WILEY | Hindawi

Research Article

A New Fractional-Order Map with Infinite Number of Equilibria and Its Encryption Application

Ahlem Gasri,[1] Amina-Aicha Khennaoui ![ORCID],[2] Adel Ouannas,[3] Giuseppe Grassi,[4] Apostolos Iatropoulos,[5] Lazaros Moysis,[6] and Christos Volos[6]

[1]*Department of Mathematics, University of Larbi Tebessi, Tebessa 12002, Algeria*
[2]*Laboratory of Dynamical Systems and Control, University of Larbi Ben M'hidi, Oum El Bouaghi, Algeria*
[3]*Department of Mathematics and Computer Science, University of Larbi Ben M'hidi, Oum El Bouaghi, Algeria*
[4]*Universita Del Salento, Dipartimento Ingegneria Innovazione, 73100 Lecce, Italy*
[5]*Department of Information and Electronic Engineering, International Hellenic University, Thessaloniki, Greece*
[6]*Laboratory of Nonlinear Systems Circuits and Complexity Physics Department, Aristotle University of Thessaloniki, Thessaloniki, Greece*

Correspondence should be addressed to Amina-Aicha Khennaoui; kamina_aicha@yahoo.fr

The study of the chaotic dynamics in fractional-order discrete-time systems has received great attention over the last years. Some efforts have been also devoted to analyze fractional maps with special features. This paper makes a contribution to the topic by introducing a new fractional map that is characterized by both particular dynamic behaviors and specific properties related to the system equilibria. In particular, the conceived one dimensional map is algebraically simpler than all the proposed fractional maps in the literature. Using numerical simulation, we investigate the dynamic and complexity of the fractional map. The results indicate that the new one-dimensional fractional map displays various types of coexisting attractors. The approximate entropy is used to observe the changes in the sequence sequence complexity when the fractional order and system parameter. Finally, the fractional map is applied to the problem of encrypting electrophysiological signals. For the encryption process, random numbers were generated using the values of the fractional map. Some statistical tests are given to show the performance of the encryption.

1. Introduction

Fractional calculus is a topic which is developed more than 300 years. However, it is only the last decades that it has been extensively and intensively investigated, due to its wide application in signal mechanical controls and other fields [1]. Compared with integer order derivatives, fractional-order derivatives are more accurate as they provide excellent tool for the description of the memory effect in all kinds of materials and processing. Based on this consideration, the application of fractional-order systems have attracted more and more researchers attention [2]. At the same time, during the last decade, attention has been focused on discrete fractional calculus and fractional difference operators [3, 4]. Several papers regarding the presence of chaotic phenomena

in fractional discrete-time systems (maps) have been published to date [5–9]. For example, in [10] the hyperchaotic dynamic of the fractional generalized Hénon map has been investigated, whereas in [11] the presence of chaos in the fractional discrete memristor system has been illustrated. In [6] the presence of chaos in the fractional sine map and in the fractional standard map has been analyzed in details. In [7], control laws for stabilizing the chaotic dynamics of the fractional Grassi-Miller map have been developed, whereas in [8] the fractional Hénon map and its chaotic attractors have been studied. In [12], the chaotic dynamics of three maps (i.e., the fractional flow map, the fractional Lozi map and the fractional Lorenz map) have been investigated, whereas in [13] the chaotic behavior of the fractional Tinkerbell map has been illustrated. To our knowledge, all of the

above reported systems have a finite number of equilibria. In general, systems with more equilibria may bring unexpected stabilities to some extent. Therefore, several efforts have been devoted to the study of fractional chaotic maps with some special features related to the system equilibria [14]. Among these studies, Zambrano-Serrano et al. [15] analyzed the dynamic properties and projective synchronization of the fractional difference map with no equilibrium, whereas in [16] Almatroud et al. found rich chaotic behaviours of a novel two-dimensional (2D) hyperchaotic fractional map with infinite line of equilibrium As a result, the analysis of chaotic dynamical behaviours of the fractional-order discrete-time systems without equilibrium points is an interesting topic.

In recent years, there has been a growing interest in discrete time systems with special complex dynamical behaviours, such as hidden attractors [17], coexisting multiple attractors [18] and hyperchaotic behaviours. For instance, in [19] the dynamic properties of a novel memristive hyperchaotic map and its application in secure communication have been illustrated. A 2D sine map was presented in [20] and several interesting behaviour like coexisting attractors and initial offset boosting were explored. General speaking, chaotic maps with coexisting attractors has drawn the attention of many researcher. Coexistence of attractors is a special phenomenon in nonlinear dynamical systems, which denotes that with fixed values of system parameters, a tiny disturbance in the initial condition can lead to the coexistence of different attractors. This property makes the chaotic maps very useful in the fields of secure communication and encryption. Since such phenomenon has not received enough attention with fractional discrete-time systems [21], this paper aims to make a contribution by introducing a new fractional map that is characterized by both particular dynamic behaviors and specific properties related to the system equilibria. Namely, the proposed map possesses infinite number of equilibria in a bounded domain, being this a new feature for fractional map, not published in literature to date. Dynamics and complexity of the conceived map are investigated in details. In particular, bifurcation diagrams, maximum Lyapunov exponents and 0-1 test are reported to highlight the coexistence of different periodic and chaotic attractors. Moreover, the map is applied to the problem of data encryption, which is a well established application of chaotic systems. As recent examples of fractional systems being applied to encryption, in the work [22] a technique to improve chaotic behavior in fractional maps is proposed, and applied to image encryption. An image encryption using the fractional logistic map is proposed in [23], and a different one in [24]. The 2D fractional Hénon map was also applied to image encryption in [25]. In [26] a graphical user interface is designed for random number generators based on integer and fractional order chaotic systems. In [27] another pseudo random number generator was designed based on the coupling of multiple fractional chaotic systems. The above works are just a small sample of the expanding use of continuous and discrete fractional systems to encryption. The use of fractional systems is drawing increasing attention by researchers, since they have more complex dynamics due

to their memory effect, and a higher key space than their integer order analogues, since the fractional order and the finite memory order constitute additional key values.

In this work, the encryption of electrophysiological signals [28–33] is considered. To do so, first, a pseudorandom bit generator (PRBG) is designed using the values of the chaotic map. This chaotic PRBG is the basis for the encryption design, since it is used as the source of deterministic randomness [34–38]. Here, to take advantage of the fractional nature of the map that is used as the basis of the PRBG, a technique is proposed that takes into account its memory effect. So first, the map is implemented using finite memory, in order to reduce its computational cost. Then, in each iteration, all previous values of the map are taken into account in generating the bits, which leads in producing 459 bits per iteration. So the proposed technique reduces the computational load of the PRBG, since fewer iterations of the map are required to reach a desired bistream length, and is specifically designed for fractional order systems.

After the PRBG is designed, to encrypt a given electrophysiological signal, two rounds of masking are performed. First, the signal is modulated to mask its structure by combining it with the values of the fractional chaotic map. Then, the modulated signal is transformed into its binary representation, and combined with a bitstream generated from the PRBG, to yield the encrypted signal. This binary signal can then be safely transmitted through a communication channel. The original signal can be retrieved back at the receiver end, by following the reverse encryption procedure. The performance of the encryption is finally evaluated by a series of statistical tests performed on the original, modulated, and encrypted signals.

Finally, the encryption process is realised in a microcontroller board. This implementation helps verify the feasibility of simulating fractional maps in low cost hardware devices, a task that is of high interest, due to the potential implementability of chaotic systems in IoT related devices [39, 40]. Such realizations have already been explored in the literature, with positive results. For example, in [41] a fractional macro-economic model was established, and a microcontroller implementation was designed on an Arduino Due. In [42] the problem of impulsive synchronization for fractional order discrete chaotic maps is considered, and the design was again implemented in two Arduino Mega boards that simulated the master and observer systems. In [43] a hyperchaotic fractional order system was proposed and discretized. The system was then simulated in an Arduino Uno board and applied to the problem of text encryption. In [44], a fractional order modified Chua's circuit was designed and implemented in an Arduino Uno microcontroller. In [45] a generalized fractional logistic map was constructed and applied to random number generation and image encryption, implemented on a Virtex-5 field-programmable gate array FPGA. In the current work, the realization is done on an STM32F103 nucleo development board, and the encrypted signal from the microcontroller has the same statistical properties to the signal generated from Matlab, as indicated from all the statistical tests performed.

1.1. Fractional Calculus and Preliminaries. In this section, some preliminaries and basic concepts associated with discrete fractional calculus are presented here for completeness. In the following we consider that our domain is the time scale $\mathbb{N}_b = \{b, b+1, b+2, \ldots\}$ with $b \in \mathbb{R}$. Let X denote any function defined from $\mathbb{N}_b$, thus the μ-th fractional sum for $\mu > 0$ is defined by [46]:

$$\Delta_b^{-\mu} X(s) = \frac{1}{\Gamma(\mu)} \sum_{l=b}^{s-\mu} (s - l - 1)^{(\mu-1)} X(l), \qquad (1)$$

where $s \in \mathbb{N}_{b+\mu}$. Observe that the term s^μ indicates to the so-called a falling function which may be defined via Gamma function, Γ, as follows:

$$s^{(\mu)} = \frac{\Gamma(s+1)}{\Gamma(s+1-\mu)}. \qquad (2)$$

Based on the above definition of the μ-th fractional sum, it is possible to define the μ-Caputo like difference operator. Let X denote any function defined from $\mathbb{N}_b$. The Caputo difference operator with order $\mu \notin \mathbb{N}$ is defined by:

Definition 1. For $n = \lceil \mu \rceil + 1$, the μ-th order Caputo-like operator can be defined as [47]:

$$^C\Delta b_\mu X(s) = \Delta_b^{-(n-\mu)},$$

$$\Delta^n X(s) = \frac{1}{\Gamma(n-\mu)} \sum_{l=b}^{s-(n-\mu)} (s - l - 1)^{(n-\mu-1)} \Delta_l^n X(l). \qquad (3)$$

For $s \in \mathbb{N}_{b+n-\mu}$.

Now a theorem is briefly summarized, in order to derive in the following the discrete formula of the new fractional map.

