electronics

Article

High-Security Image Encryption Based on a Novel Simple Fractional-Order Memristive Chaotic System with a Single Unstable Equilibrium Point

Zain-Aldeen S. A. Rahman [1,2], Basil H. Jasim [2], Yasir I. A. Al-Yasir [3,*] and Raed A. Abd-Alhameed [3,4]

[1] Department of Electrical Techniques, Technical Institute/Qurna, Southern Technical University, Basra 61016, Iraq; as.zain9391@stu.edu.iq

[2] Department of Electrical Engineering, College of Engineering, University of Basrah, Basra 61004, Iraq; basil.jasim@uobasrah.edu.iq

[3] Biomedical and Electronics Engineering, Faculty of Engineering and Informatics, University of Bradford, Bradford BD7 1DP, UK; R.A.A.Abd@bradford.ac.uk

[4] Information and Communication Engineering Department, College of Science and Technology, Basrah University, Basra 61004, Iraq

* Correspondence: y.i.a.al-yasir@bradford.ac.uk; Tel.: +44-127-423-8047

Abstract: Fractional-order chaotic systems have more complex dynamics than integer-order chaotic systems. Thus, investigating fractional chaotic systems for the creation of image cryptosystems has been popular recently. In this article, a fractional-order memristor has been developed, tested, numerically analyzed, electronically realized, and digitally implemented. Consequently, a novel simple three-dimensional (3D) fractional-order memristive chaotic system with a single unstable equilibrium point is proposed based on this memristor. This fractional-order memristor is connected in parallel with a parallel capacitor and inductor for constructing the novel fractional-order memristive chaotic system. The system's nonlinear dynamic characteristics have been studied both analytically and numerically. To demonstrate the chaos behavior in this new system, various methods such as equilibrium points, phase portraits of chaotic attractor, bifurcation diagrams, and Lyapunov exponent are investigated. Furthermore, the proposed fractional-order memristive chaotic system was implemented using a microcontroller (Arduino Due) to demonstrate its digital applicability in real-world applications. Then, in the application field of these systems, based on the chaotic behavior of the memristive model, an encryption approach is applied for grayscale original image encryption. To increase the encryption algorithm pirate anti-attack robustness, every pixel value is included in the secret key. The state variable's initial conditions, the parameters, and the fractional-order derivative values of the memristive chaotic system are used for contracting the keyspace of that applied cryptosystem. In order to prove the security strength of the employed encryption approach, the cryptanalysis metric tests are shown in detail through histogram analysis, keyspace analysis, key sensitivity, correlation coefficients, entropy analysis, time efficiency analysis, and comparisons with the same fieldwork. Finally, images with different sizes have been encrypted and decrypted, in order to verify the capability of the employed encryption approach for encrypting different sizes of images. The common cryptanalysis metrics values are obtained as keyspace = 2^{648}, NPCR = 0.99866, UACI = 0.49963, H(s) = 7.9993, and time efficiency = 0.3 s. The obtained numerical simulation results and the security metrics investigations demonstrate the accuracy, high-level security, and time efficiency of the used cryptosystem which exhibits high robustness against different types of pirate attacks.

Keywords: fractional order; nonlinear dynamics; memristor; chaotic system; image encryption

Citation: Rahman, Z.-A.S.A.; Jasim, B.H.; Al-Yasir, Y.I.A.; Abd-Alhameed, R.A. High-Security Image Encryption Based on a Novel Simple Fractional-Order Memristive Chaotic System with a Single Unstable Equilibrium Point. *Electronics* **2021**, *10*, 3130. https://doi.org/10.3390/electronics10243130

Academic Editor: Paulo Monteiro

Received: 22 November 2021
Accepted: 12 December 2021
Published: 16 December 2021

1. Introduction

Since Lorenz established chaos theory in 1963, research on chaotic systems has had a considerable practical impact [1]. Chaos phenomena in nonlinear domical systems have been widely used in science, engineering, and applied mathematics over the last few decades [2]. In fact, the most real systems in the world are nonlinear systems, but a chaotic phenomenon occurs when a deterministic system exhibits unusual exhibitions of aperiodic trajectories [3,4]. In many domains, such as biological systems that are used in the study of the human heart and brain, smart systems, secure communication systems, robotics engineering, digital signal processing, adaptive control engineering, data encryption, and nonlinear oscillator design, chaos plays a vital role [5].

In recent years, the memristor device has been employed as a fourth element in electrical circuits, in addition to the basic three elements. These three basic elements include resistor, capacitor, and inductor [6,7]. That fourth element has been proposed by Chau and is called the memristor, which is described as a two-terminal electronic mote. The first memristor was created by Williams and his team at HP Laboratories in 2008 [8]. The memristor element has a major impact on the characteristics of the electrical and electronic circuits, and it may soon act as a key device in their design. Nonlinear oscillator designs and memristive chaotic systems are the basic uses for the memristor [9]. With its distinctive characteristics, the memristor has been employed in a variety of memristor-based design applications, including digital circuits, computer systems, and neuromorphic structures. Memristor-based chaotic systems are one of these application areas. Because of its nonlinearity, the memristor can be employed in chaotic circuits, and the design of memristor-based chaotic circuits with various nonlinear equations has received a lot of attention [10]. Many different memristive chaotic systems have been designed/developed and investigated as mentioned in [11].

Because fractional calculus provides more accurate models than integer-order calculus, fractional-order derivative and fraction-order integration calculus have recently gained a lot of attention [12]. Fractional calculus is a branch of mathematics that is an extension of classical calculus. The subject of fractional calculus has recently received a lot of attention due to its potential applications in a range of fields [13]. Many systems in transdisciplinary disciplines can be described using fractional calculus. Additionally, the fractional-order model can provide an explicit description of the physical process as well as supplementary information [14]. Control, oscillators, bioengineering, circuit theory, analog filters, chemistry, and image processing encryption systems are all examples of where fractional calculus can be applied [15]. Many efforts have been undertaken in recent years to generate chaotic systems with more complex dynamics, and chaotic systems can be widely used in cryptography systems. Because fractional-order chaotic models include the fractional-order parameter as well as the original system features, they have a more complex dynamical behavior than integer models, making them useful in cryptosystems and secure communications schemes [16,17].

Many articles in the scientific research area have been focused on the application of fractional-order complex chaotic systems in image cryptosystems. In 2021, Wen H. et al. presented a complete security analysis of the CIEA-FOHS color image encrypting scheme based on a fractional-order chaotic system [18]. Haiying Hu et al. [19], in 2021, used the fractional-order chaotic system to construct an image cryptosystem. Sameh Askar et al., in 2021, proposed a hybrid encryption scheme based on a novel discrete fractional-order food chain system for encrypting colored images [20]. Yongjin Xian and Xingyuan Wanges developed a more efficient and secure chaotic image encryption algorithm than conventional approaches by presenting a new method of global pixel diffusion with two chaotic sequences, which offers good security and high encryption efficiency [21].

Lina Ding and Qun Ding in 2020 proposed a new image encryption technique based on a hyperchaotic system fractional-order Henon chaotic map [22]. In 2019, Shenli Zhu et al. introduced a novel chaotic S-box and used it in an image encryption scheme for improving the image encryption system's security and efficiency [23].

In this article, we propose a new 3D fractional-order memristive-based simple chaotic oscillator with a single unstable equilibrium. Firstly, a fractional-order memristor is developed based on [24], tested, and electronically realized. Then, this fractional-order memristor is connected in parallel with a capacitor and an inductor to construct this fractional-order memristive chaotic oscillator. Furthermore, the system dynamical behaviors were studied analytically and numerically, including system equilibria, chaotic attractors, bifurcation diagrams, and Lyapunov exponents. Additionally, a microcontroller (Arduino Due) was also employed to implement a functioning hardware digital electronic circuit for the new fractional-order memristive chaotic oscillator. Moreover, the developed system was applied in high-security image encryption. The cryptanalysis metric tests are shown in detail by histogram analysis, keyspace analysis, key sensitivity, correlation coefficients, entropy analysis, time efficiency analysis, and comparisons with similar fieldwork in order to confirm the security strength of the employed encryption approach. Finally, images of different sizes were encrypted and decrypted to prove that the utilized encryption approach was capable of encrypting/decrypting images of different sizes. Our work, testing, and results were all verified using MATLAB.

The following is the organization of the paper: In Section 2, the fundamental mathematical background of fractional-order systems is presented. Section 3 describes the development of a fractional-order memristor model, tests that memristor, and determines its parameters as well as the voltage-current characteristics. A simple fractional-order memristive chaotic system based on the developed fractional-order memristor is suggested and its' chaotic attractors as well as the system equilibria are established in Section 4. Lyapunov exponents and bifurcation diagrams are used to study the dynamical behavior properties of the suggested system as discussed in Section 5. In Section 6, the digital electronic circuit for the proposed memristive system is implemented using the Arduino Due board. An image encryption algorithm is applied based on the proposed simple fractional-order memristive chaotic system and the obtained numerical simulation results are presented in Sections 7 and 8, respectively. In Section 9, the experimental results of the image encryption effect are presented, including histogram, keyspace analysis, key sensitivity, correlation coefficients, entropy analysis, time efficiency analysis, comparisons, and encryption/decryption images with different sizes. Finally, Section 10 contains some concluding observations.

2. Preliminaries

Fractional calculus is a basic subject of mathematics that was initially proposed in a series of letters in 1695 [25]. Different definitions of fractional-order calculus exist, where the basic concepts are Grunwald–Letnikov definitions, Caputo definitions, and Riemann–Liouville definitions [26].

The Gamma function, denoted by $\Gamma(.)$, is the fundamental function in fractional-order calculus, as stated in Equation (1) [27].

$$\Gamma(n) = \int_0^{+\infty} \mathrm{e}^{-t} t^{n-1} dt; \quad n > 0;\ \Gamma(1) = 1, \Gamma(0) = +\infty \tag{1}$$

Grunwald–Letnikov approaches the fractional derivative as illustrated in Equation (2) [28]:

$$D^q x(t) = f(x,t) = \lim_{h\to 0} h^{-q}(-1)\sum_{j=0}^{t/h}(-1)\left(\begin{array}{c} q \\ j \end{array}\right) x(t-jh) \tag{2}$$

where q is the fractional-order and h represents the step size.

Caputo's fractional-order calculus is stated as follows in Equation (3) [29].

$$_{t_0}D_t^q f(t) = \begin{cases} \frac{1}{\Gamma(k-q)} \int\limits_{t_0}^{t} \frac{f^{(k)}(\tau)}{(t-\tau)^{q-k+1}} d\tau; & k-1 < q < k \\ \frac{d^k f(t)}{dt^k}; & q = k. \end{cases} \tag{3}$$

For fractional order, Riemann–Liouville established the fractional integral operator (J^q) in Equation (4) [30].

$$J^q f(t) = \begin{cases} \frac{1}{\Gamma(q)} \int_0^t (t-\tau)^{q-1} f(t) d\tau \, ; & q < 0 \\ f(t); & q = 0. \end{cases} \tag{4}$$

3. Memristor Model

The resistor, inductor, and capacitor are the three basic elements found in electronic circuits. Furthermore, since Chau introduced the fourth circuit component theoretically in 1971, and HP scientists confirmed it experimentally in 2008, this element has been named a memristor [31,32]. It has a nonlinear characteristic that allows it to add additional functionality to electronic circuits. The memristor represents the charge-flux relationship, which is considered in the model's essential variables [33].

This work focuses on the current-controlled memristor system, which is defined by Equation (5) below [34].

$$\begin{aligned} v_M &= R(z) i_M \\ \dot{z} &= f(z, i_M) \end{aligned} \tag{5}$$

where v_M and i_M represent the voltage across and current through the memristor device, z represents the internal memristor state, $f(z,\, i_M)$ represents the internal state function, and $R(z)$ represents the memristance.

3.1. Integer-Order Case

An integer voltage-controlled memristor can be presented as in the following Equation (6) for designing a chaotic system based on a memristor modeled in [24].

$$\begin{aligned} v_M &= \frac{i_M}{(\alpha z^2 - \beta)} \\ \dot{z} &= -a v_M - bz + k v_M^2 z \end{aligned} \tag{6}$$

In Equation (6), v_M and i_M represent the voltage across and current through the memristor device, z represents the internal memristor state, and α, β, a, b, and k are the constants.

The parameters of the memristor can be chosen flexibly according to the requirements of the state of the memristor. The memristor parameters are chosen as $\alpha = 0.01$, $\beta = 0.05$, $a = 0.25$, $b = 0.001$, and $k = 0.0005$. Assume that the memristor applied voltage is a sinusoidal signal presented as below in Equation (7).

$$v_M(t) = A_M cos(2\pi f t) \tag{7}$$

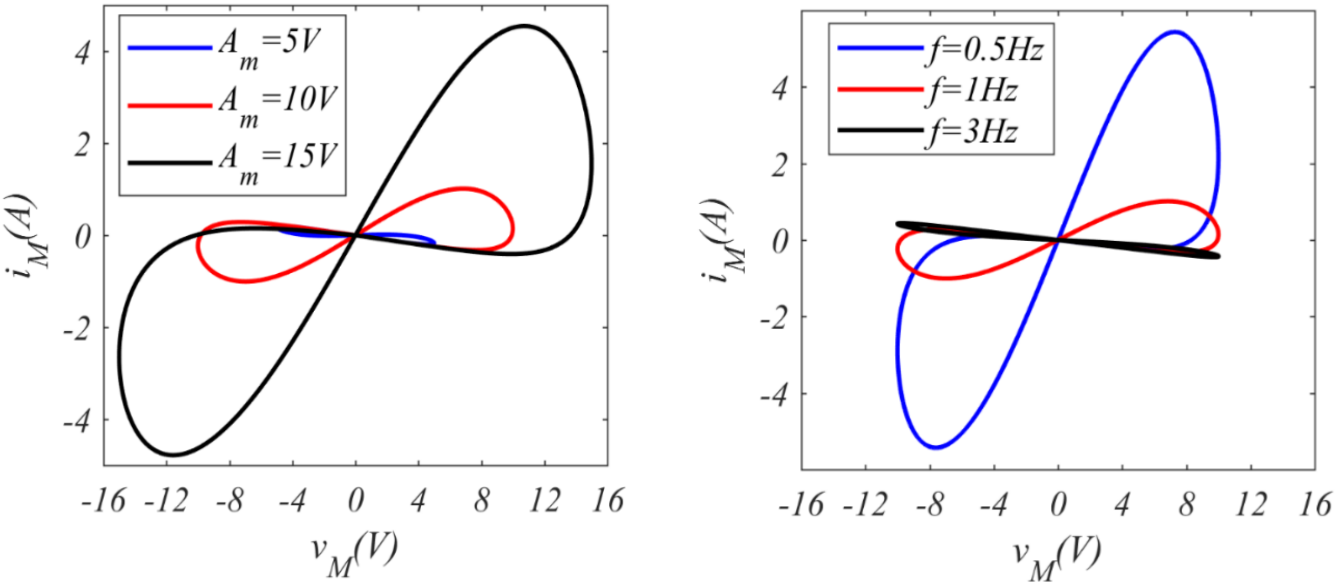
where A_M and f are the voltage amplitude and frequency, respectively. The $v_M - i_M$ characteristics curve of a memristor is specified in Figure 1 for different amplitudes and frequencies.

