IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 24, 2021, accepted December 8, 2021, date of publication December 14, 2021,
date of current version December 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3135519

On Ghost Attractor in Blinking Chaotic MVD Memristor-Based Circuit and Its Application

RAJAGOPALAN RAMASWAMY[1], A. M. A. EL-SAYED[2], A. A. ELSADANY[1,3], AND AMR ELSONBATY[1,4]

[1]Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[2]Department of Mathematics and Computer Science, Faculty of Science, Alexandria University, Alexandria 21544, Egypt
[3]Department of Basic Science, Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt
[4]Department of Mathematics and Engineering Physics, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt

Corresponding author: Rajagopalan Ramaswamy (r.gopalan@psau.edu.sa)

This work was supported by the Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia.

ABSTRACT This work is devoted to explore the possible existence of ghost attractors in a proposed nonautonomous blinking circuit with nonlinear memristors along with their potential application. The nonlinear dynamics of new memristor-based blinking circuit are significantly influenced by the speed of random switchings between its autonomous subcircuits. So, the effects of varying stochastic switching rate on the dynamical behaviors of blinking circuit are examined. It is demonstrated that it is possible to stimulate a non-stationary chaotic attractor for the blinking circuit which is surprisingly different from the attractors of composing subcircuits which exhibit simple periodic dynamics. A sufficiently small time period for random switchings in addition to precise tuning of circuit parameters are the major requirements for establishing these ghost attractors. The fascinating features of the induced ghost attractors render them appropriate noise-like source for secure communications applications. So, we proposed a new pseudo-chaos encryption algorithm that exploits the memristor-based blinking circuit in a more suitable digital platform. The proposed scheme overcomes the usual degradation in performance of digital chaos due to finite precision representation of floating numbers.

INDEX TERMS Memristors, pseudo-chaos encryption, ghost attractors, blinking circuit.

I. INTRODUCTION

The real-world systems from engineering, biology, science, astronomy and economy disciplines are great sources for interesting nonlinear phenomena which considerably attract attention of researchers and scientists [1] and [2]. The tools and methods of dynamical systems play a crucial role in analyzing, describing and interpreting of these phenomena. Indeed, the advances in our understanding of nonlinear systems stimulate the developments of new mathematical theories and methods in addition to the invention of many innovative modern technologies which reshape our lives [3]–[8].

The Chua's diode, has been introduced in the mid-1960s by L.O. Chua with a piecewise-continuous voltage-current relationship and has represented the core element in the well-recognized chaotic Chua's circuit [9]. Since then, plethora of nonlinear circuits have been introduced where several nonlinear complicated behaviors, including the interesting chaotic dynamics, have been exhibited by these systems and considerably gained a lot of scientists' interest. The modified Van der Pol oscillator [10], the chaotic autonomous Van der Pol-Duffing circuit [11] and modified autonomous Van der Pol-Duffing circuit [12] are examples of members in a single family of nonlinear circuits.

Along with resistors, capacitors and inductors, the fourth element of the fundamental elements in electronic circuits, namely, the memristor, has been proposed in 1971 by L. O. Chua [13]. The magnetic flux between memristor's terminals is a function of the electric charges passe through it [13] and [14]. The hypothetical memristor of Chua was practically fabricated by Williams et. al. [14]. Many remarkable applications of memristors have been introduced since its implementation such as nano-scale high frequency chaotic oscillators, artificial intelligence, learning networks, ultradense nonvolatile memories and digital logic circuits For more details, see [15]–[20] and references therein.

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

Random switching is a key process in diverse engineering systems which operate by varying the coupling and interaction among their components randomly in short time intervals. Examples of these systems include the pulse power converters, neural networks, the Internet, power grids and similar dynamical networks [21]–[23]. The term 'blinking system' is used to denote the dynamical system with random independent switching parameters. The dynamical behaviors of blinking systems are very interesting since they can be remarkably dissimilar from the dynamics of their composing subsystems [22]–[25]. The works of M. Hasler, V. Belykh, and I. Belykh, R. Jeter and N. Barabash provided some significant results in this line of research. More specifically, they introduced a general theory which explains the asymptotic dynamics and non-stationary attractors in stochastic blinking systems and their connection with the dynamics of corresponding time-averaged systems. In the case of sufficient fast switching rate, it is found that the trajectory of the blinking system can converge toward a vicinity of what is called ghost attractor and stick out close to it most of time [24]–[26]. Examples of blinking nonlinear rotators, Lorenz systems and Hindmarsh–Rose systems are presented to illustrate the rigorous theoretical findings, see preceding references. However, the application of the aforementioned theory to dynamical behaviors of blinking nonlinear circuits remain unexplored. This motivates the authors to investigate this point especially for the promising memristor-based chaotic circuits as a first goal for this work.

Moreover, the continuous rapid developments in the means of transferring and storing information are essential landmark of the recent technological revolution. For example, the internet, PCs, laptops, smart phones, ATMs, digital cameras, etc, have become integral part of our daily life. However, the requirements of transmitting and storing crucial data in a secured machines have also increased due to many potential threats and set up a great challenge for engineers, mathematicians and computer scientists to find appropriate security solutions [27]–[29]. The encryption/decryption operations in first generations of encryption systems can be carried out by hand and thus can be easily cracked by modern available technologies even if only sufficient ciphertext is known to the attacker. Indeed, a plethora of efficient techniques have been emanated and employed for the purpose of cryptanalysis of classical ciphers. They include brute force attack, ciphertext-only attack, frequency analysis and Kasiski's method [27]–[32].

The one-time pad is an encryption technique which has been described and studied in the works of F. Miller, G. Vernam and J. Mauborgne. It relies on pre-shared key between legitimate transmitter and receiver sides and, interestingly, it is impossible to be broken by attackers provided that three conditions are satisfied. The first is that the key is at least as long as the plaintext, the second condition is that it is used only for one time, and finally, the key should be completely random [33]. The key problem which associates with this type of encryption is how to effectively achieve secure key distribution.

The main goal of modern strong ciphers is to successfully hold up against a wide range of attacks which are more vigorous than ciphertext-only attacks. Examples of these attacks involve man in the middle attack, differential attack, chosen-ciphertext attack, known-plaintext attack and chosen-plaintext attack. In particular, the robust encryption systems apply the principles of diffusion and confusion to render any potential attacker fails in extracting the key when particular pieces of plain information and associated encrypted information are known for him, or even if he has the ability to pick out plain data and cipher data. From classification point of view, the modern cryptography techniques can be classified into two groups, namely, symmetric-key methods and public-key methods. Examples of symmetric-key cryptography include block ciphers, such as Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), and RC4 stream cipher. The first principles of public-key cryptography have been set up by J. Ellis, M. Williamson, C. Cocks and W. Diffie, M. Hellman in 1970s and then developed to many well-known encryption algorithms, e.g. RSA, Cramer–Shoup, Digital Signature Algorithm (DSA), El-Gamal, and elliptic curves [31], [32].

The attractive characteristics of chaotic systems imply that chaotic dynamics have the ability to hide information data in both of frequency and time domains. Therefore, chaos-based secure communications schemes attained a great attention in recent years where several ways are applied in hardware and software layers to achieve secret transmission of information, see [34]–[37] and references therein. For example of recent achievements, a proposed chaotic based OFDM-PON (orthogonal frequency-division multiple access-based passive optical networks) is investigated for reliable 18.86 Gb/s cipher signal transmission over 25 Km [38]. A two-dimensional adjusted logistic sine map is combined with block dividing scheme and dynamic key assignment scheme is presented to improve OFDM-PON technique[39]. The three-dimensional Brownian motion and DNA encoding are demonstrated in chaos-based encryption schemes in [40] and [41], respectively. However, it is essential to examine the security performance of chaos based communications systems and propose the necessary improvements which boost their immunity against different attacks [34], [42], [43].

In chaos-based encryption systems which rely on chaos synchronization, a drive chaotic signal is needed and transmitted in public channel to acquire synchronization state for transmitter and receiver entities [33], [44], [45]. Also, the transmitter and receiver sides should have identical values of parameters. Hence, two security issues can arise for these systems. The first one occurs when the values of parameters or secret keys are kept fixed and thus the adversary may stole one of encryption machine, utilize transmitted chaotic signal, and generate a copy of chaotic outputs at transmitter and receiver sides. If the values of parameters are to be changed

the second issue arises when distant authentic sides need to securely exchange the values of secret keys.

There are few partial attempts to solve the aforementioned security issues in literature. For example, the need for chaos synchronization can be ignored if digital implementations of identical chaotic maps are employed by both communication sides [46], [47]. Although it is known that a degradation in statistical properties of chaotic output due to finite precision of computing machine, the pseudo-chaos or finite precision error can be exploited to treat this degradation and greatly improve the performance of encryption technique, see [46] and reference therein. However, the requirements of varying secret keys render the key distribution problem still exists for this implementation. A solution for key sharing problem is provided in [44] where the encryption keys is generated simultaneously by two distant units via achieving the synchronization between them through a shared chaotic driving signal. However, the public driving chaotic signal in this scheme can induce security concerns. In addition, another weakness of this scheme is the assumption that both transmitter and receiver units are perfect identical.

Motivated by above discussion, the first goal of this paper is to investigate the existence of ghost attractors in a proposed nonautonomous chaotic blinking circuit with memristor. Then, the complicated dynamics of ghost attractors are exploited in a highly efficient one time pad-like encryption scheme. The suggested scheme has the advantage of being realizable on digital platform and uses pseudo-chaos time series to overcome the degradation in performance of digital chaos. This paper is organized as follows: mathematical preliminaries are introduced in Section 2. The mathematical model of proposed blinking circuit is presented in Section 3. The ghost attractors in phase space of blinking circuit are examined in Section 4. Section 5 introduces a proposed pseudo-chaos encryption algorithm. Conclusion and final discussion are presented in Section 6.

