Analog Integrated Circuits and Signal Processing (2022) 112:49–63
https://doi.org/10.1007/s10470-022-02040-z

RNG and circuit implementation of a fractional order chaotic attractor based on two degrees of freedom nonlinear system

Burak Arıcıoğlu[1]

Received: 4 December 2021 / Revised: 31 March 2022 / Accepted: 13 April 2022 / Published online: 6 May 2022

Abstract
In this study, fractional order form of a chaotic system based on a two degrees of freedom nonlinear mechanical system is considered for the first time in the literature. Firstly, the state variables of the fractional order chaotic attractor are obtained numerically with Grünwald–Letnikov (GL) method. Circuit implementation of the fractional order chaotic attractor is carried out based on the approximated the transfer function of fractional integration. Moreover, a PRNG is designed using the LSB of the state variables. The NIST statistical results of designed PRNG shows that it has adequate randomness. Also, an audio encryption application is realized with the designed PRNG. The performance analysis of the encryption application shows that the designed PRNG can be used in other engineering fields like data security.

Keywords Chaos · Fractional order systems · RNG · Electronic circuits · Mechanical systems · Two degrees of freedom

1 Introduction

Chaos and chaos-based applications have become one of the most popular subjects of the literature in the recent years. Chaos or chaotic systems have been employed on many different engineering areas such as communication [1], image processing [2], DC-DC converters [3], fuzzy logic [4], control [5], optimization [6] and especially random number generations [7, 8] and data encryption [9, 10]. The reason why chaos is usually preferred in random number generations and data encryption is that chaotic signals are aperiodic, noise like signals and difficult to predict.

Most of the chaotic systems used in the literature are purely mathematical which do not model a physical system or phenomenon. However, some nonlinear physical systems may exhibit chaotic behaviour for certain system parameters' values and initial conditions. In the literature, there are studies where physical system models were used and analysed [11–13]. For example, non-linear mechanical systems were used in studies [14, 15]. In these studies, chaotic behaviour was analysed by applying non-linear inputs to the systems. In this regard, a chaotic system derived from an actual physical system is considered in this study. The chaotic system used in the study models a two degrees of freedom nonlinear mechanical system and given in [16].

Chaotic systems can be categorized as integer order and fractional order chaotic systems. In the integer order chaotic systems, the order of the derivatives are integer numbers whereas in the fractional order chaotic systems, the order of the derivatives can be any real positive number. In the literature, there is a great number of studies which involve integer order chaotic systems and their applications. On the other hand, fractional order chaotic systems have attracted great attention in the recent years because the fractional order systems have higher nonlinearity and can exhibit more complex dynamical behaviour than integer order systems.

In this paper, the fractional order form of the chaotic system obtained from a two degree of freedom nonlinear mechanical system is studied. To the best of author knowledge, the fractional order chaotic system based on an two degrees of freedom nonlinear mechanical system is never studied in the literature. The state variable of the fractional order system numerically calculated with a GL

✉ Burak Arıcıoğlu
baricioglu@subu.edu.tr

[1] Department of Electrical and Electronics Engineering, Sakarya University of Applied Sciences, 54187 Sakarya, Turkey

fractional order derivative definition-based algorithm. From calculated values of the state variables of the fractional order chaotic system pseudo random numbers are generated. Then, the NIST 800-22 statistical tests [17] are performed on the generated random numbers to assess the randomness of the generated numbers. Later, as an engineering application, an audio encryption application is carried out with the generated random numbers. Moreover, the circuit realization of the fractional order chaotic system is carried out.

The paper is so organized that, Sect. 2 provides Two Degrees of Freedom Nonlinear Mechanical System, Sect. 3 contains Fractional Order Chaotic Attractor, Sect. 4 contains Circuit Implementation of the Fractional Order Chaotic Attractor, Sect. 5 contains PRNG Implementation and Audio Encryption Applications, and Sect. 6 offers Conclusion.

2 Two degrees of freedom nonlinear mechanical system

In this section, the chaotic system derived from the mechanical system is mentioned. The two degrees of freedom nonlinear mechanical system with a nonlinear spring (k_2) is given in Fig. 1. The function that defines the nonlinear spring k_2 is given in (1).

$$f_{k_2}(t) = k_2[x(t)]^2 \tag{1}$$

Using the function given in (1) , the mathematical expression of the system given in Fig. 1 is obtained as in (2) [18]

$$\begin{aligned} m_1\ddot{x_1}(t) + b_1\dot{x_1}(t) + k_1x_1(t) + k_2[x_1(t) - x_2(t)]^2 &= 0 \\ m_2\ddot{x_2}(t) + b_2\dot{x_2}(t) + k_2[x_2(t) - x_1(t)]^2 &= f(t) \end{aligned} \tag{2}$$

The equation system given in (2) has two second order nonlinear differential equations. The equation system can be expressed as a 4D differential equation system by using state variables. Moreover, the order of the differential equations becomes the first order by using state variables. As a first step, to move the system to state space, the mathematical model of the system rearranged as in (3) and the state variables given in (4).

$$\begin{aligned} \ddot{x_1}(t) &= -\frac{b_1}{m_1}\dot{x_1}(t) - \frac{k_1}{m_1}x_1(t) - \frac{k_2}{m_1}[x_1(t) - x_2(t)]^2 \\ \ddot{x_2}(t) &= \frac{1}{m_2}f(t) - \frac{b_2}{m_2}\dot{x_2}(t) - \frac{k_2}{m_2}[x_2(t) - x_1(t)]^2 \end{aligned} \tag{3}$$

$$x = x_1(t), \quad y = x_2(t), \quad z = \dot{x_1}(t), \quad w = \dot{x_2}(t) \tag{4}$$

Using (3) and (4) the system given in (2) can be redefined as in (5).

$$\begin{aligned} \dot{x} &= z \\ \dot{y} &= w \\ \dot{z} &= -\frac{b_1}{m_1}z - \frac{k_1}{m_1}x - \frac{k_2}{m_1}(x - y)^2 \\ \dot{w} &= \frac{1}{m_2}f(t) - \frac{b_2}{m_2}w - \frac{k_2}{m_2}(y - x)^2 \end{aligned} \tag{5}$$

Now, the system parameters can be defined as follows:

$$\frac{b_1}{m_1} = \alpha, \quad \frac{k_1}{m_1} = \beta, \quad \frac{k_2}{m_1} = \rho, \quad \frac{b_2}{m_2} = \sigma, \quad \frac{k_2}{m_2} = \zeta \tag{6}$$

Since the applied function is a unit step function the term $\frac{1}{m_2}f(t)$ can be defined as a separate system parameter.

$$\frac{f(t)}{m_2} = \gamma \tag{7}$$

When the defined parameters given in (6) and (7) are substituted in (5), the equation system can be expressed as in (8)

$$\begin{aligned} \dot{x} &= z \\ \dot{y} &= w \\ \dot{z} &= -\alpha z - \beta x - \rho(x - y)^2 \\ \dot{w} &= \gamma - \sigma w - \zeta(y - x)^2 \end{aligned} \tag{8}$$

The system given in (8) will exhibit chaotic behaviour for certain parameter and initial condition values and the fractional form of the system will be discussed in the next section.

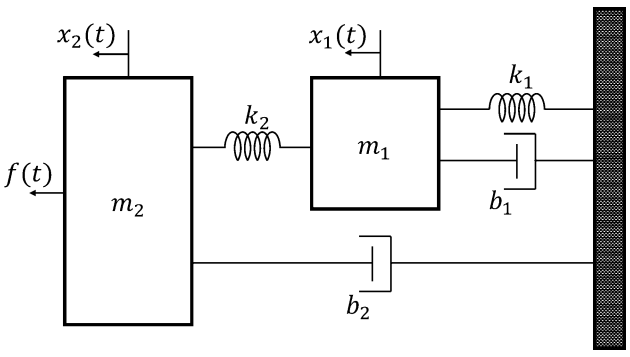

Fig. 1 A two degrees of freedom nonlinear mechanic system

3 Fractional order chaotic attractor

In this section, fractional order form of the system in (8) is given. To study fractional order systems, fractional order derivative or integral operator must be defined. There are

