IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 May 2022, accepted 30 May 2022, date of publication 8 June 2022, date of current version 30 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3181424

A Novel 3D Chaotic System With Line Equilibrium: Multistability, Integral Sliding Mode Control, Electronic Circuit, FPGA Implementation and Its Image Encryption

ACENG SAMBAS[1,2], SUNDARAPANDIAN VAIDYANATHAN[3], XUNCAI ZHANG[4], ISMAIL KOYUNCU[5], TALAL BONNY[6], MURAT TUNA[7], MURAT ALÇIN[8], SEN ZHANG[9], IBRAHIM MOHAMMED SULAIMAN[2,10], ALIYU MUHAMMED AWWAL[11,12,13], AND POOM KUMAM[11,14], (Member, IEEE)

[1]Department of Mechanical Engineering, Universitas Muhammadiyah Tasikmalaya, Tasikmalaya 46196, Indonesia
[2]School of Quantitative Sciences, Institute of Strategic Industrial Decision Modelling (ISIDM), Universiti Utara Malaysia, Sintok, Kedah 06010, Malaysia
[3]Research and Development Centre, Vel Tech University, Chennai, Tamil Nadu 600062, India
[4]College of Electric Information Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China
[5]Department of Electrical and Electronics Engineering, Afyon Kocatepe University, 03204 Afyon, Turkey
[6]Department of Computer Engineering, University of Sharjah, Sharjah, United Arab Emirates
[7]Department of Electrical, Technical Sciences Vocational School, Kırklareli University, 39100 Kırklareli, Turkey
[8]Department of Mechatronics Engineering, Faculty of Technology, Afyon Kocatepe University, 03204 Afyon, Turkey
[9]School of Artificial Intelligence, and Automation, and Key Laboratory of Image Processing, and Intelligent Control of Education Ministry of China, Huazhong University of Science, and Technology, Wuhan, 430074 China
[10]School of Quantitative Sciences, College of Art and Sciences, Universiti Utara Malaysia, Sintok, Kedah 06010, Malaysia
[11]KMUTTFixed Point Research Laboratory, the Room SCL 802 Fixed Point Laboratory, the Science Laboratory Building, the Center of Excellence in Theoretical and Computational Science (TaCS-CoE), the Department of Mathematics, the Faculty of Science, King Mongkut's University of Technology Thonburi (KMUTT), Thung Khru, Bangkok 10140, Thailand
[12]Department of Mathematics, Faculty of Science, Gombe State University, Gombe 760214, Nigeria
[13]GSU-Mathematics for Innovative Research (GSU-MIR) Group, Gombe State University, Gombe 760214, Nigeria
[14]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan

Corresponding author: Poom Kumam (poom.kum@kmutt.ac.th)

This work was supported in part by the Center of Excellence in Theoretical and Computational Science (TaCS-CoE), King Mongkut's University of Technology Thonburi (KMUTT), Thailand; and in part by the National Research Council of Thailand (NRCT) under Research Grants for Talented Mid-Career Researchers under Contract N41A640089. The work of Aliyu Muhammed Awwal was supported by the Postdoctoral Fellowship from KMUTT.

ABSTRACT This paper announces a novel three-dimensional chaotic system with line equilibrium and discusses its dynamic properties such as Lyapunov exponents, phase portraits, equilibrium points, bifurcation diagram, multistability and coexisting attractors. New synchronization results based on integral sliding mode control (ISMC) are also derived for the new chaotic system with line equilibrium. In addition, an electronic circuit implementation of the new chaotic system with line equilibrium is reported and a good qualitative agreement is exhibited between the MATLAB simulations of the theoretical model and the MultiSim results. We also display the implementation of the Field-Programmable Gate Array (FPGA) based Pseudo-Random Number Generator (PRNG) by using the new chaotic system. The throughput of the proposed FPGA based new chaotic PRNG is 462.731 Mbps. Randomness analysis of the generated numbers has been performed with respect to the NIST-800-22 tests and they have successfully passed all of the tests. Finally, an image encryption algorithm based on the pixel-level scrambling, bit-level scrambling, and pixel value diffusion is proposed. The experimental results show that the encryption algorithm not only shuffles the pixel positions of the image, but also replaces the pixel values with different values, which can effectively resist various attacks such as brute force attack and differential attack.

INDEX TERMS Chaotic system, hidden attractors, ISMC, electronic circuit, FPGA, image encryption.

I. INTRODUCTION

Chaos theory is recognized as a branch of computer science and mathematics that deals with the dynamical behavior

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

of nonlinear dynamical systems that are highly sensitive to initial conditions ([1], [2]). Chaos has applications in several areas of science and engineering. Some recent applications of chaos can be cited as DC motor [3], magnetic levitation oscillation [4], ultrasonic radar systems [5], unmanned aerial vehicles [6], micro-electro-mechanical systems (MEMS) [7], passenger biodynamics in quarter car model [8], image encryption [9], robotics [10], true random generator [11], financial risk chaotic system [12], suspension bridge model [13], electronic circuits [14], quarter-car vehicle model [15], and memristive devices [16].

The modelling of chaotic systems with infinite number of equilibrium points is an important research topic in the chaos literature ([17], [18]). Especially, finding of chaotic systems possessing line equilibrium of points has attracted significant attention in the chaos literature ([19]–[27]). Jafari *et al.* [19] implemented a systematic search algorithm to find a gallery of chaotic system with line equilibrium. Kingni *et al.* [21] constructed two family chaotic system with line equilibrium and hyperbola curve equilibrium. Moysis *et al.* [22] designed chaotic flow with line equilibrium and application to communications using a descriptor observer. Sambas *et al.* [23] presented a simple chaotic system with line equilibrium and synchronization by passive control method. Nazarimehr *et al.* [24] proposed multi-character dynamical systemlike chaotic and hyper-chaotic attractors without any equilibrium, with a line of equilibria or with unstable equilibrium. Chen *et al.* [25] investigated chaotic behavior in a 3D chaotic system with line equilibrium based on Adomian decomposition. Bao *et al.* [28] reported a 5-D two-memristor-based chaotic system with plane equilibrium.

Sliding Mode Control (SMC) is attractive for nonlinear systems due to its robustness for both parametric and nonparametric uncertainties. SMC is a well-known method for the synchronization of chaotic systems. However, the invariance of SMC is not guaranteed in a reaching phase. Integral Sliding Mode Control (ISMC) eliminates the reaching phase such that the invariance is achieved in an entire system response [29]. Hence, ISMC is also a popular method for the control and synchronization of chaotic systems. The authors in [29] propose the combination of composite nonlinear feedback (CNF) and ISMC methods for chaos synchronization of a class of uncertain chaotic systems with multiple time-varying delays, Lipschitz nonlinearities and parametric disturbances. In [30], the fixed time integral sliding mode controller with the integral expression, and utilize the continuity of fixed time expression is proposed for suppression of chaotic power systems. The integral sliding mode control (ISMC) scheme is presented in [31] for Hindmarsh-Rose neuron model and two-dimensional fractional-order chaotic FitzHugh-Nagumo neuron model. In [32], the integral sliding mode control theory based on numerically solving a state-dependent Riccati equation is used to design nonlinear feedback control for wind energy conversion systems with permanent magnet synchronous generators.

Most of the chaos-based image encryption schemes are generally composed of two main stages: permutation and diffusion. Numerous chaos-based image encryption algorithms have been studied in many works in the chaos literature ([33]–[37]). Ping *et al.* [33] proposed a new block image encryption algorithm. It uses a digit-level permutation and block diffusion with the Henon map. Wu *et al.* [34] presented the effective image encryption scheme integrating a 4D hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion. They showed that the PFDD has reliable security keys and is capable of resisting types of attacks [34]. Chen *et al.* [35] designed image encryption using high-speed scrambling and pixel adaptive diffusion for medical image encryption. It was shown that the proposed improved encryption algorithm not only maintained the merit of the original work but also effectively resisted the chosen plain image attack [35]. Li *et al.* [36] studied image encryption scheme based on the architecture of bit-level scrambling and multiplication diffusion. It was shown that the proposed encryption scheme significantly improves the security by disturbing known-plain text and chosen-plain text attacks [36]. Zhou and Wang [37] constructed a 5D conservative hyperchaotic system and closed-loop diffusion between blocks for image encryption analysis.

In this paper, a new 3D chaotic system with line equilibrium is reported. The new chaotic system has three quadratic nonlinear terms and an absolute function nonlinearity. We show that the equilibrium set of the new 3D chaotic system is the z-axis of R^3. Since the new chaotic system has an infinite number of equilibrium points, it belongs to the class of hidden chaotic attractors ([38], [39]). We have carried out a detailed bifurcation analysis of the new chaotic system with the help of bifurcation diagrams and Lyapunov exponents. Bifurcation analysis of chaotic systems is very useful to understand their qualitative properties ([40], [41]). The new chaotic system exhibits multistability and coexisting chaotic attractors. Multistability is an important property of a chaotic system which refers to the coexistence of chaotic attractors for the same values of the system parameters but different values of the initial conditions ([39], [42], [43]). Zhang *et al.* [43] reported multi-stability in a modified Duffing-Rayleigh system with a piecewise quadratic function.

As a control application, an integral sliding mode control (ISMC) is designed for the achieving global asymptotic synchronization of the proposed chaotic system with itself as master and slave systems. We implement the new chaotic system by using a field-programmable gate array (FPGA) and detail an application for Pseudo-Random Number Generators (PRNGs) based on the new chaotic system. We also apply the new chaotic system to generate a new image encryption algorithm based on the pixel-level scrambling, bit-level scrambling, and pixel value diffusion. As an engineering application, we build an electronic circuit design of the new chaotic system with line equilibrium using MultiSim (Version 13.0). Circuit design of chaotic systems is very useful for

various engineering applications ([44]–[46]). As another engineering application, we devise a new image encryption algorithm based on the new chaotic system with line equilibrium.

This paper is organised as follows. Section 2 describes the dynamics and basic properties of the new chaotic system. Section 3 details the bifurcation analysis, multistability and coexisting attractors of the new chaotic system. Section 4 presents control results using Integral Sliding Mode Control (ISMC) for the synchronization of the new chaotic system. Section 5 details the FPGA implementation and Pseudo-Random Number Generator (PRNG) based on the new chaotic system. Electronic circuit using MultiSim (Version 13.0) of the new chaotic system is given in Section 6. Section 7 describes the image encryption analysis based on the new chaotic system. Section 8 contains the conclusions of this work.

II. MATHEMATICAL MODEL OF THE NEW CHAOTIC SYSTEM

In this paper, we report a new 3-D chaotic system given by the following dynamics:

$$\begin{cases} \dot{x} = y \\ \dot{y} = -x + ayz \\ \dot{z} = -y^2 + b \mid y \mid -xy. \end{cases} \tag{1}$$

which has three quadratic nonlinear terms and an absolute function nonlinearity. Moreover, in equaton (1), x, y, z denote the states and a, b are the constant parameters.

We shall show that the system (1) is chaotic when the system parameters take the values

$$(a, b) = (2.6, 1.5). \tag{2}$$

For numerical simulations, we take the initial conditions as

$$X(0) = (x(0), y(0), z(0)) = (0.2, 0.2, 0.2). \tag{3}$$

With the parameter values as in equation (2) and the initial conditions as in equation (3), the Lyapunov exponents of the new chaotic system in equation (1) are calculated using Wolf algorithm [47] for $T = 1E4$ seconds as

$$(L_1, L_2, L_3) = (0.072567, 0, -0.995887). \tag{4}$$

Since the spectrum in equation (4) of Lyapunov exponents of the new chaotic system (1) has a positive Lyapunov exponent, it follows that the new chaotic system (1) is chaotic.

Also, the sum of the Lyapunov exponents of the system (1) is found as

$$L_1 + L_2 + L_3 = -0.92332 < 0. \tag{5}$$

Hence, the new system (1) is a dissipative chaotic system with a chaotic attractor.

The equilibrium points of the new chaotic system (1) are found by solving the equations

$$y = 0 \tag{6a}$$

$$-x + ayz = 0 \tag{6b}$$

$$-y^2 + b \mid y \mid -xy = 0. \tag{6c}$$

From (6a) and (6b), it is apparent that $x = 0$ and $y = 0$. With this choice, (6c) is also satisfied. Hence, the complete set of equilibrium points of the system (1) is given by

$$S = \left\{ X = (x, y, z) \in R^3 \mid x = 0, y = 0, z \in R \right\}. \tag{7}$$

Since the equilibrium set S is the z-axis in R^3, the new chaotic system (1) has line equilibrium in R^3. Since the new chaotic system (1) has an infinite number of equilibrium points, it is said to possess hidden attractor [48].

