Title

Integrated Time-Fractional Diffusion Processes for Fractional-Order Chaos-Based Image Encryption

Journal

Sensors, 21(20)

ISSN

1424-8220

Authors

Ge, Fudong
Qin, Zufa
Chen, YangQuan

Publication Date

2021

DOI

10.3390/s21206838

Peer reviewed

sensors

MDPI

Article

Integrated Time-Fractional Diffusion Processes for Fractional-Order Chaos-Based Image Encryption

Fudong Ge [1,*,†], Zufa Qin [1] and YangQuan Chen [2]

[1] School of Computer Science, China University of Geosciences, Wuhan 430074, China; qzf@cug.edu.cn
[2] School of Engineering (MESA-Lab), University of California, Merced, CA 95343, USA; ychen53@ucmerced.edu
* Correspondence: gefd@cug.edu.cn; Tel.: +86-027-67883716
† Current address: No. 388 Lumo Road, Hongshan District, Wuhan 430074, China.

Abstract: The purpose of this paper is to explore a novel image encryption algorithm that is developed by combining the fractional-order Chua's system and the 1D time-fractional diffusion system of order $\alpha \in (0, 1]$. To this end, we first discuss basic properties of the fractional-order Chua's system and the 1D time-fractional diffusion system. After these, a new spatiotemporal chaos-based cryptosystem is proposed by designing the chaotic sequence of the fractional-order Chua's system as the initial condition and the boundary conditions of the studied time-fractional diffusion system. It is shown that the proposed image encryption algorithm can gain excellent encryption performance with the properties of larger secret key space, higher sensitivity to initial-boundary conditions, better random-like sequence and faster encryption speed. Efficiency and reliability of the given encryption algorithm are finally illustrated by a computer experiment with detailed security analysis.

Keywords: image encryption; spatiotemporal chaos; fractional-order Chua's system; time-fractional diffusion processes

Citation: Ge, F.; Qin, Z.; Chen, Y. Integrated Time-Fractional Diffusion Processes for Fractional-Order Chaos-Based Image Encryption. *Sensors* **2021**, *21*, 6838. https://doi.org/10.3390/s21206838

Academic Editor: Paweł Pławiak

Received: 14 September 2021
Accepted: 11 October 2021
Published: 14 October 2021

1. Introduction

Owing to the rapid development of internet and multimedia technologies, a great number of images have been used in various applications. Since images are usually required to be confidential between the sending side and the receiver end, the protection of images by encryption becomes more and more important. During the past several decades, different techniques have been introduced to design the image encryptions [1,2]. Among them, chaos-based encryption, which was first explored by Matthews in [3], is considered as one of the most excellent encryption methods in consequence of the good property of chaos, such as high sensitivity to initial value conditions, state ergodicity and nonconvergence [4–6]. Based on these advantages, some more complex encryption schemes consisting of chaos and other ways, such as information entropy [7], mixed linear–nonlinear coupled map lattice [8], a pseudo-random numbers generator [9] or the genetic algorithm [10] have been investigated. However, the control parameters for permutation in above-mentioned algorithms are all fixed and the key extracted from the chaotic signals depends only on the keys, which degrade the performance of the cryptosystems.

To deal with these drawbacks, in recent years, the spatiotemporal chaos-based encryption problems have been studied, due to the fact that they can pose many excellent properties, such as a large parameter space and a random-like sequence, thereby increasing the algorithm complexity and enhancing the security. For example, in [11], a spatiotemporal chaotic cryptosystem was developed by utilizing the impulsive synchronization of reaction–diffusion systems. Based on the permutation–diffusion architecture, more sensitive chaotic image encryption schemes were proposed in [12,13]. Considering that spatiotemporal chaos is often created by local nonlinearity dynamics and spatial diffusion governed by coupled map lattices (CML), the chaos-based multiple image encryption

algorithms by using CML were developed in [14,15]. For more spatiotemporal chaos-based cryptosystems, we refer the reader to [16,17] via the cellular automata, to [18] by using the generalized heat equation associated with GVTSG, or to [19] based on the DNA operation.

It is worth noting that the last decade has witnessed a significant development in the study of fractional-order chaos-based image encryption strategies [20–22]. Due to the introduction of the fractional-order derivatives, fractional-order chaotic systems provide additional degrees of the freedom in optimization performance, hence exhibiting more complex characteristics and having a unique advantage in the secret key space extension [23]. These make the corresponding image encryption scheme more efficient, secure and reliable.

Further, nowadays, studies indicate that the canonical diffusion systems may be inadequate to describe those anomalous subdiffusion processes observed in a spatially inhomogeneous environment, such as reheating processes of the heterogeneous metal slabs [24,25] or the spread of contaminants in underground water [26]. To improve the modeling precision of these extremely complex transport processes, the authors in [27–32] have proven that time-fractional diffusion system with a time-fractional derivative of order $\alpha \in (0, 1]$ can be regarded as a powerful alternative model. Most importantly, we see that the time-fractional diffusion system can recover the traditional diffusion system if the order $\alpha \to 1^-$ [33,34]. Therefore, studies on proposing a novel spatiotemporal image encryption algorithm by integrating time-fractional diffusion system into the fractional-order chaos based image encryption should be both challenging and necessary.

Motivated by the above consideration, this paper aims to come up with a novel image encryption algorithm that is proposed by combining the fractional-order Chua's system and the time-fractional diffusion systems of order $\alpha \in (0, 1]$. The reasons why we take the fractional-order Chua's system into consideration are that (1) it is a well-known chaotic system, which generates three chaotic sequences; (2) the fractional-order Chua's system is more simply than fractional-order Lorenz system because it requires only one nonlinear function of one variable, whereas the fractional-order Lorenz system requires two nonlinear functions of two variables; (3) most standard routes to chaos from the fractional-order Lorenz equation can be produced by the fractional-order Chua's systems; (4) there exist some theoretical results for Chua's system, which are absent for the Lorenz system [35]. More precisely, we first obtain the numerical solution of the fractional-order Chua's system. Secondly, we present a novel spatiotemporal chaotic scheme by designing the chaotic sequence of fractional-order Chua's system as the initial condition and the boundary conditions of the time-fractional diffusion system under consideration. It is revealed that the proposed image encryption algorithm, which has the properties of larger secret key space, higher sensitivity to initial boundary conditions, better random-like sequence and faster encryption speed, can gain excellent encryption performance in cryptography. To the best of our knowledge, no result is available on the topic that proposes a image encryption algorithm by integrating the time-fractional diffusion processes for fractional-order Chua's system, which inspires this paper.

The structure of this paper is as follows. In Section 2, we provide some basic results to be used thereafter. Section 3 is devoted to giving the detailed image encryption algorithm. For the illustration, we perform a computer experiment in Section 4. The security analysis, including the histogram analysis, information entropy, adjacent pixel correlation and differential attack analysis to illustrate our results, are finally presented in Section 5.

