Do chaos-based communication systems really transmit chaotic signals?

Renato Candido[a], Diogo C. Soriano[b], Magno T. M. Silva[*,a], Marcio Eisencraft[a]

[a] *University of São Paulo, Brazil*
[b] *Universidade Federal do ABC, Brazil*

Abstract

Many communication systems based on the synchronism of chaotic systems have been proposed as an alternative spread spectrum modulation that improves the level of privacy in data transmission. However, depending on the map and on the encoding function, the transmitted signal may cease to be chaotic. Therefore, the sensitive dependence on initial conditions, which is one of the most interesting properties for employing chaos in Telecommunications, may disappear. In this paper, we numerically analyze the chaotic nature of signals modulated using a system that employs the Ikeda map. Additionally, we propose changes in the communication system in order to guarantee that the modulated signals are in fact chaotic.

Key words: Chaos; nonlinear systems; chaos-based communication systems; Ikeda map; attractors.

1. Introduction

Non-linear systems and chaos have been applied in all areas of Engineering [1]. This fact is particularly true when it comes to Signal Processing and Telecommunications, especially after the works by Pecora and Carroll [2] and Ott et al. [3]. Chaos has appeared in different areas as digital and analog

*Corresponding author
URL: renatocan@lps.usp.br (Renato Candido), diogo.soriano@ufabc.edu.br (Diogo C. Soriano), magno@lps.usp.br (Magno T. M. Silva), marcio@lcs.poli.usp.br (Marcio Eisencraft)

modulation, cryptography, pseudorandom sequences generation, watermarking, nonlinear adaptive filters, phase-locked loop networks, among others (see e.g., [4]-[13]).

Three defining properties of chaotic signals are their boundedness, aperiodicity and sensitive dependence on initial conditions (SDIC) [14]. This last property means that, if the generator system is initialized with a slightly different initial condition, the obtained signal quickly diverges from the original one. These three properties all together are necessary for a signal to be called *chaotic* and are the basis for the alleged advantages of using chaos in communications, as an improvement in security [15]. However, in almost all chaos-based communication schemes proposed in the literature, the facts that there is a nonlinear system that, when isolated, generates chaotic signals and that the transmitted signals are apparently aperiodic are taken as sufficient evidence of chaos, without further investigation. The SDIC is taken for granted. This is partly due to the fact that when it comes to practical applications, to verify the SDIC is not immediate.

As communication systems are always related to the transmission of probabilistic aperiodic messages, it becomes non-trivial and of paramount importance to detect if the aperiodicity in the transmitted signals comes from the nonlinearity of the transmitter or from the message itself, in which case the chaos advantages are not really present. This issue is particularly relevant when the non-linear system employed presents a stable fixed point besides the chaotic attractor. From one temporal series it is hard to visually distinguish a chaotic signal stepping through the chaotic attractor and an orbit converging to the fixed point but continuously perturbed. The difference is only in terms of SDIC.

As an example, Figure 1-(a) shows the expected behavior of chaotic signals. Two aperiodic orbits with very close initial conditions are shown. After approximately 40 samples they become apart in the state space, clearly presenting SDIC. In contrast, the signals in Figure 1-(b) does not present SDIC. Starting from different initial conditions, they start to follow almost the same path after approximately 70 samples. Although bounded and aperiodic, the signals in

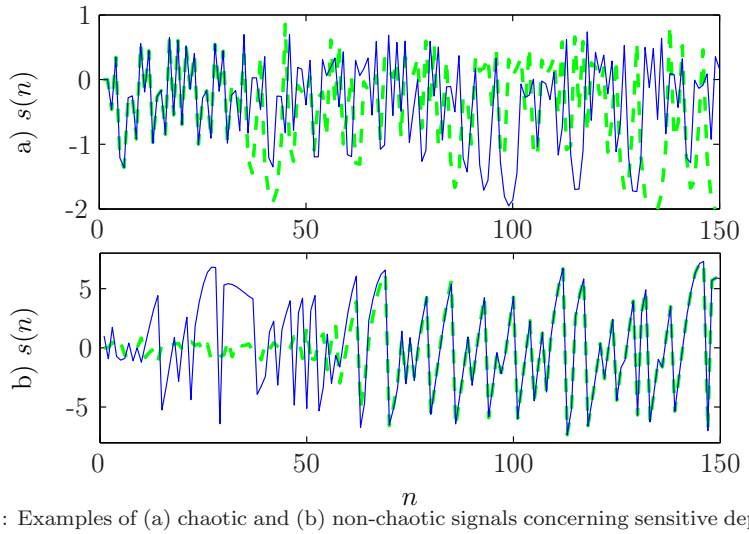

Figure 1: Examples of (a) chaotic and (b) non-chaotic signals concerning sensitive dependence on initial conditions. (a) Two aperiodic orbits with very close initial conditions turning into different signals after some iterations. (b) Two signals starting with different initial conditions leading to the same orbit after some iterations.

Figure 1-(b) are not chaotic.

The usual technique to evaluate the SDIC is via Lyapunov Exponents (LE) [14]. The Lyapunov numbers are the average per-step exponential divergence rate of nearby points along an orbit, one for each direction, and the LE are the natural logarithm of the Lyapunov numbers [14]. Given a deterministic map, it is relatively straightforward to numerically evaluate the LE of its orbits [14]. However, when it comes to chaos-based communication systems proposals where the message to be transmitted is fed back in the chaotic signal generator (CSG) [16]-[19], complications may appear.

