IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 July 2023, accepted 24 July 2023, date of publication 26 July 2023, date of current version 2 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3299171

RESEARCH ARTICLE

Multistability and Bifurcation Analysis of a Novel 3D Jerk System: Electronic Circuit Design, FPGA Implementation, and Image Cryptography Scheme

TALAL BONNY[1], SUNDARAPANDIAN VAIDYANATHAN[2], ACENG SAMBAS[3,4], KHALED BENKOUIDER[5], WAFAA AL NASSAN[1], AND OMAR NAQAWEH[1]

[1]Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates
[2]Centre for Control Systems, Vel Tech University, Chennai, Tamil Nadu 600 062, India
[3]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Gong Badak, Terengganu 21300, Malaysia
[4]Department of Mechanical Engineering, Universitas Muhammadiyah Tasikmalaya, Tasikmalaya, Jawa Barat 46196, Indonesia
[5]Non Destructive Testing Laboratory, Automatic Department, Jijel University, Jijel 18000, Algeria

Corresponding author: Talal Bonny (tbonny@sharjah.ac.ae)

ABSTRACT In this paper, we propose a novel 3-D jerk system with three quadratic nonlinear terms and demonstrate the dynamical properties of the proposed jerk system in terms of phase portraits, bifurcation diagrams, Lyapunov exponents, multistability and coexisting attractors. For practical implementations, we apply Multisim version 14.0 to design an electronic model of the proposed 3-D jerk system. To demonstrate the feasibility of the proposed chaotic jerk system, we implement the system using a field-programmable gate array (FPGA), which shows high throughput and low power consumption. Furthermore, a new image encryption scheme based on the proposed jerk system is developed, which involves permutation and diffusion operations. Experimental results and security analysis show the effectiveness of our proposed algorithm in terms of high security and excellent encryption performance.

INDEX TERMS Chaotic systems, jerk system, FPGA, image encryption, security analysis.

I. INTRODUCTION

Chaotic systems have been a trending topic for scientists and researchers for decades. The study of such systems is motivated by their complex dynamics and behavior, which are determined by their initial conditions and parameter changes. In recent years, chaotic systems have gained significant attention in various fields, such as control engineering, computer science, information technology, and beyond. This is because chaotic systems have a wide range of applications such as data encryption, secure communication (see [1], [2]), image encryption (see [3], [4]), speech transmission [5], quantum chaos [6], [7], FPGA [8], [9], [10], robotics [11], energy harvesting (see [12], [13]), etc.

Bifurcation analysis is carried out for nonlinear dynamical systems to understand the changes in the qualitative behavior of the systems with respect to changes in the system parameters (see [14], [15], [16]). Electronic circuit designs of the chaotic dynamic systems aid in the practical applications of the systems (see [17], [18], [19]).

There has been a growing interest in using chaotic systems for secure communication and encryption. Chaotic systems, with their complex dynamics, sensitivity to initial conditions, and deterministic nature, provide inherent randomness and unpredictability that can enhance the security of communication channels [20]. The application of chaos theory to cryptography, known as chaotic cryptology, has attracted much interest in recent years. Chaotic synchronization between identical systems has secured communication channels through chaotic modulation, multi-carrier and

The associate editor coordinating the review of this manuscript and approving it for publication was Yi Fang.

multiple access schemes, and encryption schemes (see [21], [22]). Various encryption algorithms have been proposed using different chaotic systems, combined with multi-shift cipher encryption and double chaotic masking to improve the security of communication channels (see [23], [24]).

Image encryption is a technique used to secure images by transforming their contents into an unintelligible form that can only be restored to its original form by authorized parties. Chaotic systems have proven to be an effective method for image encryption because of their excellent random properties and encryption performance (see [9], [25], [26]). In recent decades, many researchers have devoted themselves to studying image encryption based on chaotic systems and have made significant strides in research because of their attractive features characterized by sensitive dependence on initial conditions and aperiodic, seemingly random behavior [26].

In image encryption, chaotic systems generate a sequence of numbers that can be used to scramble the image pixels [10]. These chaotic sequences have strong statistical characteristics, which is the basis for the perfect success of the image encryption system [10]. Existing image encryption algorithms based on chaotic systems have shown some security defects due to small key space or other security weaknesses. New image encryption algorithms have been proposed to address these issues using complex, chaotic systems, coupled map lattice, or memristive chaotic systems. These algorithms combine different chaotic maps with permutation and diffusion techniques to increase the scrambling degree of the image pixels.

In literature, there are many existing image encryption schemes using chaotic systems. Zhou et al. [28] proposed a new combination chaotic system (NCCS) for image encryption, which has a larger key space and better cryptographic features than previous one-dimensional chaotic maps. The proposed bit-level encryption scheme uses NCCS, SHA-512 Hash function, and random decimal points sequence to generate key streams and perform image confusion and diffusion operations.

Sang et al. [29] developed a new image encryption method using logistic chaotic systems and deep autoencoder. The plaintext image is scrambled using a logistic chaotic system and then encoded using a deep autoencoder to produce the ciphertext image.

Zhu et al. [30] introduced a sinusoidal-polynomial composite chaotic system (SPCCS) that satisfies Devaney's definition of chaos, making it suitable for cryptography. An image encryption algorithm was developed using SPCCS, which involves pixel segmentation, block chaotic matrix confusion, and pixel diffusion operations. The simulation results demonstrated the effectiveness and superiority of the proposed image encryption algorithm.

In this paper, we propose a novel jerk system with three quadratic nonlinear terms and demonstrate the dynamical properties of the proposed jerk system in terms of phase portraits, bifurcation diagrams, and Lyapunov exponents, multistability and coexisting attractors. For practical implementations, we apply Multisim version 14.0 to design an electronic model of the proposed 3-D jerk system. To illustrate the feasibility of the proposed chaotic jerk system, we implement the new chaotic system by using a field-programmable gate array (FPGA), which shows high throughput and low power consumption. Furthermore, a new image encryption scheme based on the proposed jerk system is developed, which involves permutation and diffusion operations. Experimental results and security analysis show the effectiveness of our proposed algorithm in terms of high security and excellent encryption performance. Our research contributes to the ongoing efforts toward developing robust and secure image encryption techniques that can be utilized in various applications, such as secure communication and data storage.

II. MODELING OF JERK SYSTEM

A new jerk differential equation is proposed in this research paper, which is modelled by the third order differential equation

$$\frac{d^3x}{dt^2} = ax - b\frac{dx}{dt} - \frac{d^2x}{dt^2} - c\frac{dx}{dt}\frac{d^2x}{dt^2} - x^2 - \left(\frac{dx}{dt}\right)^2 \tag{1}$$

where a, b, c are positive parameters. In mechanical systems, the word "*jerk*" stands for the third order derivative of a scalar variable $x(t)$ with respect to t.

If we define the state variables y and z as

$$y = \frac{dx}{dt} \quad \text{and} \quad z = \frac{d^2x}{dt^2}, \tag{2}$$

then the jerk ODE (1) can be put as the following jerk system

$$\begin{cases} \dot{x} &= y \\ \dot{y} &= z \\ \dot{z} &= ax - by - z - cyz - x^2 - y^2 \end{cases} \tag{3}$$

where $X = (x, y, z)$ is the system state.

The Lyapunov exponents of the 3-D jerk system (3) with three quadratic terms can be calculated in MATLAB for $a = 7.5$, $b = 4$, $c = 0.3$, $X(0) = (0.3, -0.2, 0.3)$ and $T = 1E5$ seconds as

$$\tau_1 = 0.1631, \quad \tau_2 = 0, \quad \tau_3 = -1.1631 \tag{4}$$

which confirms that the jerk system (3) has a dissipative chaotic attractor as illustrated in Figure 1.

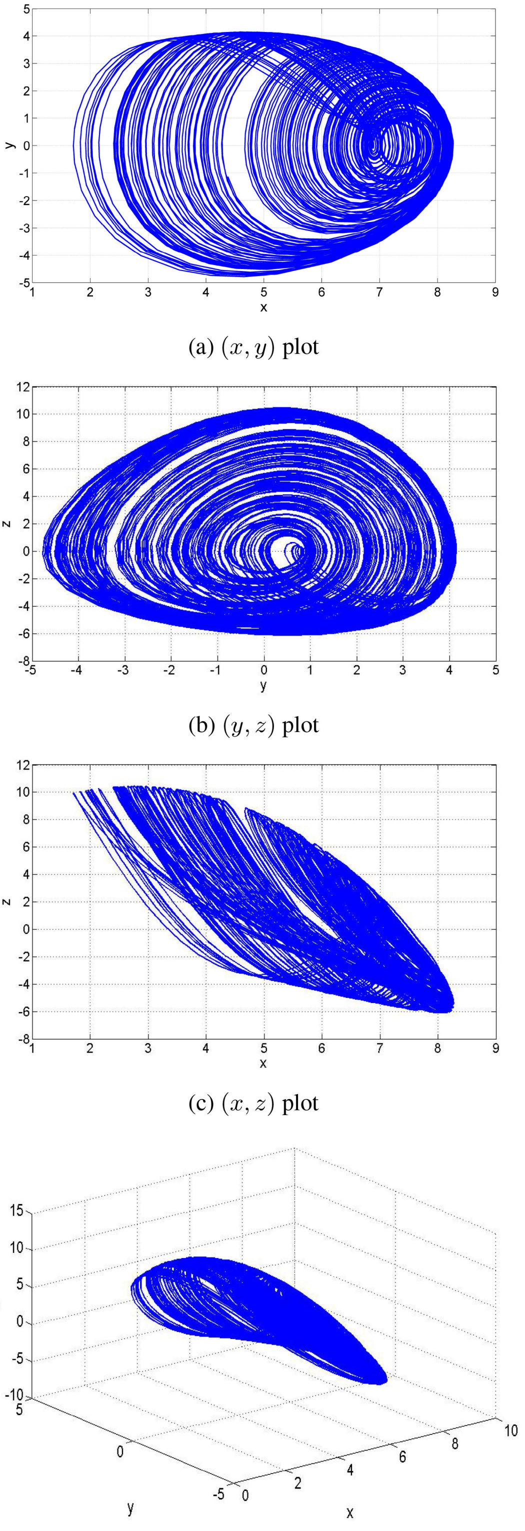
To evaluate all the equilibrium points of the 3-D jerk system (3), we are required to solve the following system of equations:

$$3y = 0 \tag{5a}$$

$$z = 0 \tag{5b}$$

$$ax - by - z - cyz - x^2 - y^2 = 0 \tag{5c}$$

From (5a) and (5b), we get $y = z = 0$.



(a) (x, y) plot

(b) (y, z) plot

(c) (x, z) plot

(d) $\mathbf{R}^3$ plot

FIGURE 1. The MATLAB simulation results depicting the state orbits of the 3-D jerk system (3) for $a = 7.5$, $b = 4$, $c = 0.3$ and $X(0) = (0.3, -0.2, 0.3)$.

Substituting these values ($y = 0, z = 0$) into Eq. (5c), we get

$$ax - x^2 = x(a - x) = 0 \tag{6}$$

Solving (6), we get the two roots $x = 0$ and $x = a$.

Thus, the 3-D jerk system (3) has two equilibrium points given by $E_0 = (0, 0, 0)$ and $E_1 = (a, 0, 0)$.

For the chaotic case, the parameters take the values $a = 7.5$, $b = 4$ and $c = 0.3$.

Hence, the 3-D jerk system (3) has two equilibrium points given by $E_0 = (0, 0, 0)$ and $E_1 = (7.5, 0, 0)$ for the chaotic case.