2. Preliminaries

In this section, we aim to give some preliminary results to be used thereafter.

2.1. Fractional-Order Chua's System

Let us consider the three-dimensional fractional-order Chua's chaotic system [36] of the following form:

$$\begin{cases} {}_0^C D_t^{q_1} y_1(t) = a(y_2(t) - y_1(t) - f(y_1)), \\ {}_0^C D_t^{q_2} y_2(t) = y_1(t) - y_2(t) + y_3(t), \\ {}_0^C D_t^{q_3} y_3(t) = -by_2(t) - cy_3(t), \end{cases} \tag{1}$$

where $y = (y_1, y_2, y_3)^T$ is the state vector, $(a, b, c)^T$ is the parameter vector,

$$f(y_1) = m_1 y_1(t) + 0.5(m_0 - m_1)(|y_1(t) + 1| - |y_1(t) - 1|) \tag{2}$$

is the nonlinear function and m_0, m_1 are two system parameters. Here, $q_i \in (0, 1]$, $i = 1, 2, 3$, denote the order of the Caputo fractional-order derivative, ${}_0^C D_t^{q_i}$ is the Caputo time-fractional derivative given by [33]:

$${}_0^C D_t^{q_i} y_i(t) = {}_0 I_t^{1-q_i} \frac{d}{dt} y_i(t), \; i = 1, 2, 3, \tag{3}$$

and ${}_0 I_t^{1-q_i} \varphi(t) = \frac{1}{\Gamma(1-q_i)} \int_0^t (t-\tau)^{-q_i} \varphi(\tau) d\tau$ represents the Riemann–Liouville fractional integral.

To illustrate the chaos property of above system (1), set $a = 10.725$, $b = 10.593$, $c = 0.268$, $m_0 = -1.1726$, $m_1 = -0.7872$, $q_1 = 0.93$, $q_2 = 0.99$ and $q_3 = 0.92$, we depict the evolution of the solution for fractional-order Chua's system (1) in Figure 1.

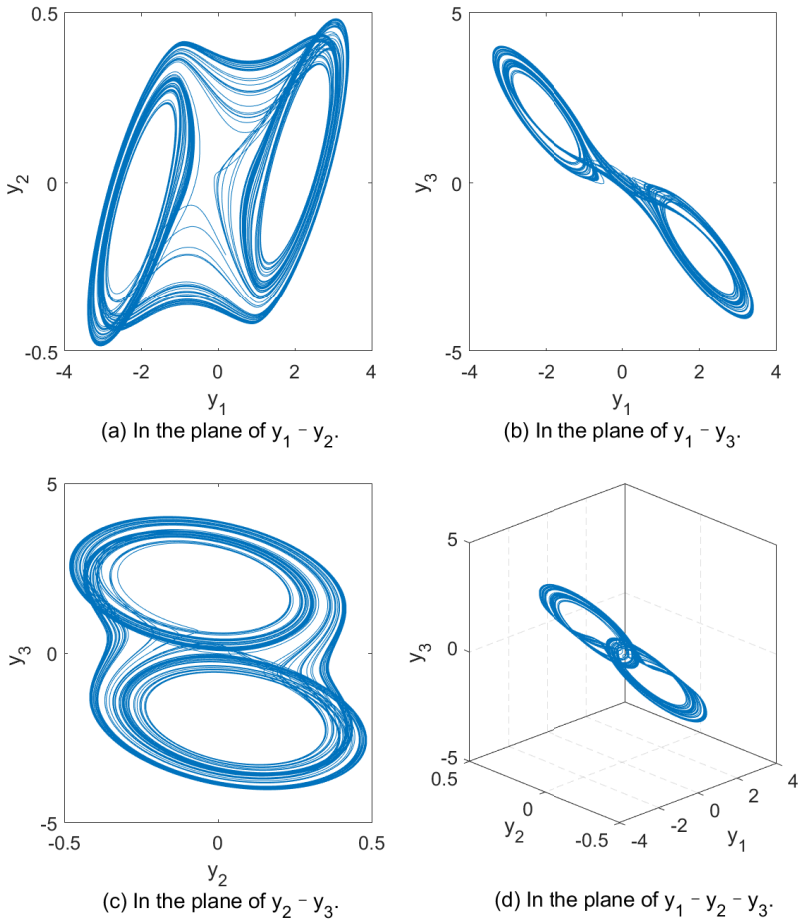

Figure 1. Evolution of the chaotic and its projections.

2.2. Time-Fractional Diffusion System

Throughout this paper, we consider the following time fractional diffusion equation:

$$\begin{cases} {}_0^C D_t^\alpha \omega(x,t) = K\frac{\partial^2 \omega(x,t)}{\partial x^2} + V\omega(x,t) + g(x,t), 0 < x < L,\ t \geq 0 \\ p_1\omega_x(0,t) + r_1\omega(0,t) = \varphi(t),\ p_2\omega_x(L,t) + r_2\omega(L,t) = \psi(t),\ t > 0, \\ \omega(x,0) = \phi(x),\ 0 < x < L, \end{cases} \tag{4}$$

where $\omega(x,t)$ denotes the system state, $L > 0$ is a constant, K is the diffusion coefficient, V represents the reaction coefficient and p_1, p_2, r_1, $r_2 > 0$ are four constants. Moreover, ${}_0^C D_t^\alpha$, $\alpha \in (0,1]$ is the Caputo time-fractional derivative with respect to t defined as [33]:

$${}_0^C D_t^\alpha y(\cdot,t) = {}_0 I_t^{1-\alpha} \frac{\partial y}{\partial t}(\cdot,t) \tag{5}$$

and φ, $\psi \in L^2[0,\infty)$, $\phi \in L^2(0,L)$ are three given functions. Here, $L^2[0,\infty)$ and $L^2(0,L)$ are, respectively, the usual Hilbert spaces with the norms induced by corresponding inner products.

For the regularity results of this system (4), based on the eigenvalue theory of operator $\triangle = \frac{\partial^2}{\partial x^2}$ under the Robin boundary condition and the semigroup theory, we refer the reader to [37,38], where the detailed solution expression of time-fractional diffusion systems and its regularity results are obtained. Further, according to the high order approximation method on Caputo time-fractional derivative in [39], set

$$\alpha = 0.5,\ K = 1,\ V = 16,\ g(x,t) = 4\sqrt{x}e^{-0.5x} \text{ and } p_1 = 3,\ r_1 = 1,\ p_2 = 1,\ r_2 = 2, \tag{6}$$

we extend to simulate above time-fractional diffusion system (4) and then have the Figure 2.