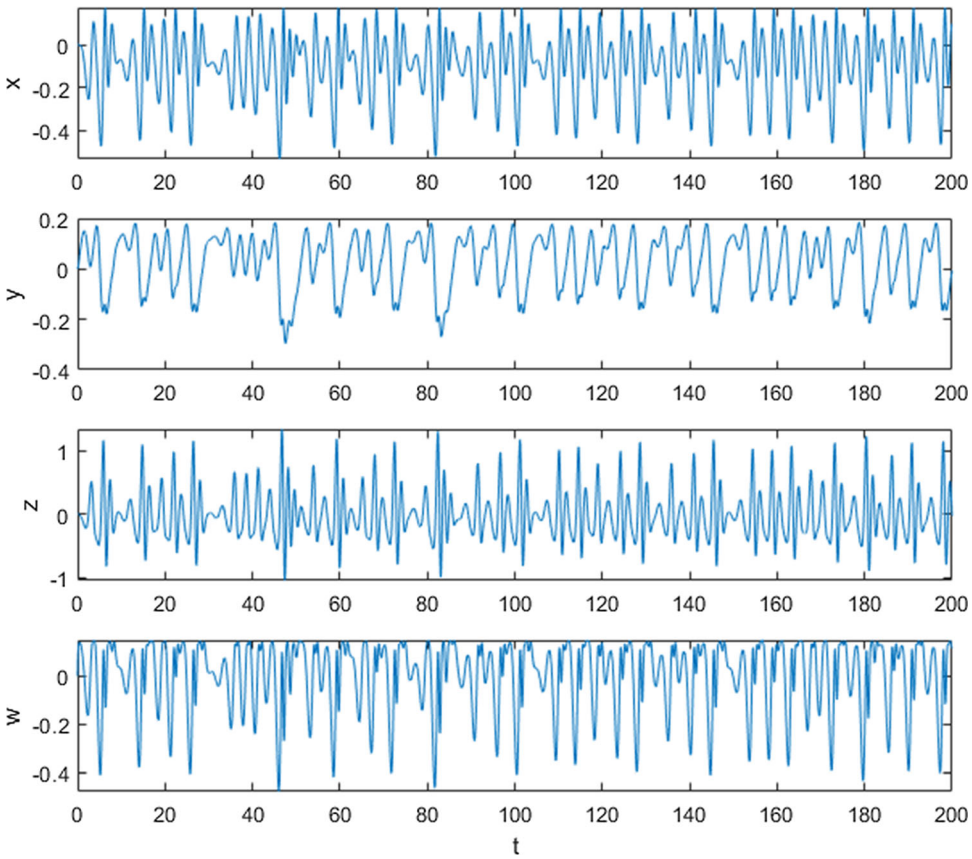

Fig. 2 The time series of the fractional order chaotic system for the fractional order $q = 0.99$, the system parameters $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$ and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$

many fractional order derivative or integral definitions in the literature. The most common used ones are the Riemann–Liouville (RL), Caputo and Grünwald–Letnikov (GL) definitions. The RL fractional order derivative definition is [19]

$$ {}^{RL}{}_aD_t^q f(t) = \frac{1}{\Gamma(n-q)} \frac{d^n}{dt^n} \int_a^t \frac{f(\tau)}{(t-\tau)^{q-n+1}} d\tau \tag{9} $$

The Caputo fractional order derivative definition is [19]

$$ {}^{C}{}_aD_t^q f(t) = \frac{1}{\Gamma(n-q)} \int_a^t \frac{f^{(n)}(\tau)}{(t-\tau)^{q-n+1}} d\tau \tag{10} $$

and the GL fractional order derivative is [19]

$$ {}^{GL}{}_aD_t^q f(t) = \frac{1}{h^q} \sum_{i=0}^{(t-a)/h} c_i f(t-ih) \tag{11} $$

where c_i is the $i^t h$ binomial coefficient and it is calculated as

$$ c_0 = 1, \quad c_i = \left(1 - \frac{q+1}{i}\right) c_{i-1}, \quad i = 1, 2, \ldots \tag{12} $$

In all the equations above D is the fractional order derivative operator, q is the fractional order, a is the initial value, Γ is the gamma function, n is the smallest integer greater than fractional order q and h is the step size. In this study, GL definition is employed for the numerical solution of the fractional order chaotic system.

The fractional form of the system (8) is given in (13)

$$ \begin{aligned} \frac{d^q x}{dt^q} &= z \\ \frac{d^q y}{dt^q} &= w \\ \frac{d^q z}{dt^q} &= -\alpha z - \beta x - \rho (x-y)^2 \\ \frac{d^q w}{dt^q} &= \gamma - \sigma w - \zeta (y-x)^2 \end{aligned} \tag{13} $$

Here fractional order is selected as $q = 0.99$, the system parameters are set as $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$. For these values, time series of the fractional order system is given in Fig. 2 and phase portraits of the fractional order chaotic system is given in Fig. 3. As seen in these figures, fractional order chaotic system exhibits chaotic behaviour for the specified parameter and initial condition values.

Also, Lyapunov exponents analysis is performed to show the fractional order system exhibits chaotic behaviour for the given parameter and initial condition values. The

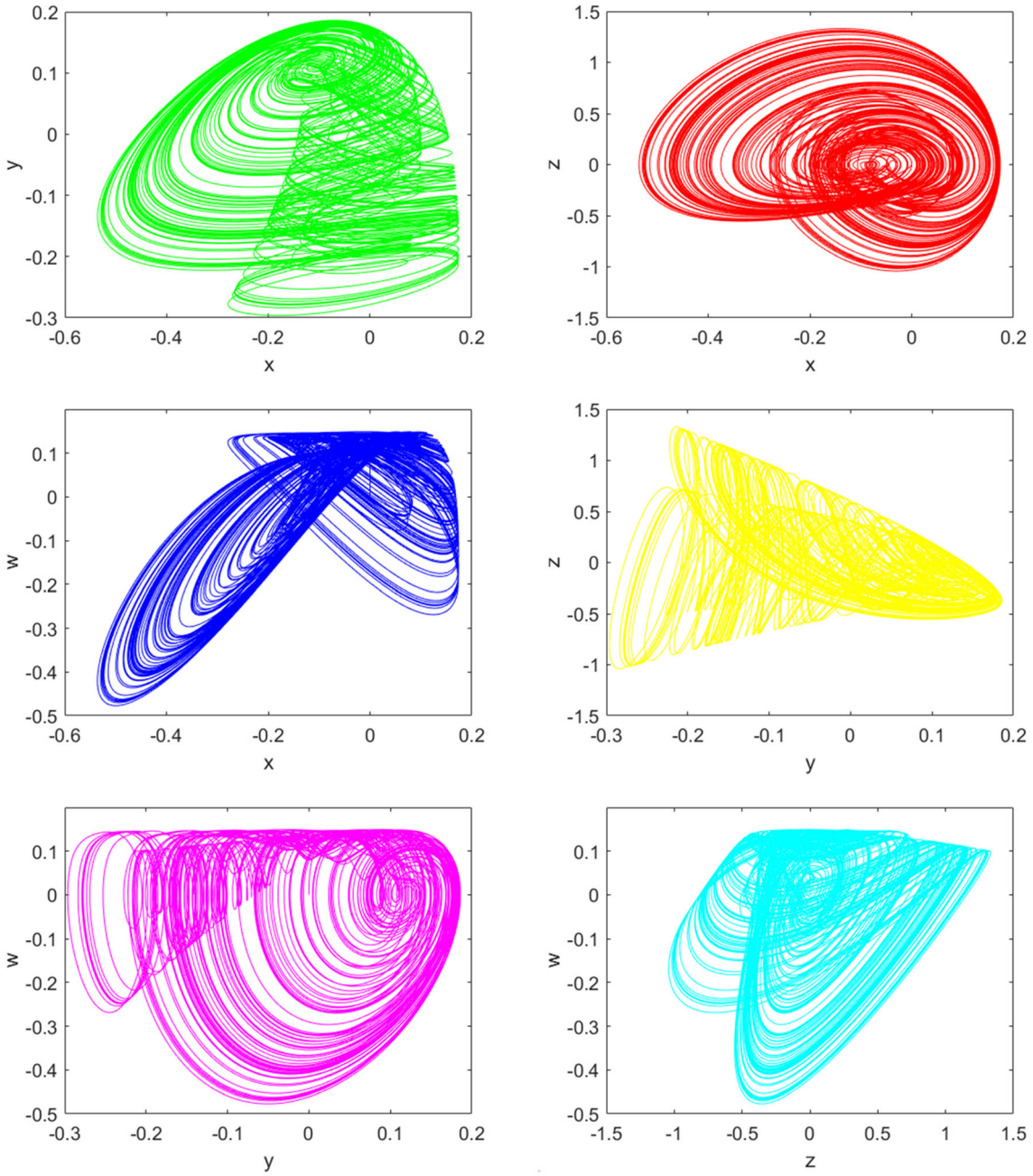

Fig. 3 The phase portraits of the fractional order chaotic system for the fractional order $q = 0.99$, the system parameters $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$

number of Lyapunov exponents of a system equals to that of system dimension. For a 4D system to show chaotic behaviour, two of the obtained exponents must be negative, one of them must be positive, and the last one must be zero. For the system parameters $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions $x_0 = y_0 = z_0 = w_0 = 0$, the Lyapunov exponent spectrum with respect to the fractional order q is given in Fig. 4. As seen in Fig. 4, the system exhibits chaotic behaviour for the values of the fractional order q are in between 0.5 and 1.

