IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 24 December 2023, accepted 4 January 2024, date of publication 9 January 2024, date of current version 22 January 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3351693

RESEARCH ARTICLE

A New Hyperjerk System With a Half Line Equilibrium: Multistability, Period Doubling Reversals, Antimonotonocity, Electronic Circuit, FPGA Design, and an Application to Image Encryption

ACENG SAMBAS[1,2], MAHDAL MIROSLAV[3], SUNDARAPANDIAN VAIDYANATHAN[4], BRISBANE OVILLA-MARTÍNEZ[5], ESTEBAN TLELO-CUAUTLE[6], AHMED A. ABD EL-LATIF[1,7,8], BASSEM ABD-EL-ATTY[9], KHALED BENKOUIDER[10], AND TALAL BONNY[11]

[1]Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Campus Besut, Terengganu 22200, Malaysia
[2]Department of Mechanical Engineering, Universitas Muhammadiyah Tasikmalaya, Tasikmalaya 46196, Indonesia
[3]Department of Control Systems and Instrumentation, Faculty of Mechanical Engineering, VSB-Technical University of Ostrava, 70800 Ostrava, Czech Republic
[4]Centre for Control Systems, Vel Tech University, Vel Nagar, Avadi, Chennai, Tamil Nadu 600054, India
[5]Computer Sciences Department, Centro de Investigacion y de Estudios Avanzados del IPN (CINVESTAV), Mexico City 07360, Mexico
[6]Department of Electronics, Instituto Nacional de Astrofísica, Optica y Electronica (INAOE), Puebla 72840, Mexico
[7]EIAS Data Science Laboratory, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[8]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebeen El-Kom 32511, Egypt
[9]Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85951, Egypt
[10]Department of Electronics, Faculty of Technology, Badji-Mokhtar University, Annaba 23000, Algeria
[11]Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Aceng Sambas (acengsambas@unisza.edu.my)

This work was supported by the European Union under the REFRESH—Research Excellence For REgion Sustainability and High-Tech Industries via the Operational Program Just Transition under Project CZ.10.03.01/00/22_003/0000048. The work of Esteban Tlelo-Cuautle was supported by the CINVESTAV (Sabbatical Leave) funded by CONAHCyT-Mexico: Apoyos Complementarios para Estancias Sabáticas Vinculadas a la Consolidación de Grupos de Investigación, in 2023.

ABSTRACT A hyperjerk system pertains to a dynamical system regulated by an ordinary differential equation of nth order, where $n \geq 4$. The main contribution of this work is the finding of a new autonomous hyperjerk system with a half line equilibrium. The mathematical framework of the proposed hyperjerk system contains eight terms with an absolute function nonlinearity. The essential dynamic characteristics of the model are explored, encompassing analysis of equilibrium points and their stability, depiction of the phase trajectories, illustration of bifurcation patterns, and visualization of Lyapunov exponent graphs. Our finding shows that the new 4D hyperjerk system exhibits special behavior like multistability, period doubling reversals and antimonotonocity. The proposed hyperjerk system has been implemented with an electronic circuit using MultiSim 14.0. Moreover, the FPGA implementation of the proposed hyperjerk system is performed by applying two numerical methods: Forward Euler and Trapezoidal. Experimental attractors are given from an oscilloscope by using the Zybo Z7-20 FPGA development board, which are in good agreement with the MATLAB and MultiSim 14.0 simulations. Finally, based on the chaotic dynamical behavior of the proposed chaotic hyperjerk system, a new image encryption approach is proposed. The experimental outcomes of the presented encryption algorithm prove its efficiency and security.

INDEX TERMS Chaos, chaotic systems, HyperJerk systems, multistability, electronic circuit, FPGA design, encryption.

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

I. INTRODUCTION

A chaotic system is a nonlinear dynamic system that exhibits chaotic behavior and highly sensitive dependence on initial conditions [1]. This means that even small differences in the initial states of a chaotic system can lead to drastically different outcomes over time ([2], [3]). In other words, tiny changes in the starting conditions can lead to divergent trajectories that seem unpredictable and random, even though the system is deterministic and follows specific rules [4]. In addition, chaotic systems can be found in various fields, including physics, meteorology, biology, economics, and engineering.

An example of a renowned chaotic system is the jerk system, where the successive time derivatives of displacement in a mechanical setup encompass acceleration, velocity and jerk ([5], [6]). A traditional self-sustained Jerk system can be formulated as a third-order differential equation as follows:

$$\frac{d^3y}{dt^3} = J\left(\frac{d^2y}{dt^2}, \frac{dy}{dt}, y\right) \tag{1}$$

Here, J is referred to as the jerk function. When we extend this concept, a chaotic system with more than three dimensions (n > 3) is defined by a collection of n interconnected first-order ordinary differential equations ([7], [8]). These equations could be reformulated into a solitary nth-order ordinary differential equation, termed as a hyperjerk differential equation.

$$\frac{d^ny}{dt^n} = J\left(\frac{d^{(n-1)}y}{dt^{(n-1)}}, \frac{d^{n-2}y}{d^{n-2}t}, \ldots, \frac{dy}{dt}, y\right) \tag{2}$$

Numerous studies have documented remarkably diverse and captivating dynamic phenomena within uncomplicated hyperjerk systems. Chlouverakis and Sprott [9] introduce a selection of elementary chaotic hyperjerks with orders of 4 and 5. They investigated two scenarios that appear to be the most straightforward chaotic flows for $n = 4$, along with various instances of hyperchaotic behavior for $n = 4$ and 5. Dalkiran and Sprott [10] introduced a hyperjerk system of fourth order through the utilization of exponential nonlinear functions, supported by outcomes from numerical analysis. Furthermore, they demonstrated the practical implementation of this hyperjerk system on a FPAA. Jiang et al. [11] explored the chaotic dynamics within a hyperjerk system exhibiting antimonotonic behavior. They examined the local stability of equilibrium points and analyzed the attributes of Hopf bifurcations in the system. Moysis et al. [12] introduced a novel hyperjerk system that solely utilizes the hyperbolic sine function as the nonlinear term, along with its application in an autonomous robotic system. Vijayakumar et al. [13] introduced a quadratic hyperjerk system demonstrating bistable characteristics, and they explored the complexity of the system's attractors by employing sample entropy as a measure of complexity. Higazy and Hamed [14] investigated hyperjerk chaotic model in five dimensions, incorporating fractional-order derivatives and an active control approach. Additionally, they devised a novel reference controller to manage the introduced framework.

Motivated by the above works, we proposed a novel 4D autonomous hyperjerk system with a half line equilibrium and conduct basic analysis of its dynamical behavior like Lyapunov Exponents (LE), Bifurcation Diagram (BD) and Multistability. The numerical analyses reveal that the system's behavior, influenced by parameters and initial conditions, exhibits greater diversity and randomness. This encompasses nonlinear phenomena like multistability, reversals in period doubling, and antimonotonic tendencies.

Bifurcation analysis is a useful tool to understand the qualitative properties of chaotic systems ([15], [16]). Antimonotonicity of a dynamical system refers to the creation of period doubling followed by their annihilation via period-doubling bifurcation, which is an active research topic for chaotic systems ([17], [18]). Multistability for a nonlinear dynamical system refers to the coexistence of chaotic attractors for a fixed set of parameter values but different sets of values for the initial states of the dynamical system ([16], [19]). Furthermore, the proposed system has been implemented with electronic circuit using MultiSIM 14.0 software.

The application of a field-programmable gate array (FPGA) gives us details of the hardware resources needed for a particular FPGA implementation, and the maximum frequency of the chaotic system. Since FPGA technology allows rapid prototyping and hardware verification, this research work also shows the FPGA implementation of this new 4-D hyperjerk system and shows experimental attractors observed in an oscilloscope to verify their chaotic behavior.

Data confidentiality plays an important role in information security and image encryption ([20], [21], [22], [23]). For preserving the confidentiality of data during transmission and storage, one of the cryptographic mechanisms is used ([24], [25]). The majority of data transmitted over communication channels is visual data such as images and videos. Image encryption has become increasingly important with the rise of digital media and the need for secure transmission and storage of visual data. The objective of image encryption is to convert a plain image into an encrypted form, making it incomprehensible to unauthorized individuals [26]. In recent years, image encryption algorithms based on chaotic systems have gained significant attention due to their ability to offer robust security and effective safeguarding of sensitive image data. Chaotic systems display intricate and unpredictable behaviors, which make them suitable choices for encryption algorithms. By utilizing the inherent chaotic dynamics, these encryption schemes introduce a high level of randomness and complexity into the encryption process.

Wang et al. [27] introduced a novel method for encrypting images using a combination of Josephus traversal and mixed chaotic mapping, in which the encryption process involves three rounds of scrambling and one round of diffusion. Also, Wang et al. [28] have introduced a new method for encrypting images based on the cyclic-shift function, piece-wise linear chaotic mapping, and a combination of hash functions. The initial values are calculated using the SHA1 and MD5 hashing algorithms. Kamal et al. [29] introduced a new method for encrypting medical images based on chaotic logistic mapping, in which the scrambling process of the medial image is based on a zigzag pattern, rotation, and random permutation.

Gao [30] presented a novel 2D hyperchaotic mapping utilizing two 1D-chaotic mappings, and demonstrated its utility in image encryption. The encryption process involves scrambling the plain image through row and column shifts, followed by diffusing pixel values forward and backward. However, it is crucial to note that the effectiveness of chaos-based encryption schemes heavily relies on the choice of the chaotic system and the design of the encryption algorithm. In this context, we have proposed a new image cryptosystem based on the chaotic dynamical behavior of the presented hyperjerk system. In the context of encryption algorithm design, the efficacy of an image cryptosystem relies on its performance and resistance to various attacks. To preserve performance, the proposed encryption scheme uses simple operations like the sorted index, XOR, and substitution box, which are sufficient for good permutation and substitution processes. The experimental outcomes of the presented encryption algorithm prove its efficiency and security.

The main contributions of this paper can be listed as follows:

1) We have described the mathematical model of a new 4-D hyperjerk system and compared its Lyapunov exponents and Kaplan-Yorke dimension with two recent hyperjerk systems with a line of equilibrium points ([31], [32]).
2) We have presented a detailed bifurcation analysis of the proprosed 4-D hyperjerk system using bifurcation diagrams and Lyapunov exponents (LEs) and observed nonlinear phenomena like multistability, reversals in period doubling, and antimonotonicity.
3) We have carried out simulations of the proposed 4-D hyperjerk system using an electronic circuit designed via MultiSim.
4) We have implemented the proposed 4-D hyperjerk system in FPGA and showed experimental attractors observed in an oscilloscope to verify their chaotic behavior.
5) We have proposed a new image cryptosystem based on the proposed 4-D hyperjerk system.

The organization of this paper is described as follows. In Section II, we describe the mathematical model of hyperjerk system with a half line equilibrium. Some results of stability, Lyapunov exponents and Kaplan-Yorke dimension are investigated. In Section III, a detailed dynamical analysis of the proposed hyperjerk system is conducted. Section IV describes the electronic circuit of the proposed hyperjerk system. Section V investigates the FPGA implementation of the proposed hyperjerk system. Section VI deals with the image encryption design using the proposed hyperjerk system. Finally, the conclusions are given in Section VII.

II. A NEW HYPERJERK SYSTEM WITH A HALF LINE EQUILIBRIUM

In the chaos literature, there are a few 4-D hyperjerk systems with a line of equilibrium points ([31], [32]).

Bao et al. [31] proposed a 4-D hyperjerk system with the dynamics

$$\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = w \\ \dot{w} = (x-1)y - az - bw \end{cases} \tag{3}$$

It is easy to see that Bao hyperjerk system [31] has a line of equilibrium points

$$S_1 = \{(x, y, z, w) | y = 0, z = 0, w = 0\} \tag{4}$$

which is the x-axis in $\mathbf{R}^4$.

Bao et al. [31] showed that the system (3) has a chaotic attractor when the parameters take the values $(a, b) = (1, 0.5)$. For the initial state $X(0) = (0.02, 0.02, 0.02, 0.02)$, Bao et al. [31] calculated the Lyapunov exponents of the system (3) using Wolf's algorithm [33] as follows:

$$\begin{cases} \rho_1 = 0.0580 \\ \rho_2 = 0 \\ \rho_3 = 0 \\ \rho_4 = -0.5583 \end{cases} \tag{5}$$

The Kaplan-Yorke dimension [34] for the Bao hyperjerk system (3) is determined as follows:

$$D_{KY} = 2 + \frac{\rho_1 + \rho_2}{|\rho_3|} = 2.1039 \tag{6}$$

which shows the complexity of the Bao hyperjerk system (3).

Wang et al. [32] proposed a 4-D hyperjerk system with the dynamics

$$\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = w \\ \dot{w} = -az - bw - y(c - dx^2) \end{cases} \tag{7}$$

It is easy to see that Wang hyperjerk system [32] has a line of equilibrium points

$$S_2 = \{(x, y, z, w) | y = 0, z = 0, w = 0\} \tag{8}$$

which is the x-axis in $\mathbf{R}^4$.