II. PRELIMINARIES

Suppose that there is $n-$dimensional blinking dynamical system with stochastic switched parameters. In particular, the parameters of the nonautonomous system are assumed to switch randomly, at identical-length time intervals, through a finite set of m values. The system can be written as

$$\dot{X}(t) = F(X(t), \varrho(t)), \quad X \in \mathbb{R}^n, \; F : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n, \\ \varrho(t) : [0, \infty) \to \{0, 1\}^m. \quad (1)$$

For each time interval $[s\tau, (s+1)\tau)$, $s = 0, 1, 2, \ldots$, the vector valued switching signal $\varrho(t)$ is randomly assigned a constant binary vector value. More specifically, the piecewise constant switching signal $\varrho(t)$ consists of $m-$components, i.e. $\varrho = (\varrho_1, \varrho_2, \ldots, \varrho_m)$, and each component can take only the value of zero or one. The particular values of its components at time interval k are denoted as $\varrho^k(t_k) = (\varrho_1^k, \varrho_2^k, \ldots, \varrho_m^k)$ where $t_k \in [k\tau, (k+1)\tau)$ and the constant τ is known as the switching time. More interestingly, the stochastic switching signal is supposed to be independent and identically distributed on the aforementioned sequences of time intervals.

Indeed, two time scales occur in blinking dynamical systems which are the time scale of the driving stochastic process and the time scale of the dynamics of the blinking system itself. For the case where the time scaling of stochastic process is considerably faster than the that of the blinking system, it has been shown that the solution of the blinking system remains close to the solution of the associated averaged system as switching time tends to zero. By the averaged system, we simply mean averaging over the random switching variables.

Definition 1: The averaged system that corresponds to blinking system (1) is defined by

$$\begin{aligned} \dot{Y}(t) &= \Psi(Y(t)) \\ &= E[F(X, \varrho)] \\ &= \sum_{\varrho \in \{0,1\}^m} P_\varrho F(X, \varrho), \end{aligned} \quad (2)$$

where the summation is taken over all possible values of ϱ and the probability P_ϱ of each value.

Moreover, the following assumptions are considered to be hold for systems (1) and (2):

- The expectation $E\,\|F(X, \varrho)\|$ has finite value $\forall\, X \in \mathbb{R}^n$,
- The function $F(X, \varrho)$ is locally Lipschitz continuous in X and continuous in ϱ. This implies that fixing any $\tilde{\varrho} \in \{0, 1\}^m$, $\exists\, L > 0$ s.t.

$$\|F(X_1, \tilde{\varrho}) - F(X_2, \tilde{\varrho})\| \leq L \|X_1 - X_2\|,$$

- For any initial state vector $X(0)$ and a particular value of ϱ, there is unique solution trajectory $X(t)$ of the system defined for $t \in [0, \infty)$.
- Similarly for the averaged system (2), the solution trajectory $Y(t)$ starting from any initial state vector $Y(0)$ is unique and defined for $t \in [0, \infty)$.

Then the following theorem can be formulated.

Theorem 2: The pair of solution trajectories of blinking system (1) and averaged system (2) which initially starting from the same initial state vectors, i.e. $X(0) = Y(0)$, satisfy

$$\|X(t) - Y(t)\| \leq \xi, \quad \xi > 0$$

on time interval $t \in [0, T)$ with probability $P_{clos} \to 1$ as switching time $\tau \to 0$.

Here $\xi > 0$ is referred to as closeness constant.

The supremum norm will be used in next section for the purpose of our analysis. It is defined for continuous function $\Omega(t)$ and matrix $\Psi = [\psi_{ij}[t]]$ as follows

$$\|\Omega\| = \sup_{t \in (0,T]} |\Omega(t)|, \quad (3)$$

$$\|\Psi\| = \sum_{i,j} \sup_{t \in (0,T]} \left|\psi_{ij}[t]\right|. \quad (4)$$

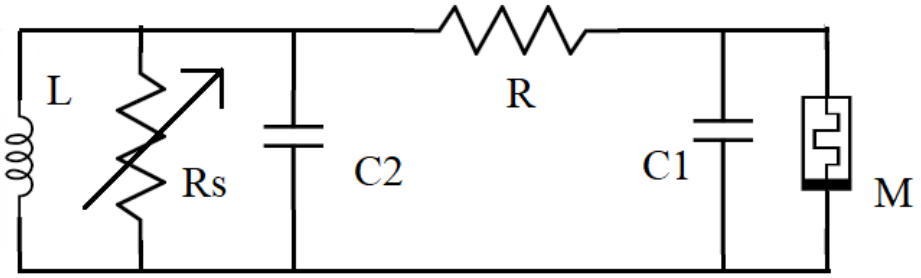


FIGURE 1. Circuit schematic of memristor-based chaotic circuit.

III. THE MATHEMATICAL MODEL

The circuit schematic of the chaotic modified Van der Pol-Duffing (MVD) memristor-based circuit is shown in Fig.1 [48]. The memristor in this circuit is of a flux controlled type where the flux-dependent rate of change of memristor's charge is described by memductance function $M(\phi)$ [18]. It is defined by

$$M(\phi) = \frac{dq(\phi)}{d\phi}, \tag{5}$$

where q and ϕ are charge and magnetic flux, respectively. A cubic nonlinearity is used for $q(\phi)$ s.t. the following relations hold

$$\begin{aligned} q(\phi) &= \alpha\phi + \beta\phi^3, \\ M(\phi) &= \alpha + 3\beta\phi^2, \\ i(t) &= (\alpha + 3\beta\phi^2)v(t), \end{aligned}$$

where $i(t)$ and $v(t)$ are the current and voltage of the memristor, respectively.

Therefore, the rate equations which describe the circuit can be derived in the following form

$$\frac{du}{dt} = \delta u + \eta v - \kappa u z^2, \tag{6}$$

$$\frac{dv}{dt} = \sigma u - v - \varepsilon w, \tag{7}$$

$$\frac{dw}{dt} = \gamma v, \tag{8}$$

$$\frac{dz}{dt} = \mu u. \tag{9}$$

A. UNIQUENESS OF THE SOLUTION TRAJECTORY AND CONTINUOUS DEPENDENCE ON INITIAL CONDITIONS

The mathematical model (6)-(9) can be expressed by

$$\frac{d\mathbf{U}}{dt} = \mathbf{G}(\mathbf{U}), \tag{10}$$

where $t \in (0, T]$, the initial state of the model is

$$\mathbf{U}(\mathbf{0}) = \mathbf{U}_0. \tag{11}$$

and the vector notations are given by

$$\mathbf{U} = \begin{bmatrix} u \\ v \\ w \\ z \end{bmatrix}, \quad \mathbf{U}_0 = \begin{bmatrix} u_0 \\ v_0 \\ w_0 \\ z_0 \end{bmatrix}, \text{ and}$$

$$\mathbf{G}(\mathbf{U}) = \begin{bmatrix} \delta u + \eta v - \kappa u z^2 \\ \sigma u - v - \varepsilon w \\ \gamma v \\ \mu u \end{bmatrix}. \tag{12}$$

Consider the region $\Phi \times J$ of phase space which contains the initial state $(\mathbf{U}_0, 0)$ and is defined as

$$\Phi = \{(x, y, z, w) : \max\{|u|, |v|, |w|, \text{ and } |z|\} \leq \Delta\},$$
$$J = (0, T]. \tag{13}$$

The initial value problem (10 – 11) is equivalent to the following system

$$\mathbf{U}(\mathbf{t}) = \mathbf{U}_0 + \int_0^t \mathbf{G}(\mathbf{U}(\varsigma))\mathbf{d}\varsigma. \tag{14}$$

Now the right hand side of (14) is referred to as $\mathbf{F}(\mathbf{U})$, hence we get

$$\mathbf{F}(\mathbf{U}_1) - \mathbf{F}(\mathbf{U}_2) = \int_0^t \mathbf{G}(\mathbf{U}_1(\varsigma)) - \mathbf{G}(\mathbf{U}_2(\varsigma))\mathbf{d}\varsigma, \tag{15}$$

and

$$|\mathbf{F}(\mathbf{U}_1) - \mathbf{F}(\mathbf{U}_2)| \leq \int_0^t \left|\mathbf{G}(\mathbf{U}_1(\varsigma)) - \mathbf{G}(\mathbf{U}_2(\varsigma))\right| \mathbf{d}\varsigma. \tag{16}$$

It can be shown that the following inequality is attained

$$\|\mathbf{F}(\mathbf{U}_1) - \mathbf{F}(\mathbf{U}_2)\| \leq T \max\{(|\delta| + |\sigma| + |\kappa|\,\Delta^2 + |\mu|), (|\eta| + |\gamma| + 1), |\varepsilon|, (2\kappa\Delta^2)\} \|\mathbf{U}_1 - \mathbf{U}_2\| \tag{17}$$

$$\leq L \|\mathbf{U}_1 - \mathbf{U}_2\|. \tag{18}$$

The mapping $\mathbf{U} = \mathbf{G}(\mathbf{U})$ is contraction map if $L < 1$ i.e.

$$T \max\{(|\delta| + |\sigma| + |\kappa|\,\Delta^2 + |\mu|), (|\eta| + |\gamma| + 1), |\varepsilon|, (2\kappa\Delta^2)\} < 1. \tag{19}$$

The sufficient condition for existence and uniqueness of system (6)-(9) solution is provided by the following theorem.

Theorem 3: The solution trajectory of system (6)-(9) that emanates from initial state $\mathbf{U}_0$ is unique for $t \in (0, T]$ if $T \max\{(|\delta| + |\sigma| + |\kappa|\Delta^2 + |\mu|), (|\eta| + |\gamma| + 1), |\varepsilon|, (2\kappa\Delta^2)\} < 1$.

Let $\mathbf{U}_{01}$ and $\mathbf{U}_{02}$ be two close sets of initial states which satisfy

$$0 < \|\mathbf{U}_{01} - \mathbf{U}_{02}\| \leq \varkappa, \quad \varkappa > 0, \tag{20}$$

thus it can be verified that

$$0 < \|\mathbf{U}_1 - \mathbf{U}_2\| \leq \frac{\varkappa}{1 - L}, \tag{21}$$

or

$$0 < \|\mathbf{U}_1 - \mathbf{U}_2\| \leq \epsilon$$

where $L < 1$ is defined above.

This indicates that the solution of system (6)-(9) exhibits continuous dependence on its initial state if $L < 1$.

