
4 ADAPT Centre, School of Computing, Dublin City University, D09 DXA0 Dublin, Ireland
5 Computer Science Department, University of Technology, Baghdad 10066, Iraq
* Correspondence: suzan@um.edu.my

Abstract: Local fractional calculus (fractal calculus) plays a crucial role in applications, especially in computer sciences and engineering. One of these applications appears in the theory of chaos. Therefore, this paper studies the dynamics of a fractal complex logistic map and then employs this map to generate chaotic sequences for a new symmetric image encryption algorithm. Firstly, we derive the fractional complex logistic map and investigate its dynamics by determining its equilibria, geometric properties, and chaotic behavior. Secondly, the fractional chaotic sequences of the proposed map are employed to scramble and alter image pixels to increase resistance to decryption attacks. The output findings indicate that the proposed algorithm based on fractional complex logistic maps could effectively encrypt various kinds of images. Furthermore, it has better security performance than several existing algorithms.

Keywords: fractal; local fractional calculus; complex logistic map; symmetric image encryption algorithm; chaotic function; subordination and superordination; open unit disk; analytic function; univalent function

Citation: Natiq, H.; Al-Saidi, N.M.G.; Obaiys, S.J.; Mahdi, M.N.; Farhan, A.K. Image Encryption Based on Local Fractional Derivative Complex Logistic Map. *Symmetry* **2022**, *14*, 1874. https://doi.org/10.3390/sym14091874

Academic Editors: Marek Berezowski and Marcin Lawnik

Received: 20 June 2022
Accepted: 28 July 2022
Published: 8 September 2022

1. Introduction

Advancements in communications and computer technologies facilitate data transmission over internet networks. However, the main issues of data transmission over the internet are the safety of the information from unauthorized users. Recently, image encryption, which aims to keep information secret, has attracted researchers from various fields [1]. In the encryption and decryption processes, security keys are an integral part. The security keys are used to convert the data to nonsense data and vice versa; thus, security keys should be shared to recover the original image [2].

The process of image encryption and decryption is based on mathematical models, which are used to encrypt images using multi-secret keys [3]. Many encryption models have been proposed. The most known image encryption algorithms are based on chaotic encryption [4–6]. Over the years, chaos theory has been applied in science and engineering [7,8]. It especially received much attention in the area of image encryption.

T. Gopalakrishnan and S. Ramakrishnan [9] presented an image encryption method given by multiple chaotic maps. The method utilizes various keys for four-round encryption cycles. The method can be employed to encrypt grayscale images and color images. Y. Luo, et al. [10] demonstrated how a grouping of a Baker map and a logistic map can be used as a two-dimensional chaotic system that can encrypt images. Li et al. [11] designed an encryption system that uses key streams depending on the input image. The system employs a chaotic system and hash function to achieve its goals. Nestor Tsafack et al. [12]

published a novel image encryption method that is formulated by a new chaotic map with dynamic analysis for the health internet of things.

Fractal calculus [13–15] (local fractional calculus) plays a major role in wide fields of science and engineering such as geology, economics, chemical physics, control theory, and fluid flow [16,17]. Fractal calculus has been utilized to generalize chaotic systems, chaotic maps, optimization, operation, and other theories of chaos [18–22]. Chaos is an extensive stimulating occurrence in nonlinear dynamical systems, which has been widely investigated through the recent period. Different researchers have proposed various new chaotic maps that have more security [23,24]. Additionally, cryptographic algorithms utilize common chaotic models such as logistic maps [25]. G. Zhang et al. [26] proposed a new chaotic logistic map called tent delay-sine cascade (TDSCL) for image encryption. The algorithm of this image encryption achieves confusion and diffusion. Y. Zhang et al. [27] proposed a new fractional-order logistic map based on S-boxes. The proposed fractional-order chaotic system provided a larger key space to make the image encryption more efficient against crypto-analytic attacks. The proposed S-boxes were used for the encryption confusion process.

Fractal calculus models are now widely used in image security due to their infinite boundaries property [28]. Sangavi and Thangavel [29] proposed an image encryption algorithm that employs fractal geometry of colored images. This proposed image encryption algorithm has a large key space with complex behavior to produce the confusion behavior. The confusion behavior of the proposed model helps to shuffle the image's pixel positions to avoid correlation between image pixels.

This paper studies the dynamics of a new fractal complex logistic (FCL) map and then investigates its performance as an essential seed for image encryption algorithms. Firstly, the dynamical characteristics of the FCL, including the equilibrium point, the geometric properties, and chaotic behaviors, are discovered. Simulation analysis proves that the FCL generates wider chaotic regions and ensures the pseudo-randomness of this map. Secondly, to demonstrate the efficiency of the FCL map in real applications, we employ it in an image encryption algorithm. In this algorithm, the fractal complex sequences of the FCL are used to alter the image's pixels to drastically increase the resistance to decryption attacks. The output findings indicate that our proposed algorithm could effectively encrypt various kinds of images with a high level of security performance.

The rest of this paper is organized as follows: Section 2 introduces the fractal complex logistic map and then defines its structure, fixed points, and geometric properties. Furthermore, this section proposes a new encryption algorithm to demonstrate the efficiency of the map. Section 3 analyzes the performance of the proposed encryption algorithm. Finally, the conclusions are presented in Section 4.

2. Materials and Methods

The proposed mathematical FCL map model that is used for the image encryption algorithm is given as follows [13–15]:

2.1. Fractal Complex Logistic (FCL) Map

Let $C_\alpha(a,b), \alpha \in (0,1]$ be a fractal set and let $f \in C_\alpha$. For $\epsilon > 0$ and $|\chi - \chi_0| < \delta$; the limit

$$f^{(\alpha)}(\chi_0) := \Delta^{(\alpha)} f(\chi_0) = lim_{\chi \to \chi_0} \frac{\Gamma(\alpha+1)(f(\chi) - f(\chi_0))}{(\chi - \chi_0)^\alpha} \tag{1}$$

is finite and exists. Here, the gamma function is defined as $\Gamma(z) = \int_0^\infty x^{(z-1)}\, e^{-x} dx$.