The Jacobian matrix of the 3-D jerk system (3) at E_0 has the eigenvalues

$$\begin{cases} \alpha_1 &= 1.1555, \\ \alpha_2 &= -1.0778 + 2.3085\, i, \\ \alpha_3 &= -1.0778 - 2.3085\, i \end{cases} \tag{7}$$

The Jacobian matrix of the 3-D jerk system (3) at E_1 has the eigenvalues

$$\begin{cases} \alpha_1 &= -1.5474, \\ \alpha_2 &= 0.2737 + 2.1845\, i, \\ \alpha_3 &= 0.2737 - 2.1845\, i \end{cases} \tag{8}$$

An equilibrium point E is called saddle-focus when it has one real eigenvalue with the sign opposite to the sign of the real part of a pair of complex-conjugate eigenvalues and this type of equilibrium is always unstable [31].

Thus, we conclude that the equilibrium points $E_0 = (0, 0, 0)$ and $E_1 = (7.5, 0, 0)$ are saddle-foci and unstable.

Hence, the jerk system (3) with three quadratic nonlinear terms has a self-excited chaotic attractor for the chaotic case $(a, b, c) = (7.5, 4, 0.3)$.

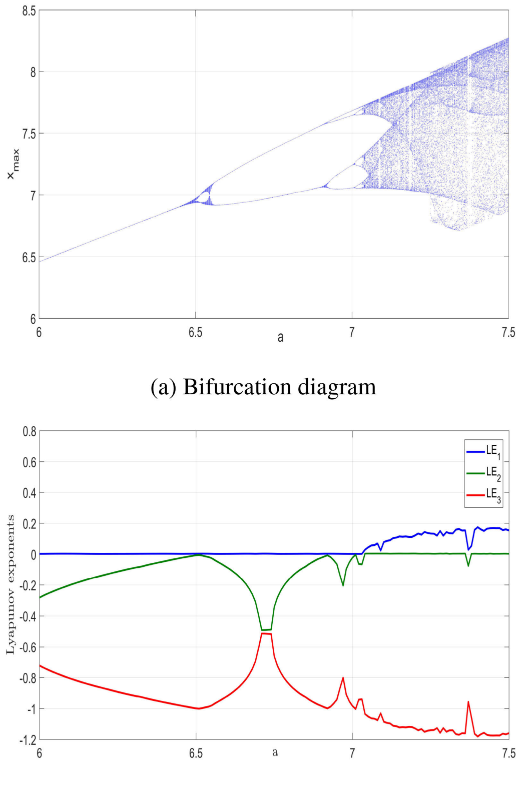
III. BIFURCATION ANALYSIS

In this section, we conduct a detailed investigation into how the behavior of the 3-D jerk system (3) with three quadratic nonlinear terms changes in response to variations in its parameters a, b and c, using bifurcation diagrams and Lyapunov exponents spectra. As the parameters a, b and c are altered separately, the jerk system (3) displays both periodic and chaotic behavior, which are visualized through phase plots. Various behaviors are identified through numerical simulations in MATLAB.

A. THE PARAMETER *a* VARYING

If we keep $b = 4$, $c = 0.3$ and change of the value of a in the interval $[6, 7.5]$, then we can examine the impact of the variation of a on the jerk system (3). Figure 2(b) presents the Lyapunov exponents spectrum and the associated bifurcation diagram for the jerk system (3). The visualizations in Figure 2 demonstrate that the jerk system (3) can exhibit periodic or chaotic behavior as a is increased from $a = 6$ to $a = 7.5$.

The jerk system (3) displays periodic behavior for $a \in [6, 7.03]$. This conclusion is based on the presence of one zero Lyapunov exponent and two negative Lyapunov exponents for the jerk system (3) when $a \in [6, 7.03]$. For instance, when $a = 6$, the Lyapunov exponents of the jerk system (3) take on



(a) Bifurcation diagram

(b) Lyapunov exponents diagram

FIGURE 2. Bifurcation diagram (a) and Lyapunov exponents spectrum (b) of the new jerk system (3) when $b = 4$, $c = 0.3$ and $a \in [6, 7.5]$.

the following values:

$$\mathrm{LE}_1 = 0,\ \mathrm{LE}_2 = -0.282,\ \mathrm{LE}_3 = -0.722 \tag{9}$$

The jerk system (3) displays chaotic behavior for $a \in [7.03, 7.5]$. This conclusion is based on the presence of one positive Lyapunov exponents for the jerk system (3) when $a \in [7.03, 7.5]$. For instance, when $a = 7.45$, the Lyapunov exponents of the jerk system (3) take on the following values:

$$\mathrm{LE}_1 = 0.169,\ \mathrm{LE}_2 = 0,\ \mathrm{LE}_3 = -1.174 \tag{10}$$

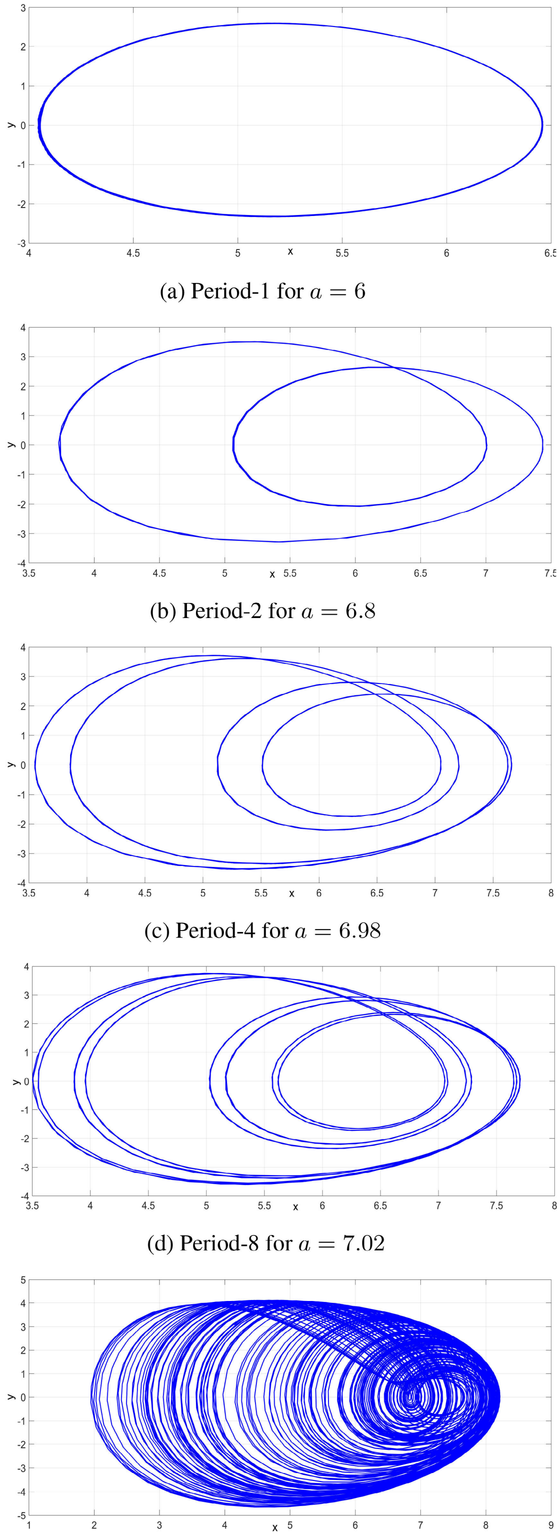
Additionally, the bifurcation diagram presented in Figure 2(a) illustrates that the jerk system (3) experiences the famous period-doubling route to chaos. Specifically as a increases within certain parameter ranges, the jerk system (3) undergoes a series of period-doubling that progresses from period-1 to period-2, then to period-4, and eventually period-8 before reaching chaotic behavior.

When $a \in [6, 6.5]$, the jerk system (3) has a period-1 attractor.

When $a \in [6.5, 6.9]$, the jerk system (3) has a period-2 attractor.

When $a \in [6.9, 7.01]$, the jerk system (3) has a period-4 attractor.

When $a \in [7.01, 7.03]$, the jerk system (3) has a period-8 attractor.



(a) Period-1 for $a = 6$

(b) Period-2 for $a = 6.8$

(c) Period-4 for $a = 6.98$

(d) Period-8 for $a = 7.02$

(e) Chaos for $a = 7.45$

FIGURE 3. Visual representation of the attractors of the jerk system (3) for parameter a varying.

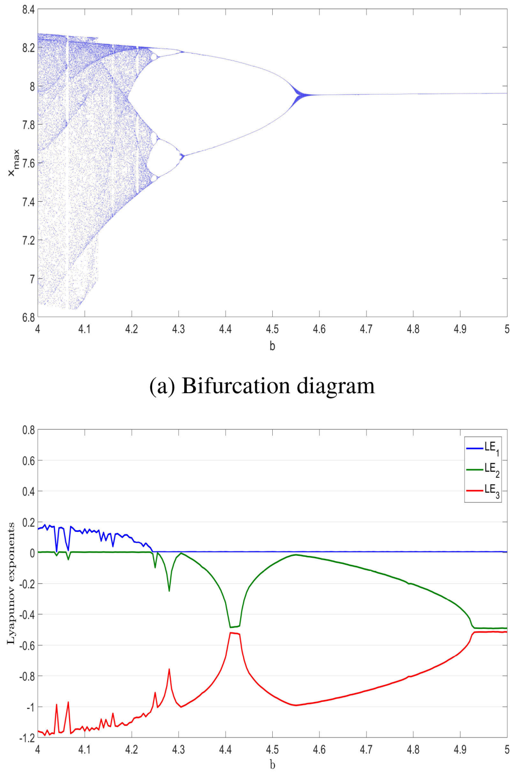
Finally, when a falls within the range $[7.03, 7.5]$, the jerk system (3) has a chaotic attractor.

TABLE 1. Period-doubling route to chaos with parameter *a* varying for the jerk system (3).

Parameter a range	Parameter a value	Dynamics	Attractor
$[6, 6.5]$	6	Period-1	Figure 3 (a)
$[6.5, 6.9]$	6.8	Period-2	Figure 3 (b)
$[6.9, 7.01]$	6.98	Period-4	Figure 3 (c)
$[7.01, 7.03]$	7.02	Period-8	Figure 3 (d)
$[7.03, 7.05]$	7.45	Chaos	Figure 3 (e)

TABLE 2. Reverse period-doubling route with parameter *b* varying for the jerk system (3).

Parameter b range	Parameter b value	Dynamics	Attractor
$[4, 4.24]$	4.1	Chaos	Figure 5 (a)
$[4.24, 4.258]$	4.25	Period-8	Figure 5 (b)
$[4.258, 4.31]$	4.28	Period-4	Figure 5 (c)
$[4.31, 4.58]$	4.4	Period-2	Figure 5 (d)
$[4.58, 5]$	4.8	Period-1	Figure 5 (e)



(a) Bifurcation diagram

(b) Lyapunov exponents diagram

FIGURE 4. Bifurcation diagram (a) and Lyapunov exponents spectrum (b) of the new jerk system (3) when $a = 7.5$, $c = 0.3$ and $b \in [4, 5]$.

The attractors observed through MATLAB simulations are summarized in Table 1, which illustrates the period-doubling route to chaos described earlier. Furthermore, Figure 3 provides a visual representation of the attractors of the jerk system (3).

