METHODOLOGIES AND APPLICATION

An exponential jerk system, its fractional-order form with dynamical analysis and engineering application

Karthikeyan Rajagopal¹ · Akif Akgul^{[2](http://orcid.org/0000-0001-9151-3052)} · Sajad Jafari³ · Anitha Karthikeyan¹ · Unal Cavusoglu⁴ · Sezgin Kacar²

© Springer-Verlag GmbH Germany, part of Springer Nature 2019

Abstract

A simple jerk system with only one exponential nonlinearity is proposed and discussed. Dynamic analysis of the integer-order jerk system shows the existence of chaotic oscillations. A model for the fractional-order jerk system is derived. The Adomian decomposition method is used to analyse the fractional-order jerk system. Stability analysis of the fractional-order jerk system shows that chaotic oscillations exist in orders less than one and bifurcation analysis shows the range of fractional orders for periodic and chaotic oscillations. To show the randomness of the fractional-order jerk system, a pseudorandom number generator is designed and tested. The NIST-800-22 tests show that the proposed fractional-order jerk system is effective in showing randomness. Finally, an image hiding application to the audio data has been realized by using the developed RNG algorithm. The encrypted image is hidden by being embedded in the audio data, and then, on the receiver side, the data are recovered by taking the image data from the hidden audio file.

Keywords Exponential jerk system (EJS) · Fractional-order chaotic systems · Dynamic analyses · Random number generator (RNG) · Sound steganography

1 Introduction

The construction of nonlinear systems with simple mathematical expressions is still an important research problem. The mathematical complexity of Lorenz system (Loren[z](#page-9-0)

Communicated by V. Loia.

 \boxtimes Akif Akgul aakgul@sakarya.edu.tr; aakgul@subu.edu.tr

Karthikeyan Rajagopal rkarthiekeyan@gmail.com

Sajad Jafari sajadjafari83@gmail.com

Anitha Karthikeyan mrs.anithakarthikeyan@gmail.com

Unal Cavusoglu unalc@sakarya.edu.tr

Sezgin Kacar skacar@sakarya.edu.tr; skacar@subu.edu.tr

- ¹ Centre for Non-Linear Dynamics, Defense University, Bishoftu, Ethiopia
- ² Department of Electrical and Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, Serdivan, Sakarya, Turkey

[1963](#page-9-0)), which is one of the most popular chaotic systems, is still an issue. Rossler introduced his system with only one quadratic nonlinearity (Rössle[r](#page-10-0) [1976](#page-10-0)) and later announced a 3D system with simpler dynamics (Rössle[r](#page-10-1) [1979\)](#page-10-1). Sprott announced chaotic systems with only six terms and one quadratic nonlinearity (Sprot[t](#page-10-2) [1996](#page-10-2)).

Jerk systems include the third derivative of *x*, which is rate of change of acceleration (Scho[t](#page-10-3) [1978;](#page-10-3) Sprot[t](#page-10-4) [1997a,](#page-10-4) [b](#page-10-5)). In different studies, snap systems were considered too (Munmuangsaen and Srisuchinwon[g](#page-9-1) [2011;](#page-9-1) Munmuangsaen et al[.](#page-9-2) [2011](#page-9-2); Sprot[t](#page-10-6) [2011;](#page-10-6) Vaidyanathan et al[.](#page-10-7) [2015](#page-10-7)). Many circuitries for jerk systems were also discussed in the literature. *N* scroll nonlinear systems on a general jerk system were discussed in Yu et al[.](#page-10-8) [\(2005](#page-10-8)), Chunxia et al[.](#page-9-3) [\(2012](#page-9-3)), Srisuchinwong and Nopchind[a](#page-10-9) [\(2013](#page-10-9)). A simple chaotic circuit with hyperbolic sinusoidal nonlinear as discussed in Volos et al[.](#page-9-4)

³ Nonlinear Systems and Applications, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City, Vietnam

⁴ Department of Computer Engineering, Faculty of Computer and Information Sciences, Sakarya University, 54187 Serdivan, Sakarya, Turkey

[\(2017](#page-9-4)) and the different chaotic systems are applied in sound encryption (Akgül et al[.](#page-9-5) [2015\)](#page-9-5).