Note that

$$\Delta^{(2\alpha)} f(\chi_0) = \Delta^{(\alpha)}\left(\Delta^{(\alpha)} f(\chi_0)\right), \Delta^{(3\alpha)} f(\chi_0) = \Delta^{(\alpha)}\left(\Delta^{(\alpha)}\left(\Delta^{(\alpha)} f(\chi_0)\right)\right) \dots$$

The 2D-fractal derivative is suggested for a complex function $f(z)$, where $z = x + iy$ expressing on a fractal set of $C_\alpha(U), U \subset C$ (the complex plane), as follows [30]:

$$\Delta^{(\alpha)} f(z_0) = lim_{z \to z_0} \frac{\Gamma(\alpha+1)(f(z) - f(z_0))}{(z - z_0)^\alpha}, z \in U, \tag{2}$$

where the difference operator is formulated by

$$D^\alpha f(z_0) = \Gamma(\alpha+1)(f(z) - f(z_0)), z \in U. \tag{3}$$

For instance, $f(z^\alpha) = z^{\alpha n}$, has a fractal derivative

$$\Delta^{(\alpha)} z^{n\alpha} = \frac{\Gamma(\alpha n + 1)}{\Gamma(\alpha(n-1)+1)} z^{(n-1)\alpha}. \tag{4}$$

Hence, generally, for an analytic function f in a complex domain, we obtain the construction of a fractal derivative, as follows Theorem 9 [30]:

$$\Delta^{(\alpha)} f(z) = \sum_{n=1}^{\infty} \frac{\Phi_n(a,b)}{\Gamma(\alpha(n-1)+1)} z^{(n-1)\alpha}, \tag{5}$$

where f is located in some fractal set.

The fractal integral can be recognized by the discrete formula

$$J^{(\alpha)} f(z) = \frac{1}{\Gamma(1+\alpha)} \sum_{n=1}^{k} f(z_n)(\delta z_n)^\alpha, \tag{6}$$

where $\delta z_n := z_n - z_{n-1}$.

Proposition 1. *Consider the fractal equation*

$$\Delta^{(\alpha)} f(z) = F(z_n, f(z_n)). \tag{7}$$

Then, the solution becomes as follows

$$f(z) = f(z_0) + \frac{1}{\Gamma(1+\alpha)} \sum_{n=1}^{k} F(z_n, f(z_n))(z_n - z_{n-1})^\alpha. \tag{8}$$

2.2. Structure of FCL Map

By using the difference fractal operator, we proceed to define the FCL map. A complex logistic map is given by the structure

$$z_{n+1} = \aleph z_n(1 - z_n), \quad z \in C, \quad \aleph \in [0,4], \tag{9}$$

where $\aleph$ is the control parameter. However, the above discrete complex logistic map can be converted to the continuous type, as follows:

$$z^\bullet = \aleph z(1 - z), \quad z \in C, \quad \aleph \in [0,4], \tag{10}$$

By considering, $z = \chi + i\Upsilon$, we have the system

$$\chi^\bullet = \aleph\chi - \aleph\left(\chi^2 - \Upsilon^2\right) \tag{11}$$

$$\Upsilon^\bullet = \aleph\Upsilon - 2\aleph\chi\Upsilon. \tag{12}$$

By considering the discrete fractal operator, we have the following FCL map,

$$\Gamma(\alpha+1)(z_{n+1}-z_n)=\Gamma(\alpha+1)(\aleph z_n(1-z_n)-z_n). \tag{13}$$

Consequently, we obtain the FCL map

$$D^\alpha z_{n+1}=\Gamma(\alpha+1)(\aleph z_n(1-z_n)-z_n), \alpha\in[0,1], \tag{14}$$

which corresponds to the dynamic system

$$D^\alpha \chi=\Gamma(\alpha+1)\Big((\aleph-1)\chi-\aleph\Big(\chi^2-\Upsilon^2\Big)\Big) \tag{15}$$

$$D^\alpha \Upsilon=\Gamma(\alpha+1)((\aleph-1)\Upsilon-2\aleph\chi\Upsilon). \tag{16}$$

It is clear that when $\alpha=0$, System (16) reduces to System (12).

2.3. *Properties of FCL Map*

2.3.1. Equilibrium Points

Consider the following two equations

$$f_1:\Gamma(\alpha+1)\Big((\aleph-1)\chi-\aleph\Big(\chi^2-\Upsilon^2\Big)\Big)=0 \tag{17}$$

$$f_2:\Gamma(\alpha+1)((\aleph-1)\Upsilon-2\aleph\chi\Upsilon)=0. \tag{18}$$

Now, we have the following set

$$\Xi:=\left\{\Sigma_0(0,0),\Sigma_1(\frac{\aleph-1}{\aleph},0),\Sigma_2(\frac{\aleph-1}{2\aleph},\frac{+i(\aleph-1)}{2\aleph}),\Sigma_3\left(\frac{\aleph-1}{2\aleph},\frac{-i(\aleph-1)}{2\aleph}\right)\right\}. \tag{19}$$

The Jacobian matrix becomes

$$J_{\Sigma(\chi,\Upsilon)}=\begin{pmatrix}\partial_\chi(f_1) & \partial_\Upsilon(f_1)\\ \partial_\chi(f_2) & \partial_\Upsilon(f_2)\end{pmatrix}$$

$$=\begin{pmatrix}\Gamma(\alpha+1)((\aleph-1)-2\chi) & 2\aleph\Gamma(\alpha+1)\Upsilon\\ -2\aleph\Gamma(\alpha+1)\Upsilon & \Gamma(\alpha+1)(\aleph-1-2\aleph\chi)\end{pmatrix}.$$

Note that

$$J_{\Sigma(0,0)}=\begin{pmatrix}\Gamma(\alpha+1)(\aleph-1) & 0\\ 0 & \Gamma(\alpha+1)(\aleph-1)\end{pmatrix},$$

which leads to two equal Eigenvalues $\lambda_{1,2}=\Gamma(\alpha+1)(\aleph-1)$.

Now, we obtain the equilibrium points of System (14) by resolving the next system

$$\chi=\Gamma(\alpha+1)\Big((\aleph-1)\chi-\aleph\Big(\chi^2-\Upsilon^2\Big)\Big) \tag{20}$$

$$\Upsilon=\Gamma(\alpha+1)((\aleph-1)\Upsilon-2\aleph\chi\Upsilon). \tag{21}$$

The set of solutions is formulated as follows:

$$\Theta:=\left\{\left(\frac{-(-\aleph b+b+1)}{2\aleph},\frac{\sqrt{-\frac{((\aleph-1)b-1)^2}{\aleph}}}{2\sqrt{\aleph}}\right),\left(\frac{(\aleph-1)b-1}{\aleph},0\right),(0,0)\right\}, \tag{22}$$

where $b:=\Gamma(\alpha+1)$.