The Kaplan-Yorke fractal dimension of the new chaotic system (1) is calculated as

$$D_{KY} = 2 + \frac{L_1 + L_2}{\mid L_3 \mid} = 2.0728667. \tag{8}$$

This gives the complexity of the new chaotic system (1) with line equilibrium. The new chaotic system (1) is invariant under the change of coordinates

$$(x, y, z) \longmapsto (-x, -y, z). \tag{9}$$

This shows that the new chaotic system (1) has rotation symmetry about the z-axis, which is the line of equilibrium points of the system. This is a special property of the new chaotic system (1). Consequently, every non-trivial trajectory of the system (1) possesses a twin trajectory. Figure 1 shows the 2-D phase portraits of the new chaotic system (1). Figure 4 shows the calculation of the Lyapunov exponents of the new chaotic system (1) with line equilibrium.

III. ROUTE TO CHAOS AND COEXISTING ATTRACTORS

Figures 3 and 4 show the Lyapunov spectrum and bifurcation diagram, respectively, of the system with variation of parameter a in the range $a = [2, 2.6]$. Periodic behavior is displayed in the specific region of the parameter $2 \leq a \leq 2.2$. However, when $a > 2.2$, the system exhibits chaotic behavior. In addition, the bifurcation diagram and Lyapunov exponents of the system with respect to parameter b are shown in Figures 5 and 6. Obviously, the new chaotic system (1) exhibits periodic behavior for $1.2 \leq b < 1.38$. Behavior of the system is more complex for $b \geq 1.38$, in which the system generates chaotic behavior.

It is easy to see that this system has rotational symmetry with respect to the z-axis as evidenced by their invariance under the transformation from (x, y, z) into $(-x, -y, z)$. It is well known that symmetric systems generally have coexisting attractors ([49], [50]). Thus, in this work, we investigate such complex dynamics of system (1) by plotting forward and backward continuations for the bifurcation parameter b. The coexisting bifurcation diagrams of the state variable y is illustrated in Fig. 7, in which the forward continuation from the initial values of (0.2,0.2, 0.2) and backward continuations from the initial values of $(-0.2, -0.2, 0.2)$. There are coexisting chaotic attractors when $b = 1.4$ as shown in

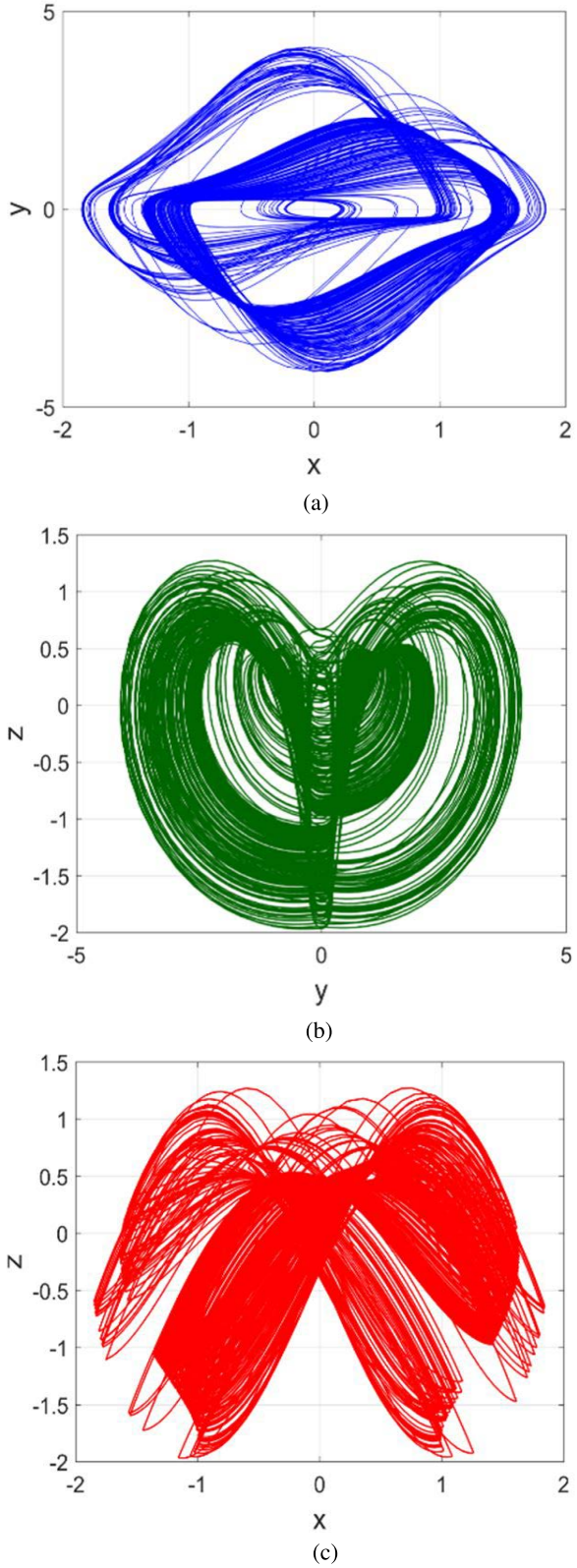

FIGURE 1. Two-dimensional phase plot of the new chaotic system (1) with $X_0 = (0.2, 0.2, 0.2)$ and $(a, b) = (2.6, 1.5)$ in the (a) (x, y)-plane (b) (y, z)-plane and (c) (x, z)-plane.

Fig. 8 and the coexisting periodic attractors mainly occur for $b = 1.3$ (see Fig. 9).

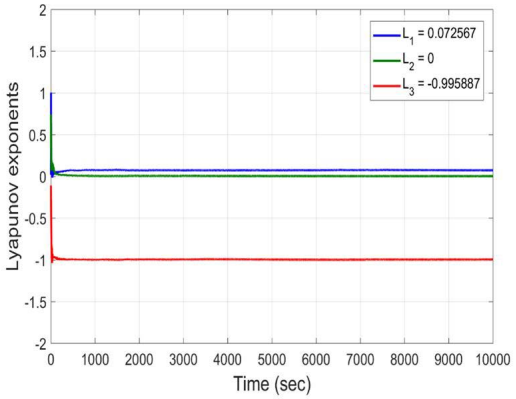

FIGURE 2. Lyapunov exponents of the new chaotic system (1) with $X_0 = (0.2, 0.2, 0.2)$ and $(a, b) = (2.6, 1.5)$.

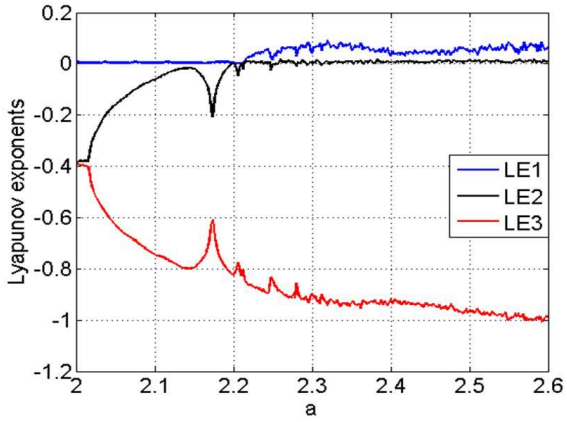

FIGURE 3. Lyapunov exponents of the new chaotic system (1) with line equilibrium when varying the bifurcation parameter a in the range [2, 2.6].

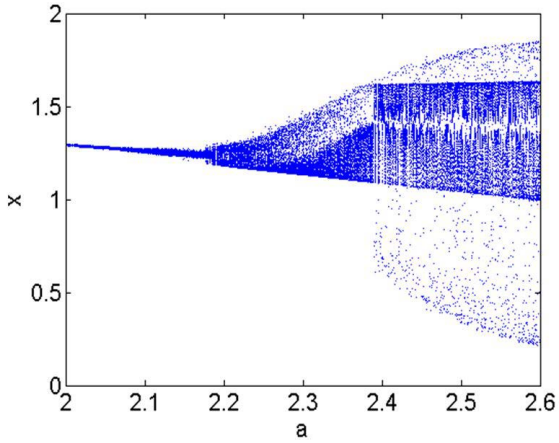

FIGURE 4. Bifurcation diagrams of the new chaotic system (1) with line equilibrium when varying the bifurcation parameter a in the range [2, 2.6].

IV. SYNCHRONIZATION OF THE NEW CHAOTIC SYSTEMS WITH LINE EQUILIBRIUM VIA INTEGRAL SLIDING MODE CONTROL

In this section, we use active integral sliding mode control to completely synchronize a pair of identical new chaotic

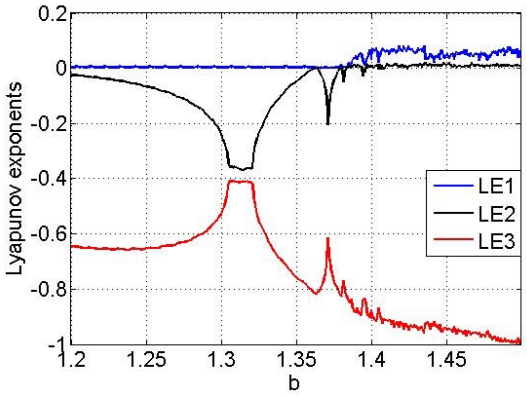

FIGURE 5. Lyapunov exponents of the new chaotic system (1) with line equilibrium when varying the bifurcation parameter b in the range [1.2, 1.5].

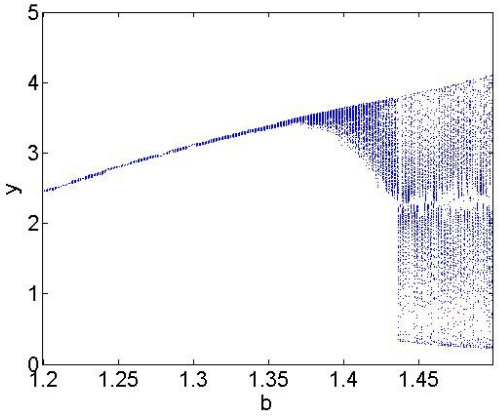

FIGURE 6. Bifurcation diagrams of the new chaotic system (1) with line equilibrium when varying the bifurcation parameter b in the range [1.2, 1.5].

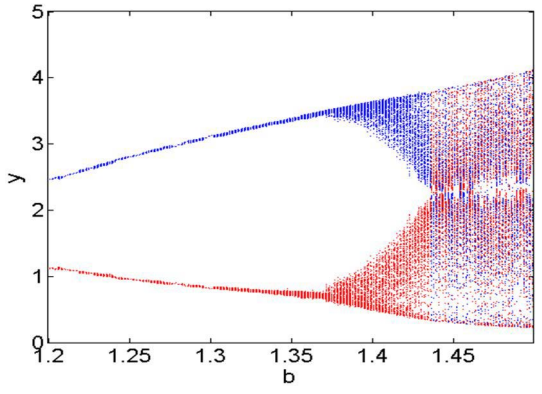

FIGURE 7. Continuations of system (1) when varying b: forward continuation (*blue*) and backward continuation (*red*).

systems with line equilibrium for all initial conditions. As the master system, we take the new chaotic system with line equilibrium given by

$$\begin{cases} \dot{x}_1 = y_1 \\ \dot{y}_1 = -x_1 + a y_1 z_1 \\ \dot{z}_1 = -y_1^2 + b \mid y_1 \mid -x_1 y_1 \end{cases} \tag{10}$$

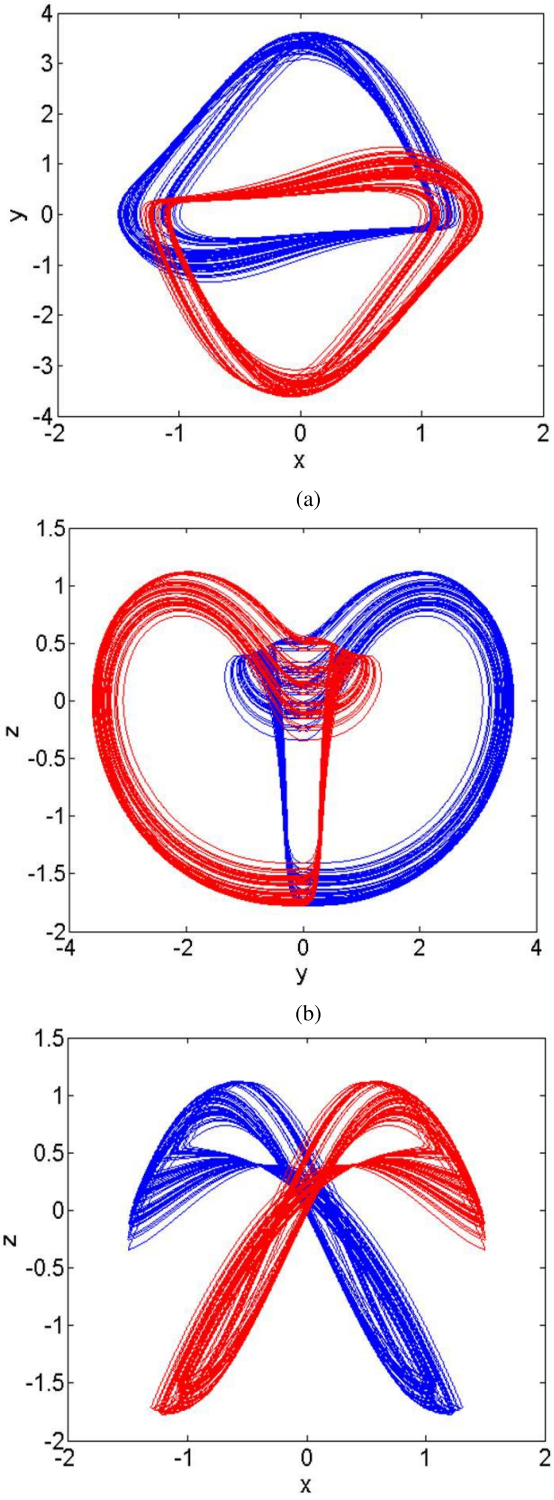

FIGURE 8. Coexisting chaotic attractors of system (1) for $b = 1.4$; the initial conditions $(x(0), y(0), z(0)) = (0.2, 0.2, 0.2)$ (*blue*) and the initial conditions $(x(0), y(0), z(0)) = (-0.2, -0.2, 0.2)$ (*red*) in (a) $x - y$ plane, (b) $y - z$ plane and (c) $y - z$ plane.

where $X_1 = (x_1, y_1, z_1)$ is the state and a, b are system parameters.