3.2. Fractional-Order Case

The memristor can be thought of as a sliding resistor whose resistance varies depending on the charge that passes through it. The memristor exhibits a hysteresis loop in the current-voltage curve when driven by a bipolar periodic signal [35]. Here, the voltage-controlled fractional-order memristor corresponding to the system (6) is modeled as follows in Equation (8):

$$\begin{aligned} v_M &= \frac{i_M}{(\alpha z^2 - \beta)} \\ \frac{d^q z}{dt^q} &= -a v_M - bz + k v_M^2 z \end{aligned} \tag{8}$$

where q represents the fractional-order derivative of the internal memristor state (z). With the same values of memristor parameters mentioned in the above integer case, the $v_M - i_M$ characteristics curve of a memristor is depicted in Figure 2 for different fractional orders, where the amplitude and frequency of the applied voltage to the mersister are 10 V and 1 Hz, respectively.



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

Figure 1. $v_M - i_M$ characteristics of memristor (6): (**a**) with f = 1 Hz and different amplitudes; (**b**) with A_m = 10 V different frequencies.

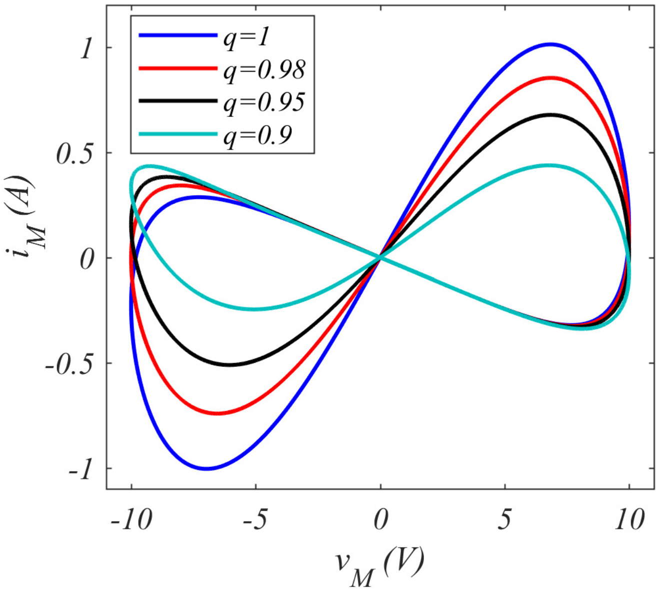


Figure 2. $v_M - i_M$ characteristics of fractional-order memristor described by Equation (8).

3.3. Circuit Realization of the Fractional-Order Memristor

The viability of using fractional memristors in real-world applications is confirmed by an electrical circuit realization of that fractional memristor. Based on Equation (6), it is clear that the realization of that memristor can be verified by classical operational amplifiers to perform the required mathematical operations in this equation including gain op-amp, weighted summer op-amp(s), inverting op-amp(s), and integer integrator op-amp(s). On the other hand, the integer integrator op-amp must be replaced by fractional-order op-amp to realize the memristor in the fractional case as noted in Equation (8). In other words, the conventional integer integrator (op-amp integrator) can be employed in the construction of these devices by substituting the capacitor with a fractance that is equivalent to the desired fractional order, resulting in a fractional-order integrator. A fractance is an electrical component with fractional-order impedance characteristics. The fractional operators cannot be directly implemented in time-domain simulations according to the usual definition of fractional differintegral [36]. Approximations to fractional operators utilizing ordinary integer-order operators must be developed to analyze such systems. According to circuit theory, the complex frequency domain of the fractance equivalent circuit can achieve the approximation formulation of fractional order (q-order). We used the fractional order (q = 0.98); the approximation of $1/s^{0.98}$ can be calculated as in Equation (9) [37].

$$\frac{1}{s^{0.98}} = \frac{1.2947(s+1125)}{(s+1423)(s+0.01125)} \tag{9}$$

Figure 3 depicts the chain fractance realization matching Equation (9).

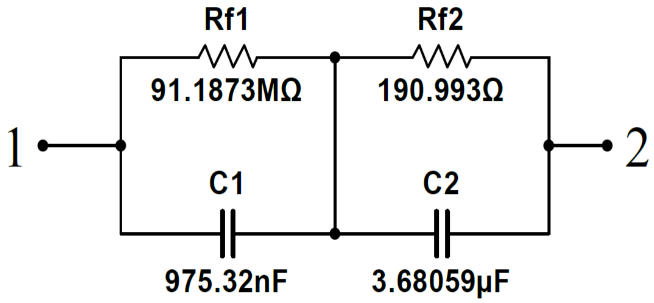


Figure 3. Chain fractance (CF) approximation of Equation (9).

In Figure 3, the transfer function between terminals 1 and 2 can be calculated as shown in Equation (10) [38].

$$\begin{aligned} H_{0.98}(s) &= \frac{R_{f1}}{\left(sR_{f1}C_1{+}1\right)} + \frac{R_{f2}}{\left(sR_{f2}C_2{+}1\right)} \\ &= \frac{1}{C_0}\left[\frac{\left(\frac{C_0C_2+C_0C_1}{C_1C_2}\right)\left(s+\frac{R_1+R_2/R_1R_2}{C_1+C_2}\right)}{\left(s+\frac{1}{R_1C_1}\right)\left(s+\frac{1}{R_2C_2}\right)}\right] \end{aligned} \tag{10}$$

In Equation (10), C_0 represents a unit parameter, selecting C_0 = 1 µF and $H_{0.98}(s)$. $C_0 = 1/s^{0.98}$, that reached the resistor (R_{f1} and R_{f2}) and capacitor values (C_1 and C_2) in Figure 3.

To achieve fractional integration of order (q = 0.98), the chain fractance circuit in Figure 3 is used to replace the capacitor in the classical integer integration circuit (op-amp integrator). So, the circuit Equation (11) of the fractional-order memristor modeled in Equation (8) is obtained as follows.

$$\begin{aligned} v_M &= \frac{i_M}{\left(\frac{R_7}{R_5}z^2 - \frac{R_7}{R_4}v_2\right)} \\ \frac{d^q z}{dt^q} &= \frac{1}{C_{eq}}\left[-\frac{1}{R_1}v_M - \frac{1}{R_2}z + \frac{1}{R_3}v_M^2 z\right] \end{aligned} \tag{11}$$

where C_{eq} acts as the fractional-order impedance equivalent to fractance cell in Figure 3, which is responsible for verifying the fractional-order integrator with order (q = 0.98). Therefore, the equivalent circuit corresponding to Equation (11) has been realized as shown in Figure 4. Figure 5 displays the results of $v_M - i_M$ characteristics corresponding to the fractional-order memristor which is illustrated in Figure 4. Multisim has been used to realize the electronic circuit of the fractional order. Figure 6 depicts the fractional-order memristor symbolic diagram.

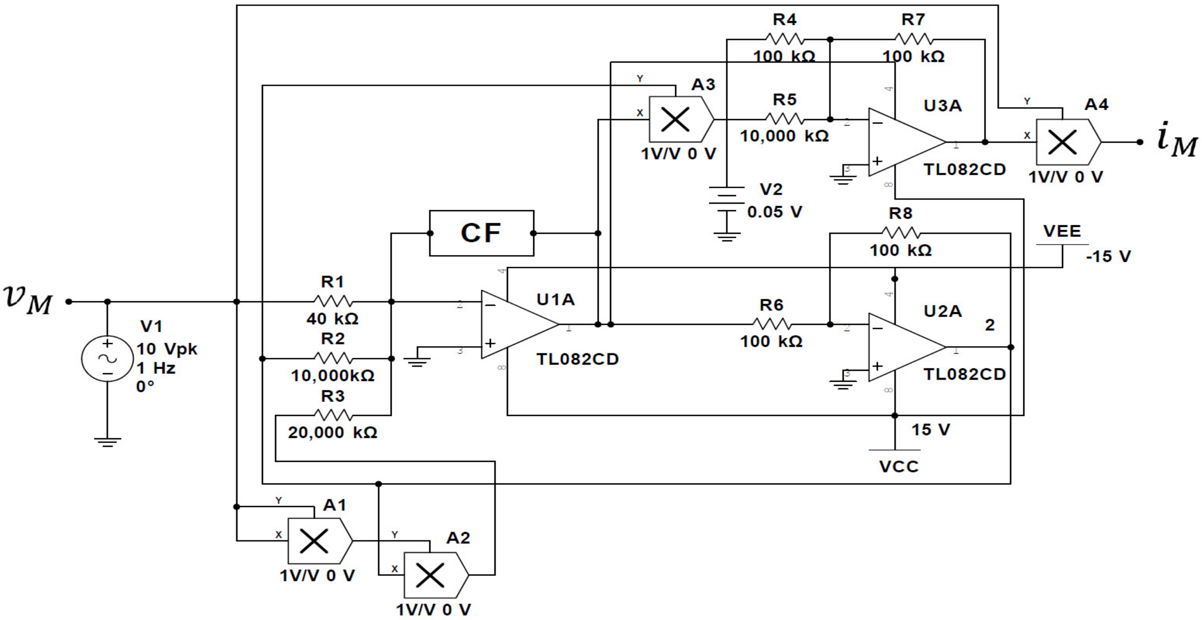
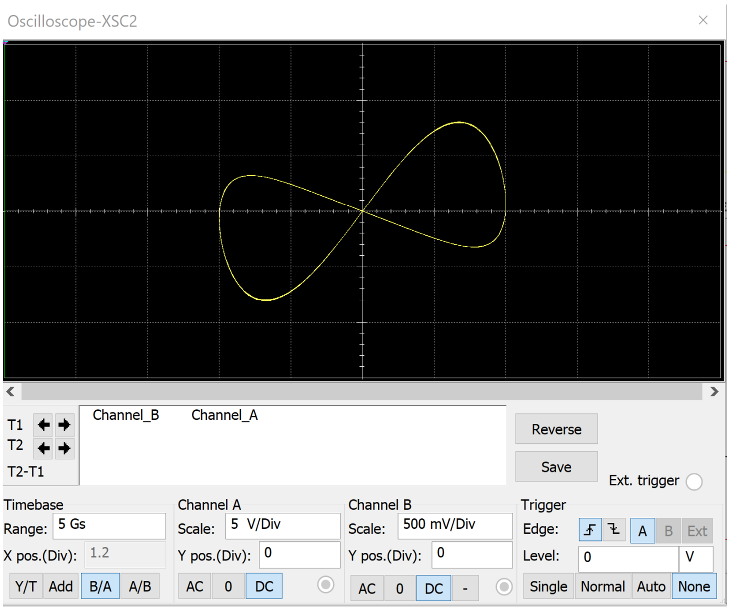


Figure 4. The realized circuit of the fractional-order memristor that is described by Equation (11).


Oscilloscope-XSC2

T1
T2
T2-T1

Channel_B Channel_A

Reverse
Save
Ext. trigger ○

Timebase
Range: 5 Gs
X pos.(Div): 1.2
Y/T Add B/A A/B

Channel A
Scale: 5 V/Div
Y pos.(Div): 0
AC 0 DC

Channel B
Scale: 500 mV/Div
Y pos.(Div): 0
AC 0 DC -

Trigger
Edge: A B Ext
Level: 0 V
Single Normal Auto None

Figure 5. $v_M - i_M$ characteristics of the realized circuit of the fractional-order memristor.

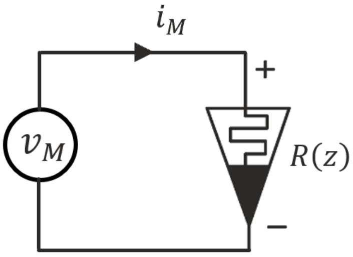


Figure 6. The symbolic diagram of the fractional-order memristor.

4. Fractional-Order Memristive-Based Simple Chaotic Circuit

Because the constricted hysteresis loop or recollection of prior states is a fundamental aspect of memristors, chaotic circuits with memristors must be evaluated with a method that takes memory effects into account and provides more degrees of freedom for analysis [10]. Thus, a simple fractional-order memristive chaotic circuit has been proposed by connecting the parallel capacitor and inductor in parallel with the fractional-order memristor modeled by Equation (8). The proposed simple fractional-order memristive chaotic circuit which contains three parallel elements is shown in Figure 7.

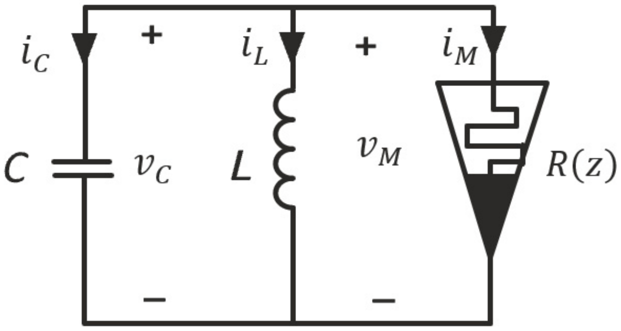


Figure 7. Simple fractional-order memristive chaotic circuit.