2.3.2. Geometric Properties

Consider an FCL map that is defined on a fractal set of the open unit disk $:=\{z\in C:|z|<1\}$. To study the geometric properties of the FCL map, we need the following definition:

Definition 1. *Two analytic functions, f, g, are subordinated in U denoted by $f \prec g$ if they occur as the function $\omega \in U, |\omega| \leq |z|$ satisfying $f(z) = g(\omega(z))$. They are majorized $(f \ll g)$ if $f(z) = \omega(z)g(z)$, which is equivalent to $|a_n| \leq |b_n|$ where a_n and b_n are the coefficients of f and g, respectively.*

The following shows the geometric behavior of the logistic map and the FCL map in terms of the limacon map $L_\wp(z) = (1 + \wp z)^2$.

Proposition 2. *Consider the logistic map $F(z) = \aleph z(1 - z)$ and its fractal the FCL map $F_\alpha = \aleph\Gamma(1 + \alpha)z(1 - z)$, where $\aleph \neq 0$.*

1. *If $|\aleph| \leq 2\wp^2, 0 < \wp \leq 1/2$ then $F(z) \prec zL'_\wp(z), 0.1 < |z| < 0.3$;*
2. *If $|\aleph| \leq \frac{2\wp^2}{\Gamma(1+\alpha)}, 0 < \wp \leq 1/2$ then $F_\alpha(z) \prec zL'_\wp(z), 0.1 < |z| < 0.3$;*

Proof. Clearly, we have

$$zL'_\wp(z) = 2\wp z(1 + \wp z), z \in U, \tag{23}$$

which is the starlike analytic function in U, whenever $\wp \in (0, 1/2]$ (see [22]). Utilizing the first condition of the theorem, we obtain

$$F(z) \ll zL'_\wp(z), \wp \in (0, 1/2]. \tag{24}$$

Similarly, the second condition implies that

$$F_\alpha(z) \ll zL'_\wp(z), \wp \in (0, 1/2]. \tag{25}$$

Since $F'(0) \neq 0$ in view of Corollary 2 [31], we obtain the first assertion

$$F(z) \prec zL'_\wp(z), \wp \in (0, 1/2], \aleph \neq 0. \tag{26}$$

In the same manner, we obtain the second inequality

$$F_\alpha(z) \prec zL'_\wp(z), \wp \in (0, \frac{1}{2}], \aleph \neq 0, \alpha \in \ < 0, 1 > . \tag{27}$$

The geometry of the logistic map and the fractal logistic map is dominated by a starlike function in the open unit disk U. Note that the analytic function $\phi(z)$is called starlike if and only if $R\left(\frac{z\phi'(z)}{\phi(z)}\right) > 0$. Proposition 2 yields a relation between the derivative of the logistic map (normal and fractal) and the second derivative of the limacon map, which represents to the convexity behavior the map following Theorem 3 [31]:

$$F'(z) \ll \left(zL'_\wp(z)\right)', |z| < 3 - \sqrt{8}; \tag{28}$$

and

$$F'_\alpha(z) \ll \left(zL'_\wp(z)\right)', |z| < 3 - \sqrt{8}. \tag{29}$$

□

2.4. The FCL Map Algorithm

From Proposition 1, we use Equation (14) to obtain

$$J^{(\alpha)}(D^\alpha z_{n+1}) = J^{(\alpha)}(\Gamma(\alpha + 1)(\aleph z_n(1 - z_n) - z_n)), \tag{30}$$

$$z_{n+1} = (z_0) + \frac{1}{\Gamma(1 + \alpha)} \sum_{n=0}^{k-1} (\Gamma(\alpha + 1)(\aleph z_n(1 - z_n) - z_n))(z_{n+1} - z_n)^\alpha \tag{31}$$

$$= z_0 + \sum_{n=1}^{k} (\aleph z_{n-1}(1 - z_{n-1}) - z_{n-1})(z_n - z_{n-1})^{\alpha}, \tag{32}$$

where $0 \le |z_0| < |z_1| < \ldots < |z_n| < 1$. It is clear that the map z_{n+1} depends on the previous information, since there is a fractional kernel $(z_n - z_{n-1})^{\alpha}$.

Figure 1 illustrates the behavior of the proposed FCL map by depicting its bifurcation diagram. From the bifurcation diagram (Figure 1a), it is obvious that the system with $\alpha = 0.5$ shows a period-doubling bifurcation with a complete absence of chaotic behavior for the range of $\aleph \in [2, 4]$. Meanwhile, Figure 1b shows that the system with $\alpha = 0.6$ enters into chaotic behavior by period-doubling bifurcation with a complete absence of periodic windows, mainly where $\aleph \in (3.7, 4]$.

Furthermore, Figure 2 illustrates the randomness of chaotic sequences of the FCL map by using the statistical package NIST SP800-22, which contains 16 empirical tests. Here, a binary sequence has been taken from the FCL map with a length of 1,000,000 bits to employ as the testing input. The sequence can be considered as random when the obtained p-value is larger than 0.01. As can be seen in Figure 2a,b, the chaotic sequence generated by the FCL map can pass all the sub-tests. That means this map is suitable for image encryption algorithms.