As the slave system, we consider the controlled new chaotic system with line equilibrium given by

$$\begin{cases} \dot{x}_2 = y_2 + u_x \\ \dot{y}_2 = -x_2 + a y_2 z_2 + u_y \\ \dot{z}_2 = -y_2^2 + b \mid y_2 \mid -x_2 y_2 + u_z \end{cases} \tag{11}$$

where $X_2 = (x_2, y_2, z_2)$ is the state and $u = (u_x, u_y, u_z)$ is the sliding mode control to be designed. The synchronization error between new chaotic systems (10) and (11) is defined via the equation

$$e = (e_x, e_y, e_z) = (x_2, y_2, z_2) - (x_1, y_1, z_1) \tag{12}$$

The dynamics of the synchronization error is easily obtained as follows:

$$\begin{aligned} \dot{e}_x &= e_y + u_x \\ \dot{e}_y &= -e_x + a(y_2 z_2 - y_1 z_1) + u_y \\ \dot{e}_z &= -y_2^2 + y_1^2 + b(|y_2| - |y_1|) \\ &\quad -x_2 y_2 + x_1 y_1 + u_z \end{aligned} \tag{13}$$

We use active integral sliding mode control for achieving global asymptotic synchronization between the master system (10) and slave system (11). For each error variable, we consider the integral sliding surface defined as follows:

$$\begin{cases} s_x = e_x + \lambda_x \int_0^t e_x(\tau) d\tau \\ s_y = e_y + \lambda_y \int_0^t e_y(\tau) d\tau \\ s_z = e_z + \lambda_z \int_0^t e_z(\tau) d\tau \end{cases} \tag{14}$$

Differentiating each equation in (14), we obtain the following:

$$\begin{cases} \dot{s}_x = \dot{e}_x + \lambda_x s_x \\ \dot{s}_y = \dot{e}_y + \lambda_y s_y \\ \dot{s}_z = \dot{e}_z + \lambda_z s_z \end{cases} \tag{15}$$

The Hurwitz stability criterion holds if we take $\lambda_x, \lambda_y, \lambda_z$ as positive constants.

Based on the exponential reaching law, we set

$$\begin{cases} \dot{s}_x = -\mu_x \mathrm{sgn}(s_x) - k_x s_x \\ \dot{s}_y = -\mu_y \mathrm{sgn}(s_y) - k_y s_y \\ \dot{s}_z = -\mu_z \mathrm{sgn}(s_z) - k_z s_z \end{cases} \tag{16}$$

By equating (15) and (16), we derive the following:

$$\begin{cases} \dot{e}_x + \lambda_x s_x = -\mu_x \mathrm{sgn}(s_x) - k_x s_x \\ \dot{e}_y + \lambda_y s_y = -\mu_y \mathrm{sgn}(s_y) - k_y s_y \\ \dot{e}_z + \lambda_z s_z = -\mu_z \mathrm{sgn}(s_z) - k_z s_z \end{cases} \tag{17}$$

Using the error dynamics (13), we can rewrite (17) as follows.

$$\begin{aligned} e_y + u_x + \lambda_x s_x &= -\mu_x \mathrm{sgn}(s_x) - k_x s_x \\ P + u_y &= -\mu_y \mathrm{sgn}(s_y) - k_y s_y \\ Q + u_z &= -\mu_z \mathrm{sgn}(s_z) - k_z s_z \end{aligned} \tag{18}$$

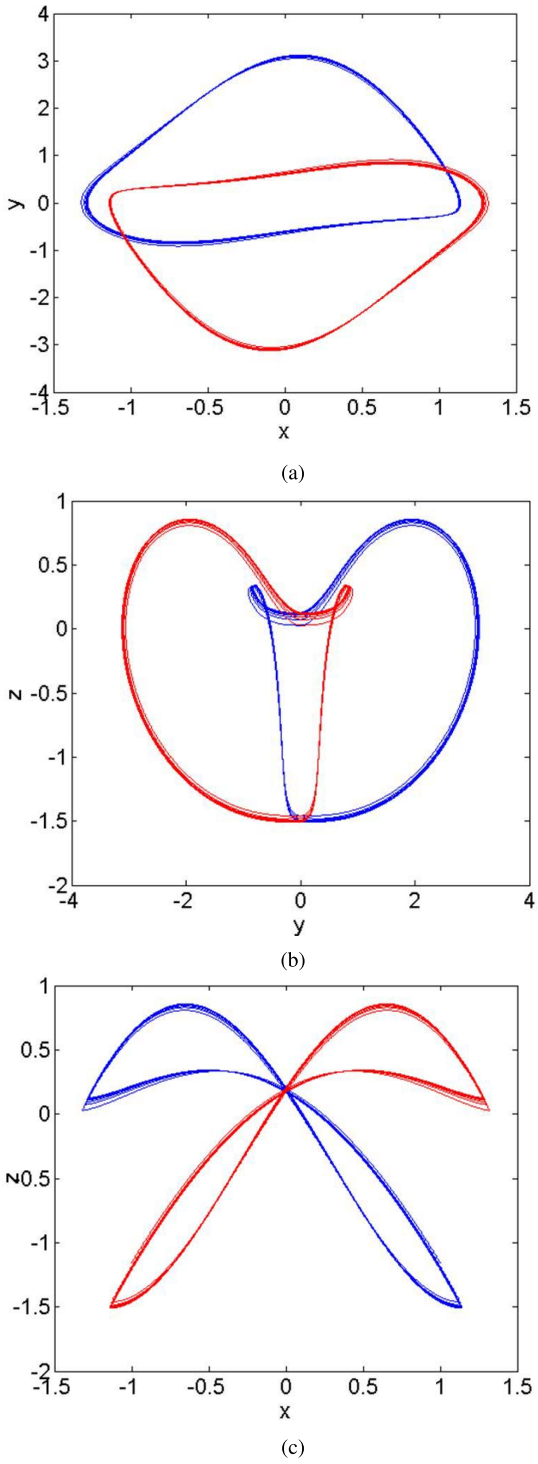

FIGURE 9. Coexisting periodic attractors of system (1) for $b = 1.3$; the initial conditions $(x(0), y(0), z(0)) = (0.2, 0.2, 0.2)$ (*blue*) and the initial conditions $(x(0), y(0), z(0)) = (-0.2, -0.2, 0.2)$ (*red*) in (a) $x - y$ plane, (b) $y - z$ plane and (c) $y - z$ plane.

where

$$\begin{aligned} P &= -e_x + a(y_2 z_2 - y_1 z_1) + \lambda_y s_y \\ Q &= -y_2^2 + y_1^2 + b(\mid y_2 \mid - \mid y_1 \mid) \\ &\quad -x_2 y_2 + x_1 y_1 + \lambda_z s_z \end{aligned} \tag{19}$$

From (18), we get the active integral sliding mode control law as follows:

$$\begin{cases} u_x = -e_y - \lambda_x s_x - \mu_x \ \mathrm{sgn}(s_x) - k_x s_x \\ u_y = -P - \mu_y \ \mathrm{sgn}(s_y) - k_y s_y \\ u_z = -Q - \mu_z \ \mathrm{sgn}(s_z) - k_z s_z \end{cases} \tag{20}$$

The main result of this section is derived as follows.

Theorem 1: The new chaotic systems with line equilibrium given by (10) and (11) are globally and asymptotically synchronized for all initial conditions $X_1(0), X_2(0) \in R^3$ *by the active integral sliding mode control law (20) where the sliding control parameters* λ_i, μ_i *and* k_i *(where* $i = 1, 2, 3$*) are all positive.*

Proof: We use Lyapunov stability theory to establish the result. We use the quadratic Lyapunov function given by

$$V(s_x, s_y, s_z) = \frac{1}{2}(s_x^2, s_y^2, s_z^2 x). \tag{21}$$

where s_x, s_y, s_z are as defined in (15). Evidently, V is a positive definite function on R^3.

We obtain the time-derivative of V as

$$\dot{V} = s_x \dot{s}_x + s_y \dot{s}_y + s_z \dot{s}_z \tag{22}$$

From (21) and (16), we have

$$\begin{aligned} \dot{V} = \ & s_x \left[-\mu_x \ \mathrm{sgn}(s_x) - k_x s_x \right] \\ & + s_y \left[-\mu_y \ \mathrm{sgn}(s_y) - k_y s_y \right] \\ & + s_x \left[-\mu_z \ \mathrm{sgn}(s_z) - k_z s_z \right] \end{aligned} \tag{23}$$

Simplifying (23), we get

$$\dot{V} = -\mu_x \mid s_x \mid -\mu_y \mid s_y \mid -\mu_z \mid s_z \mid -k_x s_x^2 - k_y s_y^2 - k_z s_z^2 \tag{24}$$

Hence, $\dot{V}$ is a negative definite function on R^3.

Thus, by Lyapunov stability theory, it follows that $(s_x(t), s_y(t), s_z(t)) \to 0$ as $t \to \infty$. Hence, we conclude that $(e_x(t), e_y(t), e_z(t)) \to 0$ as $t \to \infty$. □

For numerical simulations, we take the parameters a and b as in the chaotic case, *viz.* $(a, b) = (2.6, 1.5)$.

Also, we take the sliding control constants as follows: $\lambda_x = \lambda_y = \lambda_z = 0.1, \mu_x = \mu_y = \mu_z = 0.2$, and $k_x = k_y = k_z = 20$. The initial conditions of the master system (10) are taken as $(x_1(0), y_1(0), z_1(0)) = (2.8, 9.5, 3.7)$ The initial conditions of the slave system (11) are taken as $(x_2(0), y_2(0), z_2(0)) = (6.3, 2.1, 8.5)$.

Fig. 10 shows the complete synchronization of the new chaotic systems with line equilibrium represented by the master system (10) and the slave system (11), while Fig. 11 depicts the time-history of the synchronization error between the chaotic systems (10) and (11).

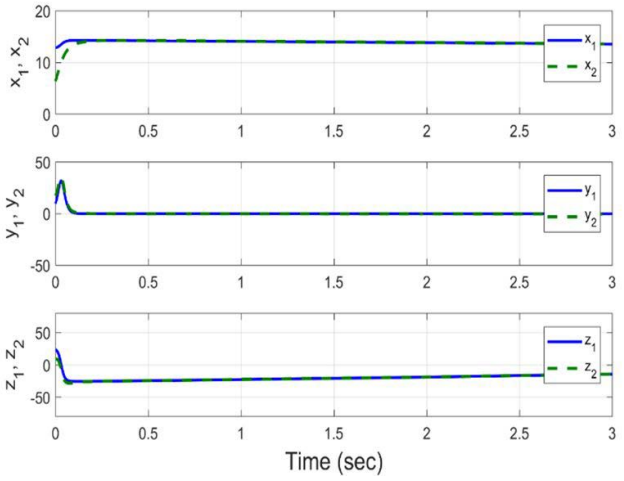

FIGURE 10. Complete synchronization of the systems (10) and (11) with $X_1(0) = (12.8, 9.5, 23.7)$, $X_2(0) = (6.3, 17.1, 8.5)$ and $(a, b) = (2.6, 1.5)$.

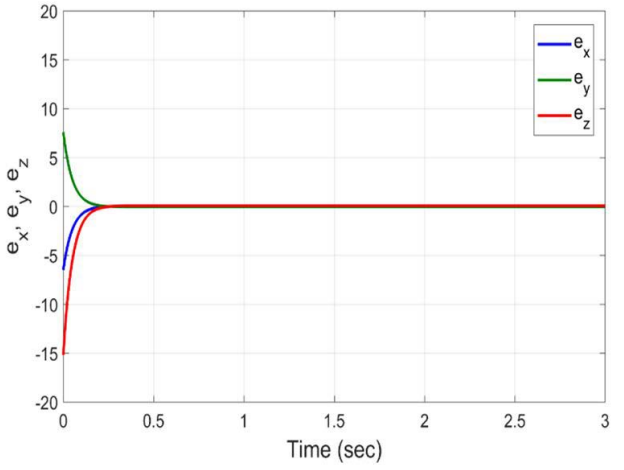

FIGURE 11. Time-history of the synchronization error between the systems (10) and (11) with $X_1(0) = (12.8, 9.5, 23.7)$, $X_2(0) = (6.3, 17.1, 8.5)$ and $(a, b) = (2.6, 1.5)$.

