IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 4, 2018, accepted December 24, 2018, date of publication January 10, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891712

Digital Communication Systems Based on Three-Dimensional Chaotic Attractors

CARLOS E. C. SOUZA, DANIEL P. B. CHAVES, (Member, IEEE), AND CECILIO PIMENTEL, (Senior Member, IEEE)
Department of Electronics and Systems, Federal University of Pernambuco, Recife 50740-550, Brazil

Corresponding author: Carlos E. C. Souza (carlos.ecsouza@ufpe.br)

This work was supported in part by the Brazilian National Council for Scientific and Technological Development (CNPq), and in part by the Foundation for Support of Science and Technology of the State of Pernambuco (FACEPE).

ABSTRACT In this paper, we propose a methodology to design chaos-based communication systems, which exploits the topological structure of 3-D chaotic attractors. The first step consists in defining a proper partition of a Poincaré section of the attractor and the subsequent encoding of the chaotic trajectories. Then, the evolution mechanism of the chaotic attractor, according to the dynamical restrictions imposed by the chaotic flow, is represented by a state diagram, where each state represents a region of the Poincaré section or a branch in the template of the chaotic attractor. The state transitions are associated with segments of chaotic trajectories that connect the corresponding regions of the Poincaré section. The chaotic signals are transmitted over both additive white Gaussian noise and Rayleigh flat fading channels, and a trellis structure derived from the state diagram is used at the decoder to estimate the transmitted information sequence. Finally, the bit error rate performance of the system is analyzed.

INDEX TERMS Chaotic attractors, chaos-based communications, chaos control, error probability, Poincaré section, symbolic dynamics, topology of chaotic systems.

I. INTRODUCTION

Chaotic signals are generated by nonlinear dynamical systems and exhibit suitable characteristics for applications in communications systems, such as decorrelation, non-periodic behavior and broadband spectrum [1]. Moreover, chaotic signals can be generated by electronic circuits with good energetic efficiency [2]–[4]. Some applications of chaotic systems occur in cryptography [5], random number generation [6], watermark [7], communications [8], [9].

Several methods have been proposed to transmit digital information using chaotic waveforms, including chaos control [10], synchronization of chaotic oscillators [11], broadband coherent communication [12], symbolic dynamics with reverse iteration [13]. Multiple access schemes have been proposed using chaos shift keying (CSK), differential chaos shift keying (DSCK) [14], correlation delay shift keying (CDSK) [15]. Improved DSCK and CDSK schemes have been recently proposed in [16]–[18]. A cooperative communication scheme with DCSK modulation is analyzed in [19]. Other possibilities include chaos-coded modulation [20]–[22] and the incorporation of powerful error correcting codes with iterative decoding to improve the performance of chaos-based communication systems [23]–[25]. It is presented in [26] a procedure to modulate information symbols into chaotic waveforms generated by three-dimensional chaotic attractors using chaos control. In this case, the estimation of the transmitted information symbols is based on the comparison of a single point of the chaotic trajectories to the minimum of the Poincaré return map. A circuit implementation of an improved system that employs matched filters in the demodulator is proposed in [27].

In this work, we propose the use of the topological structure of three-dimensional chaotic attractors to design chaos-based communication systems. The topological structure of these attractors imposes dynamical constraints on the chaotic flow that can be exploited to aggregate robustness to the communication system in noisy environments.

The proposed methodology consists in defining a proper partition of a Poincaré section of the attractor such that the regions of this section are labeled with distinct symbols and the dynamical evolution of the chaotic flow is associated with the symbolic dynamics of the chaotic trajectories. We show how to employ the symbolic dynamics of the chaotic flow in a performance-guided design of a state diagram used in the

modulator and demodulator. Each state transition represents segments of chaotic trajectories that connect the corresponding regions of the Poincaré section or branches in the template of the chaotic attractor. The state transitions are induced by chaos control. The chaotic signals generated by a variable of the chaotic system are transmitted over both additive white Gaussian noise (AWGN) and Rayleigh flat fading channels and the maximum likelihood estimation of the transmitted sequence is performed by the Viterbi algorithm [28]. We analyze the performance of the proposed chaos-based communication systems over these channels using as a case study two chaotic attractors: Rössler and Lorenz. We show that our proposal performs better than the chaos-coded modulation with the same decoding complexity.

The rest of this work is organized into six sections. In Section II, we review some properties concerning the topology of three-dimensional chaotic attractors. In Section III, we detail the dynamical structure that emerges from the partitioning of a Poincaré section of the Rössler attractor and its representation as a state diagram or trellis structure. The proposed methodology is applied to the Lorenz attractor in Section IV. In Section V, we detail the Rössler and Lorenz chaos-based communication systems. The performance of these systems is analyzed in Section VI. Performance comparisons to existing chaos-based systems are conducted in this section. Finally, we discuss the conclusions of this work in Section VII.

II. TOPOLOGICAL DESCRIPTION OF CHAOTIC ATTRACTORS

This section reviews some topological properties of chaotic attractors. More details are found in [1], [29], and [30].

A dynamical system is defined by a system of coupled ordinary or partial differential equations. In the case of nonlinear equations, the dynamical system can exhibit chaotic behavior. The solutions of the differential equations, when represented in the phase space, may have a complex structure, defining sets called strange attractors, or chaotic attractors, which are attractor sets with fractal dimension [1]. When immersed in a three-dimensional space, the topological organization of the solution curves of the chaotic system, the chaotic trajectories, emerges as consequence of two basic mechanisms that generate the chaotic behavior: stretching and squeezing. These are associated with the sensibility to initial conditions (stretching) and the recurrent and non-periodic behavior (squeezing).

The dynamical evolution of an N-dimensional chaotic attractor can be described by successive crossings between the chaotic trajectories and an $(N-1)$-dimensional surface, the Poincaré section, and the points associated with these crossings are defined by the Poincaré return map of the system [1]. A labeled partition of the Poincaré section induces an encoding of the chaotic trajectories. Each chaotic trajectory is mapped to a symbolic sequence that records the order of visitation of the trajectory in the regions defined by the partition. These successive crossings associate a continuous-time dynamical system to a discrete-time system simplifying the dynamical description while retaining the essential characteristics of the chaotic flow.

The encoding of the chaotic trajectories is also useful to analyze the topological characteristics of a chaotic attractor. These are identified by the topological organization of the unstable periodic orbits (UPO) [29] of the attractor, which are chaotic trajectories with the property of returning arbitrarily close to their initial condition after some time interval. The UPO are a dense set in the attractor, thus any chaotic trajectory can be approximated by some UPO. The set of UPO of a chaotic attractor can be represented in a geometrical structure denoted *knot holder* or *template* [29]. Templates are branched manifolds that summarize the topological properties of chaotic attractors and are useful to characterize the behavior of the chaotic flow and its symbolic dynamics defined by the encoding of sequences generated by the Poincaré return map.

III. CHAOTIC MODULATION BASED ON RÖSSLER ATTRACTOR

In this section, the proposed methodology is described for the Rössler attractor.