The following Equation (12) is obtained by applying Kirchhoff's current law for the fractional-order memristive chaotic circuit in Figure 7 and using the internal state of the fractional-order memristor described by Equation (8).

$$\begin{aligned} L\frac{d^q i_L}{dt^q} &= v_C \\ C\frac{d^q v_C}{dt^q} &= -i_L - i_M \\ \frac{d^q z}{dt^q} &= -av_M - bz + kv_M^2 z \end{aligned} \tag{12}$$

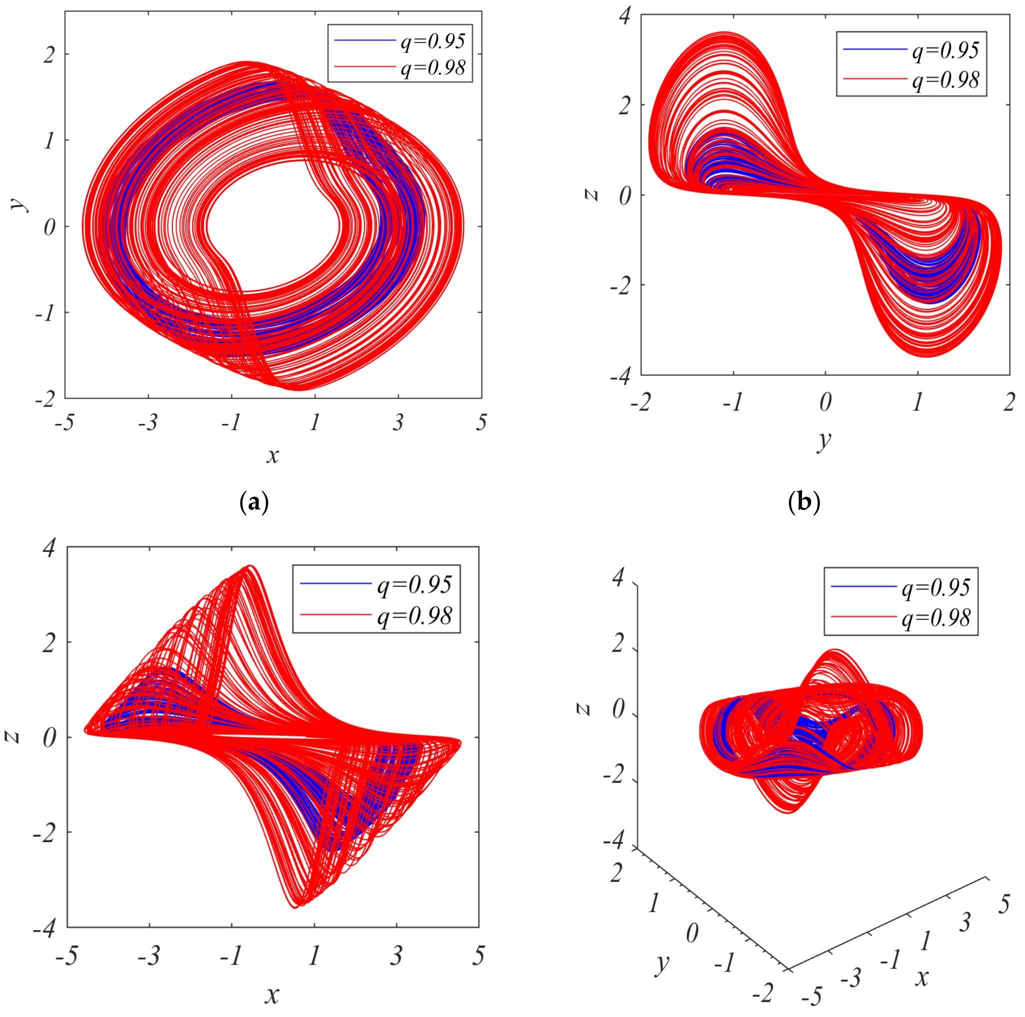
Then, by substituting the current of the fractional-order memristor (i_M) nominated by Equation (8) in Equation (12), we can determine the dynamics of the proposed fractional-order memristive chaotic circuit as follows in Equation (13).

$$\begin{aligned} \frac{d^q i_L}{dt^q} &= \frac{1}{L}v_C \\ \frac{d^q v_C}{dt^q} &= \frac{1}{C}\left(-i_L - \left(\alpha z^2 - \beta\right)v_M\right) \\ \frac{d^q z}{dt^q} &= -av_M - bz + kv_M^2 z \end{aligned} \tag{13}$$

In order to obtain dimensionless dynamics for Equation (13), let $i_L = x$, $v_C = y$, $1/L = d$, and $1/C = g$; therefore, the fractional-order memristive chaotic system can be described by the following Equation (14).

$$\begin{aligned} \frac{d^q x}{dt^q} &= dy \\ \frac{d^q y}{dt^q} &= g\left(-x - \left(\alpha z^2 - \beta\right)y\right) \\ \frac{d^q z}{dt^q} &= -ay - bz + ky^2 z \end{aligned} \tag{14}$$

In Equation (14), d, g, α, β, a, b, and k present the system parameters, x, y, and z present the system state variables, and q $(0 < q < 1)$ is the system fractional order. In the numerical simulation, the proposed system (14) exhibits chaos when its parameters are chosen as $d = 4$, $g = 0.5$, $\alpha = 1$, $\beta = 1$, $a = 0.25$, $b = 5$, and $k = 4$ with initial conditions $(x_0, y_0, z_0) = (0.8, 0.8, 0)$ and different fractional orders $(q = 0.95$ and $q = 0.98)$. The chaotic behavior of the fractional-order memristive chaotic system (14) corresponding to these parameters, initial conditions, and fractional orders is displayed in Figure 8 by a form of phase portrait chaotic attractors in two-dimensional (2D) and 3D arrangements.



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

(**c**) (**d**)

Figure 8. The chaotic attractors phase portraits of the fractional-order memristive chaotic system (14): (**a**) *x*-*y*; (**b**) *y*-*z*; (**c**) *x*-*z*; (**d**) 3D arrangement (*x*-*y*-*z*).

The equilibria (equilibrium points) of a fractional-order memristive-based simple chaotic system can be determined by equalizing the derivative representations of the system (14) to zero as in $\frac{d^q x}{dt^q} = 0$, $\frac{d^q y}{dt^q} = 0$, and $\frac{d^q z}{dt^q} = 0$. Therefore, the following Equation (15) has been obtained.

$$\begin{aligned} \frac{d^q x}{dt^q} &= dy = 0 \\ \frac{d^q y}{dt^q} &= g\left(-x - \left(\alpha z^2 - \beta\right) y\right) = 0 \\ \frac{d^q z}{dt^q} &= -ay - bz + ky^2 z = 0 \end{aligned} \tag{15}$$

The equilibria of the system (14) can be obtained by solving the above Equation (15). Thus, the fractional-order memristive chaotic system (14) has only one equilibrium point (single equilibrium) at the origin (x^*, y^*, z^*) = (0, 0, 0).

Definition 1. *Consider the following fractional-order system described by the following Equation (16) [39].*

$$\frac{d^q x(t)}{dt^q} = f(x(t)) \tag{16}$$

The equilibrium points of $f(x(t))$ are locally asymptotically stable if all eigenvalues λ_i (i = 1,2,3 ... n) of the Jacobian matrix $J = \partial f(x(t))/\partial x(t)$ evaluated at the equilibrium points satisfy $|arg(\lambda_i)| > q\frac{\pi}{2}$.

The Jacobian matrix of the system (14) is determined by linearizing as described as follows in Equation (17).

$$J = \begin{bmatrix} 0 & d & 0 \\ -g & -g(\alpha z^2 - \beta) & -2\alpha gyz \\ 0 & -a + 2kyz & -b + ky^2 \end{bmatrix} \tag{17}$$

Hence, the Jacobian matrix corresponding to the determined equilibrium point (E(0, 0, 0)) has been obtained as defined by Equation (18).

$$J = \begin{bmatrix} 0 & d & 0 \\ -g & g\beta & 0 \\ 0 & -a & -b \end{bmatrix} \tag{18}$$

The Therefore, with the selected parameters d = 4, g = 0.5, α = 1, β = 1, a = 0.25, b = 5, and k = 4, the eigenvalues have been obtained as ($\lambda_1 = -5$, $\lambda_{2,3} = 0.25 \pm 1.3919i$). According to Definition 1, the stability of the equilibrium point (E(0, 0, 0)) depends on the used value of the fractional order (q). In this work, since we used the fractional order (q = 0.98), thus, the equilibrium point (E(0, 0, 0)) can be considered as an unstable equilibrium point. Furthermore, this equilibrium point can be defined as the saddle point of index 2, that is because it has one real eigenvalue in the stable region and two complex conjugates in the unstable region [40]. This single unstable equilibrium point is responsible for exciting the chaotic behavior of the proposed fractional-order memristive chaotic system described by Equation (14).

5. Complex Dynamics of the System

Bifurcation diagrams and Lyapunov exponents are the two basic dynamical tools for investigating the dynamical characteristics of nonlinear chaotic systems [41]. The bifurcation diagrams and Lyapunov exponents are numerically investigated in this section by using MATLAB.

5.1. Bifurcation Diagrams

In nonlinear dynamics and chaos theory, bifurcation diagrams are useful tools for determining complexity and chaos exhibition [42]. The state variable *y(t)* of the new system (14) is plotted in opposition with the system parameter α, and with respect to the system fractional order (q), in order to investigate the system's dynamical behavior using bifurcation diagrams.

The bifurcation diagram, as exposed in Figure 9, was used to show the influence of the parameter α on the system's dynamical behavior. Table 1 shows the other used system parameters, including d, g, β, a, b, and k, initial conditions (x_0, y_0, z_0), and fractional order (q). As can be seen in Figure 9, the proposed system displays chaotic behavior for a not small range of parameter α ($0 < \alpha < 35$).

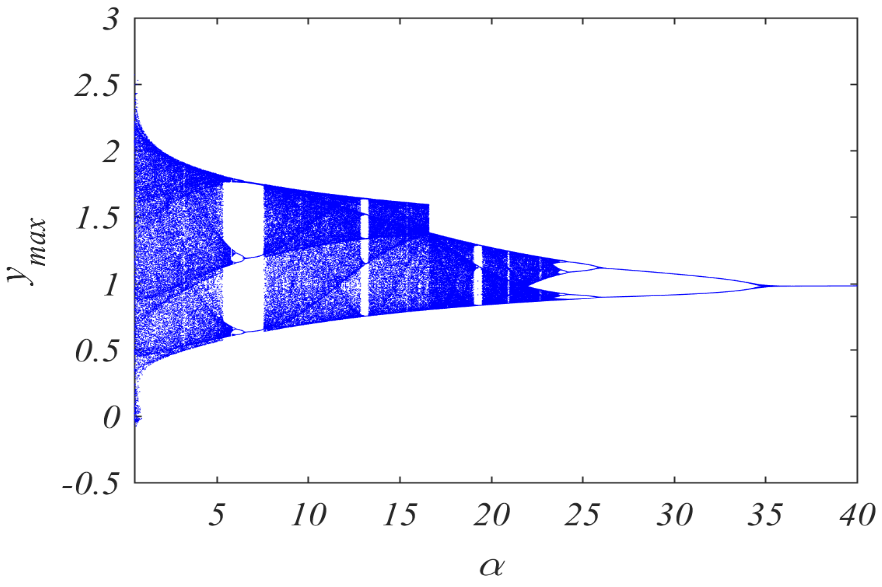


Figure 9. The system (14) bifurcation diagram with respect to changing parameter α.

Table 1. The system (14) parameters used in plots of Figures 9 and 10.

Figure 9		Figure 10	
Parameter	**Value**	**Parameter**	**Value**
d	4	d	4
g	0.5	g	0.5
α	Variable	α	1
β	1	β	1
a	0.25	a	0.25
b	5	b	5
k	4	k	4
fractional order (q)	0.98	fractional order (q)	Variable
x_0	0.8	x_0	0.8
y_0	0.8	y_0	0.8
z_0	0	z_0	0

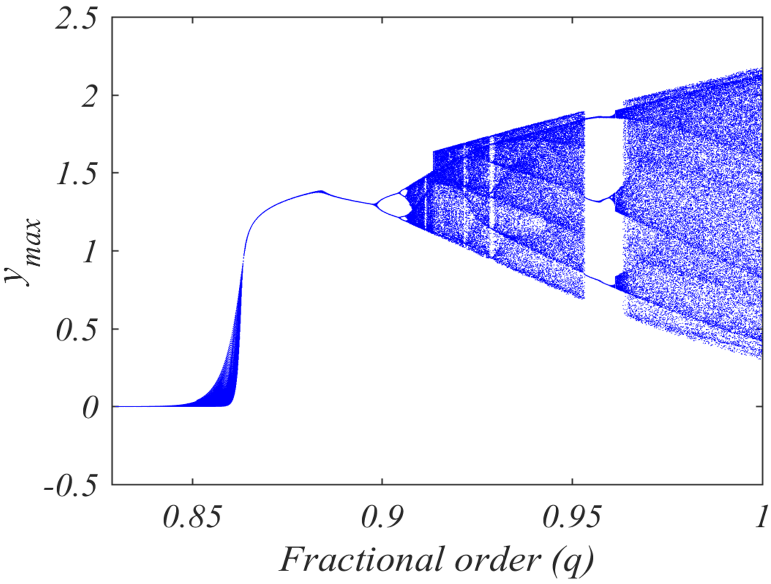


Figure 10. The system (14) bifurcation diagram with respect to changing system fractional order (q).

Moreover, the dynamical behaviors of the system (14) are investigated by the bifurcation diagrams of the system fractional order against the state variable *y(t)* as shown in Figure 10, where the used system parameter α is fixed and the other system parameters are cho-sen as illustrated in Table 1. The system (14) can excite chaotic behavior when the system fractional order is $q > 0.892$, as shown in the bifurcation diagram in Figure 10. Different bifurcation topological patterns are displayed by the suggested fractional-order memristive chaotic system described by Equation (14) as shown by the obtained bifurcation diagrams in Figures 9 and 10. These obtained results show that the new fractional-order memristive chaotic system can produce chaotic attractors. The investigated bifurcation diagrams in Figures 9 and 10, Roberto Garrappa's process [43] with a step size (h = 0.005), and an innovative code that we designed have been used to plot the bifurcation diagrams.

5.2. Lyapunov Exponents

The Lyapunov exponents are calculated to determine whether the proposed system exhibits the chaoticity phenomena; at least one positive Lyapunov exponent in the nonlinear dynamics system confirms that these systems exhibit chaos [44,45]. The Lyapunov exponents are determined versus the time (1000 s) as shown in Figure 11.