Bearing all these in mind, in this paper we analyze the chaos-based communication system proposed in [19] in order to verify if the transmitted signals are in fact chaotic. Ref. [19] employed a particular codification scheme in order to implement an efficient communication system based on Ikeda map [14, 20]. This map was considered in [19] since it can be envisioned as arising from a string of light pulses impinging on a partially transmitting mirror of a ring cavity with a nonlinear dispersive medium, and therefore, can be used to model

a discrete-time low-pass version of the optical communication scheme of [15]. However, caution must be taken, once that the Ikeda map presents co-existing attractors with close basin of attractions: a stable fixed point and a chaotic attractor [14]. This particular structure can possibly generate some drawbacks for the conception of efficient chaos-based communication systems, presenting apparently aperiodicity with lack of SDIC. Therefore, in this work, a more detailed analysis concerning the presence and the consequences of dealing with co-existing attractors is performed and illustrated by a representative set of simulations. Furthermore, a strategy guided by the LE associated with such attractors is adopted for suitably defining the amplitude of the message in order to guarantee a truly chaos-based system.

The paper is organized as follows. In Section 2, we review the system used in [17, 18, 19] and Section 3 describes the main properties of the Ikeda map. In Section 4, we numerically analyze the transmitted signals of [19] and propose changes in the system in order to guarantee that the transmitted signals are truly chaotic. Finally, in Section 5, we draft some conclusions.

2. Problem Formulation

Wu and Chua's synchronization scheme proposed in [16] is a simple way to use chaos for communication. They addressed chaotic system synchronization differently from Pecora and Carroll's seminal paper [2]. Instead of using conditional LE to check the asymptotic stability of the slave system and hence the possibility of synchronism, Wu and Chua restated the master and slave equations in such a way that it is easy to verify the convergence of the synchronization error to zero. Based on this synchronization scheme, a communication system was proposed in [16] and a discrete-time version appeared later in [21]. In this section, we succinctly revise these ideas.

Consider two discrete-time systems defined by

$$\mathbf{x}(n+1) = \mathbf{A}\mathbf{x}(n) + \mathbf{b} + \mathbf{f}(x_i(n)) \tag{1}$$

$$\widehat{\mathbf{x}}(n+1) = \mathbf{A}\widehat{\mathbf{x}}(n) + \mathbf{b} + \mathbf{f}(x_i(n)) \tag{2}$$

where $n \in \mathbb{N}$ represents time instants, $\mathbf{x}(n)$ and $\widehat{\mathbf{x}}(n)$ are real-valued column vectors of length K, i.e, $\mathbf{x}(n) = [x_1(n)\, x_2(n)\, \cdots\, x_K(n)]^T$ and $\widehat{\mathbf{x}}(n) = [\widehat{x}_1(n)\, \widehat{x}_2(n)\, \cdots\, \widehat{x}_K(n)]^T$, x_i and $\widehat{x}_i$ represent states of the system with $i = 1, \cdots, K$, and $(\cdot)^T$ stands for transposition. $\mathbf{A}$ is a square matrix and $\mathbf{b}$ a column vector, both constants, real-valued and of dimension K. The vector function $\mathbf{f}(\cdot)$: $\mathbb{R} \to \mathbb{R}^K$ is nonlinear in general and is assumed to depend solely on one component of $\mathbf{x}(n)$, having the form

$$\mathbf{f}(x_i(n)) = [\underbrace{0\ 0\ \cdots\ 0}_{i-1 \text{ zeros}}\ f\left(x_i(n)\right)\ \underbrace{0\ 0\ \cdots\ 0}_{K-i \text{ zeros}}]^T, \tag{3}$$

where $f(\cdot)$ is a scalar function. The system described by (1) is autonomous and is called *master*, whereas the one described by (2) depends on $x_i(n)$ and is called *slave*.

The synchronization error is defined as $\mathbf{e}(n) \triangleq \widehat{\mathbf{x}}(n) - \mathbf{x}(n)$ and its dynamics is given by

$$\mathbf{e}(n+1) = \mathbf{A}\mathbf{e}(n). \tag{4}$$

Master and slave are said *completely synchronized* [22] if $\mathbf{e}(n) \to \mathbf{0}$ as n grows. Consequently, a sufficient condition for complete synchronization is given by

$$|\lambda_i| < 1, \quad 1 \leq i \leq K, \tag{5}$$

where λ_i are the eigenvalues of $\mathbf{A}$ [23]. Therefore, if a system can be written as (1) with the eigenvalues of $\mathbf{A}$ satisfying (5), it is easy to set up a slave system that synchronizes with it.

Using this synchronization method, Wu and Chua [16] proposed an information transmission system using chaotic signals that leads to no errors under ideal channel conditions. A block diagram of the discrete-time version of this system is shown in Figure 2 [21]. In this scheme, the information signal $m(n)$ is encoded by using the i-th component of the state vector $\mathbf{x}(n)$ via a coding function

$$s(n) = c\left(x_i(n), m(n)\right), \tag{6}$$

so that the information signal can be decoded using the inverse function with respect to $m(n)$, i.e.,

$$m(n) = c^{-1}\left(x_i(n), s(n)\right). \tag{7}$$

The equations governing the global system have the same form as (1)-(2). The only changes are the arguments of $\mathbf{f}(\cdot)$, i.e.,

$$\mathbf{x}(n+1) = \mathbf{A}\mathbf{x}(n) + \mathbf{b} + \mathbf{f}(s(n)) \tag{8}$$

$$\widehat{\mathbf{x}}(n+1) = \mathbf{A}\widehat{\mathbf{x}}(n) + \mathbf{b} + \mathbf{f}(s(n)). \tag{9}$$