A. THE RÖSSLER ATTRACTOR

The Rössler system is defined by the system of coupled ordinary differential equations [31]

$$\begin{cases} \dot{x}(t) = -y(t) - z(t) \\ \dot{y}(t) = x(t) + ay(t) \\ \dot{z}(t) = b + (x(t) - c)z(t) \end{cases} \tag{1}$$

where a, b and c are control parameters. In this work, we set $a = 0.423$, $b = 2$ and $c = 4$ [32]. A convenient Poincaré section for the Rössler attractor is a plane parallel to the xz plane located at the y coordinate of the center of the attractor, $y = -0.53$. Fig. 1 shows the Rössler attractor and the considered Poincaré section (represented by the horizontal line segment) in projection on the xy plane.

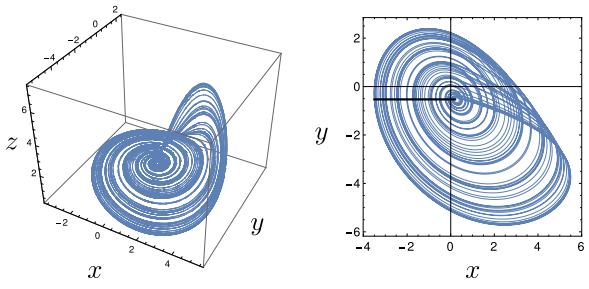

FIGURE 1. The Rössler attractor (left) and its Poincaré section (right) in projection on the *xy* plane.

B. CHAOTIC TRAJECTORIES ENCODING

Let $\mathcal{A}_n$ be an alphabet with cardinality n. A binary partition of the Poincaré section splits it into two regions with the threshold defined by the minimum of the Poincaré return

map [33], [34]. Each region is labeled with a distinct symbol $s \in \mathcal{A}_2 = \{A, B\}$. Therefore, a chaotic trajectory is represented by a symbolic sequence $s_0 s_1 s_2 \ldots$, $s_i \in \mathcal{A}_2$, where s_i is the symbol generated in the i-th crossing of the chaotic trajectory in the corresponding region of the Poincaré section.

When $n = 4$, each region of the binary partition is split into two new regions. The threshold of each new region is the point that separates two distinct behaviors of the chaotic flow in two successive crossings in the binary partition, the return to the same region and the transition from one region to the other one. We define the alphabet $\mathcal{A}_4 = \{A_1, A_2, B_1, B_2\}$ to label the four regions ($n = 4$) in such a way that the region A (resp. B) for $n = 2$ becomes A_1 and A_2 (resp. B_1 and B_2) for $n = 4$. Analogously, we can set $n = 8$ and define $\mathcal{A}_8 = \{A_{11}, A_{12}, A_{21}, A_{22}, B_{11}, B_{12}, B_{21}, B_{22}\}$. The partition of the Poincaré section for the Rössler attractor with the corresponding labeling for $n = 2$ (alphabet $\mathcal{A}_2$) and $n = 4$ (alphabet $\mathcal{A}_4$) is shown in Fig. 2 and the respective template is shown in Fig. 3. The construction of this template is detailed in [29].

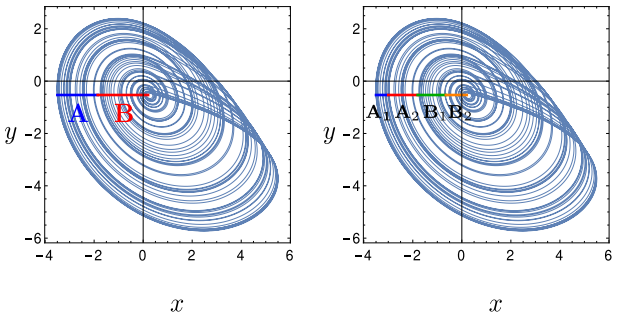

FIGURE 2. Partitioning of the Poincaré section for the Rössler attractor in projection on the *xy* plane for $n = 2$ (left) and $n = 4$ (right).

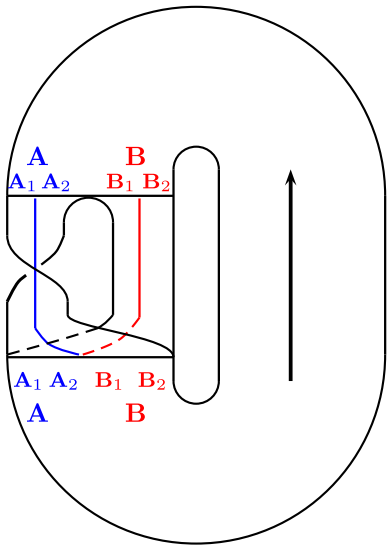

FIGURE 3. Template representation of the Rössler attractor with the regions defined by the partition of the Poincaré section for $n = 2$ and $n = 4$.

In the template representation, each branch is labeled according to the alphabet $\mathcal{A}_2$. The chaotic trajectories belonging to branch A undergo torsion and stretching to subsequently reach either branches A or B in successive crossings of the Poincaré section. The chaotic trajectories belonging to branch B also reach either branches A or B but they do not undergo torsion. The splitting procedure defined to refine the partition to $n = 4$ generates four branches over $\mathcal{A}_4$. The symbols in $\mathcal{A}_4$ with subscript 1 correspond to the subregions of the binary partition such that the chaotic trajectories crossing a subregion transition from one region to the other in the next crossing. Therefore, the label A_1 indicates that a trajectory in the subregion A_1 alternates from A to B. Similarly, the label B_1 indicates that a trajectory in B_1 alternates from B to A. The symbols in $\mathcal{A}_4$ with subscript 2 correspond to the subregions such that the chaotic trajectories return to the same region in the next crossing, thus A_2 indicates that the chaotic trajectories in the subregion A_2 return to A and B_2 indicates that the chaotic trajectories in the subregion B_2 return to B in the next crossing. For $n = 8$, the two subscripts determine the visited regions in two consecutive crossings. For example, the label A_{11} indicates that chaotic trajectories in the subregion A_{11} alternate to the region B then alternate to the region A. Proceeding with these labeling rules for all regions or branches, all transitions in the template are determined.

The dynamical structure of the chaotic flow can be represented by a state diagram with n states, where each state represents a branch of the template or a region of the Poincaré section. The state transitions are defined by two successive crossings of the chaotic flow in the section. As the regions for each n are obtained for two possible behaviors of the chaotic flow, each state has two divergent and two convergent edges. The two edges that diverge from a state are labeled with a distinct binary symbol corresponding to an information symbol. Fig. 4 shows the labeled state diagrams for the Rössler attractor for $n = 2$, $n = 4$ and $n = 8$. The structure of the state diagrams emerges from the topological characteristics of the chaotic flow, which impose dynamical constraints on the chaotic trajectories. The chaotic flow generates all sequences over $\mathcal{A}_n$ only when $n = 2$, otherwise there are restrictions in the occurrence of adjacent symbols whenever $n > 2$. Therefore, the restrictions in the occurrence of sequences of waveforms generated during the dynamical evolution of the chaotic flow can be exploited in the design of chaos-based communication systems.