4 Circuit implementation of the fractional order chaotic attractor

In this section, circuit implementation of the fractional order chaotic system is given. To realize circuit implementation of the fractional order chaotic system a

fractional order integrator circuit is needed. However, fractional order integrator circuit cannot be realized with analog discrete components directly. To overcome this setback, approximated transfer function of fractional order integrator is used. Since this problem is solved with approximated transfer function, the fractional integration is handled in frequency domain.

Let $f(t)$ a function defined in time domain and $F(s)$ to be the Laplace transform of $f(t)$. Then, the Laplace transform of fractional-order integral of $f(t)$ is

$$\frac{1}{s^q}F(s) \tag{14}$$

where q is the fractional order of the integration [20]. Then, the transfer function of the fractional order integrator is

$$\frac{1}{s^q} \tag{15}$$

This transfer function cannot be realized directly with analog discrete components. The bode plot of the transfer function given in (15) has slope of $-20q$ dB/dec. Charef et.al [21] approximate this bode plot as zig-zag lines which have slopes of 0 dB/dec and -20 dB/dec. The approximated the transfer function is [21]

$$\frac{1}{\left(1+\frac{s}{p_t}\right)^q} \approx \frac{\prod_{i=0}^{N-1}\left(1+\frac{s}{z_i}\right)}{\prod_{i=0}^{N}\left(1+\frac{s}{p_i}\right)} \tag{16}$$

where p_t is the corner frequency (or $1/p_t$ is the relaxation time), z_i and p_i are the zeros and poles of the approximated transfer function respectively and are calculated as

$$\begin{aligned} p_0 &= p_t 10^{y/20q} \\ z_i &= \left(10^{y/10q(1-q)}\right)^i 10^{y/10(1-q)} p_0 \\ p_i &= \left(10^{y/10q(1-q)}\right)^i p_0 \end{aligned} \tag{17}$$

Here y is the maximum error in dB between the actual and the approximated lines. The value of N given in Eq. 16 is calculated as [21]

$$N = Integer\left(\frac{\log\left(\frac{w_{max}}{p_0}\right)}{\frac{y}{10q(1-q)}}\right) + 1 \tag{18}$$

In this paper, the fractional order is $q = 0.99$, the maximum error $y = 0.3$ dB, the corner frequency $p_t = 0.01$ rad/s, the maximum frequency $w_max = 100$ rad/s. With these values the approximated transfer function of the fractional order ($q = 0.99$) integrator becomes

$$\frac{1.137s^2 + 12640s + 130700}{s^3 + 11920s^2 + 132300s + 1369} \tag{19}$$

This transfer function can be realized with analog discrete components. The realized fractional order integrator for $q = 0.99$ is given in Fig. 5 with normalized component values.

However, the component values in Fig. 5 are not practical. As a next step, magnitude scaling process is applied to the fractional order integrator. Magnitude scaling is a process in which all the impedances in a network are scaled with the same scaling factor so that the transfer function of the network remains the same. For magnitude scaling, scaling factor is selected as $k_m = 4 \times 10^5$. After magnitude scaling process, frequency scaling process is applied to the integrator circuit. Frequency scaling is the process of shifting the frequency response of a network up or down the frequency axis while leaving the impedance the same. For an RC network, the value of capacitors decreases with the scaling factor while that of resistors remain unchanged in frequency scaling process. Frequency scaling factor is selected as $k_f = 2500$. The component values after applying both magnitude and frequency scaling processes are given in Fig. 6.

As it is seen in Fig. 2, the amplitude values of the state variable of the fractional order chaotic system are very low. The amplitude of the state variables x, y, z and w is between 0.2 and 1. Thus, the state variables of the system are firstly scaled up to increase their amplitude values. After scaling process, the electronic circuit of the fractional order chaotic system is simulated in ORCAD-PSpice. Then, the fractional order chaotic system is realized with real electronic circuit components and the phase portraits of the system is obtained via an oscilloscope.

The state variable x is scaled up by the factor of 20, the state variable y is scaled up by the factor of 25, the state variable z is scaled up by the factor of 5, and the state variable w is scaled up by the factor of 15. For the state variable scaling process, let $X = 20x$, $Y = 25y$, $Z = 5z$, and $W = 15w$ and then the scaled state variables X, Y, Z, and W is substituted in (13), the fractional order chaotic system becomes

$$\begin{aligned} \frac{d^q x}{dt^q} &= Z/5 \\ \frac{d^q y}{dt^q} &= W/15 \\ \frac{d^q z}{dt^q} &= -\alpha Z/5 - \beta X/20 - \rho(X/20 - Y/25)^2 \\ \frac{d^q w}{dt^q} &= \gamma - \sigma W/15 - \zeta(Y/25 - X/20)^2 \end{aligned} \tag{20}$$

Since $X = 20x$, $Y = 25y$, $Z = 5z$, and $W = 15w$, the relation given in (21) can be written for the fractional order derivatives

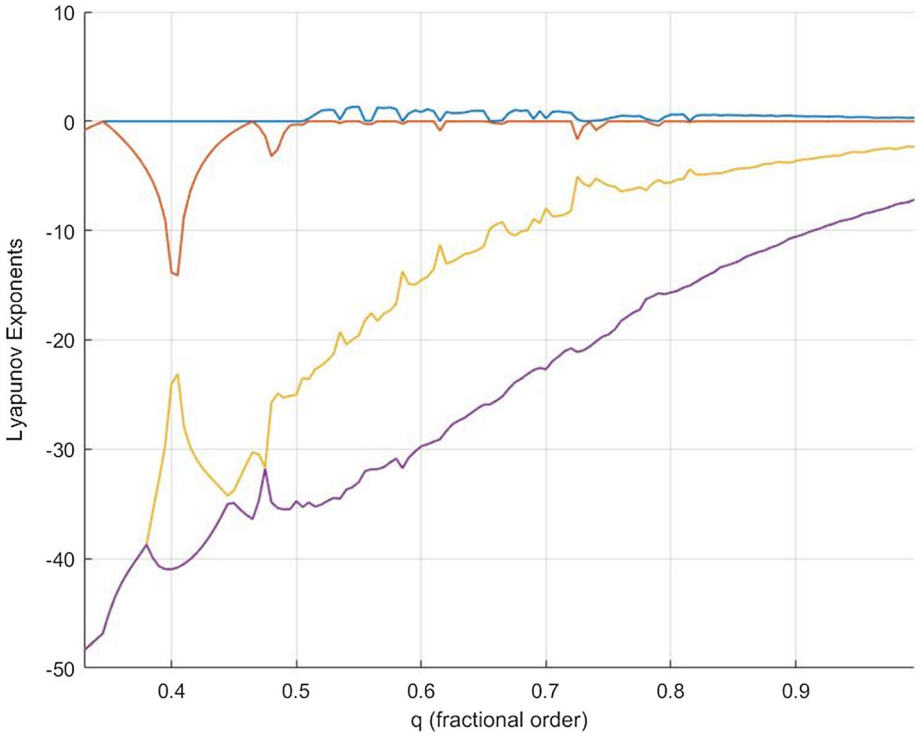

Fig. 4 Lyapunov exponent spectrum of the fractional order chaotic system with respect to the fractional order q

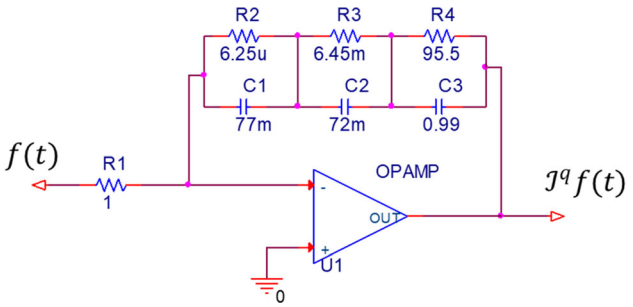

Fig. 5 Normalized fractional order integrator circuit for the fractional order is $q = 0.99$, the maximum error $y = 0.3$ dB, the corner frequency $p_t = 0.01$ rad/s, and the maximum frequency $w_{max} = 100$ rad/s