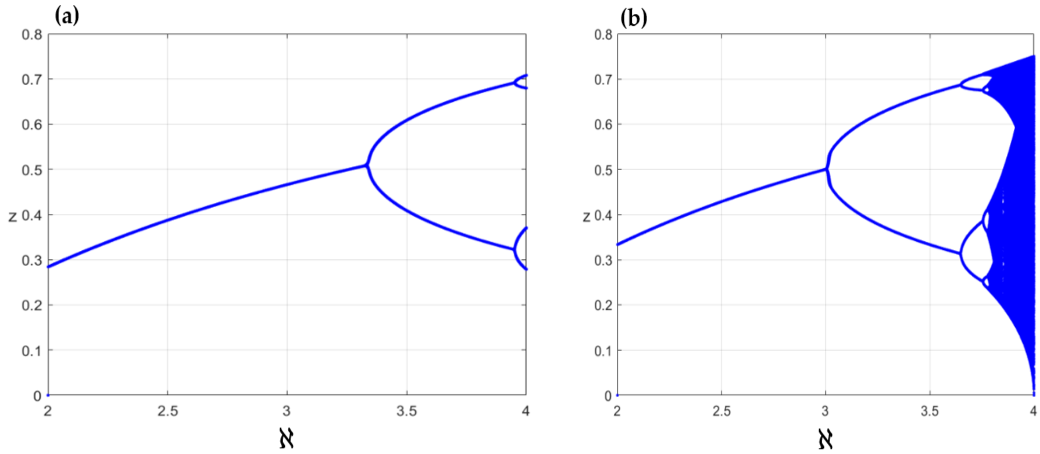

Figure 1. Bifurcation diagram of the FCL map with the initial value $z_0 = 0.1$: (**a**) α = 0.5; (**b**) α = 0.6.

2.5. The Encryption Method

The steps for symmetric image encryption by the proposed method are as follows:

1. Read the input image (I), and convert the values to a 52-bit binary stream using IEEE 754 float standard; then, the digital numbers from 33rd to 40th in each binary stream are used;
2. Set the secret key, which is mainly generated from the initial value and control parameters of the FCL map, as illustrated in Figure 3;
3. Use proposed FCL to generate the chaotic sequences $Z = \{|z_1|, |z_2|, |z_3|, \ldots\ldots, |z_n|\}$. Note that for all n, $0 \le |z_n| < 1$;
4. Start the confusion of the input image by changing the position of pixels by using conditional shift, which stops the algorithm for any shifting cases to make the variable z outside the open unit disk;
5. Convert the chaotic sequences to binary numbers using IEEE 754 float standard in which each chaotic output produces eight binary numbers;
6. Start the diffusion of the confusing image to obtain the encrypted image by using the XOR operation between the binary input image and the binary form of chaotic sequence as: I_x(i) = bitxor (Ib(i),(z(i));
7. Convert I_x into a two-dimensional encrypted image (Ie);
8. The previous steps are applied in reverse to decrypt the image.

The bifurcation diagram is used to illustrate the behavior of the proposed chaotic maps through the distribution of iterates z_n versus the control parameter $\aleph$. Essentially, the FCL map can be governed by two parameters (z_n and $\aleph$), and the map has a random behavior that is represented by an alteration in the values of either or both of the aforementioned parameters (z_n and $\aleph$). The key idea of applying the FCL map in image encryption is based on a repetition function in which the previous output value of z_{n-1} will influence the current value of z_n.

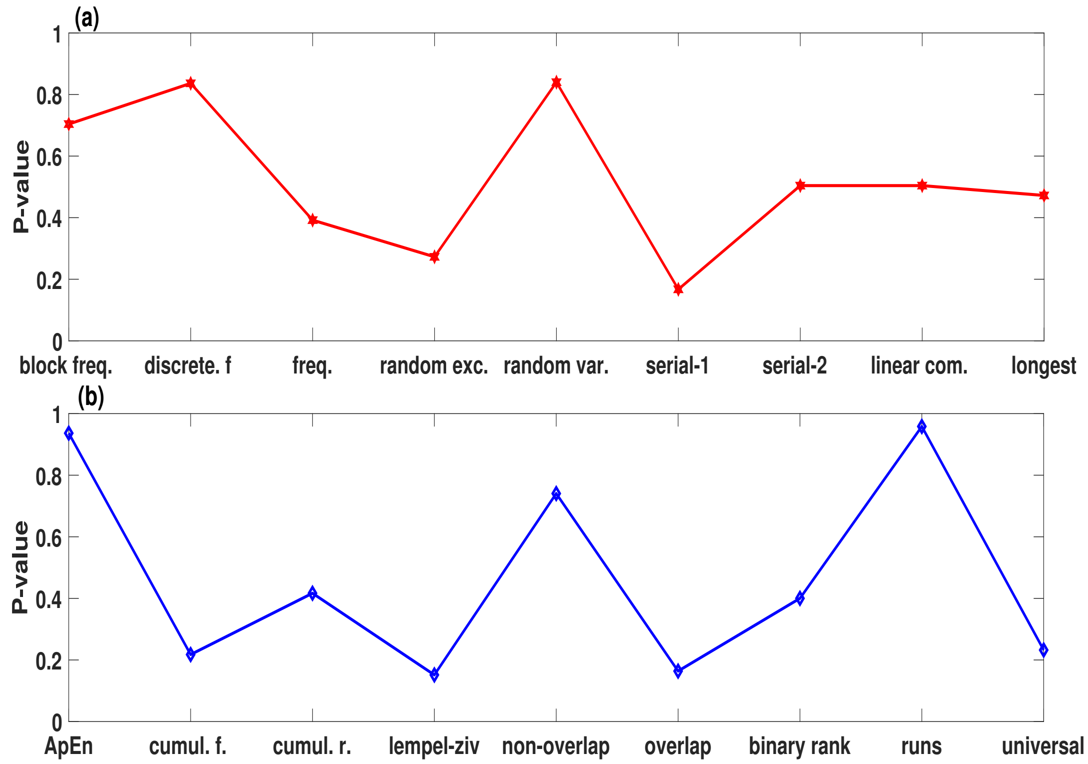

Figure 2. The NIST SP800-22 result: (**a**,**b**) represent the statistical sub-tests of the chaotic sequence generated by FCL map with the initial value $z_0 = 0.1$ and the parameters α=0.6 and $\aleph = 3.72$.

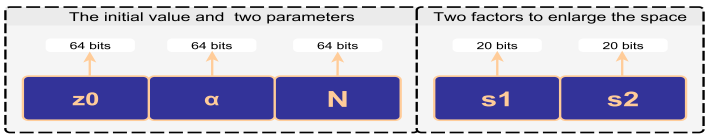

Figure 3. The secret key structure, which consists of five parts with 232 bits.