In the recent studies, the fractional-order systems (FOS) and their applications have been examined (Baleanu et al[.](#page-9-6) [2016;](#page-9-6) Lakshmikantham and Vatsal[a](#page-9-7) [2008;](#page-9-7) Diethel[m](#page-9-8) [2010](#page-9-8)). FOS with different control approaches are considered in Pourmahmood Aghabab[a](#page-9-9) [\(2012](#page-9-9)), Boroujeni and Momen[i](#page-9-10) [\(2012](#page-9-10)), Zhang and Gon[g](#page-10-10) [\(2014](#page-10-10)). Memristor-based FOS without equilibrium are introduced (Rajagopal et al[.](#page-9-11) [2017a,](#page-9-11) [b](#page-9-12), [c,](#page-9-13) [d](#page-10-11); Li and Che[n](#page-9-14) [2013](#page-9-14); Cafagna and Grass[i](#page-9-15) [2015](#page-9-15); Danca et al[.](#page-9-16) [2016\)](#page-9-16). Numerical methods and analyses are proposed, and MATLAB solutions for FOS are discussed in Trzask[a](#page-10-12) [\(2011\)](#page-10-12), Petrá[š](#page-9-17) [\(2006](#page-9-17)), Charef et al[.](#page-9-18) [\(1992](#page-9-18)), Adomia[n](#page-9-19) [\(1990](#page-9-19)), Caponetto and Fazzin[o](#page-9-20) [\(2013\)](#page-9-20), He et al[.](#page-9-21) [\(2015](#page-9-21)), Sun et al[.](#page-10-13) [\(1984\)](#page-10-13), Tavazoei and Haer[i](#page-10-14) [\(2007](#page-10-14)), Shao-Bo et al[.](#page-9-22) [\(2014](#page-9-22)).

Steganography is described as science of writing secret messages unaware of the contents of the confidential message. The data to be transmitted are hidden in a suitable media environment and transmitted in this way. One of the most important points of steganography is that it cannot be determined by statistical methods that data are placed in the data used as a carrier, but it cannot be resolved even if it is detected. Many different methods have been used in steganography procedures (Frit[h](#page-9-23) [2007](#page-9-23); Mahajan and Kau[r](#page-9-24) [2012\)](#page-9-24). When studies in the literature are examined, steganography processes are commonly performed in the form of data hiding on the image (Chang et al[.](#page-9-25) [2006](#page-9-25); Bailey and Curra[n](#page-9-26) [2006;](#page-9-26) Chang and Tsen[g](#page-9-27) [2004;](#page-9-27) Che[n](#page-9-28) [2007](#page-9-28); Du and Hs[u](#page-9-29) [2003](#page-9-29)). Besides the work performed on the image, there are also steganography works on the audio files (Agaian et al[.](#page-9-30) [2005](#page-9-30); Matsuok[a](#page-9-31) [2006](#page-9-31); Pooyan and Delforouz[i](#page-9-32) [2007](#page-9-32); Delforouzi and Pooya[n](#page-9-33) [2007](#page-9-33); Shah et al[.](#page-10-15) [2008](#page-10-15); Sun et al[.](#page-10-16) [2012\)](#page-10-16).

Motivated by the above, in this study a novel jerk system obtained by replacing the hyperbolic sinusoid (Volos et al[.](#page-9-4) [2017\)](#page-9-4) with an exponential nonlinearity is proposed. The fractional-order model of the proposed exponential jerk system is derived, and the dynamic properties of system are analysed. A new RNG algorithm is developed using fractional-order exponential jerk system (FOEJS) chaotic systems, and NIST 800-22 tests are performed. After the RNG design, an algorithm is presented to hide an encrypted picture on the audio file using the random bit sequences from obtained RNG.

2 Exponential jerk system (EJS)

In the study, an exponential jerk system is derived using the system proposed in Volos et al[.](#page-9-4) [\(2017\)](#page-9-4) by replacing the hyperbolic sinusoid with an exponential nonlinearity. The proposed EJS is represented by the dimension model defined as

$$
\begin{aligned}\n\dot{x} &= -y\\ \n\dot{y} &= -z\\ \n\dot{z} &= -x - bz + ae^y\n\end{aligned} \tag{1}
$$

where $a = 0.05$ and $b = 0.7$ with initial values [0, 0.1, 1]. Figure [1](#page-2-0) exhibits the 2D phase portraits of the EJS on different planes.

3 Dynamic properties of the EJS

3.1 Equilibrium points and eigenvalues

The system (1) has an equilibrium point O at $[a, 0, 0]$, and the eigenvalues of the system at *O* are $\lambda_1 = -1.276$, $\lambda_{2,3} =$ $0.2877 \pm 0.8374i$ with $\lambda_{2,3}$ as the saddle point of index 2. The characteristic equation of the EJS at *O* is $\lambda^3 + b\lambda^2 + a\lambda + 1$. The principal minors are

$$
\Delta_1 = \delta_1 > 0, \quad \Delta_2 = \begin{vmatrix} \delta_1 & \delta_0 \\ \delta_3 & \delta_2 \end{vmatrix} > 0, \quad \Delta_3 \Longrightarrow \begin{vmatrix} \delta_1 & \delta_0 & 0 \\ \delta_3 & \delta_2 & \delta_1 \\ 0 & 0 & \delta_3 \end{vmatrix} > 0 \tag{2}
$$

where $\delta_0 = 1, \delta_1 = b, \delta_2 = a, \delta_3 = 1$. For $a = 0.05, b =$ 0.7 and equilibrium point *O*, the values of Δ_2 < 0, and hence, the EJS is unstable and shows chaotic behaviour.