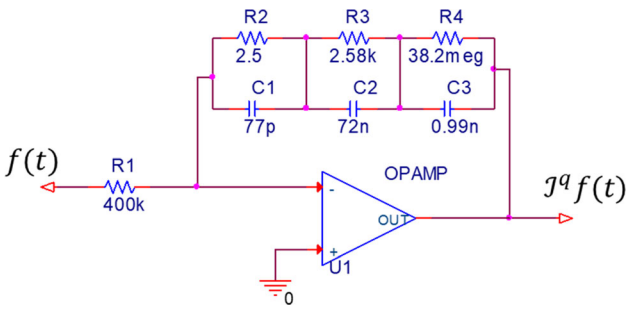

Fig. 6 The fractional order integrator circuit after applying magnitude and frequency scaling processes. (The fractional order is $q = 0.99$, the maximum error $y = 0.3$ dB, the corner frequency $p_t = 25$ rad/s, and the maximum frequency $w_{max} = 250$ krad/s)

$$\begin{aligned}
\frac{d^qX}{dt^q} &= 20\frac{d^qx}{dt^q}\\
\frac{d^qY}{dt^q} &= 25\frac{d^qy}{dt^q}\\
\frac{d^qZ}{dt^q} &= 5\frac{d^qz}{dt^q}\\
\frac{d^qW}{dt^q} &= 15\frac{d^qw}{dt^q}
\end{aligned} \tag{21}$$

By combining (20) and (21) the scaled fractional order chaotic system can be written as

$$\begin{aligned}
\frac{d^qX}{dt^q} &= 20Z/5\\
\frac{d^qY}{dt^q} &= 25W/15\\
\frac{d^qZ}{dt^q} &= -5\alpha Z/5 - 5\beta X/20 - 5\rho(X/20 - Y/25)^2\\
\frac{d^qW}{dt^q} &= 15\gamma - 15\sigma W/15 - 15\zeta(Y/25 - X/20)^2
\end{aligned} \tag{22}$$

Finally, the scaled fractional order chaotic system will be

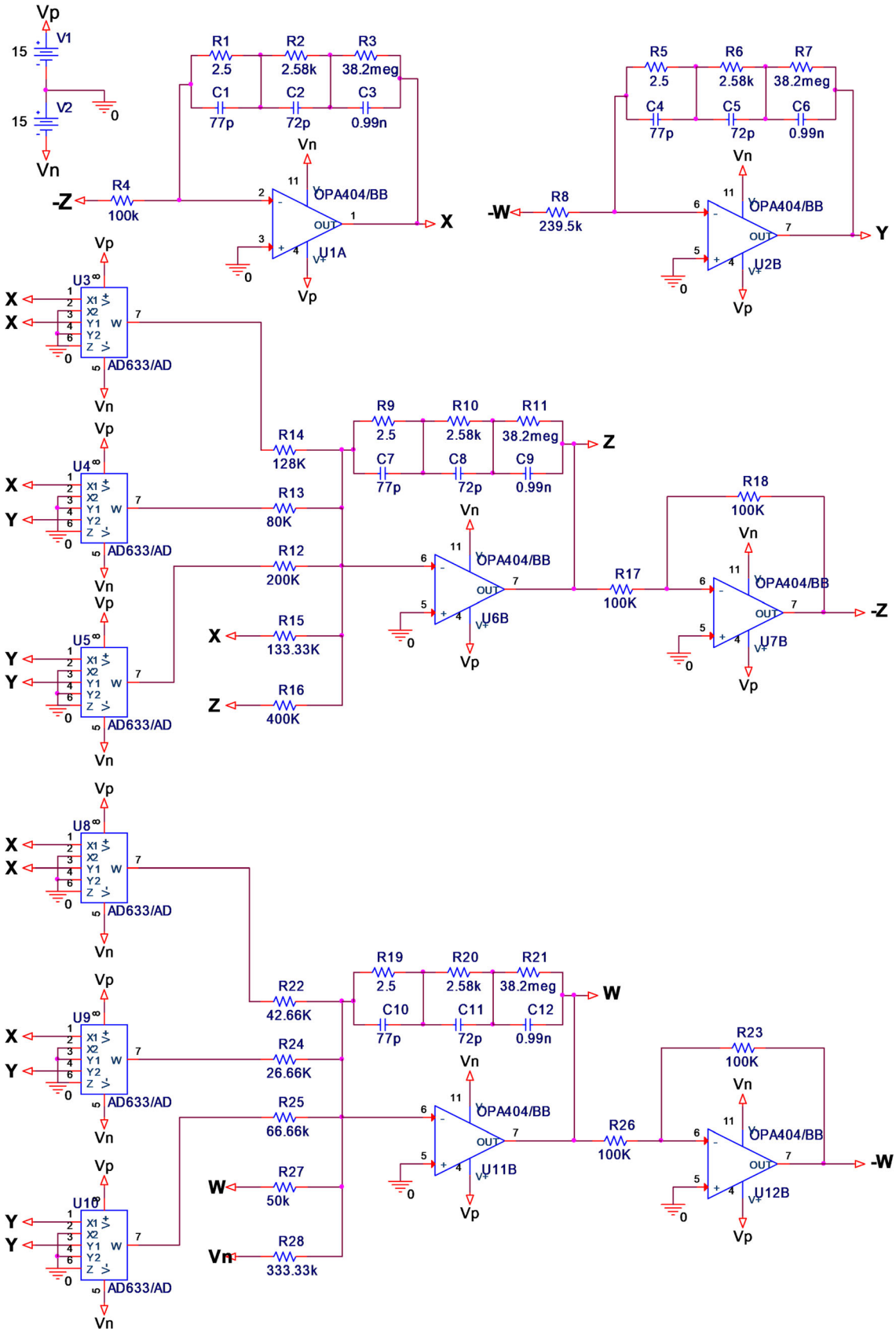

Fig. 7 Electronic circuit implementation of the fractional order chaotic system

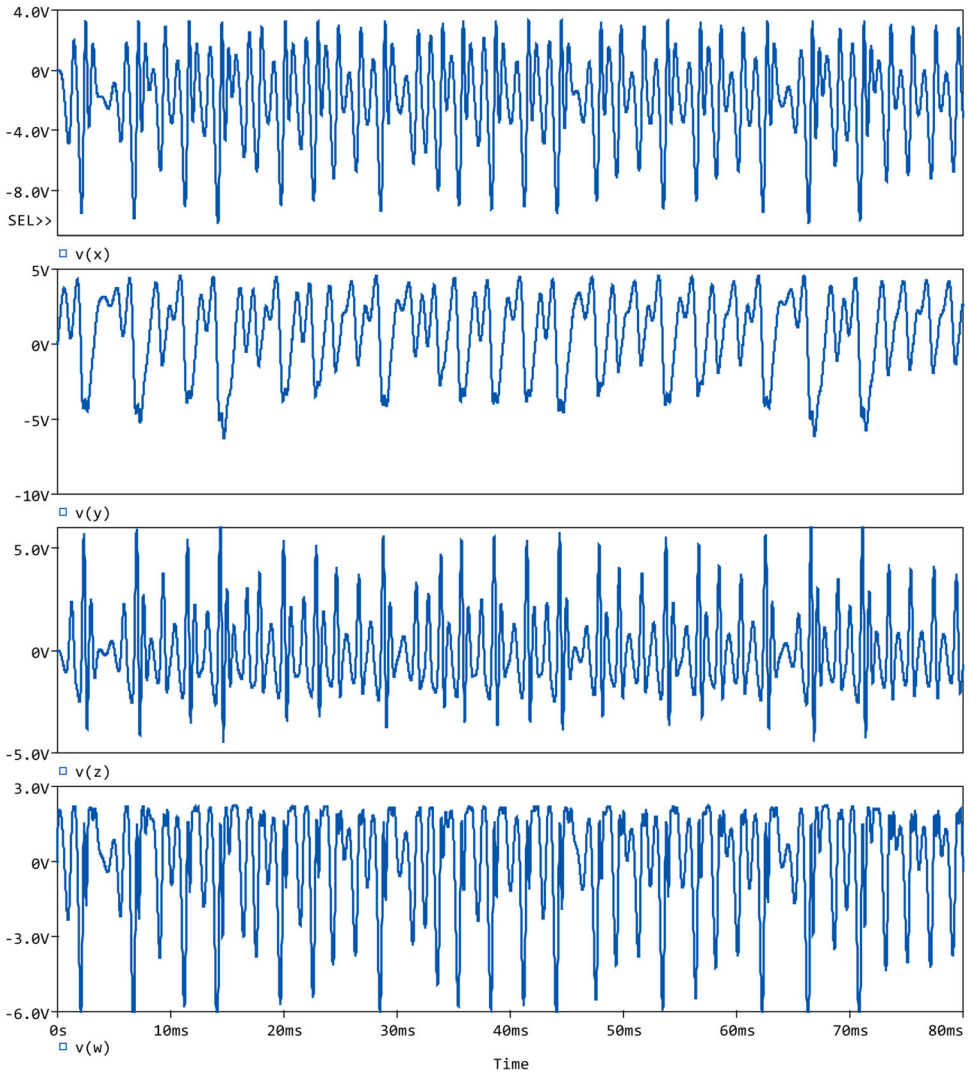

Fig. 8 The time series of the scaled fractional order chaotic system obtained in ORCAD-PSpice for the fractional order $q = 0.99$, the system parameters $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$

$$\begin{aligned}
\frac{d^q X}{dt^q} &= 4Z \\
\frac{d^q Y}{dt^q} &= 5W/3 \\
\frac{d^q Z}{dt^q} &= -\alpha Z/5 - \beta X/4 - 5\rho(X/20 - Y/25)^2 \\
\frac{d^q W}{dt^q} &= 15\gamma - \sigma W - 15\zeta(Y/25 - X/20)^2
\end{aligned} \tag{23}$$