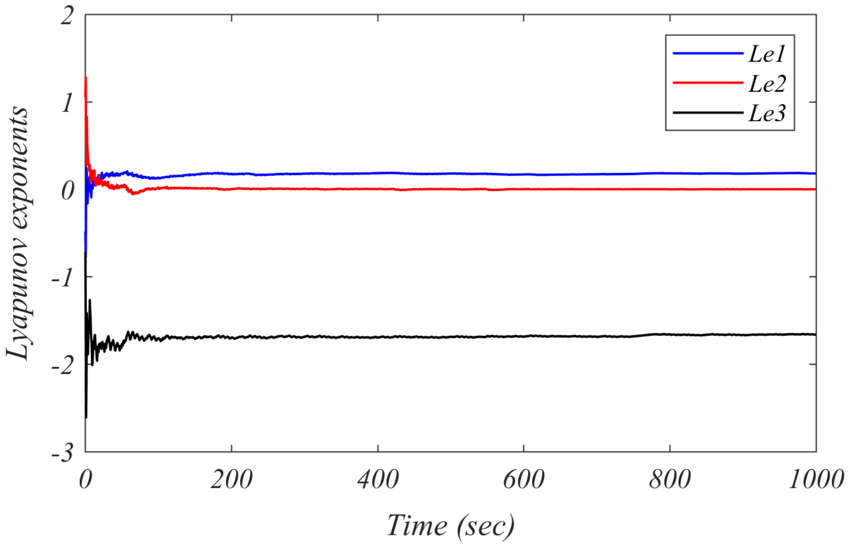


Figure 11. The system (14) Lyapunov exponents versus the time.

Where, *Le1* = 0.182613, *Le2* = 0.000821, and *Le3* = −1.664100 are the consistent Lyapunov exponents obtained. The presence of positive Lyapunov exponent (*Le1* and *Le2*) suffices to establish that the system (14) is capable of exhibiting chaos. Additionally, Lyapunov exponents are considered with respect to varying the system fractional order to $q \in [0.8, 1]$ as displayed in Figure 12. The Lyapunov exponents are *Le1* = 0.1636, *Le2* = 0.1042, and *Le3* = 0.5025, as shown in Figures 11 and 12, indicating a chaotic exhibition by the proposed system. In plotting both Figures 11 and 12, the used system parameters, initial conditions, and fractional order (q) are selected as illustrated in Table 2.

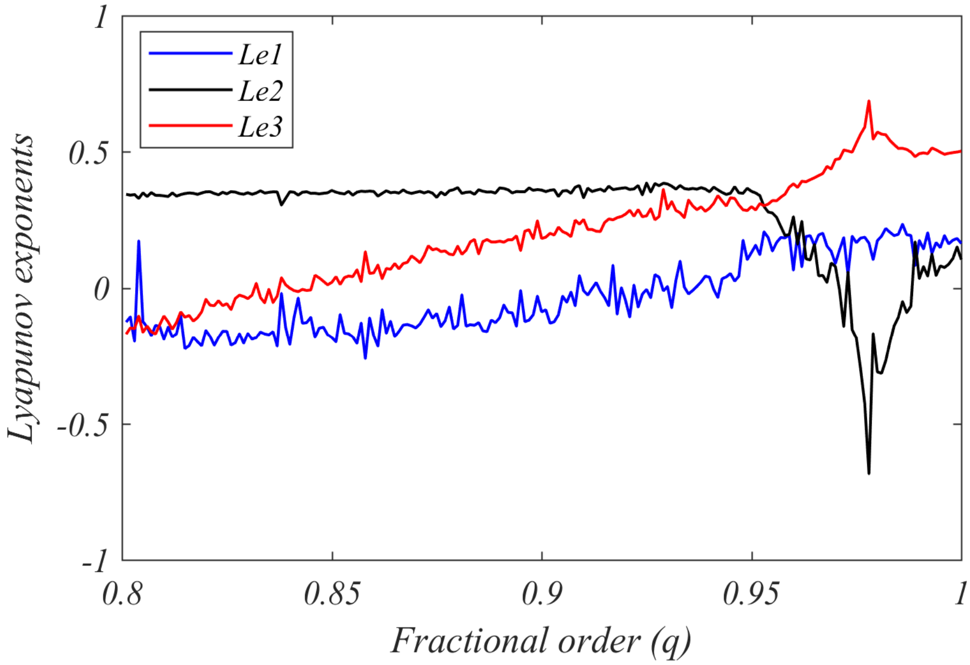


Figure 12. The system (14) Lyapunov exponents against changing the system fractional order (q).

Table 2. The system (14) parameters used in plots of Figures 11 and 12.

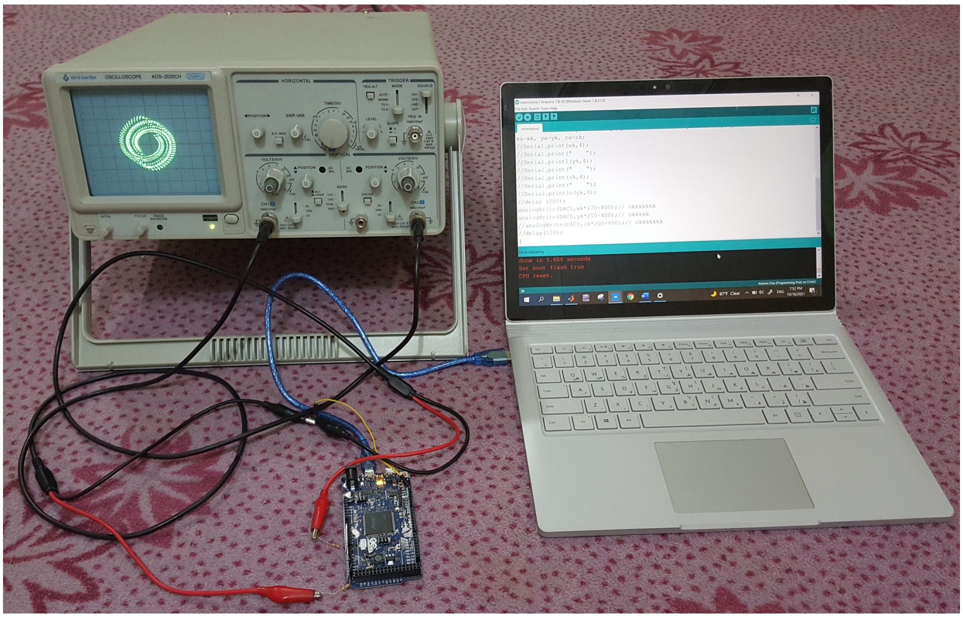
Figure 11		**Figure 12**	
Parameter	**Value**	**Parameter**	**Value**
d	4	d	4
g	0.5	g	0.5
α	1	α	1
β	1	β	1
a	0.25	a	0.25
b	5	b	5
k	4	k	4
fractional order (q)	0.98	fractional order (q)	Variable
x_0	0.8	x_0	0.8
y_0	0.8	y_0	0.8
z_0	0	z_0	0

6. Microcontroller Implementation

The key idea of this section is to demonstrate the feasibility of using the proposed fractional-order memristive chaotic system in real-world applications. In hardware, fractional-order chaotic systems can be digitally implemented using a variety of embedded devices such as Raspberry Pi, DSP boards, FPGA boards, and microcontrollers as well as implementation by an analog electronic circuit. In this work, the new fractional-order memristive chaotic system described by Equation (14) has been digitally implemented by using a microcontroller (Arduino Due). The discrete technique described in [46] was employed.

In recent years, the Arduino Due has become the most popular open-source electronic prototyping platform in a variety of disciplines [47]. The Arduino Due is a programmable microcontroller digital device that has an Atmel SAM3X8E with an ARM Cortex-M3 processor. It has a structure that allows it to perform complex arithmetic operations. In a short description, it has the following characteristics: 4 UARTs, 3.3 V operating voltage, power jack 2 TWI, 2 DAC (digital to analog), SPI header, 32-bit ARM core microcontroller, JTAG header, 84 MHz clocks, 12 analog inputs, 54 digital input/output pins, 512 KB flash memory, and USB-OTG-capable connection [48].

To program the ARM microcontroller through the native USB port (serial port), the Arduino IDE employs an Arduino-specific programming language that is equivalent to the C++ programming language [49]. The following are some of the most significant advantages of utilizing this microcontroller: it has a 12-bit resolution for its two peripherals, DAC0 and DAC1. It also has a low cost when compared to other embedded devices such as FPGAs and DSP boards. The Arduino Due microcontroller setup for implementing the new fractional-order memristive chaotic system is shown in Figure 13.



```
xa=xk, ya=yk, za=zk;
//Serial.print(xk,4);
//Serial.print("    ");
//Serial.printl(yk,4);
//Serial.print("    ");
//Serial.print(zk,4);
//Serial.print("    ");
//Serial.println(yk,4);
//delay (200);
analogWrite(DAC1,xk*170+800);// okkkkkkk
analogWrite(DAC0,yk*210+400);// okkkkk
//analogWrite(DAC0,zk*200+800);// okkkkkkk
//delay(100);
}
```

```
Done uploading
done in 5.800 seconds
Set boot flash true
CPU reset.
```

memristive | Arduino 1.8.16 (Windows Store 1.8.51.0)
File Edit Sketch Tools Help
memristive
Arduino Due (Programming Port) on COM3
OSCILLOSCOPE
AOS-2020CH

Figure 13. The hardware setup for implementing the new fractional-order memristive chaotic system via a microcontroller (Arduino Due).

As shown in Figure 14, the ADC0 and DAC1 are used to display the experimental results of the $v_M - i_M$ characteristics of the fractional-order memristor given by Equation (8) using an analog oscilloscope. The amplitude and frequency of the applied voltage to the mersister are 15 V and 1 Hz, respectively, with fractional-order derivative value (q = 0.98).

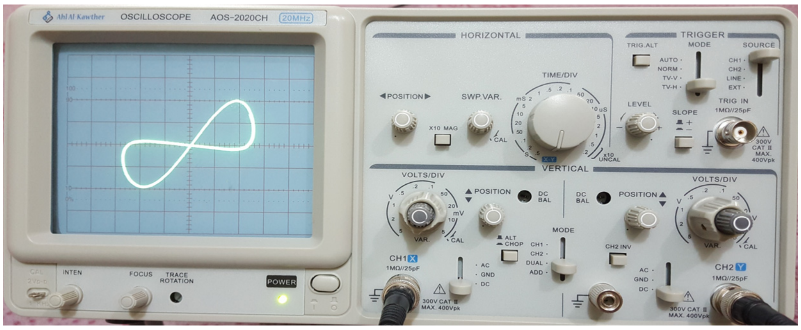
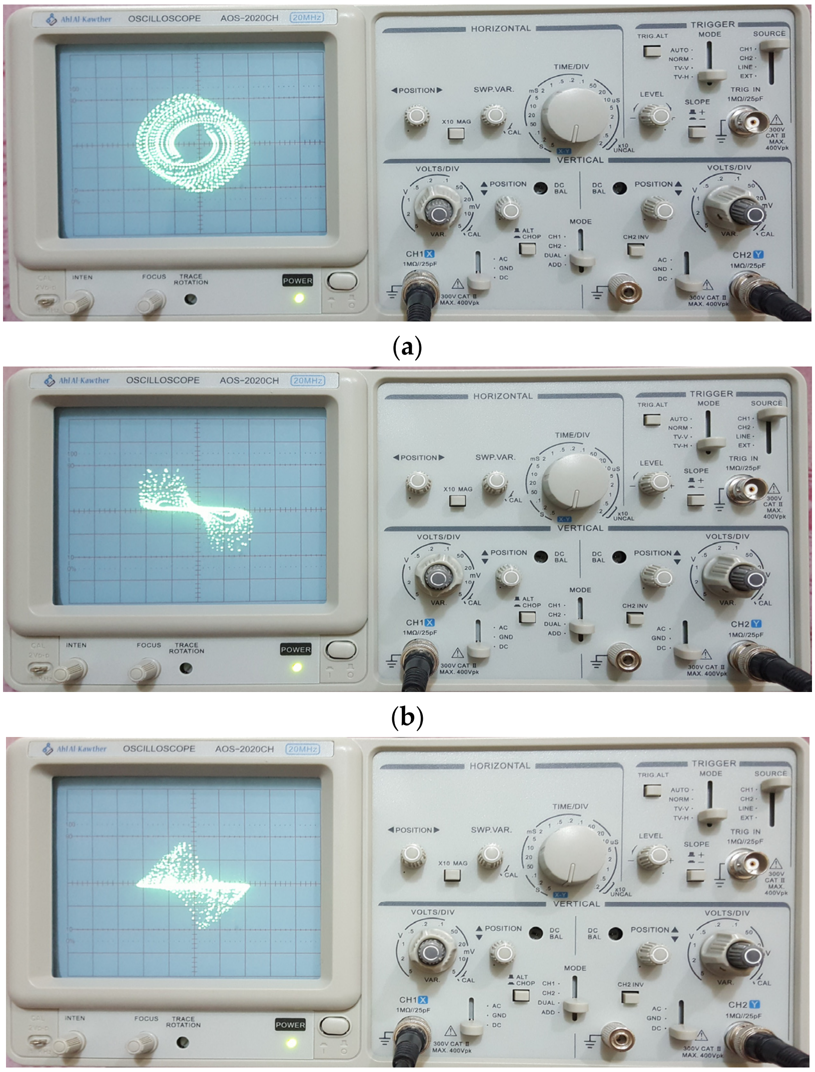


Figure 14. The obtained experimental results of the $v_M - i_M$ characteristics of the fractional-order memristor.

The phase portraits of chaotic attractors of the fractional-order memristive chaotic system described by Equation (14) are shown in Figure 15. In the experimental investigation, the system parameters are chosen as d = 4, g = 0.5, α = 1, β = 1, a = 0.25, b = 5, and k = 4 with initial conditions (x_0, y_0, z_0) = (0.8, 0.8, 0) and fractional-order derivative value (q = 0.98).



(**a**)

(**b**)

(**c**)

Figure 15. The phase portraits of chaotic attractors of the proposed fractional-order memristive chaotic system obtained from the microcontroller implementation: (**a**) *x*-*y*; (**b**) *y*-*z*; (**c**) *x*-*z*.