Wang et al. [32] showed that the system (7) has a chaotic attractor when the parameters take the values $(a, b, c, d) = (0.8, 0.5, 1, 0.1)$. For the initial state $X(0) = (0.01, 0.01, 0, 0)$, Wang et al. [32] calculated the Lyapunov exponents of the system (7) using Wolf's algorithm [33] as follows:

$$\begin{cases} \rho_1 = 0.0357 \\ \rho_2 = 0 \\ \rho_3 = 0 \\ \rho_4 = -0.5357 \end{cases} \tag{9}$$

The Kaplan-Yorke dimension [34] for the Wang hyperjerk system (7) is determined as follows:

$$D_{KY} = 2 + \frac{\rho_1 + \rho_2}{|\rho_3|} = 2.0666 \tag{10}$$

which shows the complexity of the Wang hyperjerk system (7).

The new 4-D hyperjerk system contains eight terms and two positive constant parameters. It is described by the following dynamics:

$$\begin{cases} \dot{x} = y \\ \dot{y} = z \\ \dot{z} = w \\ \dot{w} = -x - |x| - ay - bw - xz \end{cases} \tag{11}$$

In the hyperjerk system (11), x, y, z, w are the state variables, and a and b are the positive constant parameters. When the initial conditions are chosen as (0.2, 0.2, 0.2, 0.2) and the constant parameters are selected as $a = 4$ and $b = 2$, the new system (3) exhibits a complex chaotic behavior and its phase portraits using MATLAB are depicted in Figure 1.

The equilibrium points of the hyperjerk system (11) are found by solving the equations $\dot{x} = 0$, $\dot{y} = 0$, $\dot{z} = 0$ and $\dot{w} = 0$. It is easy to see the equilibrium points of the hyperjerk system (11) are described by the set

$$S = \{(x, y, z, w) | x = -|x|, y = 0, z = 0, w = 0\}. \tag{12}$$

When $x > 0$, $|x| = x$ and the equation $x + |x| = 0$ has the unique solution $x = 0$.

When $x < 0$, $|x| = -x$ and the equation $x + |x| = 0$ is readily satisfied.

Hence, we can simplify the equilibrium set S as follows:

$$S = \{(x, y, z, w) | x \leq 0, y = 0, z = 0, w = 0\}, \tag{13}$$

which is a half-line consisting of the non-positive x-axis in R^4

We have used Wolf's approach [33] to determine the Lyapunov exponents of system (11) for the initial state (0.2, 0.2, 0.2, 0.2) and the parameter values $a = 4$ and $b = 2$. The four Lyapunov exponents of the novel 4-D system (11) were calculated as follows:

$$\begin{cases} \rho_1 = 0.1214 \\ \rho_2 = 0 \\ \rho_3 = -0.7292 \\ \rho_4 = -1.3924 \end{cases} \tag{14}$$

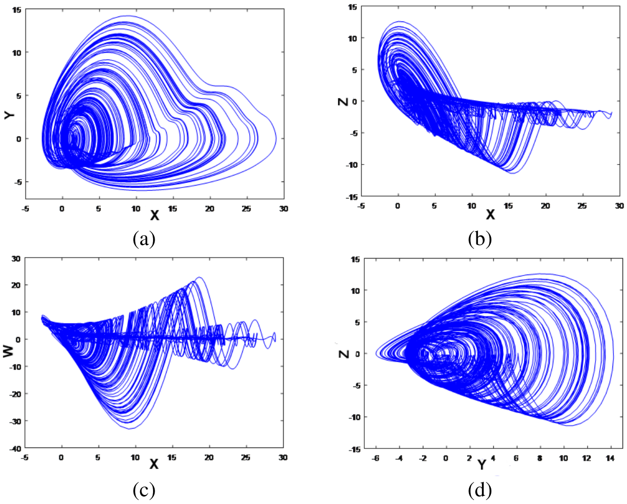
As shown in Figure 2, system (3) has: $\rho_1 > 0$, $\rho_2 = 0$, $\rho_{3,4} < 0$. This indicates that it has one positive, one zero, and two negative Lyapunov exponents and behaves chaotically. We also see that the total of the Lyapunov exponents is negative, demonstrating the dissipative nature of the suggested 4-D system (11).

The Kaplan-Yorke dimension [34] for the suggested system (11) is determined as follows:

$$D_{KY} = 2 + \frac{\rho_1 + \rho_2}{|\rho_3|} = 2.1665 \tag{15}$$

which shows the complexity of the new hyperjerk system (11).

Table 1 gives a comparison of the Lyapunov exponents (LEs), maximal Lyapunov exponent (MLE) and the Kaplan-Yorke dimension (D_{KY}) of the Bao hyperjerk system [31], Wang hyperjerk system [32] and the proposed hyperjerk system. From Table 1, it is clear that the MLE and Kaplan-Yorke dimension of the proposed hyperjerk system are greater than those of the Bao hyperjerk system [31] and Wang hyperjerk system [32]. This shows that the proposed hyperjerk system exhibits more complexity than the Bao hyperjerk system [31] and Wang hyperjerk system [32].



(a)

(b)

(c)

(d)

FIGURE 1. **Phase plots of the 4-D chaotic hyperjerk system (11): (a) $x - y$ signal plot, (b) $x - z$ signal plot (c) $x - w$ signal plot and (d) $y - z$ signal plot.**

III. DYNAMICAL ANALYSIS OF THE NEW 4-D CHAOTIC SYSTEM

A. LYAPUNOV EXPONENTS SPECTRUM AND BIFURCATION ANALYSIS

The two most crucial tools for identifying chaos in dynamical systems are the bifurcation diagram and the Lyapunov exponents spectrum. The Lyapunov exponent, as is well known, is a measurement of the exponential rates of convergence and divergence for an uncertainty on the beginning points of the trajectory. When it is positive, there is much more uncertainty, which causes trajectory divergence and the appearance of chaos. In this part, the Lyapunov exponent spectrum and bifurcation diagram are used to investigate the dynamical behaviors of the system (3) in respect to the constant parameters a and b.

TABLE 1. Comparison Table showing the Lyapunov Exponents, Maximum Lyapunov Exponent (MLE), and Kaplan Dimension for the Bao hyperjerk system [31], Wang hyperjerk system [32] and the proposed hyperjerk system (11).

Name of the System	Lyapunov exponents				MLE	Kaplan Dimension (D_{KY})
	ρ_1	ρ_2	ρ_3	ρ_4		
Bao Hyperjerk System [31]	0.0580	0	0	-0.5583	0.0580	2.1039
Wang Hyperjerk System [32]	0.0357	0	0	-0.5357	0.0357	2.0666
Proposed Hyperjerk System	0.1214	0	-0.7292	-1.3924	0.1214	2.1665

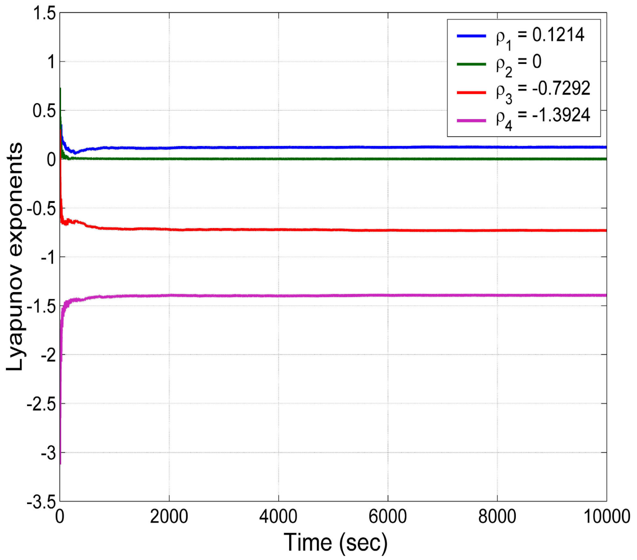


FIGURE 2. Lyapunov exponents of the new 4-D chaotic hyperjerk system (11) with $a = 4$ and b=2.

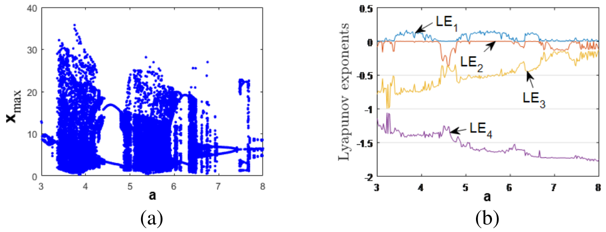
1) PARAMETER a VARYING

We fix $b = 2$ and vary a in the interval $[3, 8]$ in order to examine the sensitivity of the hyperjerk system (3) to the variation of parameter a. Lyapunov exponents spectrum and the corresponding bifurcation diagram of system (3) when a increases in the range $[3, 8]$ are depicted in Figure 3. The Lyapunov exponents spectrum and the bifurcation diagram appear in good agreement.

The simulation results reveal that the hyperjerk system (3) can exhibit diverse behaviors depending on the value of parameter a. Figure 3 shows that when a incrases, the hyperjerk 4-D system (3) can exhibit chaotic behavior with one positive Lyapunov exponent, reverse period-doubling exiting from chaos and periodic orbits with no positive Lyapunov exponent.

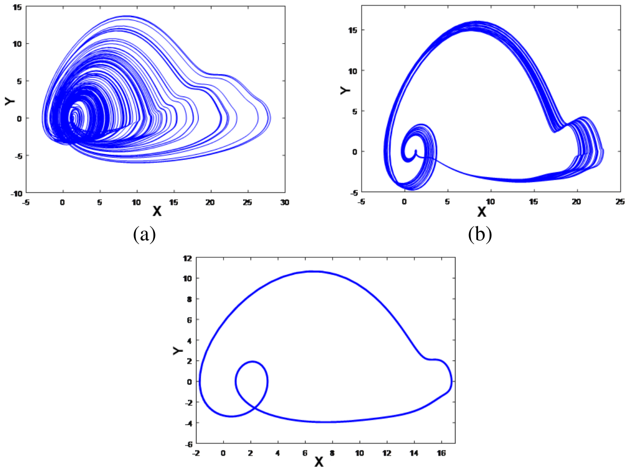
We define $A = [3.15, 3.3] \cup [3.4, 4.3] \cup [4.8, 6.1] \cup [6.3, 6.7] \cup [7.45, 7.49]$. When $a \in A$, the first Lyapunov exponent of system (3) is positive, the second one is zero, while the other two exponents are negative. Hence, in the region A, the new hyperjerk system (3) exhibits chaotic behavior with different levels of complexity according to the value of parameter a. When $a = 3.8$, the chaotic attractor of the system (3) is plotted in (x, y) plane in the Figure 4a, which has the following properties:

(a) $\rho_1 = 0.145$, $\rho_2 = 0$, $\rho_3 = -0.755$ and $\rho_4 = -1.392$.
(b) $D_{KY} = 2.192$.



(a) (b)

FIGURE 3. Phase plots of the 4-D hyperjerk system (3): (a) $x - y$ signal plot, (b) $x - z$ signal plot, (c) $x - w$ signal plot and (d) $y - z$ signal plot.



(a) (b)

(c)

FIGURE 4. Phase portraits of the new 4-D hyperjerk system (3) for different values of a: (a) $x - y$ signal plot ($a = 3.8$), (b) $x - y$ signal plot ($a = 7.47$) and (c) $x - y$ signal plot ($a = 4.5$).

When $a = 7.47$, the value of the first Lyapunov exponent decreases, providing less complexity in the system dynamics. The corresponding chaotic attractor is depicted in (x, y) plane in the Figure 4b, which has the following properties:

a) $\rho_1 = 0.012$, $\rho_2 = 0$, $\rho_3 = -0.301$ and $\rho_4 = -1.713$.
b) $D_{KY} = 2.040.$.

We define $B = [3, 3.15] \cup [3.3, 3.4] \cup [4.3, 4.8] \cup [6.1, 6.3] \cup [6.7, 7.45] \cup [7.49, 8]$. When $a \in B$, the first Lyapunov exponent is zero while the other exponents are negative. Hence, in the region B, the proposed hyperjerk system (3) generates periodic behavior. When $a = 4.5$, the periodic orbit of the system (3) is shown in (x, y) phase plane in Figure 4c, which has the following properties:

a) $\rho_1 = 0, \rho_2 = -0.253, \rho_3 = -0.450$ and $\rho_4 = -1.251$.
b) $D_{KY} = 0$..

Different attractors and dynamical behaviors for special values of a are given in Figure 4. Additionally, it is noticeable from the bifurcation diagram showed in Figure 3 that hyperjerk system (3) experiences the intriguing antimonotonicity scenario and the well-known reversal period-doubling route.

a: REVERSAL PERIOD-DOUBLING

The hyperjerk system (3) produces three independent reversal period-doubling cascades for increasing values of a as seen in the bifurcation diagram in Fig. 3. As a result, for certain regions of parameter a, we can see three cascades of the famous reverse period-doubling exit route from chaos (chaos → period-8 → period-4 → period-2 → period-1), as shown in Figure 5. The dynamical behavior for the hyperjerk system (3) with respect to various values of the parameter a can be seen in Table 1.

TABLE 2. Dynamical behavior of the hyperjerk system (3) for various values of *a*.