The electronic circuit correspond to the scaled system given in (23) is shown in Fig. 7. The circuit contains both passive and active elements which are resistors, capacitors, operational amplifiers (OPAMPs) and analog multiplier integrated circuits (ICs). The circuit is realised for parameter values $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$.

The active elements used in the circuit are OPA404 Op-amps and the AD633 analog multiplier ICs. The values of the passive elements as follow: $R_1 = R_5 = R_9 = R_{19} = 2.5\Omega, R_2 = R_6 = R_{10} = R_{20} = 2.58\ \text{k}\Omega, R_3 = R_7 = R_{11} = R_{21} = 38.2\ \text{M}\Omega, R_4 = R_{17} = R_{18} = R_{23} = R_{26} = 100\ \text{k}\Omega, R_8 = 239.5\text{k}\Omega, R_{12} = 200\ \text{k}\Omega, R_{13} = 80\ \text{k}\Omega, R_{14} = 128\ \text{k}\Omega, R_{15} = 133.33\ \text{k}\Omega, R_{16} = 400\ \text{k}\Omega, R_{22} = 42.66\ \text{k}\Omega, R_{24} = 26.66\ \text{k}\Omega, R_25 = 66.66\ \text{k}\Omega, R_27 = 50\ \text{k}\Omega, R_{28} = 33.33\ \text{k}\Omega$, and $C_1 = C_4 = C_7 = C_{10} = 0.77$ pF, $C_2 = C_5 = C_8 = C_{11} = 0.72$ pF and $C_3 = C_6 = C_9 = C_{12} = 0.99$ nF.

The time series and the phase portraits of the scaled fractional order chaotic system obtained from ORCAD-PSpice simulation are given in Figs. 8 and 9, respectively. The time series and the phase portraits shown in Figs. 2 and 3 are very similar to the time series and the phase portraits shown in Figs. 8 and 9. This shows that the scaling processes are correctly performed. Moreover, the

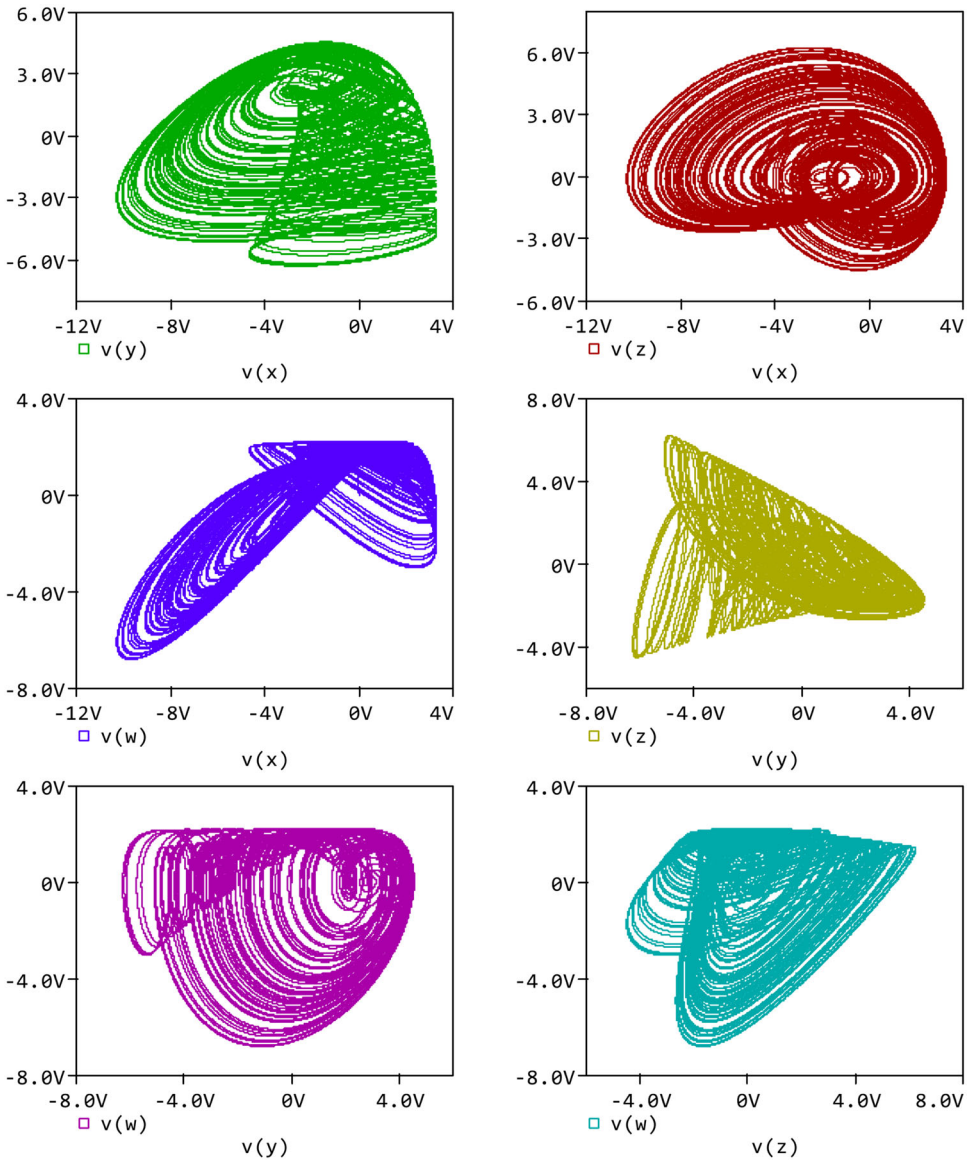

Fig. 9 The phase portraits of the scaled fractional order chaotic system obtained from ORCAD-PSpice for the fractional order $q = 0.99$, the system parameters $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$

phase portraits obtained from real circuit implementation are given in Fig. 10. The oscilloscope results shown in Fig. 10 and the simulation results shown in Fig. 9 are very similar to each other.

5 Engineering applications

In this section, pseudo random number generator (PRNG) based on the fractional order chaotic system and an audio encryption application with the generated random numbers are presented.

5.1 PRNG implementation

Random number generators (RNGs) are used in many different engineering fields such as numerical analysis, game theory, statistics, simulation and especially encryption and data security. One of the most important factors in data security and encryption applications is the randomness of the keys. Since chaotic signals are aperiodic, noise like signals and difficult to predict, it is possible to design RNGs based on chaotic system which will have sufficient randomness for encryption applications. In this section, design steps of chaos based RNG, and its NIST-800-22 test results are presented. The block diagram of PRNG design is given in Fig. 11. In the PRNG design, the continuous