3.2 Dissipativity

The system [\(3\)](#page-1-1) is define in vector notation as

$$
\dot{X} = f(X) = \begin{bmatrix} f_1(x, y, z) \\ f_2(x, y, z) \\ f_2(x, y, z) \end{bmatrix}
$$
 (3)

where

$$
\begin{cases}\nf_1(x, y, z) = -y \\
f_2(x, y, z) = -z \\
f_3(x, y, z) = -x - bz + ae^y\n\end{cases}
$$
\n(4)

 $\Phi(t) = \Phi_t(\Omega)$, where Φ_t is the flow of the vector field f. Also, $V(t)$ represents the hyper volume of $\Phi(t)$.

By Liouville's theorem,

$$
\dot{V} = \int_{\Phi(t)} (\nabla \cdot f) \, \mathrm{d}x \, \mathrm{d}y \, \mathrm{d}z \tag{5}
$$

Fig. 1 2D phase portraits of the EJS: $\mathbf{a} \times \mathbf{z} = z$; $\mathbf{b} \times \mathbf{y} = z$

where *f* is the divergence and it is easily calculated as

$$
\nabla \cdot f = \frac{\partial f_1}{\partial x} + \frac{\partial f_2}{\partial y} + \frac{\partial f_3}{\partial z} = -b \le 0
$$
 (6)

As $b > 0$, the EJS [\(1\)](#page-1-0) is dissipative.

3.3 Lyapunov exponents (LEs) and Kaplan–Yorke dimension (KYD)

LEs of a chaotic system give the convergence and divergence of the states (Li et al[.](#page-9-34) [2010;](#page-9-34) Wolf et al[.](#page-10-17) [1985](#page-10-17); Ellner et al[.](#page-9-35) [1991;](#page-9-35) Maus and Sprot[t](#page-9-36) [2013;](#page-9-36) Tavazoei and Haer[i](#page-10-14) [2007](#page-10-14)). A definition of LEs for FOS was shown in Li et al[.](#page-9-34) [\(2010\)](#page-9-34). LE calculation methods as time series based (Wolf et al[.](#page-10-17) [1985\)](#page-10-17) and Jacobian method (Ellner et al[.](#page-9-35) [1991\)](#page-9-35) are commonly used to obtain LEs for integer and FOS. The LEs of EJS system are $L_1 = 0.1156$, $L_2 = 0$, $L_3 = -0.8148$, and the KYD is 2.142.

4 Fractional-order exponential jerk system (FOEJS)

In this part, we show the FO model of the nonlinear system. There are three differential operators, viz. Riemann– Liouville [\(7\)](#page-2-1), Grunwald–Letnikov [\(8\)](#page-2-1) and Caputo [\(9\)](#page-2-1) (Baleanu et al[.](#page-9-6) [2016](#page-9-6); Lakshmikantham and Vatsal[a](#page-9-7) [2008;](#page-9-7) Diethel[m](#page-9-8) [2010\)](#page-9-8), as defined by

$$
{}_aD_t^q[x(t)] = \frac{1}{\Gamma(n-q)} \left(\frac{d^n}{dt^n} \int\limits_a^t \frac{x(\tau)}{(t-\tau)^{1-(n-q)}} d\tau \right) \tag{7}
$$

$$
{}_aD_t^q[x(t)] = \lim_{h \to 0} \frac{1}{\Gamma(q)h^q} \sum_{k=0}^{\lceil t - \frac{a}{h} \rceil} \frac{\Gamma(q+k)}{\Gamma(k+1)} x(t - kh) \tag{8}
$$

$$
{}_aD_t^q[x(t)] = \frac{1}{\Gamma(q-n)} \left(\int_a^t \frac{x(\tau)}{(t-\tau)^{q-n+1}} d\tau \right) \tag{9}
$$

where $\Gamma(\bullet)$ is the gamma function. We adopt the Caputo derivative method (Trzask[a](#page-10-12) [2011](#page-10-12)) for the fractional-order exponential jerk system given by

$$
D^{q_x} x = -y
$$

\n
$$
D^{q_y} y = -z
$$

\n
$$
D^{q_z} z = -x - bz + ae^y
$$
\n(10)

To find the numerical solutions of the FOEJS (10) , we use the Adomian decomposition method (Adomia[n](#page-9-19) [1990](#page-9-19); Caponetto and Fazzin[o](#page-9-20) [2013;](#page-9-20) He et al[.](#page-9-21) [2015](#page-9-21)). The general form of a FOS can be written as

$$
D_t^q x(t) = Lx(t) + Nx(t) + g(t)
$$
\n(11)

where $Lx(t)$ represents the linear term, $Nx(t)$ represents the nonlinear term and $g(t)$ represents the constants of the FOS. Using (11) , the FOEJS (10) can be written as

$$
\begin{bmatrix} L_{x(t)} \\ L_{y(t)} \\ L_{z(t)} \end{bmatrix} = \begin{bmatrix} -y \\ -z \\ -x - bz \end{bmatrix},
$$

$$
\begin{bmatrix} N_{x(t)} \\ N_{y(t)} \\ N_{z(t)} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ ae^y \end{bmatrix},
$$

$$
\begin{bmatrix} g_{x(t)} \\ g_{y(t)} \\ g_{z(t)} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}
$$
 (12)