Parameters a	Behaviors	Figure
4.362	Chaotic attractor	Figure 6a
4.3743	Period-4 attractor	Figure 6b
4.39	Period-2 attractor	Figure 6 6c
4.4	period-1 attractor	Figure 6d (which makes and end for the first reversal period doubling)
6.02	Chaotic attractor	Figure 7a
6.1	Period-2 attractor	Figure 7b
6.2	Period-1 attractor	Figure 7c (which makes and end for the second reversal period doubling)
6.68	Chaotic attractor	Figure 8a
6.686	Period-16 attractor	Figure 8b
6.7	Period-8 attractor	Figure 8c
6.75	Period-4 attractor	Figure 8d
7	Period-2 attractor	Figure 8e
7.45	Period-1 attractor	Figure 8f (which makes and end for the third reversal period doubling)

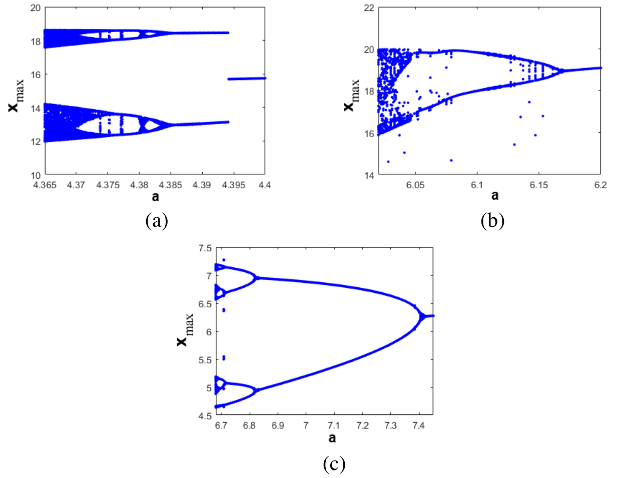


FIGURE 5. Three independents reversal period-doubling cascades exiting from chaos in the hyperjerk system (3) when parameter *a* varies: (a) *a* ∈ [4.36, 4.44], (b) *a* ∈ [6.02, 6.20] and (c) *a* ∈ [6.68, 7.45].

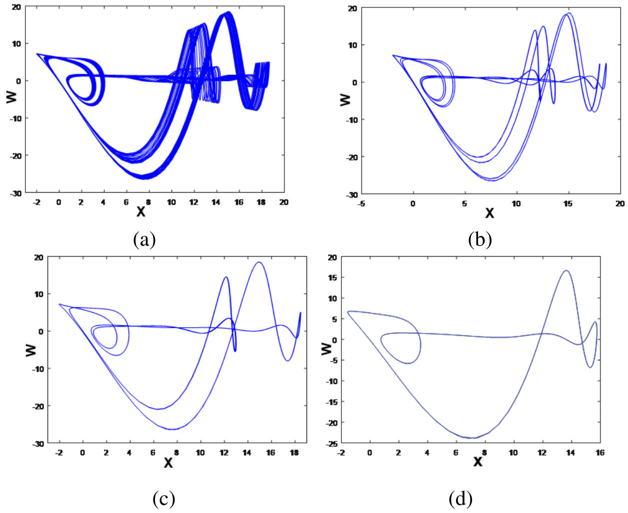


FIGURE 6. Matlab plots of the attractor in (*x*, *w*) plane show the first reversal period doubling cascade in system (3) when parameter *a* varies: (a) chaos (*a* = 4.362), (b) period-4 (*a* = 4.3743), (c) period-2 (*a* = 4.39), (d) period-1 (*a* = 4.4).

b: ANTIMONOTONOCITY

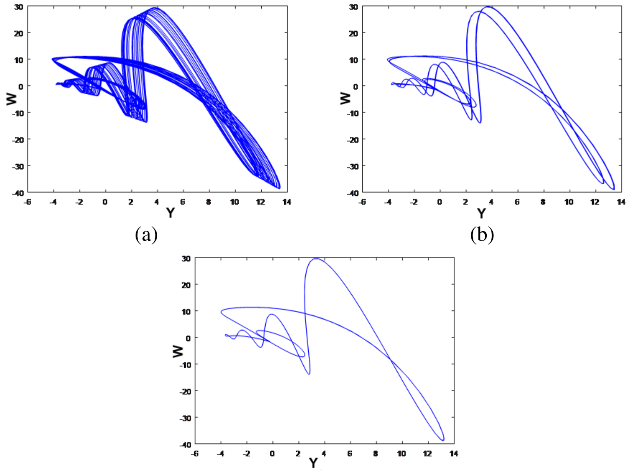
As we showed before, the hyperjerk system (3) experiences the reversal period-doubling cascade. Here, we show that the hyperjerk system (3) experiences also the famous dynamical phenomenon of antimonotonicity. As a bifurcation parameter changes, this phenomenon is described by the creation of periodic orbits via a period-doubling scenario followed by their destruction via a reverse period-doubling scenario. The antimonotonocity phenomenon is well illustrated in Fig 9, where a period-4 bubble is formed then destructed when $a \in [3.02, 3.12]$. Fig 9 is derived from the bifurcation diagram displayed in Fig 3a.

2) PARAMETER b VARYING

We fix $a = 4$ and vary b in the interval $[1, 6]$ in order to examine the sensitivity of system (3) to the variation of the parameter b. Lyapunov exponents spectrum and the corresponding bifurcation diagram of the system (3) when b increases in the range $[1, 6]$ are depicted in Figure 10. The Lyapunov exponents spectrum and the bifurcation diagram appear in good agreement.

The simulation results reveal that, when b increases, the hyperjerk 4-D system (3) can exhibit chaotic behavior with one positive Lyapunov exponent, reverse period-doubling exiting from chaos and periodic orbits with no positive Lyapunov exponent.

We define $C = [1, 1.64] \cup [1.72, 2.32] \cup [2.4, 2.5] \cup [2.56, 3]$. When $b \in C$, the first Lyapunov exponent of the hyperjerk system (3) is positive, the second one is zero, while the other two exponents are negative. Hence, in the region C, the new hyperjerk system (3) exhibits chaotic behavior with different levels of complexity according to the value of

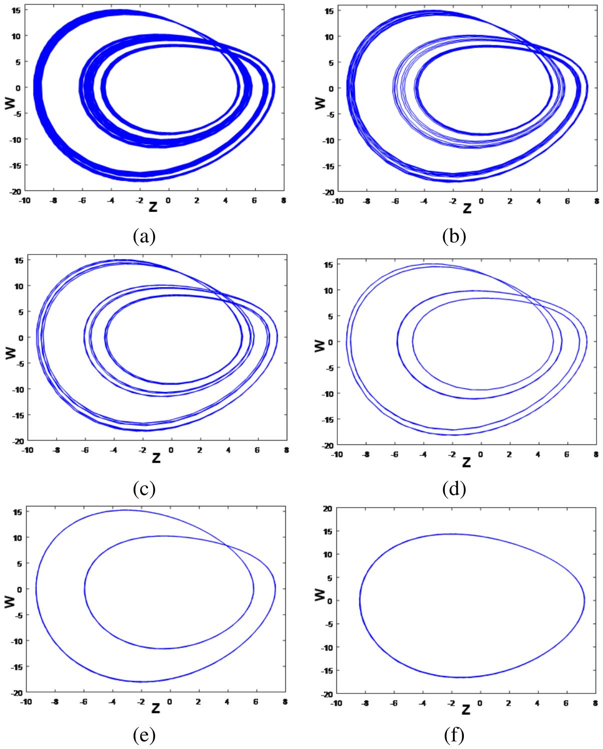


(a)

(b)

(c)

FIGURE 7. Matlab plots of the attractor in (y, w) plane show the second reversal period doubling cascade in the hyperjerk system (3) when parameter a varies: (a) chaos ($a = 6.02$), (b) period-2 ($a = 6.1$), (c) period-1 ($a = 6.2$).



(a)

(b)

(c)

(d)

(e)

(f)

FIGURE 8. Matlab plots of the attractor in (z, w) plane show the third reversal period doubling cascade in system (3) when parameter (a varies: (a) chaos (($a = 6.68$), (b) period-16 (($a = 6.686$), (c) period-8 (($a = 6.7$), (d) period-4 (($a = 6.75$), (e) period-2 (($a = 7$), (f) period-1 (($a = 7.45$).

the parameter b. When $b = 1.26$, the chaotic attractor of the system (3) is plotted in (x, z) plane in the Figure 11a, which has the following properties:

a) $\rho_1 = 0.203$, $\rho_2 = 0$, $\rho_3 = -0.517$ and $\rho_4 = -0.947$.
b) $D_{KY} = 2.392$.

When $b = 2.6$, the value of the first Lyapunov exponent decreases, providing less complexity in the system dynamics. The corresponding chaotic attractor is depicted in (x, z) plane in the Figure 11b, which has the following properties:

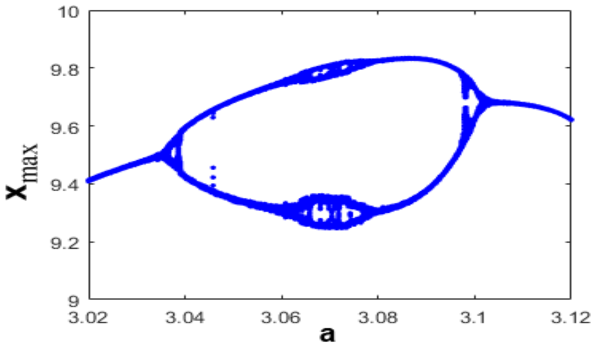


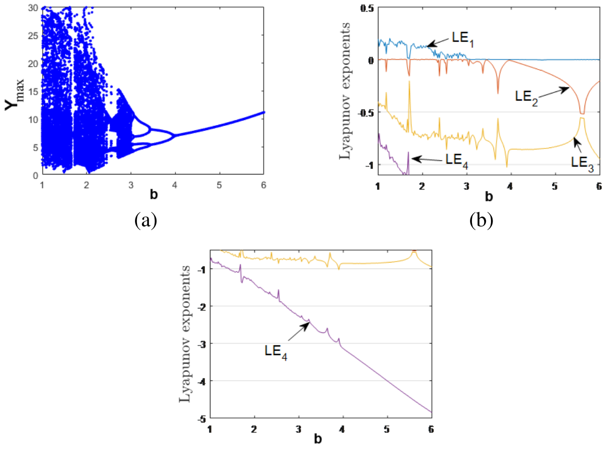
FIGURE 9. Bifurcation diagram of the hyperjerk system (1) showing period-4 bubble (Antimotonocity phenomenon) when $b = 2$ and $a \in [3.02, 3.12]$.

a) $\rho_1 = 0.018$, $\rho_2 = 0$, $\rho_3 = -0.732$ and $\rho_4 = -1.883$.
b) $D_{KY} = 2.025$.

We define $D = [1, 1.1] \cup [1.64, 1.72] \cup [2.32, 2.4] \cup [2.5, 2.56] \cup [3, 6]$. When $b \in D$, the first Lyapunov exponents is zero while the other exponents are negative. Hence, in the region D, the proposed hyperjerk system (3) exhibits a periodic orbit.

When $b = 5.5$, the periodic orbit of the system (3) in (x, z) signal plane is displayed in Figure 11c, which has the following properties:

a) $\rho_1 = 0$, $\rho_2 = -0.371$, $\rho_3 = -0.684$ and $\rho_4 = -4.446$.
b) $D_{KY} = 0$



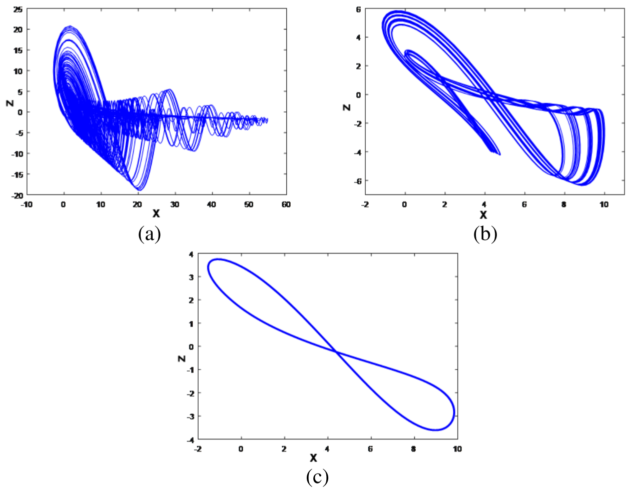
(a)

(b)

(c)

FIGURE 10. (a) Bifurcation diagram, (b) Lyapunov exponents LE_1, LE_2 and LE_3, (c) Lyapunov exponents LE_4 when $b \in [1, 6]$ and $a = 4$.

Different attractors and dynamical behaviors for special values of b are given in Figure 11. In addition, the famous reversal period-doubling route from chaos for the hyperjerk system (3) can be noticed in the bifurcation diagram shown in Figure 10.



(a) (b) (c)

FIGURE 11. Phase portraits of the new 4-D Hyperjek system (3) for different values of *a*. (a) chaotic attractor in (x, z) plane ($b = 1.26$), (b) chaotic attractor in (x, z) plane ($b = 2.6$) and (c) periodic attractor in (x, z) plane ($b = 5.5$).

a: REVERSAL PERIOD-DOUBLING

The hyperjerk system (3) produces a reversal period-doubling cascades for increasing values of b, as seen in the bifurcation diagram in Figure 10a. As a result, for a region of parameter b, we can see a cascade of the well-known reverse period-doubling exiting from chaos (chaos → period-8 → period-4 → period-2 → period-1), as shown in Figure 12. When b increases in the range [2.8, 5], the cascade of reversal period-doubling route appears as follows:

(i) When $b = 2.92$, a chaotic attractor for the system (3) is depicted in Figure 13a.