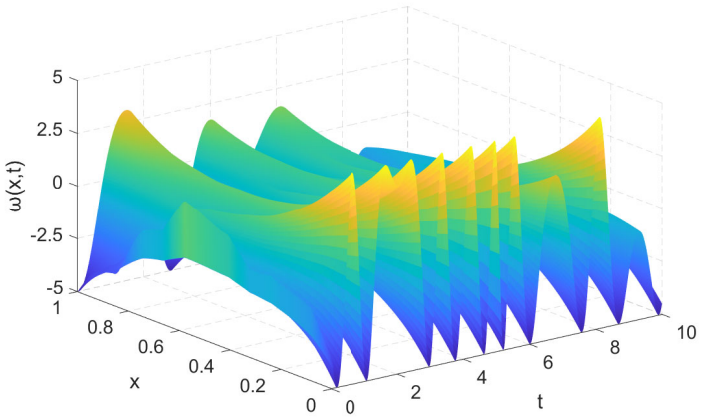

Figure 2. The behaviors of time-fractional diffusion system (4).

Remark 1. *It is worth mentioning that the reason why we use the Caputo fractional-order derivative in both the fractional-order Chua's system and time-fractional diffusion system, but not the Riemann–Liouville or the Grunwald–Letnikov formula is because of the physical significance of their initial conditions. We claim that it is okay to study the considered problems with the Riemann–Liouville or the Grunwald–Letnikov fractional-order derivatives in a mathematical sense.*

3. Algorithm Description

This section aims to perform a detailed description of the proposed image cryptosystem.

By Figure 3, the proposed spatiotemporal chaos-based cryptosystem for digital images consists of the following three parts: key stream generation, image scrambling and image diffusion.

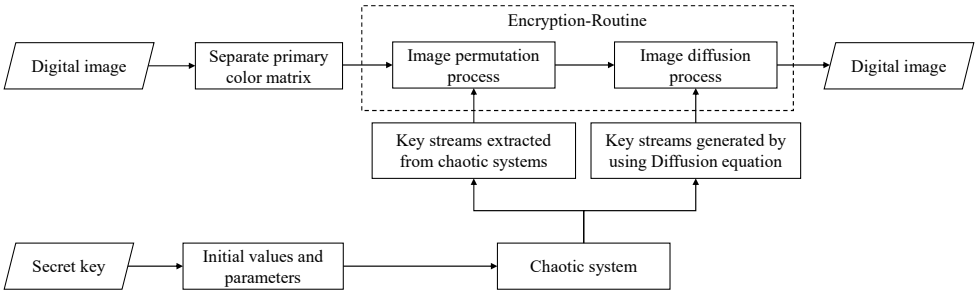

Figure 3. Block diagram of the proposed image encryption algorithm.

- **Part 1. Key stream generation**: divide the three chaotic sequences generated by iterative chaotic system into nine sub-sequences;
- **Part 2. Image scrambling**: use six of the nine sub-sequences to respectively scramble the RGB primary color components of the image; design the other three sub-sequences as the initial-boundary conditions for studied time-fractional diffusion system;
- **Part 3. Image diffusion**: utilize the new sequence obtained by numerically solving the time-fractional diffusion system under consideration to diffuse the pixel values of scrambled image, thereby obtaining the encrypted image.

3.1. Sequence Generation and Processing

(1) Solve fractional-order Chua's system (1) with given initial values $y_1(0)$, $y_2(0)$, $y_3(0)$ to obtain the three chaotic sequences. This is $\{y_1(i), y_2(i), y_3(i) \mid i = 1, 2, 3, \ldots, N_1\}$, where $N_1 = N + 4M + N_0$ denotes the number of iterations, $N_0 = 10,000$, and M, N are two constants determined by the size of the image.

(2) To enhance the dependence of chaotic sequence on initial values and to avoid transient effects, we discard the first N_0 values of the chaotic sequence and have a new chaotic sequence as follows:

$$\{\widetilde{y}_1(i), \widetilde{y}_2(i), \widetilde{y}_3(i) \mid i = 1, 2, 3, \ldots, 4M + N\}. \tag{7}$$

After these, we separate the new chaotic sequence into nine parts, according to the rules contained in Table 1.

Table 1. The sub-sequences of three chaotic sequences.

Names	Uses of Sequences	Number of Sequences
Lside	The initial boundary conditions of the time-fractional diffusion system (4)	$\{\widetilde{y}_1(1), \widetilde{y}_1(2), \ldots, \widetilde{y}_1(N)\}$
Rside		$\{\widetilde{y}_2(1), \widetilde{y}_2(2), \ldots, \widetilde{y}_2(N)\}$
Wside		$\{\widetilde{y}_3(1), \widetilde{y}_3(2), \ldots, \widetilde{y}_3(3M)\}$
MX	Scramble the rows of the primary color matrix	$\{\widetilde{y}_1(3M+1), \widetilde{y}_1(3M+2), \ldots, \widetilde{y}_1(4M)\}$
MY		$\{\widetilde{y}_2(3M+1), \widetilde{y}_2(3M+2), \ldots, \widetilde{y}_2(4M)\}$
MZ		$\{\widetilde{y}_3(3M+1), \widetilde{y}_3(3M+2), \ldots, \widetilde{y}_3(4M)\}$
NX	Scramble the columns of the primary color matrix	$\{\widetilde{y}_1(4M+1), \widetilde{y}_1(4M+2), \ldots, \widetilde{y}_1(4M+N)\}$
NY		$\{\widetilde{y}_2(4M+1), \widetilde{y}_2(4M+2), \ldots, \widetilde{y}_2(4M+N)\}$
NZ		$\{\widetilde{y}_3(4M+1), \widetilde{y}_3(4M+2), \ldots, \widetilde{y}_3(4M+N)\}$

(3) Let the sequence of Lside, Rside and Wside be the initial boundary conditions of the time-fractional diffusion system (4). More precisely, we rewrite the initial condition and the boundary conditions of the time-fractional diffusion system (4) as follows

$$\begin{cases} p_1\omega_x(0,j) + d_1\omega(0,i) = \varphi(\widetilde{y}_1(i)), \ 1 \le i \le N, \\ p_2\omega_x(L,j) + d_2\omega(L,j) = \psi(\widetilde{y}_2(j)), \ 1 \le j \le N, \\ \omega(l,0) = \phi(\widetilde{y}_3(l)), \ 1 \le l \le 3M, \end{cases} \tag{8}$$

where $\widetilde{y}_1(i) \in$ Lside, $\widetilde{y}_2(j) \in$ Rside, $\widetilde{y}_3(l) \in$ Wside.