Using the ADM, the discrete iterative mathematical model of the FOEJS is given by

$$
x(n + 1) = \sum_{j=0}^{6} A_1^j \frac{h^{jq}}{\Gamma(jq + 1)}
$$

$$
y(n + 1) = \sum_{j=0}^{6} A_2^j \frac{h^{jq}}{\Gamma(jq + 1)}
$$

$$
z(n + 1) = \sum_{j=0}^{6} A_3^j \frac{h^{jq}}{\Gamma(jq + 1)}
$$
 (13)

The initial conditions are taken as $A_1^0 = x_n$, $A_2^0 =$ y_n , $A_3^0 = z_n$. The Adomian polynomials can be obtained as $A_1^{j+1} = -A_2^j$; $A_2^{j+1} = -A_3^j$, and the first six Adomian polynomials for the nonlinear term (e^y) can be derived as

$$
A_3^1 = -A_1^0 - bA_3^0 + ae^{A_2^0}
$$

\n
$$
A_3^2 = -A_1^1 - bA_3^1 + aA_2^1e^{A_2^0}
$$

\n
$$
A_3^3 = -A_1^2 - bA_3^2
$$

\n
$$
+ a \left[e^{A_2^0} \left(A_2^2 + \frac{1}{2} \left(A_2^1 \right)^2 \right) \right] \frac{\Gamma(2q+1)}{\Gamma^2(q+1)}
$$

\n
$$
A_3^4 = -A_1^3 - bA_3^3
$$

\n
$$
+ a \left[e^{A_2^0} \left(A_2^3 + \frac{1}{6} \left(A_2^1 \right)^3 A_2^1 A_2^2 \right) \right]
$$

\n
$$
\frac{\Gamma(3q+1)}{\Gamma(q+1)\Gamma(2q+1)}
$$

\n
$$
A_3^5 = -A_1^4 - bA_3^4
$$

\n
$$
+ a \left[e^{A_2^0} \left(A_2^1 A_2^3 + \frac{1}{2^4} \left(A_2^1 \right)^4 + \frac{1}{2} \left(A_2^1 \right)^2 A_2^2 + A_2^4 \right) \right]
$$

\n
$$
\frac{\Gamma(4q+1)}{\Gamma(q+1)\Gamma(3q+1)}
$$

\n
$$
A_3^6 = -A_1^5 - bA_3^5
$$

\n
$$
+ a \left[e^{A_2^0} \left(A_2^5 + \frac{1}{2} A_2^1 \left(A_2^2 \right)^2 + \frac{1}{2} \left(A_2^1 \right)^2 A_2^3 \right) \right]
$$

\n
$$
\frac{\Gamma(5q+1)}{\Gamma(q+1)\Gamma(4q+1)}
$$

\n
$$
(14)
$$

where $h = t_{n+1} - t_n$ [.](#page-9-21) The discrete Adomian form (He et al. [2015\)](#page-9-21) of the FOEJS can be given as

$$
\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} A_1^0 A_1^1 A_1^2 A_1^3 A_1^4 A_1^5 A_1^6 \\ A_2^0 A_2^1 A_2^2 A_2^3 A_2^4 A_2^5 A_2^6 \\ A_3^0 A_3^1 A_3^2 A_3^3 A_3^4 A_3^5 A_3^6 \end{bmatrix}
$$

$$
\times \begin{bmatrix} 1 \frac{h^q}{\Gamma(q+1)} \frac{h^{2q}}{\Gamma(2q+1)} \frac{h^{3q}}{\Gamma(3q+1)} \frac{h^{4q}}{\Gamma(4q+1)} \frac{h^{5q}}{\Gamma(5q+1)} \frac{h^{6q}}{\Gamma(6q+1)} \end{bmatrix}^{\mathrm{T}}_{(15)}
$$

Using Eqs. (13) and (14) , the FOEJS is solved numerically. Figure [2](#page-4-0) shows the 2D phase planes of the FOEJS system with $h = 0.001$, $q = 0.99$ and initial values [0, 0.1, 1].

5 Dynamic analysis of the FOEJS

In this section, the dynamic analysis of the FOEJS is introduced. The equilibrium point *O* of the FOEJS system is the same like the integer order at [*a*, 0, 0].

For commensurate FOEJS of order *q*, the system is stable. It exhibits chaotic behaviour if $|\arg(eig(J_O))| = |\arg(\lambda_i)|$ $\frac{q\pi}{2}$. The EJS system has one equilibrium at [*a*, 0, 0] and the characteristic equation $q = 0.99$ for the equilibrium point *O* is given by $\lambda^{297} + 3\lambda^{199} + 0.7\lambda^{198} + 3\lambda^{101} + 3\lambda^{101} +$ $1.4\lambda^{100} + 0.05\lambda^{99} + \lambda^3 + 0.7\lambda^2 + 0.05\lambda + 1.$