7. Image Encryption Application

Chaotic encryption techniques are successfully used to encrypt a wide range of images, from medical to remote sensing and beyond [50]. In this section, we offer the application of a new simple fractional-order memristive chaotic system in an image cryptosystem approach. The fractional-order chaotic system described by Equation (14) generates chaotic signals x, y, and z. We will encrypt and decrypt an image by combining these generated chaotic signals with the original image. Figure 16 depicts the overall encryption and decryption procedure.

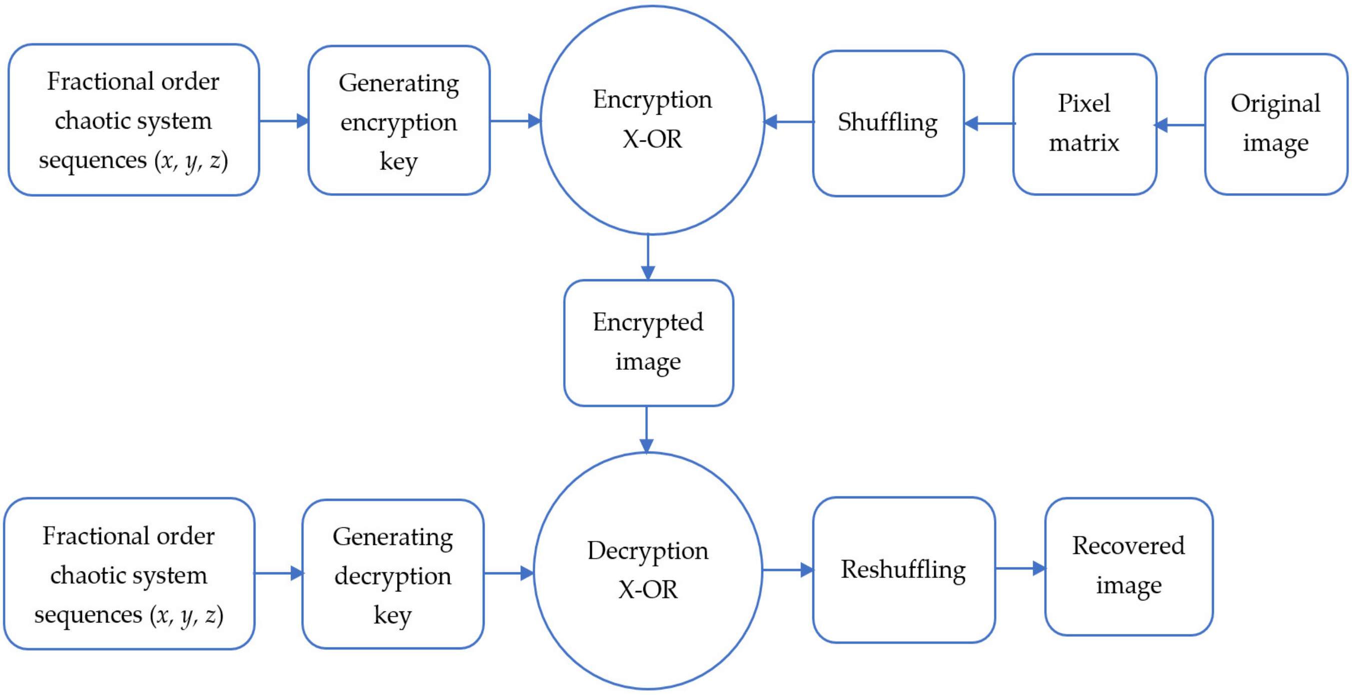

Fractional order chaotic system sequences (*x*, *y*, *z*)
Generating encryption key
Encryption X-OR
Shuffling
Pixel matrix
Original image
Encrypted image
Fractional order chaotic system sequences (*x*, *y*, *z*)
Generating decryption key
Decryption X-OR
Reshuffling
Recovered image

Figure 16. Image encryption and decryption block diagram based on the proposed fractional-order memristive chaotic system.

The following are the detailed steps for the encryption algorithm in the proposed cryptosystem:

Step 1. Read an original grayscale image to obtain its pixels as grayscale values matrix $I_{\mathrm{M*N}}$ (where M and N denote the row and column of the image pixels) and change this matrix to1D vector as $I = \{I_1, \mathrm{I}_2, \ldots, I_{\mathrm{MN}}\}$.
Step 2. Before using the obtained grayscale values 1D vector in the encryption process, shuffle this grayscale values 1D vector by arbitrarily moving these values. The histogram will not change as a result of this process, but it will make it more difficult for a burglar to decrypt the image without knowing the exact shuffling method.
Step 3. Set the initial values of the fractional-order memristive chaotic system (14) (x_0, y_0, z_0), select its fractional order (q), and its parameters (d, g, α, β, a, b, and k).
Step 4. Simulate the simple fractional-order memristive chaotic system (14), iterate constantly, and randomly choose MN set of solutions to generate the chaotic sequence. $S = \{S_1, S_2, \ldots, S_{\mathrm{MN}}\}$. (These solution sets are selected randomly from the obtained values of the system (14) variables (x, y, and z)).
Step 5. To obtain secret keys $K = \{K_1, K_2, \ldots, K_{\mathrm{MN}}\}$, preprocess the sequence $S = \{S_1, S_2, \ldots, S_{\mathrm{MN}}\}$. These secret keys are gained according to the following mathematical operations applied to the obtained system (14) chaotic sequence in Step 4 [51].

$$K_i = \left| round\left(mod(|(S_i - floor(|S_i|)|) * 5 * 10^5\right), 256)) \right|;\ i = 1,\ 2, \ldots,\ \mathrm{MN}.$$

Step 6. Encrypt the pixels of the original image $I = \{I_1, I_2, \ldots, I_{\mathrm{MN}}\}$ using the obtained code in step code as:

$$E_i = I_i \oplus K_i$$

where $\oplus$ denotes the XOR process and the $E = \{E_1, E_2, \ldots\ E_{\mathrm{MN}}\}$ is the obtained 1D vector representation of the encrypted image.

Step 7. Reform the 1D encrypted vector $E = \{E_1, E_2, \ldots\ E_{\mathrm{MN}}\}$ to obtain 2D pixels of the encrypted image.

To restore the original image, the decryption procedure is a complete inverse operation. Since we employed a symmetric encryption algorithm, the cryptosystem sides (source and destination) can exchange the encryption/decryption keys based on a secret approach. There are many common approaches for doing this, such as previously saving the encryption/decryption keys and exchanging these keys through a secret channel or via a disguised trusted postman.

8. Numerical Simulation Results

The simulation results will be presented in this section to demonstrate the efficiency of the used encryption and decryption method with "Lena.png" original image which is a 512 × 512 grayscale image. In the simulation, the system (14) parameters are selected as $d = 4$, $g = 0.5$, $\alpha = 1$, $\beta = 1$, $a = 0.25$, $b = 5$, and $k = 4$ with initial conditions $(x_0, y_0, z_0) = (0.8, 0.8, 0)$ and fractional order ($q = 0.98$) for generating 262,144 samples corresponding to the total number of the original image pixels (512 × 512). These 262,144 samples are responsible for generating the secret keys $K = \{K_1, K_2, \ldots, K_{MN}\}$ which are mentioned in Step 5 in the above section (Section 4), where MN = 262,144. Figure 17a–c show the original image, encrypted image (cipher image), and the recovered image, respectively. The results of Figure 17 show that the applied cryptosystem approach is effective: it is clear that the encrypted image in Figure 17b is completely different from the original image in Figure 17a; also, the cipher image is successfully decrypted to give the recovered image in Figure 17c, which is exactly identical to the original image.

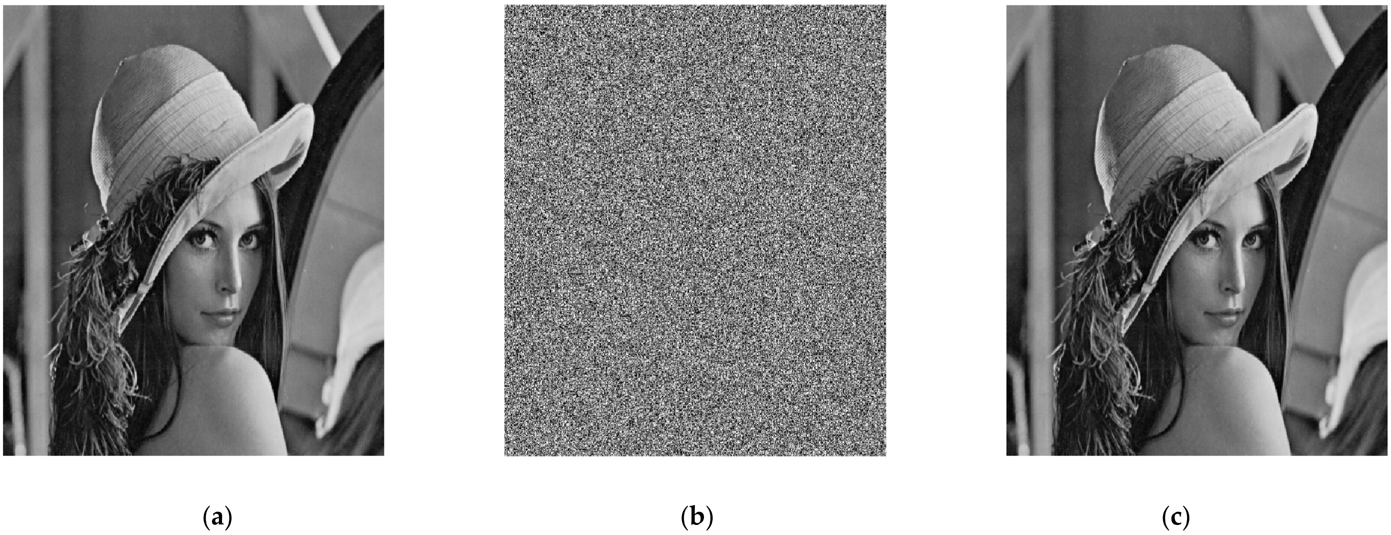


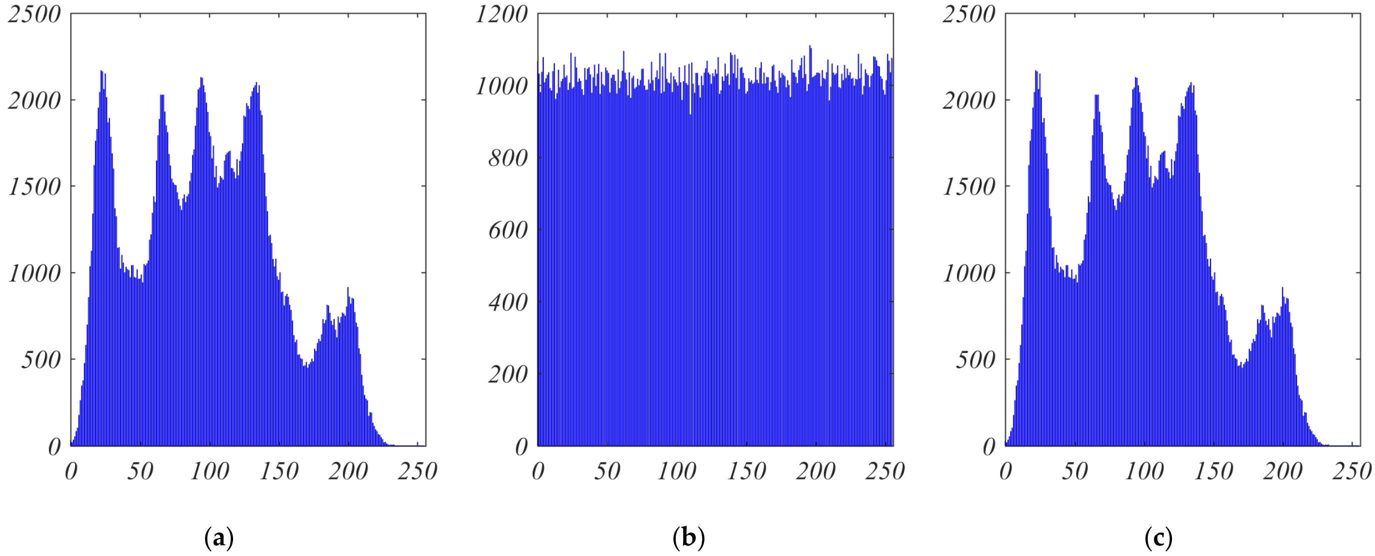
Figure 17. Simulation results of encryption and decryption process of "Lena.png" 512 × 512 grayscale image: (**a**) the original image; (**b**) encrypted image; (**c**) the decrypted image.

9. Cryptanalysis

As is known, a good encryption process should be resistant to all known attacks, be sensitive to the secret key, and have a big enough keyspace to prevent pirate attacks [52]. In this work, information entropy, plain-image sensitivity, correlation coefficient among adjacent pixels, and other standard characteristics are used to test the efficiency of image cryptosystems.

9.1. Histogram Analysis

Any image's histogram is a graph that depicts the distribution of pixel intensity levels. There are 256 different intensities in an 8-bit grayscale image, for example. As a result, the histogram will show 256 numbers indicating the distribution of pixels among the intensity values. An encrypted image's histogram should differ from the original image's histogram both statistically and visually. A decent encrypted image's histogram must have a somewhat uniform shape in order to resist the statistical attack. The histograms of the original image, encrypted image, and the recovered (decrypted) image are displayed in Figure 18a–c, respectively.



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

Figure 18. The histogram: (**a**) the original image histogram; (**b**) encrypted image histogram; (**c**) the decrypted image histogram.

When comparing the histograms in Figure 18a,b, it can be noted that the distribution of the encrypted image histograms differs significantly from that of the original image and that the grayscale values of the encrypted image have a uniform distribution, demonstrating the method's robustness against any statistical attacks. Moreover, we can note that the histogram distribution for the decrypted image in Figure 18c is identical to the original image seen in Figure 18a. As a result of these verdicts, the encrypted image is secure against statistical attacks using this encryption method, and the original image can be recovered successfully.