V. CIRCUIT REALIZATION OF THE NEW CHAOTIC SYSTEM WITH LINE EQUILIBRIUM

In this section, electronic circuit realization of the proposed chaotic system is carried out using MultiSim (Version 13.0). The dynamics of the circuit depicted in Figure 12 is simulated in MultiSim (Version 13.0).

For circuit implementation, we rescale the state variables of the new chaotic system (1) as follows: $X = 2\,x$, $Y = 2\,y$ and $Z = 2\,z$. In the new coordinates (X, Y, Z), the chaotic system (1) becomes

$$\begin{cases} \dot{X} = Y \\ \dot{Y} = -X + \dfrac{aYZ}{2} \\ \dot{Z} = \dfrac{-Y^2}{2} + b|Y| - \dfrac{XY}{2} \end{cases} \tag{25}$$

By applying Kirchhoff's laws to the designed electronic circuit, its nonlinear equations are derived in the following

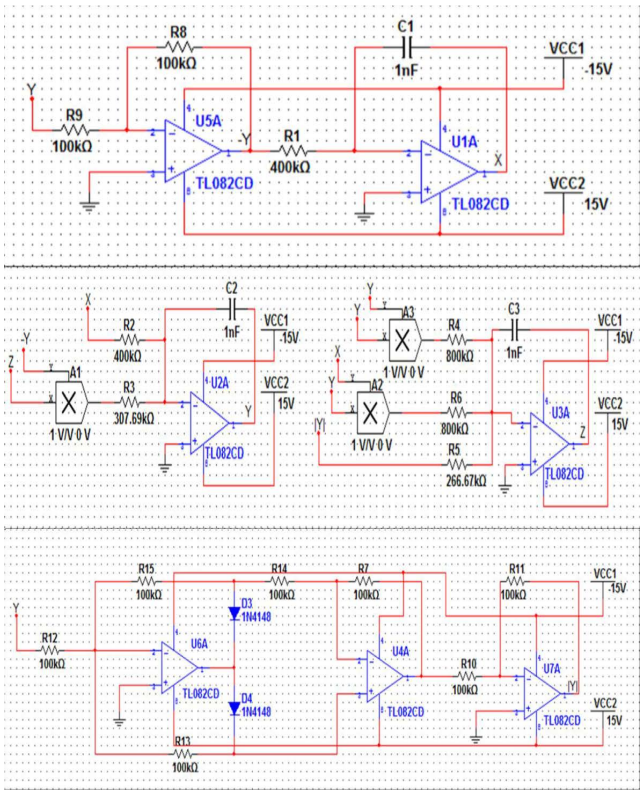

FIGURE 12. Circuit realization of the new chaotic system (26).

form

$$\begin{cases} \dot{X} = \dfrac{1}{C_1 R_1} Y \\ \dot{Y} = -\dfrac{1}{C_2 R_2} X + \dfrac{1}{C_2 R_3} YZ \\ \dot{Z} = -\dfrac{1}{C_3 R_4} Y^2 + \dfrac{1}{C_3 R_5} \mid Y \mid - \dfrac{1}{C_3 R_6} XY \end{cases} \tag{26}$$

where X,Y and Z are the voltages across the capacitors C_1, C_2 and C_3, respectively. Equations (26) match Equation (1) when the circuit components are selected as follows: $R_1 = R_2 = 400\ k\Omega, R_4 = R_6 = 800\ k\Omega$, $R_3 = 307.69\ k\Omega, R_5 = 266.67\ k\Omega, R_7 = R_8 = R_9 = R_{10} = R_{11} = R_{12} = R_{13} = R_{14} = R_{15} = 100\ k\Omega$, $C_1 = C_2 = C_3 = 1\ nF$. The supplies of all active devices are ± 15 Volt and the operational amplifiers TL082CD are used. The corresponding phase portraits on the MultiSIM results are shown in Fig. 13. The agreement between the numerical results (Fig. 1) and MultiSim results (Figure 13) shows the feasibility of the proposed line equilibrium chaotic system.

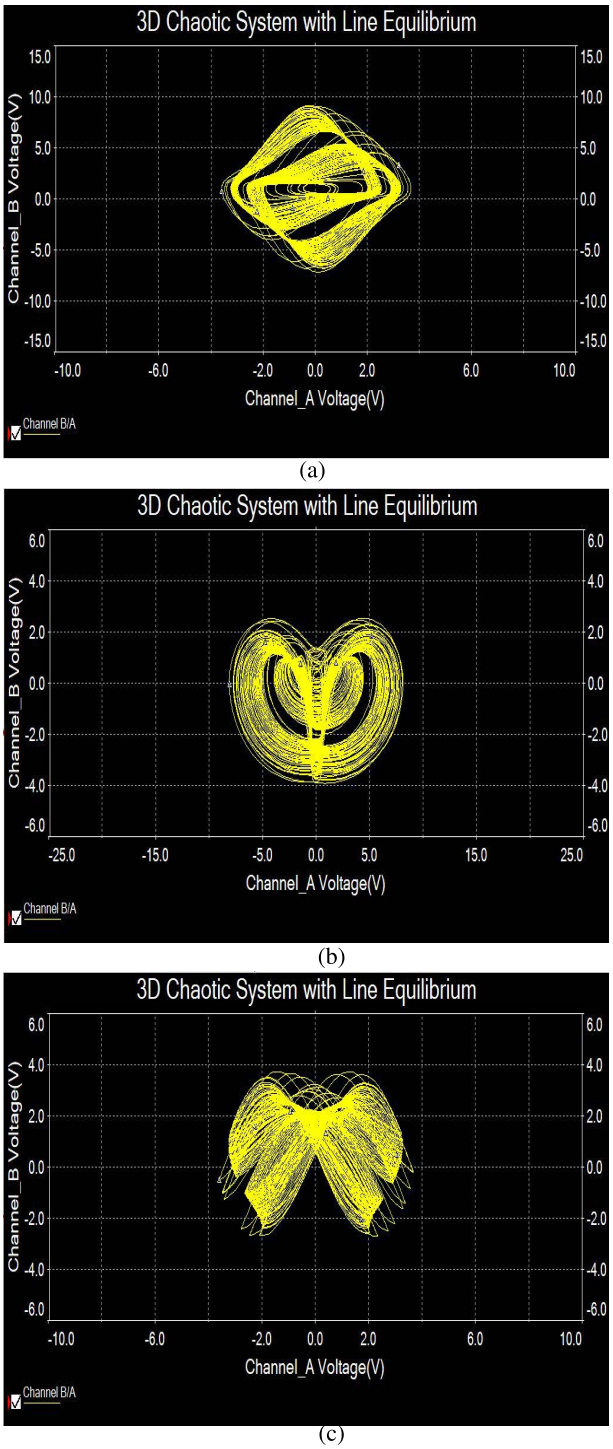

FIGURE 13. MultiSim simulations of the new chaotic system (26): (a) $X - Y$ plane (b)$Y - Z$ plane and (c)$X - Z$ plane.

VI. FPGA-BASED CHAOTIC PSEUDO-RANDOM NUMBERS GENERATORS

Chaos is defined as nonlinear dynamic systems that are exponentially sensitive to initial conditions, deterministic, and aperiodic in the long term ([51], [52]). Since chaotic systems exhibit aperiodic dynamic characteristic behaviour and extreme sensitivity to initial conditions and system parameters, chaos and chaotic systems have been extensively used in random number generators ([53], [54]). Random numbers can be defined as numbers that are within a certain range, their probability of occurrence is equal to each other, and there is no specific relationship between these numbers ([55], [56]). The generated random numbers should have good statistical properties and they cannot be predicted. Random numbers are mandatory for a wide

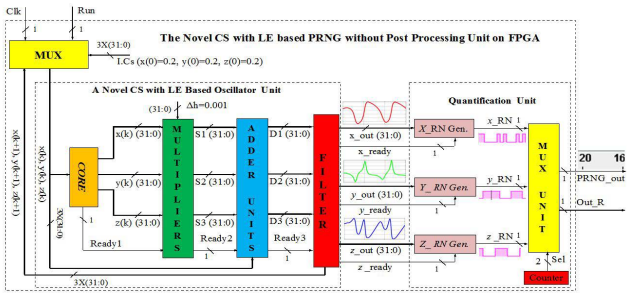

FIGURE 14. The block diagram of the novel CS with LE-based high speed PRNG unit on FPGA.

variety of cryptographic applications [57]. Because random numbers are needed in the generation and distribution of cryptographic keys, initial vector generation, authentication protocols, prime number and password generation, protection against side channel attacks and seed generation for pseudo-random numbers generators (PRNGs) ([58], [59]). PRNGs use the seed value obtained from some entropy source as randomness source and generate sequences that cannot be computationally distinguished from true random number generators. In addition, the streams begin to repeat after a certain period of time. So the system shows periodic feature ([60], [61]). The advantage of PRNGs is that they are inexpensive compared to other generators. Besides, the seed entropy should be large or high to ensure unpredictability ([62]–[64]). In this case, in order to increase the security and randomness of PRNGs, chaotic systems have been added to the system as a randomness source ([65]–[70]). The chaotic systems can be implemented using analog or digital circuits. The ability to model chaotic systems at high frequencies on FPGA-based chips makes chaotic systems more attractive to use in PRNG studies ([71]–[74]). The FPGA-based chaotic PRNG designs performed in recent years and the general information about these designs are presented in Table 1.

In this part of the presented study, high-speed PRNG design has been carried out to work on FPGA chip using the novel CS with LE, which is presented to the literature. The implemented high speed PRNG unit on FPGA has been encoded in 32-bit IEEE-752-1985 floating point number standard with VHDL (**V**ery High Speed Integrated Circuit **H**ardware **D**escription **L**anguage). The designed unit has been tested using Xilinx ISE Design Tools (X-ISE-DT) program. After the test phase, for the ML605 evolution board containing VIRTEX-6 FPGA chip (device, package, speed: XC6VLX75T, FF784, −3), the Place & Route operation has been performed using the X-ISE-DT program, and after the Place& Route process, the obtained chip statistics related to FPGA resource consumption have been presented. In the last phase, 1 Mbit random number sequence obtained from high speed RPNG unit has been subjected to NIST-800-22 international statistical randomness. The results obtained from the tests have been presented. The block diagram of the novel CS with LE-based high speed PRNG unit on FPGA has been given in Figure 14.

In the first stage of the study, the novel CS with LE, which is presented to the literature in this study, is given with a set of differential equations in continuous time. Various numerical algorithms have been used in literature to model the continuous-time chaotic systems on digital platforms in discrete time. Examples of these algorithms can be given as Euler, Heun, the fourth and the fifth order Runge-Kutta and the Dormand-Prince. The more parameters used in these numerical algorithms, the longer the algorithms calculation process. In addition, if the algorithm is implemented on a digital platform, both the resource consumption increases and the operating frequency of the designed oscillator decreases. As a result, the efficiency of implementations designed using chaotic oscillator including PRNG and TRNG generally decreases. In the present study, the continuous-time novel CS with LE oscillator has been discretizated using the Euler algorithm. The mathematical model for discrete-time novel CS with LE is given in Equation (27). In the Euler discretized model of the algorithm given in the equation, the initial values of $x(k)$, $y(k)$ and $z(k)$ are taken as $x(0) = 0.2$, $y(0) = 0.2$ and $z(0) = 0.2$ and system parameters are taken as $a = 2.6$ and $b = 1.5$.

$$\begin{aligned} x(k+1) &= x(k) + \Delta h \cdot (y(k)) \\ y(k+1) &= y(k) + \Delta h \cdot (-x(k) + a \cdot y(k) \cdot z(k)) \\ z(k+1) &= z(k) + \Delta h \cdot (-y(k)^2 + b \cdot \mid y(k) \mid -x(k) \cdot y(k)). \end{aligned} \tag{27}$$

Then, by utilizing the mathematical model of discrete time novel CS with LE, the chaotic oscillator unit has been coded with the 32-bit IEEE-752-1985 floating point number standard in VHDL (**V**ery High Speed Integrated Circuit **H**ardware **D**escription **L**anguage). Units such as the extractor and the multiplier used in the design have been created using Xilinx IP-Core generator and used in the design with VHDL. As can be observed from the block diagram of the design, the unit has two 1-bit length inputs as, Run and Clk. The Clk signal is used to synchronize subunits within the unit. Indeed, the Clk signal is sent to all units synchronously. However, this signal is only shown at the input to avoid complexity in the block diagram. On the other hand, Run signal is the start signal required for system operation. When Run signal, which equals to '1', is sent to the novel CS with LE-based high speed PRNG unit, this signal comes to MUX unit. The purpose of the MUX unit is to send the initial conditions to the Core unit. Core unit is designed to calculate the expression given in Equation (28) on FPGA.

$$\begin{aligned} x(k) &= (y(k)) \\ y(k) &= (-x(k) + a \cdot y(k) \cdot z(k)) \\ z(k) &= (-y(k)^2 + b \cdot \mid y(k) \mid -x(k) \cdot y(k)). \end{aligned} \tag{28}$$

When $x(k)$, $y(k)$ and $z(k)$ values are calculated in the Core unit, Ready1 = '1' and these values are transmitted to the Multiplier unit. Here, Δh is multiplied by each of the $x(k)$, $y(k)$ and $z(k)$ values and at this moment Ready2 = '1'.