3. Results

Here, the performance of the proposed image encryption model with the initial value $z_0 = 0.1$ and the parameters α=0.6 and $\aleph = 3.72$ is demonstrated using standard test images, commonly known as Barbara, sketch, handwriting, and Lena, with the size 256×256. We employed statistical analyses to assess the model's performance. The experiments were undertaken using MATLAB R2021a with Windows 10, 8.00 GB RAM, Intel(R) Core (TM) i7-6700HQ CPU @2.60 GHz.

3.1. Encrypting Different Kinds of Images

To demonstrate the ability of the proposed symmetric image encryption algorithm for ciphering different types of images, Figure 4 depicts the encryption results with uniformly distributed histograms of various kinds of images. The first column depicts the animal sketches, handwriting, and Lena images. The second column plots the histograms of these images. Meanwhile, the third column plots the encryption of the animal sketches, the handwriting, and Lena images, respectively. Finally, the fourth column depicts histograms of the encrypted images. It can be seen from these results that the proposed encryption algorithm can effectively encrypt various kinds of images.

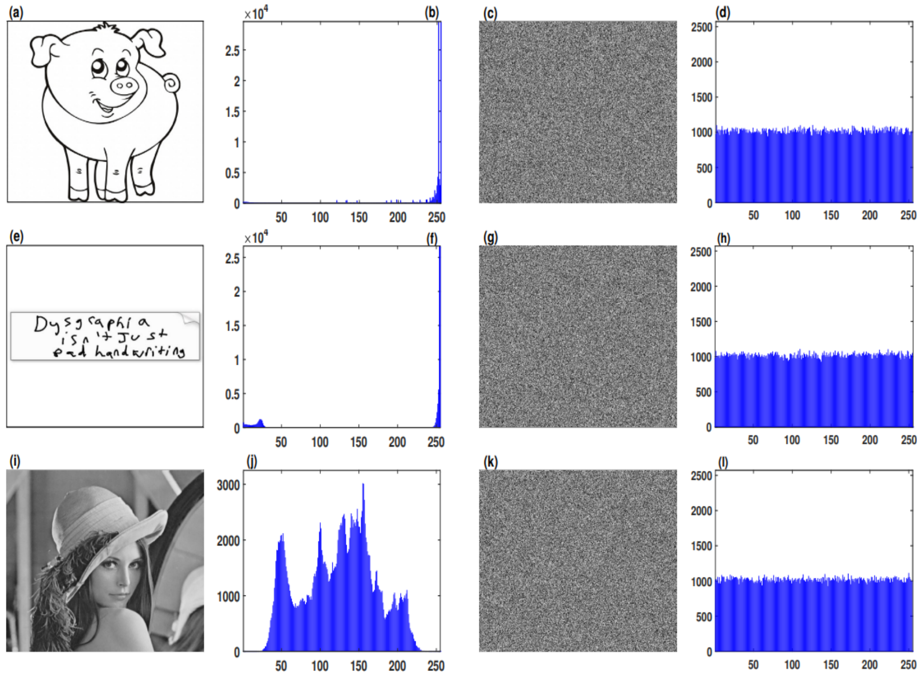

Figure 4. Simulation results of the proposed encryption model: (**a**,**e**,**i**) are the plain-text images; (**b**,**f**,**j**) are the histogram of the plain-text images; (**c**,**g**,**k**) are the encrypted images; (**d**,**h**,**l**) are the histogram of the encrypted images.

3.2. Information Entropy Analysis

The entropy measures the degree of n predictability of information. The information entropy is calculated for encrypted images to measure the degree of uncertainty; however, any certain degree of predictability will threaten the encryption security [32]. Table 1 is an assessment of the data entropy of the plaintext and the encrypted image for the suggested FCL map model.

Table 1. Comparison of information entropy between plain and encrypted images.

Images	**Plain**	**Encrypted**
Barbara	7.8056	7.9785
Baboon	7.3583	7.9995
Boat	7.1901	7.9865
Lena	7.7481	7.9995
Average	7.5255	7.9910

Table 2 illustrates the comparison of information entropy of several algorithms using Lena as a test image. As can be seen, the encrypted image produced by our FCL map algorithm is close to the value of 8, which indicates that the chaotic sequences generated by the proposed FCL map model have complex dynamic behaviors.

Table 2. Comparison of data entropy of various encryption procedures utilizing Lena.

Encryption Algorithm	Entropy
Wang and Guo 2014 [33]	7.9977
Liu Lingfeng 2016 [34]	7.9995
Li, Tao 2020 [32]	7.9894
Zhang Fangfanf 2021 [35]	7.9994
Proposed FCL map model	7.9995

3.3. Correlation Analysis

The aim of image encryption algorithms is to decrease the correlation among the image pixels in order to make the prediction of any given pixel from its neighbors more difficult. The correlation between two adjacent pixels can be calculated by Equation (33) [12]:

$$\varrho(S,T) = \frac{Corr(S,T)}{\sqrt{D(S)}\sqrt{D(T)}} \tag{33}$$

where S, T are pixel values of two adjacent pixel positions and n is the total number of adjacent pixels, where

$$Corr(S,T) = \frac{1}{n}\sum_{i=1}^{n}(S_i - E(S))(T_i - E(T)) \tag{34}$$

$$D(S) = \frac{1}{n}\sum_{i=1}^{n}(S_i - E(S))^2 \tag{35}$$

$$E(S) = \frac{1}{n}\sum_{i=1}^{n} S_i \tag{36}$$

Table 3 demonstrates the correlation coefficients of the original and encrypted images. The calculated correlation coefficients illustrate that the correlation coefficients of the encrypted images are close to zero, which proves that the FCL map of the proposed model can effectively decrease the correlation among adjacent pixels of the original images.

Table 3. The correlation between plain and encrypted images. Horizontal (H), vertical (V), and diagonal (D) indicate the correlation directions.

Image		Plain	Encrypted
Barbara	H	0.8135	−0.0006
	V	0.8708	0.0025
	D	0.9294	−0.0315
Baboon	H	0.9371	0.0007
	V	0.9485	0.0006
	D	0.9325	−0.0459
Boat	H	0.9371	0.0045
	V	0.9324	0.0006
	D	0.9342	0.0218
Lena	H	0.9387	0.0045
	V	0.9812	0.0016
	D	0.97261	0.0017

Table 3. *Cont.*

Image		Plain	Encrypted
Average	H	0.9066	0.0025
	V	0.93322	0.0013
	D	0.9421	−0.0134

Taking the average values for testing images as an experimental object, the comparison of correlation between different encryption algorithms in the horizontal (H), vertical (V), and diagonal (D) directions are illustrated in Table 4.