B. BLINKING MEMRISTOR-BASED CIRCUIT

The following blinking memristor-based circuit is considered

$$\frac{du}{dt} = \delta(t)u + \eta v - \kappa u z^2, \tag{22}$$
$$\frac{dv}{dt} = \sigma u - v - \varepsilon w, \tag{23}$$
$$\frac{dw}{dt} = \gamma v, \tag{24}$$
$$\frac{dz}{dt} = \mu u, \tag{25}$$

where $\delta(t) = (\delta_1 - \delta_2)\varrho(t) + \delta_2 > 0$ is time varying parameter whose stochastic parameter $\varrho(t)$ takes constant value in each interval $t_k \in [k\tau, (k+1)\tau)$ in the way that

$$\varrho(t) = \begin{cases} 0, & \text{with probability } P_0 \\ 1, & \text{with probability } P_1 = 1 - P_0. \end{cases}$$

Therefore, the nonautonomous system (22-25) randomly switches between its two subordinate autonomous circuits, namely, M_1 and M_2, for each switching period τ. The first circuit has the value δ_1 for parameter δ whereas second circuit has the value δ_2 for parameter δ.

The two characteristic times in system (22-25) are slow time t and fast time $\hat{t} = \frac{t}{\tau}$. The mathematical model can be expressed in terms of fast time through setting $t = \tau\hat{t}$ which yields

$$\frac{dV}{d\hat{t}} = \tau H(u, v, w, z; \delta), \tag{26}$$

where

$$V = [u, v, w, z]^T,$$

and H is the right hand side of system (22-25). Now, the parameter τ in (26) is considered as small parameters in the model and the associated averaged system to our blinking circuit can be obtained as follows

$$\frac{du}{dt} = (P_0\delta_2 + P_1\delta_1)u + \eta v - \kappa u z^2, \tag{27}$$
$$\frac{dv}{dt} = \sigma u - v - \varepsilon w, \tag{28}$$
$$\frac{dw}{dt} = \gamma v, \tag{29}$$
$$\frac{dz}{dt} = \mu u. \tag{30}$$

Definition 4: Assuming that the composing subcircuits of blinking memristor-based circuit (22)–(25) has attractors Ξ_1 and Ξ_2. If the attractor Ξ of the averaged system (27)–(30) is different from the attractors Ξ_1 and Ξ_2, then the attractor Ξ is referred to as a ghost attractor of the blinking memristor-based circuit.

The attractor of the blinking memristor-based circuit (22)–(25) at arbitrary values of τ will be denoted as Ξ_τ and it is called the non-stationary attractor of the blinking system.

IV. GHOST ATTRACTORS IN PHASE SPACE OF BLINKING CIRCUIT

In this section, bifurcation diagrams are first evaluated for state variables in the model system (6)-(9) versus parameter δ for different set of initial states of the system. The values of other parameters in the system are set as follows: $\eta = 5$, $\kappa = 16$, $\sigma = 7.82$, $\varepsilon = 10$, $\gamma = 7.8125$ and two values of μ that are $\mu = 5, 50$. The sets of initial conditions which are used in numerical simulation are: $(u(0), v(0), w(0), z(0)) \in \{(\pm 0.01, \pm 0.01, 0.01, 0.2), (0.3, 0.3, 0.2, 0.4), (-0.05, -0.01, -0.01, 0.3)\}$.

Figure 2 shows the bifurcation diagrams obtained at the two sets of initial conditions whereas Figure 3 presents the bifurcation diagrams acquired for the remaining two sets of initial states. It is obvious that dynamics of the system undergo significant qualitative changes under the variation in δ as well as the variation starting point for solution trajectories. The coexistence of multiple attractors under different initial conditions are also observed. Indeed, the memristor-based chaotic system (6)-(9) is an important example of dynamical systems which exhibit what is known as bifurcation without parameters phenomena [49].

The value of parameters δ_1 and δ_2 are taken as 2.1 and 2.93, respectively, and $\mu \in \{5, 50\}$ then the phase portraits are obtained in three dimensional state spaces of the system (6)-(9). Figure 4 shows that the circuit model exhibit periodic dynamics for initial conditions given by $(0.01, 0.01, 0.01, 0.2)$ and $\mu = 50$. For another set of initial conditions, namely, $(0.3, 0.3, 0.2, 0.4)$ and $\mu = 5$, the output of the circuit system is periodic at $\delta_1 = 2.1$ and chaotic at $\delta_2 = 2.93$ as illustrated in Figure 5.

A. DYNAMICS OF AVERAGED SYSTEM

Now the values of probabilities P_0 and P_1 in blinking system (22)-(25) and in averaged system (27)–(30) are

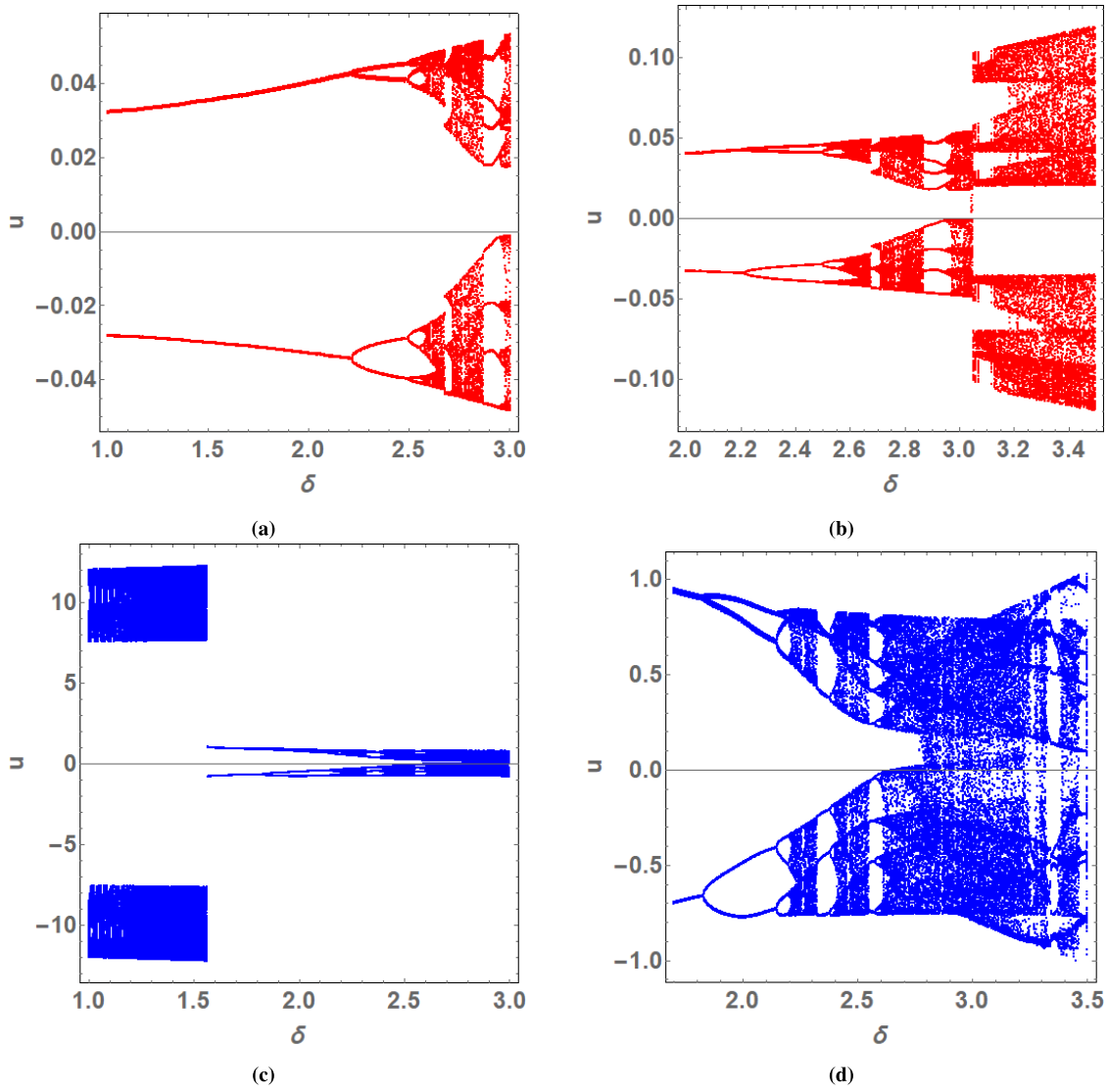


FIGURE 2. The bifurcation diagrams of (6)-(9) versus parameter δ for $\eta = 5$, $\kappa = 16$, $\sigma = 7.82$, $\varepsilon = 10$, $\gamma = 7.8125$ and (a,b) $\mu = 50$ and initial condition (0.01, 0.01, 0.01, 0.2), (c,d) $\mu = 5$ and (0.3, 0.3, 0.2, 0.4).

selected as $P_0 = 0.78$ and $P_1 = 0.22$. The phase portraits of averaged system (27)–(30) are shown in Figure 6 (a,b) for the first set of initial conditions and $\mu = 50$ whereas Figure 6 (c,d) depict the phase portraits associated with (0.3, 0.3, 0.2, 0.4) initial condition and $\mu = 5$.

B. NON-FAST SWITCHING PERIOD

In numerical simulations, fourth order Runge-Kutta method is employed to solve blinking system (22)-(25) with time step of $\Delta t = 5 \times 10^{-4}$. The values of τ considered are selected sufficiently less than those of Δt such that $\tau > 5\Delta t$. Examples of the results obtained are illustrated in Figure 7 (a,b).

C. FAST SWITCHING PERIOD

In this case, the value of τ is taken close to Δt such that the two characteristic times of the system (22)-(25). Figure 7 (c,d) show example of phase portraits acquired at fast switching rate.

D. PROXIMITY OF GHOST AND NON-STATIONARY ATTRACTORS

The Kryloff–Bogoliouboff theorem [50] indicates the occurence of certain invariant measure for deterministic dynamical systems. On other side, the steady solution of the Kolmogorov–Chapman equation represents the invariant probability measure of dynamical systems with random processes [51]. There are some primary tools which can be utilized to study the existence of these invariant measures such as Gibbs and SBR measures [52]–[54]. The discrete approximation of the invariant measures has been provided in several works, see for example [55]–[57] and references there in.