Theorem 1. *[48] For the fractional difference equation*

$$\begin{cases} ^C\Delta\mu_b^\mu X(s) = f(s + \mu - 1, X(s + \mu - 1)), \\ \Delta^r X(b) = X_r, n = \lceil \mu \rceil + 1, r = 0, 1, \ldots, n-1. \end{cases} \qquad (4)$$

Then, the discrete integral equation which is equivalent to equations in (4) is:

$$X_s = X_b + \frac{1}{\Gamma(\mu)} \sum_{l=b+n-\mu}^{s-\mu} (s - \sigma(l))^{(\mu-1)}$$

$$\cdot f(l + \mu - 1, X(l + \mu - 1)), \ t \in \mathbb{N}_{b+n}. \qquad (5)$$

Note that, for the purpose of numerical calculation, (5) can be written as [48]:

$$X_n = X_0 + \frac{1}{\Gamma(\mu)} \sum_{i=0}^{n-1} \frac{\Gamma(n-i+\mu)}{\Gamma(n-i+1)} f(i, X_i). \qquad (6)$$

2. The New Fractional Map

Let us consider the following one dimensional map, which has been recently proposed in [49] as an example of an elegant map that can display chaotic behavior:

$$x_{n+1} = A \sin\left(\frac{C}{x_n}\right) + B, \qquad (7)$$

where A, B and C are three positive parameters. In this work, we extend the original integer–order system to the fractional-order case. Specifically, we consider the effect of the fractional–order in the system dynamics by introducing the following new fractional difference equation:

$$\Delta_b^\mu x(s) = A \sin\left(\frac{C}{x(s+1-\mu)}\right) - x(s+1-\mu) + B, \qquad (8)$$

where $s \in \mathbb{N}_{(b+1-\mu)}$ and μ is the fractional order with $0 < \mu \le 1$. This fractional map is invariant under transformation $x \longrightarrow -x$ for all values of parameters A, B, C and order μ. Hence this map could display coexisting attractors for appropriate choice of initial conditions and fractional order values as well. In order to investigate this property, the numerical formula is designed as:

$$x_n = x_0 + \frac{1}{\Gamma(\mu)} \sum_{i=0}^{n-1} \frac{\Gamma(n-1-i+\mu)}{\Gamma(n-i)} \left(A \sin\left(\frac{C}{x_i}\right) - x_i + B \right). \qquad (9)$$

According to the discrete (9), the proposed fractional map (8) has memory effect, which means that the iterated solution x_n is determined by all the previous states. In order to find the equilibrium points x_f of the fractional map (8), we solve the following equation

$$ApEn = \phi^m(r) - \phi^{m+1}(r), \qquad (10)$$

Obviously, (10) is a trigonometrical equation that is very difficult to solve analytically, therefore, to analyze the equilibrium points we adopt the graphic analytic method. Taking the system parameters $A = 0.5$, $C = 3$, $B = 0$ as an example and the integer order value $\mu = 1$, Figure 1 shows the phase portrait obtained by simulating (9) in the $x_n - x_{n+1}$ plane along with the $y = x$ line. The black line in Figure 1, bisects the first and third quadrants at the interval $[-0.5, 0.5]$, and its crosses with the map are equilibrium points. As one can see, Figure 1 visually demonstrates that there are infinite equilibrium points in this case. On the other hand, Figure 2 shows different phase portraits obtained by simulating (9) for different values of order μ. In comparison to the integer-order case, the shape of the bounded attractors does not change much with the decrease of the value of μ, while the interval where equilibrium points exist is changed from $[-0.5, 0.5]$ into $[-0.6, 0.6]$.

3. Dynamics and Complexity of the New Fractional Map

In this Section the dynamic behaviors of the fractional-order map (8) are numerically investigated using bifurcation
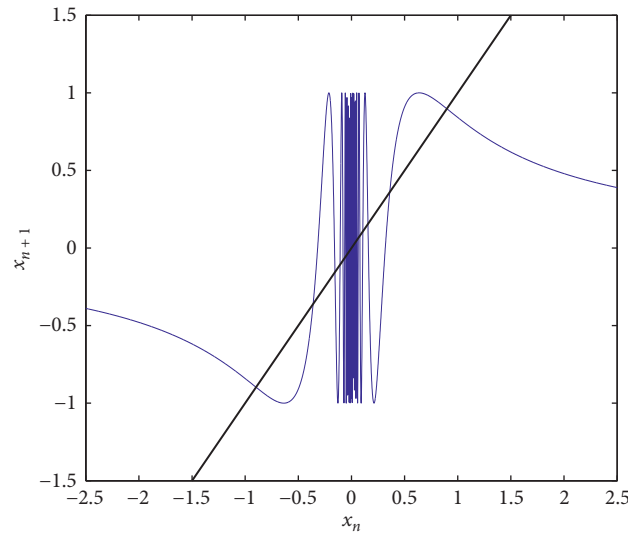
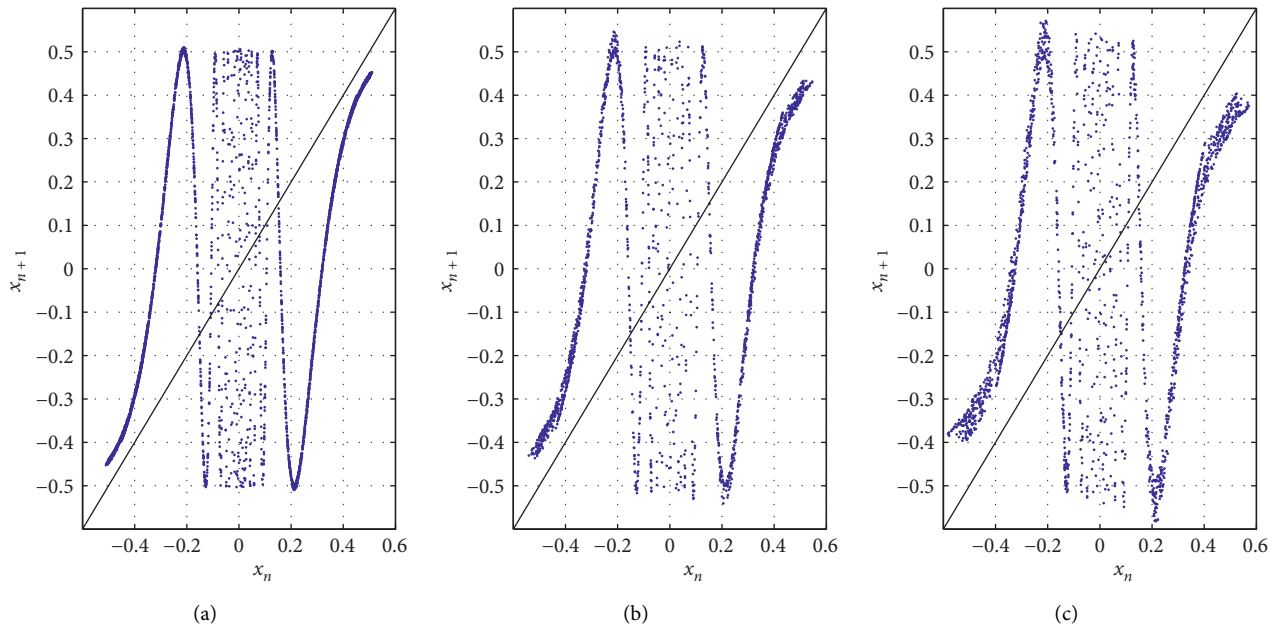FIGURE 1: Phase diagram of fractional map (8) for $\mu = 1$, $A = 0.5$, $B = 0$, $C = 1$.

FIGURE 2: Different chaotic attractors of the fractional map (8) for system parameters $A = 0.5$, $B = 0$, $C = 3$ and different values of μ: (a)$\mu = 0.9$ and (b)$\mu = 0.8$. (c)$\mu = 0.8$.

diagrams and computation of maximum Lyapunov exponents, 0-1 test and entropy. Namely, the influence of both fractional order and initial conditions on the dynamics of the novel map are investigated in detail, with the aim to highlight the coexistence of different chaotic attractors. Namely, the influence of both fractional order and initial conditions on the dynamical behaviour of the novel map are investigated in detail, with the aim to highlight the coexistence of different chaotic attractors. To give a finer analysis of our fractional map we model its dynamics for two parameter sets, i.e for the above values $A = 0.5$, $B = 0$, $C = 3$ and for $A = 0.05$, $B = 0$, $C = 1$.

3.1. Bifurcation Diagrams and MLE.

By changing the system parameters, the fractional map (8) can undertake different dynamic scenarios. Figure 3 gives the three-dimensional view of the bifurcation diagrams of the fractional map (8) for different values of μ (i.e., $\mu = 1$, $\mu = 0.6$, $\mu = 0.2$). We consider the parameter A as the bifurcation parameter and we take the other parameters as $B = 0$ and $C = 1$. We consider two values of symmetric initial conditions: $x_0 = 0.1$ and the negative one $x_0 = -0.1$. Clearly, these diagrams are different (see Figure 4). In particular, in Figure 4 the diagram in magenta color represents the dynamic behavior of the fractional map (8) for order $\mu = 1$ (i.e., for the integer-order
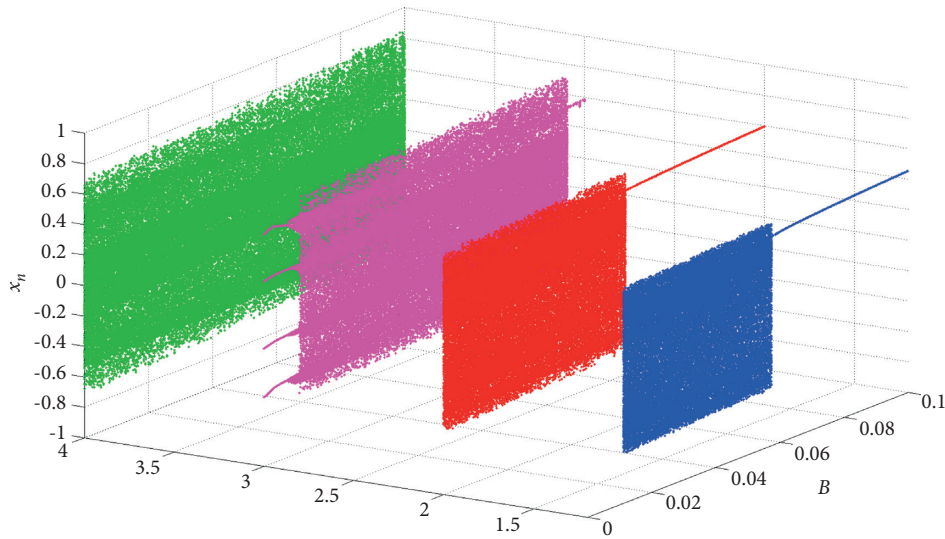
FIGURE 3: Different bifurcation diagrams of the fractional map (8) in three-dimensional space with the variation of system parameter B: blue diagram for $\mu = 1$; red diagram for $\mu = 0.8$; magneta diagram for $\mu = 0.6$; green diagram for $\mu = 0.4$.
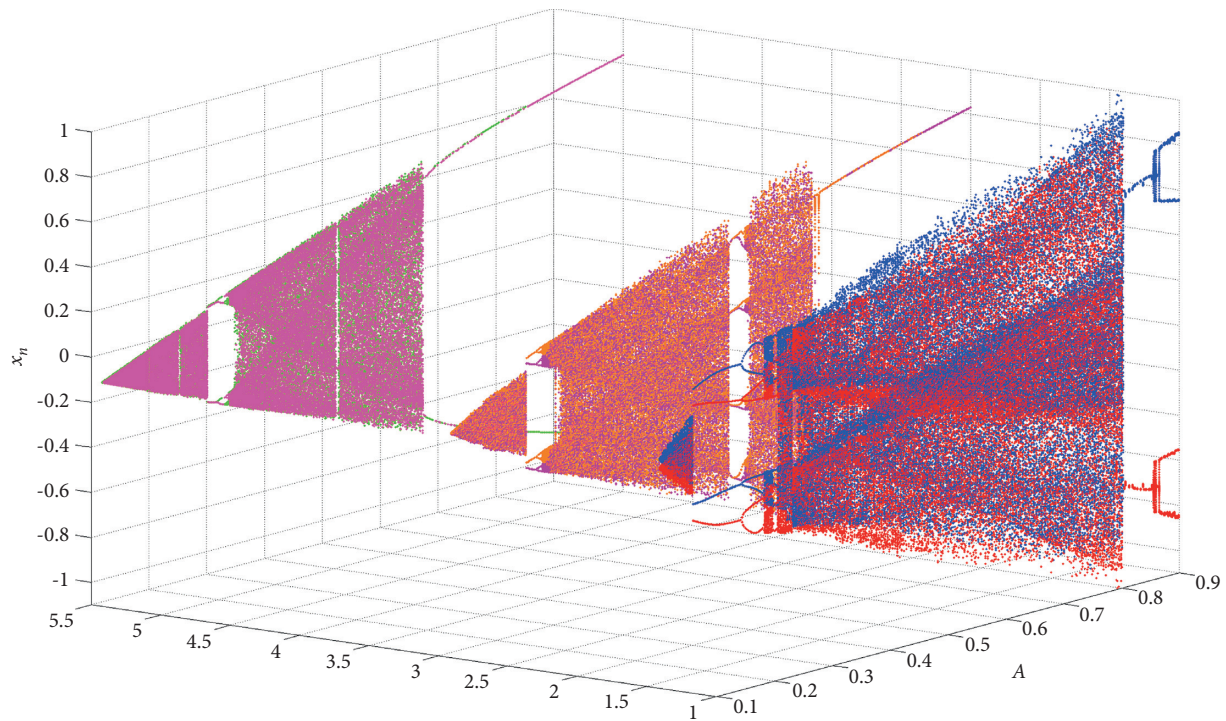

FIGURE 4: Different bifurcation diagrams of the fractional map (8) in three-dimensional space with the variation of system parameter A, and for two initial conditions: blue diagram for $\mu = 0.2$ and for initial condition $x_0 = 0.1$; red diagram $\mu = 0.2$ and for initial condition $x_0 = -0.1$; brown and green diagram for order $\mu = 0.6$; magenta diagram for order $\mu = 1$.

case). As it can be seen, the fractional map is chaotic over most of the range and is changed from chaotic to periodic with the increase of A. It is worth noting that the phenomenon of coexisting attractor is not observed in the integer-order case, where the states of our system come in the form of individual trajectories. By changing the order μ from 1 to 0.6, the bifurcation diagrams become the ones depicted in brown and green colors. In this case, coexisting periodic

orbits appear within the interval $[0.1323, 0.1723] \cup [0.489, 0.517]$, along with a symmetry breaking bifurcation.

