

A new encoding and switching scheme for chaos-based communication

Renato Candido · Magno T. M. Silva ·
Marcio Eisencraft

Received: date / Accepted: date

Abstract Many communication systems based on the synchronization of chaotic systems have been proposed as an alternative spread spectrum modulation that improves the level of privacy in data transmission. However, due to the lack of robustness of complete chaotic synchronization, even minor channel impairments are enough to hinder communication. In this paper, we propose a communication system that includes an adaptive equalizer and a switching scheme to alter between a chaos-based modulation and a conventional one, depending on the communication channel conditions. Simulation results show that the switching and equalization algorithms can successfully recover the transmitted sequence in different nonideal scenarios.

Keywords Analysis and Control of Nonlinear Dynamical Systems with Practical Applications · Chaos and Global Nonlinear Dynamics · Synchronization in Nonlinear Systems.

1 Introduction

In a digital chaos-based communication system (CBCS), each bit of information is transmitted using a different fragment of a chaotic signal [1–3]. Thus, it differs fundamentally from the conventional digital communication systems,

This work was partly supported by CNPq under Grants 304275/2014-0, 479901/2013-9, and 309275/2016-4.

Renato Candido
E-mail: renatocan@lps.usp.br

Magno T. M. Silva
E-mail: magno@lps.usp.br

Marcio Eisencraft
E-mail: marcio@lcs.poli.usp.br
University of São Paulo, São Paulo, Brazil

where each symbol is associated with a constant and predefined waveform. Although CBCSs may have interesting features, like improvement in security [4, 5], they also pose practical challenges since the conventional optimal receiver is not directly available [6].

CBCSs have been studied for at least 25 years [7, 8]. Many interesting and innovative communication schemes based on chaos synchronization were proposed [2, 4, 9] exploring the properties of chaotic signals, i.e. aperiodicity and sensitive dependence on initial conditions (SDIC) [10]. However, they seldom surpassed the frontier between theoretical or laboratory setup to practical or commercial environments [5]. This mainly occurs due to the sensitivity of the chaotic synchronization to channel imperfections [11, 12].

A particularly interesting discrete-time CBCS was proposed in [13]. It is based on the one by Wu and Chua [14], in which the message is fed back into the chaotic signal generator (CSG). It can be considered a simplified model of the optical system implemented in practice by Argyris *et al.* [5]. It was shown in [13] that under some design conditions, the message is perfectly recovered in an ideal channel. However, this CBCS presents poor performance in terms of bit error rate when channel imperfections are present. Besides, there is no guarantee that the transmitted signals are still chaotic.

In [15], we proposed a channel equalization scheme for this CBCS considering the Ikeda map [16] as CSG and the product between message and chaotic signal as encoding. Despite the reasonable performance in different channels, the question whether the transmitted signals were truly chaotic was not tackled. In fact, we have shown afterwards that the CBCS presented in [15] does not always produce chaotic signals [17]. In [18], instead of using the Ikeda map, we proposed another CBCS using the Hénon map [19] and the same encoding. In this case, the transmitted signals are easily shown to be chaotic. However, the performance of this system is still far from that of a conventional system without chaos.

In order to obtain better bit error rates than before, we propose two innovations:

- a) a new encoding and corresponding equalization scheme for the CBCS of [18]. This encoding ensures the generation of chaotic signals for a range of parameters and presents higher immunity to intersymbol interference (ISI) and noise, when compared to the encoding of [18], thus providing lower bit error rates for the same convergence rate.
- b) inspired by many conventional protocols, like IEEE 802.11 (Wi-Fi) [20], that uses modulation and coding techniques that can adapt to the channel state, we propose an algorithm to switch between chaos-based communication and conventional. The switching is triggered based on a threshold applied to the mean square error.

The paper is organized as follows. In Sec. 2, we review the CBCS of [18]. In Sec. 3, the new encoding function is presented, followed by the equalization algorithm in Sec. 4. In Sec. 5, we present the algorithm to switch between conventional and chaos-based communications. Sec. 6 contains some numerical

simulations in different scenarios. Finally, we draft conclusions and perspectives in Sec. 7.

2 Problem Formulation

Figure 1 shows the CBCS under consideration [15, 18]. In the scheme, which is a discrete-time lowpass equivalent for the communication system, a binary message $m(n) \in \{-1, +1\}$ is encoded by using the first component of the master state vector $\mathbf{x}(n)$, via a encoding function $s(n) = c(x_1(n), m(n))$, so that $m(n)$ can be recovered using the inverse function with respect to $m(n)$, i.e., $m(n) = c^{-1}(x_1(n), s(n))$. Then, the signal $s(n)$ is fed back into the CSG and transmitted through a communication channel, whose model is constituted by a transfer function $H(z)$ and additive white Gaussian noise (AWGN). We assume an M -tap adaptive equalizer, with input regressor vector $\mathbf{r}(n)$ and output $\hat{s}(n) = \mathbf{r}^T(n)\mathbf{w}(n-1)$, where $(\cdot)^T$ indicates transposition and $\mathbf{w}(n-1)$ is the equalizer weight vector. The equalizer must mitigate the ISI introduced by the channel and recover the encoded signal $s(n)$ with an unavoidable delay of Δ samples.