B. THE PARAMETER *b* VARYING

To study the impact of changes in the “b” parameter on system (1), the values of “a” and “c” are fixed at 7.5 and 0.3, respectively, while “b” is varied between 4 and 5. Figure 4 displays the Lyapunov exponents spectrum and the bifurcation diagram of system (3), demonstrating that the 3-D jerk system (3) can display both periodic and chaotic behavior as “b” increases within this range.

When the value of “b” is within the range of [4, 4.24], system (3) displays chaotic behavior with one positive Lyapunov exponent. In addition, the system’s Kaplan-Yorke dimension is a fractional value of 2.133. For instance, when b=4.1, the Lyapunov exponents of the of the jerk system (3) take on the following values:

$$\mathrm{LE}_1 = 0.154,\ \mathrm{LE}_2 = 0,\ \mathrm{LE}_3 = -1.159 \tag{11}$$

The behavior of System (3) is periodic when “b” is in the range of [4.24, 5]. In this range, one Lyapunov exponent is zero, while the other two are negative. Specifically, when b=4.8, the Lyapunov exponents of the of the jerk system (3) take on the following values:

$$\mathrm{LE}_1 = 0,\ \mathrm{LE}_2 = -0.205,\ \mathrm{LE}_3 = -0.800 \tag{12}$$

Additionally, the bifurcation diagram presented in Figure 4 illustrates that the jerk system (3) experiences the famous period-doubling route to chaos. This leads to the occurrence of the reverse period-doubling phenomenon in certain ranges of “b,” wherein the system transitions from chaotic behavior to period-8, then to period-4,period-2, and finally to period-1.

When $b \in [4, 4.24]$, the jerk system (3) has a chaotic attractor.

When $b \in [4.24, 4.258]$, the jerk system (3) has a period-8 attractor.

When $b \in [4.258, 4.31]$, the jerk system (3) has a period-4 attractor.

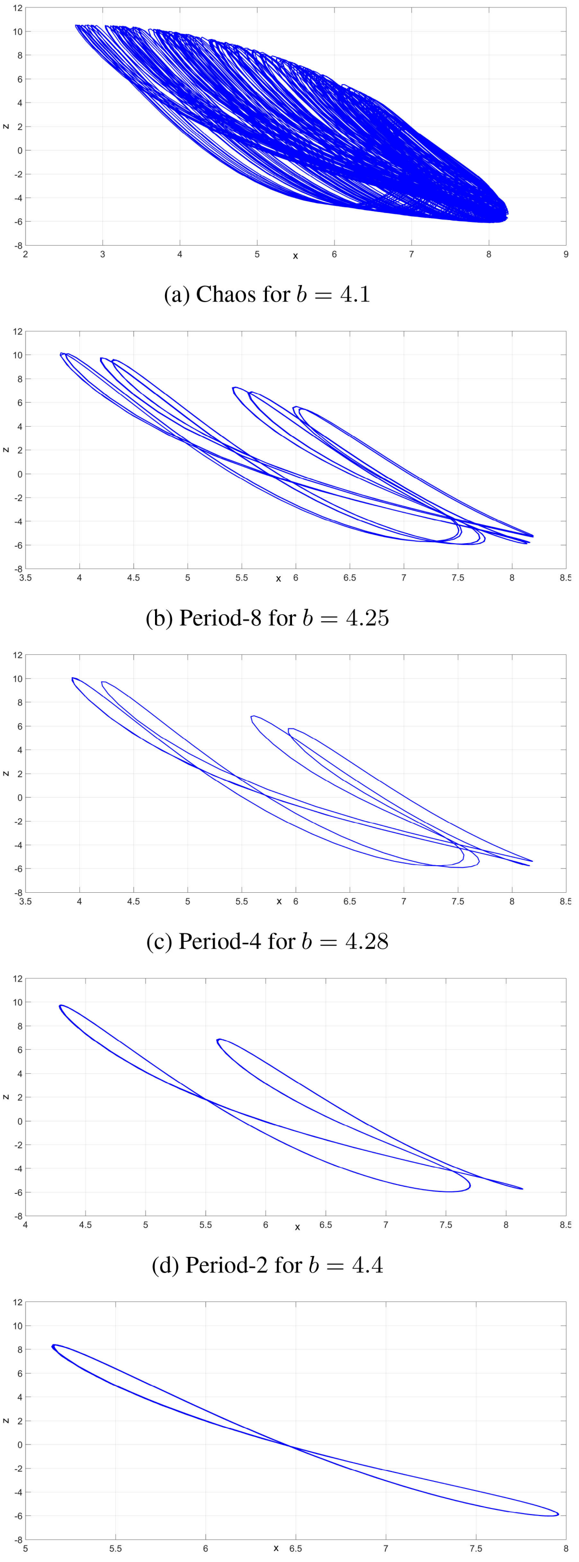
When $b \in 4.31, 4.58]$, the jerk system (3) has a period-2 attractor.

Finally, when b falls within the range [4.58, 5], the jerk system (3) has a period-1 attractor.

The attractors observed through MATLAB simulations are summarized in Table 2, which illustrates the period-doubling route to chaos described earlier. Furthermore, Figure 5 provides a visual representation of the attractors of the jerk system (3).

C. THE PARAMETER *c* VARYING

If we keep $a = 7.5$, $b = 4$ and change of the value of c in the interval [0.04, 3], then we can examine the impact of the variation of c on the jerk system (3). Figure 6 presents the Lyapunov exponents spectrum and the associated bifurcation diagram for the jerk system (3). The visualizations in Figure 6



(a) Chaos for $b = 4.1$

(b) Period-8 for $b = 4.25$

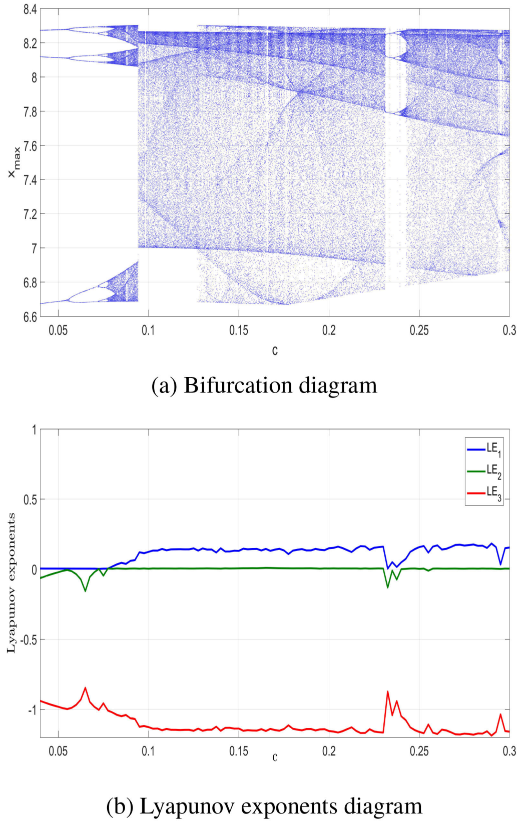
(c) Period-4 for $b = 4.28$

(d) Period-2 for $b = 4.4$

(e) Period-1 for $b = 4.8$

FIGURE 5. Visual representation of the attractors of the jerk system (3) for parameter *b* varying.

demonstrate that the jerk system (3) can exhibit periodic or chaotic behavior as c is increased from $c = 0.04$ to $c = 3$.



(a) Bifurcation diagram

(b) Lyapunov exponents diagram

FIGURE 6. Bifurcation diagram (a) and Lyapunov exponents spectrum (b) of the new jerk system (3) when *a* = 7.5, *b* = 4 and *c* ∈ [0.04, 3].

The jerk system (3) displays periodic behavior for $c \in [0.04, 0.077]$. This conclusion is based on the presence of one zero Lyapunov exponent and two negative Lyapunov exponents for the jerk system (3) when $c \in [0.04, 0.077]$. For instance, when $c = 0.05$, the Lyapunov exponents of the jerk system (3) take on the following values:

$$\mathrm{LE}_1 = 0,\ \mathrm{LE}_2 = -0.022,\ \mathrm{LE}_3 = -0.982 \tag{13}$$

The jerk system (3) displays chaotic behavior for $c \in [0.077, 3]$. This conclusion is based on the presence of one positive Lyapunov exponents for the jerk system (3) when $c \in [0.077, 3]$. For instance, when $c = 0.2$, the Lyapunov exponents of the jerk system (3) take on the following values:

$$\mathrm{LE}_1 = 0.149,\ \mathrm{LE}_2 = 0,\ \mathrm{LE}_3 = -1.155 \tag{14}$$

Additionally, the bifurcation diagram presented in Figure 6(a) illustrates that the jerk system (3) experiences the famous period-doubling route to chaos. Specifically as c increases within certain parameter ranges, the jerk system (3) undergoes a series of period-doubling that progresses from period-3 to period-6, from period-6 to period-12 and eventually to a chaotic attractor.

When $c \in [0.04, 0.055]$, the jerk system (3) has a period-3 attractor.

TABLE 3. Period-doubling route to chaos with parameter c varying for the jerk system (3).

Parameter c range	Parameter c value	Dynamics	Attractor
$[0.04, 0.05]$	0.05	Period-3	Figure 7 (a)
$[0.055, 0.072]$	0.065	Period-6	Figure 7 (b)
$[0.072, 0.077]$	0.073	Period-12	Figure 7 (c)
$[0.077, 0.3]$	0.2	Chaos	Figure 7 (d)

When $c \in [0.055, 0.072]$, the jerk system (3) has a period-6 attractor.

When $c \in [0.072, 0.077]$, the jerk system (3) has a period-12 attractor.

Finally, when c falls within the range $[0.077, 0.3]$, the jerk system (3) has a chaotic attractor.

The attractors observed through MATLAB simulations are summarized in Table 3, which illustrates the period-doubling route to chaos described earlier. Furthermore, Figure 7 provides a visual representation of the attractors of the jerk system (3).

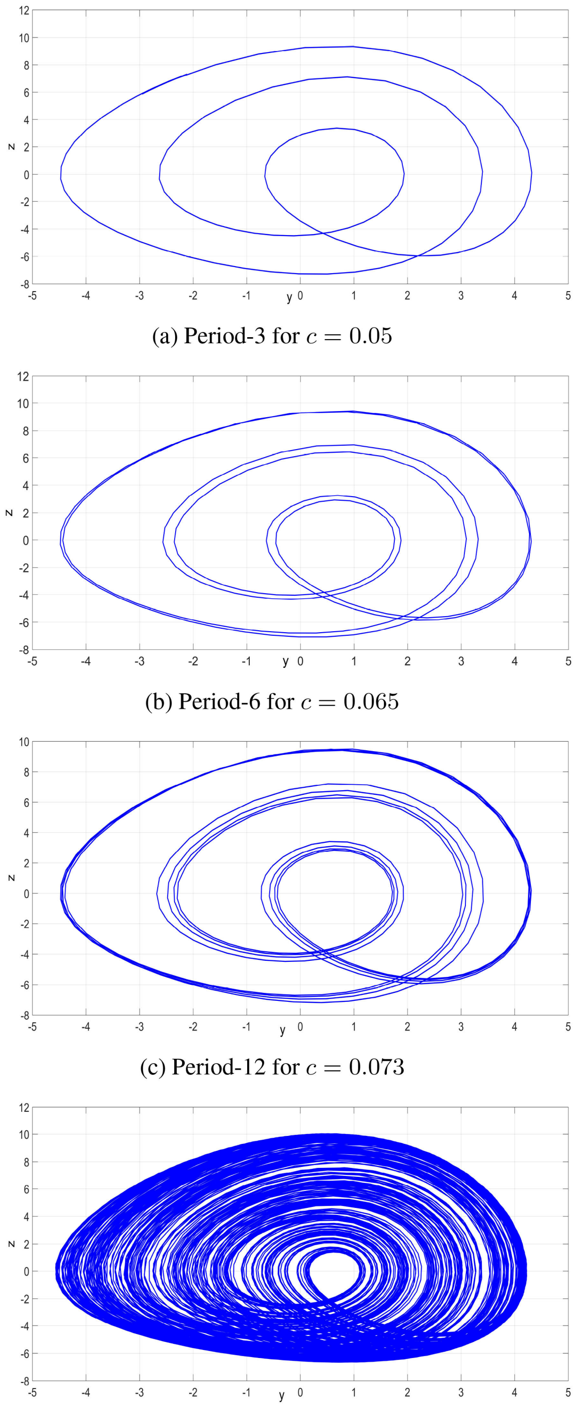
D. MULTISTABILITY AND COEXISTING ATTRACTORS

The dynamic behavior of the 3-D jerk system (3) is affected by changes in the initial conditions (x_0, y_0, z_0), while the parameters of the system are kept fixed. This can lead to the emergence of coexisting chaotic attractors for the jerk system (3). To explore this multistability phenomenon for the jerk system (3), we generated a bifurcation diagram by varying z_0 in the range $-0.5 < z_0 < 0.5$ as depicted in Figure 8 (a). The obtained results indicate that the jerk system (3) exhibits a distinctly different chaotic attractor colored in red in the range $-0.5 < z_0 < -0.1$, when compared to the chaotic attractor colored in blue and observed in the range $-0.1 < z_0 < 0.5$.