TABLE 1. The chaos-based pseudo-random numbers generators designs realized on FPGA.

Reference	Used System	The Property of the Chaotic System	Discretization	NIST Test	Post Processing	Maximum Operating Frequency (MHz)	Through put (Mbps)
[60]	3-D chaotic system	Continuous time	Runge-Kutta 4	Passed	XOR	—	—
[64]	3-D chaotic system	Continuous time	Xilinx system generator	Passed	—	30.02	—
[65]	1-D Logistic map	Discrete time		Passed	XOR	132	1
[66]	4-D Hyper-chaotic system	Continuous time	Runge-Kutta 4	Passed	XOR	135.04	62.5
[67]	Lorenz + Lü	Continuous time	Euler	Passed	XOR	78.149	—
[68]	1-D Hénon chaotic map	Discrete time		Passed	—	50	3.9
[66]	1-D Bernoulli map	Discrete time		Passed	XOR	36.90	7.380
[66]	1-D Tent map	Discrete time		Passed	XOR	33.26	6.652
[66]	1-D Zigzag map	Discrete time		Passed	XOR	31.33	6.266
[70]	2-D chaotic system	Continuous time	ANN	Passed	XOR	241	241
[73]	1-D chaotic map	Discrete time		Passed	XOR	60	0.145
[74]	3-D chaotic system	Continuous time	Euler	Passed	—	298.597	—
[75]	1-D chaotic map	Discrete time		Passed	XOR	37.89	—
[76]	1-D chaotic map	Discrete time		Passed	XOR	92	—
This Work	3-D chaotic system	Continuous time	Euler	Passed	—	462.731	462.731

$S1$, $S2$ and $S3$ values calculated in the Multiplier unit are sent to the Adder Unit.

$$\begin{aligned} S1 &= \Delta h \cdot (y(k)) \\ S2 &= \Delta h \cdot (-x(k) + a \cdot y(k) \cdot z(k)) \\ S3 &= \Delta h \cdot (-y(k)^2 + b \cdot \mid y(k) \mid -x(k) \cdot y(k)). \end{aligned} \quad (29)$$

$x(k), y(k)$ and $z(k)$ values from the MUX unit and $S1, S2$ and $S3$ values are entered into the adder unit. Here, the calculation of Equation (29) is performed by summing $S1$ signal with $x(k)$, $S2$ signal with $y(k)$ and $S3$ signal with $z(k)$, respectively. The values calculated here are sent to the Filter unit. The function of the filter unit is to filter the unwanted signals generated by the novel CS with LE-based oscillator unit.

The initial conditions have been sent to the oscillator by MUX, before the oscillator produces its first results. As the novel CS with LE-based oscillator unit starts to produce its first results, the MUX unit sends these results produced by the the novel CS with LE-based oscillator unit to the input of the oscillator unit as the initial condition. The novel CS with LE-based oscillator unit generates its first results at the end of 57 clock cycle by using the initial conditions taken from the MUX unit. 3 32-bit signals namely, x_{out}, y_{out} and z_{out} receiving from the oscillator unit and 3 1-bit signals as, x_{ready}, y_{ready} and z_{ready} which indicate that x_{out}, y_{out} and z_{out}

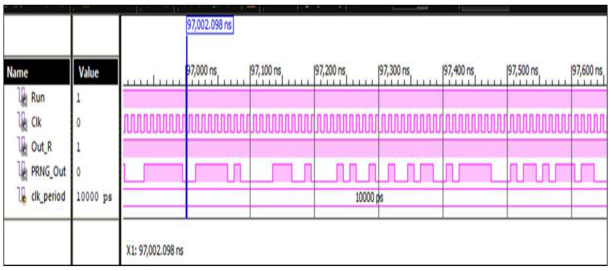

FIGURE 15. Xilinx ISE Design Tools result of the novel CS with LE based PRNG unit on FPGA.

TABLE 2. FPGA utilization statistics of the novel CS with LE based PRNG.

	Number of Slice Registers	Number of BUFGs	Number of Slice LUTs	Number of Occupied Slices	Number of DSP48E1s	Number of IOBs	Maximum Clock Frequency (MHz)
Used	8,479	1	7,681	2,335	–	4	462.731
Utilization (%)	9	3	16	20	–	1	
	93,120	32	46,560	11,640	288	360	

signals have been sent to the output of the oscillator unit, all have been transferred to the Quantification unit. There are 5 sub-units in the quantification unit: X_{RN}, Y_{RN} and Z_{RN} generator units, Mux and Counter unit. X_{RN}, Y_{RN} and Z_{RN} generator units take 19 bits from the LSB (Least Significant Bit) to MSB (Most Significant Bit), which is the most variable part of the 32-bit number receiving from oscillator unit, and send these bits to the MUX unit. Counter unit is a counter that is connected to the MUX unit and operates as 00-01-10. Whenever the value of the counter changes, the MUX unit receives the numbers from the 3 parallel outputs in a fragmented form respectively and transfers them to the PRNG output. PRNG structures presented in the literature generally consist of three main parts: oscillator part, quantification part and post/art processing part. Post Processing is generally used for the numbers generated by PRNG to successfully pass the NIST-800-22 statistical randomness tests. If Post Processing is used, the bit generation rate of PRNG decreases depending on the Post Processing structure used in PRNG design. In this presented study, apart from the PRNG structures presented to the literature, a high-speed PRNG unit design, that successfully passes randomness tests without the need of using Post Processing unit, is presented. A test bench unit has been coded in VHDL in order to test the design in X-ISE-DT program.

In Figure 15, simulation results of A Novel CS with LE-based high speed PRNG unit designed on FPGA using X-ISE-DT are given. As can be seen from the results, the A Novel CS with LE-based high speed PRNG unit on the FPGA can produce a result with every clock pulse. In Fig. 15, the simulation results of the novel CS with LE-based high speed PRNG unit designed on FPGA are given using X-ISE-DT. As can be seen from the results, the novel CS with LE-based high speed PRNG unit on the FPGA can generate the iterated results for each clock pulse after producing the first results.

Then, for the ML605 evolution board containing VIRTEX-6 FPGA chip (device, package, speed: XC6VLX75T, FF784, −3), after performing the Place & Route operation using the X-ISE-DT program, the chip statistics of FPGA resource usage have been obtained and presented in Table 2. The minimum clock period and the throughput of the novel CS with LE-based high speed PRNG unit have been observed as 2.161 ns and 462.731 Mbps, respectively.

In the final stage of the study, 1 Mbit random number sequence obtained from the novel CS with LE-based high speed PRNG unit has been recorded in a text file. Then, 1 Mbit number sequence has been subjected to NIST-800-22 tests, which are international statistical randomness tests. NIST-800-22 randomness tests consist of 16 tests as, frequency test, frequency test within a block, runs test, longest runs of ones test, binary matrix rank test, fast fourier transform test, non-overlapping template matching test, overlapping template matching test, Maurer's universal statistical test, linear complexity test, serial tests, approximate entropy test, cumulative sums test, random excursions and random excursions variant test. In order for the randomness tests to be successful, P-values should be equal or greater than 0.01 (P-values $\geq$0.01). In this case, the related test is considered as successful. In order for the generated number sequence to be considered as random, it should pass all tests in the NIST-800-22. Table 3 shows the NIST-800-22 test results for the novel CS with LE-based PRNG unit on FPGA. As can be seen in Table 3, the novel CS with LE based PRNG unit on FPGA has successfully passed all NIST-800-22 tests.

VII. IMAGE ENCRYPTION

Chaotic systems have many applications in image encryption ([42], [77]–[80]). Bao *et al.* [77] proposed a discrete memristive neuron model and discussed its interspike interval-encoded application in image encryption. Wang *et al.* [78] proposed an effective sine modular arithmetic chaotic model and applied it to image encryption. Lai *et al.* [42] presented a new memristive neuron hyper-chaotic model and proposed a new encryption scheme to apply the memristive neuron to the application of image encryption. Xian *et al.* [79] proposed a new spatiotemporal chaotic system and constructed a new cryptographic system to implement permutation–diffusion synchronous encryption. Zhu *et al.* [80] proposed a new sinusoidal-polynomial composite chaotic system and applied it to build a new image encryption scheme.

In this section, the proposed a novel 3D chaotic system with line equilibrium is applied for image encryption to resist statistical attack, brute force attack and differential attack. The image encryption system mainly includes pixel-level scrambling, bit-level scrambling, and pixel value diffusion.

The encryption algorithm not only shuffles the pixel positions of the image, but also replaces the pixel values with different values, which can effectively resist various attacks such as brute force attack and differential attack. The flow of image encryption system is shown in Figure 16.

TABLE 3. The NIST-800-22 test results for the novel CS with LE based PRNG unit on FPGA.

NIST-800-22 Statistical Tests		P-values	Results
Frequency Test		0.94101	Successful
Frequency Test within a Block		0.94541	Successful
Runs Test		0.51698	Successful
Longest Runs of Ones Test		0.04255	Successful
Binary Matrix Rank Test		0.77208	Successful
Fast Fourier Transform (Spectral) Test		0.91231	Successful
Non-overlapping Temp. Matching Test		0.97228	Successful
Overlapping Template Matching Test		0.05453	Successful
Maurer's Universal Statistical Test		0.29933	Successful
Linear Complexity Test		0.03896	Successful
Serial Test-1		0.22572	Successful
Serial Test-2		0.12419	Successful
Approximate Entropy Test		0.21660	Successful
Cumulative Sums (Forward) Test		0.77377	Successful
Random Excursions Test	x=-4	0.30687	Successful
	x=-3	0.47777	Successful
	x=-2	0.28668	Successful
	x=-1	0.27066	Successful
	x=1	0.99570	Successful
	x=2	0.96031	Successful
	x=3	0.85694	Successful
	x=4	0.67732	Successful
Random Excursions Variant Test	x=-9	0.91176	Successful
	x=-8	0.41148	Successful
	x=-7	0.22675	Successful
	x=-6	0.41754	Successful
	x=-5	0.92532	Successful
	x=-4	0.83167	Successful
	x=-3	0.71184	Successful
	x=-2	0.50957	Successful
	x=-1	0.80565	Successful
	x=1	0.88819	Successful
	x=2	0.56991	Successful
	x=3	0.53468	Successful
	x=4	0.60903	Successful
	x=5	0.41886	Successful
	x=6	0.40846	Successful
	x=7	0.78114	Successful
	x=8	0.65655	Successful
	x=9	0.46089	Successful

A. THE PROPOSED CRYPTOSYSTEM

1) KEY GENERATION

Using SHA-256 algorithm, a 256-bit binary hash value H is obtained by encrypting plain image, which is used to generate the initial values of 3D chaotic system. H is divided into 32 bytes by byte, denoted as: $h_1, h_2, \ldots, h_{32}$. According to formula (30), the initial values of the 3D chaotic system x_0, y_0 and z_0 are obtained. The initial values generated in this way has the advantage of randomness.

$$\begin{cases} x_0 = \frac{1}{256}(h_1 \oplus h_2 \oplus h_3 \oplus h_4) + h_5 + h_6 + h_7 + h_8 + x_0' \\ y_0 = \frac{1}{256}(h_9 \oplus h_{10} \oplus h_{11} \oplus h_{12}) + h_{13} + h_{14} \\ \qquad\qquad + h_{15} + h_{16} + y_0' \\ z_0 = \Sigma_{i=205}^{256} H_i * 2^{-i)} + z_0'. \end{cases} \tag{30}$$

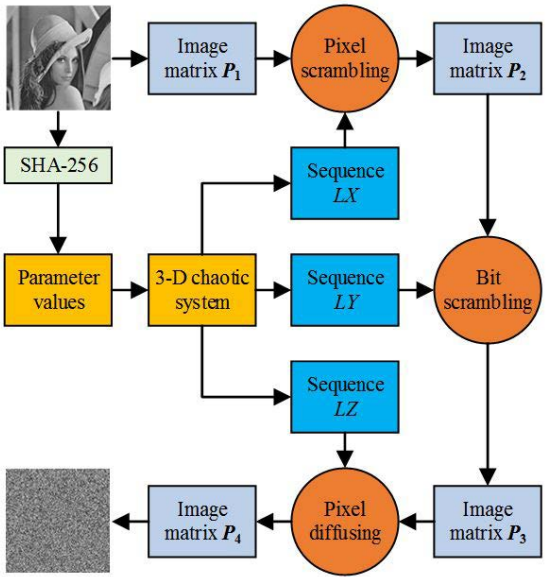

FIGURE 16. The proposed cryptosystem architecture.

where x_0', y_0' and z_0' are given values. Then, the proposed 3D chaotic system will produce three pseudo-random sequences, denoted as sequence LX, LY and LZ, respectively.