(4) By extending the numerical method in [39], we here numerically solve the time-fractional diffusion system (4) and obtain a sequence W of size $3M \times N$. Notice that each pixel value of the image is usually an integer number ranging from 0 to 255, while the obtained sequence W is a real matrix. The following optimization procedure is needed:

$$W_t = mod(round(abs(W - floor(W) \times 10^m)), 256), \tag{9}$$

where $abs(x)$ denotes the absolute value of x, floor(x) represents the maximum integer that is not greater than x, mod(x, y) means x mod y and $m > 0$ is an integer.

(5) Splitting the optimized sequence W_t into three matrices TX, TY and TZ with the size of $M \times N$, one has the following:

$$\begin{cases} TX = W_t(1:3:end-2,:), \\ TY = W_t(2:3:end-1,:), \\ TZ = W_t(3:3:end,:). \end{cases} \tag{10}$$

3.2. Specific Encryption Process

Suppose that M and N are, respectively, the width and height of the original digital image I_0. The detailed encryption process is given as follows.

Step 1. Separate the three primary color matrices of R, G and B of image I_0. We have the following:

$$I_0R = I_0(:,:,1), \ I_0G = I_0(:,:,2) \ \text{ and } \ I_0B = I_0(:,:,3). \tag{11}$$

Step 2. Sort the six sequences of MX, MY, MZ, NX, NY and NZ in ascending order of numerical value respectively to obtain new array sequences. After this, we replace the value of the new array sequences with the position index of the original sequence and then, have six new array sequences: $indMX$, $indMY$, $indMZ$, $indNX$, $indNY$ and $indNZ$.

Step 3. Use the above six scrambled array sequences $indMX$, $indMY$, $indMZ$, $indNX$, $indNY$ and $indNZ$ to scramble the rows and columns of the primary color matrix I_0R, I_0G and I_0B, respectively, to obtain I_1R, I_1G and I_1B. Then, we transform the matrices TX, TY and TZ and the matrices of primary color I_1R, I_1G and I_1B into the one-dimensional array of KX, KY and KZ and primary color component arrays of I_2R, I_2G and I_2B in size of MN.

Step 4. Utilize the one-dimensional arrays KX, KY and KZ to perform the ciphertext diffusion operation on the scrambled image I_2. The details are as follows:

S4-1 Process the first pixel values of the primary color component arrays I_2R, I_2G, and I_2B as the following:

$$\begin{aligned} I_3R(1) = &\ (((I_2R(1) \oplus I_2R(M*N)) \oplus (I_2G(M*N) \oplus I_2B(M*N))) \oplus KX(1)), \\ I_3G(1) = &\ (((I_2G(1) \oplus I_2G(M*N)) \oplus (I_2R(M*N) \oplus I_2B(M*N))) \oplus KY(1)), \\ I_3B(1) = &\ (((I_2B(1) \oplus I_2B(M*N)) \oplus (I_2R(M*N) \oplus I_2G(M*N))) \oplus KZ(1)). \end{aligned} \tag{12}$$

Here, $\oplus$ denotes the bitwise XOR operator, and I_3R, I_3G, I_3B are three arrays that have been diffused.

S4-2 Encrypt the $i(i \geq 2)$ element value of each primary color component array according to the formula as follows:

$$\begin{array}{ll} I_3R(i) = & (((I_2R(i) \oplus I_3R(i-1)) \oplus (I_3G(i-1) \oplus I_3B(i-1))) \oplus KX(i)), \\ I_3G(i) = & (((I_2G(i) \oplus I_3G(i-1)) \oplus (I_3R(i-1) \oplus I_3B(i-1))) \oplus KY(i)), \\ I_3B(i) = & (((I_2B(i) \oplus I_3B(i-1)) \oplus (I_3R(i-1) \oplus I_3G(i-1))) \oplus KZ(i)). \end{array} \quad (13)$$

S4-3 Check i; if $i \leq MN$, go to step **S4-2**. Otherwise, stop the loop and go to Step 5.

Step 5. A second round of ciphertext diffusion is conducted on I_3R, I_3G and I_3B. The specific processes are:

S5-1 Conduct the process on the primary color component arrays I_3R, I_3G and I_3B according to the following formula and obtain I_4R, I_4G, I_4B following:

$$\begin{array}{ll} I_4R(1) = & (((I_3R(1) \oplus I_3R(M*N)) \oplus (I_3G(M*N) \oplus I_3B(M*N))) \oplus KZ(1)), \\ I_4G(1) = & (((I_3G(1) \oplus I_3G(M*N)) \oplus (I_3R(M*N) \oplus I_3B(M*N))) \oplus KX(1)), \\ I_4B(1) = & (((I_3B(1) \oplus I_3B(M*N)) \oplus (I_3R(M*N) \oplus I_3G(M*N))) \oplus KY(1)). \end{array} \quad (14)$$

S5-2 Encrypt the $j(j \geq 2)$ element value of each primary color component array as follows:

$$\begin{array}{ll} I_4R(i) = & (((I_3R(i) \oplus I_4R(i-1)) \oplus (I_4G(i-1) \oplus I_4B(i-1))) \oplus KZ(j)), \\ I_4G(i) = & (((I_3G(i) \oplus I_4G(i-1)) \oplus (I_4R(i-1) \oplus I_4B(i-1))) \oplus KX(j)), \\ I_4B(i) = & (((I_3B(i) \oplus I_4B(i-1)) \oplus (I_4R(i-1) \oplus I_4G(i-1))) \oplus KY(j)). \end{array} \quad (15)$$

S5-3 Check j; if $j \leq MN$, go to process **S5-2**. Otherwise, stop the loop and then, complete the second round of ciphertext diffusion.

Step 6. Transform the three encrypted array I_4R, I_4G and I_4B with length MN into three matrices with size $M \times N$, named CR, CG, CB. Finally, we use CR, CG and CB to obtain the final ciphertext image C by:

$$\begin{cases} C(:,:,1) = CR(:,:), \\ C(:,:,2) = CG(:,:), \\ C(:,:,3) = CB(:,:). \end{cases} \quad (16)$$

It is worth pointing out that the encryption algorithm designed in this paper belongs to a symmetric cryptographic system and the original image can be decrypted by using the reverse encryption process.

4. Simulation Results

To illustrate the performance of proposed encryption strategy, we select the Lena digital image with a size of 256×256 and use the Matlab 9.4 programming platform. The parameters of the fractional-order chaotic system are $a = 10.725$, $b = 10.593$, $c = 0.268$, $m_0 = -1.1726$, $m_1 = -0.7872$, $q_1 = 0.93$, $q_2 = 0.99$, and $q_3 = 0.92$ and the initial values read as $y_1(0) = 0.2000$, $y_2(0) = -0.2120$, and $y_3(0) = -0.0810$. The coefficient and fractional order of the time-fractional diffusion system are:

$$\alpha = 0.5,\ K = 1,\ V = 16,\ g(x,t) = 4\sqrt{x}e^{-0.5x} \text{ and } p_1 = 3,\ r_1 = 1,\ p_2 = 1,\ r_2 = 2. \quad (17)$$

Following the encryption steps presented in Section 3.2, we show the effect of using proposed image encryption algorithm to encrypt the plaintext Lena image in Figure 4. Based on this, one can find that the encrypted image is messy and is impossible to distinguish any plaintext information. Most importantly, the original plaintext image can be decrypted accurately by using the correct key. Therefore, we conclude that the proposed image encryption algorithm is secure, efficient and reliable.