Meanwhile, the region of chaotic motion increases with the value of A. Finally, the bifurcation diagrams with $\mu = 0.2$ are considered and plotted in red and blue colors for different initial conditions. Specifically, the states colored in blue are those starting from the positive initial condition, whereas the states colored in red are those starting from the

negative initial condition. In this case, the fractional map (8) displays symmetric separate coexisting diagrams. Figure 5 shows some coexisting chaotic and periodic attractors for different values of the system parameter A. Specifically, when we select the parameter $A = 0.04$, the fractional map (8) highlights the coexistence of two symmetric chaotic attractors corresponding to the positive and negative initial conditions, respectively. Similarly, when we choose the parameter $A = 0.2$, the phase plot in Figure 5 shows the coexistence of two periodic symmetric attractors corresponding to the positive and negative initial conditions, respectively. The analysis conducted so far clearly highlights that the dynamics of the fractional map (8) become very complex when the value of the order μ is significantly decreased.

(b) In order to deeply investigate the properties of coexisting attractors in the fractional map (8), bifurcation diagrams and computations of maximum Lyapunov exponents (LE) with respect to the fractional order are carried out. Various dynamic behaviors can be observed by changing the value of μ at the interval $[0, 1]$. By considering the values $B = 0$, $A = 0.5$ and $C = 3$, Figure 5(a) displays the bifurcation diagram of the state variable x_n corresponding to the positive initial condition (blue diagram) and the negative initial condition (red diagram). For $C = 3$, the trajectories of the fractional map change from chaos to coexisting chaotic attractors with some periodic orbits through period doubling route to chaos. When $\mu \leq 0.31$ the chaotic behavior disappears and separate coexisting periodic orbits appear. This indicates that the dynamics of system (8) for $C = 3$ become simpler as the value of μ decreases. This result is also confirmed by the maximum Lyapunov exponents reported in Figure 5(b). Now the bifurcation diagram and the MLE of the fractional map (8) are illustrated in Figure 7 for $A = 0.05$, $B = 0$ and $C = 1$. Similarly, the dynamic behavior of the map (8) depends on the initial condition and the value of μ. The computation of the MLE shows that the states of the fractional map (8) go from chaotic to periodic with the decrease of order μ. From both the Figures 6 and 7 it can be deduced that the property of having coexisting attractors is observed when the fractional order assumes small values. In order to further investigate this property, we choose to plot the phase portraits of the fractional map (8) for multiple initial conditions and for the same parameters used in Figure 6. The obtained results are plotted in Figure 8. When $\mu = 0.9$, a chaotic attractor is observed. When $\mu = 0.6$, there are two symmetric separate chaotic attractors and a chaotic attractor in magenta color. On the other hand, four coexisting attractors are obtained when $\mu = 0.3$, as depicted in Figure 8(c). Suppose now that $A = 0.05$, $B = 0$, $C = 1$ and $\mu = 0.3$, then the corresponding phase diagram for the map (8) is shown in Figure 9 using different initial conditions. In particular, Figure 9 reveals the presence of four coexisting chaotic attractors, i.e., the blue attractor for $x_0 = 0.1$, the red attractor for $x_0 = -0.1$, the green attractor for $x_0 = 2$ and the magenta attractor for $x_0 = -2$. Figure 9 confirms the rich dynamics of the conceived fractional map, indicating that a number of different coexisting chaotic attractors could be

found by taking other suitable values of the fractional order as well as other proper initial conditions.

3.2. 0-1 Test.

Another tool that can be used to study the influence of the fractional order on the dynamic of a fractional map is "0-1 test." This test, proposed in [50] for fractional-order systems, is able to check the presence of chaos in a series of data that originates from a deterministic system. For the fractional-order model, consider a set of data $x(n)$ where $n = 1, \ldots N$. Using the approach in [50], we transform the trajectories of the fractional-order map into $p - q$ plots. Generally, unbounded $p - q$ trajectories imply chaotic behavior, whereas bounded trajectories implies regular behavior. Herein, we apply the $0 - 1$ test method directly to the solution x_n that is obtained from the discrete formula (9). Herein, we simulate the translation components of the system (8) in the $p - q$ plane. By taking $A = 0.5$, $B = 0$, $C = 3$ and by varying the value of μ, the results of the application of the 0-1 test to the fractional map (8) are reported in Figure 10. In particular, Figure 10(a) depicts the Brownian–like trajectories for all initial conditions, indicating that the suggested map is chaotic for $\mu = 0.9$. On the other hand, Figure 10(b) depicts the Brownian–like trajectories for two different initial conditions, confirming the coexistence of chaotic attractors for $\mu = 0.6$. Finally, when $\mu = 0.3$ the coexistence of chaotic attractors and periodic orbits is confirmed by the plot in Figure 10(c), which depicts bounded–like trajectories for the initial state $x_0 = 0.1$ and Brownian–like trajectories for the initial state $x_0 = 2$. It is concluded that the 0-1 test proves to be a valuable tool for checking the coexistence of different chaotic attractors as well as the coexistence of periodic one in the proposed fractional map (8).

3.3. Approximate Entropy.

The approximate entropy (ApEn) [51] is the measurement of the degree of complexity of a series of data from multi-dimensional perspective. This method estimates the regularity by assigning a non-negative number, where higher values indicate higher complexity. By applying the technique in [52], we consider a set of points $x(1), \ldots, x(N)$ that are obtained from the discrete formula (9). The value of the approximate entropy depends on two important parameters, i.e., m and r, where the input r is the similar tolerance whereas m is the embedding dimension. Here, to calculate ApEn values we set $m = 2$ and $r = 0.2\text{std}(x)$ where $\text{std}(x)$ presents the standard deviation of the data x. Those values are preferred values according to similar previous studies. We reconstruct a subsequence of x such that $X(i) = [x(i), \ldots, x(i + m - 1)]$, where m presents the points from $x(i)$ to $x(i + m - 1)$. Let K be the number of $x(i)$ such that the maximum absolute difference of two vectors $x(i)$ and $X(j)$ is lower or equal to the tolerance r. The relative frequency of $x(i)$ being similar to $X(j)$ is given by

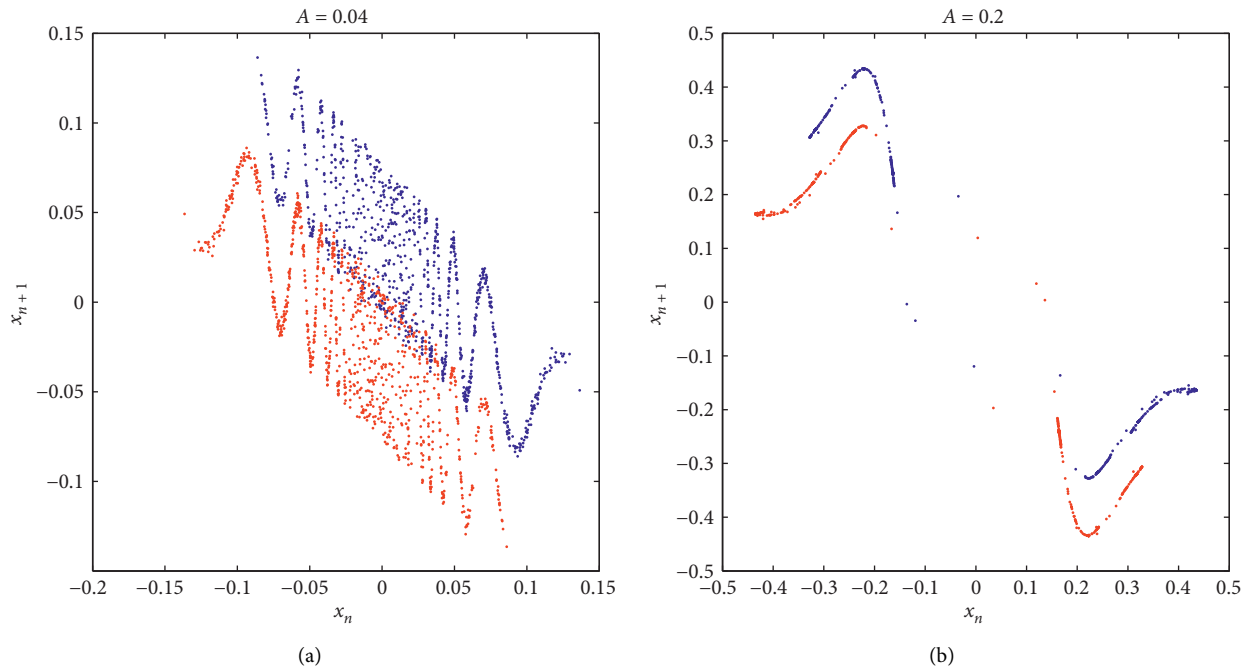$$\phi^m(r) = \frac{1}{n - m - 1} \sum_{i=1}^{n-m+1} \log C_i^m(r). \tag{11}$$

(a)

(b)

FIGURE 5: Two coexisting chaotic attractors for $A = 0.04$ and $\mu = 0.2$ (a); two coexisting periodic attractors for $A = 0.2$ and $\mu = 0.2$ (b).
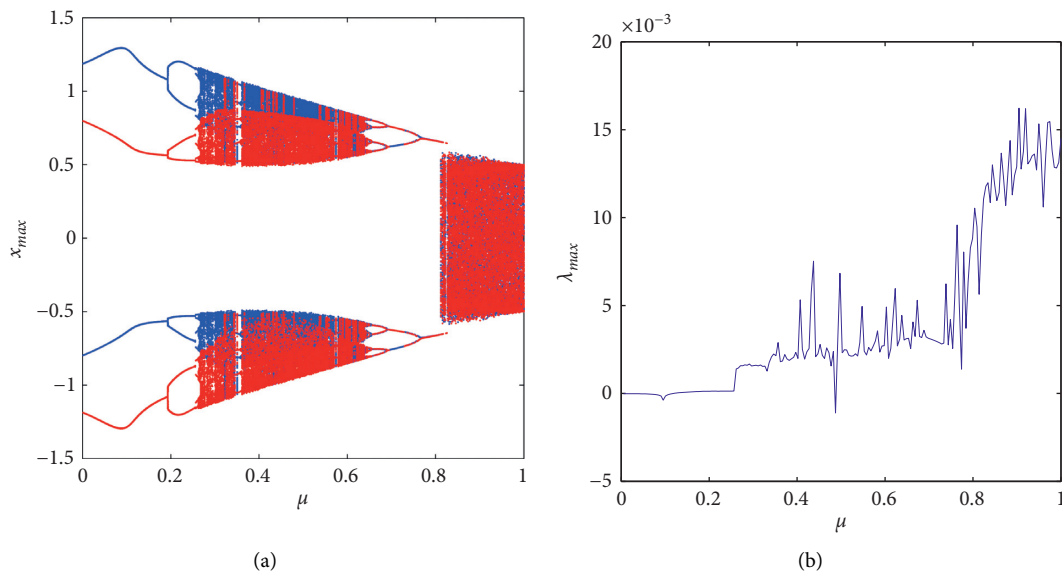

(a)

(b)

FIGURE 6: Bifurcation and maximum LE of system (8) versus μ depicted in (a) and (b), respectively, for parameters $A = 0.5$, $B = 0$, $C = 3$, and two symmetric initial conditions ($x_0 = 0.1$ for the blue diagram and $x_0 = -0.1$ for the red diagram).