C. CHAOTIC WAVEFORMS

The chaotic waveforms associated with the state transition from state i to state j are segments of chaotic trajectories associated with two consecutive crossings in the Poincaré section from region i to region j, for $i, j \in \mathcal{A}_n$. To generate a chaotic trajectory, we choose an arbitrary point (x_0, y_0, z_0) in the basin of attraction of the chaotic attractor and let the system evolve in time. After some time, the trajectory falls into the chaotic attractor and remains in it. From now on the system is ready to transmit information and this procedure is equivalent to remove the transient behavior. Since we choose points in the basin of attraction to start the system

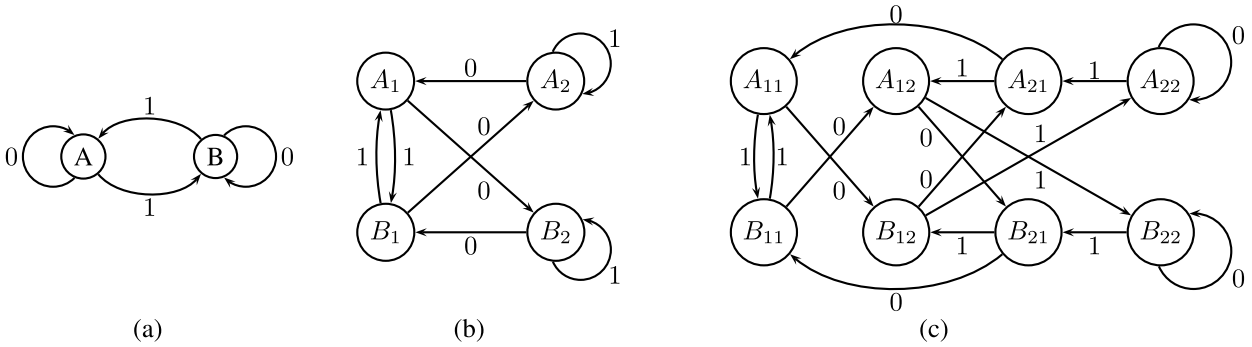

FIGURE 4. Labeled state diagrams for the Rössler attractor for $n = 2$ (a), $n = 4$ (b) and $n = 8$ (c).

evolution, the chaotic trajectories do not leave the attractor nor collapse in fixed points. We denote the chaotic waveforms generated in a state transition by *transition curves*. Each initial condition corresponds to a realization of the transition curves. The transition curves can be generated by any variable of the chaotic system x, y or z, as well as by functions of these variables. In order to exploit the characteristics of the waveforms generated by all variables of the system, we also consider the Euclidean distance between a point (x, y, z) of the attractor to the origin of the coordinate system

$$\rho = \sqrt{x^2 + y^2 + z^2}. \tag{2}$$

The time interval between two successive crossings in the Poincaré section (the duration of the transition curves) is not constant due to the aperiodicity of the chaotic behavior. Since a communication system must have a constant signaling interval, we introduce the angular variable θ as the angle between the Poincaré section and the vector obtained by connecting the center of the attractor to a point of the chaotic trajectory. This procedure ensures periodicity to the signals with an angular period 2π. Fig. 5 shows a realization of the transition curves on the xy plane for $n = 4$, $\forall i, j \in \mathcal{A}_4$. It is also shown the angle θ associated with the angular period. Fig. 6 shows the curves $x(\theta)$ versus θ in one angular period for $n = 4$. We observe from this figure that the transition curves associated with state transitions that diverge from the same state (labeled with distinct information symbols) are relatively close to each other. Thus, we introduce two modifications to be employed in the design of the communication system.

1) INVERSION OF TRANSITION CURVES

We introduce the inversion of the curves (multiplication by -1) associated with bit 0. This procedure splits the set of transition curves into two groups, one associated with bit 1 (not inverted) and the other associated with 0 (inverted). The modified transition curves associated with state transitions that diverge from (or converge to) the same state become nearly antipodals so this procedure is in agreement with the ideas introduced by Ungerboeck to design trellis coded modulation systems [35].

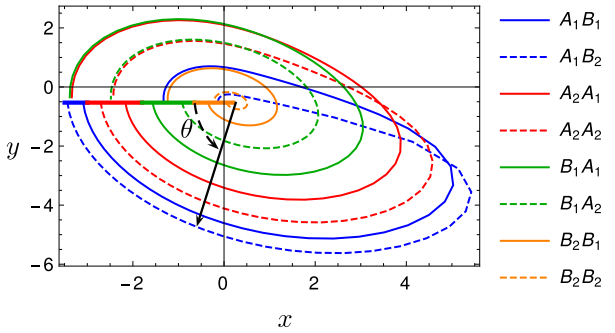

FIGURE 5. A realization of the transition curves of the Rössler attractor on the xy plane for $n = 4$. It is also shown the angle θ used to define the angular period.

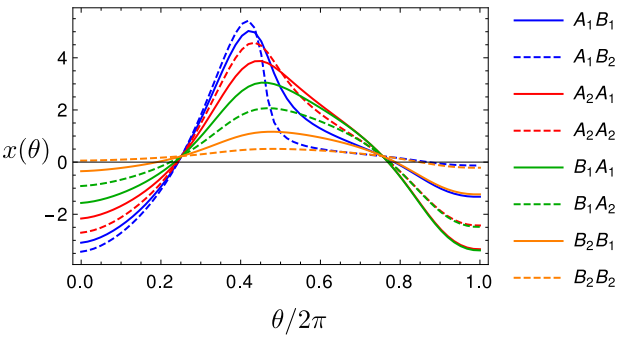

FIGURE 6. A realization of the transition curves of the Rössler attractor $x(\theta)$ versus θ for $n = 4$.

2) AMPLIFICATION

The transition curves associated with transitions that diverge from state B_2 (B_2B_1 and B_2B_2) for the case $n = 4$ have lower amplitude than the other ones, being more susceptible to noise degradation. Therefore, we introduce a gain that amplifies the signal whenever the system reaches the state B_2. This procedure increases the average energy of the system and separates these curves. When $n = 8$ the gain is applied to the transitions derived from the partition of the state B_2, that is, states B_{21} and B_{22}. The system with $n = 2$ does not use amplification.

It is worth noting that these modifications increase the overall complexity of the system but in this case we trade

complexity for performance. Now we detail how these procedures are implemented in a communication system with the Lorenz attractor.

IV. CHAOTIC MODULATION BASED ON LORENZ ATTRACTOR

The Lorenz system is defined by the system of coupled ordinary differential equations [36]

$$\begin{cases} \dot{x}(t) = \sigma(y(t) - x(t)) \\ \dot{y}(t) = x(t)(r - z(t)) - y(t) \\ \dot{z}(t) = x(t)y(t) - \beta z(t). \end{cases} \tag{3}$$

The control parameters σ, ρ and β are set to $\sigma = 10$, $r = 28$ and $\beta = 8/3$ [36]. The attractor behavior is characterized by reversions in the flow orientation. In projection on the xz plane, the chaotic flow rotates clockwise when $x < 0$ and counter-clockwise when $x > 0$. A suitable Poincaré section for this attractor should include crossings in both $x > 0$ and $x < 0$ regions. A commonly used Poincaré section is composed by two semi-planes parallels to the xy plane and located at $z = 27$ [37]. A binary partition of this section is defined by labeling each semi-plane with a distinct symbol $s \in \mathcal{A}_2$. Fig. 7 shows the Lorenz attractor and its Poincaré section in projection on the xz plane for $n = 2$ and the template is shown in Fig. 8. The construction of this template is detailed in [38]. Another template representation of the Lorenz attractor uses a single hole, like the Rössler attractor template illustrated in Fig. 3 but without torsion. Its construction is detailed in [29]. The labeling rules for the Lorenz template is the same employed in Section III. The state diagrams for the Lorenz attractor are the same as those shown in Fig. 4 for the Rössler attractor.