2) PIXEL SCRAMBLING

Image scrambling is to destroy the correlation of adjacent pixels by rearrangement of pixel positions, so as to achieve the purpose of information confusion and secure image transmission. Given a 2D image matrix **P** with the size $M * N$, image scrambling is mainly to find a 2D scrambling matrix **Q**, and the 2D matrix **P'** can be obtained after the transformation of the matrix **P** through the matrix **Q**. Then the corresponding relationship between **P** and **P'** as follows:

$$p_{i,j} = p'_{u,v}, \tag{31}$$

where

$$u = \text{div}(Q_{i,j} - 1, M) + 1,$$
$$v = \text{mod}(Q_{i,j} - 1, N) + 1; 1 \le i \le M, 1 \le j \le N.$$

Given the pseudo-random sequence LX, the sequence is arranged in ascending order to obtain the permutation index sequence IX. The scrambling matrix **Q** can be obtained by filling IX with M values in each row, each element $T_{i,j}$ in **T** corresponds to each element IX_k in IX as follows:

$$T_{i,j} = IX_{(i-1)*j+j}, \tag{32}$$

where $1 \le i \le M, 1 \le j \le N$.

3) BIT SCRAMBLING

Josephus is a cyclic traversal problem, which is described as follows: there are n people sitting around a round table, numbered from 1 to n. Now start counting from the person whose number is s, and the person who counts to r is removed, and then count again from the next person listed,

and the person who counts to r is removed again. Repeat this until all the people are removed. For any given n, s and r, the order in which the n people are removed can be obtained, the order is a Josephus sequence, and this process is called Josephus traversal. If the outgoing order is regarded as a traversal sequence, it is called Josephus traversal. The Josephus traversal function is defined as: $J = f(T, n, s, r)$, T stores the initial sequence before the function execution, and J stores the sequence after the traversal. n is the length of the sequence T, s is the starting position of the traversal ($1 \leq s \leq n$), and r is the interval value of traversal ($1 \leq r \leq n$).

In this paper, Josephus traversal is combined with chaotic sequence, and the pseudo-random sequence generated by 3D chaotic system is used as the starting positions of Josephus traversal to scramble the binary sequence of pixel. For each pixel, a different starting position is used. The pseudo random sequence LY generated by 3D chaotic system is processed according to the equation (33) to obtain the sequence LY', which is transformed into a matrix of the same size as the image. This matrix will be used for the starting position of Josephus traversal for image pixels.

$$ly'_i = mod(floor(10^{15} \times ly_i), 4) + 1, \tag{33}$$

where $i \in \{1, 2, \ldots, M * N\}$.

4) DIFFUSION USING BIT MANIPULATION

Good diffusion method can transform the plain image into the encrypted image with uniform distribution of pixel values, which is not vulnerable to statistical attack. In this paper, the pseudo-random sequence LZ generated by 3D chaotic system is used to perform bit-XOR operation on pixel values. The LZ sequence was preprocessed according to equation (34).

$$lz'_i = mod(floor(10^{15} \times lz_i), 256). \tag{34}$$

Transform the image into a one-dimensional sequence of length $M \times N$ in row-first order $S = \{s_1, s_2, s_3, \ldots, s_{M\times N}\}$, suppose the sequence after ciphertext diffusion is $D = \{d_1, d_2, d_3, \ldots, d_{M\times N}\}$, the diffusion equation (35) is shown as follows:

$$d_i = s_i \oplus d_{i-1} \oplus lz'_i, \tag{35}$$

where the initial element $d(0) = 127,\ i = 1, 2, \ldots, M * N$.

5) THE PROPOSED ALGORITHM

The steps of the proposed algorithm are as follows: Step 1:

- Transform plain image P into a 2D matrix P_1 with size $M * N$;
- According to the plain image, the hash value is obtained by using SHA-256 algorithm, and the initial values x_0, y_0, z_0 of 3D chaotic system are generated;
- Iterating 3D chaotic system, discard a certain number of iteration values to remove the transient effect, and three sequences LX, LY, and LZ with length of $M * N$ are obtained;
- Sort the sequence LX in ascending order, generate the index sequence and convert it into matrix form, and use the index matrix to scramble the pixel positions of the image; and get the scrambled image matrix P_2.
- Preprocess the sequence LY according to equation (33), and convert it into matrix form, denoted as sequence matrix MY, as the starting positions of Josephus traversal, scrambling each pixel in bit-level to obtain the scrambled image matrix P_3.
- Preprocess the sequence LZ according to equation (34), and the image is diffused according to equation (35) to obtain the image matrix P_4, which is the cipher image.

B. EXPERIMENTAL RESULTS AND ANALYSIS

To test the feasibility and effectiveness of the cryptosystem, four different test images (Lena, Baboon, Boat and Pepper) are taken. Given the values $x'_0 = y'_0 = z'_0 = 0.01$, the experimental results are shown in Fig. 17. All images used in this experiment are $256 * 256$ pixels in size. To prove the security of the encryption algorithm, the security analysis is carried out from the aspects of the histogram, correlation and information entropy.

1) HISTOGRAM ANALYSIS

Histogram shows the distribution of image pixel values. Histogram analysis of image can reflect the ability of encryption algorithm to resist statistical attack in terms of scrambling and diffusion. The histogram of plain image has a certain statistical rule, while cipher image should provide as little statistical information as possible. Fig. 18 shows the histograms of Lena image and its cipher image. It can be clearly seen from the figure that the pixel values of the plain image are distributed in a concentrated and regular manner, and the pixel values of the corresponding cipher image are uniform distributed, so it is difficult for attackers to obtain valuable statistical information from cipher image.

2) CORRELATION ANALYSIS

Pearson correlation coefficient is used to quantify the correlation degree of two adjacent pixels of an image, and its calculation formula is shown in (36):

$$R = \frac{\Sigma_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\Sigma_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}}, \tag{36}$$

where (x_i, y_i) is a pair of adjacent pixels, the adjacent direction can be horizontal, vertical or diagonal. N is the number of randomly selected adjacent pixel pairs. $\bar{x}$ is the average of all x_i and $\bar{y}$ is the average of all y_i.

In this paper, the correlation between adjacent pixels of different plain images and their cipher images is analyzed. The results are shown in Table 4. The distributions of correlations for lena image are shown in Fig. 19. The results show that the algorithm can effectively reduce the correlation between adjacent pixel values.

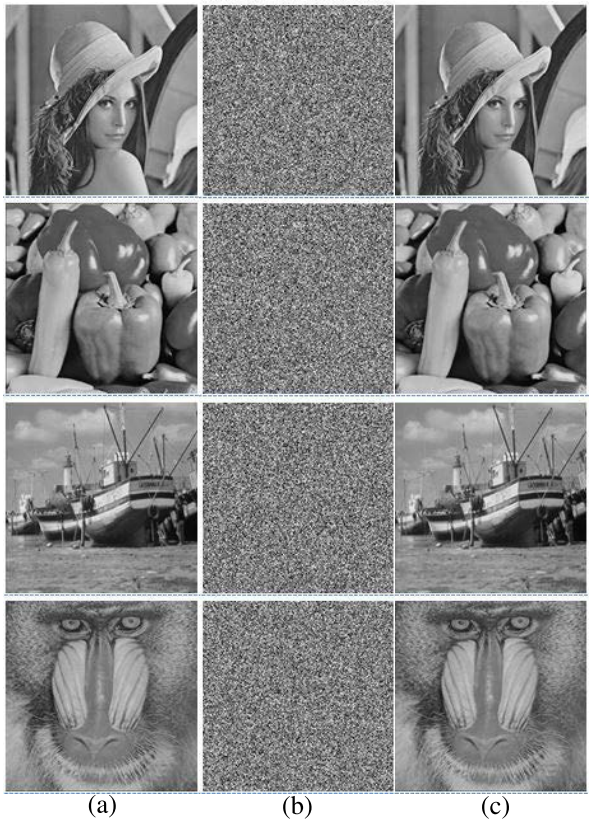

FIGURE 17. Experimental result of the proposed method. (a) Plain images, (b) Cipher images, and (c) Decrypted images.

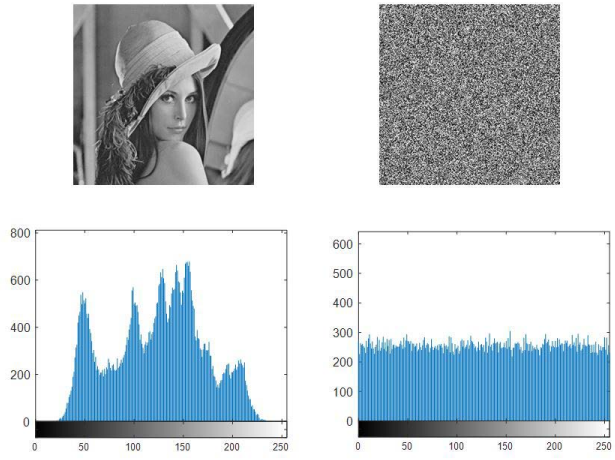

FIGURE 18. Histograms for plain image Lena and its cipher image.

3) INFORMATION ENTROPY ANALYSIS

Information entropy reflects the chaotic degree of a system, and its calculation method is shown in formula (37):

$$H = -\sum_{i=1}^{L} h(i) \log_2 h(i). \tag{37}$$

Here, $h(i)$ represents the probability of the grayscale value i. The gray level of test images in this paper is $L = 256$. The theoretical value for an cipher image is 8. The experimental data are shown in Table 5. The information entropy of the plain image is small, and the information entropy of the cipher image is very close to 8.

TABLE 4. Correlation coefficient of each direction of plain image and cipher image.

Image		Horizontal	Vertical	Diagonal
Lena	Plain image	0.9655	0.9310	0.9052
	Cipher image	-0.0028	-0.0318	-0.0043
Baboon	Plain image	0.8303	0.8777	0.7883
	Cipher image	-0.0044	-0.0097	0.0128
Boat	Plain image	0.9458	0.9277	0.8896
	Cipher image	0.0193	-0.0007	0.0038
Pepper	Plain image	0.9710	0.9663	0.9322
	Cipher image	-0.0045	0.0059	0.0001

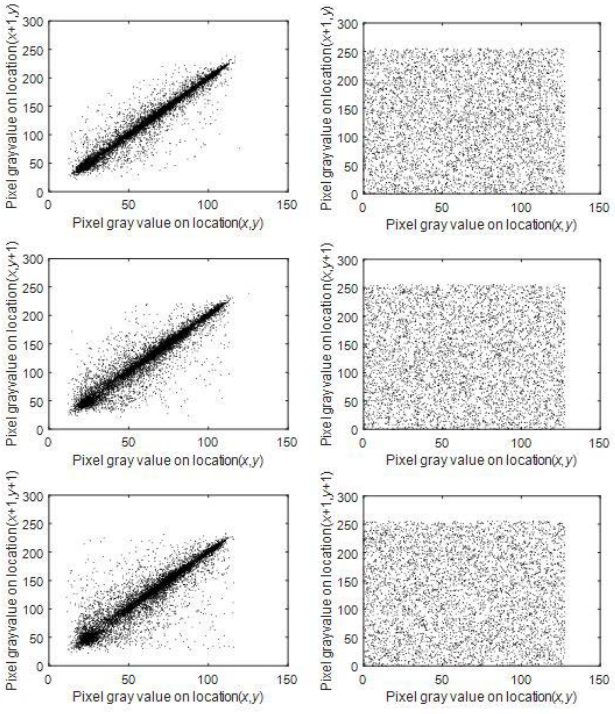

FIGURE 19. Correlation horizontally, vertically and diagonally for two adjacent pixels in plain and encrypted lena image.

TABLE 5. Information entropy.

Image	Plain image	Cipher image
Lena	7.4532	7.9976
Baboon	7.0092	7.9972
Boat	7.1572	7.9975
Pepper	7.5797	7.9971

VIII. CONCLUSION

In this work, we introduced a new chaotic system with line equilibrium. The proposed system with an absolute function nonlinearity has rich dynamics as confirmed by various attractors, Lyapunov exponents and bifurcation diagram. It is multistable as it generates coexisting chaotic attractors. As an engineering application, we have shown new synchronization results for the new chaotic system

with line equilibrium using Integral Sliding Mode Control (ISMC). In addition, the designed circuit shows the feasibility of the proposed new chaotic system with line equilibrium. Furthermore, implementation of the new chaotic system by using a field-programmable gate array (FPGA) based on Pseudo-Random Number Generators (PRNGs) was presented in this work. By using FPGA-based implementation of the new chaotic system, a novel high-speed Pseudo-Random Number Generators (PRNGs) algorithm was contructed and its implementation was detailed. Finally, an image encryption algorithm based on the pixel-level scrambling, bit-level scrambling, and pixel value diffusion is proposed. The experimental results show that the encryption algorithm not only shuffles the pixel positions of the image, but also replaces the pixel values with different values, which can effectively resist various attacks such as brute force attack and differential attack.