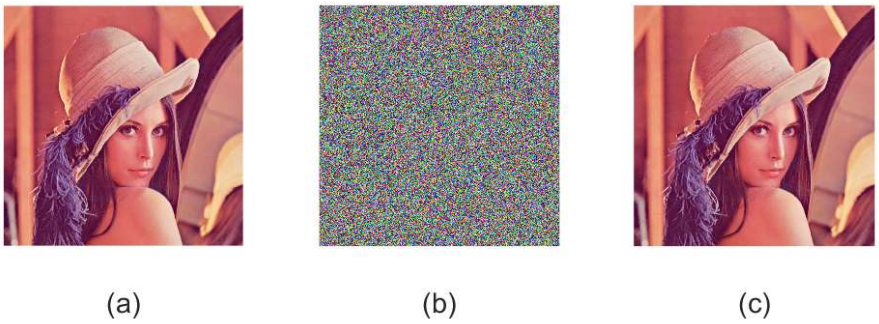

Figure 4. Experimental results for Lena image. (**a**) Original image of Lena, (**b**) encrypted image of Lena, (**c**) decrypted image of Lena.

5. The Security Analysis

In this section, several security analyses, such as key analysis, statistical analysis and information entropy analysis are performed to illustrate the quality of our proposed image encryption algorithm.

5.1. Key Analysis

As stated in [40], the key space of the encryption algorithm should not be smaller than $2^{100} \approx 10^{30}$ to ensure the security of the encryption algorithm. In our algorithm, the keys are divided into four parts: the initial values $y_1(0)$, $y_2(0)$, $y_3(0)$, the orders q_1, q_2, q_3 of the fractional-order Chua's chaotic system, the coefficients K, V and the order α in time-fractional diffusion system. Since the accuracy of the computer is 10^{15} and key space of the algorithm is 10^{135}, it is sufficient to resist exhaustive attack.

Moreover, an efficient encryption scheme must also be sensitive to the keys. To illustrate this, suppose the two key values are changed separately: $y_3(0) = 0.08100000001$ and $\alpha = 0.50000000001$. By Figure 5, it implies that our proposed algorithm has a strong key sensitivity.

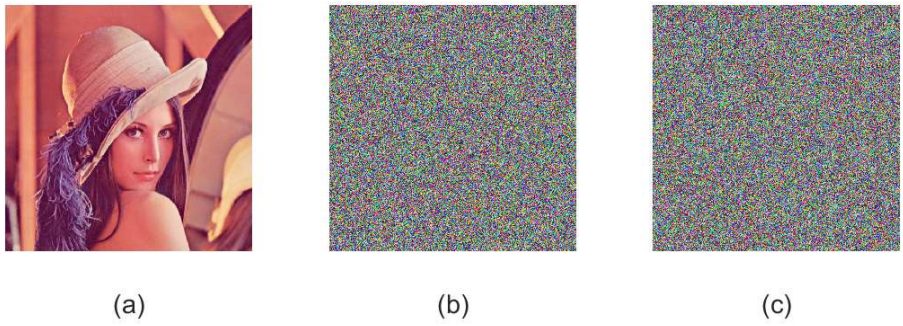

Figure 5. Key sensitive test. (**a**) Decrypted image with original key, (**b**) decrypted image with $y_3(0) = 0.08100000001$, (**c**) decrypted image with $\alpha = 0.50000000001$.

5.2. Histogram Analysis

A histogram is mainly used to count the frequency of each pixel, which is an important feature of image analysis [41]. An image histogram reflects the statistical characteristics of the image, so a standard to measure the encryption effect is to make the histogram distribution of the ciphertext image as uniform as possible. To this end, we refer the reader to Figure 6, where the histogram of the plaintext image and the ciphertext image are displayed. We take into account that the pixel values of the ciphertext image on the three primary color matrices of R, G and B are more distributed than the plaintext image. Then, we obtain that the encryption algorithm proposed in this paper has a strong ability to resist statistical attacks.

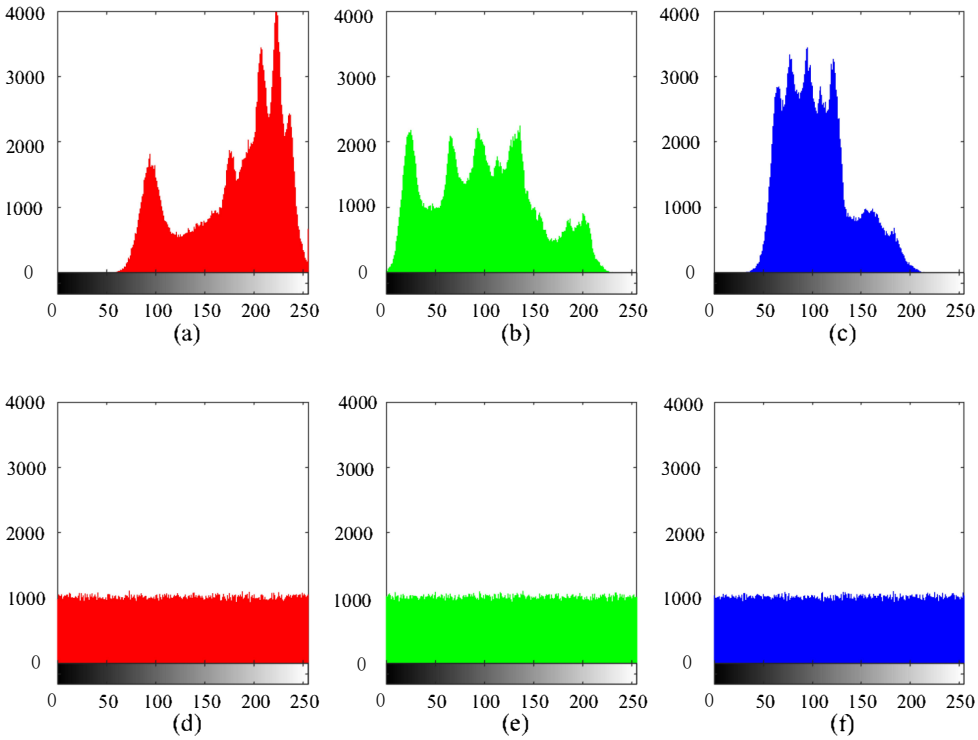

Figure 6. Histograms of plaintext images ((**a**) red, (**b**) green, and (**c**) blue components) and ciphertext images ((**d**) red, (**e**) green, and (**f**) blue components).