(ii) When $b = 3.02$, a period-8 attractor for the system (3) is depicted in Figure 13b.

(iii) When $b = 3.2$, a period-4 attractor for the system (3) is depicted in Figure 13c.

1) (iv)[] When $b = 3.7$, a period-2 attractor for the system (3) is depicted in Figure 13d.

(v) When $b = 5$, a period-1 attractor for the system (3) is depicted in Figure 13e, which makes and end for the reversal period doubling.

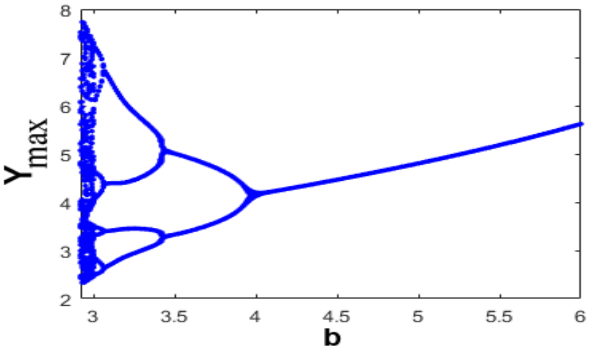
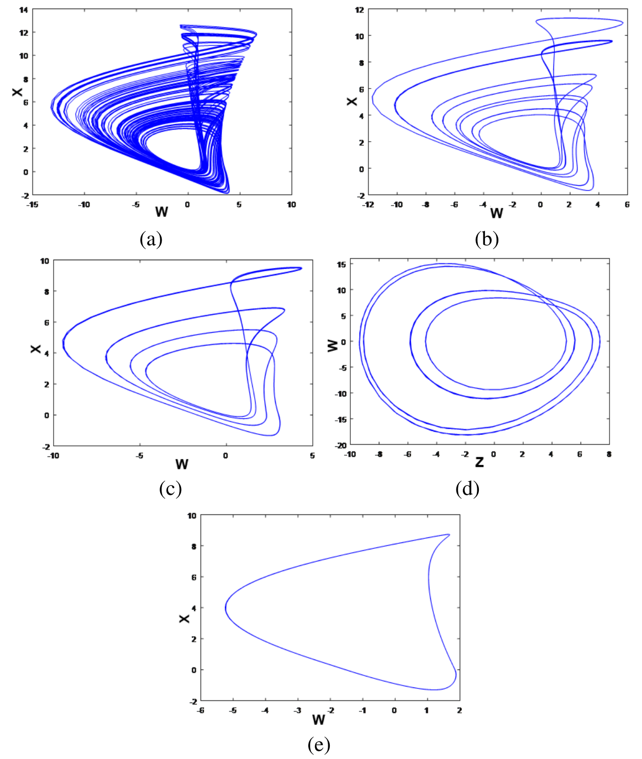


FIGURE 12. The reversal period-doubling cascades exiting from chaos in the hyperjerk system (3) when parameter $b \in [2.8, 5]$.

b: MULTISTABILITY AND COEXISTING ATTRACTORS

Coexisting attractors are two or more attractors that arise at the same time from different initial conditions [35]. This strange phenomenon is known as multistability. Let x_{01} and x_{02} represent two distinct starting points for the new hyperjerk system (3), where:

$$x_{01} = (1, 1, 1, 1) \quad \text{(Blue color)}$$
$$x_{02} = (0.2, 0.2, 0.2, -0.2) \quad \text{(Red color)}$$



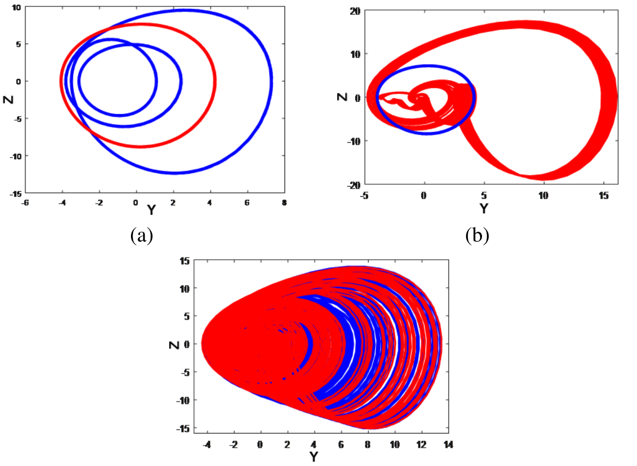
(a) (b) (c) (d) (e)

FIGURE 13. Matlab plots of the hyperjerk system (3) in the (w, x) plane show the reversal period doubling cascade when parameter *b* varies: (a) chaos ($b = 2.92$), (b) period-8 ($b = 3.02$), (c) period-4 ($b = 3.2$), (d) period-2 ($a = 3.7$), (e) period-1 ($b = 5$).

As displayed in Figure 14a, when we fix $a = 7.9$ and $b = 2$, the hyperjerk system (3) exhibits two coexisting periodic attractors. Where the blue attractor starts from x_{01} and defined by the following values of Lyapunov exponents: ρ_1=0, ρ_2=-0.011, ρ_3=-0.224, ρ_4=-1.773. The red attractor begins from x_{02} and defined by the following values of Lyapunov exponents: ρ_1=0, ρ_2=-0.110, ρ_3=-0.150, ρ_4=-1.747.

When we fix $a = 7.46$ and $b = 2$, Figure 14b shows that system (3) has coexistence of one periodic attractor and one chaotic attractor. Where the blue is the periodic attractor which starts from x_{01} and defined by the following values of Lyapunov exponents: $\rho_1 = 0$, $\rho_2 = -0.017$, $\rho_3 = -0.259$, $\rho_4 = -1.729$. The red one is the chaotic attractor which begins from x_{02} and defined by the following values of Lyapunov exponents: $\rho_1 = 0.024$, $\rho_2 = 0$, $\rho_3 = -0.333$, $\rho_4 = -1.692$.

As displayed in Figure 14c, when we fix $a = 6.35$ and $b = 2$, the hyperjerk system (3) exhibits two coexisting chaotic attractors. Where the blue attractor starts from x_{01} and defined by the following values of Lyapunov exponents: $\rho_1 = 0.089$, $\rho_2 = 0$, $\rho_3 = -0.468$ and $\rho_4 = -1.622$. The red attractor begins from x_{02} and defined by the following values of Lyapunov exponents: $\rho_1 = 0.105$, $\rho_2 = 0$, $\rho_3 = -0.452$ and $\rho_4 = -1.651$.



(a) (b)

(c)

FIGURE 14. Numerical phase plots of various coexisting attractors of the hyperjerk system (3) in the (y, z) plane: (a) the coexisting periodic attractors, (b) coexistance of periodic and chaotic attractors, (c) the coexisting chaotic attractors.

IV. ELECTRONIC CIRCUIT

To explore the behaviors and validate the viability of a theoretical chaotic model, it's a common practice to employ circuitry that replicates their associated mathematical models. Utilizing electronic circuits to mimic chaotic systems is advantageous due to their widespread utility in engineering applications ([36], [37], [38]). Therefore, in this section, we create and validate the electronic circuitry for the novel chaotic Hyperjerk system (3). The utilization of standard electronic elements such as resistors, capacitors, analog multipliers, and operational amplifiers allows for the realization of the system.

By employing Kirchhoff's laws to the electronic circuit, the set of circuit state equations corresponding to the newly introduced chaotic system can be formulated as follows:

$$\begin{cases} C_1\dot{x} = \dfrac{1}{R_1}y \\ C_2\dot{y} = \dfrac{1}{R_2}z \\ C_3\dot{z} = \dfrac{1}{R_3}w \\ C_4\dot{w} = -\dfrac{1}{R_4}x - \dfrac{1}{R_5}\left|x\right| - \dfrac{1}{R_6}y - \dfrac{1}{R_7}w - \dfrac{1}{10R_8}xz \end{cases} \tag{16}$$

The determined values of each electronic component in Figure 15 are as outlined as follows: $R_1 = R_2 = R_3 = R_4 = R_5 = 400\,k\Omega$, $R_7 = 200\,k\Omega$, $R_8 = 40\,k\Omega$, $R_6 = R_9 = R_1 0 = R11 = R_{12} = R_{13} = R_{14} = R_{15} = R_{16} = R_{17} = R_{18} = R_{19} = 400\,k\Omega$, $C_1 = C_2 = C_3 = C_4 = 1$ nF. The simulation results, which are oscilloscope, are shown in Figure 16. Evidently, the simulation outcomes of the circuit's state equation (Eq. 16), as shown in Figure 16, closely resemble the theoretical numerical phase trajectories display in Figure 7.

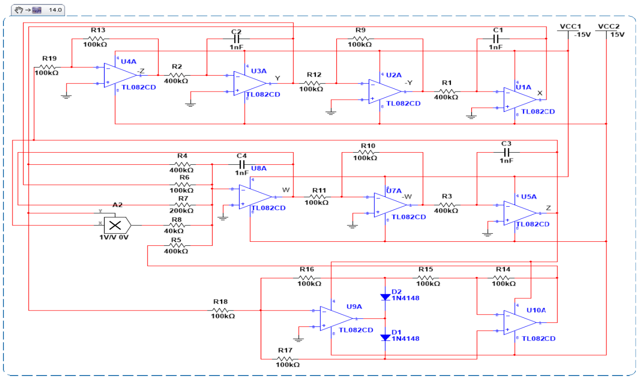
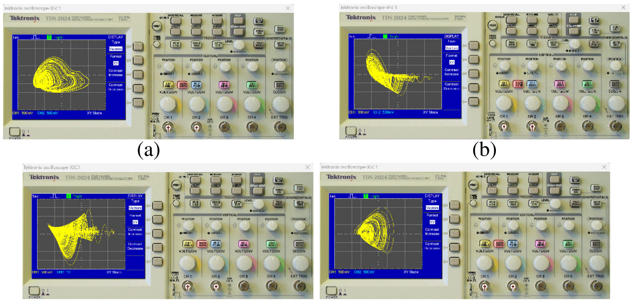


FIGURE 15. Electronic circuit of the Hyperjerk system using MultiSIM 14.0.



(a) (b)

(c) (d)

FIGURE 16. Chaotic attractor of novel HyperJerk system using MultiSIM 14.0.

V. FPGA IMPLEMENTATION

By applying the Forward Euler method, we obtain the discretized equations of the hyperjerk system (3) as given in (17). Similarly, by applying the trapezoidal method, the discretized equations of the hyperjerk system (11) can be obtained. Usually, explicit methods such as the Forward Euler method are applied to numerically solve the hyperjerk system (17) [39]. Other numerical methods such as Runge-Kutta method can be also used to perform the FPGA implementation, but some issues must be taken into consideration, as discussed in [40]. In this work, we use the parameter values as $(a, b) = (4, 2)$ with the initial state $(0.2, 0.2, 0.2, 0.2)$, and the time-step for the iteration scheme is taken as $h = 0.001$.

$$\begin{aligned} x_{n+1} &= x_n + \frac{h}{2}(y_n + y_{n+1}) \\ y_{n+1} &= y_n + \frac{h}{2}(z_n + z_{n+1}) \\ z_{n+1} &= z_n + \frac{h}{2}(w_n + w_{n+1}) \\ w_{n+1} &= w_n + \frac{h}{2}(-x_n - |x_n| - ay_n - bw_n - x_n z_n \\ &\qquad - x_{n+1} - |x_{n+1}| - ay_{n+1} - bw_{n+1}) \end{aligned} \tag{17}$$

The FPGA implementation is performed from the block description of the discretized equations, for example: by applying forward Euler method, the block description of (7) is shown in Fig. 17. One can see the four state variables, the step-size h, and the coefficients a and b. Multipliers and adders can be easily seen and the registers and multiplexers help to reuse hardware resources. The absolute value of variable x is described by block ABS. Observing (7), 11 multiplications must be performed. One multiplier is needed to evaluate each state variable xn+1, y_{n+1}, and z_{n+1}. However, calculating w requires eight multiplications. The block description shown in Fig. 17, includes a reordering in the execution of the operations, as well as a precomputation of new constants to consume just two clock cycles to evaluate an iteration.

To control the iterations, we implemented a finite state machine (FSM) in our work. In this manner, five states were defined: IDLE, STEP1, STEP2, LOAD, and STOP. The control signals are: sel0, which controls the first column of multiplexers to define whether it is an input or feedback; sel1, which controls the second column of multiplexers and selects the input of each multiplier; newout, the signal that indicates that there is a new valid value and that it will be output from the entity; finally, the load signal, which when active enables the loading of a new value in the input registers to the circuit. The IDLE state sets all signals to logic ‘0’ and waits for the start = ‘1’ signal to pass to the STEP1 state. The STEP1 state sets sel1 = ‘1’ and unconditionally transitions to the STEP2 state. The STEP2 state sets sel1 = ‘0’ and unconditionally transitions to the LOAD state. LOAD activates load = ‘1’, sel0 = ‘1’ and newout = ‘1’ and unconditionally transits to the STOP state. This last state verifies the signal start = ‘1’ to transit to the STEP1 state. Otherwise it remains in the same state, and also changes newout = ‘0’ and load = ‘0’. The FPGA design was coded in hardware descriptive language (VHDL). For the implementation, the Vivado tool of Xilinx was used. Each arithmetic unit (multipliers, adders and subtractor) is in the standard fixed-point arithmetic representation using 32-bits. Table 3 provides a summary of the hardware resources of the FPGA implementation.