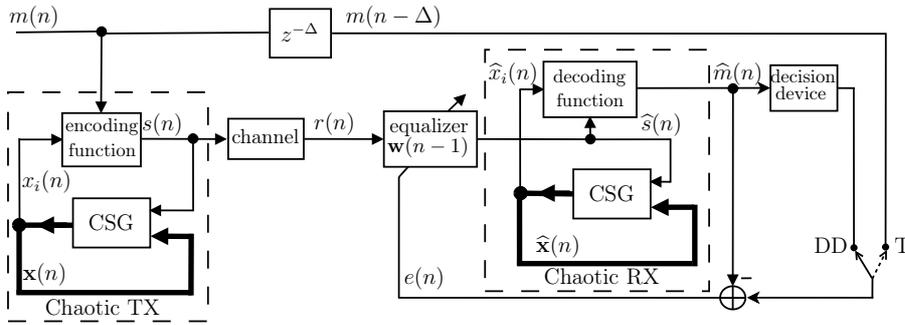


Fig. 1 Chaos-based communication system with an equalizer.

If transmitter and receiver identically synchronize [21], i.e., if $\hat{\mathbf{x}}(n) \rightarrow \mathbf{x}(n)$, then using the output of the equalizer and the estimate of $x_1(n)$, $m(n)$ can be decoded via

$$\hat{m}(n) \triangleq c^{-1}(\hat{x}_1(n), \hat{s}(n)) \rightarrow m(n), \quad (1)$$

where $\hat{x}_1(n)$ is the first component of the slave state vector $\hat{\mathbf{x}}(n)$. Thus, the estimation error $e(n) = m(n - \Delta) - \hat{m}(n)$ can be used as an equalization criterion. Once identical synchronization between master-slave is obtained, $m(n)$ can be used to transmit information between the two systems, being $\hat{m}(n)$ the decoded binary message. We assume that there is a training sequence $\{m(n - \Delta)\}$, known in advance at the receiver. In this case, the equalizer works in the *training* (T) mode and updates its coefficients in a supervised manner, using the estimation error in conjunction with an adaptive algorithm. If we

intend to transmit information using $m(n)$, the receiver will not have access to $\{m(n - \Delta)\}$ and this sequence will be replaced by the output of the decision device [6,22]. In this case, the equalizer works in the so-called *decision-directed* (DD) *mode*.

In this paper, the Hénon map [19] is used in both CSGs of Figure 1. Therefore, the equations governing the global dynamical system can be written as

$$\mathbf{x}(n+1) = \mathbf{A}\mathbf{x}(n) + \mathbf{b} + \mathbf{f}(s(n)), \quad (2)$$

$$\hat{\mathbf{x}}(n+1) = \mathbf{A}\hat{\mathbf{x}}(n) + \mathbf{b} + \mathbf{f}(\hat{s}(n)), \quad (3)$$

where $\mathbf{x}(n) \triangleq [x_1(n) \ x_2(n)]^T$, $\hat{\mathbf{x}}(n) \triangleq [\hat{x}_1(n) \ \hat{x}_2(n)]^T$,

$$\mathbf{A} = \begin{bmatrix} 0 & 1 \\ \beta & 0 \end{bmatrix}, \mathbf{b} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{f}(s(n)) = \begin{bmatrix} -\alpha s^2(n) \\ 0 \end{bmatrix}, \quad (4)$$

being α and β real constant parameters of the map.

In [13] it was shown that, under ideal channel conditions, i.e., when $r(n) \equiv s(n)$ and the equalizer is an identity system, identical synchronization between master and slave is obtained if all the eigenvalues of \mathbf{A} are inside the unit circle. Since the eigenvalues of \mathbf{A} are $\pm\sqrt{\beta}$, we conclude that for $|\beta| < 1$, master and slave identically synchronize under ideal conditions. Therefore, from (1), $\hat{m}(n) \rightarrow m(n)$.

3 Message encoding

In [15,18] the product

$$s(n) = x_1(n)m(n) \quad (5)$$

was employed as an encoding function. However, the obtained performance in nonideal channels was far from that of a conventional modulation. Therefore, it is of interest to find other encodings that could provide better performance and generate chaotic signals.

In [23] the linear combination

$$s(n) = (1 - \eta)x_1(n) + \eta m(n), \quad (6)$$

was proposed where $0 < \eta \leq 1$ is a parameter that controls the strength of the chaotic signal $x_1(n)$ with respect to the message $m(n)$. It was shown that the chaos synchronization can be more robust for higher values of η . However, it was not checked if the transmitted signals were in fact chaotic.