The required condition for the FOEJS to show chaotic behaviour in the incommensurate case is $\frac{\pi}{2M}$ – min_i $(|arg(\lambda i)|) > 0$. If $q_x = 0.99$, $q_y = 0.98$, $q_z = 0.97$, then $M = 100$. At the equilibriums are det(diag[$\lambda^{Mq_x}, \lambda^{Mq_y}$, λ^{Mq_z}] – *J*_O $)$ = 0 and the FO det(diag[λ^{99} , λ^{98} , λ^{97}] – *J*_O $)$ = 0, and the characteristic equation at equilibrium point *O* is $\lambda^{294} + \lambda^{198} + 1.7\lambda^{197} + \lambda^{196} + \lambda^{101} + 1.7\lambda^{100} + 1.75\lambda^{99} + \lambda^{3} +$ $0.7\lambda^2+0.05\lambda+1$. The minimum argument of the roots of the characteristic equation is 0.0112, and the required stability condition is $\frac{\pi}{200} - 0.0112 > 0$ which solves for $0.0045 > 0$, and thus, the incommensurate FOEJS shows a chaotic attractor similar to the integer-order EJS.

5.1 Lyapunov exponents

The LEs of the FOEJS are obtained with the ADM method with QR decomposition (Caponetto and Fazzin[o](#page-9-20) [2013](#page-9-20)). For the fractional-order $q = 0.99$, the LEs of the FOEJS system are $L_1 = 0.1227, L_2 = 0, L_3 = -0.9214.$

5.2 Bifurcation

To investigate the importance of the parameters *a*, *b* on the FOEJS, the bifurcation diagrams are examined. First, the values of *b* and *q* are kept constant ($b = 0.7$, $q = 0.99$) and the value of a is varied between $[0, 0.2]$ with a very small range. In Fig. [3a](#page-4-1), the bifurcation diagram of FOEJS with respect to the parameter *a* is shown. The FOEJS exhibits chaotic behaviour for region $0 < a < 0.15$. Figure [3b](#page-4-1) shows the variation in maximum Lyapunov exponent (MLE) with

Fig. 2 2D phase planes of the FOEJS for commensurate fractional-order $q = 0.99$: **a** $x - z$; **b** $y - z$

Fig. 3 a Bifurcation diagram of FOEJS for *a*; **b** MLE for change in *a*

respect to the parameter *a*. Similarly, bifurcation plots and MLE for parameter *b* are derived and presented in Fig. [4a](#page-5-0), b. Both the bifurcation plots confirm that the FOEJS system exits chaotic regime with inverse period doubling, and additionally, the bifurcation of parameter *b* shows that the FOEJS system enters to chaos.

Another important bifurcation of interest when discussing about a FOS is the bifurcation plots with FO. In Fig. [5a](#page-5-1), the bifurcation diagrams of the FOEJS and in Fig. [5b](#page-5-1) the MLE for the FOEJS are given. The system shows positive LE when the FO $q > 0.935$ and has a small band of periodic state when the MLE is zero for $0.975 < b < 0.978$. The most dominant

MLE (0.1227) of the FOEJS system is seen for the order $0.99 < q < 0.994$.

6 Fractional-order-based RNG

In this part, a RNG has been developed using a new fractionalorder exponential jerk system (FOEJS) that is introduced in the article. The pseudocode of RNG algorithm is shown in Algorithm 1. In the RNG algorithm, the necessary system values are entered in first. The appropriate step value used by the system for sampling is determined. Unlike other chaos

 0.14

 0.12

 0.1

 0.08

 0.06

 0.04

 0.02

 $\sqrt{2}$

 -0.02

 0.4

 0.6

 0.8

Fig. 4 a Bifurcation diagram of FOEJS for *b*; **b** MLE for change in *b*

Fig. 5 a Bifurcation plot of FOEJS for *q*; **b** MLE for change in *q*

based on RNGs, orders of derivates values are determined and binomial coefficients are calculated. Fractional-order (*q*1, *q*2, *q*3) values are used as 0.99. The memo function used in the algorithm is used to solve the system and to obtain the values using the calculated binomial coefficients. The Grunwald–Letnikov approach is used (Trzask[a](#page-10-12) [2011](#page-10-12); Kilbas et al[.](#page-9-37) [2006\)](#page-9-37) for the numerical analysis of FOEJS. In this approach, the values that the memory function produces are subtracted from the values obtained by the analysis of the system. The float values obtained from the state variables are converted into a 32-bit binary sequence. The 5 bits of precision value are taken from the 32-bit array and added to the 1 Mbit random numbers of the each phase. NIST 800-22 tests are performed in order to evaluate the randomness levels of the bit sequences. Bit sequences must pass all NIST tests in order to have sufficient randomness.