To provide futher clarification, we consider two starting points as $X_{01} = (0.3, 0.2, -0.3)$ and $X_{02} = (0.3, -0.2, 0.3)$, which belong to separate basins of attraction. For each starting point, we generated a bifurcation diagram within the parameter range of $0.04 < c < 0.1$ to visualize the dynamic behavior of the jerk system (3). We used blue color for X_{01} and red color for X_{02}. Figure 8 (b) effectively demonstrates that the new jerk system (3) exhibits two distinct behaviors within the specific interval of the parameter c.

A bifurcation diagram was then generated for the jerk system (3) for each of these starting points for the jerk system (3) within the range of $0.04 < c < 0.1$ to visualize the behavior of the system and depicted in Figure 8, where the blue color corresponds to the trajectory starting from X_{01}, while the red color corresponds to the trajectory starting from X_{02}.

For example, when the parameters are chosen as $a = 7.5$, $b = 4$ and $c = 0.08$, the 3-D jerk system (3) displays two coexisting attractors as depicted in Figure 8 (c). These results are in complete agreement with the observations in Figure 8 (a).



(a) Period-3 for $c = 0.05$

(b) Period-6 for $c = 0.065$

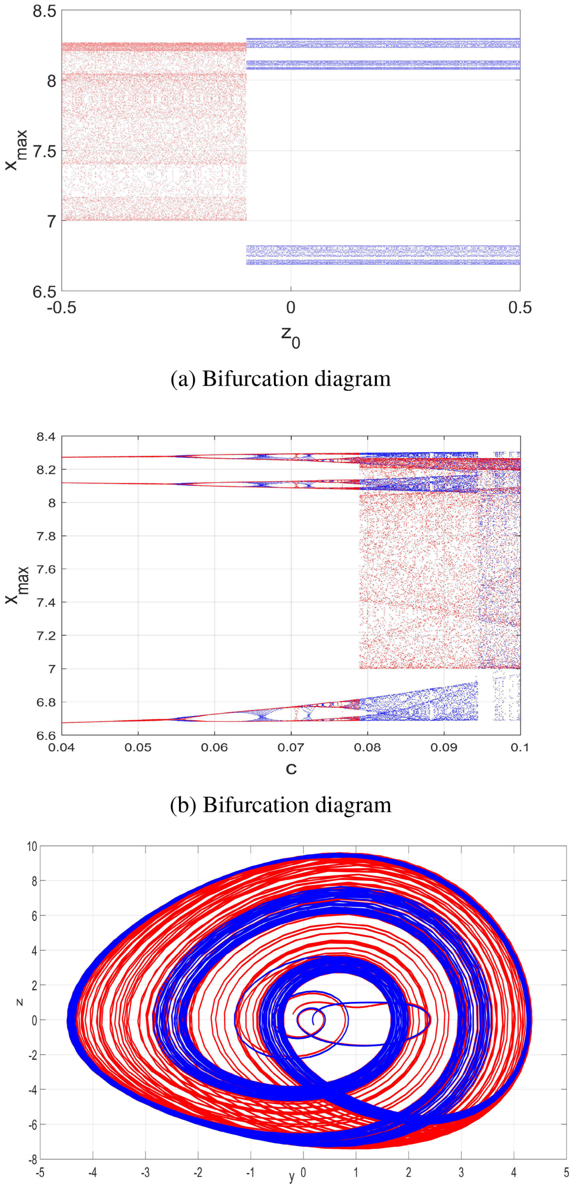
(c) Period-12 for $c = 0.073$

(d) Chaos for $c = 0.2$

FIGURE 7. Visual representation of the attractors of the jerk system (3) for parameter c varying.

IV. CIRCUIT DESIGN

The circuit implementation of their respective mathematical models is frequently employed to explore dynamics and



(a) Bifurcation diagram

(b) Bifurcation diagram

(c) Coexisting attractors

FIGURE 8. Multistability for the jerk system (3) where $a = 7.5$, $b = 4$ and $c = 0.08$: (a) Bifurcation diagram of the system (3) for z_0, (b) Bifurcation diagram of the system (3) for X_{01} (blue color) and X_{02} (red color) and (c) MATLAB plots of the coexisting chaotic attractors of the system (3).

confirm the viability of a theoretical chaotic model. Because electronic circuits are widely used in engineering, it is feasible to utilise them to simulate chaotic systems. In this section, the electronic circuit of the new Jerk chaotic system (15) is designed and confirmed.

The relevant circuit state equation set of the proposed new Jerk chaotic system can be described as by applying Kirchhoff principles to the electronic circuit

$$C_1\dot{x} = \frac{1}{R_1}y$$
$$C_2\dot{y} = \frac{1}{R_2}z$$
$$C_3\dot{z} = \frac{1}{R_3}x - \frac{1}{R_4}y - \frac{1}{R_5}z - \frac{1}{10R_6}yz - \frac{1}{10R_7}x^2 - \frac{1}{10R_8}y^2 \quad (15)$$

where x, y, z are the voltages across the capacitors C_1, C_2, C_3, respectively. The entire circuit is put into practise on the Multisim electronic simulation platform, where Figure 9 shows the planned circuit put into practise using Multisim simulation. The values of all electronic components in Figure 9 are determined as follows: $R_3 = 13.33$ kΩ, $R_4 = 25$ kΩ, $R_6 = 33.33$ kΩ5 $R_7 = R_8 = 10$ kΩ, $R_1 = R_2 = R_5 = R_9 = R_{10} = R_{11} = R_{12} = R_{13} = R_{14} = 100$ kΩ. The simulation results, which are phase portraits of the new Jerk chaotic system, are shown in Figure 10.

Figure 11 shows the spectral distribution for three coordinates of chaotic signals: x, y and z. The power spectra of the produced signals span to a frequency range that goes beyond 5 kHz. The peak of the frequency spectrum was measured to be at 1.05 kHz (for y and z). Signal x has two peaks of the frequency spectrum: I - 0.3 kHz, II - 1.05 kHz.

V. FPGA HARDWARE IMPLEMENTATION

We describe the chaotic oscillator system with the set of equations in (16) where a, b, and c are constant coefficients.

$$\dot{x} = y$$
$$\dot{y} = z$$
$$\dot{z} = ax{-}by{-}z{-}cyz - x^2 - y^2 \quad (16)$$

Regarding the numerical solutions of the above system, we will apply the forward Euler integration method. Thus, the numerical solution for the chaotic oscillator system would be as follows (17).

$$x[n+1] = x[n] + hy[n]$$
$$y[n+1] = y[n] + hz[n]$$
$$z[n+1] = z[n] + h(ax[n] - by[n] - z[n] - cy[n]z[n] - x^2[n] - y^2[n]) \quad (17)$$

here, h is the discretization step size. The digital FPGA implementation of the chaotic oscillator system will be based on the discrete-time equations provided above.

We provide the Python code for the chaotic oscillator system to create a high-level perspective of the algorithm and to aid us in designing the VHDL code for the system, as well as verifying the behavior when comparing the results of the VHDL system to the Python system.

Using Python we are going to describe (17) in Algorithm 1. For the simulation, the coefficient parameters will take the following values $a = 7.5$, $b = 4$, and $c = 0.3$. The initial values of the variables are going to be $x_{init} = 0.3$, $y_{init} = 0.2$, $z_{init} = 0.3$.

The Top Level Hardware implementation of the chaotic oscillator system is shown in Figure 12; the top level block has three input buses and three output buses: x_{init}, y_{init}, z_{init},