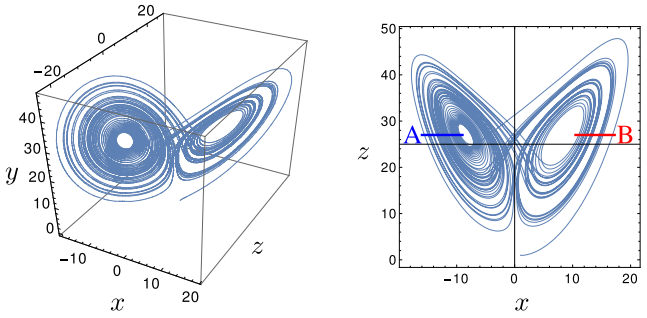

FIGURE 7. The Lorenz attractor (left) and its projection on the *xz* plane with the Poincaré section partition for $n = 2$ (right).

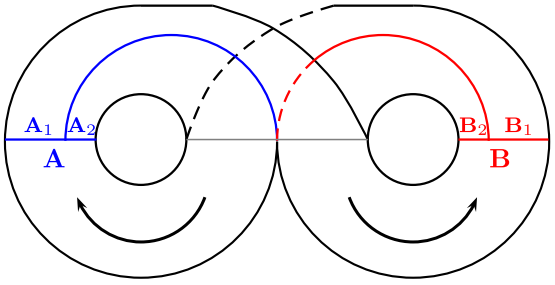

FIGURE 8. Template representation of the Lorenz attractor with the regions defined by the partition of the Poincaré section for $n = 2$ and $n = 4$.

To define an angular period we need to use two angles associated with the planes of the Poincaré section. We define θ_1 for $x < 0$ and θ_2 for $x > 0$. Therefore, the chaotic trajectories are parameterized by

$$\theta = \begin{cases} \theta_1, & x \leq 0 \\ \theta_2, & x > 0. \end{cases} \tag{4}$$

This procedure ensures periodicity of the transition curves with angular period 2π. A realization of the transition curves for $n = 4$ as well as the angles θ_1 and θ_2 are shown in Fig. 9. The amplification procedure has no effect in increasing the separation of the transition curves. Therefore, this modification is not applied to the Lorenz-based communication system. Moreover, inversions are implemented.

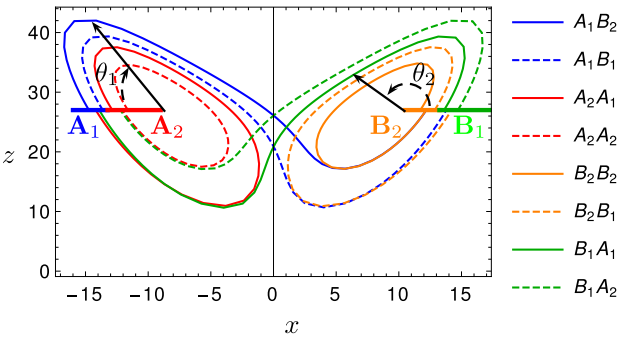

FIGURE 9. A realization of the transition curves of the Lorenz attractor on the *xz* plane for $n = 4$. It is also shown the angles θ_1 and θ_2.

V. THE COMMUNICATION SYSTEM

The block diagram of the proposed communication system is shown in Fig. 10. The binary information sequence is $b_0b_1b_2\ldots$. Each block is described in the following.

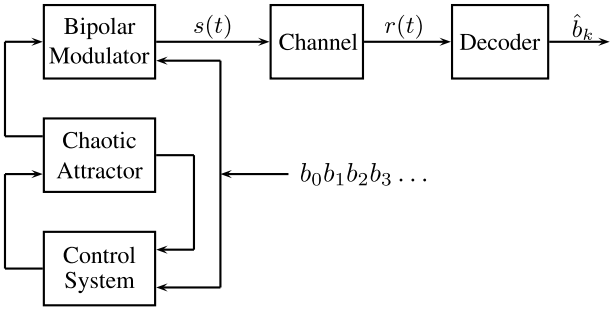

FIGURE 10. Block diagram of the communication system based on three-dimensional chaotic attractors.

1) Chaotic Attractor: The chaotic attractor is the signal source of the system. The chaotic signals can be generated by any variable of the system x, y, z, or by $\rho = \sqrt{x^2 + y^2 + z^2}$.

2) Chaos Control: The control block is coupled to the signal source and receives the binary information sequence.

This block induces the transitions in the state diagram, directing the chaotic trajectories to the regions that generate the required transition [39]. For example, if we consider the system with $n = 2$ in Fig. 4(a) and the trajectory crosses the region A and the information bit to be transmitted is 1, the control system directs the trajectory to the sub-interval of the region A that generates the transition AB, which is labeled by bit 1. Otherwise, when the chaotic trajectory crosses the region in the required sub-interval, no control action is needed.

3) Bipolar Modulator: The bipolar modulator transmits the transition curves. These curves in one angular period 2π are the transmitted signals $s(t)$ in one signaling interval of duration T. This block also receives the binary information sequence and inverts the chaotic signals associated with the bit 0 as well as amplifies the transition curves.

The encoding of the information bits in the chaotic trajectories can be summarized in the following steps:

- Step 1: Take an initial condition in the basin of attraction of the chaotic attractor and let the system evolve in time.
- Step 2: Employ the control system to keep the chaotic trajectories close to the unstable periodic orbits that cross the Poincaré section in a neighborhood of the threshold point of each region defined by the partitioning [39], [40].
- Step 3: Define one of the regions to be the initial state.
- Step 4: Take the current information bit to be transmitted. If the chaotic trajectory follows the state transition indicated by this bit, then the control system does not modify the system evolution. Otherwise, the control system modifies the chaotic trajectory to move it to the left or right of the threshold point of the region of the Poincaré section visited in the next crossing.
- Step 5: The variables of the chaotic system are combined to form the transmitted signal $s(t)$ in a signaling interval.
- Step 6 If the next state requires amplification, then the chaotic signal is amplified when the chaotic trajectory reaches the corresponding region.
- Step 7: If the information bit is 0, then the chaotic signal is inverted when the state transition occurs and the inversion lasts until the next transition.
- Step 8: Return to Step 4.