The encryption time is used to measure the efficiency of the encryption algorithm and it depends on certain parameters such as CPU cycles and memory usage. The image encryption time of the proposed algorithm is the time that it takes to encrypt the input image using proposed algorithm. In this study, the average encryption time of test images was measured using the stopwatch timer MATLAB functions, tic and toc.

The test results of the encryption speeds of different image encryption algorithms are also included in Table 4. Because the source codes of the encryption algorithms illustrated in Table 4 are not publicly available, all encryption times are reported in Table 4 according to what is given by these references. The proposed FCL map model has the fastest encryption speed with the lowest time complexity, so it can be used in real-time image applications such as video stream cyphering.

Table 4. Comparison of the encryption time (second), and the correlation of different encryption algorithms using average values for testing images. Horizontal (H), vertical (V), and diagonal (D) indicate the correlation directions.

Algorithm	Encryption Time (s)		Encrypted
Hua et al. 2015 [36]	0.2338	H	0.0024
		V	−0.0086
		D	0.0402
Tong et al. 2015 [37]	0.1900	H	0.0038
		V	0.0058
		D	0.0133
Liu, Lingfeng 2016 [34]	0.0659	H	0.0021
		V	0.0046
		D	0.0033
Li, Tao 2020 [32]	0.4604	H	0.0033
		V	0.0011
		D	0.0008
Proposed FCL map model	0.0589	H	0.0025
		V	0.0013
		D	−0.0134

3.4. Key Sensitivity Analysis

The image encryption algorithm primarily depends on the key sensitivity. Even one bit change to the key combinations can produce a different encrypted image. The proposed FCL map model is proven to be highly sensitive to changes in the encryption key. As shown in Figure 5, the model is sensitive to changes as small as one bit. As a result, if the decryption key is slightly changed, the decryption algorithm will not be able to correctly decrypt the image.

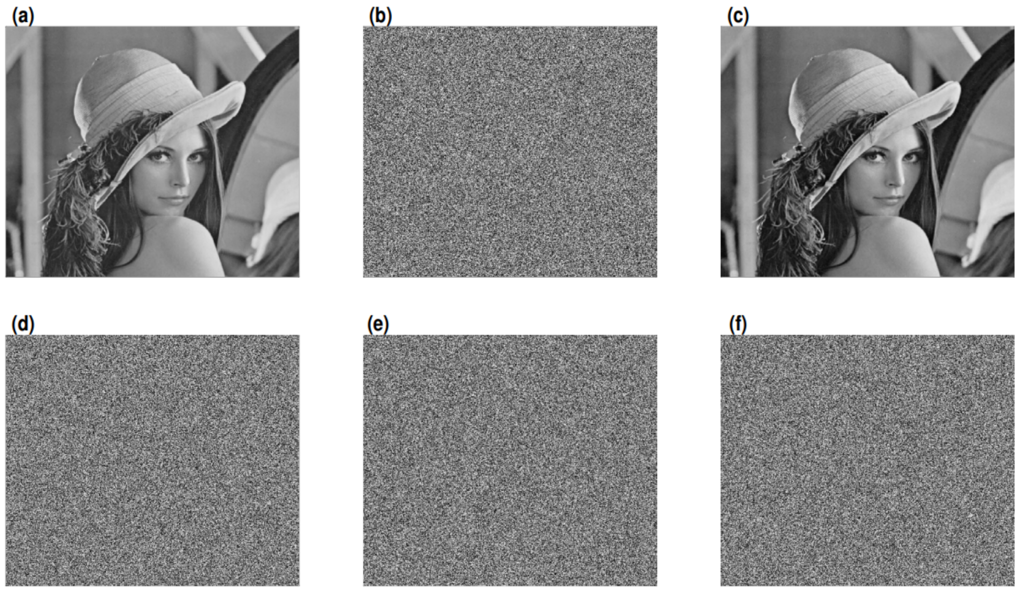

Figure 5. Key sensitivity analysis: (**a**) plain-image, (**b**) the encrypted image, (**c**) the decrypted image with the right key, (**d**–**f**) the decrypted images with wrong keys.

3.5. Differential Attack Analysis

To check the ability of our encryption algorithm to resist differential attack, we use the two metrics: the NPCR and UACI, which are the abbreviations for (Number of Pixel Change Rate) and (Unified Average Changing Intensity), respectively. The NPCR indicates the changed pixel numbers in the cipher image for which only one pixel is changed in the plain image. Meanwhile, the UACI refers to the average value of difference between two cipher images. The NPCR and UACI are given by:

$$NPCR = \frac{\sum_{i,j} A(i,j)}{H} \times 100\% \tag{37}$$

$$UACI = \frac{1}{H}\left[\sum_{i,j} \frac{|G1(i,j) - G2(i,j)|}{255}\right] \times 100\% \tag{38}$$

where $A(j,j) = \begin{cases} 1, & (G1(i,j) \neq G2(i,j)) \\ 0, & otherwise \end{cases}$, where $G1$ and $G2$ are two pixels with the same coordinates and H represents the image size. Table 5 shows the NPCR and UACI for the proposed FCL map encryption algorithm. Furthermore, the comparisons of NPCR and UACI for the "Lena" image with other algorithms are presented in Table 6. From the results shown in Tables 5 and 6, it is clear that our encryption algorithm has superior or competitive performance in defending from differential attacks (which are also called chosen-plaintext attacks).

Table 5. The NPCR and UACI of the proposed model for the given testing images.

Image	NPCR	UACI
Barbara	0.9967	0.3343
Baboon	0.9966	0.3396
Boat	0.9968	0.3358
Lena	0.99 68	0.3312

Table 6. Comparison of the NPCR and UACI for the testing image "Lena".

Algorithm	NPCR	UACI
Liu Lingfeng 2016 [34]	0.9949	0.3156
Li Tao [32]	0.9949	0.3156
Zhang Fangfang 2021 [35]	0.9960	0.3347
Proposed FCL map model	0.9968	0.3312

3.6. Noise And Data Loss Analysis

Several types of noise and data lose can spoil the encrypted images. Therefore, image encryption algorithms should be able to resist these kinds of noise and data lose. The first and second columns of Figure 6 show the quality results of the recovered image when the encrypted image undergoes Gaussian noise with 5% density, as well as salt and pepper noise with 12% density. It can be observed that, although the encrypted images contain noise, the recovered images have most of the visual information of the original images.