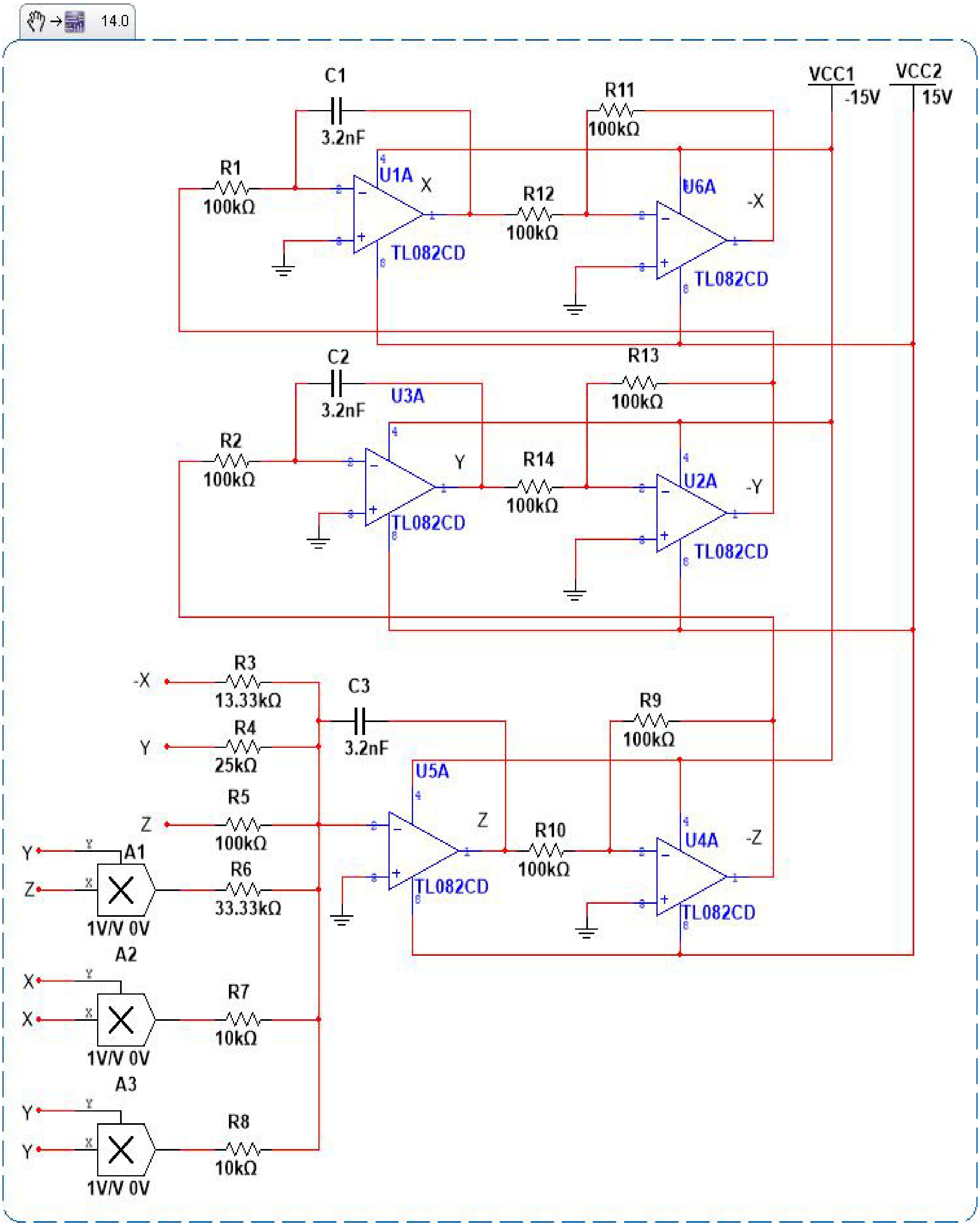
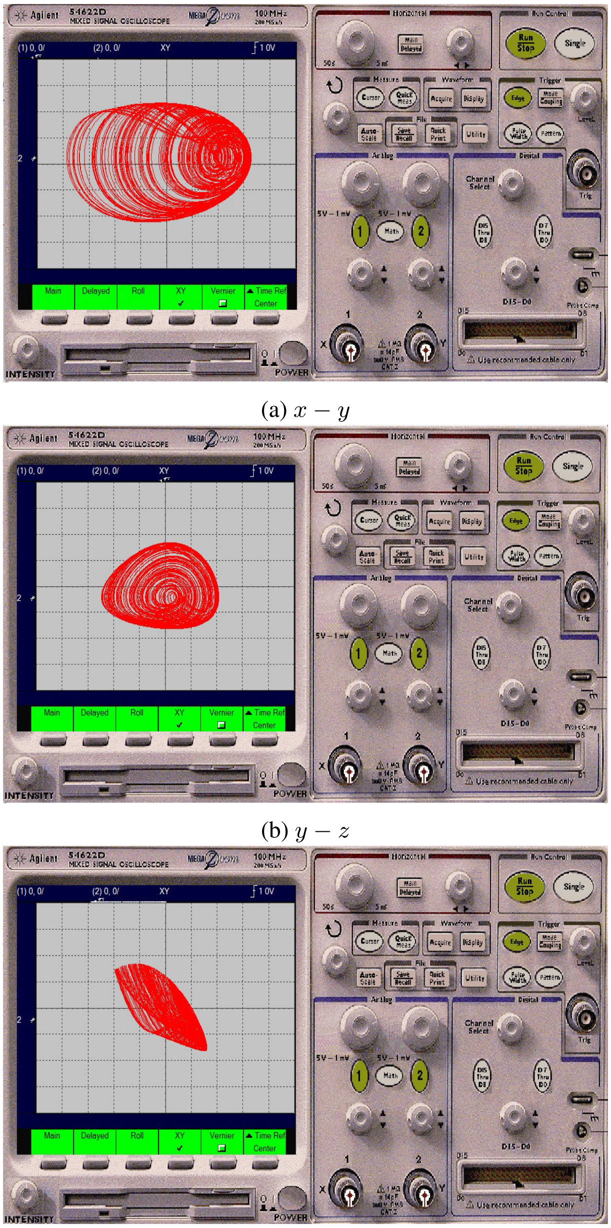


FIGURE 9. Electronic circuit schematic of the proposed the new Jerk chaotic system (15).

$xout$, $yout$, $zout$. Additional inputs are the coefficient parameters a, b, and c. Note that the output buses are being fed back into the block to generate the values of the following iteration of the system.

Regarding the implementation in VHDL code, we are going to use an architecture that takes in all system coefficients and values as inputs. Variables and constants possess high precision in which 32 bits are used to represent them in

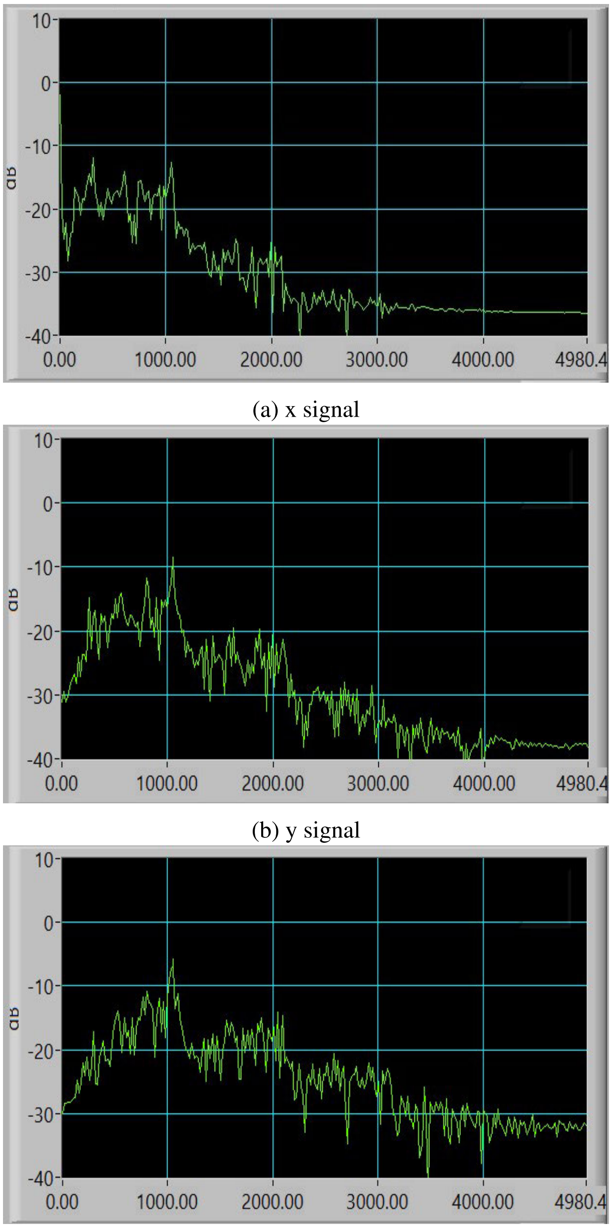


(a) $x-y$

(b) $y-z$

(c) $x-z$

FIGURE 10. Chaotic attractor of new Jerk chaotic system (15) using MultiSIM circuit simulation.



(a) x signal

(b) y signal

(c) z signal

FIGURE 11. The spectral distribution of the x, y, z signals of the chaotic jerk circuit (15).

fixed point; the sign is represented with 1 bit, the integer part with 7 bits, and the fractional part with 24 bits as shown in Figure 13.

To implement the equations described in (17) on an FPGA platform, the basic building blocks are the adder, subtractor, multiplier, and the D flipflop (DFF) as in Figure 14. All basic block components are sequential, taking in a clock (clk) and an asynchronous reset (rst) as inputs; each block requires one clock pulse to generate output. The DFF is used to delay the output of a system. All systems are delayed with DFF blocks such that their delay matches the system's with the greatest number of clock cycles required to generate its output. The basic components' VHDL codes are provided in Algorithms 2-5.

According to the equation described in (17), the variables x and y are implemented as per the schematic shown in Figure 15. Two operations are required for these systems, a multiplication and an addition(i.e., two hardware blocks). At the bottom of the figure is a graph of the number of clock cycles required to generate the output, which shows the propagation time of two clocks for the x and y systems. The z system on the other hand, requires seven multipliers, three adders, and three subtractors, as shown in Figure 16, which results in a total number of six clock cycles for the

Algorithm 1 Chaotic Oscillator System

```
Input : Initial states $x_{init}$, $y_{init}$, and $z_{init}$. Coefficient
        parameters $a$, $b$, and $c$.
Output: $xout$, $yout$, and $zout$
$i = 0$
$x = x_{init}$
$y = y_{init}$
$z = z_{init}$
while $i < step$ do
    $xout$.insert($i, x + h * y$)
    $yout$.insert($i, y + h * z$)
    $zout$.insert($i, z + h * (a * x - b * y - z - c * y * z - x * x - y * y)$)
    $x = xout[i]$
    $y = yout[i]$
    $z = zout[i]$
    $i = i + 1$
```

Algorithm 2 Adder VHDL Code

```
entity adder is port(
          clk, rst: in std_logic;
          in1, in2: in std_logic_vector(31 downto 0);
          out1: out std_logic_vector(31 downto 0):=(others => ‘0’)
);
end entity;
architecture adder_arch of adder is
begin
          process(clk,rst,in1,in2)
          begin
               if rst = ‘0’ then
                    out1 <= (others => ‘0’);
               elsif (clk’event and clk = ‘1’) then
                    out1 <= std_logic_vector(signed(in1) + signed(in2));
               end if;
          end process;
end architecture;
```

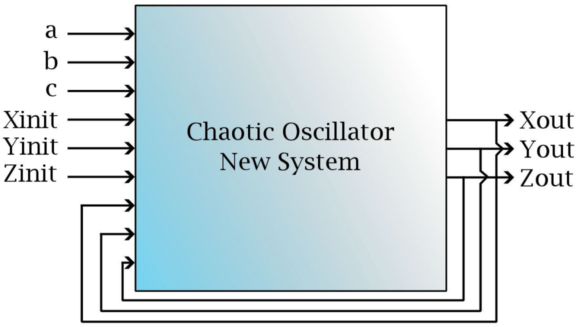


FIGURE 12. Top Level map of the VHDL implementation.

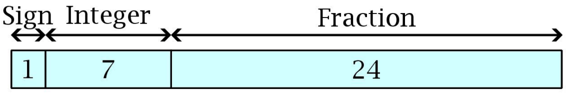


FIGURE 13. Full Precision Fixed Point Representation.

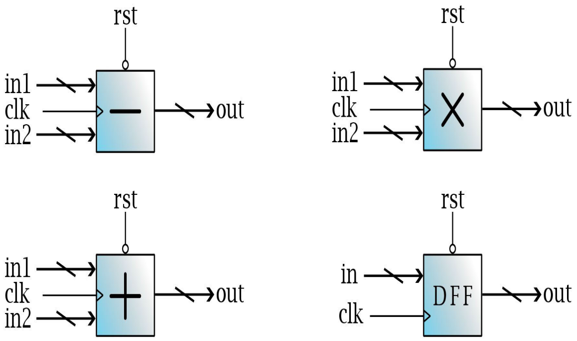


FIGURE 14. Basic Components used to build the Chaotic Oscillator System.

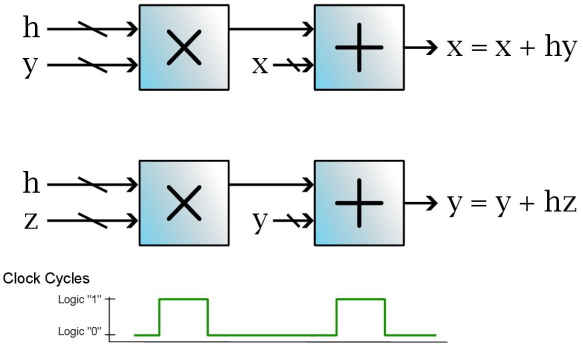


FIGURE 15. Connections of the basic blocks to implement the *x* and *y* systems of the chaotic oscillator.

propagation time since some of the blocks can work in parallel. Because synchronization is important to generate correct values, we delay the output of both the x and y systems by four clock cycles by connecting four D flip flops in series to the output, as shown in Figure 17.