The NIST 800-22 test [\(http://csrc.nist.gov/publications/](http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf) [nistpubs/800-22/sp-800-22-051501.pdf\)](http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf) is an internationally accepted test for the testing of random numbers. To show that the number sequence has enough randomness, it has to pass all the tests. Table [1](#page-7-0) gives the results of the NIST 800-22

 1.2

a

 (b)

 1.4

 1.6

 1.8

 $\overline{2}$

Fig. 7 Block diagram of steganography application

Table 1 NIST-800-22 test results

Algorithm 1 RNG Algorithm Pseudocode

1: Start

- 2: Entering system parameters (*a*, *b*)
- 3: Initial condition of chaotic systems (x_0, y_0, z_0)
- 4: Determination of the orders of derivatives (*q*1, *q*2, *q*3)
- 5: Determination of the appropriate value of (Δh)
- 6: Binomial coefficients calculation (*c*1, *c*2, *c*3)
- 7: $rngx = []$; $rngy = []$; $rngz = []$;
- 8: *memo* → (*memor y f unction*)
- 9: **for** $i = 2$: 1000000 **do**
10: $x(i) = -y(i-1) *$
- 10: $x(i) = -y(i 1) * h^{q} \text{memo}(x, c_1, i);$
11: $y(i) = -z(i 1) * h^{q} \text{memo}(y, c_2, i);$
- 11: $y(i) = -z(i 1) * h^{q2} \text{memo}(y, c2, i);$
12: $z(i) = (-x(i) b * z(i 1) + a * e)$ $z(i) = (-x(i) - b * z(i - 1) + a * exp(y(i))) * h^{q3}$
- $memo(z, c3, i);$
- 13: Convert float to binary array (32 bit) for each phase (x, y, z)
- 14: $rngx + [x(LSB 5bit)]$
15: $rngy + [y(LSB 5bit)]$
- 15: $rngy+=[y(LSB-5bit)]$
16: $rngz+=[z(LSB-5bit)]$
- $rngz+=[z(LSB-5bit)]$
- 17: **end for**
- 18: The Implementation of NIST Tests to 1 M. bit for each phase (*rngx*,*rngy*,*rngz*) 19: End

tests that are performed on the bit sequence obtained with the RNG algorithm. As shown in Table [1,](#page-7-0) it can be seen that all the numbers pass all the tests. As a result, it can be said that the RNG algorithm produces enough randomness.

7 Fractional-order-based sound steganography application

In this section, the image hiding application to the audio file has been realized by using the developed RNG algorithm. The encrypted picture shown in Fig. [6b](#page-6-0) is obtained by encrypting the original ['logo.bmp'](http://logo.bmp) image file shown in Fig. [6a](#page-6-0). The encrypted image is hidden by being embedded in the audio file. Then, on the receiver side, the data are resolved by taking the image data from the hidden audio file. Figure [6c](#page-6-0) shows the resolved image file.

Figure [7](#page-6-1) gives the block diagram of the steganography application. FOEJS based on RNG is used for random number generation in the steganography algorithm.

The working principle of the algorithm is explained in the following items.

- The related files (image and sound) are read and transferred to the relevant variables.
- The image file is converted to a binary system for bitbased encryption.
- The float values provided from the each phase of the PRNG are converted to the binary system.
- A binary sequence is obtained by bit selection from each phase, and this sequence is converted to a decimal value. *x* = [0101101]*y* = [1010111]*z* = [0111100]
- *bin*2*dec*(010110110101110111100) = 748,476
- The obtained decimal value is done mode operation with the size value of the sound file string to determine the location of the sound file where a bit in the encrypted image file will be inserted.

mod(*bin*2*dec*([010110110101110111100]),*length* (*trans*))

 $mod(748, 476, 661, 501) = 86,975$

• In this way, a decimal array with singular values is obtained in image file bit size.

array = [86,975, 5362,, 78,210]

Fig. 8 Original and embedded audio file, **a** original sound file, **b** embedded sound file

Fig. 9 Histogram results, **a** original sound file, **b** embedded sound file

 $enc - img = bitxor(img_{h}in, rngx, rngy, rngz)$

- The audio file is converted to binary form. $temp = flt2bin(trains(array(i));$
- Each bit of the image file is placed in the 32nd bit of the audio file in the binary format, using the random bit values generated by the RNG and the random values generated by the mode operation. In this way, the entire image file is completely randomly embedded in the audio file in an encrypted form.

 $temp(32) = enc - img(i)$

- Embedded sound file is obtained.
- To extract the embedded image in the audio file, the original image is extracted from the audio file by performing the reverse of the steps described above.

The sound file obtained after the encryption process is shown in Fig. [8b](#page-8-0), and the original sound file is shown in

Fig. [8a](#page-8-0). When the original and buried sound file is examined, it appears that there is no difference between the original sound file and the sound file embedded in the image file. In Fig. [9,](#page-8-1) the histogram diagrams of embedded and original audio files are shown. When the histogram graphs are examined, it is seen that there is no change in the histogram after data embedding. As a result, it has been determined that there is no appreciable change in the audio file with the embedding process. The steganography process has been successfully accomplished.