9.2. Keyspace Analysis

When a pirate force assault occurs, the keyspace of a cryptosystem is a critical aspect of security [53]. In our work, the fractional-order memristive chaotic system (14) is responsible for generating the secret keys $K = \{K_1, K_2, \ldots, K_{MN}\}$. Thus, the system (14) fractional order (q), its initial values (x_0, y_0, z_0), and its parameters (d, g, α, β, a, b, and k) can be considered as the secret keys. As mentioned in the introduction section, the fractional-order chaotic systems exhibit very high sensitivity to small changes in the used fractional order, initial conditions, and the system parameters. We assume that each entered key has a 10^{-15} step-change, then the total keyspace can be calculated as $(10^{15})^{13} = 10^{195} \approx 2^{648}$. As a result, the used encryption method's keyspace is large enough for resisting all types of pirate force attacks.

9.3. Key Sensitivity Analysis

Highly secure encryption algorithms request high key sensitivity, which means that the encrypted image cannot be decrypted correctly even if the encryption and decryption keys change only slightly [54]. The strong encryption technique should be highly sensitive to any changes in the encryption/decryption keys. This ensures a cryptosystem's security against pirate force attacks. Here, the fractional-order derivative value (q), initial values (x_0, y_0, z_0), and the parameters (d, g, α, β, a, b, and k) of the fractional-order memristive chaotic system (14) determine the key sensitivity in the applied encryption approach. In this work, the key sensitivity was measured using the net pixels change rate (NPCR) and the unified average changing intensity (UACI). They calculate the impact of small changes to a secret key in recovering the original image. Higher NPCR and UACI scores indicate that the encryption approach is more robust to different attacks [55]. The NPCR determines the difference in pixel's absolute number change rate between two images as a percentage. On the other hand, the average intensity of discrepancies between the two images is computed by UACI. The NPCR and UACI can be calculated by the following Equations (19) and (20), respectively [56].

$$NPCR = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |sign(I(i,j) - D(i,j))|}{M.N} \times 100\% \tag{19}$$

$$UACI = \frac{1}{255} \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} |I(i,j) - D(i,j)|}{M.N} \times 100\% \tag{20}$$

where $M \times N$ presents the image size, $I(i, j)$ the original image, $D(i, j)$ is the decrypted image, (i, j) the image pixels at the same location, and $I(i, j) \neq \text{D}(i, j)$, ∣sign(·)∣ = 1, otherwise, ∣sign(·)∣= 0. Here, the encryption keys $K = \{K_1, K_2, \ldots, K_{\text{MN}}\}$ are generated from the system (14) with elected parameters as $d = 4$, $g = 0.5$, $\alpha = 1$, $\beta = 1$, $a = 0.25$, $b = 5$, and $k = 4$, initial conditions $(x_0, y_0, z_0) = (0.8, 0.8, 0)$, and fractional order $(q = 0.98)$. By these encryption keys, the 512 × 512 grayscale "Lena.png" original image is encrypted. Consequently, in the NPCR and UACI tests for checking the key sensitivity, only the fractional-order has been very slightly changed to be $q = 0.98 + 10^{-15}$ for the decryption process, and the corresponding NPCR and UACI are found to be 0.99866 and 0.49963, respectively. The obtained simulation results of the recovered image with the abovementioned very slight change in the decryption keys are illustrated in Figure 19.

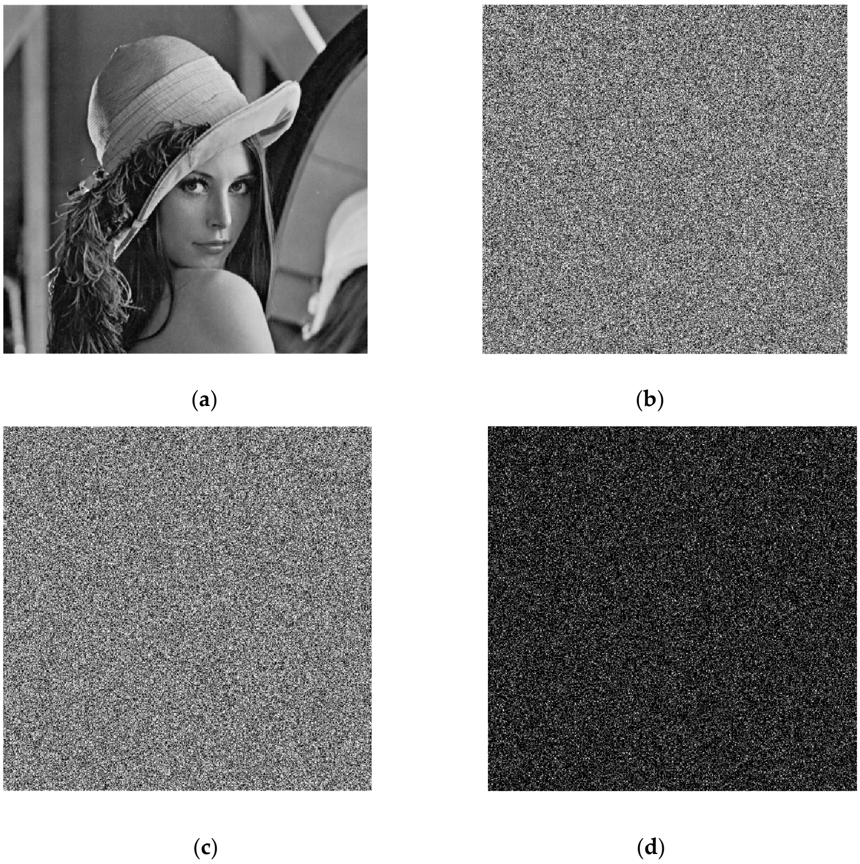

(**a**) (**b**) (**c**) (**d**)

Figure 19. Key sensitivity analysis: (**a**) the original image; (**b**) the encrypted image; (**c**) the recovered image with very slight change (10^{-16} in the fractional order only) in decryption keys; (**d**) the difference between (**a**,**c**).

These findings indicate that the original image cannot be recovered using the wrong keys (even if they differ only slightly from the original key). As a result, the image encryption based on the fractional-order memristive chaotic system (14) is very highly sensitive to the secret keys and it efficiently resists the pirate force attacks.

9.4. Correlation Analysis

The correlation coefficient is computed between the grayscale values of two adjacent pixels and it is used to quantify the unpredictability of data in encrypted images. The original image displays a very strong correlation between its adjacent pixels [57]. A highly secure (efficient) image cryptosystem should be able to reduce the correlation between adjacent pixels, i.e., the security of the cryptosystem is inversely proportional to the obtained correlation coefficient scores [58].

In an image, the correlation coefficient between the grayscale values of two neighboring pixels x, y can be calculated as follows in Equation (21) [59].

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{21}$$

where, x and y represent the adjacent pixel values in the image, $cov(x, y)$ is the covariance, and $D(k)$ (k means x and y) is the variance with which these values can be computed by Equations (22) and (23), respectively, as in the following [60].

$$cov(x,y) = \frac{\sum_{i=1}^{N} (x_i - E(x))(x_i - E(y))}{N} \tag{22}$$

$$D(k) = \frac{\sum_{i=1}^{N} (k_i - E(k))^2}{N} \tag{23}$$

In Equation (22), the image's total number of selected pixels is N and *E(k)* is the average and it can be calculated as follows in Equation (24) [61].

$$E(k) = \frac{\sum_{i=1}^{N} k_i}{N} \tag{24}$$

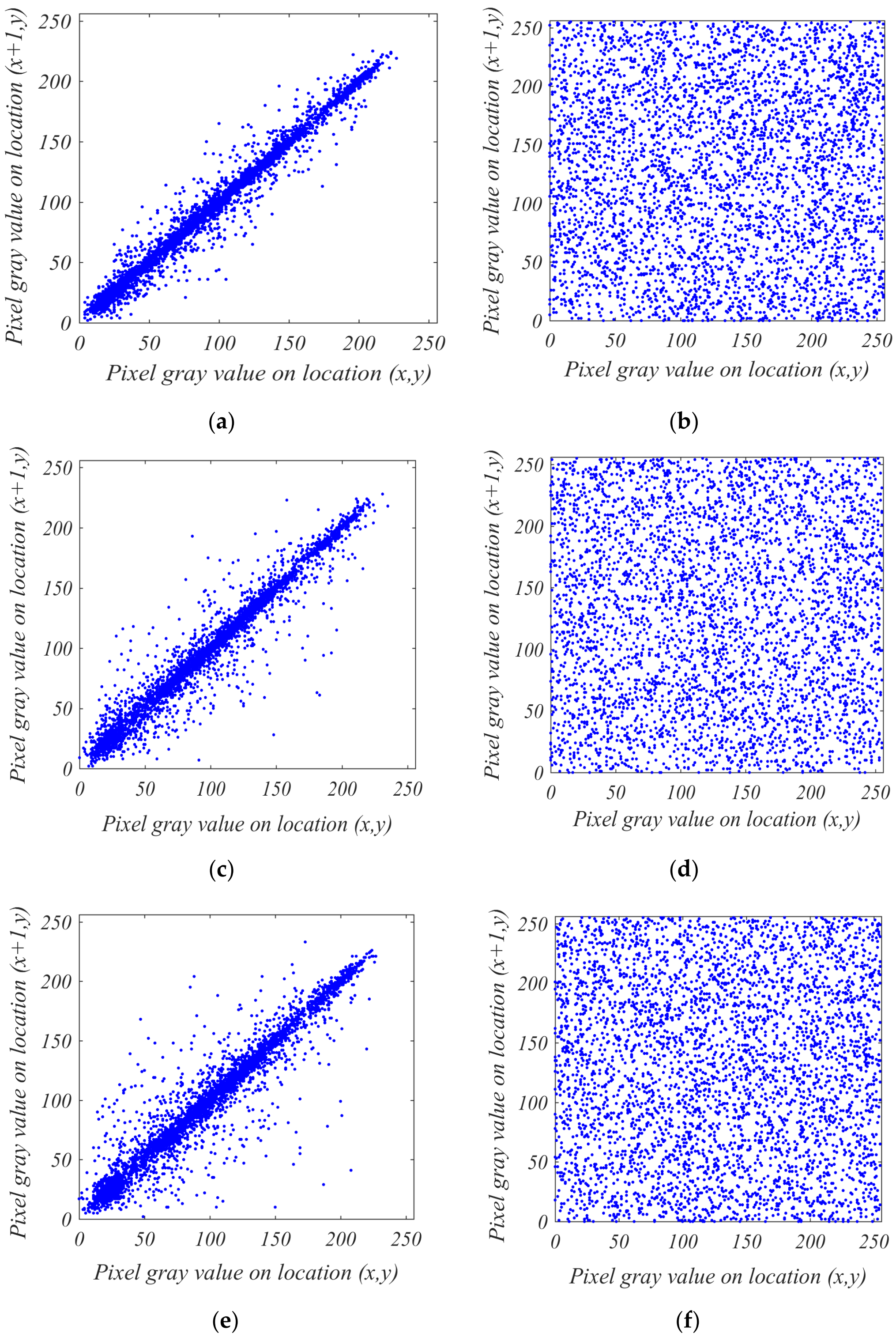
In this analysis, we randomly select 4000 pairs of two neighboring pixels of the original and encrypted images in vertical, horizontal, and diagonal forms, for the correlation confections computation. The obtained correlation confections between two neighboring pixels for the original Lena image and its corresponding encrypted image are shown in Table 3.

Table 3. Correlation coefficients of the original Lena image and its consistent encrypted image.

Direction	Original Image	Encrypted Image
Vertical	0.97241	0.00032
Horizontal	0.98671	0.00054
Diagonal	0.96181	0.00011

The obtained Table 3 data demonstrate that the original image has an extremely strong correlation, whereas encrypted images have very little correlation, indicating that the used encryption approach exhibits high robustness against the pirate force attacks.

Furthermore, the correlation distributions of two vertically, horizontally, and diagonally adjacent pixels for the original Lena image and its corresponding encrypted image are displayed in Figure 20 to visibly show the correlation of the original and encrypted photos.



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

(**c**) (**d**)

(**e**) (**f**)

Figure 20. Correlation distribution between two adjacent pixels of original Lena image and its corresponding encrypted image: (**a**,**b**) vertical correlation; (**c**,**d**) horizontal correlation; (**e**,**f**) diagonal correlation.

It can be seen from Figure 20a,c,e that the original image displays a very significant correlation between the two adjacent pixels. In other words, all of the pixel dots in the original image are clustered along the diagonal, as shown in Figure 20a,c,e. The corresponding encrypted image pixel dots, on the other hand, are dispersed across the whole plane, as seen in Figure 20b,d,f. This means that the encrypted image's correlations between various pixels have considerably decreased. Thus, the encrypted image produces significantly more randomness, making statistical analysis difficult for attackers. This indicates the high security effectiveness of the applied encryption approach.

9.5. Entropy Analysis

The distribution of an image's grayscale values between 0 and 255 is determined by the entropy of the image [62]. It calculates the image's degree of randomness and uncertainty. Because each of the 256 intensity levels of a grayscale image is specified by 8 bits, thus, the ideal theoretical value of information entropy in the encrypted image is 8. The entropy of information is expressed as follows in Equation (25) [63].

$$H(s) = \sum_{i=1}^{255} p(s_i) log_2\left(\frac{1}{p(s_i)}\right) \tag{25}$$

where $p(s_i)$ is the probability of symbol (s_i). The calculated information entropy values of the original grayscale Lena image and its corresponding encrypted images are 7.5946 and 7.9993, respectively. As is clear, the obtained results show that all of the encrypted image's entropy values are very near to the ideal theoretical value of 8. Thus, our cryptosystem shows good performance in resisting the entropy attack.

9.6. Time Efficiency Analysis

The encryption/decryption time efficiency is a critical metric for assessing an encryption algorithm's performance. A computational task's execution time is the maximum amount of time it might take to be completed by any device with perfect accuracy [64]. A practical cryptosystem should have a better encryption speed in addition to security performance [65]. The average time efficiency of the employed encryption/decryption algorithm for the original grayscale Lina image with size 512 × 512 is obtained as 0.3 s. These findings demonstrate the employed encryption algorithm's advantages in terms of time efficiency.