5.3. Correlation Analysis

Notice that the correlation of adjacent pixels reflects the correlation degree of pixel values of adjacent positions in the image and a good image encryption algorithm can make adjacent pixels reach zero correlation as far as possible. More precisely, we see that the correlation of adjacent pixel points can be computed with the following formula:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}}, \tag{18}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{19}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2, \tag{20}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i, \tag{21}$$

where r_{xy} is the correlation coefficient, x and y represent pixel values, respectively, $cov(x,y)$ is the covariance of x and y, $E(x)$ is the mean value of x, $D(x)$ is the variance of x, and N is the total number of pixels selected from the image.

To this end, we randomly select 15,000 pairs of adjacent pixels from original images and encrypted image to test horizontal, vertical, and diagonal correlations and obtain Figure 7, which shows that high correlation between adjacent pixels of a plaintext image no longer exists in a ciphertext image. For more detailed values of correlation between the three color components of a plaintext image and ciphertext image in horizontal, vertical and diagonal directions, we refer the reader to Table 2. In addition, we perform a detailed comparison of correlation coefficients in horizontal, vertical and diagonal direction for

several different image encryption algorithms in Table 3, which yields that the image encryption algorithm designed in this paper is more efficient and reliable.

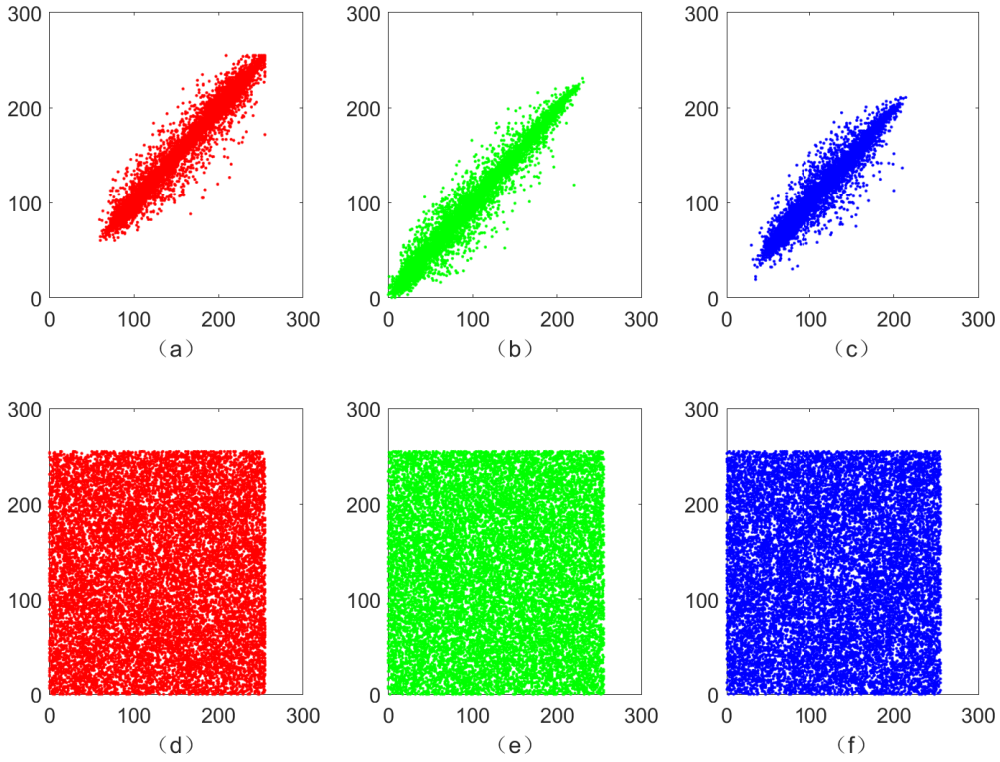

Figure 7. Correlation of adjacent pixels in vertical direction in plaintext images ((**a**) red, (**b**) green, and (**c**) blue components) and ciphertext images ((**d**) red, (**e**) green, and (**f**) blue components).

Table 2. The correlation coefficient of adjacent pixels.

Direction	Plaintext Image			Ciphertext Image		
	Red	Green	Blue	Red	Green	Blue
Horizontal	0.98770	0.98831	0.97456	−0.00076	−0.00478	0.00622
Vertical	0.97527	0.97472	0.95420	0.01125	−0.01236	0.00950
Diagonal	0.96437	0.96551	0.93511	−0.00255	0.00442	0.00172

Table 3. Comparison of correlation coefficients for different encryptions.

	Correlation Direction		
	Horizontal	Vertical	Diagonal
The original Lena image	0.98353	0.96806	0.95499
The proposed algorithm	0.00342	0.00279	0.00120
Ref. [42]	0.07700	−0.07236	−0.06153
Ref. [15]	−0.00273	−0.00515	−0.00902
Ref. [43]	−0.00960	−0.00680	0.01447

5.4. Information Entropy Analysis

Image information entropy is an important indicator to measure the randomness of information in information theory. The distribution of image pixel values can be measured by information entropy as follows:

$$H(s) = -\sum_{i=1}^{2^N-1} p(s_i) \log_2 p(s_i), \tag{22}$$

where s denotes the information source, N represents the $s_i(s_i \in s)$ bit number of the symbol, and $p(s_i)$ is the probability that the symbol s_i appears. For a 256-level grayscale image, each pixel has 2^8 possible values, and the ideal information entropy is 8. In fact, the information source difficulty generates completely random information. Therefore, the entropy of information is usually lower than the ideal value and a good cryptographic system's information entropy should be as close to the ideal value as possible.

According to Formula (22), we obtain that the information entropy values of the ciphertext image on the three color matrices of R, G and B are 7.9993, 7.9993 and 7.9992, which are very close to the ideal expectations 8. Moreover, we refer the reader to Table 4 for more comparisons of information entropy values between the proposed algorithm and other algorithms.

Table 4. Comparison of ciphertext image information entropy for different encryptions.