8 Conclusions

In the study, a novel exponential jerk system with its fractional-order form is proposed and discussed. Dynamic analysis is examined for both integer- and fractional-order cases. ADM is employed to numerically analyse the fractional-

order jerk system. A PRNG is designed with the fractionalorder jerk system, and NIST-800-22 test results confirm that the RNG is efficient in randomness. An image encryption application is developed with the RNG algorithm, and the encrypted image is embedded to a audio file. In the receiver side, the encrypted image is obtained and decrypted with the fractional-order RNG to recover the original image.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

- Adomian G (1990) A review of the decomposition method and some recent results for nonlinear equations. Math Comput Modell 13(7):17–43
- Agaian SS, Akopian D, Caglayan O, D'Souza SA (2005) Lossless adaptive digital audio steganography. In: Conference record of the thirty-ninth asilomar conference on signals, systems and computers 2005. IEEE, pp 903–906
- Akgül A, Kaçar S, Pehlivan İ (2015) An audio data encryption with single and double dimension discrete-time chaotic systems. TOJSAT 5(3):14–23
- Bailey K, Curran K (2006) An evaluation of image based steganography methods. Multimed Tools Appl 30(1):55–88
- Baleanu D, Diethelm K, Scalas E, Trujillo JJ (2016) Fractional calculus: models and numerical methods, vol 5. World Scientific, Singapore
- Boroujeni EA, Momeni HR (2012) Non-fragile nonlinear fractional order observer design for a class of nonlinear fractional order systems. Signal Process 92(10):2365–2370
- Cafagna D, Grassi G (2015) Fractional-order systems without equilibria: the first example of hyperchaos and its application to synchronization. Chin Phys B 24(8):080502
- Caponetto R, Fazzino S (2013) An application of Adomian decomposition for analysis of fractional-order chaotic systems. Int J Bifurc Chaos 23(03):1350050
- Chang C-C, Tseng H-W (2004) A steganographic method for digital images using side match. Pattern Recognit Lett 25(12):1431–1437
- Chang C-C, Lin C-Y, Wang Y-Z (2006) New image steganographic methods using run-length approach. Inf Sci 176(22):3393–3408
- Charef A, Sun HH, Tsao YY, Onaral B (1992) Fractal system as represented by singularity function. IEEE Trans Autom Control 37(9):1465–1470
- Chen W-Y (2007) Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation. Appl Math Comput 185(1):432–448
- Christos V, Akif A, Viet-Thanh P, Ioannis S, Ioannis K (2017) A simple chaotic circuit with a hyperbolic sine function and its use in a sound encryption scheme. Nonlinear Dyn 89:1–15
- Chunxia L, Jie Y, Xiangchun X, Limin A, Yan Q, Yongqing F (2012) Research on the multi-scroll chaos generation based on jerk mode. Procedia Eng 29:957–961
- Danca M-F, Tang WKS, Chen G (2016) Suppressing chaos in a simplest autonomous memristor-based circuit of fractional order by periodic impulses. Chaos Solitons Fractals 84:31–40
- Delforouzi A, Pooyan M (2007) Adaptive digital audio steganography based on integer wavelet transform. In: Third international conference on intelligent information hiding and multimedia signal processing 2007, IIHMSP 2007, vol 2. IEEE, pp 283–286
- Diethelm K (2010) The analysis of fractional differential equations: an application-oriented exposition using differential operators of Caputo type. Springer, Berlin
- DuW-C, HsuW-J (2003) Adaptive data hiding based on VQ compressed images. IEE Proc Vis Image Signal Process 150(4):233–238
- Ellner S, Gallant AR, McCaffrey D, Nychka D (1991) Convergence rates and data requirements for jacobian-based estimates of Lyapunov exponents from data. Phys Lett A 153(6–7):357–363
- Frith D (2007) Steganography approaches, options, and implications. Netw Secur 2007(8):4–7
- He S-B, Sun K-H, Wang H-H (2014) Solution of the fractional-order chaotic system based on adomian decomposition algorithm and its complexity analysis
- He S, Sun K, Wang H (2015) Complexity analysis and dsp implementation of the fractional-order Lorenz hyperchaotic system. Entropy 17(12):8299–8311
- Kilbas AAA, Srivastava HM, Trujillo JJ (2006) Theory and applications of fractional differential equations, vol 204. Elsevier Science Limited
- Lakshmikantham V, Vatsala AS (2008) Basic theory of fractional differential equations. Nonlinear Anal Theory Methods Appl 69(8):2677–2682
- Li RH, Chen WS (2013) Fractional order systems without equilibria. Chin Phys B 22:040503
- Li C, Gong Z, Qian D, Chen YQ (2010) On the bound of the Lyapunov exponents for the fractional differential systems. Chaos Interdiscip J Nonlinear Sci 20(1):013127
- Lorenz EN (1963) Deterministic nonperiodic flow. J Atmos Sci 20(2):130–141
- Mahajan M, Kaur N (2012) Adaptive steganography: a survey of recent statistical aware steganography techniques. Int J Comput Netw Inf Secur 4(10):76
- Matsuoka H (2006) Spread spectrum audio steganography using subband phase shifting. In: International conference on intelligent information hiding and multimedia signal processing 2006, IIH-MSP'06. IEEE, pp 3–6
- Maus A, Sprott JC (2013) Evaluating Lyapunov exponent spectra with neural networks. Chaos Solitons Fractals 51:13–21
- Munmuangsaen B, Srisuchinwong B (2011) Elementary chaotic snap flows. Chaos Solitons Fractals 44(11):995–1003
- Munmuangsaen B, Srisuchinwong B, Sprott JC (2011) Generalization of the simplest autonomous chaotic system. Phys Lett A 375(12):1445–1450
- National institute of standards and 2001 tech., NIST-800-22. A statistical test suite for random and pseudo rngs for cryptographic applications. [http://csrc.nist.gov/publications/nistpubs/](http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf) [800-22/sp-800-22-051501.pdf](http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf)
- Petráš I (2006) Method for simulation of the fractional order chaotic systems. Acta Montan Slovaca 11(4):273–277
- PooyanM, Delforouzi A (2007) Lsb-based audio steganography method based on lifting wavelet transform. In: IEEE international symposium on signal processing and information technology 2007. IEEE, pp 600–603
- Pourmahmood Aghababa M (2012) Robust finite-time stabilization of fractional-order chaotic systems based on fractional Lyapunov stability theory. J Comput Nonlinear Dyn 7(2):021010
- Rajagopal K, Karthikeyan A, Duraisamy P (2017a) Hyperchaotic chameleon: fractional order FPGA implementation. Complexity. <https://doi.org/10.1155/2017/8979408>
- Rajagopal K, Karthikeyan A, Srinivasan AK (2017b) FPGA implementation of novel fractional-order chaotic systems with two equilibriums and no equilibrium and its adaptive sliding mode synchronization. Nonlinear Dyn 87(4):2281–2304
- Rajagopal K, Guessas L, Karthikeyan A, Srinivasan A, Adam G (2017c) Fractional order memristor no equilibrium chaotic system with its adaptive sliding mode synchronization and genetically optimized