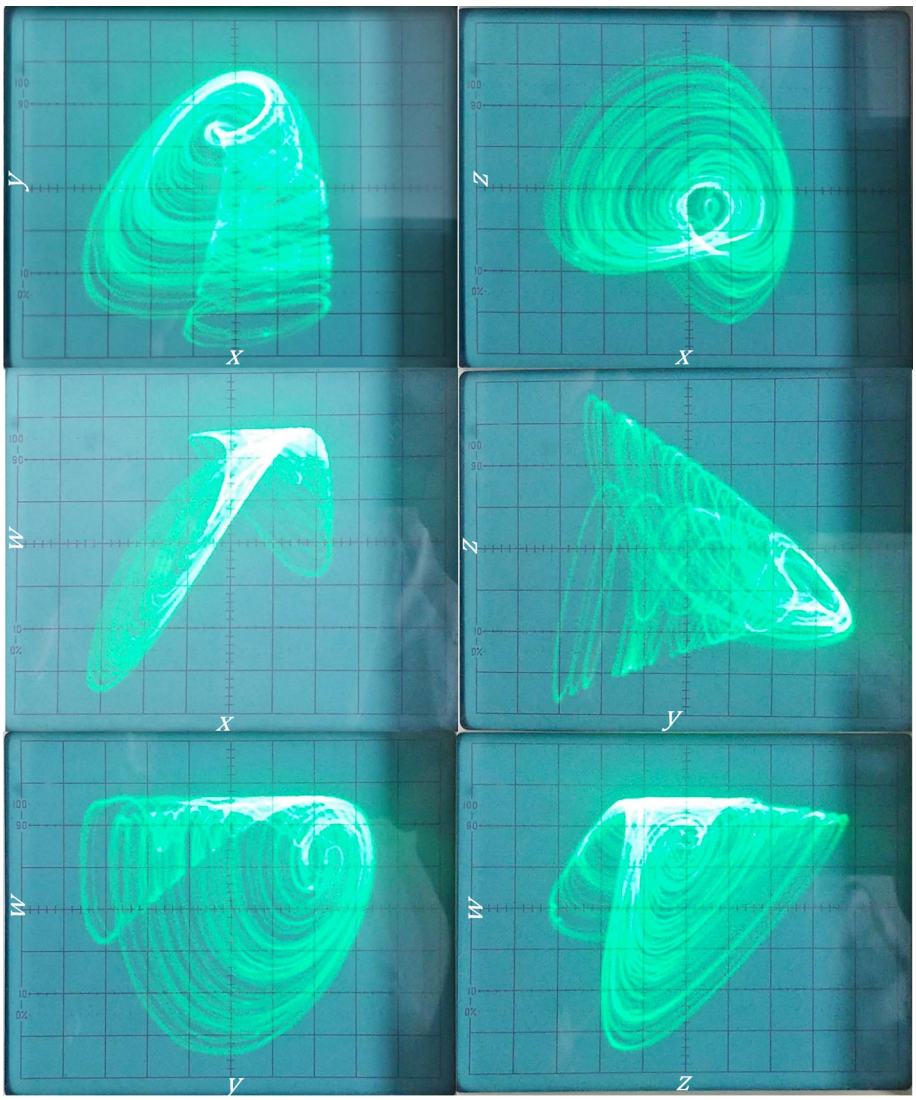

Fig. 10 The phase portraits of the scaled fractional order chaotic system obtained from oscilloscope for the fractional order $q = 0.99$, the system parameters $\alpha = 1,\ \beta = 12,\ \gamma = 1.2,\ \sigma = 8,\ \zeta = 25,\ \rho = 25$, and initial conditions are $x_0 = y_0 = z_0 = w_0 = 0$

time fractional order chaotic system is discretized with GL algorithm as a first step. Then, the numerically calculated state variables with GL algorithm are converted from floating point format into binary format. Then, the last least significant bit (LSB) of every converted binary number is selected. Since there are four state variables, in each iteration total 4 bits are selected and added to the bit series. When the total bit number of the array is reached to a million, the NIST tests can be performed (The NIST-800-22 test suit require a bit series consists of one million bits). The NIST-800-22 statistical tests consist of 16 different tests. If the bit series fail even one of any NIST-800-22 tests, the RNG design process must be redone by changing system parameters and/or initial conditions.

The results of NIST-800-22 statistical tests are assessed according to the defined P value. If the predetermined P value is 0.001, the resultant P values must be greater than or equal to predefined value 0.001 ($P \geq 0.001$) to pass the test successfully for all the 16 tests. The results of the NIST 800-22 tests are given in Table 1 for the designed PRNG. As it is seen in Table 1, the designed PRNG has passed all the 16 statistical tests successfully. The generated numbers can be used in applications that need high security like encryption since they passed the NIST-800-22 tests.

5.2 Audio encryption application

In this section, an example audio encryption application which utilizes the designed chaos based PRNG is presented. In Fig. 12, the block diagram of the audio encryption and decryption processes is shown. For the encryption process, the amplitude value of the audio data in

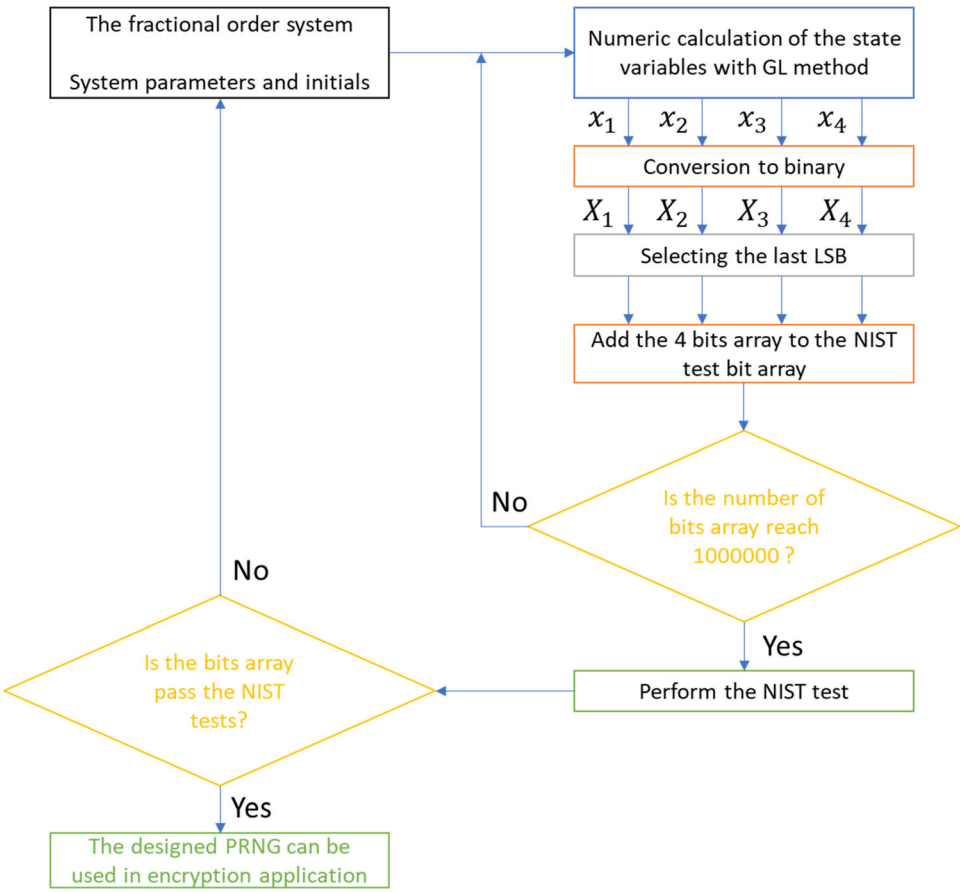

Fig. 11 The block diagram of chaos PRNG design

Table 1 NIST-800-22 test results of designed PRNG

Statistical Tests	*P* value	Result
Frequency (Monobit) Test	0.448450982733033	Successful
Block-Frequency Test	0.415232118095908	Successful
Cumulative-Sums Test	0.698898965106277	Successful
Runs Test	0.612453155069222	Successful
Longest-Run Test	0.158253951739692	Successful
Binary Matrix Rank Test	0.599229102250439	Successful
Discrete Fourier Transform Test	0.354009839268338	Successful
Non-Overlapping Templates Test	0.003858187857881	Successful
Overlapping Templates Test	0.118100273951313	Successful
Maurer's Universal Statistical Test	0.269768360616614	Successful
Approximate Entropy Test	0.122875059468984	Successful
Random-Excursions Test ($x = -4$)	0.193928910985971	Successful
Random-Excursions Variant Test ($x = -9$)	0.703739874119503	Successful
Serial Test-1	0.270373206413360	Successful
Serial Test-2	0.127429195257392	Successful
Linear-Complexity Test	0.145190935638397	Successful

floating point format is converted into binary format. Then, the binary bits of the converted audio data are XORed with the random bits generated from the fractional order chaotic system. Then, the resultant bit series are converted back to floating format to obtained encrypted audio data. In the audio decryption process, the encrypted audio data in floating point format is converted into binary format. Then, the decryption process is performed by XORing the bits