The ApEn is calculated as following

$$b_{8n:\ 8n+7} = \text{de2bi}\left(\text{mod}\left(\lfloor 10^{15} |x_n| \rfloor, 256\right)\right), \qquad (12)$$

where $\phi^m(r)$ is denoted to be

$$x_n = x_0 + \frac{1}{\Gamma(\mu)} \sum_{i=1}^{m} \frac{\Gamma(m-i+\mu)}{\Gamma(m-i+1)}$$

$$\cdot \left(A \sin\left(\frac{C}{x_{n-m+i-1}}\right) - x_{n-m+i-1} + B \right), \qquad (13)$$

We apply the ApEn method to simulated complexity of the fractional map (8) by varying the fractional order and control parameter from 0 to 10. For each value of order μ, we analyze a series of points of length 3500 with different values of C. Figure 11 presents the 3D plots of the approximate entropy for fractional map (8). It is observed that, the fractional map (8) can have a higher complexity with relatively larger parameters values C and fractional order μ; which consist with the previous results. The analysis results in Figure 11 indicate that the change of system parameter C has little effect on the complexity. Thus, in real applications,
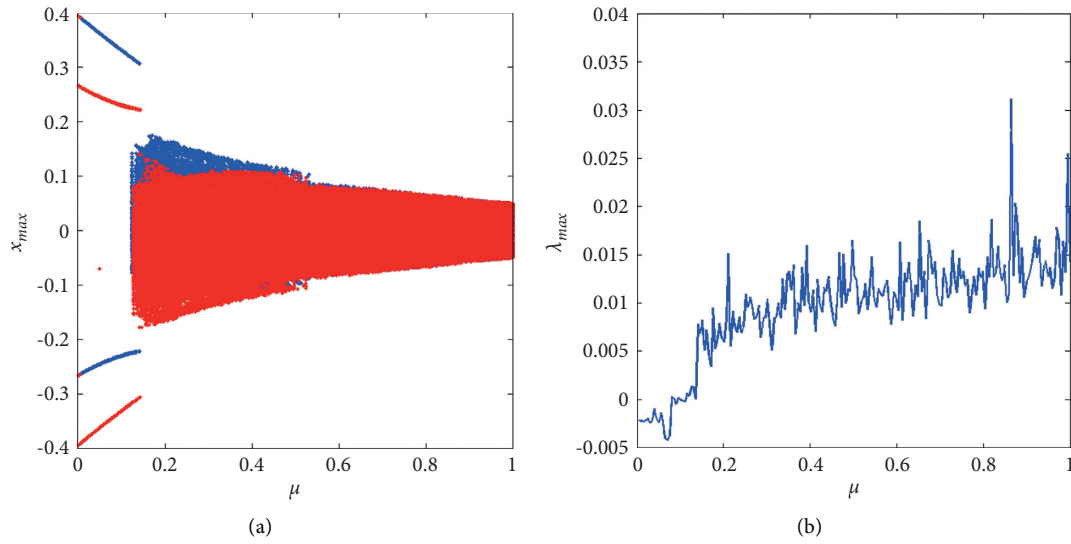
(a)

(b)

FIGURE 7: Bifurcation and maximum LE of system (8) versus μ depicted in (a) and (b), respectively, for parameters $A = 0.05$, $B = 0$, $C = 1$, and two symmetric initial conditions ($x_0 = 0.1$ for the blue diagram and $x_0 = -0.1$ for the red diagram).
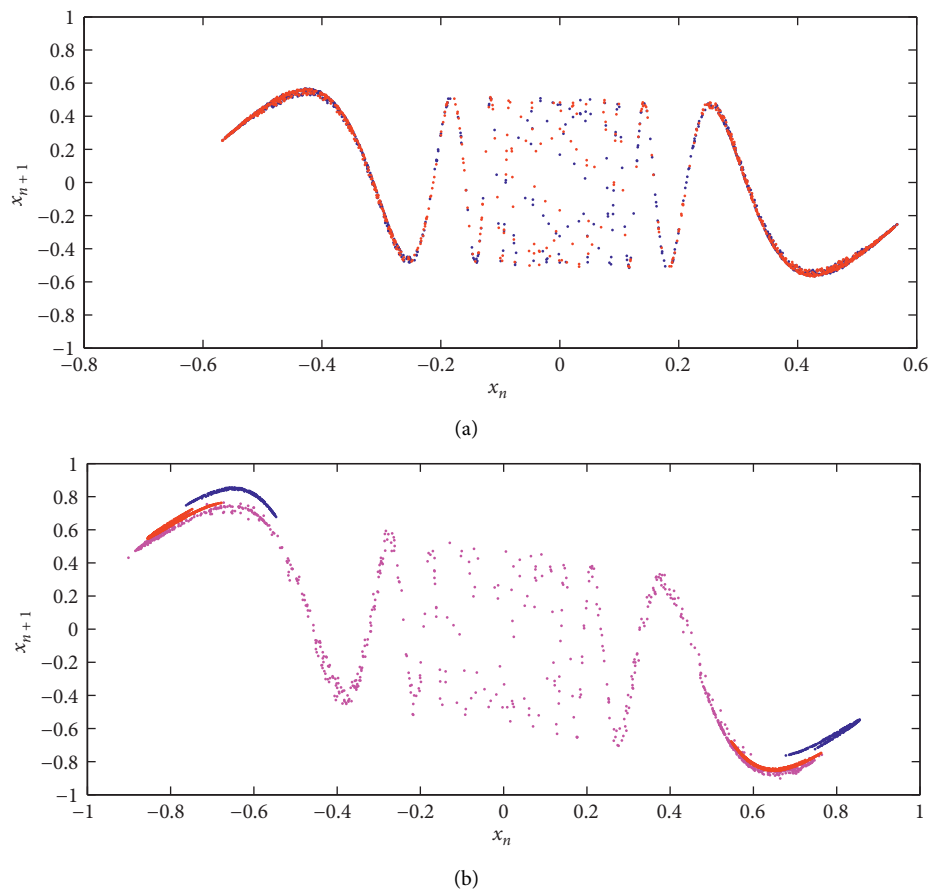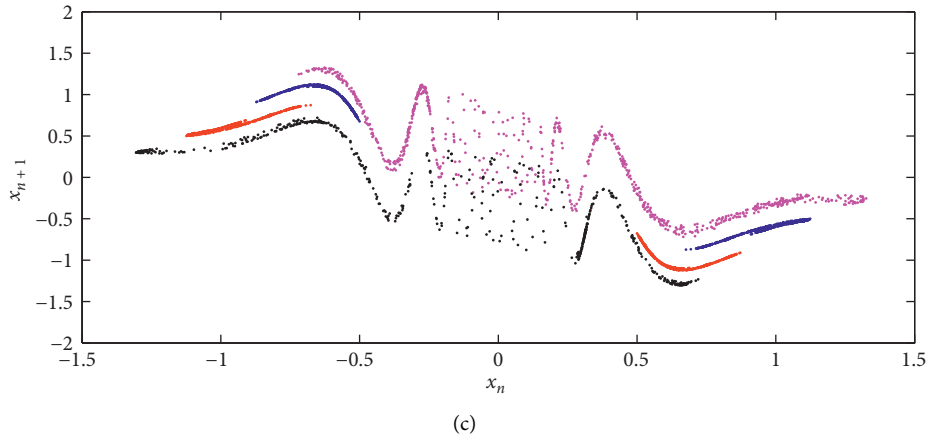

(a)

(b)

FIGURE 8: Continued.

(c)

FIGURE 8: The coexisting attractors of the fractional-order map (8) with parameters $A = 0.5$, $B = 0$, $C = 3$ and with the initial condition $x_0 = -0.1$ for the red attractor and $x_0 = 0.1$ for the blue attractor; (a) chaotic attractor for $\mu = 0.9$, (b) three coexisting chaotic attractors for $\mu = 0.6$ with initial condition $x_0 = 10$ for the magenta attractor; (c) four coexisting chaotic attractors for $\mu = 0.3$ with initial condition $x_0 = 10$ for the magenta attractor and $x_0 = -10$ for the black attractor.
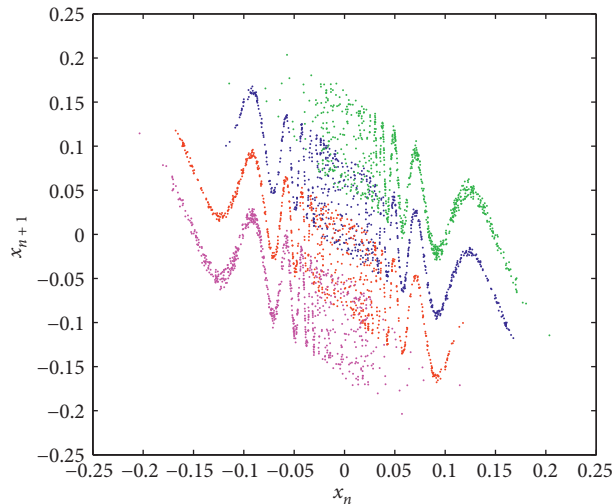