fractional order pid synchronization. Complexity. [https://doi.org/](https://doi.org/10.1155/2017/1892618) [10.1155/2017/1892618](https://doi.org/10.1155/2017/1892618)

- Rajagopal K, Guessas L, Vaidyanathan S, Karthikeyan A, Srinivasan A (2017d) Dynamical analysis and fpga implementation of a novel hyperchaotic system and its synchronization using adaptive sliding mode control and genetically optimized pid control. Math Prob Eng. <https://doi.org/10.1155/2017/7307452>
- Rössler OE (1976) An equation for continuous chaos. Phys Lett A 57(5):397–398
- Rössler OE (1979) Continuous chaos—four prototype equations. Ann N Y Acad Sci 316(1):376–392
- Schot SH (1978) Jerk: the time rate of change of acceleration. Am J Phys 46(11):1090–1094
- Shah P, Choudhari P, Sivaraman S (2008) Adaptive wavelet packet based audio steganography using data history. In: IEEE region 10 and the third international conference on industrial and information systems 2008, ICIIS 2008. IEEE, pp 1–5
- Sprott JC (1996) Some simple chaotic flows. Phys Rev E 50(2):R647
- Sprott JC (1997a) Some simple chaotic jerk functions. Am J Phys 65(6):537–543
- Sprott JC (1997b) Simplest dissipative chaotic flow. Phys Lett A 228(4– 5):271–274
- Sprott JC (2011) A new chaotic jerk circuit. IEEE Trans Circuits Syst II Express Briefs 58(4):240–243
- Srisuchinwong B, Nopchinda D (2013) Current-tunable chaotic jerk oscillator. Electron Lett 49(9):587–589
- Sun HH, Abdelwahab A, Onaral B (1984) Linear approximation of transfer function with a pole of fractional power. IEEE Trans Autom Control 29(5):441–444
- Sun W, Shen R-J, Yu F-X, Lu Z-M (2012) Data hiding in audio based on audio-to-image wavelet transform and vector quantization. In: Eighth international conference on intelligent information hiding and multimedia signal processing (IIH-MSP) 2012. IEEE, pp 313– 316
- Tavazoei MS, Haeri M (2007) Unreliability of frequency-domain approximation in recognising chaos in fractional-order systems. IET Signal Process 1(4):171–181
- Trzaska Z (2011) Matlab solutions of chaotic fractional order circuits. In: Assi A (ed) Engineering education and research using MAT-LAB, chapter 19. Intech, Rijeka
- Vaidyanathan S, Volos C, Pham V-T, Madhavan K (2015) Analysis, adaptive control and synchronization of a novel 4-D hyperchaotic hyperjerk system and its spice implementation. Arch Control Sci 25(1):135–158
- Wolf A, Swift JB, Swinney HL, Vastano JA (1985) Determining Lyapunov exponents from a time series. Phys D 16(3):285–317
- Yu S, Lu J, Leung H, Chen G (2005) Design and implementation of *n*-scroll chaotic attractors from a general jerk circuit. IEEE Trans Circuits Syst I Regul Pap 52(7):1459–1476
- Zhang R, Gong J (2014) Synchronization of the fractional-order chaotic system via adaptive observer. Syst Sci Control Eng Open Access J 2(1):751–754

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.