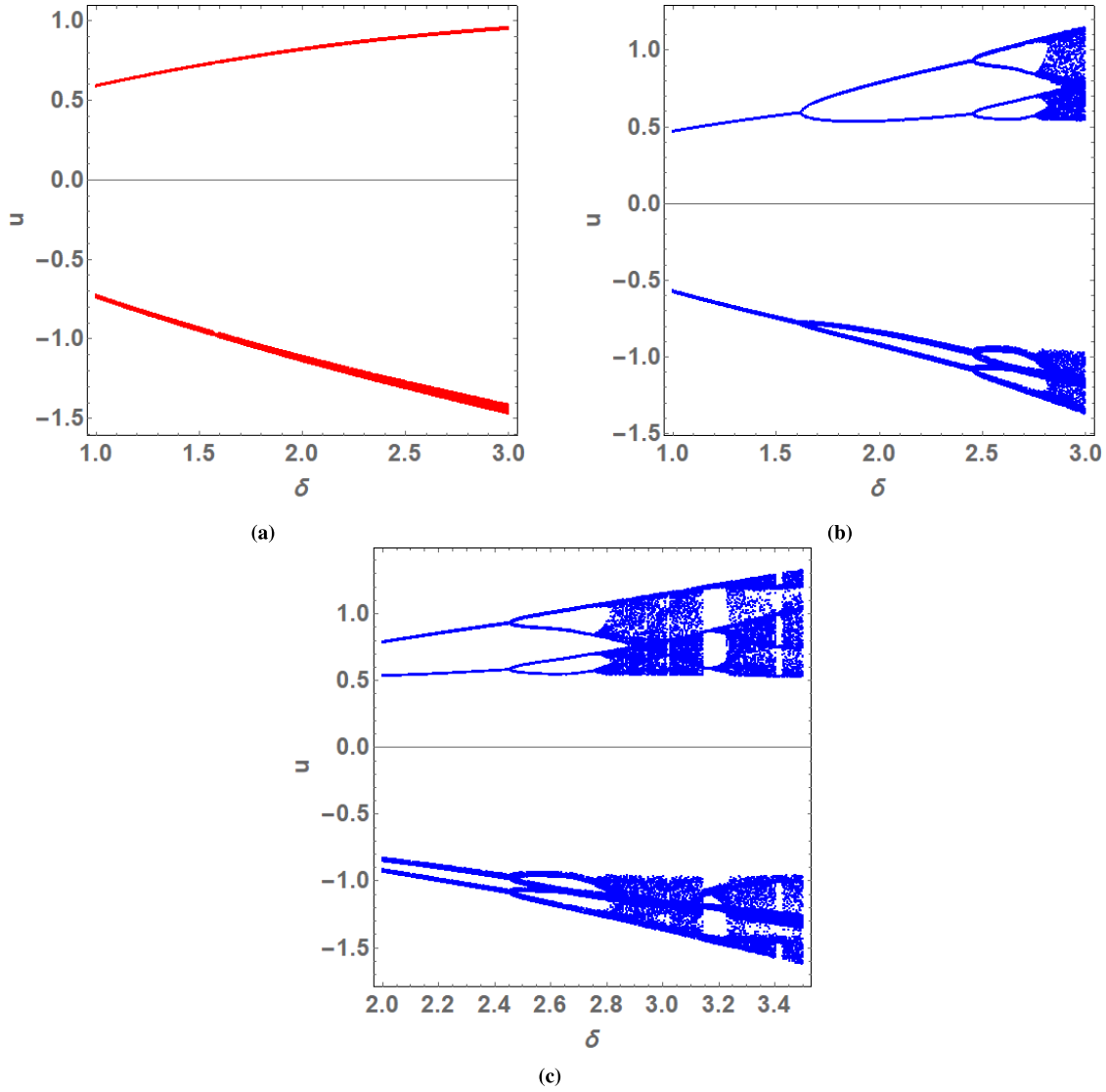


FIGURE 3. The bifurcation diagrams of (6)-(9) versus parameter δ for $\eta = 5$, $\kappa = 16$, $\sigma = 7.82$, $\varepsilon = 10$, $\gamma = 7.8125$ and (a) $\mu = 5$ and initial condition $(-0.05, -0.01, -0.01, 0.3)$, (b,c) $\mu = 5$ and $(-0.01, -0.01, 0.01, 0.2)$.

In this work, we assume that there exist invariant probability measures concentrated on ghost and non-stationary attractors of the blinking memristor-based circuit and denote them as $\pi_1(\Xi)$ and $\pi_2(\Xi_\tau)$, respectively. Numerical investigation of the Euclidean distance between these measures are carried out as it is described below.

Define Θ as the absorbing region in phase space of the model which contains both Ξ and Ξ_τ attractors. It can be described as

$$\Theta : \{\theta_{i,1} < \theta_i < \theta_{i,2}\}, \quad \theta_i \in \{u, v, w, z\},$$

where $\theta_{i,1}$ and $\theta_{i,2}$ are left and right boundaries, respectively, of domain Θ. Subsequently, the four coordinates axes of Θ is divided into N_i, $i = 1, 2, 3, 4$, equal subintervals, for u, v, w and z, in the way that the whole domain Θ is divided into $\hat{N} = \prod_{j=1}^{4} N_i$ small contiguous boxes. In order to construct the intended approximation of the invariant measures, the value of τ is fixed and the starting point of solution trajectory is randomly assigned to one of the $\hat{N}$ boxes. The simulation is executed for sufficiently long time where the initial transient points of the trajectory are ignored. Thus, the solution trajectory along Ξ_τ contains $\hat{M}$ phase points after neglecting transient solution. The number of hits that were made to the border of a certain box j is then computed and will be referred to as b_τ^j. The distribution $\hat{\pi}_2(\Xi_\tau)$ of these values along the boxes is considered the discrete approximation of $\pi_2(\Xi_\tau)$ and it is given by

$$\hat{\pi}_2(\Xi_\tau) = \{\frac{b_\tau^j}{\hat{M}}\}, \quad j = 1, 2, \ldots, \hat{N}.$$

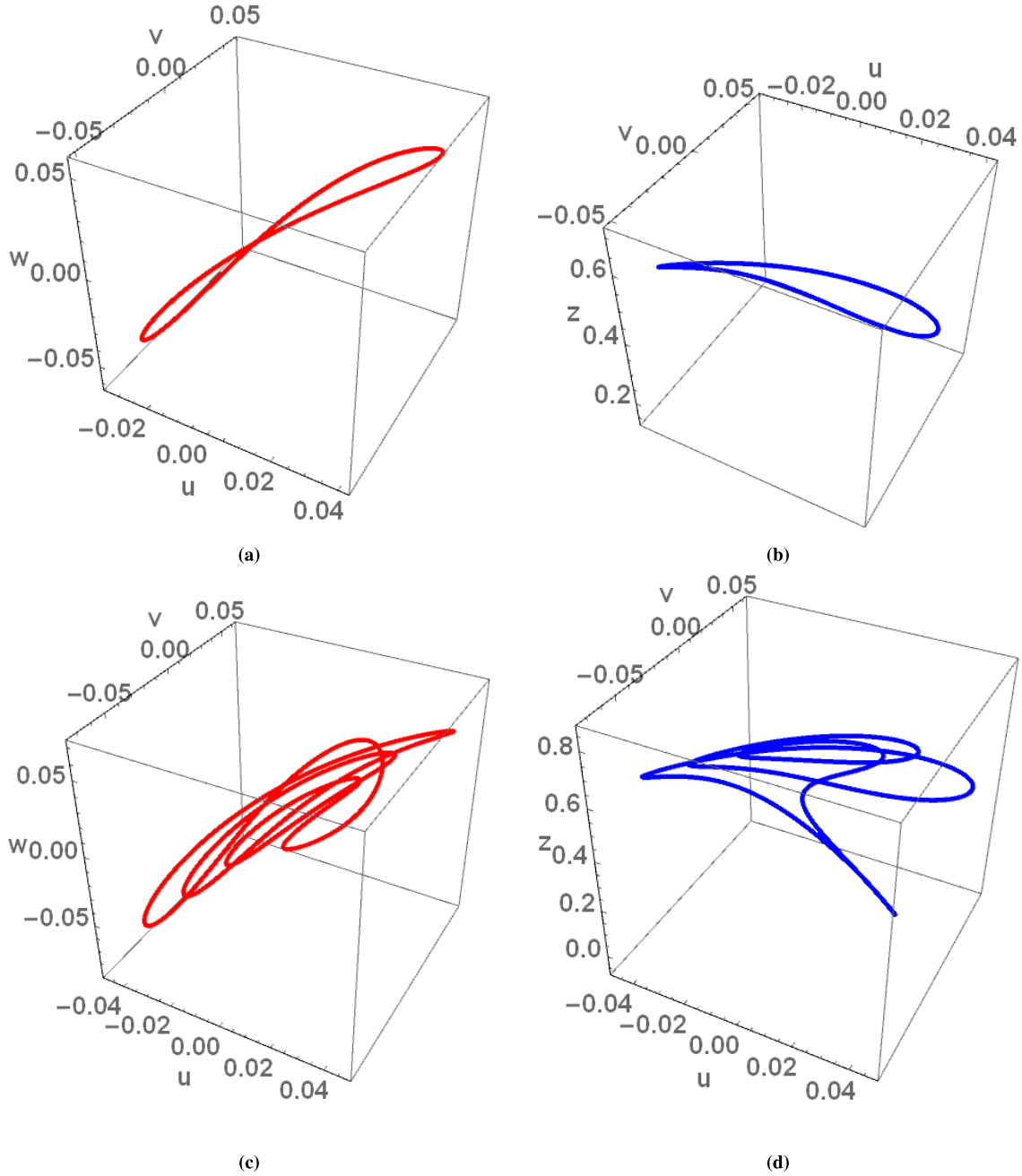


FIGURE 4. The three dimensional phase portraits of system (6)-(9) obtained at (0.01, 0.01, 0.01, 0.2) and (a) $\delta_1 = 2.1$, (c,d) $\delta_2 = 2.93$.

By the same way, the discrete approximation of $\pi_1(\Xi)$ along the solution trajectory of averaged system can be determined as

$$\hat{\pi}_1(\Xi) = \{\frac{b^j}{\hat{M}}\}, \quad j = 1, 2, \ldots, \hat{N},$$

where b^j refers to the number of hits to the border of box j in phase space domain of the averaged system and $\hat{M}$ is the number of points on the trajectory.

The distance between the two invariant measures $\pi_1(\Xi)$ and $\pi_2(\Xi_\tau)$ can be approximated via computing the following Euclidean distance

$$\Delta = \frac{1}{\hat{N}} \sqrt{\sum_{j=1}^{\hat{N}} (b^j - b_\tau^j)^2}.$$

Indeed, this distance is an appropriate measure for similarity of the attractors Ξ and Ξ_τ when the value of τ is varied.