4) Channel: The signal $s(t)$ is transmitted over a noisy channel. In an AWGN channel, the noise $n(t)$, with uniform power spectral density $N_0/2$ is added to the signal $s(t)$, resulting in the received signal

$$r(t) = s(t) + n(t). \tag{5}$$

In a Rayleigh flat fading channel, the received signal is

$$r(t) = h(t)\, s(t) \, + \, n(t) \tag{6}$$

where $h(t)$ is a complex Gaussian process with zero-mean and unit variance. Furthermore, the random variable $|h(t)|$ has the Rayleigh probability density function with unit second moment. In fast fading, the fading coefficient $h(t)$ is constant during a signaling interval but changes independently in consecutive intervals.

5) Decoder: The decoder performs the maximum likelihood estimation of the transmitted binary sequence using the Viterbi algorithm [28]. It works on the trellis derived from the state diagrams shown in Fig. 4. The complexity of this algorithm for a trellis with n states with two edges diverging from each state is linear in 2 n [41, Th. 7.2]. A *typical transition curve* associated with a state transition is the mean curve obtained with several initial conditions in the same region of the Poincaré section. Therefore, all possible state transitions are associated in the decoder with the corresponding typical transition curve. The metric increments in the Viterbi algorithm are obtained with the typical transition curves.

VI. PERFORMANCE ANALYSIS

In this section, we analyze the error performance of the proposed schemes based on union bound techniques and the distance spectrum over the AWGN [41, Ch. 6] and Rayleigh fading channels [42, Ch. 12]. The decoder operates over a trellis with n states with $k = 1$ information bits per trellis interval.

A. UNION BOUND

The union bound on the first error event probability, $P_{\text{fe}}(e)$, is an important tool in the theoretical performance analysis of trellis codes and is closed related to the bit error rate (BER), and is bounded by [41, Ch. 6], [43]

$$P_{\text{fev}}(e) \leq \sum_{\mathbf{c}} P(\mathbf{c}) \sum_{\mathbf{e}} P\left(\mathbf{c} \rightarrow \mathbf{e}\right) \tag{7}$$

where $\mathbf{e}$ is the erroneous sequence that starts to diverge from the transmitted sequence $\mathbf{c}$ at a fixed trellis interval and remerges exactly once at some time later (pairwise simple error event), and $P\left(\mathbf{c} \rightarrow \mathbf{e}\right)$ is the pairwise error probability. In particular, for the AWGN channel

$$P\left(\mathbf{c} \rightarrow \mathbf{e}\right) = Q\left(\sqrt{\frac{\bar{E}_s}{2N_0}\, d^2(\mathbf{c}, \mathbf{e})}\right) \tag{8}$$

where $d^2(\mathbf{c}, \mathbf{e})$ is the squared Euclidean distance (normalized by the average energy $\bar{E}_s$) between $\mathbf{c}$ and $\mathbf{e}$, and the function $Q(\cdot)$ is defined as

$$Q\left(\alpha\right) = \int_{\alpha}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\, dx.$$

For a first error event of length L, $d^2(\mathbf{c}, \mathbf{e}) = \sum_{k=1}^{L} |c_k - e_k|^2$. Therefore

$$P_{\text{fev}}(e) \leq \sum_{\mathbf{c}} P(\mathbf{c}) \sum_{\mathbf{e}} Q\left(\sqrt{d^2(\mathbf{c}, \mathbf{e}) \frac{\bar{E}_s}{2N_0}}\right). \tag{9}$$

Let the infinite set of pairs $\{(B_i, d_i^2)\}$ be the distance spectrum (the distances are in ascending order), where the smallest distance is denoted by free distance (d_{free}) and B_i is the

average number of bit errors on erroneous sequences with distance d_i. The BER is then bounded by [41, Ch. 6]:

$$\text{BER} \leq \sum_i \frac{1}{k} B_i Q\left(\sqrt{d_i^2 \frac{\bar{E}_s}{2N_0}}\right). \tag{10}$$

The distance spectrum is typically found from the transfer function $T(x, y)$ of the trellis code

$$T(x, y) = \sum_{d=d_{\text{free}}}^{\infty} \sum_{b=1}^{\infty} c_{b,d}\, x^b\, y^{d^2} \tag{11}$$

where $c_{b,d}$ is the average number of single error events with information Hamming distance b and Euclidean distance d.

The calculation of the transfer function for trellis codes is detailed in [41], [44], and [45]. By applying the inequality

$$Q\left(\sqrt{d_i^2 \frac{\bar{E}_s}{2N_0}}\right) < e^{-d_i^2 \frac{\bar{E}_s}{4N_0}} \tag{12}$$

the BER is written as

$$\text{BER} \leq \frac{1}{k} \frac{\partial\, T(x, y)}{\partial x}\Big|_{x=1, y=e^{-\frac{\bar{E}_s}{4N_0}}}. \tag{13}$$

We now consider the fading channel, where the fading variables associated to a first error event $(|h_1|, \cdots, |h_L|)$ are independent and identically distributed Rayleigh random variables. Thus

$$P(\mathbf{c} \to \mathbf{e}) = \mathbf{E}\left[Q\left(\sqrt{\frac{\bar{E}_s}{2N_0} \sum_{\mathbf{c},\mathbf{e}} |h_k|^2 |e_k - c_k|^2}\right)\right] \tag{14}$$

where $\mathbf{E}[\cdot]$ denotes expected value. Using the alternative form for the Q function known as Craig's formula [42]

$$Q(x) = \frac{1}{\pi} \int_0^{\pi/2} e^{-\frac{x^2}{2\sin^2\theta}}\, d\theta \tag{15}$$

we obtain [42, Ch. 12]

$$P(\mathbf{c} \to \mathbf{e}) = \prod_k \frac{\sin^2\theta}{\sin^2\theta + \frac{\bar{E}_s}{4N_0}|e_k - c_k|^2}.$$

Let the transfer function be defined as

$$T(x, \theta) = \sum_{\mathbf{c}} P(\mathbf{c}) \sum_{\mathbf{e}} \prod_k x^{b_k} \frac{\sin^2\theta}{\sin^2\theta + \frac{\bar{E}_s}{4N_0}|e_k - c_k|^2} \tag{16}$$

where b_k is the number of bit errors in the k-th interval of the first error event. The calculation of $T(x, \theta)$ can be performed using standard techniques proposed in [41], [44], and [45]. Therefore,

$$\text{BER} < \frac{1}{k} \frac{1}{\pi} \int_0^{\pi/2} \left[\frac{\partial}{\partial x} T(x, \theta)|_{x=1}\right] d\theta. \tag{17}$$

B. NUMERICAL RESULTS

We apply the union bounds (13) and (17) to evaluate the BER of the proposed communication system. The SNR is defined as

$$\text{SNR} = \bar{E}_s / N_0 \tag{18}$$

where $\bar{E}_s$ is the average energy of the typical transition curves. Firstly, we compare the BER performance of systems employing the variable ρ and the other individual variables and find that better results are achieved with the variable ρ for the two attractors considered in this work. Therefore, we only consider systems with this variable in this subsection. We also investigate the optimal gain that amplifies some transition curves (as discussed in Subsection III-C) that minimizes that BER for a given SNR. This gain is approximately 3.5 for the range of SNR considered.

Figs. 11 and 12 present the union bound on the BER (solid curves) for the Rössler and Lorenz based communication systems, respectively, with two ($n = 2$), four ($n = 4$), and eight ($n = 8$) states over the AWGN and Rayleigh channels.