Figure 18 illustrates the $x - y, x - z, andy - z$ attractors obtained from the oscilloscope. Note that the cursor must have "trace" on in the Oscilloscope settings so that the cursor draws the plot as it goes through the values.

VI. IMAGE CRYPTOGRAPHY SCHEME BASED THE PROPOSED JERK SYSTEM

This section presents a novel image cryptography scheme based on the Jerk system. Figure 19 depicts the encryption scheme that utilizes the state vector [x, y, z] generated by the jerk system to encrypt the original grayscale image. Firstly, the x state variable is used to permute the original image,

Algorithm 3 Subtractor VHDL Code

```
entity sub is port(
        clk, rst: in std_logic;
        in1, in2: in std_logic_vector(31 downto 0);
        out1: out std_logic_vector(31 downto 0):=(others => '0')
);
end entity;
architecture sub_arch of sub is
begin
        process(clk,rst,in1,in2)
        begin
            if rst = '0' then
                out1 <= (others => '0');
            elsif (clk'event and clk = '1') then
                out1 <= std_logic_vector(signed(in1) - signed(in2));
            end if;
        end process;
end architecture;
```

Algorithm 4 Multiplier VHDL Code

```
entity mul is port(
        clk, rst: in std_logic;
        in1, in2: in std_logic_vector(31 downto 0);
        out1: out std_logic_vector(31 downto 0):=(others => '0')
);
end entity;
architecture mul_arch of mul is
signal sig_64:signed(63 downto 0);
begin
        process(clk,rst,in1,in2)
        begin
            if rst = '0' then
                out1 <= (others => '0');
            elsif (clk'event and clk = '1') then
                sig_64 <= (signed(in1) * signed(in2));
                out1 <= std_logic_vector(sig_64(55 downto 24);
            end if;
        end process;
end architecture;
```

Algorithm 5 D FlipFlop VHDL Code

```
entity D_Flip_Flop is port(
        clk, rst: in std_logic;
        in1: in std_logic_vector(31 downto 0);
        out1: out std_logic_vector(31 downto 0):=(others => '0')
);
end entity;
architecture D_Flip_Flop_arch of D_Flip_Flop is
begin
        process(clk,rst,in1)
        begin
            if rst = '0' then
                out1 <= (others => '0');
            elsif (clk'event and clk = '1') then
                out1 <= in1;
            end if;
        end process;
end architecture;
```

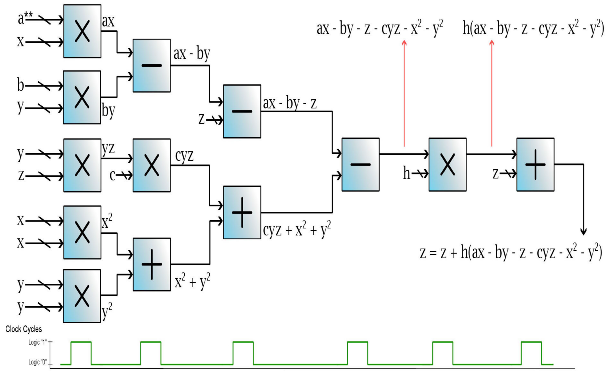


FIGURE 16. Connections of the basic blocks to implement the *z* system of the chaotic oscillator.

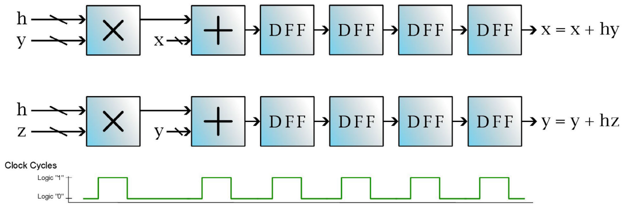


FIGURE 17. *x* and *y* systems delayed by four clock cycles for propagation time delay synchronization.

while the y state variable is utilized to diffuse the permuted image. Finally, an XOR operation is performed between the diffused images and the z state variable generated by the Jerk system to produce the encrypted image.

A. SECURITY ANALYSIS

This section analyzes the security of the proposed cryptography system using different tests; histogram analysis, correlation distribution, information entropy, key space analysis, and NIST test.

1) HISTOGRAM

To display the distribution of image pixel intensity, a histogram is used. When an image is properly encrypted, it should have a uniform frequency distribution. This makes it difficult for attackers to extract any useful statistical information. Figure 22 illustrates the histogram distribution of various images, indicating the uniformity of gray values in the results. where is the intensity level and represents the observed frequency and the expected occurrence frequency for each gray value, respectively.

For a given image in Figure 22a, the histogram is shown in 22c. After applying the proposed system's encryption algorithm, we got the encrypted image as shown in Figure 22b. The histogram of the encrypted image is shown in Figure 22d, which is fairly uniform and different from the original histogram. Therefore, the proposed system is effective against attacks and provides high security.

Subsequently, Figure 20 illustrates the image decryption scheme. Firstly, the encrypted image is XOR-ed with the z-state variable generated by the Jerk system. Then, the y-state variable is used to un-diffuse the obtained image. Finally, the x state variable is used to un-permuted the image producing the recovered image.

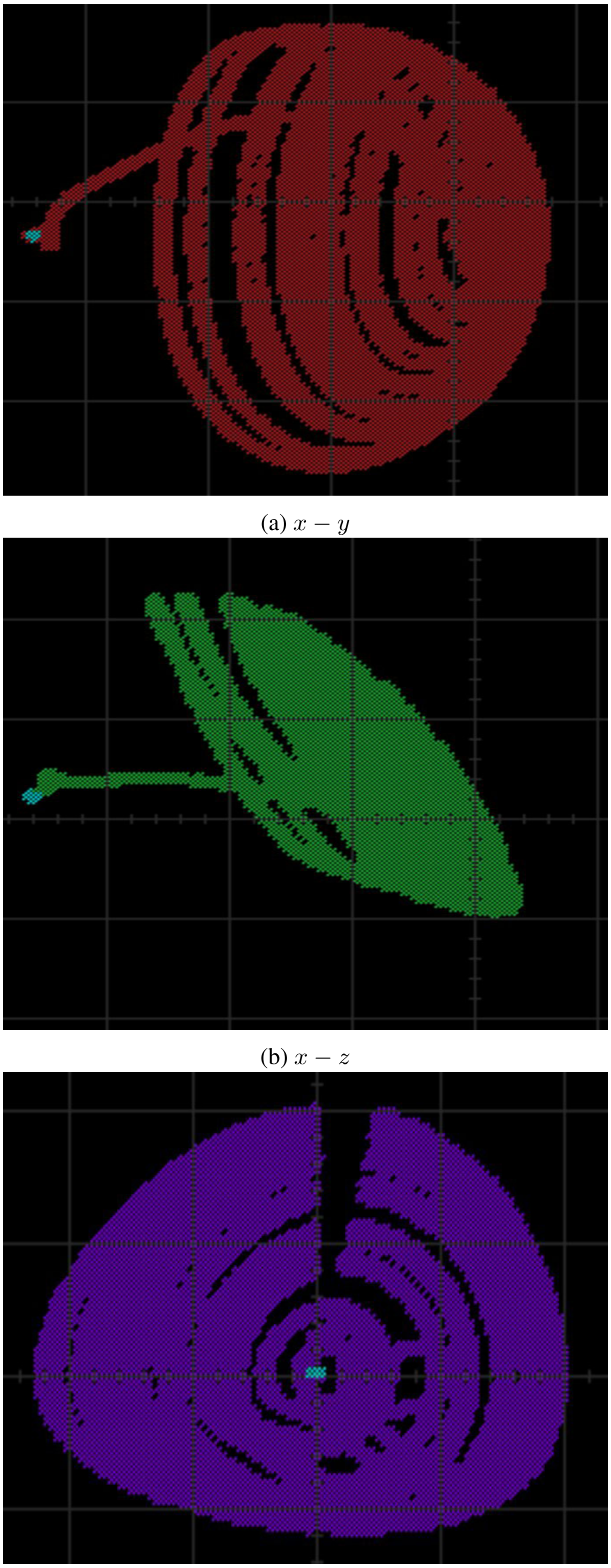
Figure 21 shows the proposed cryptography system's results on the standard cameraman image. The proposed image encryption scheme offers enhanced security features, owing to the use of the Jerk system, and is expected to find applications in various fields, such as secure communication and image processing.

2) CORRELATION

The correlation coefficient measures the degree of linear correlation between adjacent pixels in an image. Typically, plain images strongly correlate with adjacent pixels, whereas encrypted images should not exhibit any such correlation. We experimented on both the original and encrypted images and analyzed the correlation between adjacent pixels to investigate this. Figures 23a and 23b show the correlation distribution in the original and encrypted images, respectively. The correlation distribution in the original image is linear, indicating a strong correlation between adjacent pixels. In contrast, the encrypted image shows a random and scattered contribution, suggesting no correlation between pixels. Therefore, we can conclude that our cryptography system is secure against correlation analysis.

3) INFORMATION ENTROPY

Information entropy, denoted by H(X), measures the randomness or uncertainty in a data set. In image encryption, information entropy can measure the amount of randomness or unpredictability in the encrypted image. In image encryption, the original pixel values of an image are transformed to produce an encrypted image that appears random to an observer without the encryption key. The information entropy of the encrypted image is used to measure the amount of unpredictability or randomness in the encrypted image. A higher information entropy of an encrypted image indicates a higher level of security against attacks, making it more challenging for an attacker to extract useful information from


(a) $x - y$

(b) $x - z$

(c) $y - z$

FIGURE 18. Oscilloscope images of the chaotic oscillator plot from three perspectives.

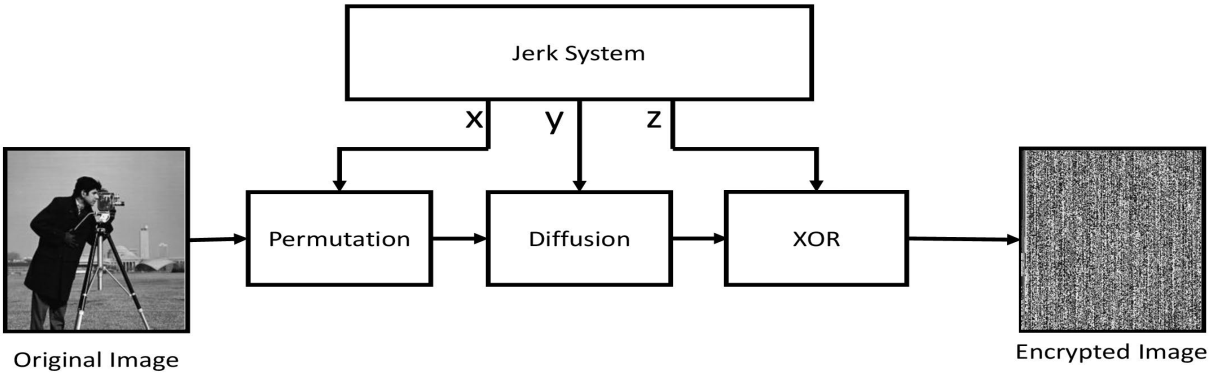


FIGURE 19. The proposed image encryption scheme using Jerk system.