In numerical simulations, the values of N_i are taken as $N_1 = N_2 = N_3 = N_4 = 50$ and the number of points is selected as $\hat{M} = 5 \times 10^7$ after ignoring the initial 10^6 points

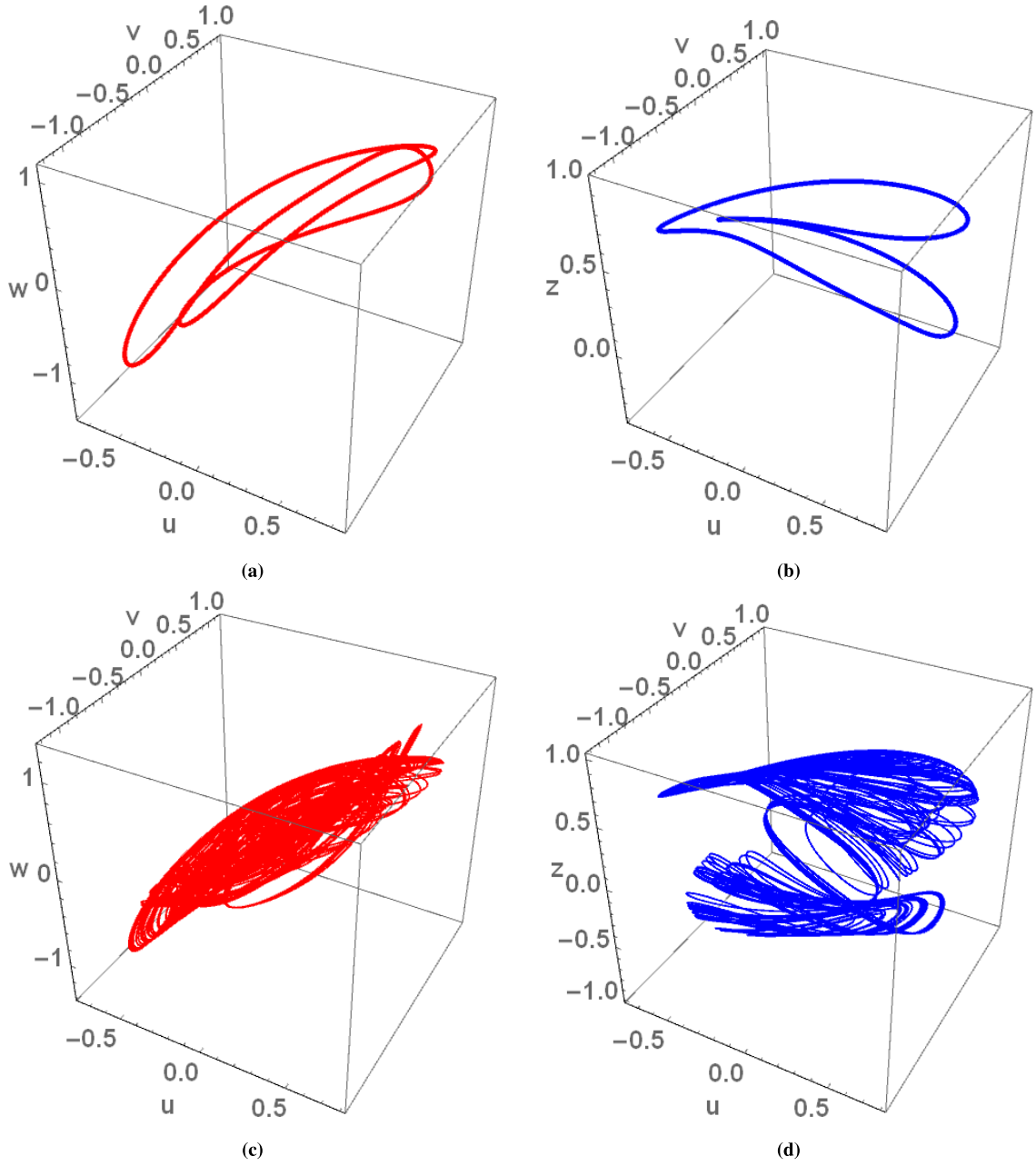


FIGURE 5. The three dimensional phase portraits of system (6)-(9) obtained at (0.3, 0.3, 0.2, 0.4) and (a) $\delta_1 = 2.1$, (c,d) $\delta_2 = 2.93$.

of the trajectories. From Figure 7(e), it is shown that this distance is a monotonically increasing function with the value of switching time τ and hence can be used as suitable measure for the similarity of dynamical behaviors of the averaged system and the blinking system.

V. A PROPOSED PSEUDO-CHAOS ENCRYPTION ALGORITHM

In this section, the guidelines for a proposed encryption algorithm which utilizes pseudo-chaos of ghost attractors are introduced for the first time, to the best of author's knowledge. In particular, both the sender and transmitter sides have two blinking systems which are mathematically equivalent but computationally inequivalent, due to finite precision of computing machines. For example, if the present memristor-base blinking system is employed, we have

$$\begin{aligned}
\frac{du_1}{dt} &= \delta(t)u_1 + \eta v_1 - \kappa u_1 z_1^2, \\
\frac{dv_1}{dt} &= \sigma u_1 - v_1 - \varepsilon w_1, \\
\frac{dw_1}{dt} &= \gamma v_1, \\
\frac{dz_1}{dt} &= \mu u_1,
\end{aligned}$$