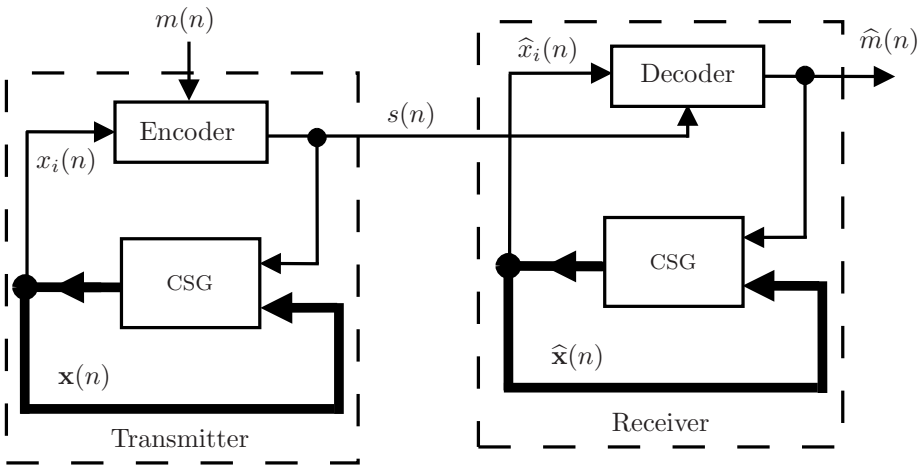

Figure 2: Chaotic communication system.

Since the synchronization error dynamics is given again by (4) and if (5) holds, then $\widehat{\mathbf{x}}(n) \to \mathbf{x}(n)$ and, in particular, $\widehat{x}_i(n) \to x_i(n)$. Thus, using (7), we obtain

$$\widehat{m}(n) = c^{-1}\left(\widehat{x}_i(n), s(n)\right) \to c^{-1}\left(x_i(n), s(n)\right) = m(n). \tag{10}$$

Therefore, when transmitter and receiver parameters are perfectly matched over an ideal channel, the message is recovered without degradation at the receiver except for a synchronization transient.

In this context, different chaotic maps can be written in a form similar to (8) and (9) and therefore, can be used in a chaos-based communication system.

These are the cases of Hénon [24] and Ikeda [20] maps, as we shall see in the sequel.

2.1. Communication system using the Hénon map

The Hénon map can be described by the following equations [14, 24]

$$\mathbf{x}(n+1) = \begin{bmatrix} x_1(n+1) \\ x_2(n+1) \end{bmatrix} = \begin{bmatrix} \alpha - x_1^2(n) + \beta x_2(n) \\ x_1(n) \end{bmatrix}, \tag{11}$$

that can be rewritten as (1) with $K = 2$, $\mathbf{A} = \begin{bmatrix} 0 & \beta \\ 1 & 0 \end{bmatrix}$, $\mathbf{b} = [\,\alpha \;\; 0\,]^T$, and $\mathbf{f}(x_1(n)) = \begin{bmatrix} -x_1^2(n) & 0 \end{bmatrix}^T$. The eigenvalues of $\mathbf{A}$ are $\lambda_{1,2} = \pm\sqrt{\beta}$ and, according to (5), there is chaotic synchronization for $|\beta| < 1$.

The equations governing the communication system based on (11) have the same form as (8) and (9) with $\mathbf{f}(s(n)) = \begin{bmatrix} -s^2(n) & 0 \end{bmatrix}^T$. As coding function, we may choose [18]

$$s(n) = c\,(x_1(n), m(n)) = m(n)x_1(n), \tag{12}$$

being $m(n) = \pm 1$ a binary polar message. For this particular choice of $c(\cdot\,,\,\cdot)$, the decoding function can be implemented by

$$\widehat{m}(n) = c^{-1}\,(\widehat{x}_1(n), s(n)) = \frac{s(n)}{\widehat{x}_1(n)}. \tag{13}$$

The encoding function (12) associated to the Hénon map has an interesting property: for a binary polar message, we can observe from (12) that $s^2(n) = x_1^2(n)$. Thus, $\mathbf{f}(s(n)) = \mathbf{f}(x_1(n))$ does not depend on $m(n)$. Consequently, the message does not disturb the Hénon CSGs. This means that the transmitted signal is in fact chaotic as long as the signals generated by the CSGs are chaotic.

Figure 3 shows an example of a binary message $m(n)$, transmitted signal $s(n)$ encoded by the Hénon map with $\alpha = 1.4$ and $\beta = 0.3$, and recovered message $\widehat{m}(n)$ for an ideal channel. We can observe in this case that the message is recovered perfectly after a transient, as expected.