9.7. Comparison Summary

As is known, any work should be compared with similar works in the subject area to prove the performance efficiency of the developed work. Therefore, for all the used cryptanalysis tests, we compare our obtained results with other highlighted works in the introduction section in order to show the high-performance efficiency and security of the suggested fractional-order memristive chaotic system (14) in image encryption application. Table 4 shows this comparison for the encrypted image, where the optimal values of the cryptanalysis test coefficients are selected from the papers that have been used in the comparison. As can be noted from Table 4, in summary, the image encryption approach based on the new fractional-order memristive chaotic system (14) exhibits an excellent encryption effect as well as a high level of security and perfect time efficiency.

Table 4. Cryptosystem metrics comparison with other works.

Algorithm	**Key Space**	*NPCR*	*UACI*	**Vertical** r_{xy}	**Horizontal** r_{xy}	**Diagonal** r_{xy}	*H(s)*	**Time Efficiency**
Ref. [19]	2^{449}	0.99606	0.33489	0.0002	0.0046	0.0005	7.9951	0.9 s
Ref. [20]	2^{530}	0.99640	0.33537	-	-	-	7.9978	-
Ref. [21]	2^{154}	99.6096	0.33459	0.000333	0.000524	0.000872	7.9993	0.3261 s
Ref. [22]	2^{598}	0.9955	0.3325	0.0059	0.0082	0.0007	7.9866	1.02 s
Ref. [23]	2^{285}	0.9964	0.3355	0.000312	0.002088	0.001444	7.9976	1.708 s
Ours	2^{648}	0.99866	0.49963	0.00032	0.00054	0.00011	7.9993	0.3 s

Finally, grayscale peppers with 256 × 256 size and penguins with 546 × 636 size have been encrypted and decrypted. This has been exposed in order to examine the performance of the used encryption approach for encrypting different-sized images. Figure 21a–c show the peppers' original image, encrypted image, and recovered image, respectively. Consequentially, Figure 21d–f demonstrate the histogram graph corresponding to Figure 21a–c, respectively. The penguins' original image, encrypted image, and the recovered image are illustrated in Figure 22a–c respectively. Figure 22d–f show the histogram graph consistent with Figure 22a–c, respectively.

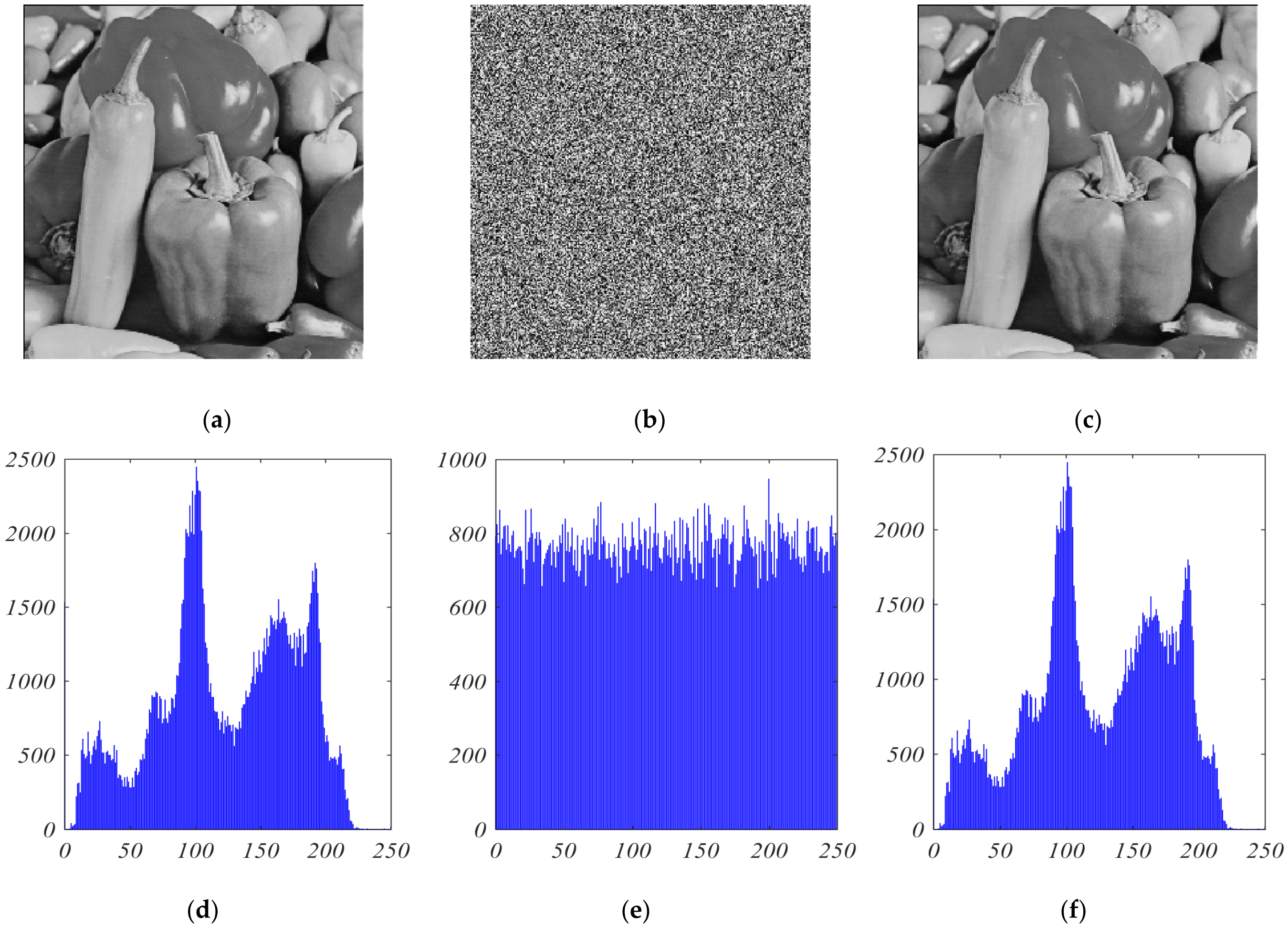


Figure 21. Encryption and decryption of "Peppers.pmb" 256 × 256 grayscale image: (**a**) the original image; (**b**) encrypted image; (**c**) the decrypted image; (**d**) histogram corresponding to (**a**); (**e**) histogram corresponding to (**b**); (**f**) histogram corresponding to (**c**).

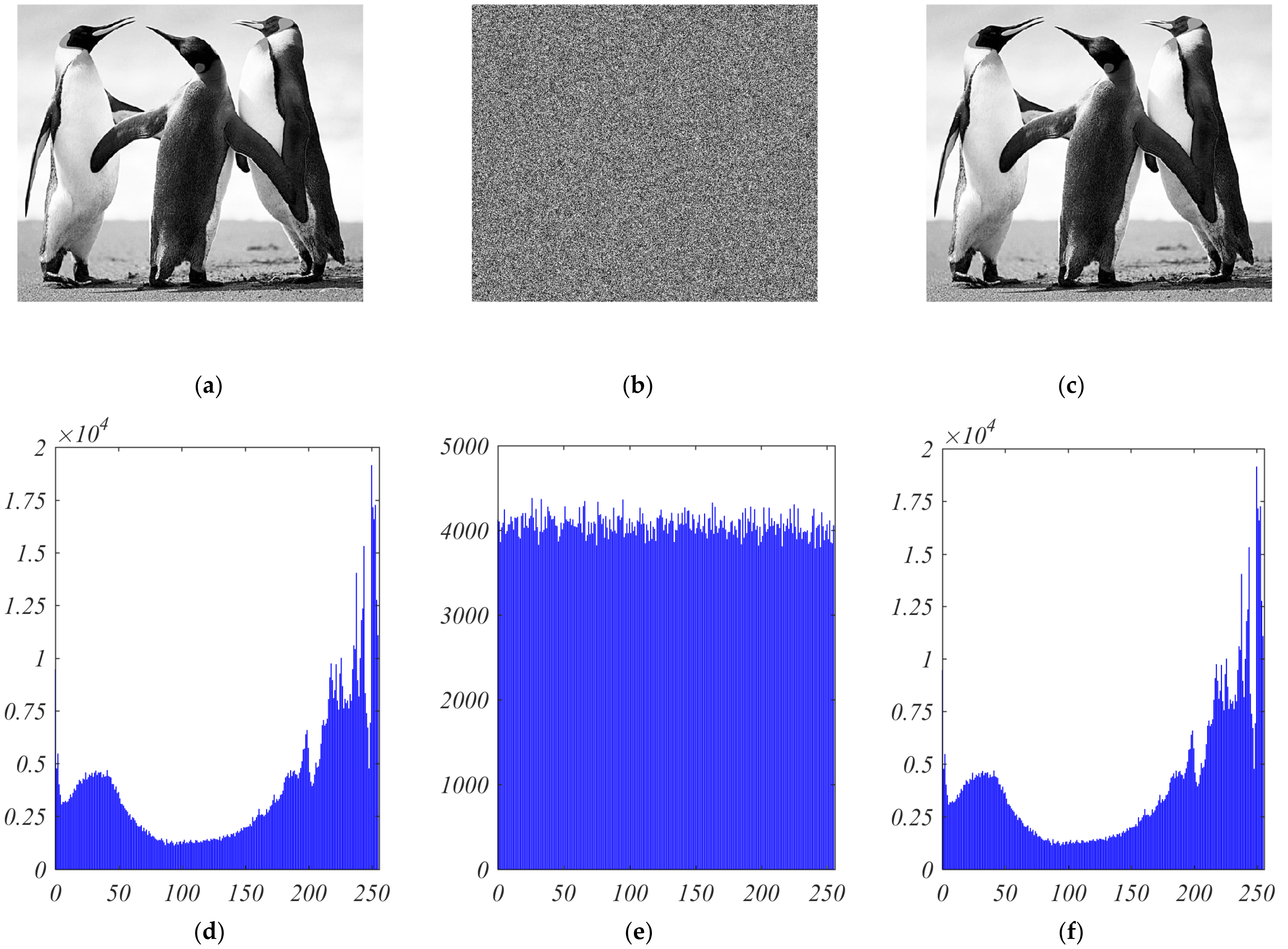


Figure 22. Encryption and decryption of "penguins.jpg" 546 × 636 grayscale image: (**a**) the original image; (**b**) encrypted image; (**c**) the decrypted image; (**d**) histogram corresponding to (**a**); (**e**) histogram corresponding to (**b**); (**f**) histogram corresponding to (**c**).

10. Conclusions

The development, testing, analysis, and electronic realization of a fractional-order memristor are described in this article. As a result, this memristor is used to suggest a new simple 3D fractional-order memristive chaotic system with a single unstable equilibrium point. The equilibrium point, chaotic attractors, bifurcation diagrams, and Lyapunov exponents were investigated analytically and numerically to show the nonlinear dynamical behaviors of this system. Furthermore, a microcontroller (Arduino Due) was also used to show that the proposed memristive system can be implemented simply in real-world applications. The new simple fractional-order memristive chaotic system exhibits extreme sensitivity to small changes in initial values, parameters, and its fractional-order derivative value (q), according to the dynamic analysis. Moreover, the state variables in the current model display a wide range of nonlinear dynamical behaviors. Therefore, the system generates chaotic sequences with a high level of randomness. Consequently, it was used in a cryptosystem algorithm for encrypting grayscale original images. The memristive chaotic system's initial conditions, state variables, parameters, and fractional-order derivative values were used to contract the keyspace of the employed cryptosystem. The key benefits of using the Arduino Due board to implement the proposed memristive system are its simplicity and low cost of implementation when compared to other more expensive devices such as DSPs and FPGAs. The MATLAB simulation findings are congruent with the experimental results, demonstrating that the system is suitable for use in real-world applications. The cryptanalysis metric tests are exposed in detail, including histogram analysis, keyspace analysis, key sensitivity, correlation coefficients, entropy analysis, time efficiency analysis, and comparisons with articles in a similar subject area in order to test the utilized encryption algorithm security strength. Encrypted and decrypted images with different sizes verified the capability of the employed encryption algorithm for encrypting and decrypting images with different sizes. The common cryptanalysis metrics values were determined as keyspace = 2^{648}, *NPCR* = 0.99866, *UACI* = 0.49963, *H(s)* = 7.9993, and time efficiency = 0.3 s. The obtained numerical simulation results and the comprehensive security analyses confirm the effectiveness, high-level security, and excellent time efficiency of the used cryptosystem, as well as its great resistance against various sorts of pirate attacks.