	Entropy		
	Red	**Green**	**Blue**
The proposed algorithm	7.9993	7.9993	7.9992
Ref. [14]	7.9893	7.9898	7.9894
Ref. [17]	7.9971	7.9975	7.9974
Ref. [44]	7.9892	7.9898	7.9899

5.5. Differential Attack Analysis

In general, the number of pixels change rate (NPCR) or the unified average changing intensity (UACI) are used to measure the encryption algorithm's ability to resist differential attacks. So, if a slight change is made to the plaintext pixel value, a large change in the encrypted pixel value happens. This means that the encryption scheme is good. Consider that NPCR and UACI are usually given by:

$$D(i,j) = \begin{cases} D(i,j) = 0, C_1(i,j) = C_2(i,j), \\ D(i,j) = 1, C_1(i,j) \neq C_2(i,j), \end{cases} \tag{23}$$

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times 100\%, \tag{24}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{25}$$

where M and N are the number of rows and columns of the image matrix, respectively, $C_1(i,j)$ and $C_2(i,j)$ represent the pixels value of the ciphertext images at the coordinate (i,j) when only one pixel value is different between two plaintext images, respectively.

As a illustration, for digital images with 256×256 pixels, the expected values of $NPCR$ and $UACI$ are $NPCR = 99.6094\%$ and $UACI = 33.4635\%$, respectively. For this purpose, we refer the reader to Table 5, which the average values of $NPCR$ and $UACI$ obtained for different algorithms to encrypt Lena plaintext images are presented. Taking into account that the $NPCR$ and $UACI$ encryptions based on the proposed algorithm exceed 99.96% and 36.36%, respectively, we conclude that the proposed encryption algorithm is very

sensitive to small changes in the plaintext image and then, has a stronger ability to carry a differential attack.

Table 5. Comparison of differential attack analysis for different encryptions.

Algorithm	Average NPCR (%)	Average UACI (%)
The proposed algorithm	99.9648	36.3651
Ref. [9]	99.6100	33.4500
Ref. [18]	99.6174	33.4404
Ref. [45]	99.6078	33.4531
Ref. [43]	99.6133	30.3633

5.6. Speed Performance Analysis

For an encryption algorithm, the speed of the algorithm directly affects its performance, especially in the era of the rapid development of the internet. To perform the comparisons, we validate the proposed image encryption algorithm by using Matlab 9.4. The Lena plaintext image with size 256×256 is tested in a personal computer with a Microsoft Windows 10 64-bit operating system, Intel Core i7-7700 CPU @3.60 GHz and 8.00 GB memory. As depicted in Table 6, it is shown that the speed of our designed encryption algorithm is faster than many available encryption algorithms.

Table 6. Comparison of speed performance for different encryptions.

Algorithm	Encryption Time (Seconds)
The proposed algorithm	0.0718
Ref. [7]	0.2621
Ref. [12]	0.4170
Ref. [19]	2.2234
Ref. [46]	0.1272

Remark 2. *According to the above security analyses for illustrating the quality of the proposed encryption algorithm, the best orders of the fractional derivative in systems* (1) *and* (4) *can be determined by optimizing the penalty function that consists of the correlation coefficient, the information entropy and the numbers of NPCR and UACI. For this purpose, however, more constraints on both the studied systems and the encryption algorithms are required. This is beyond the scope of this paper. While interesting, we consider this question in our forthcoming papers.*

6. Conclusions

In this paper, fractional-order Chau's system and time-fractional diffusion system with Caputo fractional derivatives are combined to greatly improve the security, efficiency and reliability of the image encryption algorithm. Simulation results and the detailed security analysis are conducted to illustrate that the image encryption algorithm proposed in this paper can gain excellent encryption performance with the advantages of larger secret key space, higher sensitivity to initial-boundary conditions, better random-like sequence and faster encryption speed. Notice that there exist several different fractional-order systems that can drive into chaos, such as the fractional-order Lorenz system, the fractional-order van der Pol system, and these fractional-order chaotic system with Riemann–Liouville or Grunwald–Letnikov fractional derivatives. Then, investigation on proposing image encryption algorithms by combining different types of fractional-order chaotic systems with more complex nonlinear fractional partial differential equations (PDEs), such as time-fractional diffusion systems with space-time-varying coefficients, space-fractional systems or a hybrid diffusion–propagation system are also of great interest. Here, the considered fractional-order chaotic systems can also be of variable-order, distributed-order or even variable-distributed-order. Furthermore, we see that the problem of determining the optimal value of parameters and orders for fractional derivatives in the considered

fractional-order chaotic system and nonlinear fractional-order PDEs, which yield the best encrypt performance, is also worth discussing.

Author Contributions: All authors contributed to this research. F.G. designed the research and wrote the paper. Z.Q. contributed in the numerical simulation and assisted in writing the paper. Y.C. contributed in designing the research and revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (Nos. 61907039 and 41801365) and the Fundamental Research Funds for the Central Universities, China University of Geosciences, Wuhan (No. CUGGC05).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Yang, Y.; Pan, Q.; Sun, S.; Xu, P. Novel image encryption based on quantum walks. *Sci. Rep.* **2015**, *5*, 1–9. [CrossRef] [PubMed]
2. Li, J.; Li, J.S.; Pan, Y.Y.; Li, R. Compressive optical image encryption. *Sci. Rep.* **2015**, *5*, 10374. [CrossRef]
3. Matthews, R. On the derivation of a chaotic encryption algorithm. *Cryptologia* **1989**, *13*, 29–42. [CrossRef]
4. Uhl, A.; Pommer, A. *Image and Video Encryption: From Digital Rights Management To Secured Personal Communication*; Springer Science & Business Media: Boston, MA, USA, 2004.
5. Abd El-Samie, F.E.; Ahmed, H.E.H.; Elashry, I.F.; Shahieen, M.H.; Faragallah, O.S.; El-Sayed, M.; Alshebeili, S.A. *Image Encryption: A Communication Perspective*; CRC Press: Boca Raton, FL, USA, 2013.
6. Hua, Z.; Zhou, Y.; Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* **2019**, *480*, 403–419. [CrossRef]
7. Ye, G.; Pan, C.; Huang, X.; Zhao, Z.; He, J. A chaotic image encryption algorithm based on information entropy. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850010. [CrossRef]
8. Zhang, Y.; Wang, X. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Inf. Sci.* **2014**, *273*, 329–351. [CrossRef]
9. Sahari, M.L.; Boukemara, I. A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. *Nonlinear Dyn.* **2018**, *94*, 723–744. [CrossRef]
10. Kaur, M.; Kumar, V. Beta chaotic map based image encryption using genetic algorithm. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850132. [CrossRef]
11. Chen, W.; Luo, S.; Zheng, W.X. Impulsive synchronization of reaction–diffusion neural networks with mixed delays and its application to image encryption. *IEEE Trans. Neural Networks Learn. Syst.* **2016**, *27*, 2696–2710. [CrossRef] [PubMed]
12. Yin, Q.; Wang, C. A new chaotic image encryption scheme using breadth-first search and dynamic diffusion. *Int. J. Bifurc. Chaos* **2018**, *28*, 1850047. [CrossRef]
13. Cheng, G.; Wang, C.; Chen, H. A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. *Int. J. Bifurc. Chaos* **2019**, *29*, 1950115. [CrossRef]
14. Wu, X.; Li, Y.; Kurths, J. A new color image encryption scheme using CML and a fractional-order chaotic system. *PLoS ONE* **2015**, *10*, e0119660. [CrossRef] [PubMed]
15. Zhang, H.; Wang, X.; Wang, X.; Yan, P. Novel multiple images encryption algorithm using CML system and DNA encoding. *IET Image Process.* **2019**, *14*, 518–529. [CrossRef]
16. Souyah, A.; Faraoun, K.M. An image encryption scheme combining chaos-memory cellular automata and weighted histogram. *Nonlinear Dyn.* **2016**, *86*, 639–653. [CrossRef]
17. Niyat, A.Y.; Moattar, M.H.; Torshiz, M.N. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt. Lasers Eng.* **2017**, *90*, 225–237. [CrossRef]
18. Kumar, M.; Sathish, G.; Alphonse, M.; Lahcen, R.A.M. A new RGB image encryption using generalized heat equation associated with generalized Vigenere-type table over symmetric group. *Multimed. Tools Appl.* **2019**, *78*, 28025–28061. [CrossRef]
19. Kang, X.; Guo, Z. A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system. *Signal Process. Image Commun.* **2020**, *80*, 115670.
20. Hou, J.; Xi, R.; Liu, P.; Liu, T. The switching fractional order chaotic system and its application to image encryption. *IEEE/CAA J. Autom. Sin.* **2016**, *4*, 381–388. [CrossRef]
21. Wang, X.; Su, Y.; Luo, C.; Wang, C. A novel image encryption algorithm based on fractional order 5D cellular neural network and Fisher-Yates scrambling. *PLoS ONE* **2020**, *15*, e0236015. [CrossRef]
22. Talhaoui, M.Z.; Wang, X. A new fractional one dimensional chaotic map and its application in high-speed image encryption. *Inf. Sci.* **2021**, *550*, 13–26. [CrossRef]