REFERENCES

[1] T. Liu, H. Yan, S. Banerjee, and J. Mou, "A fractional-order chaotic system with hidden attractor and self-excited attractor and its DSP implementation," *Chaos, Solitons Fractals*, vol. 145, Apr. 2021, Art. no. 110791.

[2] C. Li, Z. Gu, Z. Liu, S. Jafari, and T. Kapitaniak, "Constructing chaotic repellors," *Chaos, Solitons Fractals*, vol. 142, Jan. 2021, Art. no. 110544.

[3] S. Vaidyanathan, A. Sambas, B. Abd-El-Atty, A. A. A. El-Latif, E. Tlelo-Cuautle, O. Guillen-Fernandez, M. Mamat, M. A. Mohamed, M. Alcin, M. Tuna, I. Pehlivan, I. Koyuncu, and M. A. H. Ibrahim, "A 5-D multi-stable hyperchaotic two-disk dynamo system with no equilibrium point: Circuit design, FPGA realization and applications to TRNGs and image encryption," *IEEE Access*, vol. 9, pp. 81352–81369, 2021.

[4] M. Gao, Y. Wang, Y. Wang, and P. Wang, "Experimental investigation of non-linear multi-stable electromagnetic-induction energy harvesting mechanism by magnetic levitation oscillation," *Appl. Energy*, vol. 220, pp. 856–875, Jun. 2018.

[5] F. Alonge, M. Branciforte, and F. Motta, "A novel method of distance measurement based on pulse position modulation and synchronization of chaotic signals using ultrasonic radar systems," *IEEE Trans. Instrum. Meas.*, vol. 58, no. 2, pp. 318–329, Feb. 2009.

[6] H. Bi, G. Qi, J. Hu, P. Faradja, and G. Chen, "Hidden and transient chaotic attractors in the attitude system of quadrotor unmanned aerial vehicle," *Chaos, Solitons Fractals*, vol. 138, Sep. 2020, Art. no. 109815.

[7] M. F. P. Polo, M. P. Molina, and J. G. Chica, "Chaotic dynamic and control for micro-electro-mechanical systems of massive storage with harmonic base excitation," *Chaos, Solitons Fractals*, vol. 39, no. 3, pp. 1356–1370, Feb. 2009.

[8] D. Singh, "Ride comfort analysis of passenger body biodynamics in active quarter car model using adaptive neuro-fuzzy inference system based super twisting sliding mode control," *J. Vib. Control*, vol. 25, no. 12, pp. 1866–1882, Jun. 2019.

[9] A. Sambas, S. Vaidyanathan, E. Tlelo-Cuautle, B. Abd-El-Atty, A. A. A. El-Latif, O. Guille-Fernandez, 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.

[10] S. Vaidyanathan, A. Sambas, M. Mamat, and W. M. Sanjaya, "A new three-dimensional chaotic system with a hidden attractor, circuit design and application in wireless mobile robot," *Arch. Control Sci.*, vol. 27, no. 4, pp. 541–554, 2017.

[11] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed CMOS true random number generators based on chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 12, pp. 3124–3137, Dec. 2010.

[12] A. Sambas, S. He, H. Liu, S. Vaidyanathan, Y. Hidayat, and J. Saputra, "Dynamical analysis and adaptive fuzzy control for the fractional-order financial risk chaotic system," *Adv. Difference Equ.*, vol. 674, no. 1, pp. 1–12, Dec. 2020.

[13] M. S. T. De Freitas, R. L. Viana, and C. Grebogi, "Multistability, basin boundary structure, and chaotic behavior in a suspension bridge model," *Int. J. Bifurcation Chaos*, vol. 14, no. 3, pp. 927–950, Mar. 2004.

[14] A. Sambas, S. Vaidyanathan, T. Bonny, S. Zhang, Y. Hidayat, G. Gundara, and M. Mamat, "Mathematical model and FPGA realization of a multi-stable chaotic dynamical system with a closed butterfly-like curve of equilibrium points," *Appl. Sci.*, vol. 11, no. 2, p. 778, 2021.

[15] G. Litak, M. Borowiec, M. I. Friswell, and W. Przystupa, "Chaotic response of a quarter car model forced by a road profile with a stochastic component," *Chaos, Solitons Fractals*, vol. 39, no. 5, pp. 2448–2456, Mar. 2009.

[16] C. Li, J. C. T. Wesley, H. C. I. Herbert, and T. Lu, "A memristive chaotic oscillator with increasing amplitude and frequency," *IEEE Access*, vol. 6, pp. 12945–12950, 2018.

[17] S. Mobayen, A. Fekih, S. Vaidyanathan, and A. Sambas, "Chameleon chaotic systems with quadratic nonlinearities: An adaptive finite-time sliding mode control approach and circuit simulation," *IEEE Access*, vol. 9, pp. 64558–64573, 2021.

[18] P. Zhou and F. Yang, "Hyperchaos, chaos, and horseshoe in a 4D nonlinear system with an infinite number of equilibrium points," *Nonlinear Dyn.*, vol. 76, no. 1, pp. 473–480, Apr. 2014.

[19] S. Jafari and J. C. Sprott, "Simple chaotic flows with a line equilibrium," *Chaos, Solitons Fractals*, vol. 57, pp. 79–84, Dec. 2013.

[20] K. Benkouider, T. Bouden, A. Sambas, M. A. Mohamed, I. M. Sulaiman, M. Mamat, and M. A. H. Ibrahim, "Dynamics, control and secure transmission electronic circuit implementation of a new 3D chaotic system in comparison with 50 reported systems," *IEEE Access*, vol. 9, pp. 152150–152168, 2021.

[21] S. T. Kingni, V.-T. Pham, S. Jafari, and P. Woafo, "A chaotic system with an infinite number of equilibrium points located on a line and on a hyperbola and its fractional-order form," *Chaos, Solitons Fractals*, vol. 99, pp. 209–218, Jun. 2017.

[22] L. Moysis, C. Volos, V.-T. Pham, S. Goudos, I. Stouboulos, M. K. Gupta, and V. K. Mishra, "Analysis of a chaotic system with line equilibrium and its application to secure communications using a descriptor observer," *Technologies*, vol. 7, no. 4, p. 76, Oct. 2019.

[23] A. Sambas, M. Mamat, A. A. Arafa, G. M. Mahmoud, M. A. Mohamed, and W. S. Sanjaya, "A new chaotic system with line of equilibria: Dynamics, passive control and circuit design," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 4, pp. 2365–2376, 2019.

[24] F. Nazarimehr, K. Rajagopal, J. Kengne, S. Jafari, and V.-T. Pham, "A new four-dimensional system containing chaotic or hyper-chaotic attractors with no equilibrium, a line of equilibria and unstable equilibria," *Chaos, Solitons Fractals*, vol. 111, pp. 108–118, Jun. 2018.

[25] H. Chen, T. Lei, S. Lu, W. Dai, L. Qiu, and L. Zhong, "Dynamics and complexity analysis of fractional-order chaotic systems with line equilibrium based on Adomian decomposition," *Complexity*, vol. 2020, Oct. 2020, Art. no. 5710765.

[26] K. Benkouider, T. Bouden, A. Sambas, M. A. Mohamed, I. M. Sulaiman, and M. Mamat, "A new 10-D hyperchaotic system with coexisting attractors and high fractal dimension: Its dynamical analysis, synchronization and circuit design," *PLoS ONE*, vol. 17, no. 4, pp. 1–31, Apr. 2022.

[27] K. Benkouider, A. Sambas, I. M. Sulaiman, M. Mamat, and S. N. Kottakkaran, "Secure communication scheme based on a new hyperchaotic system," *Comput., Mater. Continua*, vol. 2022, pp. 1–15, Jan. 2022.

[28] H. Bao, M. Chen, H. Wu, and B. Bao, "Memristor initial-boosted coexisting plane bifurcations and its extreme multi-stability reconstitution in two-memristor-based dynamical system," *Sci. China Technol. Sci.*, vol. 63, no. 4, pp. 603–613, Apr. 2020.

[29] S. Mobayen, "Chaos synchronization of uncertain chaotic systems using composite nonlinear feedback based integral sliding mode control," *ISA Trans.*, vol. 77, pp. 100–111, Jun. 2018.

[30] J.-B. Wang, C.-X. Liu, Y. Wang, and G.-C. Zheng, "Fixed time integral sliding mode controller and its application to the suppression of chaotic oscillation in power system," *Chin. Phys. B*, vol. 27, no. 7, Jul. 2018, Art. no. 070503.

[31] V. Vafaei, H. Kheiri, and A. J. Akbarfam, "Synchronization of fractional-order chaotic systems with disturbances via novel fractional-integer integral sliding mode control and application to neuron models," *Math. Methods Appl. Sci.*, vol. 42, no. 8, pp. 2761–2773, May 2019.

[32] B. Sarsembayev, K. Suleimenov, B. Mirzagalikova, and T. D. Do, "SDRE-based integral sliding mode control for wind energy conversion systems," *IEEE Access*, vol. 8, pp. 51100–51113, 2020.