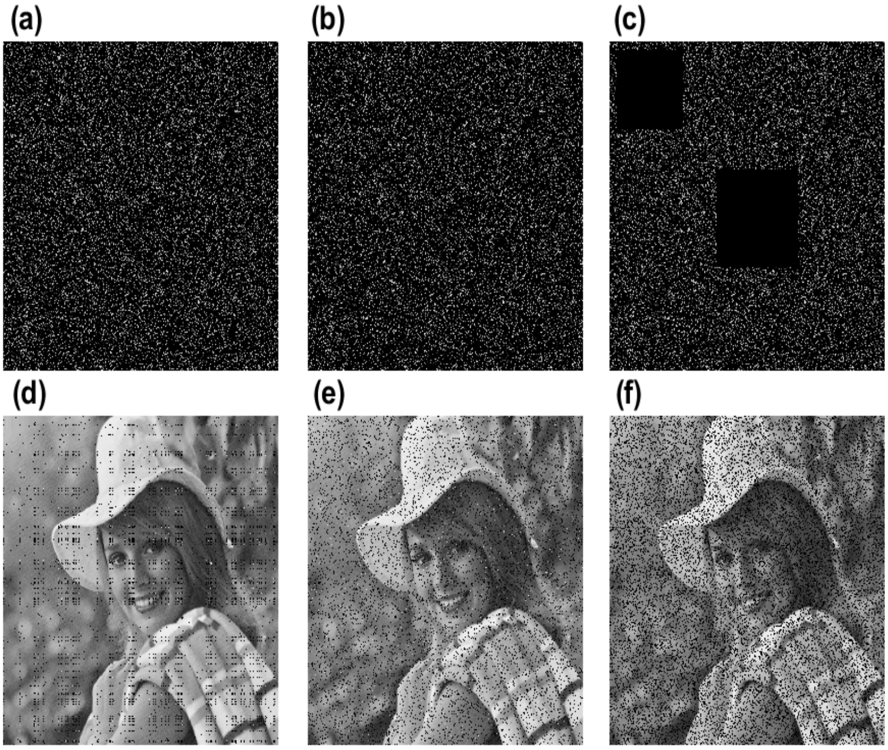

Figure 6. Noise and data loss analysis: (**a**,**d**) plot the encrypted image with 5% Gaussian noise and the decrypted image, respectively; (**b**,**e**) plot the encrypted image with 12% salt and pepper noise and the corresponding decrypted image, respectively; (**c**,**f**) plot the encrypted image with 15% data loss and the decrypted image, respectively.

4. Conclusions

This paper studied the dynamics of a new fractal complex logistic (FCL) map, including the equilibrium point, geometric properties, and chaotic behaviors. Furthermore, the randomness of the FCL map was examined by the statistical test NIST SP800-22, which revealed that the map is suitable for cryptographical applications. To further investigate the FCL map, we designed a simple symmetric image encryption algorithm that used the FCL map to generate chaotic sequences. Simulation results demonstrated the efficiency of the encryption algorithm for the encryption of various kinds of images. We also analyzed the information entropy, correlation coefficients between adjacent pixels, the sensitivity of the key, and the resistance to chosen-plaintext attack. The analysis results show that the proposed encryption algorithm has a high-security level and has superiority over several encryption algorithms. That indicates the effectiveness of the FCL map in such applications.

Author Contributions: Conceptualization, H.N. and N.M.G.A.-S.; methodology, H.N.; software, A.K.F.; validation, H.N., N.M.G.A.-S. and, M.N.M.; formal analysis, H.N.; investigation, M.N.M.; writing—original draft preparation, H.N.; writing—review and editing, N.M.G.A.-S.; visualization, A.K.F.; supervision, S.J.O.; project administration, S.J.O.; funding acquisition, S.J.O. All authors have read and agreed to the published version of the manuscript.

Funding: This research is funded by University of Malaya International Collaboration Grant ST008-2022.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research is funded by University of Malaya International Collaboration Grant ST008-2022(UM.0001082/HRU.OP). We thank the reviewers and associate editor for their comments which improved this manuscript.