TABLE 3. Hardware resources for the design of the hyperjerk system (3) using the FPGA Xilinx Zybo Z7-20 (X C 7Z 020C L G 400-1).

Resources	Used	Available
LUTs	701	98.78%
FFs	292	99.72%
DSPs	10	95.45%
Frequency Max	111 MHz	–

Figure 18 shows the experimental chaotic time series of each state variable.

Figure 19 displays the phase plots of the discretized hyperjerk system (17).

Finally, Figure 20 shows the experimental setup and design of the FPGA Zybo Z7-20 (XC7Z020CLG400-1).

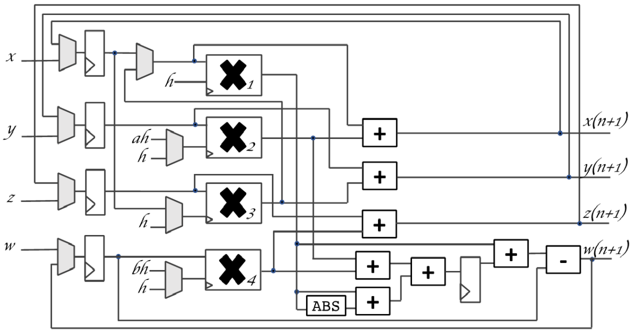


FIGURE 17. Block diagram of the proposed new discretized hyperjerk system (17).

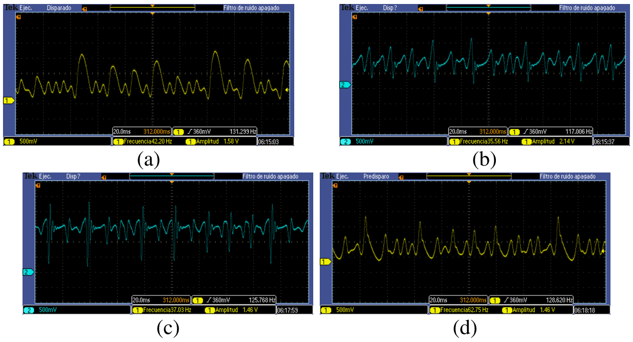

(a)
(b)
(c)
(d)

FIGURE 18. Chaotic attractor of novel HyperJerk system using MultiSIM 14.0.

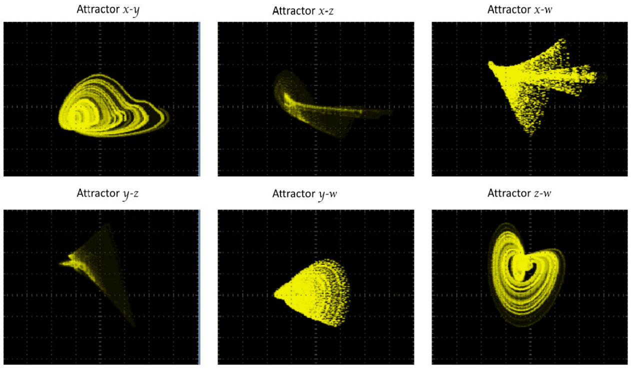


FIGURE 19. Experimental views for the hyperchaotic attractors, by setting α=4, b=2, initial conditions (0.2, 0.2, 0.2, 0.2), and time-step h=0.001.

VI. APPLICATION TO IMAGE ENCRYPTION

In this section, we propose a new image encryption technique based on the proposed hyperjerk system. The effectiveness of an image cryptosystem relies on its performance and resistance to various attacks. These two crucial properties determine the system’s ability to encrypt images efficiently and securely. In this context, the proposed encryption method uses simple operations like the sorted index, XOR, and substitution box, which are sufficient for good permutation and substitution processes. To preserve the plain image sensitivity of the presented encryption algorithm, the SHA-256 hash algorithm is executed on the plain image, and the resulting hash code is employed for updating the original conditions of the 4-D HyperJerk system. The 4-D HyperJerk system is solved using the Runge-Kutta fourth-order method for generating four chaotic sequences $\{X\}$, $\{Y\}$, $\{Z\}$, and $\{W\}$ each of length mn, in which mn represents the dimension of the plain image. The sequence $\{X\}$ is employed for performing the permutation process of the encryption algorithm, while the sequences $\{Y\}$ and $\{Z\}$ are utilized to construct an 8×8 substitution box (S-box) for substituting the permutated image. Finally, the sequence $\{W\}$ is applied to perform the bitwise XOR operation on the substituted image for generating the final cipher image. The encryption process is outlined in Figure 21 and the pseudocode for the encryption algorithm is provided in Algorithm 1, whereas detailed steps of the encryption procedure are given in the following lines.

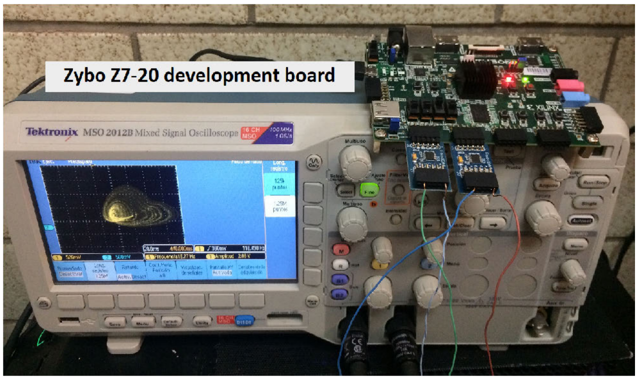

Zybo Z7-20 development board
Tektronix MSO 2012B Mixed Signal Oscilloscope

FIGURE 20. Experimental setup using FPGA Zybo Z7-20 (XC7Z020CLG400-1).

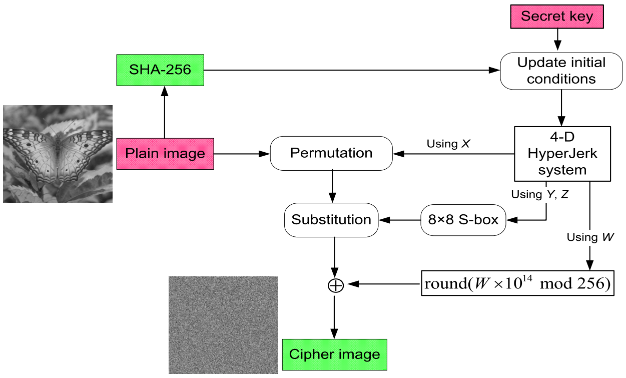


FIGURE 21. General steps of the presented encryption approach.

Step 1: Choice control parameters and initial conditions as a secret key ($x_{initial}, y_{initial}, z_{initial}, w_{initial}, a, b$).

Step 2: Perform a SHA256 hashing algorithm on the pristine image (I) for generating 256 bits, and transform these bits into 32 integers ($t_1, t_2, \ldots, t_{32}$) each 8-bit, then update the initial conditions ($x_{initial}$, $y_{initial}, z_{initial}$, and $w_{initial}$) using $t_1, t_2, \ldots$, and t_{32} as stated in the following equations.

$$d1 = \frac{1}{2048}\sum_{j=1}^{8} t_j \tag{18}$$

$$d2 = \frac{1}{2048}\sum_{j=9}^{16} t_j \tag{19}$$

$$d3 = \frac{1}{2048}\sum_{j=17}^{24} t_j \tag{20}$$

$$d4 = \frac{1}{2048}\sum_{j=25}^{32} t_j \tag{21}$$

$$x_{new} = (x_{initial} + d1)/2 \tag{22}$$

$$y_{new} = (y_{initial} + d2)/2 \tag{23}$$

$$z_{new} = (z_{initial} + d3)/2 \tag{24}$$

$$w_{new} = (w_{initial} + d4)/2 \tag{25}$$

Step 3: Utilizing the updated initial conditions and the selected control parameters (x_{new}, y_{new}, z_{new}, w_{new}, a, b) solve the 4-D HyperJerk system by Runge Kutta fourth-order method for generating four chaotic sequences $\{X\}$, $\{Y\}$, $\{Z\}$, and $\{W\}$ each of length $m \times n$ representing the dimension of the plain image.

Step 4: Arrange the components of the sequence $\{X\}$ from the smallest to the largest as sequence A, and obtain the index of each component of A in X as a vector B.

Step 5: Transform the pristine image I to a one vector IV, and permute IV by vector B as stated below:

$$IPV\ (j) = IV\ (B\ (j))\,,$$

for $j = 1$ to $m \times n$.

Step 6: To construct an S-box 8×8, add the elements of $Y(20 : 275)$ to the elements of $Z(200 : 455)$ as a sequence Q, arrange the components of Q from the smallest to the largest as a sequence D, and obtain the index of each component of D in Q as S-box SB.

Step 7: Substitute the permutated image vector IPV using SB sequence as stated below:

$$ISV\ (j) = SB\ (IPV\ (j) + 1) - 1$$

for $j = 1$ to $m \times n$.

Step 8: Convert $\{W\}$ sequence into integers in the range of 0 to 255, and then perform a bitwise XOR operation on the generated integer sequence and the ISV sequence.

$$K = round(W \times 10^{14}\ mod\ 256) \tag{26}$$

$$CV = ISV \oplus K \tag{27}$$

Step 9: Transform the sequence CV into a matrix to generate the final cipher image C.

$$C = reshape\ (CV, m, n) \tag{28}$$

VII. EXPERIMENTAL RESULTS

For evaluating the performance of the presented image encryption approach, we employed a laptop with 6.0 GB of RAM and an Intel Core^{TM} i5 CPU 2.5 GHz and equipped with MATLAB R2016b. The utilized dataset of test images consists of four standard gray-scale images with dimensions

Algorithm 1 Pseudocode for the Encryption Algorithm

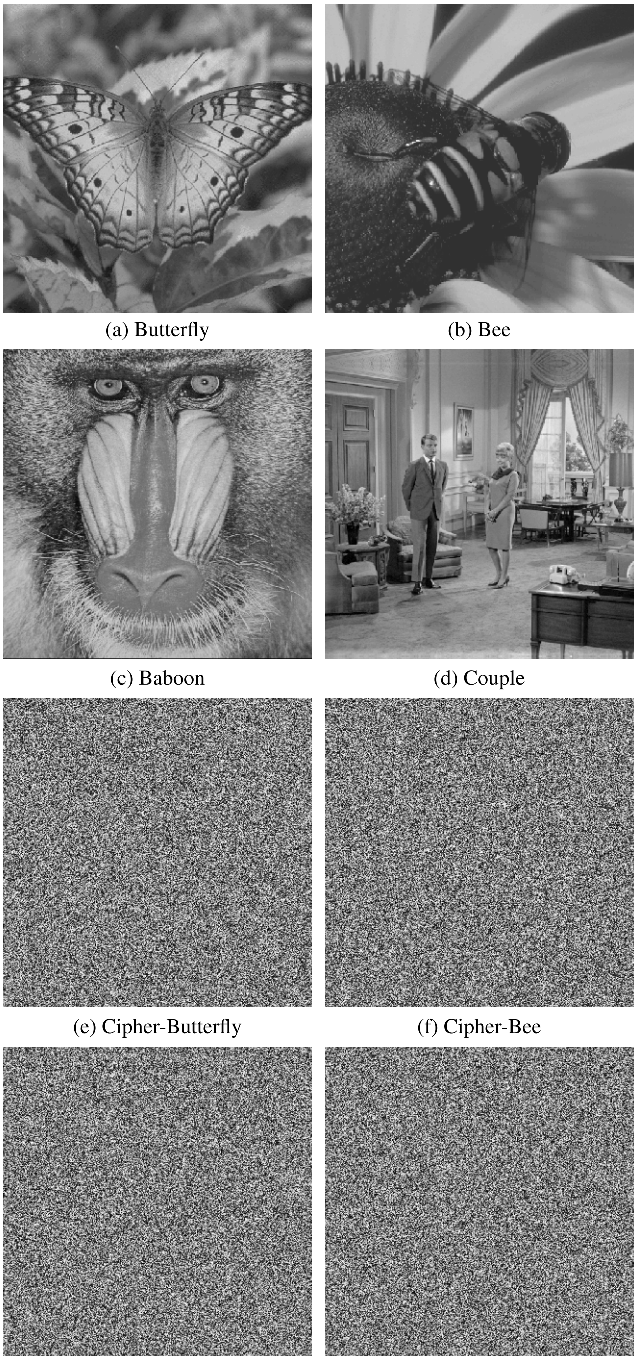
```
parameter: $x_{initial}, y_{initial}, z_{initial}, w_{initial}, a, b$
Input: Pristine image ($I$)
Output: Cipher image ($C$) and some information about pristine image ($d1, d2, d3, d4$)
$[m \;\; n] \leftarrow size(I)$// Obtain the size of $I$
$T \leftarrow SHA256\,(I)$// Get the hash code for $I$
$t \leftarrow uint8(T)$// Transform each 8-bit of $T$ into an integer value $t_i$
// Transform the integers ($t_1$, $t_2$, ..., $t_{32}$) into four decimal values ($d1$, $d2$, $d3$,
    $d4$)
$d1 \leftarrow \frac{1}{2048}\sum_{j\leftarrow 1}^{8} t_j$
$d2 \leftarrow \frac{1}{2048}\sum_{j\leftarrow 9}^{16} t_j$
$d3 \leftarrow \frac{1}{2048}\sum_{j\leftarrow 17}^{24} t_j$
$d4 \leftarrow \frac{1}{2048}\sum_{j\leftarrow 25}^{32} t_j$
$x_{new} \leftarrow (x_{initial} + d1)/2$// Update $x_{initial}$ using $d1$
$y_{new} \leftarrow (y_{initial} + d2)/2$
$z_{new} \leftarrow (z_{initial} + d3)/2$
$w_{new} \leftarrow (w_{initial} + d4)/2$
$[X \;\; Y \;\; Z \;\; W] \leftarrow 4DHyperJerkSystem\,(x_{new}, y_{new}, z_{new}, w_{new}, a, b, mn)$// Solve the 4-D HyperJerk system
    by Runge Kutta fourth-order method for generating four chaotic sequences $\{X\}$,
    $\{Y\}$, $\{Z\}$, and $\{W\}$ each of length $m \times n$ representing the dimension of the plain
    image.
$A \leftarrow sort(X, ascending)$// Sort the components
$B \leftarrow index(A\ in\ X)$// Obtain the index of each component
$IV \leftarrow reshape(I, 1, mn)$// Transform the pristine image $I$ to a one vector $IV$
// Permutation of $IV$ using $B$ sequence
for $j \leftarrow 1 : mn$ do
    $IPV\,(j) \leftarrow IV\,(B\,(j))$
// Constructing an S-box $8 \times 8$
$Q \leftarrow Y(20:275) + Z(200:455)$// Add the elements of $Y(20:275)$ to the elements of
    $Z(200:455)$
$D \leftarrow sort(Q, ascending)$
$SB \leftarrow index(D\ in\ Q)$
// Substituting the permutated image vector $IPV$ using $SB$
for $j \leftarrow 1 : mn$ do
    $ISV\,(j) \leftarrow SB\,(IPV\,(j) + 1) - 1$
$K \leftarrow round(W \times 10^{14}) \mod 256$// Convert $\{W\}$ sequence into integers in the range of
    0 to 255
$CV \leftarrow ISV \oplus K$// Perform the bitwise XOR operation
$C \leftarrow reshape(CV, m, n)$// Cipher image $C$
```