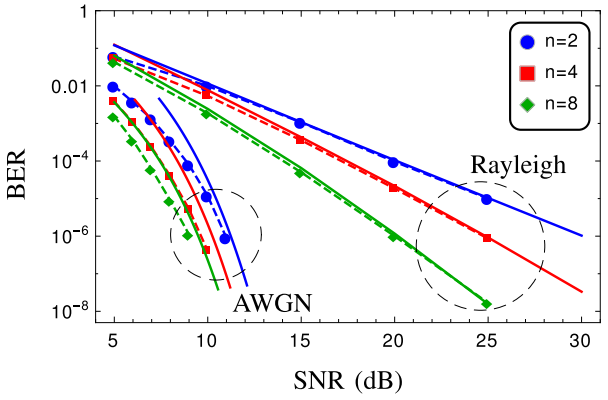

FIGURE 11. Union bound on BER versus SNR (solid curves) for the Rössler attractor communication systems with two, four and eight states over the AWGN and Rayleigh flat fading channels. Simulations are shown in dashed curves. The chaotic signals are generated by the variable ρ.

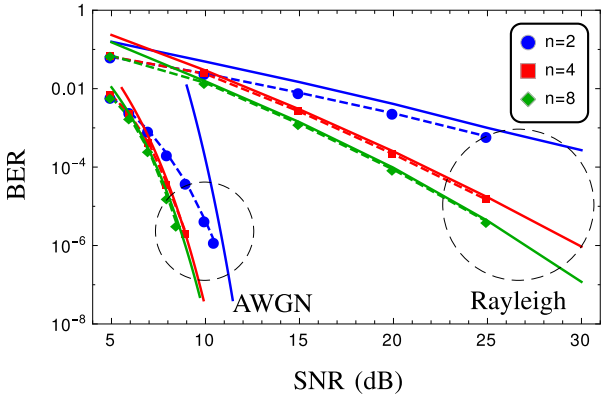

FIGURE 12. Union bound on BER versus SNR (solid curves) for the Lorenz attractor communication systems with two, four and eight states over the AWGN and Rayleigh flat fading channels. Simulations are shown in dashed curves. The chaotic signals are generated by the variable ρ.

Simulation results are shown in dashed curves. The derived upper bounds are quite effective in predicting the performance of the proposed systems and are in a good agreement with simulation results in the low BER region (BER below 10^{-6}). A comparison of the curves of these figures reveals that, for the AWGN channel, the Lorenz system with $n = 2$ outperforms the corresponding Rössler system. When $n = 4$ and $n = 8$ the performance of the Lorenz systems is better for high SNR. For the Rayleigh fading channel, the Rössler system achieves better performance for the three values of n considered. The trade-off between complexity (by increasing n) and BER is shown in these figures.

Fig. 13 compares the performance of the proposed scheme with that of the chaos trellis coded modulation proposed in [21] and [22]. The latter schemes combine a convolutional code with n states and a chaotic map at the transmitter and the decoder uses the Viterbi algorithm over a trellis with n states. It is well known that the complexity of this algorithm is proportional to the number of states. The performance of the Rössler and Lorenz systems with 8 states is better than that of the system in [21] with 256 states. However, the system in [21] with 512 states performs better than the proposed schemes for a BER below 10^{-6} with substantially more states, and consequently with higher decoding complexity. It is analyzed in [22] a chaos trellis coded modulation with a convolutional code with 32 states combined with a chaotic map, the multi tent map (mTM) and the multi Bernoulli shift map (mBSM). The scheme in [22] with 32 states and the mBSM map outperforms the proposed systems with 8 states. The curve of the non-chaotic system composed of a convolutional code with 8 states and a BPSK modulation (marked with label CC+BPSK) is also shown for reference purposes. A BER comparison for the Rayleigh channel is shown in Fig. 14. The scheme with 32 states and the mBSM map provides the best results. Table 1 summarizes the complexity versus performance tradeoff displayed in these figures, where the SNR (in dB) required to achieve a given BER (we consider BER $= 10^{-6}$) is shown for the AWGN and Rayleigh fading channels. For example, for the AWGN channel, the mBSM scheme saves 0.8 dB compared to the Lorenz attractor with $n = 8$ at the expense of an increase in the number of states.

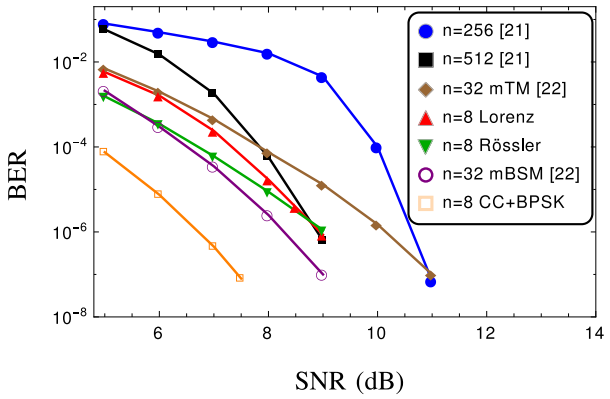

FIGURE 13. BER comparison of the Rössler and Lorenz systems with eight states ($n = 8$), the chaos trellis coded modulation system with 256 and 512 states [21], and the multi tent map (mTM) and multi Bernoulli shift map (mBSM) with 32 states [22]. The label CC+BPSK stands for a convolutional code with BPSK modulation. AWGN channel.

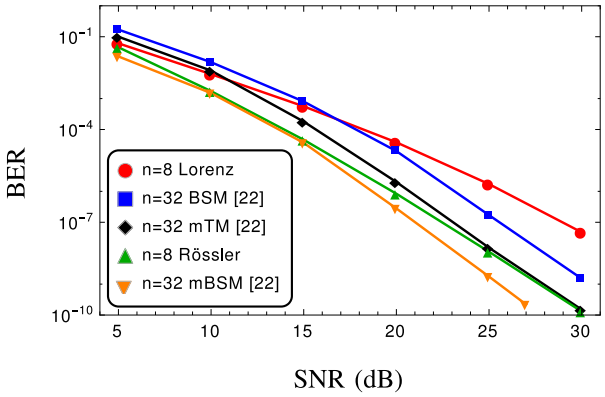

FIGURE 14. BER comparison of the Rössler and Lorenz systems with eight states ($n = 8$) and the chaos trellis coded modulation system with the multi tent map (mTM) and multi Bernoulli shift map (mBSM) with 32 states [22]. Rayleigh channel.

TABLE 1. SNR values (in dB) for chaotic communication systems over AWGN and Rayleigh fading channels to achieve BER = 10^{-6}.

	AWGN	Rayleigh
$n = 2$ Rössler	11.5	30.2
$n = 4$ Rössler	10.6	25
$n = 8$ Rössler	9.6	20
$n = 2$ Lorenz	10.3	42
$n = 4$ Lorenz	9.3	30
$n = 8$ Lorenz	9	26
$n = 256$ [21]	10.7	
$n = 512$ [21]	8.8	
$n = 32$ mTM [22]	10.2	20.8
$n = 32$ mBSM [22]	8.2	18.5

C. ENCODING OF MULTIPLE BITS

The partitioning procedure described in the previous sections implies two possible transitions from each state and the transitions curves, constructed from the variable ρ, carry one information bit.