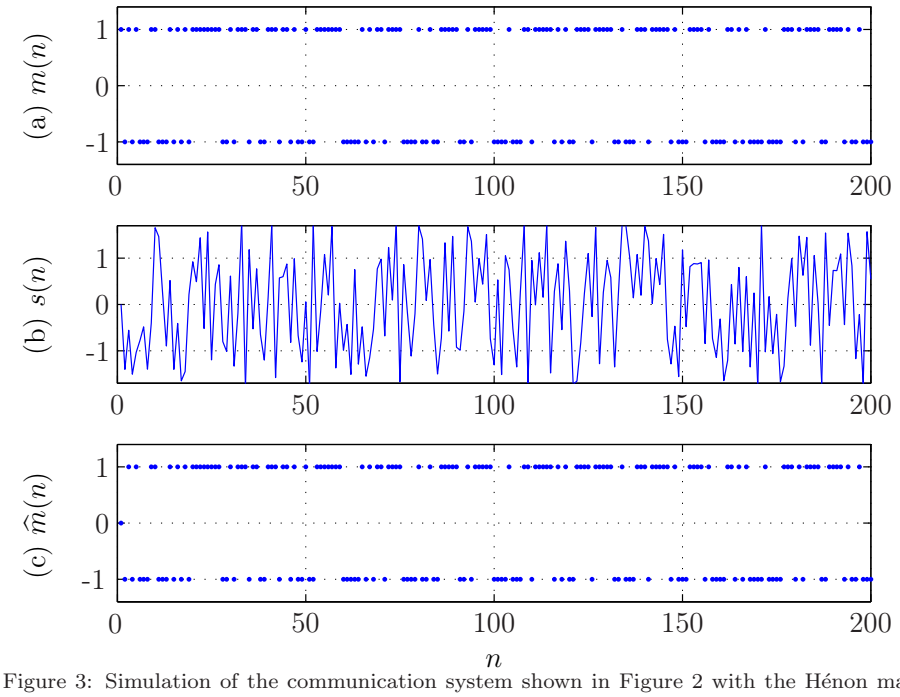

Figure 3: Simulation of the communication system shown in Figure 2 with the Hénon map ($\alpha = 1.4$ and $\beta = 0.3$): (a) message $m(n)$; (b) transmitted signal $s(n)$; and (c) recovered message $\widehat{m}(n)$.

2.2. Communication system using the Ikeda map

Under some simplifying assumptions, the Ikeda map is a model for a type of cell that might be used in an optical computer [14, 20]. It is a bidimensional map given by

$$\mathbf{x}(n+1) = \begin{bmatrix} x_1(n+1) \\ x_2(n+1) \end{bmatrix} = \begin{bmatrix} C_2 x_1(n)\cos\theta(n) - C_2 x_2(n)\sin\theta(n) + R \\ C_2 x_1(n)\sin\theta(n) + C_2 x_2(n)\cos\theta(n) \end{bmatrix}, \quad (14)$$

where

$$\theta(n) = C_1 - \frac{C_3}{1 + x_1^2(n) + x_2^2(n)}, \quad (15)$$

and C_1, C_2, C_3, and R are real constants.

The equations governing the communication system based on (14) can be

written in a form similar to (8) and (9), i.e.,

$$\mathbf{x}(n+1) = \mathbf{A}_t(n)\mathbf{x}(n) + [\,R \;\; 0\,]^T, \tag{16}$$

$$\widehat{\mathbf{x}}(n+1) = \mathbf{A}_r(n)\widehat{\mathbf{x}}(n) + [\,R \;\; 0\,]^T, \tag{17}$$

where

$$\mathbf{A}_t(n) = C_2 \begin{bmatrix} \cos\theta_t(n) & -\sin\theta_t(n) \\ \sin\theta_t(n) & \cos\theta_t(n) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & m(n) \end{bmatrix},$$

$$\mathbf{A}_r(n) = C_2 \begin{bmatrix} \cos\theta_r(n) & -\sin\theta_r(n) \\ \sin\theta_r(n) & \cos\theta_r(n) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \widehat{m}(n) \end{bmatrix},$$

$$\theta_t(n) = C_1 - \frac{C_3}{1 + x_1^2(n) + s^2(n)}, \qquad \theta_r(n) = C_1 - \frac{C_3}{1 + \widehat{x}_1^2(n) + \widehat{s}^2(n)},$$

$s(n) = m(n)x_2(n)$, and $\widehat{s}(n) = \widehat{m}(n)\widehat{x}_2(n)$. Again, we have assumed the same encoding function of the previous example [Eq. (12)] with $x_2(n)$ in place of $x_1(n)$ as in [19] and a binary message. It is important to notice that, differently from the communication system based on the Hénon map, the matrices $\mathbf{A}_t$ and $\mathbf{A}_r$ are now time-dependent and contain the nonlinear encoding function.

In this case, the dynamics of the synchronization error is given by

$$\mathbf{e}(n+1) = [\mathbf{A}_r(n) - \mathbf{A}_t(n)]\,\mathbf{e}(n). \tag{18}$$

Ensuring the exponential stability of (18) is a sufficient (but not necessary) condition for complete synchronization between master and slave. From linear system theory, (18) is uniformly exponentially stable if there exist a constant $0 \leq \rho < 1$ such that the maximum absolute eigenvalue of $[\mathbf{A}_r(n) - \mathbf{A}_t(n)]$ satisfies [25]

$$\prod_{n=N_1}^{N_2} |\lambda_{\max}(n)| \leq \rho^{N_2 - N_1 + 1} \;\text{ for all } N_2 \text{ and } N_1 \text{ such that } N_2 \geq N_1, \tag{19}$$

where $|\lambda_{\max}(n)| \triangleq \max\{|\lambda_1(n)|,\ |\lambda_2(n)|\}$ and $\lambda_i(n)$, $i = 1, 2$ are the eigenvalues of $[\mathbf{A}_r(n) - \mathbf{A}_t(n)]$. In other words, if $|\lambda_{\max}(n)| < 1$ for all $n \geq N_1$, master and slave synchronize completely in an Ikeda-based communication system.