512×512 and labeled as Butterfly, Bee, Baboon, and Couple (see Figure 22). The selected control parameters and original conditions for solving the 4-D HyperJerk system are set as: $x_{initial}$=0.2, $y_{initial}$=0.2, $z_{initial}$=0.2, $w_{initial}$=0.2, a=4, and b=2.

The effectiveness of an image cryptosystem relies on its performance and resistance to various attacks. These two crucial properties determine the system's ability to encrypt images efficiently and securely. In this context, performance refers to how quickly an image can be encrypted on a given computer, while resistance to attacks involves withstanding attacks such as brute force, differential cryptoanalysis, statistical cryptoanalysis, and others. These properties will be discussed in the following subsections to demonstrate the effectiveness of the image encryption algorithm being presented.

A. TIME EFFICIENCY

The speed at which an image can be encrypted or decrypted plays a crucial role, especially when dealing with large image files or real-time applications. To showcase the efficiency of the introduced cryptosystem regarding encryption speed, Table 4 provides a brief comparison of time encryption between the proposed cryptosystem and other relevant encryption algorithms reported in [27], [28], [41], and [42].


(a) Butterfly

(b) Bee

(c) Baboon

(d) Couple

(e) Cipher-Butterfly

(f) Cipher-Bee

(g) Cipher-Baboon

(h) Cipher-Couple

FIGURE 22. Dataset of test images in which the upper row denotes the plain images and the lower row denotes the ciphered images.

Based on the details presented in Table 4, it can be inferred that our cryptosystem excels in terms of time encryption compared to others.

TABLE 4. Comparison of time encryption (in s) between the proposed cryptosystem and other relevant encryption algorithms reported in [27], [28], [41], [42].

Mechanism	Image size		
	256×256	512×512	1024×1024
Proposed	0.234	0.843	3.375
Ref. [41]	0.393	1.358	5.136
Ref. [42]	2.637	-	-
Ref. [28]	1.172	-	-
Ref. [27]	1.243	-	-

B. CORRELATION ANALYSIS

One of the most important tools for evaluating the meaning of an image is its correlation coefficient between neighboring pixels (CC). Normal images have CC values near one in each direction, while cipher images should have CC values near zero. To calculate the values of CC for the original and ciphered images, we randomly picked 10,000 pairs of neighboring pixels. CC can be expressed as stated in Eq. (29).

$$CC = \frac{\sum_{j=1}^{R}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{j=1}^{R}(x_i - \bar{x})^2 \sum_{j=1}^{R}(y_i - \bar{y})^2}} \tag{29}$$

here x and y are the intensity values of two adjacent pixels, and R points to the number of adjacent pixels. Table 5 displays the CC results for the ciphered images and their corresponding plain ones, in which the values of the cipher images are close to 0. Also, Figure 23 states the correlation distribution per direction for the Butterfly image and its ciphered one. From the values stated in Table 5 and the information displayed in Figure 23, no useful data was gained about the ciphered image by analyzing the correlation.

TABLE 5. ***CC*** **outcomes.**

image	Direction		
	H	V	D
Butterfly	0.9504	0.9587	0.9316
Cipher-Butterfly	0.0003	0.0004	0.0002
Bee	0.9839	0.9829	0.9741
Cipher-Bee	0.0007	0.0004	-0.0005
Baboon	0.7589	0.8672	0.7311
Cipher-Baboon	-0.0006	-0.0007	0.0013
Couple	0.9523	0.9471	0.9102
Cipher-Couple	0.0015	0.0007	-0.0001

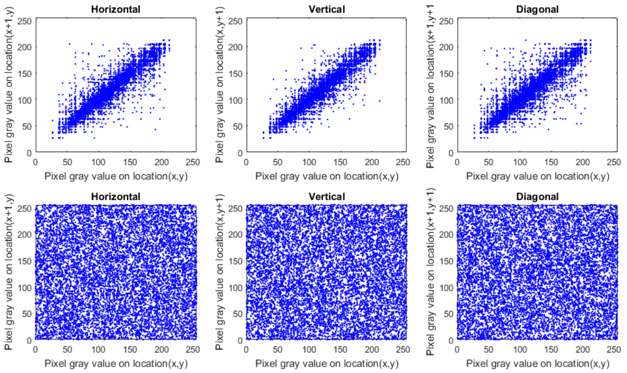


FIGURE 23. Correlation distribution for Butterfly image, in which the upper row represents the plain version and the lower row represents the ciphered version of the image.

C. PLAIN IMAGE SENSITIVITY

Plain-image sensitivity points to any minor changes in the plain image leading to huge variations in the ciphered image. To evaluate the plain-image sensitivity for the presented encryption algorithm, two measures are employed: NPCR (“Number of Pixel Change Rate”) and UNCI (“Unified Average Changing Intensity”), which are defined as follows:

$$NPCR = \frac{\sum_{x;y} Df(x,y)}{R} \times 100\%,$$
$$Df(x,y) = \begin{cases} 0 \ if \ \ Cip1(x,y) = Cip2(x,y) \\ 1 \ if \ \ Cip1(x,y) \neq Cip2(x,y) \end{cases} \tag{30}$$
$$UACI = \frac{1}{R}\left(\sum_{x,y} \frac{|Cip(x,y) - Cip(x,y)|}{255}\right) \times 100\% \tag{31}$$

where $Cip1$ and $Cip2$ indicate two encrypted images for one plain image, which varies by one bit, and R signifies the full number of image pixels. The values of NPCR and UNCI are displayed in Table 6, which proves the proposed cryptosystem’s high sensitivity to small changes in the plain image.

TABLE 6. UACI and NPCR results.

Image	UACI %	NPCR %
Butterfly	33.390495	99.611282
Bee	33.492745	99.627686
Baboon	33.426132	99.618530
Couple	33.455812	99.612808

D. HISTOGRAM ANALYSIS

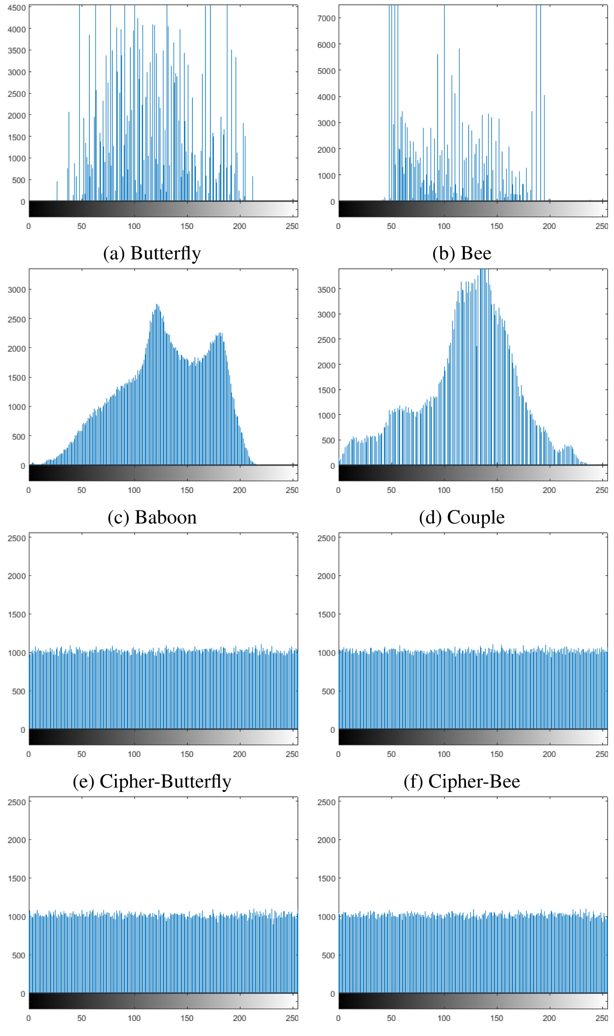
In order to estimate the distribution of pixel values in cipher images, the histogram measure is utilized. A reliable encryption approach should ensure that the distribution remains consistent across different ciphered images. Figure 24 displays the histograms of the experimented images, in which the histograms of the pristine images are dissimilar and those of their respective encrypted counterparts are uniform. Therefore, the suggested encryption approach is capable of withstanding histogram analysis attacks.

E. ENTROPY ANALYSIS

The entropy test is used to assess the bit distribution per level of the image’s pixel values, which is expressed mathematically as follows:

$$E(X) = -\sum_{j=0}^{255} p(x_j)\log_2\left(p(x_j)\right) \tag{32}$$

where $p(x_j)$ is the probability of x_j. The probable values of a grayscale image are 2^8, so the ideal entropy is 8 bits. As a result, the entropy of the encrypted images must be near 8. Table 7 shows the results of the information entropy for each image tested, where all the information entropy values for encrypted images are near 8 bits. As a result of this, the given cryptosystem is resistant to entropy assaults.



(a) Butterfly
(b) Bee
(c) Baboon
(d) Couple
(e) Cipher-Butterfly
(f) Cipher-Bee
(g) Cipher-Baboon
(h) Cipher-Couple

FIGURE 24. Histogram test.

TABLE 7. Information entropy.

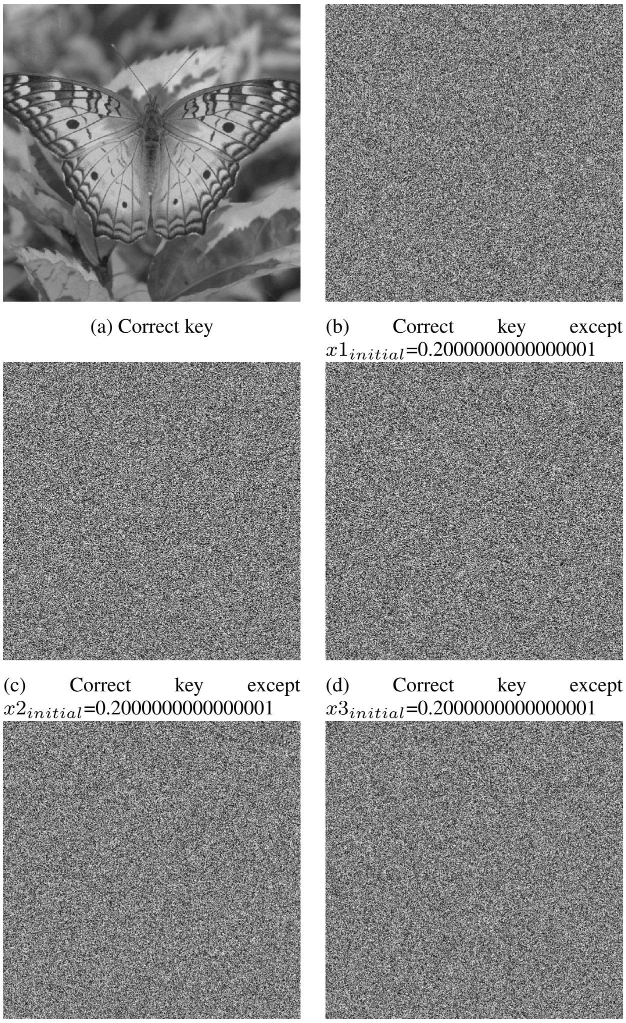
Image	Plain	Encrypted
Butterfly	6.614438	7.999345
Bee	5.803842	7.999395
Baboon	7.357949	7.999247
Couple	7.058103	7.999331

F. KEY SPACE ANALYSIS

The term “key space” alludes to the number of keys that can be employed in brute force attacks, and it needs to be sufficiently large to withstand such attacks. The presented cryptosystem utilizes key parameters ($x_{initial}$, $y_{initial}$, $z_{initial}$, $w_{initial}$, a, b) to execute the 4-D hyperjerk system during both the encryption and decryption procedures for images. With a computation precision for digital computers set at 10^{-16}, the calculated key space for our algorithm stands at an impressive 10^{96}, a figure that significantly surpasses the requirements for contemporary cryptographic mechanisms, thus reinforcing the robustness and security of our encryption approach.