FIGURE 9: Four coexisting chaotic attractors for different initial conditions and system parameters $A = 0.05$, $B = 0$, $C = 1$ and $\mu = 0.3$: blue attractor for $x_0 = 0.1$, red attractor for $x_0 = -0.1$, green attractor for $x_0 = 2$ and magenta attractor for $x_0 = -2$.
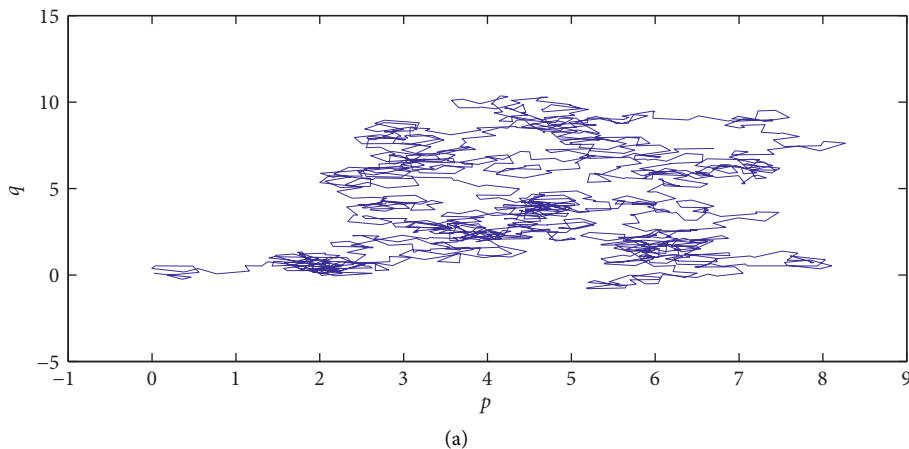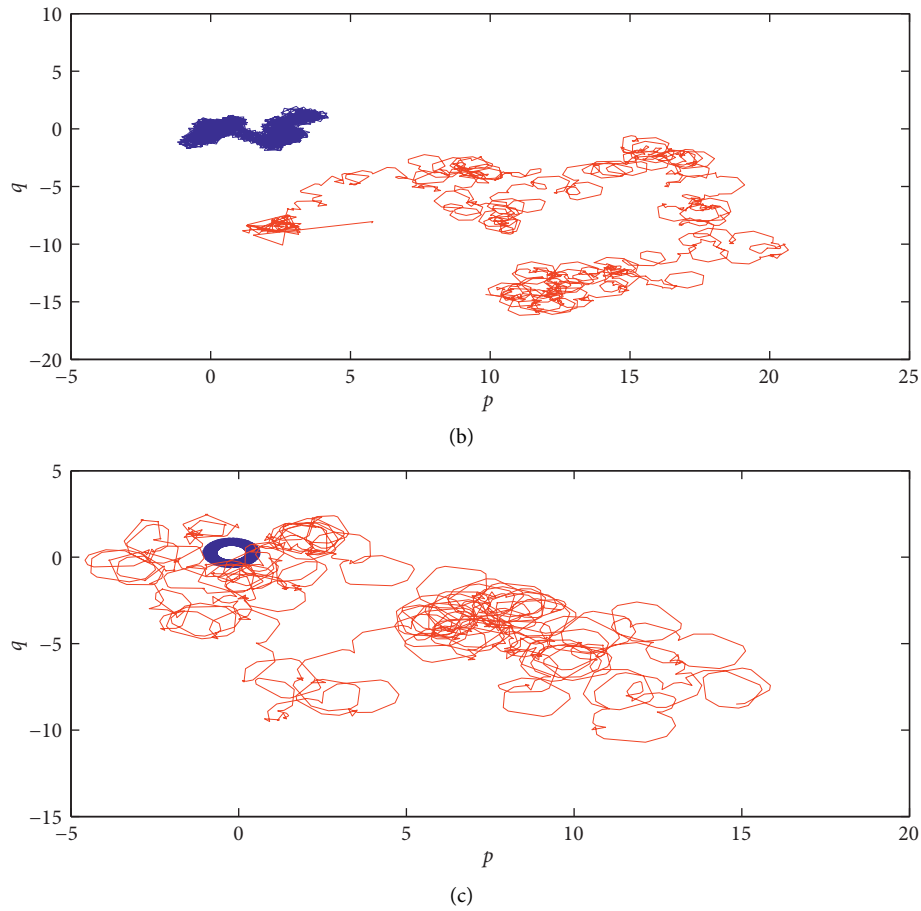

(a)

FIGURE 10: Continued.

(b)

(c)

FIGURE 10: 0-1 test of the fractional map (8) for system parameters $A = 0.5$, $B = 0$ and $C = 3$: (a) Brownian-like trajectories for $\mu = 0.9$; (b) Brownian-like trajectories for $\mu = 0.6$ and for two different initial condition (red color for $x_0 = 10$ and blue color for $x_0 = 0.1$); (c) Brownian-like trajectories for $\mu = 0.3$ and initial condition $x_0 = 10$ (in red), along with bounded like trajectories for $x_0 = 0.1$ (in blue).
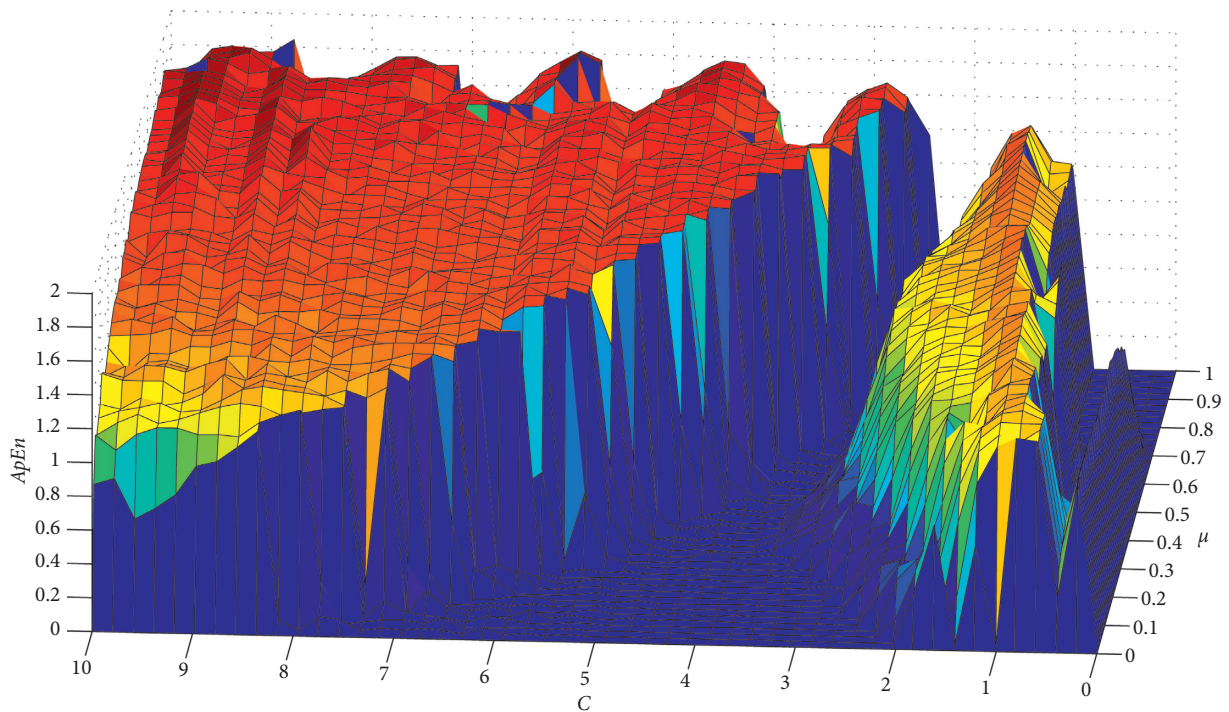

FIGURE 11: The approximate entropy ApEn of the fractional map (8) in three-dimensional space with the variation of system parameter C and fractional order μ, for $A = 0.5$ and $B = 0$.

we should be careful for the range of parameters and fractional order μ.

4. Encryption of Electrophysiological Signals

In this section, an electrophysiological signal will be encrypted using the proposed chaotic map. Here, the signal that will be considered as a sample is a 10 second EEG (electroencephalogram) recording (fp_1) of a subject during arithmetic tasks. More details on the other types of EEG signals can be found in the PhysioBank database [53, 54].

4.1. Design a PRBG. The first step in the encryption scheme is to design a chaotic pseudo-random bit generator. Since the main computational drawback of fractional order systems is their memory effect, the system will be implemented using a finite memory. Thus, its finite form is given as

$$\mathcal{M}_i = \varepsilon_i + \frac{\lfloor 10^5 x_i \rfloor}{10^3}, i = 1, \ldots, \ell, \qquad (14)$$

where m denotes the memory used. As one can see from (14), when $i = 1, \ldots, m$ the fractional map states depends on the past m variable, i.e, $x_1(1), \ldots, x_1(m)$. After some trial and error, the memory is chosen as $m = 50$, which satisfyingly models the dynamical behavior of the system, as can be seen in Figure 12. Although the diagram is not identical to the one of the fractional map shown in Figure 4, it accurately showcases chaotic behavior in the range of around 0.2 to 0.8. Implementing fractional systems using finite memory is a standard approach in reducing computational cost and avoiding overflow, and it is used in most microcontroller implementations of fractional chaotic systems [41, 42, 55].

In order to take advantage of the fractional nature of the proposed map, each individual term inside the finite sum (14) is used in the bit generation. So in each iteration of the map, the PRBG generates bits using the following rules:

$$\varepsilon_{enc-bin} = \mathcal{M}_{bin} \oplus \mathcal{B}, \qquad (15)$$

where $\lfloor \cdot \rfloor$ denotes the floor operation. So in each iteration, each individual term of the sum in (14), as well as the value x_n of the map are multiplied by 10^{15} and the integer part of this product is taken modulo 512. The result of this operation is then transformed to binary representation. Since the outcome of the modulo is an integer from 0 to 511, transforming it to binary generates nine bits per iteration. Thus, each of the terms $b_{n,1}, \ldots, b_{n,51}$ corresponds to nine bits. The resulting bitstream is taken by concatenating the bits as

$$\mathcal{B} = \{b_{n-1,1}, \ldots, b_{n-1,51}, b_{n,1}, \ldots, b_{n,51}, \ldots\}. \qquad (16)$$

With the algorithm, there are 459 bits generated in each iteration. So this approach brings an advantage over classic techniques that generate only one bit per iteration, takes advantage of the fractional nature of the map, and also reduces bit generation speed, since fewer iterations of the map are required to reach the required bitstream length.

As noted above, since the sum in (14) is limited from $i = 1$ to $i = n$ when $n < 50$, for $n = 0$ there are 9 bits generated, for $n = 1$ there are 18 bits, and so on, until $n = 49$ where 450 bits are generated. Thus, to reach a bitstream of length N, there are $\lceil N/459 + 9\sum_{i=0}^{49} i/459 \rceil$ iterations required.

To test the PRBG, a set of $100 \cdot 10^6$ bitstreams is generated and tested through the National Institute of Standards and Technology (NIST) statistical test package SP 800-22 [56]. The test suite consists of 15 statistical tests that are used to verify if a bit sequence is indistinguishable from a random sequence. Each test returns a P value and if the value is higher than a significance level, chosen as the default value 0.01 here, the test is successful. For a PRBG to be classified as random, it should pass all 15 tests. This is verified from Table 1.

4.2. Encryption of Electrophysiological Signal. After the appropriate design of the PRBG, the encryption process is presented. The process consists of two rounds, and a different chaotic map of the form (14) is used in each round, each with parameters x_0, A_1, B_1, C_1 and y_0, A_2, B_2, C_2. In the first round, the source signal is modulated by adding to it the values of the first chaotic map, in order to mask its structure. Then, the modulated signal is transformed into its binary representation, and encrypted using the PRBG of the previous section, generated using the second chaotic map. The encryption is performed using the bitwise XOR operator between the information bitstream and the chaotic bitstream. The complete process is outlined in Algorithm 1.

The transformation of the modulated signal into its binary representation in Step 2 of Algorithm 1 is performed as follows. The modulated signal takes values in the range [−127.999, 127.999]. In order to sustain a low run time execution we chose to convert the sampled values by mixing a fixed-point-format with a two's complement representation. So each sample is split into its sign, integer and a decimal parts. The first bit of the binary representation is used to denote the sign. Then, seven bits are used to represent the integer part and ten bits to represent the decimal part. Hence, there are 18 bits overall for each sample, resulting in a bitstream of length $18 \times \ell$. This transformation is outlined in Figure 13.