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

References

1. Pourasad, Y.; Ranjbarzadeh, R.; Mardani, A. A new algorithm for digital image encryption based on chaos theory. *Entropy* **2021**, *23*, 341. [CrossRef] [PubMed]
2. Askar, S.S.; Karawia, A.A.; Alshamrani, A. Image Encryption Algorithm Based on Chaotic Economic Model. *Math. Probl. Eng.* **2015**, *2015*, 341729. [CrossRef]
3. Tang, Z.; Yang, Y.; Xu, S.; Yu, C.; Zhang, X. Image encryption with double spiral scans and chaotic maps. *Secur. Commun. Netw.* **2019**, *2019*, 8694678. [CrossRef]
4. Erkan, U.; Toktas, A.; Toktas, F.; Alenezi, F. 2D eπ-map for image encryption. *Inf. Sci.* **2022**, *589*, 770–789. [CrossRef]
5. Erkan, U.; Toktas, A.; Enginoğlu, S.; Akbacak, E.; Thanh, D.N. An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimed. Tools Appl.* **2022**, *81*, 7365–7391. [CrossRef]
6. Toktas, A.; Erkan, U. 2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm. *Neural Comput. Appl.* **2022**, *34*, 4295–4319. [CrossRef]
7. Martsenyuk, V.; Augustynek, K.; Urbas, A. On qualitative analysis of the nonstationary delayed model of coexistence of two-strain virus: Stability, bifurcation, and transition to chaos. *Int. J.-Non-Linear Mech.* **2021**, *128*, 103630. [CrossRef]
8. Al-Saidi, N.M.; Younus, D.; Natiq, H.; Ariffin, M.R.K.; Asbullah, M.A.; Mahad, Z. A new hyperchaotic map for a secure communication scheme with an experimental realization. *Symmetry* **2020**, *12*, 1881. [CrossRef]
9. Gopalakrishnan, T.; Ramakrishnan, S. Chaotic image encryption with hash keying as key generator. *IETE J. Res.* **2017**, *63*, 172–187. [CrossRef]
10. Luo, Y.; Yu, J.; Lai, W.; Liu, L. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimed. Tools Appl.* **2019**, *78*, 22023–22043. [CrossRef]
11. Aslam, M.N.; Belazi, A.; Kharbech, S.; Talha, M.; Xiang, W. Fourth order MCA and chaos-based image encryption scheme. *IEEE Access* **2019**, *7*, 66395–66409.
12. Tsafack, N.; Sankar, S.; Abd-El-Atty, B.; Kengne, J.; Jithin, K.; Belazi, A.; Mehmood, I.; Bashir, A.K.; Song, O.-Y.; Abd El-Latif, A.A. A new chaotic map with dynamic analysis and encryption application in internet of health things. *IEEE Access* **2020**, *8*, 137731–137744. [CrossRef]
13. Yang, X.-J. *Advanced Local Fractional Calculus and Its Applications*; World Science Publisher: New York, NY, USA, 2012.
14. Yang, X.-J.; Baleanu, D.; Srivastava, H.M. *Local Fractional Integral Transforms and Their Applications*; Academic Press: Cambridge, MA, USA, 2015.
15. Yang, X.-J.; Baleanu, D.; Srivastava, H. Local fractional similarity solution for the diffusion equation defined on Cantor sets. *Appl. Math. Lett.* **2015**, *47*, 54–60. [CrossRef]
16. Kilbas, A.A.; Srivastava, H.M.; Trujillo, J.J. *Theory and Applications of Fractional Differential Equations*; Elsevier: Amsterdam, The Netherlands, 2006; Volume 204.
17. Zhou, Y.; Wang, J.; Zhang, L. *Basic Theory of Fractional Differential Equations*; World Scientific: Singapore, 2016.
18. Ibrahim, R.W.; Altulea, D. Controlled homeodynamic concept using a conformable calculus in artificial biological systems. *Chaos Solitons Fractals* **2020**, *140*, 110132. [CrossRef]
19. Jalab, H.A.; Ibrahim, R.W.; Hasan, A.M.; Karim, F.K.; Al-Shamasneh, A.a.R.; Baleanu, D. A New Medical Image Enhancement Algorithm Based on Fractional Calculus. *CMC-Comput. Mater. Contin.* **2021**, *68*, 1467–1483. [CrossRef]
20. Ibrahim, R.W. A new image.)denoising model utilizing the conformable fractional calculus for multiplicative noise. *SN Appl. Sci.* **2020**, *2*, 1–11. [CrossRef]

21. Ramakrishnan, B.; Nkandeu Kamdeu, P.Y.; Natiq, H.; Pone, J.R.M.; Karthikeyan, A.; Kingni, S.T.; Tiedeu, A. Image encryption with a Josephson junction model embedded in FPGA. *Multimed. Tools Appl.* **2022**, *81*, 23819–23843. [CrossRef]
22. Meshram, C.; Ibrahim, R.W.; Obaidat, M.S.; Sadoun, B.; Meshram, S.G.; Tembhurne, J.V. An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps. *Soft Comput.* **2021**, *25*, 8905–8920. [CrossRef]
23. Ji, Y.; Lai, L.; Zhong, S.; Zhang, L. Bifurcation and chaos of a new discrete fractional-order logistic map. *Commun. Nonlinear Sci. Numer. Simul.* **2018**, *57*, 352–358. [CrossRef]
24. Natiq, H.; Al-Saidi, N.M.G.; Said, M.R.M.; Kilicman, A. A new hyperchaotic map and its application for image encryption. *Eur. Phys. J. Plus* **2018**, *133*, 6. [CrossRef]
25. Zahmoul, R.; Ejbali, R.; Zaied, M. Image encryption based on new Beta chaotic maps. *Opt. Lasers Eng.* **2017**, *96*, 39–49. [CrossRef]
26. Zhang, G.; Ding, W.; Li, L. Image encryption algorithm based on tent delay-sine cascade with logistic map. *Symmetry* **2020**, *12*, 355. [CrossRef]
27. Zhang, Y.-Q.; Hao, J.-L.; Wang, X.-Y. An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map. *IEEE Access* **2020**, *8*, 54175–54188. [CrossRef]
28. Veeman, D.; Natiq, H.; Al-Saidi, N.M.; Rajagopal, K.; Jafari, S.; Hussain, I. A New Megastable Chaotic Oscillator with Blinking Oscillation terms. *Complexity* **2021**, *2021*, 5518633. [CrossRef]
29. Sangavi, V.; Thangavel, P. An image encryption algorithm based on fractal geometry. *Procedia Comput. Sci.* **2019**, *165*, 462–469. [CrossRef]
30. Cattani, C.; Srivastava, H.M.; Yang, X.-J. *Fractional Dynamics*; De Gruyter Open Poland: Berlin, Germany, 2016.
31. Campbell, D.M. Majorization-subordination theorems for locally univalent functions, II. *Can. J. Math.* **1973**, *25*, 420–425. [CrossRef]
32. Li, T.; Du, B.; Liang, X. Image encryption algorithm based on logistic and two-dimensional lorenz. *IEEE Access* **2020**, *8*, 13792–13805. [CrossRef]
33. Wang, X.; Guo, K. A new image alternate encryption algorithm based on chaotic map. *Nonlinear Dyn.* **2014**, *76*, 1943–1950. [CrossRef]
34. Liu, L.; Miao, S. A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus* **2016**, *5*, 1–12. [CrossRef]
35. Zhang, F.; Zhang, X.; Cao, M.; Ma, F.; Li, Z. Characteristic Analysis of 2D Lag-Complex Logistic Map and Its Application in Image Encryption. *IEEE Multimed.* **2021**, *28*, 96–106. [CrossRef]
36. Hua, Z.; Zhou, Y.; Pun, C.-M.; Chen, C.P. 2D Sine Logistic modulation map for image encryption. *Inf. Sci.* **2015**, *297*, 80–94. [CrossRef]
37. Tong, X.J.; Wang, Z.; Zhang, M.; Liu, Y.; Xu, H.; Ma, J. An image encryption algorithm based on the perturbed high-dimensional chaotic map. *Nonlinear Dyn.* **2015**, *80*, 1493–1508. [CrossRef]