23. Yang, Q.; Chen, D.; Zhao, T.; Chen, Y. Fractional calculus in image processing: a review. *Fract. Calc. Appl. Anal.* **2016**, *19*, 1222–1249. [CrossRef]
24. Ge, F.; Chen, Y. Event-triggered boundary feedback control for networked reaction-subdiffusion processes with input uncertainties. *Inf. Sci.* **2019**, *476*, 239–255. [CrossRef]
25. Ge, F.; Chen, Y. Observer-based event-triggered control for semilinear time-fractional diffusion systems with distributed feedback. *Nonlinear Dyn.* **2020**, *99*, 1089–1101. [CrossRef]
26. Meerschaert, M.M.; Mortensen, J.; Wheatcraft, S.W. Fractional vector calculus for fractional advection—Dispersion. *Phys. Stat. Mech. Its Appl.* **2006**, *367*, 181–190. [CrossRef]
27. Ge, F.; Chen, Y.; Kou, C. *Regional Analysis of Time-Fractional Diffusion Processes*; Springer: Cham, Switzerland, 2018.
28. Hilfer, R. *Applications of Fractional Calculus in Physics*; World Scientific: Lodon, UK, 2000.
29. Metzler, R.; Klafter, J. The random walk's guide to anomalous diffusion: A fractional dynamics approach. *Phys. Rep.* **2000**, *339*, 1–77. [CrossRef]
30. Ge, F.; Chen, Y.; Kou, C. Regional controllability analysis of fractional diffusion equations with Riemann–Liouville time fractional derivatives. *Automatica* **2017**, *76*, 193–199. [CrossRef]
31. Ge, F.; Chen, Y. Optimal vaccination and treatment policies for regional approximate controllability of the time-fractional reaction-diffusion SIR epidemic systems. *ISA Trans.* **2021**, *115*, 143–152. [CrossRef]
32. Song, W.; Ge, F.; Chen, Y. Subdiffusive Source Sensing by a Regional Detection Method. *Sensors* **2019**, *19*, 3504. [CrossRef]
33. Kilbas, A.A.; Srivastava, H.M.; Trujillo, J.J. *Theory and Applications of Fractional Differential Equations*; Elsevier Science Limited: Lodon, UK, 2006.
34. Ge, F.; Chen, Y.; Kou, C.; Podlubny, I. On the regional controllability of the sub-diffusion process with Caputo fractional derivative. *Fract. Calc. Appl. Anal.* **2016**, *19*, 1262–1281. [CrossRef]
35. Pivka, L.; Wu, C.W.; Huang, A. Lorenz Equation and Chua's Equation. *Int. J. Bifurc. Chaos* **1996**, *6*, 2443–2489. [CrossRef]
36. Petráš, I. *Fractional-Order Nonlinear Systems: Modeling, Analysis and Simulation*; Springer: Berlin/Heidelberg, Germany, 2011.
37. Ge, F.; Chen, Y. Regional output feedback stabilization of semilinear time-fractional diffusion systems in a parallelepipedon with control constraints. *Int. J. Robust Nonlinear Control.* **2020**, *30*, 3639–3652. [CrossRef]
38. Ge, F.; Chen, Y.; Kou, C. On the regional gradient observability of time fractional diffusion processes. *Automatica* **2016**, *74*, 1–9. [CrossRef]
39. Li, H.; Cao, J.; Li, C. High-order approximation to Caputo derivatives and Caputo-type advection–diffusion equations (III). *J. Comput. Appl. Math.* **2016**, *299*, 159–175. [CrossRef]
40. Stinson, D.R.; Paterson, M. *Cryptography: Theory and Practice*; CRC Press: Boca Raton, FL, USA, 2018.
41. Li, T.; Du, B.; Liang, X. Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. *IEEE Access* **2020**, *8*, 13792–13805. [CrossRef]
42. Ye, G.; Wong, K. An efficient chaotic image encryption algorithm based on a generalized Arnold map. *Nonlinear Dyn.* **2012**, *69*, 2079–2087. [CrossRef]
43. Wen, W.; Wei, K.; Zhang, Y.; Fang, Y.; Li, M. Colour light field image encryption based on DNA sequences and chaotic systems. *Nonlinear Dyn.* **2020**, *99*, 1587–1600. [CrossRef]
44. Wu, X.; Wang, K.; Wang, X.; Kan, H.; Kurths, J. Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Process.* **2018**, *148*, 272–287. [CrossRef]
45. Wang, X.; Su, Y. Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform. *Sci. Rep.* **2020**, *10*, 1–19. [CrossRef]
46. Alawida, M.; Teh, J.S.; Samsudin, A.; Alshoura, W. An image encryption scheme based on hybridizing digital chaos and finite state machine. *Signal Process.* **2019**, *164*, 249–266. [CrossRef]