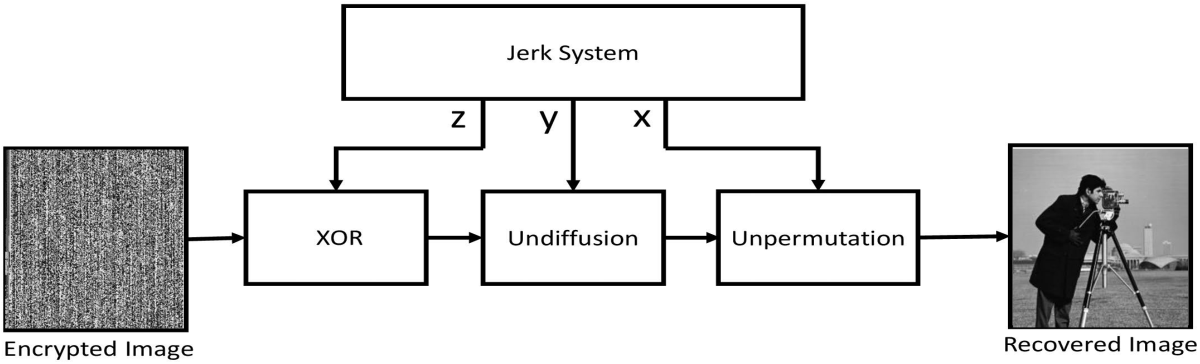


FIGURE 20. The scheme of the proposed image decipher.

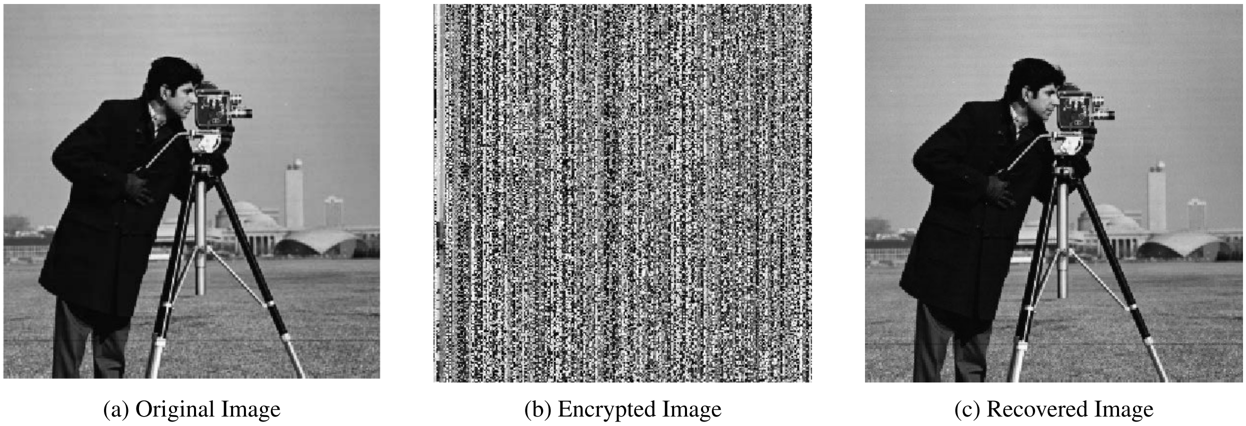
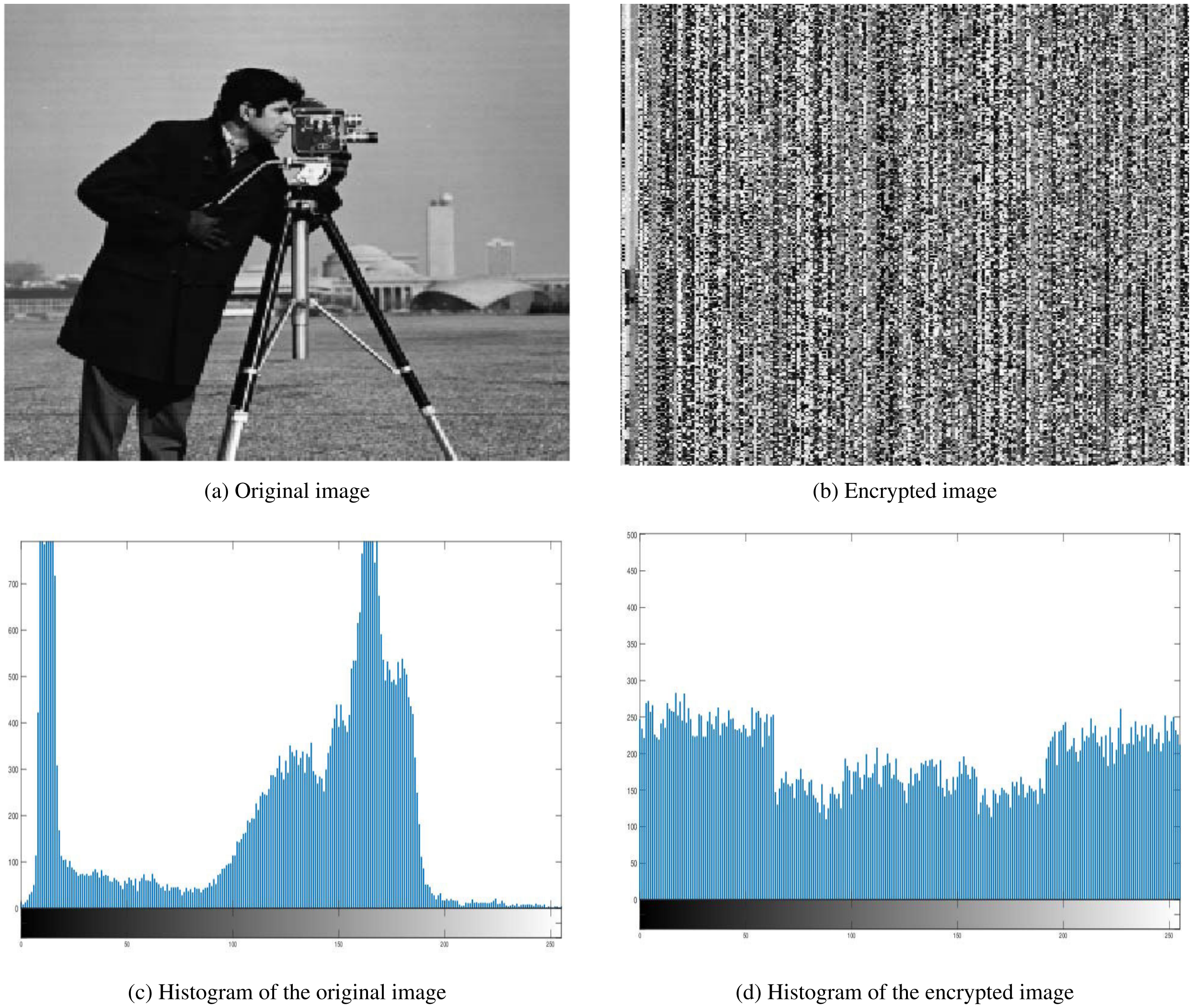

(a) Original Image (b) Encrypted Image (c) Recovered Image

FIGURE 21. The results of applying the proposed cryptography scheme on the standard cameraman image.

it. Therefore, high information entropy is desirable in image encryption schemes. The entropy of the original image is calculated to be 7.0412, whereas the encrypted image exhibits an entropy of 7.9667. It is evident from the outcomes that the entropy value of the encrypted image closely approximates the ideal value of 8. In contrast, the entropy of the unencrypted image markedly deviates from the theoretical expectation.

4) KEY SPACE ANALYSIS

Keyspace analysis is a type of cryptanalysis that examines the total number of possible encryption keys and the size of the key space to evaluate the security of an image encryption algorithm. In our proposed cryptography system, the keystream length matches that of the image, comprising 50176 values image of size 224 × 224. The vast number of potential combinations resulting from



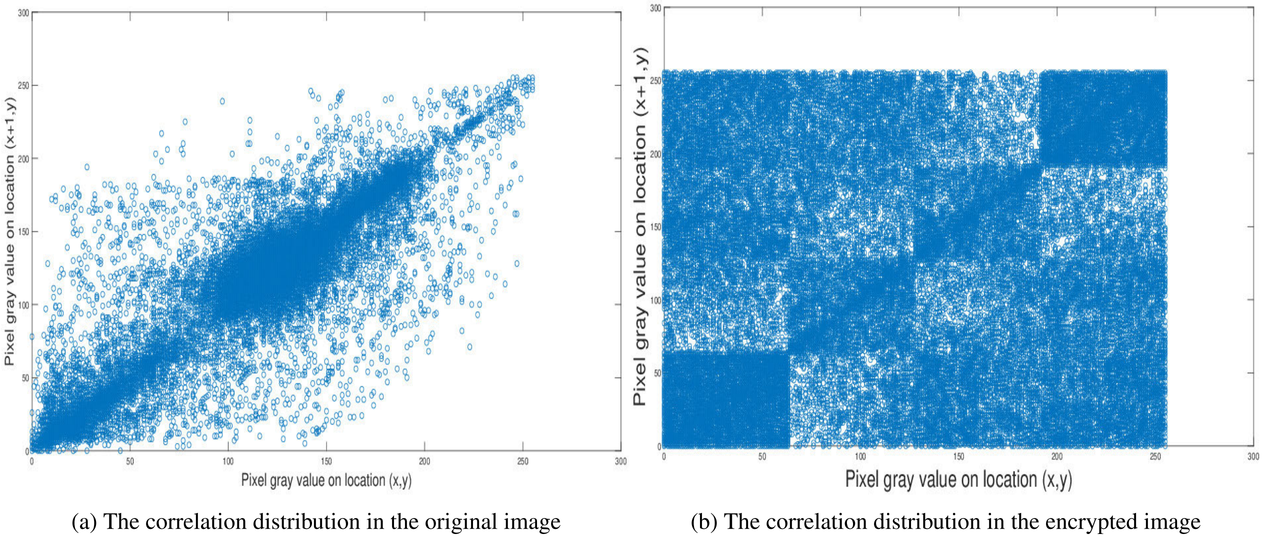
(a) Original image

(b) Encrypted image

(c) Histogram of the original image

(d) Histogram of the encrypted image

FIGURE 22. Histogram analysis for the proposed cryptography scheme.



(a) The correlation distribution in the original image

(b) The correlation distribution in the encrypted image

FIGURE 23. Correlation of two adjacent pixels in the original and encrypted images of size 224 × 224.

TABLE 4. NIST SP 800-22 tests for the x,y, and z key streams that are generated from the jerk system.

Test name	Result		
	x	y	z
Rank	Pass	Pass	Pass
Random excursions variant	Pass	Pass	Pass
Random excursions	Pass	Pass	Pass
Overlapping templates	Pass	Pass	Pass
Long runs of ones	Pass	Pass	Pass
Frequency	Pass	Pass	Pass
Block-frequency	Pass	Pass	Pass
Linear complexity	Pass	Pass	Pass
Runs	Pass	Pass	Pass
No overlapping templates	Pass	Pass	Pass
Universal statistical	Pass	Pass	Pass
Spectral DFT	Pass	Pass	Pass
Approximate entropy	Pass	Pass	Pass
Cumulative sums	Pass	Pass	Pass
Serial	Pass	Pass	Pass

this makes it difficult for a brute-force attack to pose a threat.