For the decryption process, the original EEG signal can be reconstructed at the receiver end by following the reverse procedure, that is, performing an XOR between the encrypted binary signal and the same bitstream from the PRBG, generated using the same parameter values, transforming the result back to its decimal format, and then performing the demodulation process, as described in Algorithm 2.

Note that the only information that the receiver needs to know in order to decrypt the signal is the parameter values for the two chaotic maps used to modulate the signal and generate the PRBG. These parameters constitute the key values of the encryption design. Since each chaotic map has four parameters and one initial condition, there are overall ten key values, $x_0, A_1, B_1, C_1, \mu_1, y_0, A_2, B_2, C_2, \mu_2$. Assuming
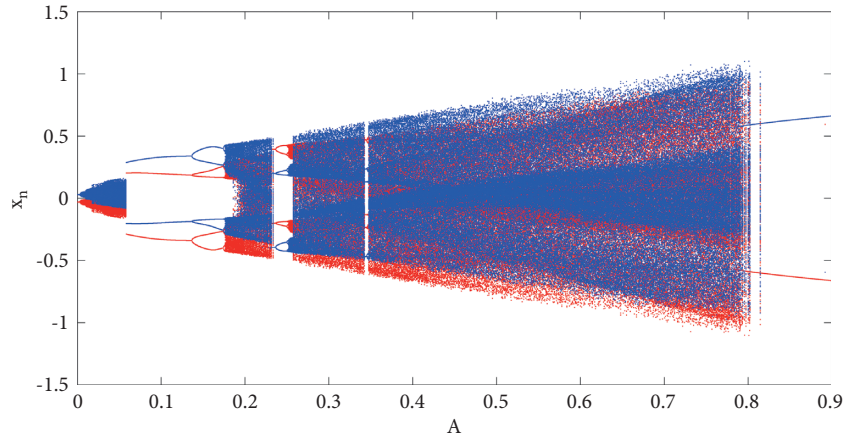
FIGURE 12: Bifurcation diagram of (14) with respect to parameter A, for $B = 0, C = 1, \mu = 0.2, m = 50$, and $x_0 = 0.1$ (blue), $x_0 = -0.1$ (red).

TABLE 1: NIST test results ($x_0 = 0.1$, $A = 0.7$, $B = 0$, $C = 1$, $\mu = 0.2$, $m = 50$).

No.	Test	Chi-square P-value	Rate
1	Frequency	0.971 699	100/100
2	BlockFrequency	0.437 274	100/100
3	CumulativeSums	0.213 309	100/100
4	Runs	0.494 392	96/100
5	LongestRun	0.319 084	99/100
6	Rank	0.275 709	99/100
7	FFT	0.366 918	99/100
8	NonOverlappingTemplate	0.554 420	100/100
9	OverlappingTemplate	0.897 763	99/100
10	Universal	0.897 763	100/100
11	ApproximateEntropy	0.455 937	98/100
12	RandomExcursions	0.031 497	63/64
13	RandomExcursionsVariant	0.834 308	61/64
14	Serial	0.051 942	99/100
15	LinearComplexity	0.657 933	99/100

Input: An EEC signal $\mathscr{E}$ of length ℓ. The key values of two chaotic maps of the form (14), $x_0, A_1, B_1, C_1, \mu_1$ and $y_0, A_2, B_2, C_2, \mu_2$.
Output: An encrypted signal $\mathscr{E}_{enc}$ of the same length.
Step 1. Generate ℓ values of the first chaotic map x_i, $i = 1, \ldots, \ell$. Modulate the EEG signal to mask its structure, as
  $\mathscr{M}_i = \mathscr{E}_i + \lfloor 10^5 x_i \rfloor / 10^3$, $i = 1, \ldots, \ell$.
Step 2. Transform the modulated signal $\mathscr{M}$ into its binary representation $\mathscr{M}_{bin}$ of length $18 \times \ell$.
Step 3. Generate a bitstream $\mathscr{B}$ of length $16 \times \ell$ using the map y_i as a basis for the PRBG of the previous section (15). Since 8 bits are generated per iteration, the map y_i needs to be iterated $\lceil 2.25 \times \ell \rceil$ times.
Step 4. Encrypt the information bitstream $\mathscr{M}_{bin}$ by combining it with the chaotic bistream as
  $\mathscr{E}_{enc-bin} = \mathscr{M}_{bin} \oplus \mathscr{B}$.
Step 5. Transform the binary encrypted signal $\mathscr{E}_{enc-bin}$ to decimal form, to obtain the encrypted signal $\mathscr{E}_{enc}$.
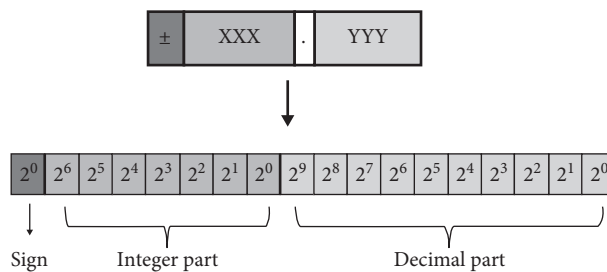
ALGORITHM 1: Chaotic Encryption of EEG signal.

FIGURE 13: Binary representation of the modulated samples using 18 bits.

Input: An encrypted signal $\mathscr{E}_{\text{enc}}$ of length ℓ. The key values of two chaotic maps of the form (14), x_0, A_1, B_1, C_1 and y_0, A_2, B_2, C_2.

Output: A decrypted signal $\mathscr{E}$ of the same length.

Step 1. Transform the encrypted signal $\mathscr{E}_{\text{enc}}$ to its binary form, to obtain the encrypted bitstream $\mathscr{E}_{\text{enc-bin}}$ of length $18 \times \ell$.

Step 2. Generate a bitstream $\mathscr{B}$ of length $18 \times \ell$ using the map y_i as a basis for the PRBG of the previous section (15). Since 8 bits are generated per iteration, the map y_i needs to be iterated $\lceil 2.25 \times \ell \rceil$ times.

Step 3. Decrypt the bitstream $\mathscr{E}_{\text{enc-bin}}$ by combining it with the chaotic bistream as.

$\mathscr{M}_{\text{bin}} = \mathscr{B} \oplus \mathscr{E}_{\text{enc-bin}}$

Step 4. Transform the modulated binary signal $\mathscr{M}_{\text{bin}}$ into its decimal representation $\mathscr{M}$ of length ℓ.

Step 5. Generate ℓ values of the chaotic map $x_i, i = 1, \ldots, \ell$. Demodulate the signal $\mathscr{M}$ as to obtain the original signal $\mathscr{E}$.

$\mathscr{E}_i = \mathscr{M}_i - \lfloor 10^5 x_i \rfloor / 10^3, i = 1, \ldots, \ell$

ALGORITHM 2: Chaotic Decryption of EEG signal.

a 16-digit accuracy, an upper bound for the key space is $10^{8 \cdot 16} = 10^{128} \approx (10^3)^{42.6} \approx 2^{426}$. This is higher than the bound of 2^{100} required to resist brute force attacks [57]. Note though, that since the system is not chaotic for all parameter values, the real key space is lower than 2^{426}.

4.3. Microcontroller Implementation.

The encryption and decryption process was simulated in a microcontroller. For this, an STM32F103 nucleo development board is used, which incorporates a high-performance ARM M3 32-bit RISC core operating at 72 MHz, depicted at Figure 14.

Since an embedded system usually has low ram storage, the modulated signal was saved at the flash memory of the STM32F103RB which embeds an 128 K Byte of flash memory.

The simulation results are shown in Figure 15, where the original (plaintext), modulated, and encrypted signals are shown. Clearly, there is visually no relation between these signals, something that is verified in the next section, through a series of measures. The signals are plotted in Matlab, where the data are loaded from the txt files resulting from the microcontroller simulation. The numerical simulations for the encryption performed in Matlab yield similar results and are thus omitted.

Note that the computation time for the complete procedure of modulating the signal, transforming it to binary format and encrypting it, takes around 8.5 seconds. To reduce computational load and increase speed, the terms $\Gamma(m - i + \mu)/\Gamma(m - i + 1)$ where precomputed and saved in the memory before execution begins. Additionally, further experimentation could lead to reduction in the execution time. For example, in the modulation step the fractional map could be implemented using a shorter memory.

4.4. Encryption Performance.

To test the performance of the encryption algorithm, a series of tests are performed on the original, modulated and encrypted signals. The results are gathered on Table 2, for the simulation performed in Matlab R2018b, as well as the microcontroller implementation. The key values of the maps are $x_0 = 0.111$, $A_1 = 0.7$, $B_1 = 0$, $C_1 = 1$, $\mu_1 = 0.2$ and $y_0 = 0.1$, $A_2 = 0.7$, $B_2 = 0$, $C_2 = 1$, $\mu_2 = 0.2$.

Note that apart from the Approximate Entropy measure that is computed for each individual signal, the rest of the measures are computed in each case between the original

and modulated signal, and between the original and encrypted signal, and shown in their respective columns.

In all cases, it can be seen that the measures for the Matlab and microcontroller implementations are very close to each other. This means that the microcontroller encryption performs equally well compared to Matlab.

4.4.1. Histogram.

Initially, the histogram of the original, modulated and encrypted signals are plotted in Figure 16 for the microcontroller simulation. An encrypted signal should have a uniform histogram, so that no information on the distribution of the signal's values are revealed. Indeed it can be seen that the histogram of the encrypted signal is much more uniform compared to the original signal and modulated ones, that have a shape closer to a normal distribution. The simulation performed in Matlab yields similar histograms, so both simulations perform the same.

4.4.2. Structural Similarity Index (SSIM).

The SSIM is a measure of the structural similarity between two signals [29], initially considered for images [58]. It is given by

$$\text{SSIM} = \frac{\left(2\mu_x\mu_y + S_1\right)\left(2\delta_{xy} + S_2\right)}{\left(\mu_x^2 + \mu_y^2 + S_1\right)\left(\delta_x^2 + \delta_y^2 + S_2\right)}, \tag{17}$$

where μ_x, μ_y the mean values of the original and encrypted (or modulated) signals respectively, δ_x^2, δ_y^2 their variances, and δ_{xy} their cross-covariance. The parameters S_1, S_2 take small values, to avoid unstable results when the denominator is close to zero.

The SSIM value is between $[-1, 1]$, with 1 for identical signals, and 0 for signals with no similarity. So, the closest the measure is to zero, the better the encryption. Indeed, the SSIM between the original and modulated signal performed in Matlab is equal to -0.1160, and between the original and encrypted signal is 0.0016, which is indeed very close to zero.