The encoding of multiple bits per chaotic waveform improves the spectral efficiency of the communication system [46]. In this case, k bits are mapped into 2^k distinct transition curves generated by the chaotic attractor at each signaling interval. Therefore, a state diagram for this scheme has 2^k transitions diverging from each state. To accomplish this goal, it is possible to combine the three individual variables of the chaotic attractor (along with their inversions), x, y and z, to define all transition curves. To illustrate this procedure, we detail the design of a communication system based on the Rössler attractor with four states and $k = 2$ and $k = 3$.

When $k = 2$, the system requires four transition curves for each state transition to encode the sequences {00, 01, 10, 11}. Fig. 15 shows the state diagram and a possible labeling of

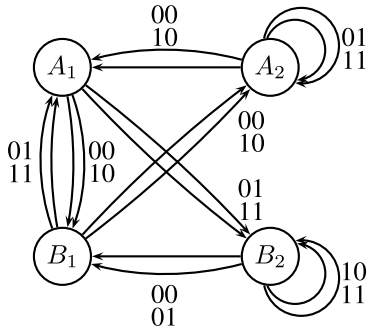

FIGURE 15. Labeled state diagram for the Rössler attractor for $n = 4$ and $k = 2$.

the state transitions. We employ antipodal curves in parallel transitions and choose individual variables that maximize the distance between the transition curves diverging from and converging to each state. For example, in state A_1 the mapping is

$$\begin{aligned} 00 &\longrightarrow x_{A_1B_1} \\ 10 &\longrightarrow -x_{A_1B_1} \\ 01 &\longrightarrow y_{A_1B_2} \\ 11 &\longrightarrow -y_{A_1B_2}. \end{aligned}$$

When $k = 3$, it is necessary to combine the individual variables. Again, from a distance analysis, we choose chaotic signals generated by x, y, $x + y$ and $y + z$. Employing these four signals and their inversions, the eight required transition curves at each state are defined. For example, a mapping in state A_1 is

$$\begin{aligned} 000 &\longrightarrow x_{A_1B_1} \\ 001 &\longrightarrow -x_{A_1B_1} \\ 010 &\longrightarrow y_{A_1B_2} \\ 011 &\longrightarrow -y_{A_1B_2} \\ 100 &\longrightarrow (x+y)_{A_1B_1} \\ 101 &\longrightarrow -(x+y)_{A_1B_1} \\ 110 &\longrightarrow (y+z)_{A_1B_2} \\ 111 &\longrightarrow -(y+z)_{A_1B_2}. \end{aligned}$$

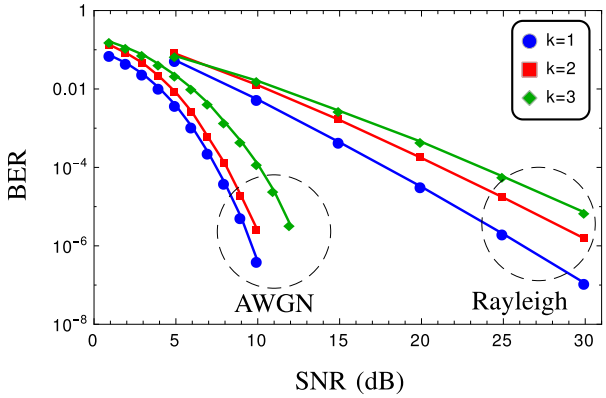

FIGURE 16. BER versus SNR for the Rössler attractor communication system with four states and $k = 1$, $k = 2$ and $k = 3$ over AWGN and Rayleigh fading channels.

Fig. 16 shows the performance of the system with $k = 1$ (using variable ρ), $k = 2$ and $k = 3$ over AWGN and Rayleigh fading channels. In the AWGN channel, the case $k = 1$ shows a performance gain of approximately 1.2 dB and 3 dB for a BER 10^{-5} in comparison to $k = 2$ and $k = 3$, respectively. The encoding of higher number of bits per waveform is possible if we use another combinations of the individual variables.

VII. CONCLUSIONS

In this work, we proposed a methodology to design communication systems based on three-dimensional chaotic attractors and detailed the construction of the system for the Rössler and Lorenz attractors. A state diagram models the structure of the symbolic dynamics that represents the dynamical evolution of the chaotic flow and the transitions curves are segments of chaotic trajectories that connect two states of the diagram. We also proposed procedures to modify the chaotic waveforms generated by the chaotic attractors in order to obtain performance gains at the cost of increasing complexity. We analyzed the performance of the proposed systems over AWGN and Rayleigh fading channels. An interesting future direction is to employ capacity approaching error correction codes, like turbo and LDPC codes, to improve the performance of the proposed system.

REFERENCES

[1] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering* (Studies in Nonlinearity Series). Boulder, CO, USA: Westview Press, 2001.

[2] P. Dudek and V. D. Juncu, "Compact discrete-time chaos generator circuit," *Electron. Lett.*, vol. 39, no. 20, pp. 1431–1432, Oct. 2003.

[3] 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.

[4] J. V. C. Evangelista, J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, "Emitter-coupled pair chaotic generator circuit," *AEU-Int. J. Electron. Commun.*, vol. 77, pp. 112–117, Jul. 2017.

[5] L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications* (Studies in Computational Intelligence). Berlin, Germany: Springer-Verlag, 2011.

[6] T. Stojanovski and L. Kocarev, "Chaos-based random number generators—Part I: Analysis [cryptography]," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 3, pp. 281–288, Mar. 2001.

[7] F. Liu and C. K. Wu, "Robust visual cryptography-based watermarking scheme for multiple cover images and multiple owners," *IET Inf. Secur.*, vol. 5, no. 2, pp. 121–128, Jun. 2011.

[8] P. Stavroulakis, *Chaos Applications in Telecommunications*. London, U.K.: Taylor & Francis, 2005.

[9] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621–2648, May 2016.

[10] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.*, vol. 64, pp. 1196–1199, Mar. 1990.

[11] R. T. Fontes and M. Eisencraft, "A digital bandlimited chaos-based communication system," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 37, pp. 374–385, Aug. 2016.

[12] B. Jovic, "Class of novel broadband chaos-based coherent communication systems," *IET Commun.*, vol. 11, no. 12, pp. 1970–1984, Sep. 2017.

[13] D. P. B. Chaves, C. E. Souza, and C. Pimentel, "A smooth chaotic map with parameterized shape and symmetry," *EURASIP J. Adv. Signal Process.*, vol. 2016, no. 1, pp. 1–10, Nov. 2016.

[14] F. Lau and C. Tse, *Chaos-Based Digital Communication Systems* (Engineering Online Library). Berlin, Germany: Springer-Verlag, 2003.