5) NIST

The NIST SP800-22 is a statistical test suite developed by the National Institute of Standards and Technology (NIST) for evaluating the randomness of binary sequences, such as those generated by cryptographic algorithms. The suite consists of 15 statistical tests designed to detect specific types of non-randomness or patterns in the binary sequence. This test is often used in cryptography to assess the quality and randomness of cryptographic keys, random number generators, and other cryptographic primitives. It is important to ensure that cryptographic keys and other parameters used in encryption are truly random, as attackers could exploit any predictable patterns or biases in the generated values to compromise the security of the encryption. The chaotic sequence generated by the Jerk was tested for randomness using NIST SP800-22 in Table 4, where the three random sequences generated from the jerk system have been extensively tested and found to exhibit a high degree of randomness, with no discernible patterns or correlations.

VII. CONCLUSION

In this paper, we presented a novel 3-D jerk system with three quadratic nonlinear terms and demonstrated the dynamical properties of the proposed jerk system in terms of phase portraits, bifurcation diagrams, Lyapunov exponents, multistability and coexisting attractors. For practical implementations, we designed an electronic model of the proposed 3-D jerk system using Multisim version 14.0. To demonstrate the feasibility of the proposed chaotic jerk system, we implemented the proposed jerk system using a field-programmable gate array (FPGA), which shows high throughput and low power consumption. Security analysis shows the effectiveness of our proposed algorithm in terms of high security and excellent encryption performance. Our research contributes to the ongoing efforts toward developing robust and secure image encryption techniques that can be utilized in various applications, such as secure communication and data storage.

REFERENCES

[1] T. Bonny, W. A. Nassan, S. Vaidyanathan, and A. Sambas, “Highly-secured chaos-based communication system using cascaded masking technique and adaptive synchronization,” *Multimedia Tools Appl.*, pp. 1–30, Mar. 2023. [Online]. Available: https://link.springer.com/article/10.1007/s11042-023-14643-3#article-info

[2] M. Akraam, T. Rashid, and S. Zafar, “An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers,” *Multimedia Tools Appl.*, vol. 82, no. 11, pp. 16861–16879, May 2023.

[3] H. R. Shakir, S. A. Mehdi, and A. A. Hattab, “A new four-dimensional hyper-chaotic system for image encryption,” *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1744–1756, 2023.

[4] H. Wu, Y. Zhang, H. Bao, Z. Zhang, M. Chen, and Q. Xu, “Initial-offset boosted dynamics in memristor-sine-modulation-based system and its image encryption application,” *AEU Int. J. Electron. Commun.*, vol. 157, Dec. 2022, Art. no. 154440.

[5] H. A. Abdullah and R. K. Mohammed, “FPGA-based modified chaotic system for speech transmission,” *Int. J. Speech Technol.*, vol. 25, no. 3, pp. 651–657, Sep. 2022.

[6] N. Xiao, S. Shi, H. Ouyang, and H. Yang, “Physical-layer security analysis of a quantum noise randomized cipher assisted by chaos masking,” *Opt. Fiber Technol.*, vol. 78, Jul. 2023, Art. no. 103330.

[7] M. Sadhukhan and B. M. Deb, “Quantum chaos in atoms and molecules under strong external fields,” *Theor. Chem. Accounts*, vol. 142, no. 5, p. 47, May 2023.

[8] X. Yu, H. Bao, M. Chen, and B. Bao, “Energy balance via memristor synapse in Morris–Lecar two-neuron network with FPGA implementation,” *Chaos, Solitons Fractals*, vol. 171, Jun. 2023, Art. no. 113442.

[9] F. AlMutairi and T. Bonny, “Image encryption based on Chua chaotic oscillator,” in *Proc. 3rd Int. Conf. Signal Process. Inf. Secur. (ICSPIS)*, Nov. 2020, pp. 1–4.

[10] T. Bonny, R. Al Debsi, S. Majzoub, and A. S. Elwakil, “Hardware optimized FPGA implementations of high-speed true random bit generators based on switching-type chaotic oscillators,” *Circuits, Syst., Signal Process.*, vol. 38, pp. 1342–1359, 2019.

[11] L. Wu, D. Wang, C. Zhang, and A. Mohammadzadeh, “Chaotic synchronization in mobile robots,” *Mathematics*, vol. 10, no. 23, p. 4568, Dec. 2022.

[12] L. Mastroeni and P. Vellucci, “Replication in energy markets: Use and misuse of chaos tools,” *Entropy*, vol. 24, no. 5, p. 701, May 2022.

[13] J. G. T. Ribeiro, M. Pereira, A. Cunha, and L. Lovisolo, “Controlling chaos for energy harvesting via digital extended time-delay feedback,” *Eur. Phys. J. Special Topics*, vol. 231, no. 8, pp. 1485–1490, Mar. 2022.

[14] H. Wang, G. Ke, J. Pan, and Q. Su, “Modeling, dynamical analysis and numerical simulation of a new 3D cubic Lorenz-like system,” *Sci. Rep.*, vol. 13, no. 1, Apr. 2023, Art. no. 6671.

[15] A. Singh and V. S. Sharma, “Codimension-2 bifurcation in a discrete predator–prey system with constant yield predator harvesting,” *Int. J. Biomath.*, vol. 16, no. 5, Jul. 2023, Art. no. 2250109.

[16] Q. Chen, B. Li, W. Yin, X. Jiang, and X. Chen, “Bifurcation, chaos and fixed-time synchronization of memristor cellular neural networks,” *Chaos, Solitons Fractals*, vol. 171, Jun. 2023, Art. no. 113440.

[17] H. Qiu, X. Xu, Z. Jiang, K. Sun, and C. Cao, “Dynamical behaviors, circuit design, and synchronization of a novel symmetric chaotic system with coexisting attractors,” *Sci. Rep.*, vol. 13, no. 1, Feb. 2023, Art. no. 1893.

[18] F. Yang and J. Ma, “A controllable photosensitive neuron model and its application,” *Opt. Laser Technol.*, vol. 163, Aug. 2023, Art. no. 109335.

[19] L. Ren, S. Li, S. Banerjee, and J. Mou, “A new fractional-order complex chaotic system with extreme multistability and its implementation,” *Phys. Scripta*, vol. 98, no. 5, May 2023, Art. no. 055201.

[20] T. Bonny, W. A. Nassan, and A. Baba, “Voice encryption using a unified hyper-chaotic system,” *Multimedia Tools Appl.*, vol. 82, no. 1, pp. 1067–1085, Jan. 2023.

[21] S. Bendoukha, S. Abdelmalek, and A. Ouannas, "Secure communication systems based on the synchronization of chaotic systems," in *Mathematics Applied to Engineering, Modelling, and Social Issues*, 2019, pp. 281–311. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-12232-4_9#:~:text=If%20a%20master%20chaotic%20system,make%20sense%20of%20the%20data

[22] M. Wang, X. Wang, Y. Zhang, S. Zhou, T. Zhao, and N. Yao, "A novel chaotic system and its application in a color image cryptosystem," *Opt. Lasers Eng.*, vol. 121, pp. 479–494, Oct. 2019.

[23] A. Ouannas, A. Karouma, G. Grassi, V.-T. Pham, and V. S. Luong, "A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 1873–1884, Feb. 2021.

[24] S. Hashemi, M. A. Pourmina, S. Mobayen, and M. R. Alagheband, "Design of a secure communication system between base transmitter station and mobile equipment based on finite-time chaos synchronisation," *Int. J. Syst. Sci.*, vol. 51, no. 11, pp. 1969–1986, Aug. 2020.

[25] F. Al Mutairi and T. Bonny, "New image encryption algorithm based on switching-type chaotic oscillator," in *Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA)*, Nov. 2019, pp. 1–5.

[26] T. Bonny, "Chaotic or hyper-chaotic oscillator? Numerical solution, circuit design, MATLAB HDL-coder implementation, VHDL code, security analysis, and FPGA realization," *Circuits, Syst., Signal Process.*, vol. 40, pp. 1061–1088, Aug. 2020.

[27] W. A. Nassan, T. Bonny, and A. Baba, "A new chaos-based cryptoystem for voice encryption," in *Proc. 3rd Int. Conf. Signal Process. Inf. Secur. (ICSPIS)*, Dubai, United Arab Emirates, 2020, pp. 1–4, doi: 10.1109/ICSPIS51252.2020.9340132.

[28] W. Zhou, X. Wang, M. Wang, and D. Li, "A new combination chaotic system and its application in a new bit-level image encryption scheme," *Opt. Lasers Eng.*, vol. 149, Feb. 2022, Art. no. 106782.

[29] Y. Sang, J. Sang, and M. S. Alam, "Image encryption based on logistic chaotic systems and deep autoencoder," *Pattern Recognit. Lett.*, vol. 153, pp. 59–66, Jan. 2022.

[30] H. Zhu, J. Ge, W. Qi, X. Zhang, and X. Lu, "Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system," *Math. Comput. Simul.*, vol. 198, pp. 188–210, Aug. 2022.

[31] Y. A. Kuznetsov, *Elements of Applied Bifurcation Theory*, 3rd ed. Berlin, Germany: Springer, 2004.

TALAL BONNY received the M.Sc. degree from the Technical University of Braunschweig, Germany, in 2002, and the Ph.D. degree from the Karlsruhe Institute of Technology, Germany, in 2009. He has been an Associate Professor with the Department of Computer Engineering, College of Computing and Informatics, University of Sharjah, as a Faculty Member, since 2013. His current research interests include embedded systems, hardware digital design, image processing, chaotic oscillator realizations, secure communication systems, AI and machine learning, and bioinformatics. He served as a reviewer/TPC member for many IEEE/ACM journals/conferences. He was the Session Chair of the IEEE Conference on Advances in Artificial Intelligence.

SUNDARAPANDIAN VAIDYANATHAN received the D.Sc. degree in electrical and systems engineering from Washington University in St. Louis, St. Louis, MO, USA, in 1996. He is currently a Professor and the Dean of the Research and Development Centre, Vel Tech University, Chennai, India. He has published over 550 Scopus-indexed research publications. His current research interests include linear and nonlinear control systems, chaotic and hyperchaotic systems, circuits, intelligent control, optimal control, mathematical modeling, and scientific computing.

ACENG SAMBAS received the Ph.D. degree in mathematics from Universiti Sultan Zainal Abidin (UniSZA), Malaysia, in 2020. He has been a Lecturer with the Universiti Sultan Zainal Abidin, Malaysia, and the Muhammadiyah University of Tasikmalaya, Indonesia. His current research interests include dynamic systems, chaotic signals, electrical engineering, computational science, signal processing, robotics, embedded systems, and artificial intelligence.

KHALED BENKOUIDER received the M.S. and Ph.D. degrees in automatic control from the University of Jijel, Jijel, Algeria, in 2015 and 2021, respectively. His M.S. research was on secure communications based on chaotic systems. His main research interests include dynamical systems, control systems, delayed systems, LPV systems, and chaotic systems synchronization.

WAFAA AL NASSAN received the bachelor's degree in electronic engineering from the University of Aleppo, Syria, in 2013. She is a Research Assistant with Sharjah University. Her current research focuses on modeling and simulating dynamic systems, control systems, embedded systems, information security, machine vision, and intelligent robotics.

OMAR NAQAWEH is currently pursuing the B.Sc. degree in computer engineering with the University of Sharjah, as a third-year student with a CGPA of 4.0. His work experience includes working as a Research Assistant for two months. He is very passionate about teaching, his interests include software development, hardware design using hardware description languages, and mathematics as a broad subject.