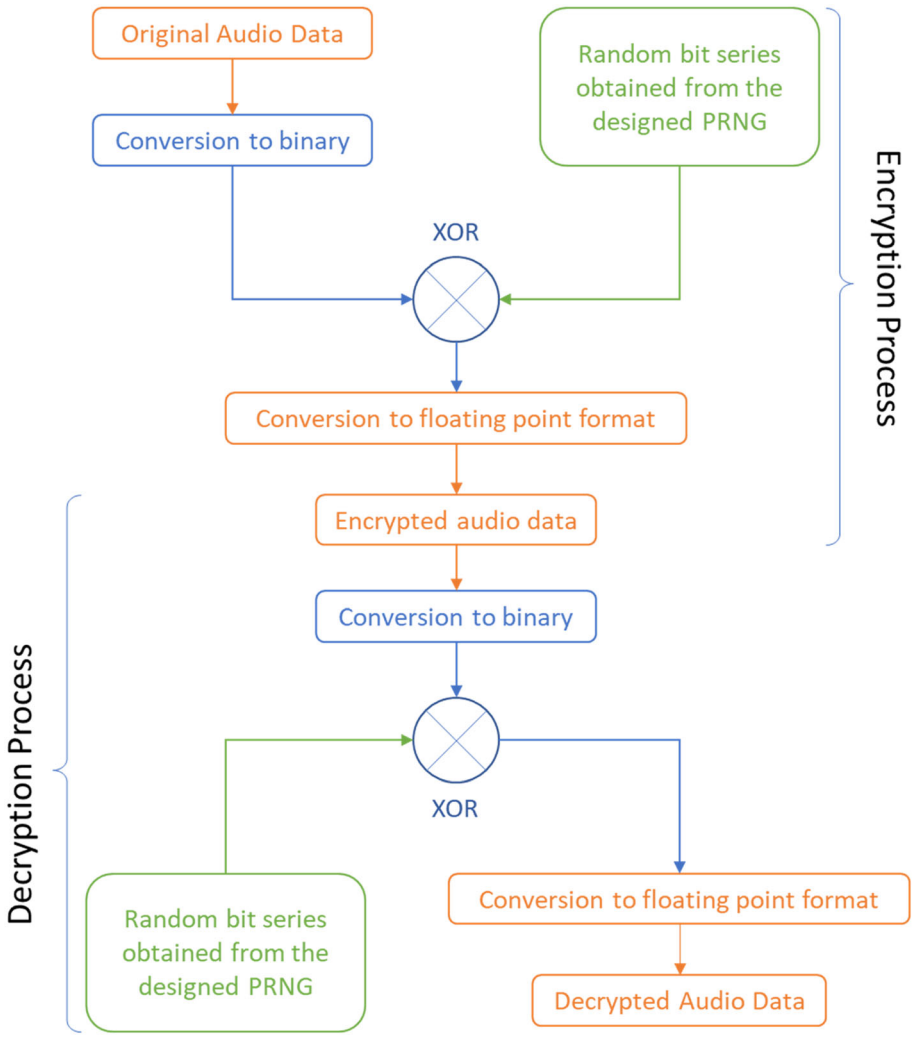

Fig. 12 The block diagram of the audio encryption and decryption processes

obtained from the audio data and the bit series generated from the fractional chaotic system. After XOR operation, the resultant bit series are converted to floating point format to obtain the decrypted audio data in its original waveform.

In the encryption and decryption application, a 1.8-second-long male audio data is used. The waveforms of the original, encrypted, and decrypted audio data are given in Fig. 13. As it is seen in Fig. 13, the waveform of the encrypted audio data is completely different from those of the original and decrypted audio data while the waveforms of the original and decrypted audio data are exactly the same. This is a good indicator that the encryption and the decryption processes are carried out with high accuracy and performance.

For furthermore performance evaluation of the encryption and decryption processes, frequency domain analysis of the original, encrypted, and decrypted audio data is performed by applying the fast Fourier transform (FFT). The frequency spectrum of the original, encrypted, and decrypted audio data is given in Fig. 14. As it is seen in Fig. 14, the spectrum of the encrypted audio data is completely different from the spectrums of the original and decrypted audio data whereas there is no difference in the spectrums of the original and decrypted audio data. Moreover, the spectrum of the encrypted audio data is uniformly distributed across the spectrum. This is another indicator that the encryption and decryption processes have sufficient and acceptable performance.

As a next analysis, bit error rate (BER) calculations are performed with respect to the different fractional order of the system. Different keys are generated by changing the fractional order of the system between 0.9 and 1 with 0.01 step size. The keys are generated as described in Sect. 5.1 for each different fractional order. Then the encrypted bit series of the audio signal is decrypted with the obtained keys. Then BER is calculated by comparing the original data and the decrypted data. BER is calculated by using formula given in (24)

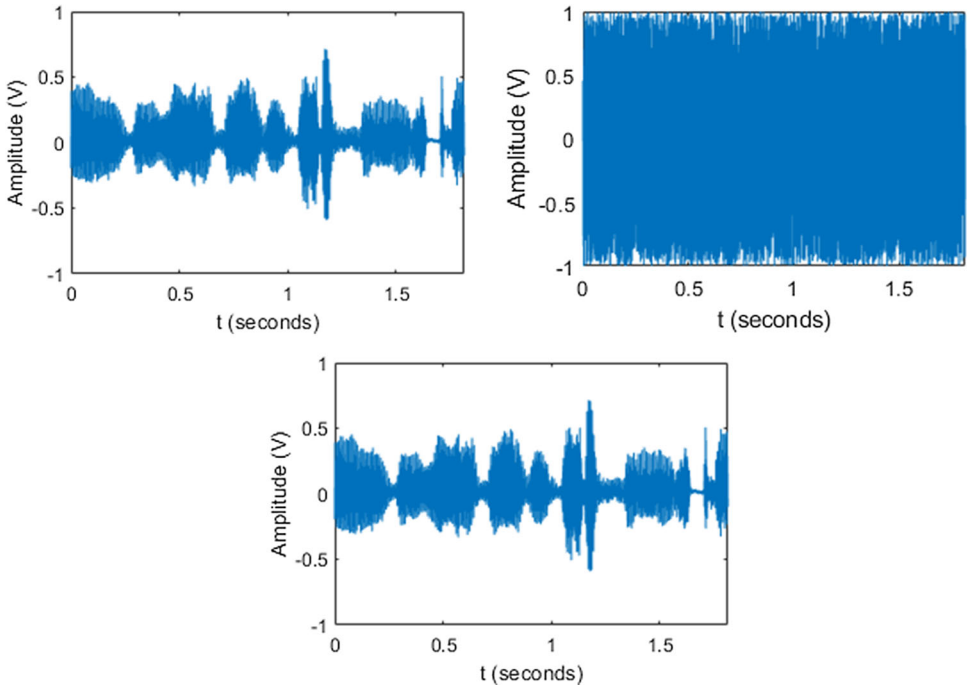

Fig. 13 The waveforms of the original (left), encrypted(right), and decrypted (bottom) audio data

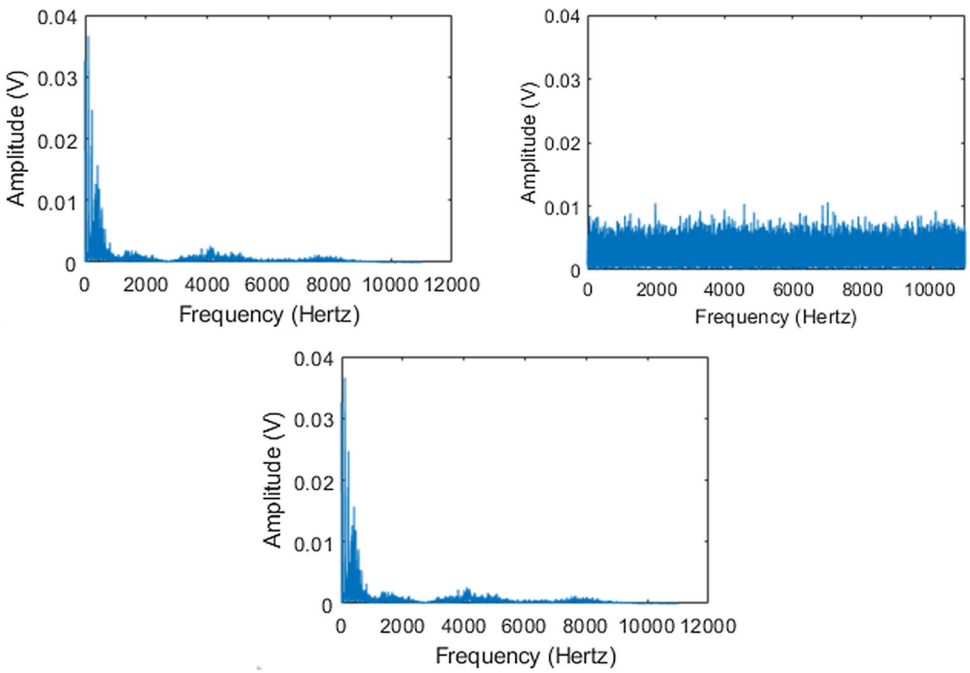

Fig. 14 The frequency spectrum of the original (left), encrypted(right), and decrypted (bottom) audio data

$$\frac{\sum_{i=1}^{L} D_i}{L}, D_i = \begin{cases} 1, & dec_i \neq orig_i \\ 0, & dec_i = orig_i \end{cases} \tag{24}$$

Here dec_i and $orig_i$ is the ith bit of the decrypted and original data respectively, and L is the total number of bits. In the calculations the total number of bits L is selected as 100,000.