[33] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A chaos based image encryption scheme using digit-level permutation and block diffusion," *IEEE Access*, vol. 6, pp. 67581–67593, 2018.
[34] J. Wu, J. Shi, and T. Li, "A novel image encryption approach based on a hyperchaotic system, pixel-level filtering with variable kernels, and DNA-level diffusion," *Entropy*, vol. 22, no. 1, p. 5, Dec. 2019.
[35] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 167, Feb. 2020, Art. no. 107286.
[36] C.-L. Li, Y. Zhou, H.-M. Li, W. Feng, and J.-R. Du, "Image encryption scheme with bit-level scrambling and multiplication diffusion," *Multimedia Tools Appl.*, vol. 80, no. 12, pp. 18479–18501, May 2021.
[37] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107484.
[38] Q. Lai, Z. Wang, and P. D. K. Kuate, "Dynamical analysis, FPGA implementation and synchronization for secure communication of new chaotic system with hidden and coexisting attractors," *Mod. Phys. Lett. B*, vol. 36, no. 1, Jan. 2022, Art. no. 2150538.
[39] K. Rajagopal, Y. Shekofteh, F. Nazarimehr, C. Li, and S. Jafari, "A new chaotic multi-stable hyperjerk system with various types of attractors," *Indian J. Phys.*, vol. 96, no. 5, pp. 1501–1507, Apr. 2022.
[40] X. Wang, X. Long, X. Yue, H. Dai, and S. N. Atluri, "Bifurcation analysis of stick–slip vibration in a 2-DOF nonlinear dynamical system with dry friction," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 111, Aug. 2022, Art. no. 106475.
[41] B. Zhou, Y. Jin, and H. Xu, "Subharmonic resonance and chaos for a class of vibration isolation system with two pairs of oblique springs," *Appl. Math. Model.*, vol. 108, pp. 427–444, Aug. 2022.
[42] Q. Lai, C. Lai, H. Zhang, and C. Li, "Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption," *Chaos, Solitons Fractals*, vol. 158, May 2022, Art. no. 112017.
[43] W. Zhang, F. Min, J. Chen, and Y. Dou, "Discontinuous dynamic analysis of a modified Duffing-Rayleigh system with a piecewise quadratic function," *IEEE Access*, vol. 8, pp. 32312–32320, 2020.
[44] J. M. Muñoz-Pacheco, E. Zambrano-Serrano, O. Félix-Beltrán, L. C. Gómez-Pavón, and A. Luis-Ramos, "Synchronization of PWL function-based 2D and 3D multi-scroll chaotic systems," *Nonlinear Dyn.*, vol. 70, no. 2, pp. 1633–1643, Oct. 2012.
[45] R. Montero-Canela, E. Zambrano-Serrano, E. I. Tamariz-Flores, J. M. Muñoz-Pacheco, and R. Torrealba-Meléndez, "Fractional chaos based-cryptosystem for generating encryption keys in ad hoc networks," *Ad Hoc Netw.*, vol. 97, Feb. 2020, Art. no. 102005.
[46] J. M. Munoz-Pacheco, L. C. Lujano-Hernández, C. Muñiz-Montero, A. Akgül, L. A. Sánchez-Gaspariano, C.-B. Li, and M. Ç. Kutlu, "Active realization of fractional-order integrators and their application in multiscroll chaotic systems," *Complexity*, vol. 2021, pp. 1–16, Jan. 2021.
[47] 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, 1985.
[48] S. Zhang, J. Zheng, X. Wang, Z. Zeng, and S. He, "Initial offset boosting coexisting attractors in memristive multi-double-scroll Hopfield neural network," *Nonlinear Dyn.*, vol. 102, no. 4, pp. 2821–2841, Dec. 2020.
[49] S. Zhang and Y. Zeng, "A simple Jerk-like system without equilibrium: Asymmetric coexisting hidden attractors, bursting oscillation and double full Feigenbaum remerging trees," *Chaos, Solitons Fractals*, vol. 120, pp. 25–40, Mar. 2019.
[50] 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.
[51] M. Alcin, I. Koyuncu, M. Tuna, M. Varan, and I. Pehlivan, "A novel high speed artificial neural network-based chaotic true random number generator on field programmable gate array," *Int. J. Circuit Theory Appl.*, vol. 47, no. 3, pp. 365–378, Mar. 2019.
[52] İ. Koyuncu, M. Tuna, İ. Pehlivan, C. B. Fidan, and M. Alçın, "Design, FPGA implementation and statistical analysis of chaos-ring based dual entropy core true random number generator," *Anal. Integr. Circuits Signal Process.*, vol. 102, no. 2, pp. 445–456, Feb. 2020.
[53] İ. Koyuncu and A. T. Özcerit, "The design and realization of a new high speed FPGA-based chaotic true random number generator," *Comput., Electr. Eng.*, vol. 58, pp. 203–214, Feb. 2017.
[54] M. Tuna and C. B. Fidan, "A study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems," *J. Fac. Eng. Archit. Gazi Univ.*, vol. 33, no. 2, pp. 469–486, 2018.
[55] E. Avaroğlu, İ. Koyuncu, A. B. Özer, and M. Türk, "Hybrid pseudo-random number generator for cryptographic systems," *Nonlinear Dyn.*, vol. 82, nos. 1–2, pp. 239–248, Oct. 2015.
[56] E. Avaroğlu, "Pseudorandom number generator based on Arnold cat map and statistical analysis," *TURKISH J. Electr. Eng. Comput. Sci.*, vol. 25, no. 1, pp. 633–643, 2017.
[57] B. F. Vajargah and R. Asghari, "A novel pseudo-random number generator for cryptographic applications," *Indian J. Sci. Technol.*, vol. 9, no. 6, pp. 1–5, Feb. 2016.
[58] P. Prakash, K. Rajagopal, I. Koyuncu, J. P. Singh, M. Alcin, B. K. Roy, and M. Tuna, "A novel simple 4-D hyperchaotic system with a saddle-point index-2 equilibrium point and multistability: Design and FPGA-based applications," *Circuits, Syst., Signal Process.*, vol. 39, pp. 4259–4280, Feb. 2020.
[59] A. M. Garipcan and E. Erdem, "Implementation and performance analysis of true random number generator on FPGA environment by using non-periodic chaotic signals obtained from chaotic maps," *Arabian J. Sci. Eng.*, vol. 44, no. 11, pp. 9427–9441, Nov. 2019.
[60] E. Avaroğlu, T. Tuncer, A. B. Özer, and M. Türk, "A new method for hybrid pseudo random number generator," *Informacije MIDEM*, vol. 44, no. 4, pp. 303–311, 2014.
[61] E. Avaroglu, T. Tuncer, A. B. Ozer, B. Ergen, and M. Turk, "A novel chaos-based post-processing for TRNG," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 189–199, Jul. 2015.
[62] M. J. Barani, P. Ayubi, M. Y. Valandar, and B. Y. Irani, "A new pseudo random number generator based on generalized Newton complex map with dynamic key," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102509.
[63] T. Tuncer, "The implementation of chaos-based PUF designs in field programmable gate array," *Nonlinear Dyn.*, vol. 86, no. 2, pp. 975–986, 2016.
[64] L. Merah, A. Ali-Pacha, N. H. Said, and M. Mamat, "A pseudo random number generator based on the chaotic system of Chua's circuit, and its real time FPGA implementation," *Appl. Math. Sci.*, vol. 7, no. 55, pp. 2719–2734, 2013.
[65] M. Garcia-Bosque, A. Pérez-Resa, C. Sánchez-Azqueta, C. Aldea, and S. Celma, "Chaos-based bitwise dynamical pseudorandom number generator on FPGA," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 1, pp. 291–293, Jan. 2019.
[66] F. Yu, Q. Wan, J. Jin, L. Li, B. He, L. Liu, S. Qian, Y. Huang, S. Cai, Y. Song, and Q. Tang, "Design and FPGA implementation of a pseudo-random number generator based on a four-wing memristive hyperchaotic system and Bernoulli map," *IEEE Access*, vol. 7, pp. 181884–181898, 2019.
[67] A. A. Rezk, A. H. Madian, A. G. Radwan, and A. M. Soliman, "Reconfigurable chaotic pseudo random number generator based on FPGA," *AEU-Int. J. Electron. Commun.*, vol. 98, pp. 174–180, Jan. 2019.
[68] M. O. Meranza-Castillón, M. A. Murillo-Escobar, R. M. López-Gutiérrez, and C. Cruz-Hernández, "Pseudorandom number generator based on enhanced Hénon map and its implementation," *AEU-Int. J. Electron. Commun.*, vol. 107, pp. 239–251, Jul. 2019.
[69] L. De la Fraga, E. Torres-Pérez, E. Tlelo-Cuautle, and C. Mancillas-López, "Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dyn.*, vol. 90, no. 3, pp. 1661–1670, Nov. 2017.
[70] M. Tuna, "A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: Design and its FPGA implementation," *Anal. Integr. Circuits Signal Process.*, vol. 105, no. 2, pp. 167–181, Nov. 2020.
[71] P. Dabal and R. Pelka, "A chaos-based pseudo-random bit generator implemented in FPGA device," in *Proc. 14th IEEE Int. Symp. Design Diag. Electron. Circuits Syst.*, Apr. 2011, pp. 151–154.
[72] M. Garcia-Martinez and E. Campos-Canton, "Pseudo-random bit generator based on multi-modal maps," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 2119–2131, Dec. 2015.
[73] L. Palacios-Luengas, J. L. Pichardo-Méndez, J. A. Díaz-Méndez, F. Rodríguez-Santos, and R. Vázquez-Medina, "PRNG based on skew tent map," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 3817–3830, Apr. 2019.
[74] A. A. Rezk, A. H. Madian, A. G. Radwan, and A. M. Soliman, "Multiplierless chaotic pseudo random number generators," *AEU-Int. J. Electron. Commun.*, vol. 113, Jan. 2020, Art. no. 152947.

[75] R. A. Elmanfaloty and E. Abou-Bakr, "Random property enhancement of a 1D chaotic PRNG with finite precision implementation," *Chaos, Solitons Fractals*, vol. 118, pp. 134–144, Jan. 2019.
[76] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Design and FPGA implementation of a pseudo random bit generator using chaotic maps," *IETE J. Res.*, vol. 59, no. 1, pp. 63–73, 2013.
[77] H. Bao, Z. Hua, W. Liu, and B. Bao, "Discrete memristive neuron model and its interspike interval-encoded application in image encryption," *Sci. China Technol. Sci.*, vol. 64, no. 10, pp. 2281–2291, Oct. 2021.
[78] X. Wang, N. Guan, and P. Liu, "A selective image encryption algorithm based on a chaotic model using modular sine arithmetic," *Optik*, vol. 258, May 2022, Art. no. 168955.
[79] Y. Xian, X. Wang, L. Teng, X. Yan, Q. Li, and X. Wang, "Cryptographic system based on double parameters fractal sorting vector and new spatiotemporal chaotic system," *Inf. Sci.*, vol. 596, pp. 304–320, Jun. 2022.
[80] 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.

ACENG SAMBAS received the Ph.D. degree in mathematics from Universiti Sultan Zainal Abidin (UniSZA), Malaysia, in 2021. He has been a Lecturer with the Muhammadiyah University of Tasikmalaya, Indonesia, since 2015. His current research interests include dynamical systems, chaotic signals, electrical engineering, computational science, signal processing, robotics, embedded systems, and artificial intelligence.

SUNDARAPANDIAN VAIDYANATHAN received the D.Sc. degree in electrical and systems engineering from Washington University, St. Louis, USA, in 1996. He is currently a Professor with the Research and Development Centre, Vel Tech University, Chennai, India. He has published three text-books on mathematics and 12 research books on control engineering. He has published over 410 Scopus-indexed research publications. He has also conducted many workshops on control systems and chaos theory using MATLAB and SCILAB. His current research interests include control systems, chaotic and hyperchaotic systems, backstepping control, sliding mode control, intelligent control, computational science, and robotics.

XUNCAI ZHANG was born in Zhoukou, China, in 1981. He received the Ph.D. degree from the Huazhong University of Science and Technology, in 2009. From 2010 to 2012, he accomplished the Postdoctoral Research with Peking University. He is currently an Associate Professor with the School of Electrical and Information Engineering, Zhengzhou University of Light Industry. His research interests include DNA computing and information security.

ISMAIL KOYUNCU received the M.Sc. degree from Abant Izzet Baysal University, Bolu, Turkey, and the Ph.D. degree from the Department of Electrical and Electronics Engineering, Sakarya University, Sakarya, Turkey, in 2014. Since 2017, he has been an Associate Professor with the Department of Electrical and Electronic Engineering, Afyon Kocatepe University, Afyon, Turkey. His research interests include FPGA-based digital system design, chaos, TRNG, and reconfigurable computing. He is also interested in FPGA-based artificial neural networks and computer graphics.

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 is currently an Associate Professor with the Department of Computer Engineering, College of Computing and Informatics, University of Sharjah, where he has been 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/a TPC member in many IEEE/ACM journals/conferences. He was a Session Chair of the IEEE Conference in Advances in Artificial Intelligence.

MURAT TUNA received the B.Sc. degree in electrical education from the Kocaeli University of Technical Education, in 2004, the M.Sc. degree in electrical education from the University of Institute of Science, Kocaeli, Turkey, in 2008, and the Ph.D. degree from the Department of Electrical and Electronics Engineering, Karabuk University, Karabuk, Turkey, in 2017. He has been working as an Assistant Professor with Kirklareli University, Turkey, since 2009. His research interests include chaos, TRNG, FPGA-based digital system design, and reconfigurable computing. He is also interested in mathematical model and control of nonlinear systems.

MURAT ALÇIN received the B.Sc. and M.Sc. degrees in electronic and computer teaching from the University of Marmara, Turkey, in 2006 and 2009, respectively, and the Ph.D. degree in electronic and computer teaching from the Department of Electrical and Electronics Engineering, Sakarya University, Sakarya, Turkey, in 2017. From 2008 to 2012, he was an Instructor under the Electronic Technology Program with the Bolu Vocational School, Abant Izzet Baysal University, Bolu, Turkey. Since 2018, he has been an Assistant Professor with the Department of Mechatronics Engineering, Afyon Kocatepe University, Afyon, Turkey. His research interests include neural networks, chaotic systems, and FPGA-based digital system design.

SEN ZHANG received the B.Sc. degree in electronic science and technology from the Zhengzhou University of Light Industry, Zhengzhou, China, in 2015, and the M.S. degree in electronic science and technology from the School of Physics and Opotoelectric Engineering, Xiangtan University, Xiangtan, China, in 2019. He is currently pursuing the Ph.D. degree in artificial intelligence with the School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan, China. His current research interests include memristive systems and circuits, chaos and fractional-order chaotic systems and circuits, and design and implementation of brain-like intelligent computing circuits based on memristor.

IBRAHIM MOHAMMED SULAIMAN received the Ph.D. degree specializing in the field of fuzzy systems from Universiti Sultan Zainal Abidin (UniSZA), Malaysia, in 2018. He has been a Postdoctoral Researcher with the Faculty of Informatics and Computing, UniSZA, since 2019. He has published research papers in various international journals and attended international conferences. His research interests include numerical research, fuzzy nonlinear systems, and unconstrained optimization.

ALIYU MUHAMMED AWWAL received the B.Sc. degree from Gombe State University, the M.Sc. degree from Bayero University Kano, and the Ph.D. degree in applied mathematics from the King Mongkut's University of Technology Thonburi (KMUTT). He has authored and coauthored a number of research articles in high impact journals. His current research interests include iterative algorithms for solving nonlinear problems, such as numerical optimization problems, nonlinear least squares problems and system of nonlinear equations with applications in signal recovery, image deblurring, and motion control.

POOM KUMAM (Member, IEEE) received the Ph.D. degree in mathematics from Naresuan University, Thailand. He is currently a Full Professor with the Department of Mathematics, King Mongkut's University of Technology Thonburi (KMUTT), where he is also the Head of the Fixed Point Theory and Applications Research Group, and also with the Theoretical and Computational Science Center (TaCS-Center). He is also the Director of the Computational and Applied Science for Smart Innovation Cluster (CLASSIC Research Cluster), KMUTT. His research interests include fixed point theory, variational analysis, random operator theory, optimization theory, and approximation theory. Also, fractional differential equations, differential game, entropy and quantum operators, fuzzy soft set, mathematical modeling for fluid dynamics and areas of interest inverse problems, dynamic games in economics, traffic network equilibria, bandwidth allocation problem, wireless sensor networks, image restoration, signal and image processing, game theory, and cryptology. He has provided and developed many mathematical tools in his fields productively over the past years. He has over 800 scientific papers and projects either presented or published. Moreover, he is the editorial board of more than 50 journals and also he delivers many invited talks on different international conferences every year all around the world.