G. KEY SENSITIVITY ANALYSIS

It is crucial to test the impact of minor changes in the initial key parameters to ensure the security of an encryption method. Key sensitivity refers to the degree to which slight modifications to initial key parameters affect the decryption outcome. To assess the key sensitivity of the proposed cryptosystem, minor alterations were made to the initial keys in order to decrypt the Cipher-Butterfly image, as illustrated in Figure 25.


(a) Correct key

(b) Correct key except $x1_{initial}$=0.2000000000000001

(c) Correct key except $x2_{initial}$=0.2000000000000001

(d) Correct key except $x3_{initial}$=0.2000000000000001

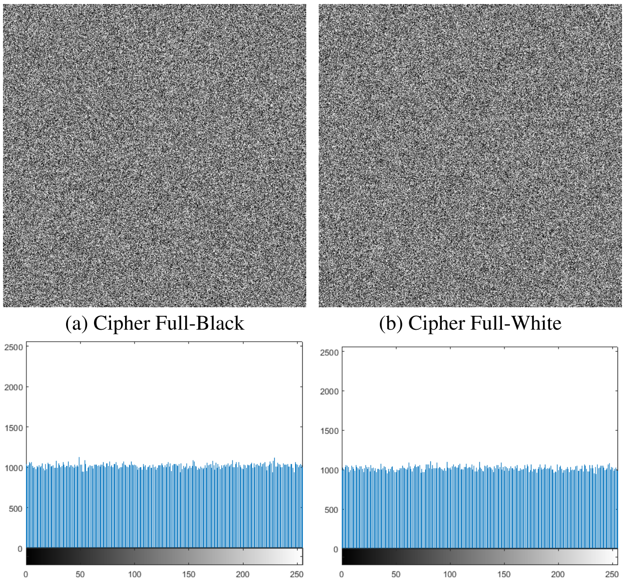
(e) Correct key except $x4_{initial}$=0.2000000000000001

(f) Correct key except a=4.000000000000001

FIGURE 25. key sensitivity effects.

H. CLASSICAL TYPES OF ATTACK

In general, when analyzing a cryptosystem, it is assumed that the structure of the system is fully understood by the analysts. This includes knowledge of the encryption and decryption algorithms, with the exception of the secret key used in the process. There are four common types of attacks in cryptanalysis: known-plaintext, chosen-plaintext, ciphertext-only, and chosen-ciphertext attacks. Among these, the chosen-plaintext attack is considered the most effective. It involves a cyberpunk gaining temporary access to the system and generating ciphertext for a specific plaintext. If an encryption algorithm can withstand the chosen plaintext attack, it demonstrates its ability to resist other types of attacks as well. In our proposed encryption algorithm, even a small modification to any of the initial keys ($x_{initial}$, $y_{initial}$, $z_{initial}$, $w_{initial}$, a, and b) results in a significant change in the output. Additionally, our encryption approach incorporates the use of SHA-256 on the plain image to update the initial parameters. This means that our cryptosystem relies not only on the secret key but also on the plain image itself. To disable the permutation/substitution procedures and gain useful information about the secret key, the cryptanalyst tries to analyze full-white and full-black images. These images are specifically designed to provide no visual information. Figure 26 shows the resulting cipher images for the full-white and full-black images, along with their corresponding histograms. As can be observed, no meaningful visual information can be extracted from these cipher images. Table 8 presents statistical analyses of these images. Due to these properties and characteristics, our cryptosystem demonstrates the ability to withstand classical types of attacks.



(a) Cipher Full-Black

(b) Cipher Full-White

(c) Histogram of cipher Full-Black

(d) Histogram of cipher Full-White

FIGURE 26. Ciphers of full-white and full-black images along with their corresponding histogram representations.

TABLE 8. Statistical analyses of cipher full-white image and cipher full-black image.

Image	Correlation			Entropy
	H	V	D	
Full-White	0.0004	-0.0004	0.0002	7.999365
Full-Black	-0.0006	0.0003	-0.0001	7.999384

I. NOISE AND DATA LOSS ATTACKS

The presence of noise in data transmission networks is a common occurrence. When data is transmitted over such noisy networks, it is susceptible to distortion caused by noise or data loss attacks. Therefore, a well-designed encryption algorithm should be able to withstand these types

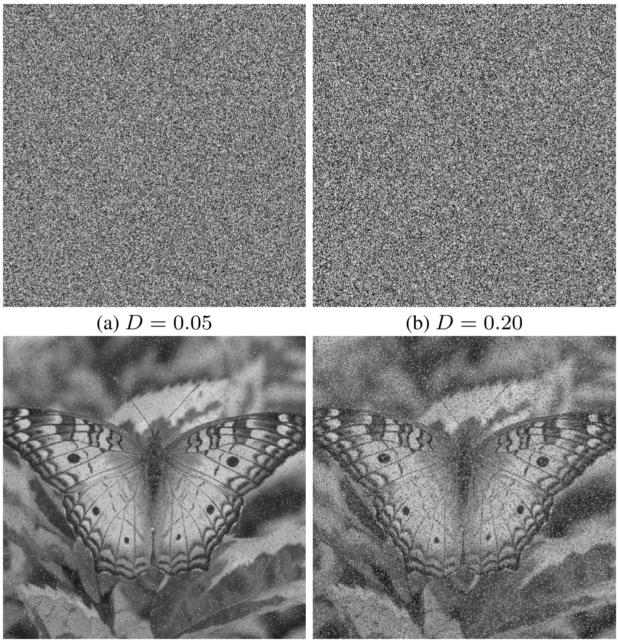

(a) $D = 0.05$ (b) $D = 0.20$

FIGURE 27. Results of the noise attack, in which the first row shows the defective Cipher-Butterfly image with Salt & Pepper noise added at different densities (D), while the second row displays the related deciphered images.

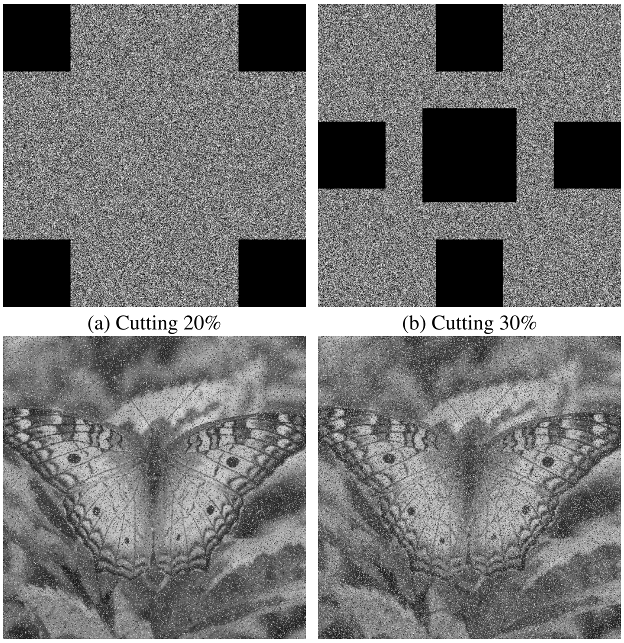

(a) Cutting 20% (b) Cutting 30%

FIGURE 28. Results of the data loss attack, in which the first row displays the defective Cipher-Butterfly image created by cutting blocks of various sizes, while the second row shows the related deciphered images.

of attacks. To evaluate the effectiveness of the proposed image cryptosystem in countering data loss and noise attacks, we conducted experiments by intentionally introducing defects to the Cipher-Butterfly image. In the data loss attack, we applied cutting blocks to the data, varying the sizes of the blocks. In the noise attack, we introduced Salt & Pepper noise with different density levels. Subsequently, we deciphered the defective images to assess the performance of the cryptosystem under these attack scenarios. The results of the noise and data loss attacks are presented in Figures 27 and 28, respectively. Remarkably, the deciphered images exhibit high visual quality and preserve the essential visual details within the affected regions, despite the presence of noise or data loss. This demonstrates the robustness of the proposed image cryptosystem against these types of attacks, as it successfully mitigates the impact of noise and data loss, ensuring the visual fidelity of the decrypted images.

TABLE 9. Average values of UACI, NPCR, correlation coefficient, and information entropy for the proposed method and the related methods.

Method	UACI (%)	NPCR (%)	Correlation Coefficient			Entropy
			Diagonal	Vertical	Horizontal	
Our work	33.44129	99.61758	0.00023	0.00020	0.00048	7.99933
[43]	33.46575	99.61306	-0.00015	-0.00039	0.00014	7.99985
[44]	33.45969	99.61070	-0.00008	0.00003	-0.00004	7.99984
[45]	33.45960	99.60960	0.00087	0.00033	0.00052	7.99930
[46]	33.41178	99.59958	0.00273	-0.00074	0.00113	7.99720
[47]	33.48417	99.61427	0.00001	0.00014	0.00022	7.99985

J. COMPARATIVE ANALYSIS

To validate the effectiveness of the proposed encryption method in conjunction with related encryption approaches, Table 9 provided a simple comparison of the average values of NPCR, UACI, information entropy, and the correlation coefficient for the presented approach and the related approaches. From the stated values in Table 9, we can conclude the efficacy of the proposed method compared to the related methods.

VIII. CONCLUSION

In this paper, a novel 4D autonomous hyperjerk system with a half line equilibrium and consisting of one absolute function nonlinearity was proposed. Our finding show that novel the 4D hyperjerk system exhibits special behavior like multistability, period doubling reversals, antimonotonicity. Furthermore, the proposed system has been implemented with electronic circuit and FPGA implementation. It was shown that the FPGA implementation generates experimental chaotic attractors that are in good agreement with Matlab simulation and MultiSim simulation. Finally, this study introduced a new image cryptosystem based on the chaotic dynamical behavior of the presented hyperjerk system. The experimental outcomes of the presented encryption method proved its efficiency and security. In future research, we aim to employ the proposed 4-D hyperjerk system in designing a new video cryptosystem for real-time Internet of Things applications.

REFERENCES

[1] S. Yan, Y. Ren, Z. Song, W. Shi, and X. Sun, "A memristive chaotic system with rich dynamical behavior and circuit implementation," *Integration*, vol. 85, pp. 63–75, Jul. 2022.

[2] J. M. Munoz-Pacheco, T. García-Chávez, V. R. Gonzalez-Diaz, G. de La Fuente-Cortes, and L. D. C. del Carmen Gómez-Pavón, "Two new asymmetric Boolean chaos oscillators with no dependence on incommensurate time-delays and their circuit implementation," *Symmetry*, vol. 12, no. 4, p. 506, Apr. 2020.

[3] S. Liu, X. An, Y. Wang, and Q. Shi, "Design of a new multi-wing chaotic system and its application in color image encryption," *Optik*, vol. 290, Oct. 2023, Art. no. 171334.

[4] K. Karawanich and P. Prommee, “High-complex chaotic system based on new nonlinear function and OTA-based circuit realization,” *Chaos, Solitons Fractals*, vol. 162, Sep. 2022, Art. no. 112536.

[5] S. Vaidyanathan, E. Tlelo-Cuautle, K. Benkouider, A. Sambas, and B. Ovilla-Martínez, “FPGA-based implementation of a new 3-D multistable chaotic jerk system with two unstable balance points,” *Technologies*, vol. 11, no. 4, Jul. 2023, Art. no. 11040092.

[6] Y. Xia, S. Hua, and Q. Bi, “Quasi-periodic structure in chaotic bursting attractor for a controlled jerk oscillator,” *Chaos, Solitons Fractals*, vol. 174, Sep. 2023, Art. no. 113902.

[7] B. A. Idowu, L. G. Dolvis, O. G. Fernández, A. Sambas, S. Vaidyanathan, and E. T. Cuautle, “A new multistable hyperjerk dynamical system with self-excited chaotic attractor, its complete synchronisation via backstepping control, circuit simulation and FPGA implementation,” *Int. J. Model., Identificat. Control*, vol. 35, no. 3, pp. 177–190, 2020.

[8] R. Kengne, J. T. Mbe, J. Fotsing, A. B. Mezatio, F. J. N. Manekeng, and R. Tchitnga, “Dynamics and synchronization of a novel 4D-hyperjerk autonomous chaotic system with a van der Pol nonlinearity,” *Zeitschrift Naturforschung A, J. Phys. Sci.*, vol. 78, no. 9, pp. 801–821, Sep. 2023.

[9] K. E. Chlouverakis and J. C. Sprott, “Chaotic hyperjerk systems,” *Chaos, Solitons Fractals*, vol. 28, no. 3, pp. 739–746, May 2006.

[10] F. Y. Dalkiran and J. C. Sprott, “Simple chaotic hyperjerk system,” *Int. J. Bifurcation Chaos*, vol. 26, no. 11, Oct. 2016, Art. no. 1650189.