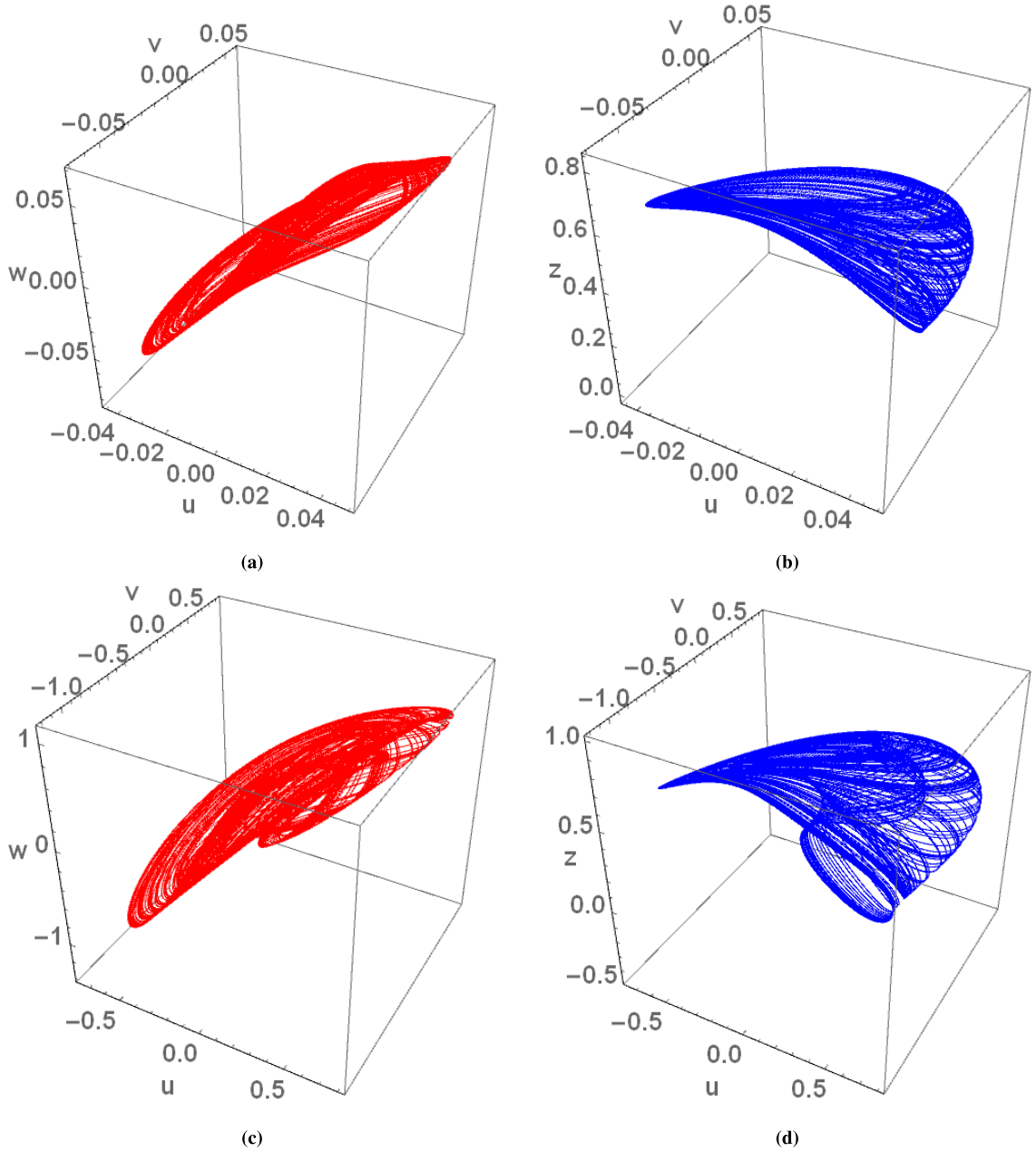


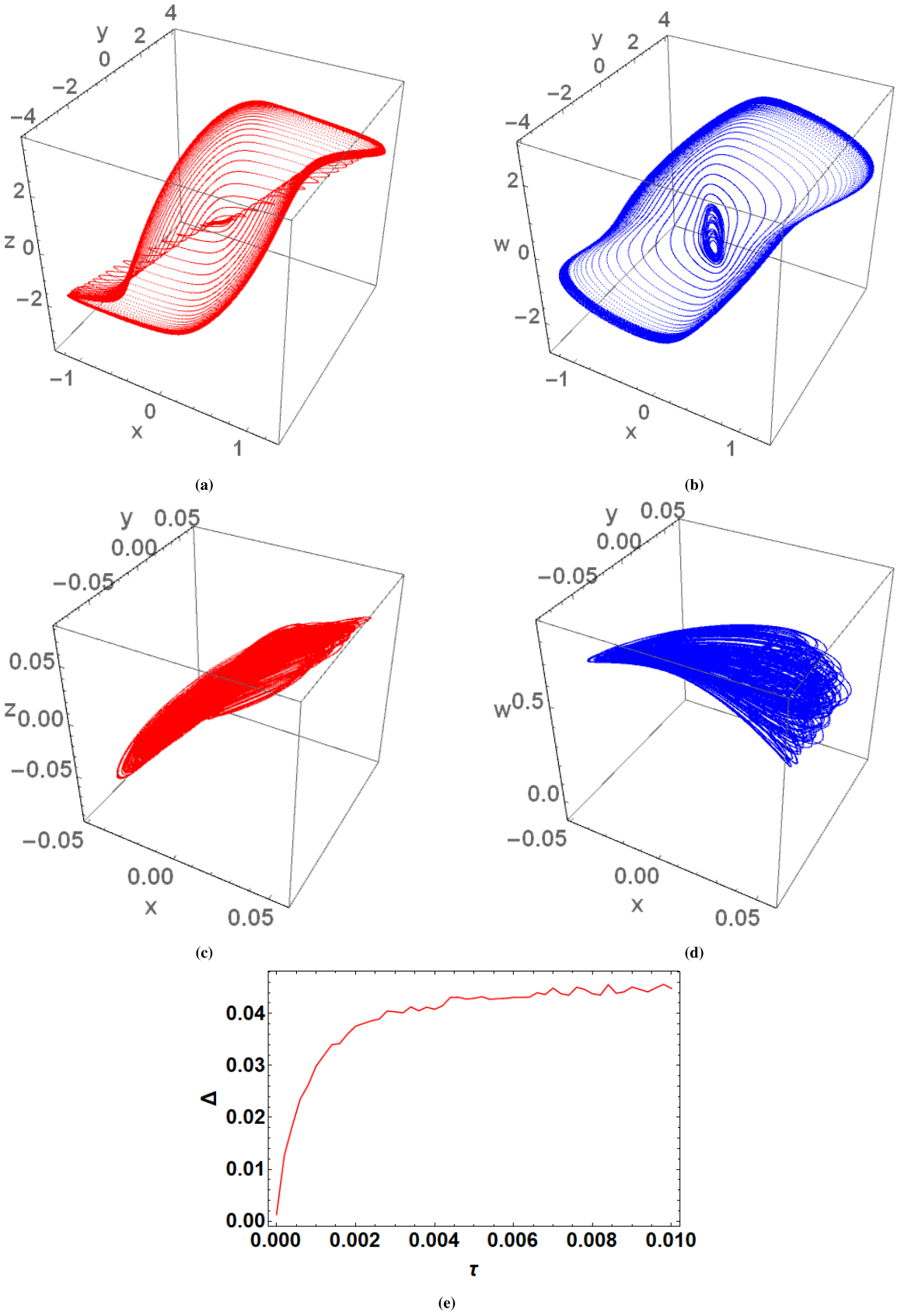
FIGURE 6. The phase portraits of averaged system (27)–(30) are shown in (a,b) for the initial condition (0.01, 0.01, 0.01, 0.2) and $\mu = 50$ whereas (c,d) depict the phase portraits associated with (0.3, 0.3, 0.2, 0.4) initial condition and $\mu = 5$. The values of probabilities P_0 and P_1 are selected as $P_0 = 0.78$ and $P_1 = 0.22$.

as a first system and

$$\begin{aligned}
\frac{du_2}{dt} &= \frac{u_1}{z_2}(\delta(t)z_2 - \kappa z_2^3) + \eta v_2,\\
\frac{dv_2}{dt} &= \sigma u_2 - v_2 - \varepsilon w_2,\\
\frac{dw_2}{dt} &= \gamma v_2,\\
\frac{dz_2}{dt} &= \mu u_2,
\end{aligned}$$

as the second system. The two systems can be digitally represented using DSPs, FPGAs, or microcontrollers at each side of the communication link. The specific values of parameters in the two systems are shared between transmitter and receiver just before encryption session starts using one of the elliptic curves-based key agreement protocols. Examples of reliable and efficient elliptic curves which can be employed are P-256 or Curve25519.

Now, select one of the highly efficient physical random number generators, such as the one introduced in [58]. The generated random bits are shared between the two



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

FIGURE 7. The phase portraits of blinking system (22)-(25) are shown in (a,b) for $\tau = 12\Delta t$. and (c,d) depict the phase portraits associated $\tau = 2\Delta t$. The probabilities P_0 and P_1 are selected as $P_0 = 0.78$ and $P_1 = 0.22$. The distance Δ as a function of τ is illustrated in (e).

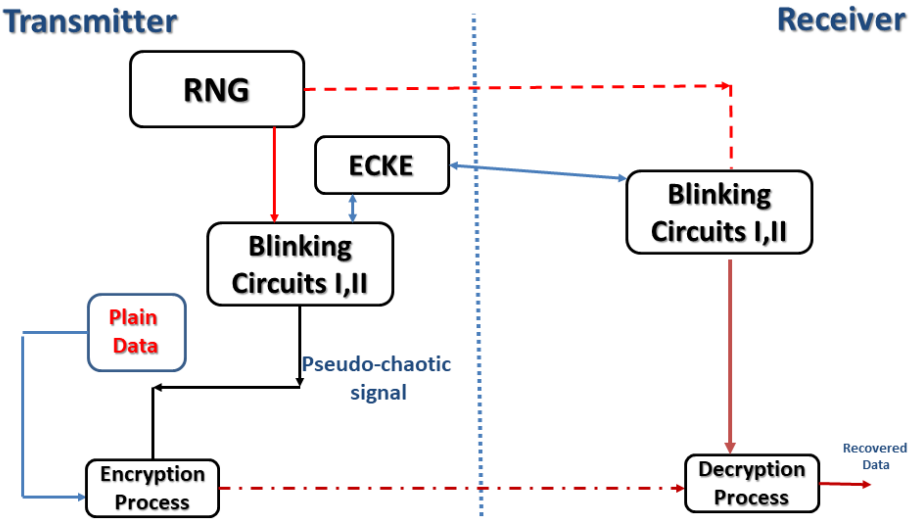


FIGURE 8. Structure of the proposed encryption algorithm.

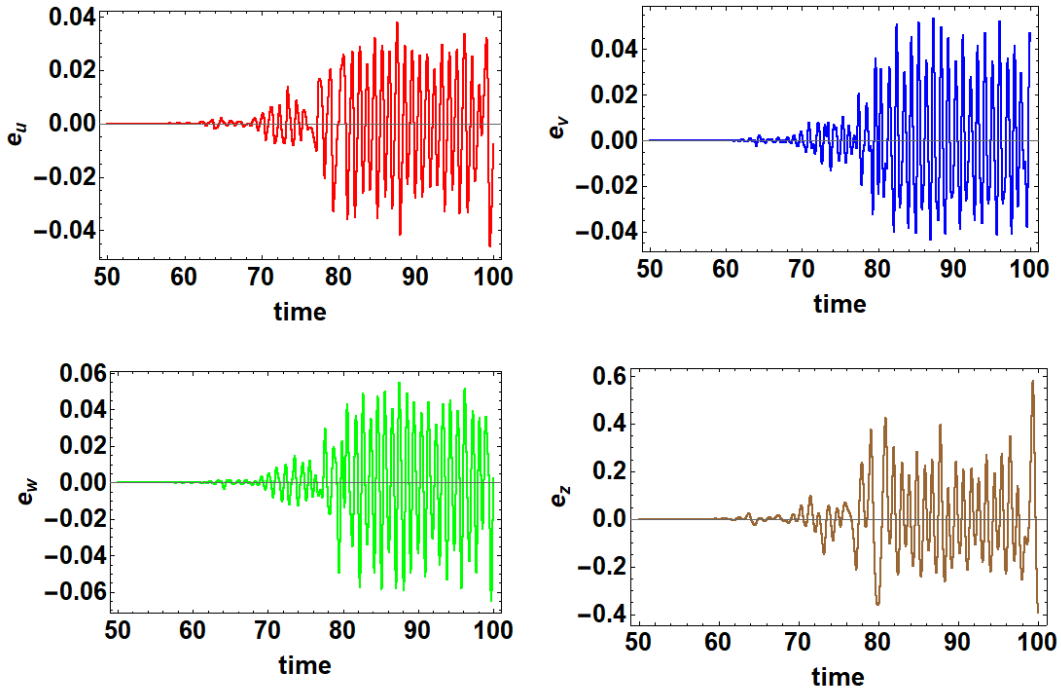


FIGURE 9. The time series plots of the four pseudo-chaotic signals.

communicating sides. The sequence of random bits are grouped into 7 bits-length sets which are supposed to be uniformly distributed. The decimal value representation of a set at time t determines the instant value of $\varrho(t)$ at this time through the following rule

$$\varrho(t) = \begin{cases} 0, & \text{if the decimal value } \leq 99 \\ 1, & \text{otherwise} \end{cases}$$

Clearly, transmission delay of the signal should first be firstly compensated at both sides of transmitter and receiver.

The pseudo-chaotic time series of the outputs of blinking system I and blinking system II are then obtained by

$$e_u = u_1 - u_2, \quad e_v = v_1 - v_2,$$
$$e_w = w_1 - w_2, \quad e_z = z_1 - z_2.$$

The one-time pad is an encryption technique which has been described and studied in the works of F. Miller, G. Vernam and J. Mauborgne. It relies on pre-shared key between legitimate transmitter and receiver sides and, interestingly, it is impossible to be broken by attackers provided that three conditions are satisfied: the first is that the key is at least as long as the plaintext, the second condition is that it is used only for one time, and finally, the key should be completely random [22]. The one-time pad encryption is used essentially for crucial military and diplomatic communications. The key problem which associates with this type of encryption is how to effectively achieve secure key distribution.