Proving that $|\lambda_{\max}(n)| < 1$ for all n greater than some N_1 is not a simple task and some assumptions on the transmitted and recovered message are necessary, even when the channel is ideal. This occurs since in the Ikeda map $\mathbf{A}_t(n)$ and $\mathbf{A}_r(n)$ depend on $m(n)$ and $\widehat{m}(n)$, respectively. Therefore, we show next some numerical simulations to illustrate that the synchronization between master and slave may be achieved for an ideal channel, considering the usual parameters for the Ikeda map [14]:

$$C_1 = 0.4, \quad C_2 = 0.9, \quad C_3 = 6, \quad \text{and} \quad R = 1. \tag{20}$$

Assuming a binary equiprobable random message $m(n) \in \{-1,\ +1\}$ and initializing the state vectors as $\mathbf{x}(0) = \mathbf{0}$ and $\widehat{\mathbf{x}}(0) = [\,0.1\ \ -0.1\,]^T$, we performed $L = 10^4$ independent runs of Eqs. (16) and (17). For each iteration n, we observed $|\lambda_{\max}(n)|$ along all the L runs. Figure 4-(a) shows the maximum value of $|\lambda_{\max}(n)|$ for each iteration among the L runs and Figure 4-(b) shows a histogram of $|\lambda_{\max}(n)|$ at $n = 30$. From the histogram, we can observe that the maximum absolute value of the eigenvalues may be greater than one at $n = 30$, but this occurs with a low frequency (only 16 times in 10^4 runs). As n grows, the frequency of $|\lambda_{\max}(n)| > 1$ decreases and after 64 iterations, $\max_L\{|\lambda_{\max}(n)|\}$ converges to a value smaller than one. Therefore, (19) is satisfied and master and slave completely synchronize. By means of simulations with different initializations, we have noticed that this is the typical behavior when master and slave are initialized in the same basin of attraction.

3. Basins of attraction of the Ikeda map

Although we can observe synchronization in the communication system described by (16) and (17), there is no guarantee that the transmitted signal is actually chaotic. This occurs since the Ikeda map presents a stable fixed point besides the chaotic attractor, as described next.

In certain ranges of the parameters C_1, C_2, C_3, and R, the Ikeda map presents two fixed point sinks. For instance, setting these parameters as (20),

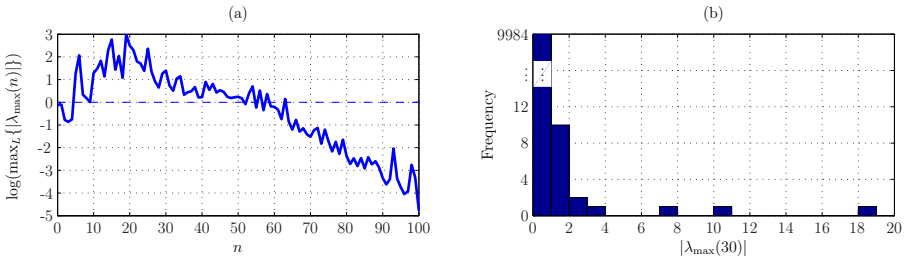

Figure 4: (a) Logarithm of the maximum value of $|\lambda_{\max}(n)|$ in $L = 10^4$ independent runs and (b) histogram of the maximum absolute values of the eigenvalues of $\mathbf{A}_r(n) - \mathbf{A}_t(n)$ at $n = 30$, assuming a binary equiprobable random message.

one of these sinks has developed into what is numerically observed to be a chaotic attractor, with LE $h_1 = 0.51$ and $h_2 = -0.72$. The remaining stable fixed point is located at $\mathbf{x}^* \approx [2.97 \;\; 4.15]^T$ with LE $h_1 \approx -0.11$ and $h_2 = -0.10$. For this set of parameters, the orbits of (14) present two possible behaviors: (i) convergence to the fixed point $\mathbf{x}^*$ or (ii) convergence to the chaotic attractor. Figure 5 shows both attractors in the phase state along with their basins of attraction. The chaotic attractor is shown in black and the fixed point attractor is indicated by a cross. The highlighted area indicates the points of the map that lead to the chaotic attractor, whereas the points outside this area lead to the fixed point attractor. Hence, we can conclude that using a map like Ikeda's in a scheme as the one described in Figure 2 requires caution. Depending on the perturbation represented by the message encoding, the orbit can easily escape from the basin of attraction of the chaotic regime.

In the following, the co-existing attractors are characterized in terms of their LE, which, afterwards, are taken as a criteria for suitably setting the amplitude of the message, avoiding transitions of basin of attractions and ensuring chaos-based operation for such communicating system. To accomplish this task, the procedure for LE numerical evaluation is briefly described in Appendix A.

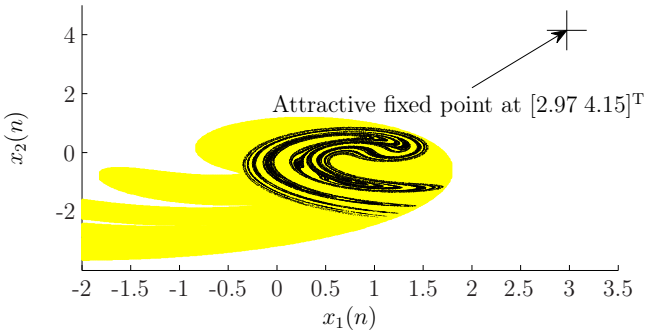

Figure 5: Ikeda map attractors.