[15] M. Sushchik, L. S. Tsimring, and A. R. Volkovskii, "Performance analysis of correlation-based communication schemes utilizing chaos," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 12, pp. 1684–1691, Dec. 2000.
[16] G. Kaddoum, E. Soujeri, C. Arcila, and K. Eshteiwi, "I-DCSK: An improved noncoherent communication system architecture," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 62, no. 9, pp. 901–905, Sep. 2015.
[17] W. Xu, Y. Tan, F. C. M. Lau, and G. Kolumbán, "Design and optimization of differential chaos shift keying scheme with code index modulation," *IEEE Trans. Commun.*, vol. 66, no. 5, pp. 1970–1980, May 2018.
[18] J. Y. Duan and H. Yang, "Phase-orthogonality CDSK: A reliable and effective chaotic communication scheme," *IET Commun.*, vol. 12, no. 9, pp. 1116–1122, May 2018.
[19] P. Chen, Y. Fang, G. Han, and G. Chen, "An efficient transmission scheme for DCSK cooperative communication over multipath fading channels," *IEEE Access*, vol. 4, pp. 6364–6373, Sep. 2016.
[20] S. Kozic, T. Schimming, and M. Hasler, "Controlled one- and multidimensional modulations using chaotic maps," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 9, pp. 2048–2059, Sep. 2006.
[21] N. Khodor, J.-P. Cances, V. Meghdadi, and R. Quere, "Performances of chaos-coded modulation concatenated with Alamouti's space–time block code," *Ann. Telecommun.*, vol. 67, no. 1, pp. 27–55, Feb. 2012.
[22] F. J. Escribano, L. Lopez, and M. A. F. Sanjuan, "Chaos-coded modulations over Rician and Rayleigh flat fading channels," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 55, no. 6, pp. 581–585, Jun. 2008.
[23] C. Zhou, W. Hu, L. Wang, and G. Chen, "Turbo trellis-coded differential chaotic modulation," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 2, pp. 191–195, Feb. 2018.
[24] P. Chen, Y. Fang, K. Su, and G. Chen, "Design of a capacity-approaching chaos-based multiaccess transmission system," *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10806–10816, Dec. 2017.
[25] Q. Chen, L. Wang, Y. Lyu, and G. Chen, "Designing protograph-based LDPC codes for iterative receivers on M-ary DCSK systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 4, pp. 466–470, Apr. 2018.
[26] H. P. Ren, M. S. Baptista, and C. Grebogi, "Uncovering missing symbols in communication with filtered chaotic signals," *Int. J. Bif. Chaos*, vol. 22, no. 8, pp. 1250199-1–1250199-11, Aug. 2012.
[27] H.-P. Ren, C. Bai, J. Liu, M. S. Baptista, and C. Grebogi, "Experimental validation of wireless communication with chaos," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 26, no. 8, pp. 083117-1–083117-9, Aug. 2016.
[28] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms*, 1st ed. Hoboken, NJ, USA: Wiley, 2005.
[29] R. Gilmore and M. Lefranc, *The Topology of Chaos: Alice in Stretch and Squeezeland*, 2nd ed. Hoboken, NJ, USA: Wiley, 2012.
[30] K. Alligood, T. Sauer, and J. Yorke, *Chaos: An Introduction to Dynamical Systems*. New York, NY, USA: Springer, 1997.
[31] O. E. Rössler, "An equation for continuous chaos," *Phys. Lett. A*, vol. 57, no. 5, pp. 397–398, Sep. 1976.
[32] J.-M. Ginoux and C. Letellier, "Flow curvature manifolds for shaping chaotic attractors: I. Rössler-like systems," *J. Phys. A, Math. Theor.*, vol. 42, no. 28, pp. 285101-1–285101-17, 2009.
[33] H.-P. Ren, M. S. Baptista, and C. Grebogi, "Wireless communication with chaos," *Phys. Rev. Lett.*, vol. 110, pp. 184101-1–184101-5, Apr. 2013.
[34] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, no. 20, pp. 3031–3034, May 1993.
[35] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inf. Theory*, vol. 28, no. 1, pp. 55–67, Jan. 1982.
[36] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.
[37] D. Viswanath, "Symbolic dynamics and periodic orbits of the Lorenz attractor," *Nonlinearity*, vol. 16, no. 3, pp. 1035–1056, Apr. 2003.
[38] J. S. Birman and R. F. Williams, "Knotted periodic orbits in dynamical systems I: Lorenz's equations," *Topology*, vol. 22, no. 1, pp. 47–82, 1983.
[39] T. Shinbrot, E. Ott, C. Grebogi, and J. A. Yorke, "Using chaos to direct trajectories to targets," *Phys. Rev. Lett.*, vol. 65, pp. 3215–3218, Dec. 1990.
[40] K. Pyragas, "Continuous control of chaos by self-controlling feedback," *Phys. Lett. A*, vol. 170, no. 6, pp. 421–428, Nov. 1992.
[41] C. B. Schlegel and L. C. Pérez, *Trellis and Turbo Coding*, 1st ed. Hoboken, NJ, USA: Wiley, 2003.
[42] M. Simon and M. Alouini, *Digital Communication Over Fading Channels*. Hoboken, NJ, USA: Wiley, 2000.
[43] A. P. D. Rosiers and P. H. Siegel, "On performance bounds for space-time codes on fading channels," *IEEE Trans. Commun.*, vol. 52, no. 10, pp. 1688–1697, Oct. 2004.
[44] J. Shi and R. D. Wesel, "Efficient computation of trellis code generating functions," *IEEE Trans. Commun.*, vol. 52, no. 2, pp. 219–227, Feb. 2004.
[45] D. Aktas and M. P. Fitz, "Distance spectrum analysis of space-time trellis-coded modulations in quasi-static Rayleigh-fading channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3335–3344, Dec. 2003.
[46] J. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2007.

CARLOS E. C. SOUZA received the Ph.D. degree in electrical engineering from the Federal University of Pernambuco, Recife, Brazil, in 2018. His current research interests include chaos communication, classical and quantum information theory, and random matrix theory.

DANIEL P. B. CHAVES received the B.S. degree in electronics engineering and the M.S. degree in electrical engineering from the Federal University of Pernambuco, Recife, Brazil, in 2004 and 2006, respectively, and the Ph.D. degree in electrical engineering from the State University of Campinas, São Paulo, Brazil, in 2011. In 2012, he joined the Department of Electronics and Systems, Federal University of Pernambuco, as an Assistant Professor. His current interests include information theory, coding theory, symbolic dynamics, system modeling, chaos communication, chaotic circuits, and chaos-based random number generators.

CECILIO PIMENTEL was born in Recife, Brazil, in 1966. He received the B.Sc. degree in electrical engineering from the Federal University of Pernambuco, Recife, in 1987, the M.Sc. degree in electrical engineering from the Catholics University of Rio de Janeiro, Rio de Janeiro, Brazil, in 1990, and the Ph.D. degree in electrical engineering from the University of Waterloo, ON, Canada, in 1996. From 2007 to 2008, he was a Visiting Research Scholar with the Department of Mathematics and Statistics, Queen's University, Kingston, Canada. Since 1996, he has been with the Department of Electronics and Systems, Federal University of Pernambuco, where he is currently an Associate Professor. His research interests include digital communications, information theory, and error correcting coding.