(a)

```
▯ ▯  NYsm ▯SN6 ]lJ?<>s=▯knb4 ▯ ,bp`)JF?j_<▯W ▯Q ▯N`  =)WQP;2▯ \\n;]▯Xe =▯
6u8d64  ▯ %VMk  \"   v ▯ ,▯ <▯ ▯ −3MQdX▯ nTfQQwTo  k  #▯D )▯ ;J%(IL  <  _,
pRNJ1▯A  ^/+j▯J  ;Z)e?\\t▯   ▯jJM  '▯ ▯ ▯ +▯$ ▯Br  ?e$  \\Ue▯ ▯f  ]Fo=P>o  /V+_D;  ▯L
▯ ▯f  ▯ ▯k  \\nd  GjY  @9▯ ▯ = 4jOd  kWp ▯ ▯P  ?E'0vs  ?=  ▯L5a ▯Q  /Z▯H  ]aS6  &O▯
4m  ▯ ▯  s  ▯ =−!\\n  j ▯ :<(?&+W6▯vp ▯ ▯I8  \\>Q,+▯ )#kJ    \\▯A  >Mj∗A▯T ▯ +W,m
▯   ?@DV\\n^v▯ @C(dYKR<\\n:▯bf1 ▯ @5▯gU ▯ ] ▯ &  =1▯AI ▯e ▯M  5_  6▯03  =D#F
#MRc^VOcSE?▯IuQ ▯ .dk▯a3  ).JB▯XGg  ^1D▯ ▯ −Lc▯ ▯O ▯ ∗▯Ru ▯ \\n/▯9  )\\DVeaRZ
▯t`s  ]▯F  ▯Gu  /▯ \"  ▯3  \\nc(I:\\iU▯c69p  !▯J  &G  ∗;▯O  =▯  /X▯  \\t\\nQiCpB▯  ,..▯  3a  .:▯
HpY▯  +qIa▯ ▯  ETM−pB+ ▯   +,wtv▯G \\▯SUJ  wb  &=@▯  TD  /2lW▯  \\n▯  +A  5be ▯a
∗  ▯a  'K  \"▯  ▯R ▯ ▯ ▯S  &  <i3_\\t▯p    m  \\no]−0]▯  b  :▯Q  (k  ▯ ▯ ▯VZ  ]▯  ?#]JB
X▯Z6Fvg ▯W  1gM  (XhasM▯  (▯Y2 ▯ ▯kn  ^0uo  e0G \\n▯B  (7Y4▯uFAVKf  \\F(−0
gZ47GEX▯I  ▯D  ,\\n▯  <Q7&b>q ∗▯  #\\t?I▯C  \\n\\n▯  −Y▯  ^c∗u2▯  .+`▯  ▯N  −(▯d  −▯
```

(b)

FIGURE 10. (a)Plain text supplied to encryption algorithm and (b) the resulting cipher text.

The two system are set to the same initial condition, Nevertheless, when the values of secret keys are chosen appropriately, the finite precision of real numbers representation in computing devices renders the orbits of the two blinking systems diverge from each other after sufficient period of time. So, the first N elements are discarded from each series $\{e_s\}$, $s = u, v, w, z$ where N is large enough to eliminate the unfavorable transient values. The four generated pseudo-chaotic signals are to be employed in encryption process. More specifically, the four signals are firstly amplified by a factor 10^q where q is an integer number greater than 12. Then the mod function is applied to integer parts of the resulting signals as follows

$$p_s = Mod\{IntegerPart\ [e_s \times 10^q],\ M_s\}, \quad s = u, v, w, z,$$

where the value of M is appropriately chosen according to the characteristics of plain text.

The structure of the proposed encryption algorithm is illustrated in Figure 8. In this figure, RNG refers to random number generator and ECKE denotes elliptic curve key exchange step which confirms the agreement on identical values of constant parameters for legal communicating sides. The encrypting step is undertaken by sequentially bit-xoring the plain data with the four streams of perturbing values p_s. The decryption process can be conducted by reversing the order of bit-xoring steps in encryption process. Therefore, the cipher data is obtained as

$$D^{cipher} = p_z \oplus \{p_w \oplus [p_v \oplus (p_u \oplus D^{plain})]\},$$

while the decrypted data is recovered by

$$D^{decrypt} = p_u \oplus \{p_v \oplus [p_w \oplus (p_z \oplus D^{cipher})]\}.$$

Figure 9 depicts the time series plots of the four pseudo-chaotic signals. It is obvious that after the transient time is discarded, these signals span a range of values, in phase

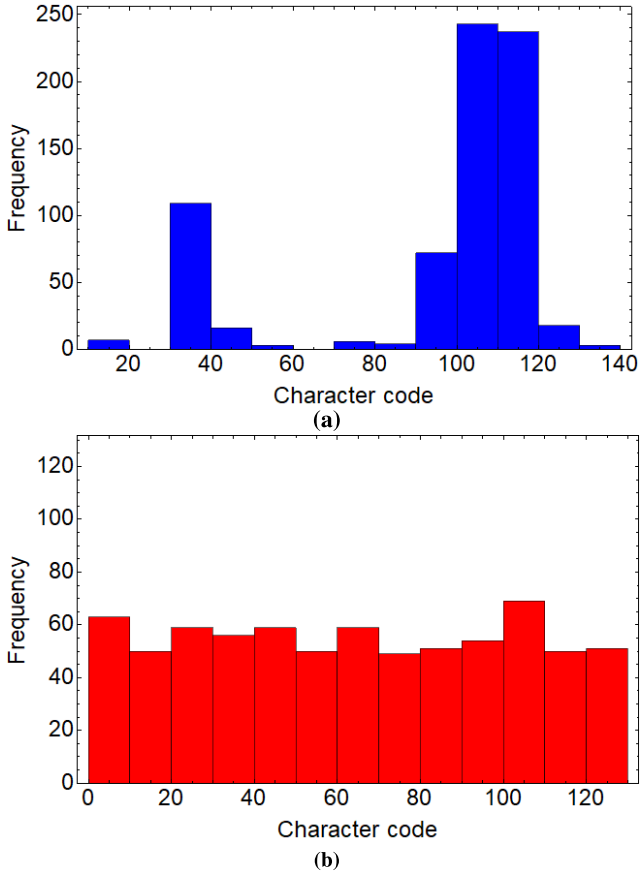


FIGURE 11. Frequency distribution of character codes in plain text and cipher text are given in (a) and (b), respectively.

space, with a size close to that of the region occupied by original chaotic ghost attractor. A plain text example is presented in Figure 10 along with the corresponding cipher text. The frequency distributions of character codes in plain text and cipher text are attained and shown in Figure 11. In numerical simulations, the values of M_s are taken as $M_u = M_v = 145$ and $M_w = M_z = 120$. It is demonstrated that the proposed algorithm randomizes the patterns of frequency distributions of character codes in plain text to be almost flat. This indicates that the encryption system can defeat the usual statistical attacks. In addition, the values of secret keys of the system are perturbed and reshared for each encryption session. Also, the streams of physical random bits utilized in blinking models are independent and are not repeated for sequential plain texts supplied to the encryption algorithm. Hence, the differential, chosen-ciphertext, and chosen-plaintext attacks can be dealt with. The uniformity of encrypted character codes distribution is evaluated by variance of histogram measure, known as ς. Let υ_i denote the number of characters having character code i, then ς can be calculated by

$$\varsigma = \frac{1}{2 \times 128^2} \sum_{i=0}^{127} \sum_{j=0}^{127} (\upsilon_i - \upsilon_j)^2. \tag{31}$$

For the present numerical example, it is found that the value of ς for plain text is given as 74.6493. On the other side, the value of histogram variance ς for generated encrypted text is found to be 0.3738 which indicates that the variance of histogram is considerably reduced by 0.99499% and shows the efficiency of the proposed scheme.

VI. CONCLUSION

The ghost attractors in a proposed blinking chaotic circuit with memristor are investigated for the first time. It is found that the occurrence of these attractors depends on the rate of random switching in blinking circuit. More specifically, the non-stationary ghost attractors of blinking circuit converges to the ghost attractors at sufficiently fast switching rate. The induced dynamics can be different from composing subsystems of blinking memristor circuit. The realization of the proposed blinking system on digital appliances can be undertaken using Digital Signal Processors, such as TMS320C6452 or ADSP-2136x, Arduino boards, such as ARDUINO NANO 33 BLE or ARDUINO MEGA 2560 REV3, or field-programmable gate arrays.

A suggested pseudo-chaos encryption algorithm which utilizes the complicated dynamics of ghost attractors is presented for first time, to the best of authors' knowledge. Future work may include extending this work to investigate the possible existence of ghost attractors in coupled networks of blinking circuits and their applications. Also, the occurrence of non-stationary ghost attractors in discrete systems is unexplored point and can be examined in future work.

REFERENCES

[1] P. N. V. Tu, *Dynamical Systems—An Introduction with Applications in Economics and Biology*. Berlin, Germany: Springer-Verlag, 1994.
[2] S. H. Strogatz, *Nonlinear Dynamics and Chaos With Applications to Physics, Biology, Chemistry, and Engineering*. Boulder, CO, USA: Westview Press, 2001.
[3] Y. A. Kuznetsov, *Elements of Applied Bifurcation Theory*. New York, NY, USA: Springer-Verlag, 2004.
[4] L. Kocarev and S. Lian, *Chaos-Based Cryptography*. Berlin, Germany: Springer, 2011.
[5] E. M. Izhikevich, *Dynamical Systems in Neuroscience: The Geometry of Excitability and Bursting*. Cambridge, MA, USA: MIT Press, 2007.
[6] P. Stavroulakis, *Chaos Applications in Telecommunications*. Boca Raton, FL, USA: CRC Press, 2006.
[7] G. Chen and X. Yu, *Chaos Control-Theory and Applications*. Berlin, Germany: Springer-Verlag, 2003.
[8] J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems, and Bifurcations of Vector Fields*. New York, NY, USA: Springer, 2013.
[9] T. Matsumoto, "A chaotic attractor from Chua's circuit," *IEEE Trans. Circuits Syst.*, vol. CS-31, no. 12, pp. 1055–1058, Dec. 1984.
[10] M. Shinriki, M. Yamamoto, and S. Mori, "Multimode oscillations in a modified van der pol oscillator containing a positive nonlinear conductance," *Proc. IEEE*, vol. 69, no. 3, pp. 394–395, Mar. 1981.
[11] G. P. King and S. T. Gaito, "Bistable chaos. I. Unfolding the cusp," *Phys. Rev. A, Gen. Phys.*, vol. 46, pp. 3092–3099, Apr. 1992.
[12] A. E. Matouk and H. N. Agiza, "Bifurcations, chaos and synchronization in ADVP circuit with parallel resistor," *J. Math. Anal. Appl.*, vol. 341, no. 1, pp. 259–269, May 2008.
[13] L. Chua, "Memristor—The missing circuit element," *IEEE Trans. Circuit Theory*, vol. CT-18, no. 5, pp. 507–519, Sep. 1971.
[14] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, pp. 80–83, May 2008.