4. Numerical analysis

Assuming the multiplication as encoding function, i.e., $s(n) = m(n)x_2(n)$ and a binary message, we show next an example to illustrate that the orbit may escape from the basin of attraction of the chaotic regime for the system described in Section 2.2. Figure 6 shows a portion of a binary message $m(n)$, the corresponding portion of the signal $s(n)$, and the phase space $x_1(n)$ by $x_2(n)$. The yellow area in Figure 6-(c) indicates the basin of attraction of the chaotic attractor shown with black and red points. Depending on the value of the state $x_2(n)$, when it is multiplied by -1, we can observe two different behaviors: i) if $x_2(n)$ is one of the black points in the yellow area, the orbit remains in it and $s(n)$ remains chaotic or ii) if $x_2(n)$ is one of the red points in the yellow area, the coordinate $[x_1(n),\ -x_2(n)]$ is outside the basin of attraction, and therefore the orbit escapes from the chaotic regime. For instance, in the iteration n_1, $x_2(n_1)$ is a black point and the encoding of $m(n_1) = -1$ does not perturb the chaotic regime. On the other hand, in the iteration n_2, $x_2(n_2)$ is a red point and the encoding of $m(n_2) = -1$ leads the orbit to the fixed point, indicated by the cross in the figure. Notice that once the orbit has left the basin of attraction of the chaotic attractor, it will never come back. Each time a -1 is presented, the orbit just oscillates next to the attractive fixed point, generating a signal as shown in Figure 1-(b). These signals are not chaotic.

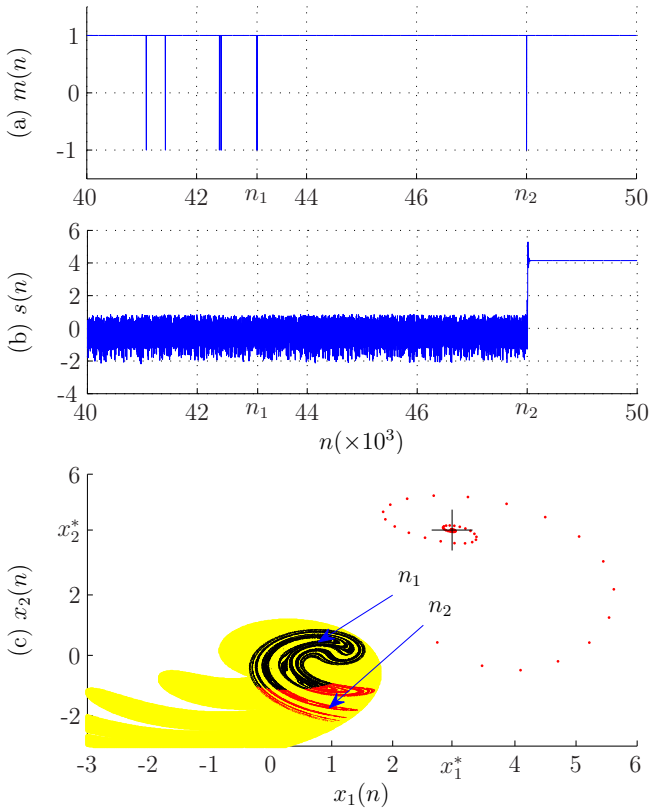

Figure 6: Example where the encoding of the message leads to a non-chaotic behavior: (a) Portion of the message to be encoded; (b) Portion of the signal obtained after the encoding of the message; (c) Phase space ($x_1(n)$ by $x_2(n)$) converging to the fixed point indicated by the cross; Ikeda map with parameters as (20).

To solve this problem, instead of using the multiplication, we can consider the following encoding function

$$s(n) = x_2(n) + \frac{\gamma}{2}[1 + m(n)]. \tag{21}$$

Figure 7 shows attractors in the phase state along with their basins of attraction considering (21) as encoding function. Figures 7-(a), (b), and (c) consider (21) with $\gamma = 1$, $\gamma = 10^{-2}$, and $\gamma = 10^{-3}$, respectively. We can observe that $\gamma = 1$ is not a good choice, since there are many points in the yellow area that lead the orbit to the fixed point. For $\gamma = 10^{-2}$, few points in the yellow area may lead the orbit to the fixed point. Finally, using $\gamma = 10^{-3}$ the orbit always remains

in the yellow area.