4.4.3. Log-Likelihood Ratio (LLR).

The LLR gives an estimation on the quality of encryption [29, 59–61]. It is based on the assumption that the segment can be represented by a p-th order all-pole linear predictive coding model
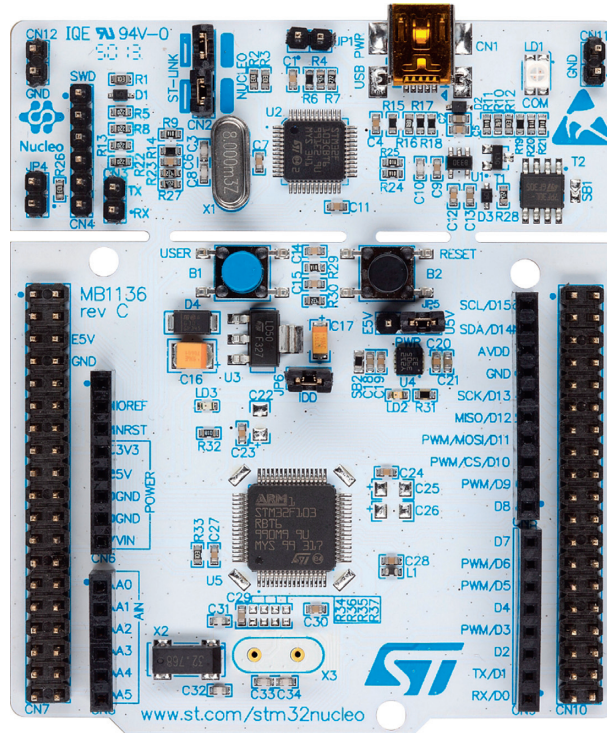
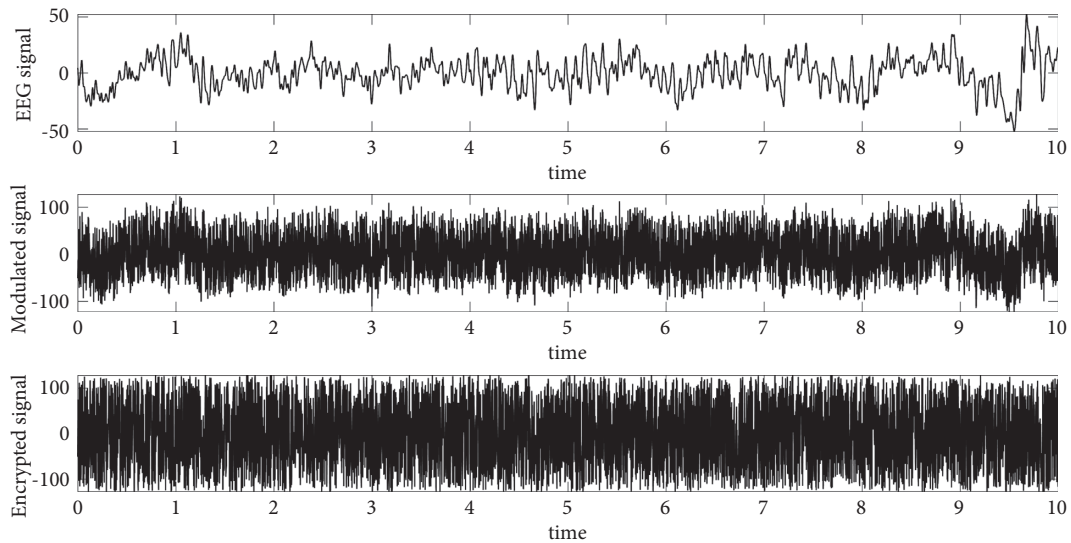FIGURE 14: STM32F103 nucleo board with a 32bit RISC processor.

FIGURE 15: Original EEG signal, modulated signal, and encrypted signal.

TABLE 2: Performance measures of the encryption design.

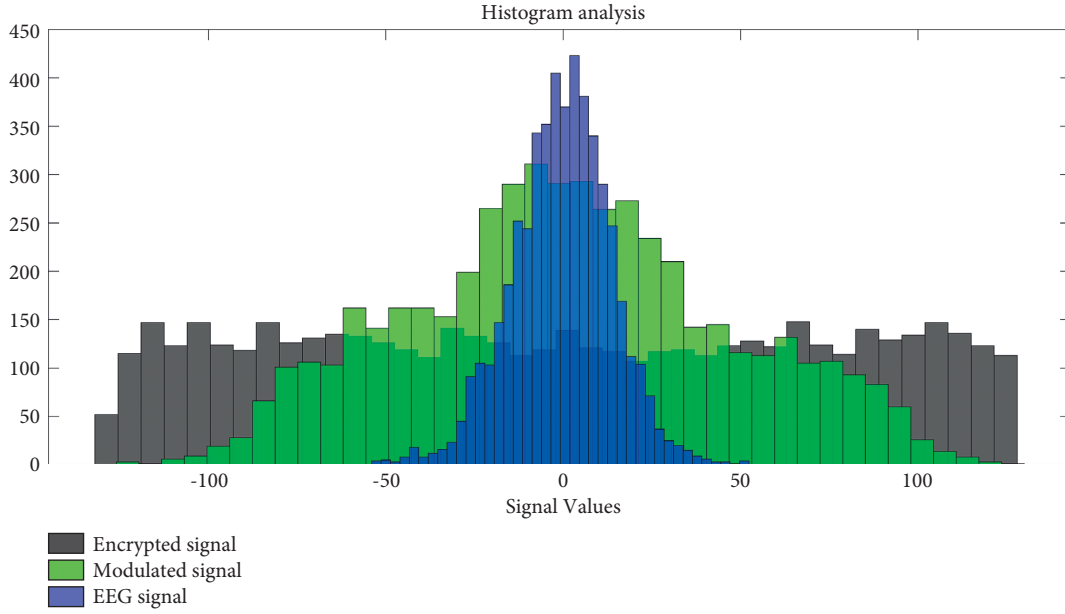| Signals	EEC	Matlab		Microcontroller	
		Modulated	Encrypted	Modulated	Encrypted
SSIM	—	−0.1160	0.001 6	−0.0894	0.006 8
LLR	—	1.995 5	1.993 7	1.973 3	2.045 6
SNR	—	−9.7873	−14.6874	−9.8402	−14.6757
r_{xy}	—	0.307 6	−0.0126	0.303 7	0.021 0
SD	—	39.494 9	44.053 6	39.652 1	43.864 9
ApEn	0.497 0	1.577 4	2.270 2	1.579 8	2.228 2

Figure 16: Histograms of the encrypted, modulated, and encrypted signals.

$$x_i = \sum_{m=1}^{p} a_m x_{i-m} + G_x u_i, \tag{18}$$

where x_i is the ith signal sample, a_m, $m = 1, \ldots, p$ the coefficients of the all-pole filter, G_x the gain of the filter and u_i an appropriate excitation input to the signal. The LLR is then defined as:

$$LLR = \left| \log\left(\frac{a_x R_y a_x^T}{a_y R_z a_y^T} \right) \right|, \tag{19}$$

where a_x the vector of Linear Prediction Coefficients (LPCs) $[1, a_1, a_2, \ldots, a_m]$ of the original signal, a_z the LPCs of the encrypted (or modulated) signal, and R_y the autocorrelation matrix of the encrypted (or modulated) signal. A higher LLR value indicates a good encryption. The LLR between the original and modulated signal is 1.995 5 and between the original and encrypted signals is 1.993 7. The values are both high, which indicates a good encryption.

4.4.4. Signal to Noise Ratio (SNR). The SNR is defined as [29, 60]:

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^{N} x_i^2}{\sum_{i=1}^{N} (x_i - y_i)^2}, \tag{20}$$

where x, y the encrypted and decrypted (or modulated) signals respectively, and N the number of samples. A low SNR indicates a good encryption. The SNR between the original and modulated signal is -9.7873, while the SNR between the original and encrypted signal is -14.6874. Both values are very low and indicate a good encryption.

4.4.5. Correlation Coefficient. The correlation coefficient [29] between the original and encrypted (or modulated) signals is computed as:

$$r_{xy} = \frac{c_v(x, y)}{\sqrt{\delta_x^2}\sqrt{\delta_y^2}}, \tag{21}$$

where $c_v(x, y)$ the covariance of the two signals and δ^2 their variances. For uncorrelated signals, the correlation coefficient should be close to zero. The correlation coefficient between original and modulated signal is 0.307 6, while the coefficient between original and encrypted is -0.0126.

4.4.6. Spectral Distortion (SD). The SD measures the difference between the spectrum of the original and encrypted (or modulated) signals [29, 60–62]. It is computed as:

$$SD = \frac{1}{M} \sum_{i=0}^{M-1} \left| V_{x,i} - V_{y,i} \right|, \tag{22}$$

where $V_{x,i}, V_{y,i}$ the spectrum of the original and encrypted (or modulated) signal in decibel at instance *i*. A higher value of SD indicates a better encryption. The SD between the original and moculated signals is 39.494 9, and the SD between the original and encrypted signals is 44.053 6, so both values are high.

4.4.7. Approximate Entropy (ApEn). The ApEn is applied to measure the complexity of the serie of data [51]. A series with a higher ApEn is considered as being more complex, so for the proposed scheme, the encrypted signal should have a higher value of ApEn compared to the original signal. Indeed the ApEn of the original signal is 0.497 0, for the modulated signal is 1.577 4, and for the encrypted signal is 2.270 2, so the encrypted signal has the highest ApEn.

Overall, each of the measures computed indicates a good encryption performance. Moreover, the design can be accurately replicated on a microcontroller board.

5. Conclusions

Referring to fractional-order discrete-time systems with special features, this paper has introduced the first example of a fractional map with infinite number of equilibria in a bounded domain. The conceived map has also shown coexistence of different types of periodic and chaotic attractors. Dynamics and complexity of the conceived map have been analyzed in details via bifurcation diagrams, maximum Lyapunov exponents, 0-1 test and approximate entropy. Compared with the integer order map, the fractional map has more complexity when the fractional order values is smaller. That is the integer-order map do not have the property of coexisting attractors, while fractional map have it. Afterwards, the proposed map was applied to the problem of encrypting an electrophysiological signal. A PRBG was designed based on the values of the chaotic map, and two rounds of modulation and encryption were performed on the signal. A set of measures were then computed for the original and encrypted signals to verify the performance of the encryption. The design was realised in a microcontroller board, so to increase speed, the fractional map was implemented with finite memory. Future extensions of this work can consider modifications of the encryption design, for example different methods to modulate the signal.

Also, in order to improve execution time, the use of a higher frequency CPU combined with hardware accelerators, such as CORDIC (COordinate Rotation DIgital Computer), will allow faster sinusoidal calculations and floating point arithmetic operations.

Finally, FPGA based realizations of the encryption design are among the future goals set by the authors, since they have been proven an efficient low cost option for implementing fractional [45] and integer order maps [63].

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

References

[1] C. Goodrich and A. C. Peterson, *Discrete Fractional Calculus*, Springer, Berlin, Germany, 2015.

[2] B. Yan, S. He, and S. Wang, "Multistability and formation of spiral waves in a fractional-order memristor-based hyperchaotic Lu system with No equilibrium points," *Mathematical Problems in Engineering*, vol. 2020, Article ID 2468134, 12 pages, 2020.

[3] P. Ostalczyk, *Discrete fractional calculus: applications in control and image processing*, World Scientific, vol. 4, Singapore, , 2015.

[4] M. Edelman, E. E. Macau, and M. A. Sanjuan, *Chaotic, fractional, and complex dynamics: new insights and perspectives*, Springer International Publishing, New York, NY, USA, 2018.

[5] G. C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dynamics*, vol. 75, no. 1, pp. 283–287, 2014.

[6] G. C. Wu, D. Baleanu, and S. D. Zeng, "Discrete chaos in fractional sine and standard maps," *Physics Letters A*, vol. 378, no. 5-6, pp. 484–487, 2014.

[7] A. Ouannas, A.-A. Khennaoui, G. Grassi, and S. Bendoukha, "On chaos in the fractional-order Grassi-Miller map and its control," *Journal of Computational and Applied Mathematics*, vol. 358, pp. 293–305, 2019.

[8] T. Hu, "Discrete chaos in fractional Hénon map," *Applied Mathematics*, vol. 5, no. 15, 2014.

[9] A.-A. Khennaoui, A. Ouannas, S. Bendoukha, X. Wang, and V.-T. Pham, "On chaos in the fractional-order discrete-time unified system and its control synchronization," *Entropy*, vol. 20, no. 7, p. 530, 2018.

[10] M. K. Shukla and B. B. Sharma, "Investigation of chaos in fractional order generalized hyperchaotic Henon map," *AEU - International Journal of Electronics and Communications*, vol. 78, pp. 265–273, 2017.