[15] I. A. Korneev, V. V. Semenov, and T. E. Vadivasova, "Synchronization of periodic self-oscillators interacting via memristor-based coupling," *Int. J. Bifurcation Chaos*, vol. 30, no. 7, Jun. 2020, Art. no. 2050096.
[16] N. S. Soliman, M. E. Fouda, and A. G. Radwan, "Memristor-CNTFET based ternary logic gates," *Microelectron. J.*, vol. 72, pp. 74–85, Feb. 2018.
[17] A. G. Radwan and M. E. Fouda, *On the Mathematical Modeling of Memristor, Memcapacitor, and Meminductor*, vol. 26. Berlin, Germany: Springer, 2015.
[18] B. Muthuswamy and P. Kokate, "Memristor-based chaotic circuits," *IETE Tech. Rev.*, vol. 26, no. 6, pp. 1–16, 2009.
[19] K. S. Sudheer and M. Sabir, "Adaptive function projective synchronization of two-cell quantum-CNN chaotic oscillators with uncertain parameters," *Phys. Lett. A*, vol. 373, no. 21, pp. 1847–1851, May 2009.
[20] P. K. Roy and A. Basuray, "A high frequency chaotic signal generator: A demonstration experiment," *Amer. J. Phys.*, vol. 71, no. 1, pp. 34–37, Jan. 2003.
[21] F. Parastesh, H. Azarnoush, S. Jafari, B. Hatef, M. Perc, and R. Repnik, "Synchronizability of two neurons with switching in the coupling," *Appl. Math. Comput.*, vol. 350, pp. 217–223, Jun. 2019.
[22] R. Jeter and I. Belykh, "Synchronization in on-off stochastic networks: Windows of opportunity," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 5, pp. 1260–1269, May 2015.
[23] C. K. Tse and M. Di Bernardo, "Complex behavior in switching power converters," *Proc. of IEEE*, vol. 90, no. 5, pp. 768–781, May 2002.
[24] M. Hasler, V. Belykh, and I. Belykh, "Dynamics of stochastically blinking systems. Part I: Finite time properties," *SIAM J. Appl. Dyn. Syst.*, vol. 12, no. 2, pp. 1007–1030, Jan. 2013.
[25] M. Hasler, V. Belykh, and I. Belykh, "Dynamics of stochastically blinking systems. Part II: Asymptotic properties," *SIAM J. Appl. Dyn. Syst.*, vol. 12, no. 2, pp. 1031–1084, Jan. 2013.
[26] N. V. Barabash and V. N. Belykh, "Non-stationary attractors in the blinking systems: Ghost attractor of Lorenz type," *Cybern. Phys.*, no. 8, no. 4, pp. 209–214, Dec. 2019.
[27] D. Kahn, *The Codebreakers: The Story of Secret Writing*. New York, NY, USA: Scribner, 1996.
[28] F. B. Wrixon, *Codes, Ciphers, and Secret Languages*. New York, NY, USA: Bonanza Books, 1989.
[29] J. Laffin, *Codes and Ciphers: Secret Writing Through the Ages*. London, U.K.: Abelard-Schuman, 1964.
[30] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. Boca Raton, FL, USA: CRC Press, 2014.
[31] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 2018.
[32] N. P. Smart, *Cryptography Made Simple*. Cham, Switzerland: Springer, 2016.
[33] F. Böhm, S. Sahakian, A. Dooms, G. Verschaffelt, and G. Van der Sande, "Stable high-speed encryption key distribution via synchronization of chaotic optoelectronic oscillators," *Phys. Rev. A, Gen. Phys.*, vol. 13, no. 6, Jun. 2020, Art. no. 064014.
[34] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "Simultaneous suppression of time-delay signature in intensity and phase of dual-channel chaos communication," *IEEE J. Quantum Electron.*, vol. 51, no. 9, pp. 1–9, Sep. 2015.
[35] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.
[36] A. A. Elsadany, A. M. Yousef, and A. Elsonbaty, "Further analytical bifurcation analysis and applications of coupled logistic maps," *Appl. Math. Comput.*, vol. 338, pp. 314–336, Dec. 2018.
[37] Z. Liu and T. Xia, "Novel two dimensional fractional-order discrete chaotic map and its application to image encryption," *Appl. Comput. Informat.*, vol. 14, no. 2, pp. 177–185, Jul. 2018.
[38] W. Zhang, C. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524–1530, May 1, 2017.
[39] T. Wu, C. Zhang, H. Wei, and K. Qiu, "PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," *Opt. Exp.*, vol. 27, no. 20, p. 27946, Sep. 2019.
[40] T. Wu, C. Zhang, C. Chen, H. Hou, H. Wei, S. Hu, and K. Qiu, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," *Opt. Exp.*, vol. 26, no. 18, pp. 22857–22865, Sep. 2018.
[41] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 1, 2018.
[42] Z. Lin, G. Wang, X. Wang, S. Yu, and J. Lü, "Security performance analysis of a chaotic stream cipher," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1003–1017, Oct. 2018.
[43] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "Simultaneous concealment of time delay signature in chaotic nanolaser with hybrid feedback," *Opt. Lasers Eng.*, vol. 107, pp. 342–351, Aug. 2018.
[44] L. Keuninckx, M. C. Soriano, I. Fischer, C. R. Mirasso, R. M. Nguimdo, and G. Van der Sande, "Encryption key distribution via chaos synchronization," *Sci. Rep.*, vol. 7, no. 1, Apr. 2017, Art. no. 43428.
[45] K. Yoshimura, J. Muramatsu, P. Davis, T. Harayama, H. Okumura, S. Morikatsu, H. Aida, and A. Uchida, "Secure key distribution using correlated randomness in lasers driven by common random light," *Phys. Rev. Lett.*, vol. 108, no. 7, Feb. 2012, Art. no. 070602.
[46] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany, and E. A. A. Hagras, "Hybrid cryptosystem based on pseudo chaos of novel fractional order map and elliptic curves," *IEEE Access*, vol. 8, pp. 57733–57748, 2020.
[47] A. E. Elfiqi, H. S. Khallaf, S. F. Hegazy, A. Elsonbaty, H. M. Shalaby, and S. S. Obayya, "Chaotic polarization-assisted *L* DPSK-MPPM modulation for free-space optical communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 9, pp. 4225–4237, Sep. 2019.
[48] A. M. A. El-Sayed, A. Elsaid, H. M. Nour, and A. Elsonbaty, "Dynamical behavior, chaos control and synchronization of a memristor-based ADVP circuit," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 1, pp. 148–170, Jan. 2013.
[49] S. Liebscher, *Bifurcation Without Parameters*. Berlin, Germany: Springer, 2015.
[50] N. Kryloff and N. Bogoliouboff, "La théorie générale de la mesure dans son application à l'étude des systèmes dynamiques de la mécanique non linéaire," *Ann. Math.*, vol. 38, pp. 65–113, Dec. 1937.
[51] N. V. Barabash, T. A. Levanova, and V. N. Belykh, "Ghost attractors in blinking Lorenz and Hindmarsh–Rose systems," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 30, no. 8, Aug. 2020, Art. no. 081105.
[52] J. P. Eckmann and D. Ruelle, *The Theory of Chaotic Attractors*. New York, NY, USA: Springer, 1985, pp. 273–312.
[53] E. A. Sataev, "Invariant measures for hyperbolic maps with singularities," *Russian Math. Surv.*, vol. 47, no. 1, pp. 191–251, Feb. 1992.
[54] V. S. Afraimovich, N. I. Chernov, and E. A. Sataev, "Statistical properties of 2-D generalized hyperbolic attractors," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 5, no. 1, pp. 238–252, Mar. 1995.
[55] V. S. Anishchenko, A. S. Kopeikin, T. E. Vadivasova, G. I. Strelkova, and J. Kurths, "Influence of noise on statistical properties of nonhyperbolic attractors," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 62, no. 6, pp. 7886–7893, Dec. 2000.
[56] M. Muskulus and S. Verduyn-Lunel, "Wasserstein distances in the analysis of time series and dynamical systems," *Phys. D, Nonlinear Phenomena*, vol. 240, no. 1, pp. 45–58, Jan. 2011.
[57] V. Chigarev, A. Kazakov, and A. Pikovsky, "Kantorovich–Rubinstein–Wasserstein distance between overlapping attractor and repeller," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 30, no. 7, Jul. 2020, Art. no. 073114.
[58] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "Numerical analysis of ultrafast physical random number generator using dual-channel optical chaos," *Opt. Eng.*, vol. 55, no. 9, Sep. 2016, Art. no. 094105.

RAJAGOPALAN RAMASWAMY received the Bachelor of Science degree in mathematics, in 1991, the Master of Computer Applications and Master of Science degrees in mathematics from Madurai Kamraj University, Madurai, and the Ph.D. degree from Singhania University, Rajasthan, India. He is currently an Assistant Professor of mathematics at PSAU, Al-Kharj. His research interests include fixed point theory and applications, game theory, and non linear analysis.

A. M. A. EL-SAYED works as a Professor of mathematics with the Mathematics and Computer Science Department, Faculty of Science, Alexandria University. He has more than 250 publications in the areas of fractional calculus, applied functional analysis, functional differential and functional integral equations, and dynamical systems.

A. A. ELSADANY received the B.Sc. degree in mathematics and the M.Sc. and Ph.D. degrees in applied mathematics from Mansoura University, Egypt, in 1996, 2002, and 2007, respectively. He was an Assistant Professor of applied mathematics with the Faculty of Computers and Informatics, Suez Canal University, Egypt, from 2011 to 2016, where he has been an Associate Professor, since October 2016. He is currently an Associate Professor with the Mathematics Department, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia. His current research interests include applied mathematics, economic dynamics, mathematical biology, chaos, nonlinear dynamical systems, and fractional calculus.

AMR ELSONBATY received the B.Sc. degree in electronics and communications engineering and the M.Sc. and Ph.D. degrees in engineering mathematics from Mansoura University, Egypt, in 2006, 2011, and 2015, respectively. He was an Assistant Professor with the Faculty of Engineering, Mansoura University, Egypt, and a Postdoctoral Fellow with the Center for Photonics and Smart Materials, Zewail City of Science and Technology, from 2015 to 2019. He is currently an Associate Professor with the Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia, and the Faculty of Engineering, Mansoura University. His current research interests include nonlinear dynamics of electronic circuits, bifurcation theory, chaos control and synchronization, and chaos-based optical communication systems.