Author Contributions: Conceptualization, Z.-A.S.A.R. and B.H.J.; methodology, Z.-A.S.A.R.; software, Z.-A.S.A.R. and B.H.J.; validation, Z.-A.S.A.R. and B.H.J.; formal analysis, Z.-A.S.A.R., B.H.J. and Y.I.A.A.-Y.; investigation, Z.-A.S.A.R. and B.H.J..; resources, Z.-A.S.A.R., B.H.J., Y.I.A.A.-Y. and R.A.A.-A.; data curation, Z.-A.S.A.R. and B.H.J.; writing—original draft preparation, Z.-A.S.A.R. and B.H.J.; writing—review and editing, Z.-A.S.A.R., B.H.J. and Y.I.A.A.-Y.; visualization, Z.-A.S.A.R., B.H.J. and Y.I.A.A.-Y.; supervision, B.H.J. and R.A.A.-A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Meng-Lewis, Y.; Wong, D.; Zhao, Y.; Lewis, G. Understanding complexity and dynamics in the career development of eSports athletes. *Sport Manag. Rev.* **2021**. [CrossRef]
2. Rahman, Z.-A.S.A.; Jasim, B.H.; Al-Yasir, Y.I.A.; Hu, Y.-F.; Abd-Alhameed, R.A.; Alhasnawi, B.N. A New Fractional-Order Chaotic System with Its Analysis, Synchronization, and Circuit Realization for Secure Communication Applications. *Mathematics* **2021**, *9*, 2593. [CrossRef]
3. Mahmoud, E.E.; Trikha, P.; Jahanzaib, L.S.; Almaghrabi, O.A. Dynamical analysis and chaos control of the fractional chaotic ecological model. *Chaos Solitons Fractals* **2020**, *141*, 110348. [CrossRef]
4. Liao, T.-L.; Chen, H.-C.; Peng, C.-Y.; Hou, Y.-Y. Chaos-based secure communications in biomedical information application. *Electronics* **2021**, *10*, 359. [CrossRef]
5. Rahman, Z.-A.S.A.; Jasim, B.H.; Al-Yasir, Y.I.A.; Abd-Alhameed, R.A.; Alhasnawi, B.N. A New No Equilibrium Fractional Order Chaotic System, Dynamical Investigation, Synchronization, and Its Digital Implementation. *Inventions* **2021**, *6*, 49. [CrossRef]
6. Vaidyanathan, S.; Volos, C. *Advances in Memristors, Memristive Devices and Systems*; Springer: Berlin/Heidelberg, Germany, 2017; Volume 701.
7. Rahma, F.; Muneam, S. *Memristive Nonlinear Electronic Circuits: Dynamics, Synchronization and Applications*; Springer: Berlin/Heidelberg, Germany, 2019.
8. Shen, Y.; Wang, G. History Erase Effect of Real Memristors. *Electronics* **2021**, *10*, 303. [CrossRef]
9. Peng, Y.; He, S.; Sun, K. A higher dimensional chaotic map with discrete memristor. *AEU-Int. J. Electron. Commun.* **2021**, *129*, 153539. [CrossRef]
10. Akgül, A.; Rajagopal, K.; Durdu, A.; Pala, M.A.; Boyraz, Ö.F.; Yildiz, M.Z. A simple fractional-order chaotic system based on memristor and memcapacitor and its synchronization application. *Chaos Solitons Fractals* **2021**, *152*, 111306. [CrossRef]
11. Zhou, L.; Wang, C.; Zhou, L. Generating four-wing hyperchaotic attractor and two-wing, three-wing, and four-wing chaotic attractors in 4D memristive system. *Int. J. Bifurc. Chaos* **2017**, *27*, 1750027. [CrossRef]
12. Lozynskyy, A.; Chaban, A.; Perzyński, T.; Szafraniec, A.; Kasha, L. Application of Fractional-Order Calculus to Improve the Mathematical Model of a Two-Mass System with a Long Shaft. *Energies* **2021**, *14*, 1854. [CrossRef]
13. Rahman, Z.-A.S.A.; Jassim, B.H.; Al-Yasir, Y.I.A. New Fractional Order Chaotic System: Analysis, Synchronization, and it's Application. *Iraqi J. Electr. Electron. Eng.* **2021**, *17*, 116–123. [CrossRef]
14. Yang, C.; Xie, F.; Chen, Y.; Xiao, W.; Zhang, B. Modeling and analysis of the fractional-order flyback converter in continuous conduction mode by caputo fractional calculus. *Electronics* **2020**, *9*, 1544. [CrossRef]
15. Tavazoei, M.S. Fractional order chaotic systems: History, achievements, applications, and future challenges. *Eur. Phys. J. Spec. Top.* **2020**, *229*, 887–904. [CrossRef]
16. Tlelo-Cuautle, E.; Pano-Azucena, A.D.; Guillén-Fernández, O.; Silva-Juárez, A. *Analog/Digital Implementation of Fractional Order Chaotic Circuits and Applications*; Springer: Berlin/Heidelberg, Germany, 2020.
17. 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]

18. Wen, H.; Zhang, C.; Huang, L.; Ke, J.; Xiong, D. Security Analysis of a Color Image Encryption Algorithm Using a Fractional-Order Chaos. *Entropy* **2021**, *23*, 258. [CrossRef] [PubMed]
19. Alanazi, A.S.; Munir, N.; Khan, M.; Asif, M.; Hussain, I. Cryptanalysis of Novel Image Encryption Scheme Based on Multiple Chaotic Substitution Boxes. *IEEE Access* **2021**, *9*, 93795–93802. [CrossRef]
20. Askar, S.; Al-Khedhairi, A.; Elsonbaty, A.; Elsadany, A. Chaotic Discrete Fractional-Order Food Chain Model and Hybrid Image Encryption Scheme Application. *Symmetry* **2021**, *13*, 161. [CrossRef]
21. Xian, Y.; Wang, X. Fractal sorting matrix and its application on chaotic image encryption. *Inf. Sci.* **2021**, *547*, 1154–1169. [CrossRef]
22. Ding, L.; Ding, Q. A Novel Image Encryption Scheme Based on 2D Fractional Chaotic Map, DWT and 4D Hyper-chaos. *Electronics* **2020**, *9*, 1280. [CrossRef]
23. Zhu, S.; Wang, G.; Zhu, C. A secure and fast image encryption scheme based on double chaotic S-boxes. *Entropy* **2019**, *21*, 790. [CrossRef]
24. Ma, X.; Mou, J.; Liu, J.; Ma, C.; Yang, F.; Zhao, X. A novel simple chaotic circuit based on memristor-memcapacitor. *Nonlinear Dyn.* **2020**, *100*, 2859–2876. [CrossRef]
25. Baleanu, D.; Fernandez, A. On fractional operators and their classifications. *Mathematics* **2019**, *7*, 830. [CrossRef]
26. Sabatier, J.; Agrawal, O.P.; Machado, J.A.T. *Advances in Fractional Calculus*; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4.
27. Oprzędkiewicz, K.; Rosół, M.; Żegleń-Włodarczyk, J. The Frequency and Real-Time Properties of the Microcontroller Implementation of Fractional-Order PID Controller. *Electronics* **2021**, *10*, 524. [CrossRef]
28. Kozioł, K.; Stanisławski, R.; Bialic, G. Fractional-order sir epidemic model for transmission prediction of COVID-19 disease. *Appl. Sci.* **2020**, *10*, 8316. [CrossRef]
29. Khan, H.; Shah, R.; Baleanu, D.; Kumam, P.; Arif, M. Analytical solution of fractional-order hyperbolic telegraph equation, using natural transform decomposition method. *Electronics* **2019**, *8*, 1015. [CrossRef]
30. Jiang, Y.; Zhang, B. Comparative study of Riemann-liouville and caputo derivative definitions in time-domain analysis of fractional-order capacitor. *IEEE Trans. Circuits Syst. II Express Briefs* **2019**, *67*, 2184–2188. [CrossRef]
31. Rahman, Z.-A.S.A.; Al-Kashoash, H.A.A.; Ramadhan, S.M.; Al-Yasir, Y.I.A. Adaptive control synchronization of a novel memristive chaotic system for secure communication applications. *Inventions* **2019**, *4*, 30. [CrossRef]
32. Buscarino, A.; Fortuna, L.; Frasca, M.; Gambuzza, L.V. A gallery of chaotic oscillators based on HP memristor. *Int. J. Bifurc. Chaos* **2013**, *23*, 1330015. [CrossRef]
33. Ascoli, A.; Corinto, F.; Senger, V.; Tetzlaff, R. Memristor model comparison. *IEEE Circuits Syst. Mag.* **2013**, *13*, 89–105. [CrossRef]
34. Guo, Q.; Wang, N.; Zhang, G. A novel current-controlled memristor-based chaotic circuit. *Integration* **2021**, *80*, 20–28. [CrossRef]
35. Tahir, F.R.; Ramadhan, S.M. Analog programmable circuit implementation for memristor. *Iraqi J. Electr. Electron. Eng.* **2018**, *14*, 1–9. [CrossRef]
36. Liu, Y.; Pu, Y.-F.; Shen, X.-D.; Zhou, J.-L. Design of 1/2 (n) order analog fractance approximation circuit based on continued fractions decomposition. *J. Sichuan Univ. Eng. Sci. Ed.* **2012**, *44*, 153–158.
37. Hammouch, Z.; Mekkaoui, T. Circuit design and simulation for the fractional-order chaotic behavior in a new dynamical system. *Complex Intell. Syst.* **2018**, *4*, 251–260. [CrossRef]
38. Zouad, F.; Kemih, K.; Hamiche, H. A new secure communication scheme using fractional order delayed chaotic system: Design and electronics circuit simulation. *Analog Integr. Circuits Signal Process.* **2019**, *99*, 619–632. [CrossRef]
39. Hosseinnia, S.H.; Ghaderi, R.; Mahmoudian, M.; Momani, S. Sliding mode synchronization of an uncertain fractional order chaotic system. *Comput. Math. Appl.* **2010**, *59*, 1637–1643. [CrossRef]
40. Munmuangsaen, B.; Srisuchinwong, B. A hidden chaotic attractor in the classical Lorenz system. *Chaos Solitons Fractals* **2018**, *107*, 61–66. [CrossRef]
41. Jasim, B.H.; Hassan, K.H.; Omran, K.M. A new 4-D hyperchaotic hidden attractor system: Its dynamics, coexisting attractors, synchronization and microcontroller implementation. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 2068–2078. [CrossRef]
42. Mouelas, A.N.; Fozin, T.F.; Kengne, R.; Kengne, J.; Fotsin, H.B.; Essimbi, B.Z. Extremely rich dynamical behaviors in a simple nonautonomous Jerk system with generalized nonlinearity: Hyperchaos, intermittency, offset-boosting and multistability. *Int. J. Dyn. Control* **2020**, *8*, 51–69. [CrossRef]
43. Garrappa, R. Numerical solution of fractional differential equations: A survey and a software tutorial. *Mathematics* **2018**, *6*, 16. [CrossRef]
44. Al-Hussein, A.-B.A.; Tahir, F.R.; Ouannas, A.; Sun, T.-C.; Jahanshahi, H.; Aly, A.A. Chaos Suppressing in a Three-Buses Power System Using an Adaptive Synergetic Control Method. *Electronics* **2021**, *10*, 1532. [CrossRef]
45. Jasim, B.H.; Mjily, A.H.; Al-Aaragee, A.M.J. A novel 4 dimensional hyperchaotic system with its control, synchronization and implementation. *Int. J. Electr. Comput. Eng.* **2021**, *11*, 2974–2985. [CrossRef]
46. Sánchez-López, C. An experimental synthesis methodology of fractional-order chaotic attractors. *Nonlinear Dyn.* **2020**, *100*, 3907–3923. [CrossRef]
47. Kondaveeti, H.K.; Kumaravelu, N.K.; Vanambathina, S.D.; Mathe, S.E.; Vappangi, S. A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations. *Comput. Sci. Rev.* **2021**, *40*, 100364. [CrossRef]
48. Soler-Llorens, J.L.; Galiana-Merino, J.J.; Nassim-Benabdeloued, B.Y.; Rosa-Cintas, S.; Zamora, J.O.; Giner-Caturla, J.J. Design and implementation of an Arduino-based plug-and-play acquisition system for seismic noise measurements. *Electronics* **2019**, *8*, 1035. [CrossRef]

49. Zamora-Arellano, F.; López-Bonilla, O.R.; García-Guerrero, E.E.; Olguín-Tiznado, J.E.; Inzunza-González, E.; López-Mancilla, D.; Tlelo-Cuautle, E. Development of a Portable, Reliable and Low-Cost Electrical Impedance Tomography System Using an Embedded System. *Electronics* **2021**, *10*, 15. [CrossRef]
50. Masood, F.; Boulila, W.; Ahmad, J.; Sankar, S.; Rubaiee, S.; Buchanan, W.J. A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos. *Remote Sens.* **2020**, *12*, 1893. [CrossRef]
51. Xu, Y.; Wang, H.; Li, Y.; Pei, B. Image encryption based on synchronization of fractional chaotic systems. *Commun. Nonlinear Sci. Numer. Simul.* **2014**, *19*, 3735–3744. [CrossRef]
52. Lin, C.-Y.; Wu, J.-L. Cryptanalysis and improvement of a chaotic map-based image encryption system using both plaintext related permutation and diffusion. *Entropy* **2020**, *22*, 589. [CrossRef] [PubMed]
53. Xiang, Y.; Xiao, D.; Zhang, R.; Liang, J.; Liu, R. Cryptanalysis and improvement of a reversible data-hiding scheme in encrypted images by redundant space transfer. *Inf. Sci.* **2021**, *545*, 188–206. [CrossRef]
54. El-Latif, A.A.A.; Abd-El-Atty, B.; Belazi, A.; Iliyasu, A.M. Efficient Chaos-Based Substitution-Box and Its Application to Image Encryption. *Electronics* **2021**, *10*, 1392. [CrossRef]
55. ElKamchouchi, D.H.; Mohamed, H.G.; Moussa, K.H. A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion. *Entropy* **2020**, *22*, 180. [CrossRef] [PubMed]
56. Yousif, B.; Khalifa, F.; Makram, A.; Takieldeen, A. A novel image encryption/decryption scheme based on integrating multiple chaotic maps. *AIP Adv.* **2020**, *10*, 75220. [CrossRef]
57. Hou, W.; Li, S.; He, J.; Ma, Y. A Novel Image-Encryption Scheme Based on a Non-Linear Cross-Coupled Hyperchaotic System with the Dynamic Correlation of Plaintext Pixels. *Entropy* **2020**, *22*, 779. [CrossRef] [PubMed]
58. Wang, X.; Li, Y.; Jin, J. A new one-dimensional chaotic system with applications in image encryption. *Chaos Solitons Fractals* **2020**, *139*, 110102. [CrossRef]
59. Kari, A.P.; Navin, A.H.; Bidgoli, A.M.; Mirnia, M. A new image encryption scheme based on hybrid chaotic maps. *Multimed. Tools Appl.* **2021**, *80*, 2753–2772. [CrossRef]
60. Wang, X.; Teng, L.; Qin, X. A novel colour image encryption algorithm based on chaos. *Signal Process.* **2012**, *92*, 1101–1108. [CrossRef]
61. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [CrossRef]
62. Tlelo-Cuautle, E.; Díaz-Muñoz, J.D.; González-Zapata, A.M.; Li, R.; León-Salas, W.D.; Fernández, F.V.; Guillén-Fernández, O.; Cruz-Vega, I. Chaotic image encryption using hopfield and hindmarsh–rose neurons implemented on FPGA. *Sensors* **2020**, *20*, 1326. [CrossRef] [PubMed]
63. Peng, X.; Zeng, Y. Image encryption application in a system for compounding self-excited and hidden attractors. *Chaos Solitons Fractals* **2020**, *139*, 110044. [CrossRef]
64. Vaseghi, B.; Hashemi, S.S.; Mobayen, S.; Fekih, A. Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems. *IEEE Access* **2021**, *9*, 21332–21344. [CrossRef]
65. Hafsa, A.; Sghaier, A.; Malek, J.; Machhout, M. Image encryption method based on improved ECC and modified AES algorithm. *Multimed. Tools Appl.* **2021**, *80*, 19769–19801. [CrossRef]