[11] L. Jiang, J. Li, and W. Zhang, “Bifurcations and chaos dynamics of a hyperjerk system with antimonotonicity,” *Eur. Phys. J. Plus*, vol. 135, no. 9, p. 767, Sep. 2020.

[12] L. Moysis, E. Petavratzis, M. Marwan, C. Volos, H. Nistazakis, and S. Ahmad, “Analysis, synchronization, and robotic application of a modified hyperjerk chaotic system,” *Complexity*, vol. 2020, pp. 1–15, Apr. 2020.

[13] M. D. Vijayakumar, A. Bahramian, H. Natiq, K. Rajagopal, and I. Hussain, “A chaotic quadratic bistable hyperjerk system with hidden attractors and a wide range of sample entropy: Impulsive stabilization,” *Int. J. Bifurcation Chaos*, vol. 31, no. 16, Dec. 2021, Art. no. 2150253.

[14] M. Higazy and Y. S. Hamed, “Dynamics, circuit implementation and control of new Caputo fractional order chaotic 5-dimensions hyperjerk model,” *Alexandria Eng. J.*, vol. 60, no. 4, pp. 4177–4190, Aug. 2021.

[15] A. Q. Khan and S. S. Kazmi, “Dynamical analysis of a three-species discrete biological system with scavenger,” *J. Comput. Appl. Math.*, vol. 440, Apr. 2024, Art. no. 115644.

[16] G. Sani, J. Awrejcewicz, and Z. N. Tabekoueng, “Modeling, analysis and control of parametrically coupled electromechanical oscillators,” *Mechanism Mach. Theory*, vol. 191, Jan. 2024, Art. no. 105514.

[17] L. Laskaridis, C. Volos, and I. Stouboulos, “Antimonotonicity, hysteresis and coexisting attractors in a Shinriki circuit with a physical memristor as a nonlinear resistor,” *Electronics*, vol. 11, no. 12, p. 1920, Jun. 2022.

[18] C. Zhang, “Dynamics of a simple third-order autonomous MLC circuit,” *Phys. Scripta*, vol. 98, no. 10, Oct. 2023, Art. no. 105237.

[19] D. Jiang, N. Tsafack, W. Boulila, J. Ahmad, and J. J. Barba-Franco, “ASB-CS: Adaptive sparse basis compressive sensing model and its application to medical image encryption,” *Expert Syst. Appl.*, vol. 236, Feb. 2024, Art. no. 121378.

[20] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, C. Wang, and X. Tang, “Asynchronous updating Boolean network encryption algorithm,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 8, pp. 4388–4400, Jan. 2023.

[21] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, and X. Tang, “A 3D model encryption scheme based on a cascaded chaotic system,” *Signal Process.*, vol. 202, Jan. 2023, Art. no. 108745.

[22] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, and X. Tang, “EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory,” *Inf. Sci.*, vol. 621, pp. 766–781, Apr. 2023.

[23] R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan, and X. Tang, “AEA-NCS: An audio encryption algorithm based on a nested chaotic system,” *Chaos, Solitons Fractals*, vol. 165, Dec. 2022, Art. no. 112770.

[24] B. Abd-El-Atty, “A robust medical image steganography approach based on particle swarm optimization algorithm and quantum walks,” *Neural Comput. Appl.*, vol. 35, no. 1, pp. 773–785, Jan. 2023.

[25] B. Abd-El-Atty, M. A. El-Affendi, S. A. Chelloug, and A. A. Abd El-Latif, “Double medical image cryptosystem based on quantum walk,” *IEEE Access*, vol. 11, pp. 69164–69176, 2023.

[26] B. Abd-El-Atty, “Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem,” *Complex Intell. Syst.*, vol. 9, no. 5, pp. 4817–4835, Feb. 2023.

[27] X. Wang, X. Zhu, and Y. Zhang, “An image encryption algorithm based on Josephus traversing and mixed chaotic map,” *IEEE Access*, vol. 6, pp. 23733–23746, 2018.

[28] X. Wang, X. Zhu, X. Wu, and Y. Zhang, “Image encryption algorithm based on multiple mixed hash functions and cyclic shift,” *Opt. Lasers Eng.*, vol. 107, pp. 370–379, Aug. 2018.

[29] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, “A new image encryption algorithm for grey and color medical images,” *IEEE Access*, vol. 9, pp. 37855–37865, 2021.

[30] X. Gao, “Image encryption algorithm based on 2D hyperchaotic map,” *Opt. Laser Technol.*, vol. 142, Oct. 2021, Art. no. 107252.

[31] B. Bao, X. Zou, Z. Liu, and F. Hu, “Generalized memory element and chaotic memory system,” *Int. J. Bifurcation Chaos*, vol. 23, no. 8, Aug. 2013, Art. no. 1350135.

[32] R. Wang, C. Li, S. Çiçek, K. Rajagopal, and X. Zhang, “A memristive hyperjerk chaotic system: Amplitude control, FPGA design, and prediction with artificial neural network,” *Complexity*, vol. 2021, pp. 1–17, Feb. 2021.

[33] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, “Determining Lyapunov exponents from a time series,” *Phys. D, Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, Jul. 1985.

[34] P. Frederickson, J. L. Kaplan, E. D. Yorke, and J. A. Yorke, “The Liapunov dimension of strange attractors,” *J. Differ. Equc.*, vol. 49, no. 2, pp. 185–207, Aug. 1983.

[35] 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, p. 1893, Feb. 2023.

[36] A. Sambas, S. Vaidyanathan, X. Zhang, I. Koyuncu, T. Bonny, M. Tuna, M. Alcin, S. Zhang, I. M. Sulaiman, A. M. Awwal, and P. Kumam, “A novel 3D chaotic system with line equilibrium: Multistability, integral sliding mode control, electronic circuit, FPGA implementation and its image encryption,” *IEEE Access*, vol. 10, pp. 68057–68074, 2022.

[37] A. Sambas, S. Vaidyanathan, S. Zhang, Y. Zeng, M. A. Mohamed, and M. Mamat, “A new double-wing chaotic system with coexisting attractors and line equilibrium: Bifurcation analysis and electronic circuit simulation,” *IEEE Access*, vol. 7, pp. 115454–115462, 2019.

[38] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A. A. A. El-Latif, O. Guillén-Fernández, Sukono, Y. Hidayat, and G. Gundara, “A 3-D multi-stable system with a peanut-shaped equilibrium curve: Circuit design, FPGA realization, and an application to image encryption,” *IEEE Access*, vol. 8, pp. 137116–137132, 2020.

[39] K. Benkouider, S. Vaidyanathan, A. Sambas, E. Tlelo-Cuautle, A. A. A. El-Latif, B. Abd-El-Atty, C. F. Bermudez-Marquez, I. M. Sulaiman, A. M. Awwal, and P. Kumam, “A new 5-D multistable hyperchaotic system with three positive Lyapunov exponents: Bifurcation analysis, circuit design, FPGA realization and image encryption,” *IEEE Access*, vol. 10, pp. 90111–90132, 2022.

[40] O. Guillén-Fernández, M. F. Moreno-López, and E. Tlelo-Cuautle, “Issues on applying one- and multi-step numerical methods to chaotic oscillators for FPGA implementation,” *Mathematics*, vol. 9, no. 2, p. 151, Jan. 2021.

[41] Y. Hong, Y. Wang, J. Su, Y. Wen, and Z. Yang, “Image encryption algorithm based on chaotic mapping and binary bidirectional zigzag transform,” *IEEE Access*, vol. 11, pp. 78498–78510, 2023.

[42] D. Zou, T. Pei, G. Xi, and L. Wang, “Image encryption based on hyperchaotic system and improved zigzag diffusion method,” *IEEE Access*, vol. 11, pp. 95396–95409, 2023.

[43] B. Abd-El-Atty and A. A. Abd EL-Latif, “Applicable image cryptosystem using bit-level permutation, particle swarm optimisation, and quantum walks,” *Neural Comput. Appl.*, vol. 35, no. 25, pp. 18325–18341, Sep. 2023.

[44] B. Abd-El-Atty, “Quaternion with quantum walks for designing a novel color image cryptosystem,” *J. Inf. Secur. Appl.*, vol. 71, Dec. 2022, Art. no. 103367.

[45] Y. Xian and X. Wang, “Fractal sorting matrix and its application on chaotic image encryption,” *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.

[46] X. Wang and S. Gao, “Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory,” *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.

[47] A. A. A. El-Latif and B. Abd-El-Atty, “Adaptive particle swarm optimization with quantum-inspired quantum walks for robust image security,” *IEEE Access*, vol. 11, pp. 71143–71153, 2023.

ACENG SAMBAS received the Doctor of Philosophy (Ph.D.) degree in mathematics from Universiti Sultan Zainal Abidin (UniSZA), Malaysia, in 2020. He has been a Lecturer with UniSZA and Universitas Muhammadiyah Tasikmalaya (UMTAS), Indonesia. His current research interests include chaotic signals, nonlinear dynamical systems, control systems, electrical engineering, circuits, robotics, signal processing, embedded systems, and artificial intelligence (AI).

MAHDAL MIROSLAV is currently pursuing the Ph.D. degree with the Faculty of Mechanical Engineering, VSB-Technical University of Ostrava, Czech Republic. He is also the Vice-Dean for Science, Research with the Faculty of Mechanical Engineering, VSB-Technical University of Ostrava, and an Associate Professor with the Department of Control Systems and Instrumentation. His research interests include the control of mechatronic systems, control systems, automatic control theory, wireless technologies, artificial intelligence, cloud computing, optimization methods, and the programming of control systems. He has over 80 research articles to his credit.

SUNDARAPANDIAN VAIDYANATHAN received the Doctor of Science degree in electrical and systems engineering from Washington University in St. Louis, St. Louis, MO, USA, in 1996. He is currently a Professor with the Centre for Control Systems, Vel Tech University, Vel Nagar, Avadi, Chennai, India. He has published over 630 Scopus-indexed research articles in various international journals. He is an editor in many international journals related to control systems. His current research interests include control systems engineering, chaos, hyperchaos, electrical circuits, FPGA, cryptography, mathematical modeling, data science, and computational science.

BRISBANE OVILLA-MARTÍNEZ received the B.S. degree in electronics engineering from Universidad Autonoma Metropolitana, in 2007, and the M.Sc. and Ph.D. degrees in computer science from Centro de Investigacion y de Estudios Avanzados del IPN (CINVESTAV), in 2009 and 2015, respectively. She was a Postdoctoral Fellow with the Hubert Curien Laboratory, Saint Étienne, France. Currently, she is a Researcher with CINVESTAV. Her main research interest include hardware security, cryptography, and reconfigurable hardware.

ESTEBAN TLELO-CUAUTLE received the M.Sc. and Ph.D. degrees from Instituto Nacional de Astrofisica, Optica y Electronica (INAOE), Mexico, in 1995 and 2000, respectively. In 2001, he was appointed as a Professor/Researcher with INAOE. He has authored five books, edited 11 books, and published around 300 papers in book chapters, international journals, and conferences. His research interests include FPGA, analog signal processing, integrated circuits, optimization by metaheuristics, the design and applications of chaotic systems, security in the Internet of Things, symbolic analysis, and analog/RF and mixed-signal design automation tools. He serves as an Associate Editor for *Engineering Applications of Artificial Intelligence*, *International Journal of Circuit Theory and Applications*, *Electronics*, *Integration the VLSI Journal*, and *Fractal and Fractional*.

AHMED A. ABD EL-LATIF received the Graduate degree from the Harbin Institute of Technology, China, in 2013. Since 2013, he has been carried out a number of successful research projects and grants in Egypt, Russian federation, and Tunisia. Since 2018, he has been an Associate Professor in computer science with Menoufia University, Egypt. Since 2022, he has been an Associate Professor in computer science with Prince Sultan University, Saudi Arabia. In more than 17 years of his professional experience, he published over 280 papers in journals and conferences, including 13 books. Since 2022, he has been the Head of the MEGANET 6G Laboratory Research in Russian Federation. His current research interests include the development of new algorithms in quantum computing, chaotic dynamical systems, and AI for cybersecurity, and the artificial Intelligence of Things. One of his pioneering achievements lies in his expertise in designing discrete-time quantum walks and chaotic systems, which have found applications in a spectrum of cybersecurity domains, including encryption, authentication, S-boxes, hash functions, watermarking, and steganography.

BASSEM ABD-EL-ATTY received the Ph.D. degree in computer science from Menoufia University, Egypt, in 2020. Currently, he is an Assistant Professor with the Faculty of Computers and Information, Luxor University, Egypt. He is author and coauthor of more than 40 research works comprising journal articles, conference papers, and book chapters. He is a reviewer in many journals in Elsevier and Springer. His research interests include cryptography, quantum information processing, and image processing.

KHALED BENKOUIDER received the M.S. degree in automatic control and the Ph.D. degree from the University of Jijel, Jijel, Algeria, in 2015 and 2021, respectively. His M.S. research was on secure communications based on chaotic systems. He is currently an Assistant Professor with the Electronics Institute, Annaba University, Algeria. His main research interests include chaos, chaotic systems, control systems, dynamical systems, delayed systems, LPV systems, transmission security, and watermarking.

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 FPGA, chaotic oscillator realizations, image processing, embedded systems, hardware digital design, secure communication systems, artificial intelligence (AI), and machine learning and bioinformatics.