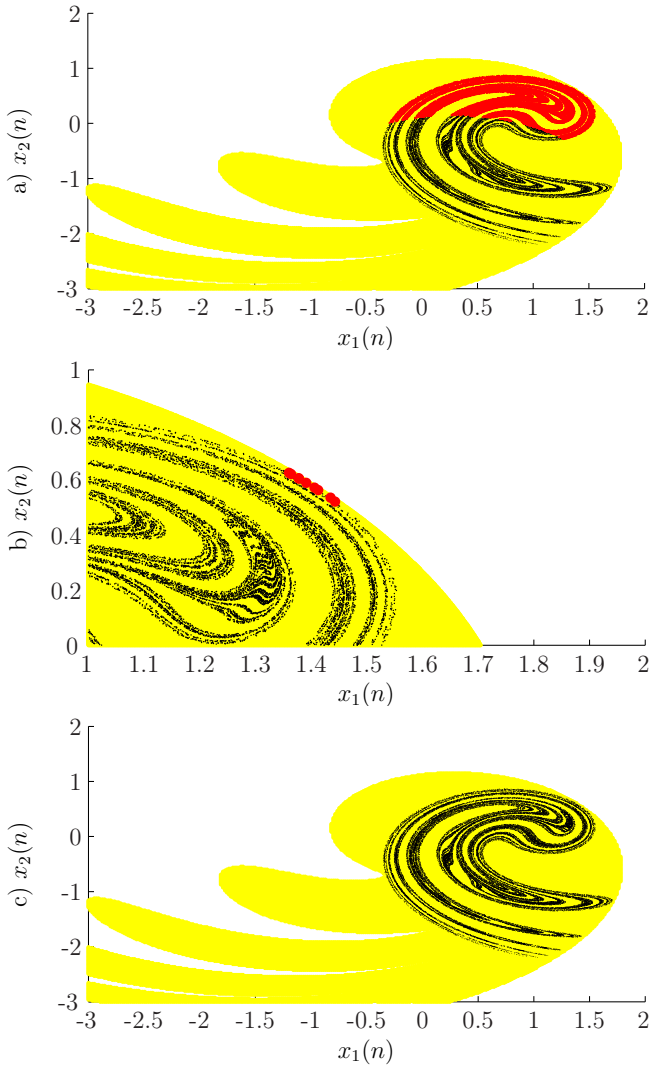

Figure 7: Phase space ($x_1(n)$ by $x_2(n)$), indicating the points that would lead the orbit to converge to the fixed point if a "-1" bit were encoded using (21) with (a) $\gamma = 1$, (b)$\gamma = 10^{-2}$, and (c) $\gamma = 10^{-3}$; Ikeda map with parameters as (20).

180 As a way to access the chaotic nature of the transmitted signals, we can calculate the major LE of the orbits of (14)-(15), using $s(n)$ as in (21) in the place of $x_2(n)$. For this, we used the usual Jacobian method as described in

Appendix A and considered $m(n)$ as a time varying parameter. The substitution of $x_2(n)$ by $s(n)$ can be seen as a perturbation of the original orbit and it still tends to one of the attractors of the Ikeda map: the fixed point with $h_1 \approx -0.11$ or the strange attractor with $h_1 = 0.51$. Assuming (21) as encoding function, Figure 8 shows the Lyapunov exponent obtained numerically as a function of γ for random initial conditions, equally probable symbols, a transitory of 10^6 samples and 10^6 samples used in the h_1 calculation. The resulting curve clearly agree with Figure 7. For γ lower than approximately 0.8×10^{-2} the transmitted signal is in fact chaotic.

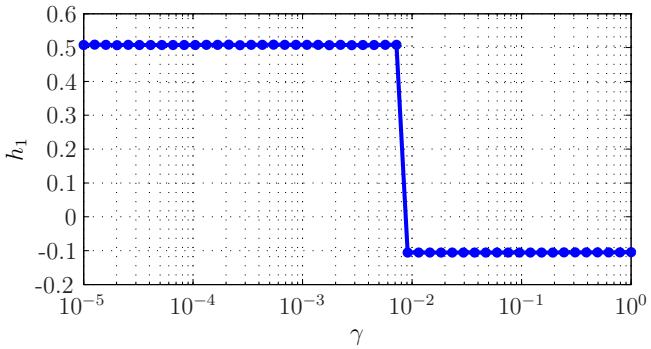

Figure 8: Maximum Lyapunov exponent h_1 as a function of γ of (21) for equiprobable messages.

5. Conclusion

Many works in the literature present chaos-based communication schemes. However, they seldom worry if the transmitted signals are in fact chaotic. In this paper, we numerically analyzed the chaotic nature of the transmitted signals of a system that employs the Ikeda map. It is shown that depending on the encoding function, the generated signals can cease to be chaotic, although remaining aperiodic due to the random nature of the message itself. In such cases, the sensitive dependence on initial conditions, fundamental property for employing chaotic signals in Telecommunications, disappears. The same issue can arise in many other maps where two different attractors coexist. In these cases,

to verify the sensitive dependence on initial conditions, the numerical analysis presented here can be straightforwardly extended by calculating the major LE of the orbits using the Jacobian method and considering $m(n)$ as a time varying parameter. As a main conclusion of this paper, we state that in proposing a chaos-based communication system, it is very relevant to study the dynamics of the underlying chaotic system and not just count on the aperiodicity of the transmitted signals.

A. Lyapunov Exponents

The LE are classically defined as the mean divergence (or convergence) rate of initially close trajectories, which can be numerically computed by means of the classical Jacobian method [14].

The Jacobian method consists in monitoring the expanding or contracting effects associated to the application of the Jacobian of the map on linearly independent vectors with unitary norm that span all space phase directions (vector basis). Once a initial basis is chosen, the Jacobian should be applied to the vectors of this basis and an orthonormalization provided by the Gram-Schmidt procedure should be made. The LE are computed as the average of the natural logarithms of the norm of the resulting vectors along the N iterations of the map. The whole computation process can be summarized in the following steps:

For each point $\mathbf{x}$ of the trajectory do:

1. Compute the Jacobian $\mathbf{J}(\mathbf{x})$ of the map on that point;
2. Apply the Jacobian to orthogonal and linearly independent set of vectors $\mathbf{W} = [\mathbf{w}_1\ \mathbf{w}_2\ ...\ \mathbf{w}_k]$, in order to obtain $\mathbf{Z} = \mathbf{JW}$. For the first iteration, $\mathbf{W}$ can be set as the identity matrix $\mathbf{I}_K$, being K the order of the map;
3. Apply the Gram-Schmidt procedure on $\mathbf{Z} = [\mathbf{z}_1\ \mathbf{z}_2\ ...\ \mathbf{z}_k]$ to obtain a numerically corrected set of vectors $\mathbf{V} = [\mathbf{v}_1\ \mathbf{v}_2\ ...\ \mathbf{v}_k]$ and their normalized versions $\mathbf{U} = [\mathbf{u}_1\ \mathbf{u}_2\ ...\ \mathbf{u}_k]$, where $\mathbf{u}_i = \frac{\mathbf{v}_i}{\|\mathbf{v}_i\|}$ for $i = 1, 2, \cdots, K$;
4. Compute the norm of the vectors $\mathbf{v}_i$, i.e., $r_i = \|\mathbf{v}_i\|$, with $i = 1, 2, \cdots, K$;

5. Update the orthogonal, normalized and linearly independent set of vector $\mathbf{W}$ as $\mathbf{W} \leftarrow \mathbf{U}$ for the next iteration of the algorithm, i.e., for the next point in the trajectory;

Finally, the Lyapunov exponent h_i for each direction $i = 1, 2, \cdots, K$ can be obtained by

$$h_i = \lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} \ln \|r_i(k)\|. \tag{22}$$

In practice, N is chosen sufficiently large. For instance, in our simulations, we considered $N = 10^6$.