The BER results are given in Fig. 15. The BER values are very close to 0.5 as shown in the figure. The lowest obtained BER value is 0.488 while the highest one is 0.511. When the encrypted data is decrypted with the correct keys which are obtained when the fractional order of the chaotic system equals 0.99, the BER results is zero as expected. This indicates that decryption process is successful. However, if the fractional order of the chaotic system is changed for the generation of the keys, the BER results are quite high. This also indicates a very good security performance of the encryption process that even small change in the

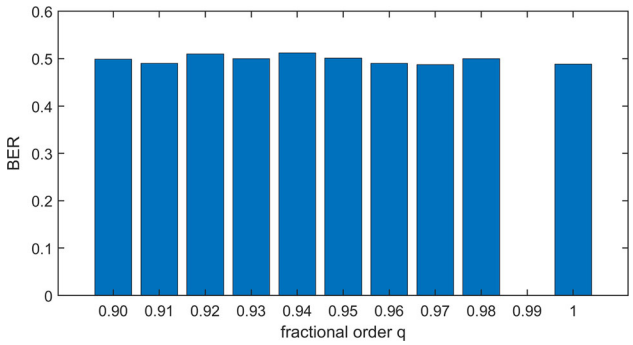

Fig. 15 BER results with respect to decryption keys generated for different fractional order of the chaotic system

Table 2 Entropy and correlation values of original, encrypted, and decrypted audio data

	Entropy	Correlation
Original audio	13.6147	0.9251
Encrypted audio	15.2875	− 0.0019
Decrypted audio	13.6147	0.9251

fractional order causes the decrypted data and original data to be very different.

As a final analysis, entropy and correlation analysis are carried out and their results are given in Table 2 for the original, encrypted, and decrypted audio data. As it is seen in Table 2, the entropy and correlation values of the original and decrypted audio data is the same while the entropy and the correlation values of the encrypted audio data is different than those of the original and decrypted audio data. From all these performed analysis on the original, encrypted, and decrypted audio data, it can be concluded that the use of designed fractional order chaotic system based PRNG is suitable for the data security applications.

6 Conclusion

In this study, a fractional order form of a chaotic system based on two degrees of freedom mechanical system is considered. One of the most important aspect of the paper is that a fractional order chaotic system based on an actual two degrees of freedom nonlinear mechanical system is studied for the first time in the literature. Moreover, the circuit implementation of the fractional order chaotic system is realized. In order to evaluate the accuracy of the circuit realization, the fractional order chaotic system is numerically solved with GL method. The time series and phase portraits obtained from numerical solution and circuit implementation are in good accordance. This shows that the circuit implementation of the fractional order chaotic system is successful. Moreover, a PRNG based on this fractional order chaotic system is designed and an audio encryption application is realized with the designed PRNG. The NIST tests are applied to the designed PRNG to evaluate the randomness of the generated numbers. The designed PRNG passes all the NIST-800-22 statistical tests successfully. This shows the generated numbers have sufficient randomness. Finally, an audio encryption and decryption are performed to show that the fractional order chaotic system can be used engineering applications.

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

1. Wang, L., Mao, X., Wang, A., Wang, Y., Gao, Z., Li, S., & Yan, L. (2020). Scheme of coherent optical chaos communication. *Optics Letters, 45*(17), 4762–4765.
2. Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos based S-Box. *Chaos, Solitons & Fractals, 95*, 92–101.
3. di Bernardo, M., Garefalo, F., Glielmo, L., & Vasca, F. (1998). Switchings, bifurcations, and chaos in DC/DC converters. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 45*(2), 133–141.
4. Pahnehkolaei, S. M. A., Alfi, A., & Machado, J. T. (2020). Fuzzy logic embedding of fractional order sliding mode and state feedback controllers for synchronization of uncertain fractional chaotic systems. *Computational and Applied Mathematics, 39*(3), 1–16.
5. Rajagopal, K., Jahanshahi, H., Jafari, S., Weldegiorgis, R., Karthikeyan, A., & Duraisamy, P. (2021). Coexisting attractors in a fractional order hydro turbine governing system and fuzzy PID based chaos control. *Asian Journal of Control, 23*(2), 894–907.
6. Chen, H., Li, W., & Yang, X. (2020). A whale optimization algorithm with chaos mechanism based on quasi-opposition for global optimization problems. *Expert Systems with Applications, 158*, 113612.
7. Koyuncu, I., Tuna, M., Pehlivan, I., Fidan, C. B., & Alçın, M. (2020). Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator. *Analog Integrated Circuits and Signal Processing, 102*(2), 445–456.
8. Ayubi, P., Setayeshi, S., & Rahmani, A. M. (2020). Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application. *Journal of Information Security and Applications, 52*, 102472.
9. Nguyen, N., Pham-Nguyen, L., Nguyen, M. B., & Kaddoum, G. (2020). A low power circuit design for chaos-key based data encryption. *IEEE Access, 8*, 104432–104444.
10. Long, M., & Tan, L. (2010). A chaos-based data encryption algorithm for image/video. In *2010 Second international conference on multimedia and information technology* (Vol. 1, pp. 172-175), IEEE.
11. Luo, G. W., Zhu, X. F., & Shi, Y. Q. (2015). Dynamics of a two-degree-of freedom periodically-forced system with a rigid stop: Diversity and evolution of periodic-impact motions. *Journal of Sound and Vibration, 334*, 338–362.

12. Chung, K. W., Chan, C. L., & Xu, J. (2003). An efficient method for switching branches of period-doubling bifurcations of strongly non-linear autonomous oscillators with many degrees of freedom. *Journal of Sound and Vibration, 267*(4), 787–808.
13. Chung, K. W., He, Y. B., & Lee, B. H. K. (2009). Bifurcation analysis of a two-degree-of-freedom aeroelastic system with hysteresis structural nonlinearity by a perturbation-incremental method. *Journal of Sound and Vibration, 320*(1–2), 163–183.
14. Borowiec, M., & Litak, G. (2012). Transition to chaos and escape phenomenon in two-degrees-of-freedom oscillator with a kinematic excitation. *Nonlinear Dynamics, 70*(2), 1125–1133.
15. Luo, G. W., Lv, X. H., & Zhu, X. F. (2008). Dynamics of vibro-impact mechanical systems with large dissipation. *International Journal of Mechanical Sciences, 50*(2), 214–232.
16. Kacar, S., Wei, Z., Akgul, A., & Aricioglu, B. (2018). A novel 4D chaotic system based on two degrees of freedom nonlinear mechanical system. *Zeitschrift für Naturforschung A, 73*(7), 595–607.
17. Rukhin, A., Soto, J., Nechvatal, J., Barker, E., Leigh, S., Levenson, M., ... & Iii, L. E. B. (2002). *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22 (revised May 15).
18. Nise, N. S. (2011). *Control system engineering*. New York: Wiley.
19. Podlubny, I. (1998). *Fractional differential equations: An introduction to fractional derivatives, fractional differential equations, to methods of their solution and some of their applications*. Amsterdam: Elsevier.
20. Monje, C. A., Chen, Y., Vinagre, B. M., Xue, D., & Feliu-Batlle, V. (2010). *Fractional-order systems and controls: Fundamentals and applications*. Berlin: Springer.
21. Charef, A., Sun, H. H., Tsao, Y. Y., & Onaral, B. (1992). Fractal system as represented by singularity function. *IEEE Transactions on Automatic Control, 37*(9), 1465–1470.

Burak Aricioglu was born in 1989. He received B.Sc. and M.Sc. degrees in Electrical and Electronics Engineering from Bogazici University in 2011 and 2014, respectively and Ph.D. degree in Electrical & Electronics Engineering from Sakarya University in 2019. He is, currently, an Assistant Professor at Sakarya University of Applied Sciences. His main research interests are nonlinear systems analysis, nonlinear circuit, modelling and simulation, and bioelectromagnetic interactions.