[11] Y. Peng, S. He, and K. Sun, "Chaos in the discrete memristor-based system with fractional-order difference," *Results in Physics*, vol. 24, Article ID 104106, 2021.

[12] A.-A. Khennaoui, A. Ouannas, S. Bendoukha, G. Grassi, R. P. Lozi, and V.-T. Pham, "On fractional-order discrete-time systems: chaos, stabilization and synchronization," *Chaos, Solitons & Fractals*, vol. 119, pp. 150–162, 2019.

[13] A. Ouannas, A.-A. Khennaoui, S. Bendoukha, T. Vo, V.-T. Pham, and V. Huynh, "The fractional form of the Tinkerbell map is chaotic," *Applied Sciences*, vol. 8, no. 12, p. 2640, 2018.

[14] A. Ouannas, A. A. Khennaoui, S. Momani, V. T. Pham, and R. El-Khazali, "Hidden attractors in a new fractional–order discrete system: chaos, complexity, entropy, and control," *Chinese Physics B*, vol. 29, no. 5, Article ID 50504, 2020.

[15] E. Zambrano-Serrano, S. Bekiros, M. A. Platas-Garza, C. Posadas-Castillo, and P. Agarwal, H. Jahanshahi and A. A. Aly, On and projective synchronization of a fractional difference map with no equilibria using a fuzzy-based state feedback control," *Physica A: Statistical Mechanics and Its Applications*, vol. 578, Article ID 126100, 2021.

[16] A. O. Almatroud, A. A. Khennaoui, A. Ouannas, and V. T. Pham, "Infinite line of Equilibriums in a novel fractional map with coexisting infinitely many attractors and initial offset boosting," *International Journal of Nonlinear Science and Numerical Simulation*, vol. 2021, 2021.

[17] Y. Peng, K. Sun, and S. He, "A discrete memristor model and its application in Hénon map," *Chaos, Solitons & Fractals*, vol. 137, Article ID 109873, 2020.

[18] H. Li, K. Li, M. Chen, and B. Bao, "Coexisting infinite orbits in an area-preserving Lozi map," *Entropy*, vol. 22, no. 10, p. 1119, 2020.

[19] H. Li, Z. Hua, H. Bao, L. Zhu, M. Chen, and B. Bao, "Two-dimensional memristive hyperchaotic maps and application in secure communication," *IEEE transactions on industrial electronics*, vol. 68, no. 10, 2020.

[20] H. Bao, Z. Hua, N. Wang, L. Zhu, M. Chen, and B. Bao, "Initials-Boosted Coexisting Chaos in 2D Sine Map and Its Hardware Implementation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1132–1140, 2020.

[21] A. A. Khennaoui, A. O. Almatroud, A. Ouannas et al., "An unprecedented 2-dimensional discrete-time fractional-order system and its hidden chaotic attractors," *Mathematical Problems in Engineering*, vol. 2021, Article ID 6768215, 10 pages, 2021.

[22] Y. Li, X. He, and W. Zhang, "The fractional difference form of sine chaotification model," *Chaos, Solitons & Fractals*, vol. 137, Article ID 109774, 2020.

[23] Y.-R. Bai, D. Baleanu, and G.-C. Wu, "A novel shuffling technique based on fractional chaotic maps," *Optik*, vol. 168, pp. 553–562, 2018.

[24] G.-C. Wu, D. Baleanu, and Z.-X. Lin, "Image encryption technique based on fractional chaotic time series," *Journal of Vibration and Control*, vol. 22, no. 8, pp. 2092–2099, 2016.

[25] L. Ding and Q. Ding, "A novel image encryption scheme based on 2D fractional chaotic map, dwt and 4D hyper-chaos," *Electronics*, vol. 9, no. 8, p. 1280, 2020.

[26] A. Akgül, C. Arslan, and B. Aricioğlu, "Design of an interface for random number generators based on integer and fractional order chaotic systems," *Chaos Theory and Applications*, vol. 1, no. 1, pp. 1–18, 2019.

[27] C. Yang, I. Taralova, J. J. Loiseau, and S. El-Assad, "A Stream Cipher Based on Fractional Pseudo Chaotic Random Number Generator," in *Proceedings of the 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 1–6, IEEE, London, UK, December 2020.

[28] A. Akgul, O. F. Boyraz, K. Rajagopal, E. Guleryuz, M. Z. Yildiz, and M. Kutlu, "An unforced megastable chaotic oscillator and its application on protecting electrophysiological signals," *Zeitschrift für Naturforschung A*, vol. 75, no. 12, pp. 1025–1037, 2020.

[29] A. D. Algarni, N. F. Soliman, H. A. Abdallah, and F. E. Abd El-Samie, "Encryption of ecg signals for telemedicine applications," *Multimedia Tools and Applications*, vol. 80, pp. 1–25, 2020.

[30] C.-F. Lin, C.-H. Chung, and J.-H. Lin, "A chaos-based visual encryption mechanism for clinical EEG signals," *Medical, & Biological Engineering & Computing*, vol. 47, no. 7, pp. 757–762, 2009.

[31] C. F. Lin, S. H. Shih, and J. D. Zhu, "Chaos based encryption system for encrypting electroencephalogram signals," *Journal of Medical Systems*, vol. 38, no. 5, pp. 49–10, 2014.

[32] C. F. Lin, "Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals," *Journal of Medical Systems*, vol. 40, no. 3, pp. 1–10, 2016.

[33] M. A. Murillo-Escobar, L. Cardoza-Avendaño, R. M. López-Gutiérrez, and C. Cruz-Hernández, "A double chaotic layer encryption algorithm for clinical signals in telemedicine," *Journal of Medical Systems*, vol. 41, no. 4, p. 59, 2017.

[34] M. Irfan, A. Ali, M. A. Khan, M. Ehatisham-ul-Haq, S. N. M. Shah, and W. Ahmad, "Pseudorandom number generator (prng) design using hyper-chaotic modified robust logistic map (hc-mrlm)," *Electronics*, vol. 9, no. 1, p. 104, 2020.

[35] P. Ayubi, S. Setayeshi, and A. M. Rahmani, "Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, vol. 52, Article ID 102472, 2020.

[36] B. Stoyanov and T. Ivanova, "CHAOSA: chaotic map based random number generator on Arduino platform," *AIP Conference Proceedings*, AIP Publishing LLC, vol. 2172, no. 1, , Article ID 90001, 2019.

[37] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.

[38] L. Liu, S. Miao, M. Cheng, and X. Gao, "A pseudorandom bit generator based on new multi-delayed Chebyshev map," *Information Processing Letters*, vol. 116, no. 11, pp. 674–681, 2016.

[39] X. Tang and S. Mandal, "Encrypted physical layer communications using synchronized hyperchaotic maps," *IEEE Access*, vol. 9, Article ID 13286, 2021.

[40] C. Meshram, R. W. Ibrahim, A. J. Obaid, S. G. Meshram, A. Meshram, and A. M. Abd El-Latif, "Fractional chaotic maps based short signature scheme under human-centered iot environments," *Journal of Advanced Research*, vol. 32, 2020.

[41] Y.-M. Chu, S. Bekiros, E. Zambrano-Serrano et al., "Artificial macro-economics: a chaotic discrete-time fractional-order laboratory model," *Chaos, Solitons & Fractals*, vol. 145, Article ID 110776, 2021.

[42] O. Megherbi, H. Hamiche, S. Djennoune, and M. Bettayeb, "A new contribution for the impulsive synchronization of fractional-order discrete-time chaotic systems," *Nonlinear Dynamics*, vol. 90, no. 3, pp. 1519–1533, 2017.

[43] A. M. A. El-Sayed, A. Elsonbaty, A. A. Elsadany, and A. E. Matouk, "Dynamical analysis and circuit simulation of a new fractional-order hyperchaotic system and its discretization," *International Journal of Bifurcation and Chaos*, vol. 26, no. 13, Article ID 1650222, 2016.

[44] J. Wang, L. Xiao, K. Rajagopal, A. Akgul, S. Cicek, and B. Aricioglu, "Fractional-order analysis of modified chua's circuit system with the smooth degree of 3 and its micro-controller-based implementation with analog circuit design," *Symmetry*, vol. 13, no. 2, 2021.

[45] S. M. Ismail, L. A. Said, A. A. Rezk et al., "Generalized fractional logistic map encryption system based on fpga," *AEU - International Journal of Electronics and Communications*, vol. 80, pp. 114–126, 2017.

[46] F. Atici and P. Eloe, "Initial value problems in discrete fractional calculus," *Proceedings of the American Mathematical Society*, vol. 137, no. 3, pp. 981–989, 2009.

[47] T. Abdeljawad, "On Riemann and Caputo fractional differences," *Computers & Mathematics with Applications*, vol. 62, no. 3, pp. 1602–1611, 2011.

[48] G. A. Anastassiou, "Principles of delta fractional calculus on time scales and inequalities," *Mathematical and Computer Modelling*, vol. 52, no. 3-4, pp. 556–566, 2010.

[49] Z. Wang, A. J. M. Khalaf, H. Tian, A. Alsaedi, and T. Hayat, "A chaotic map with infinite number of equilibria in a bounded domain," *The European Physical Journal - Special Topics*, vol. 229, no. 6-7, pp. 1109–1116, 2020.

[50] D. Cafagna and G. Grassi, "An effective method for detecting chaos in fractional-order systems," *International Journal of Bifurcation and Chaos*, vol. 20, no. 3, pp. 669–678, 2010.

[51] L. Liu, H. Xiang, and X. Li, "A novel perturbation method to reduce the dynamical degradation of digital chaotic maps," *Nonlinear Dynamics*, vol. 103, no. 1, pp. 1–17, 2021.

[52] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences*, vol. 88, no. 6, pp. 2297–2301, 1991.

[53] I. Zyma, S. Tukaev, I. Seleznov et al., "Electroencephalograms during mental arithmetic task performance," *Data*, vol. 4, no. 1, p. 14, 2019.

[54] A. L. Goldberger, L. A. Amaral, L. Glass et al., "PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–20, 2000.

[55] X. Liao, Z. Gao, and H. Huang, "Synchronization Control of Fractional-Order Discrete-Time Chaotic Systems," in *Proceedings of the 2013 European control conference (ECC)*, pp. 2214–2219, IEEE, Zurich, Switzerland, July 2013.

[56] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Booz-allen and hamilton inc mclean va*, 2001.

[57] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[58] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[59] G. Manjunath and G. V. Anand, "Speech Encryption Using Circulant Transformations," *Proceedings. IEEE International Conference on Multimedia and Expo*, vol. 1pp. 553–556, IEEE, Lausanne, Switzerland, August 2002.

[60] E. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, "Chaotic encryption of speech signals," *International Journal of Speech Technology*, vol. 14, no. 4, pp. 285–296, 2011.

[61] E. M. Elshamy, E.-S. M. El-Rabaie, O. S. Faragallah, O. A. Elshakankiry, F. E. A. El-Samie, and S. F. El-Zoghdy, "Efficient audio cryptosystem based on chaotic maps and double random phase encoding," *International Journal of Speech Technology*, vol. 18, no. 4, pp. 619–631, 2015.

[62] D. Renza, S. Mendoza, and D. M. Ballesteros, "High-uncertainty audio signal encryption based on the Collatz conjecture," *Journal of Information Security and Applications*, vol. 46, pp. 62–69, 2019.

[63] L. Gerardo, D. L. Fraga, E. T. Pérez, E. Tlelo-Cuautle, and C. Mancillas-López, ".Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dynamics*, vol. 90, no. 3, pp. 1661–1670, 2017.