The Gram-Schmidt procedure is required to avoid numerical problems, for instance, the collapse of the Jacobian matrix into a single (most expansive) direction and also ensure orthogonality to the referential vectors ($\mathbf{W}$) to which the Jacobian is applied.

In the master system considered here, there is a random binary message $m(n)$ that affects the dynamical system. In order to numerically evaluate the LE, we employed the computation process described above, considering $m(n)$ as a time variant parameter.

Acknowledgments

This work was partly supported by FAPESP under Grants 2012/24835-1 and 2014/04864-2 and by CNPq under Grants 302423/2011-7, 311575/2013-7, and 479901/2013-9.

References

[1] S. H. Strogatz, Nonlinear Dynamics and Chaos: with Applications to Physics, Biology, Chemistry and Engineering, Perseus Books Group, 2001.

[2] L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (8) (1990) 821–824.

[3] E. Ott, C. Grebogi, J. A. Yorke, Controlling chaos, Phys. Rev. Lett. 64 (1990) 1196–1199.

[4] U. Feldmann, M. Hasler, W. Schwarz, Communication by chaotic signals: the inverse system approach, in: Proc. of IEEE Int. Symp. Circuits and Systems (ISCAS'1995), Seattle, USA, 1995, pp. 680–683.

[5] M. P. Kennedy, G. Setti, R. Rovatti (Eds.), Chaotic Electronics in Telecommunications, CRC Press, Inc., Boca Raton, FL, USA, 2000.

[6] M. P. Kennedy, G. Kolumban, Digital communications using chaos, Signal Processing 80 (7) (2000) 1307–1320.

[7] S. Tsekeridou, V. Solachidis, N. Nikolaidis, A. Nikolaidis, A. Tefas, I. Pitas, Statistical analysis of a watermarking system based on Bernoulli chaotic sequences, Signal Processing 81 (6) (2001) 1273–1293.

[8] M. Hasler, G. Mazzini, M. Ogorzalek, R. Rovatti, G. Setti, Scanning the special issue - special issue on applications of nonlinear dynamics to electronic and information engineering, Proceedings of the IEEE 90 (5) (2002) 631–640.

[9] F. C. M. Lau, C. K. Tse, Chaos-based digital communication systems, Springer, Berlin, 2003.

[10] M. Eisencraft, R. R. F. Attux, R. Suyama (Eds.), Chaotic Signals in Digital Communications, CRC Press, Inc., 2013.

[11] T. Endo, L. O. Chua, Chaos from phase-locked loops, IEEE Transactions on Circuits and Systems 35 (8) (1988) 987–1003.

[12] M. S. Tavazoei, M. Haeri, Chaos in the apfm nonlinear adaptive filter, Signal Processing 89 (5) (2009) 697–702.

[13] L. H. A. Monteiro, A. C. Lisboa, M. Eisencraft, Route to chaos in a third-order phase-locked loop network, Signal Processing 89 (8) (2009) 1678–1682.

[14] K. T. Alligood, T. Sauer, J. A. Yorke, Chaos: An Introduction to Dynamical Systems, Textbooks in Mathematical Sciences, Springer, 1997.

[15] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, K. A. Shore, Chaos-based communications at high bit rates using commercial fibre-optic links, Nature 438 (7066) (2005) 343–346.

[16] C. W. Wu, L. O. Chua, A simple way to synchronize chaotic systems with applications to secure communication systems, International Journal of Bifurcation and Chaos 3 (6) (1993) 1619–1627.

[17] R. Candido, M. T. M. Silva, M. Eisencraft, Channel equalization for chaotic communications systems, in: M. Eisencraft, R. Attux, R. Suyama (Eds.), Chaotic Signals in Digital Communications, CRC Press, Inc., 2013, pp. 239–263.

[18] R. Candido, M. Eisencraft, M. T. M. Silva, Channel equalization for synchronization of chaotic maps, Digital Signal Processing 33, (2014) 42–49.

[19] R. Candido, M. Eisencraft, M. T. M. Silva, Channel equalization for synchonization of Ikeda maps, in: Proc. of 21st European Signal Processing Conference (EUSIPCO'2013), Marrakesh, Marocco, 2013.

[20] K. Ikeda, Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system, Optics Communications 30 (2) (1979) 257–261.

[21] M. Eisencraft, R. D. Fanganiello, L. A. Baccala, Synchronization of discrete-time chaotic systems in bandlimited channels, Mathematical Problems in Engineering 2009.

[22] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares, C. S. Zhou, The synchronization of chaotic systems, Physics Reports 366 (2002) 1–101.

[23] R. P. Agarwal, Difference equations and inequalities, Vol. 155 of Monographs and Textbooks in Pure and Applied Mathematics, Marcel Dekker Inc., New York, 1992, theory, methods, and applications.

[24] M. Hénon, A two-dimensional mapping with a strange attractor, Communications in Mathematical Physics 50 (1976) 69–77.

[25] W. Rugh, Linear System Theory, Prentice-Hall Information & System Sciences Series, Prentice Hall, 1996.