To tackle this point, consider a more general form of (6), i.e.,

$$s(n) = \eta_1 x_1(n) + \eta_2 m(n) \quad (7)$$

where $\{\eta_1, \eta_2\} \subset [0, 1]$. Figure 2 shows the maximum Lyapunov exponent λ [10] obtained in the transmitter as a function of η_1 and η_2 considering a

random equiprobable binary $m(n) \in \{-1, 1\}$. This Lyapunov exponent was obtained using the method described in Sec. 5.2 of [10], considering $m(n)$ as a variable parameter. The region where λ is negative, i.e., the generated signals are not chaotic, is shown in gray. The colored region indicates the area where the generated signals are chaotic ($\lambda > 0$, i.e., the signals present SDIC). For the values of η_1 and η_2 in the white area of the figure, the transmitter diverged and it was not possible to calculate λ . The dashed line $\eta_1 + \eta_2 = 1$ represents the parameter space associated with the encoding (6), with $\eta = \eta_2$. Therefore, (6) generates chaotic signals only when η is small and $s(n) \approx x_1(n)$. However, in this case, the CBCS does not present a reasonable performance under AWGN [23].

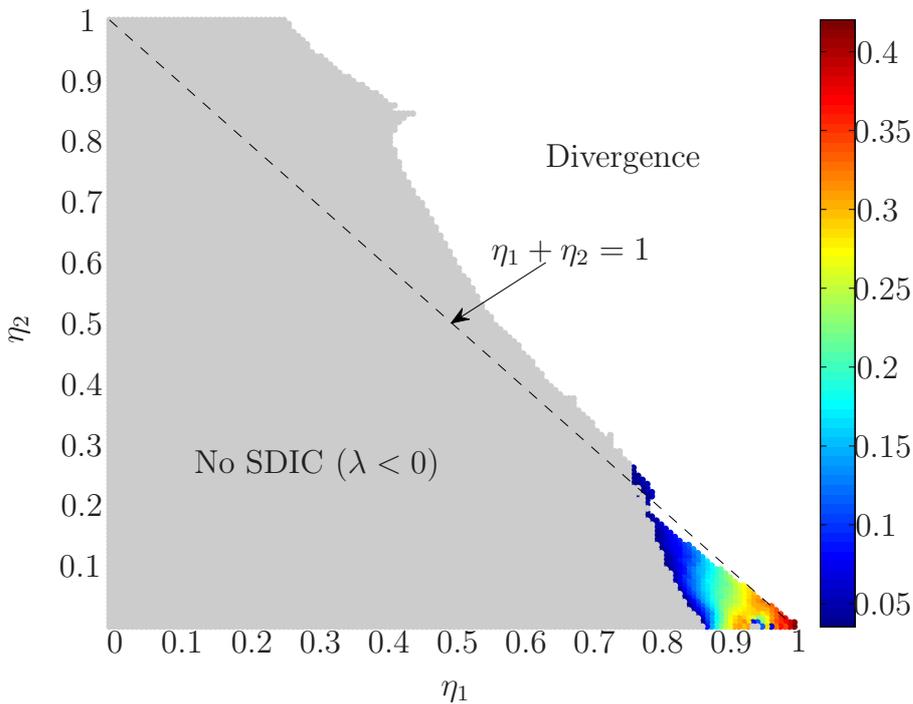


Fig. 2 Maximum Lyapunov exponent λ obtained when using (7) as a function of η_1 and η_2 . The gray area indicates a negative value. The white area indicates divergence of the transmitter.

As a way to increase the parameter space where chaotic signals are generated, we propose the encoding function

$$s(n) = \eta_1 x_1(n) - \eta_2 [m(n) + 1] \text{sign}[\eta_1 x_1(n)], \quad (8)$$

where $\text{sign}[\cdot]$ is the signal function. The idea behind (8) is to decrease the disturbance on $x_1(n)$ caused by the message. In this case, if $m(n) = -1$,

$s(n) = \eta_1 x_1(n)$ and if $m(n) = 1$ a constant with signal opposite to $x_1(n)$ is added to it. The corresponding decoding function is given by

$$\hat{m}(n) = \frac{\eta_1 \hat{x}_1(n) - \hat{s}(n)}{\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]} - 1. \quad (9)$$

Figure 3 is analogous to Figure 2 for the encoding (8). As can be seen, using (8) it is possible to obtain a larger set of parameter η_1 and η_2 that generates chaotic signals. Besides, as will be shown in Sec. 6, it is possible to find values for η_1 and η_2 in the colored region that give good equalization performance. Specifically, we consider $\eta_1 = 0.9$ and $\eta_2 = 0.3$.

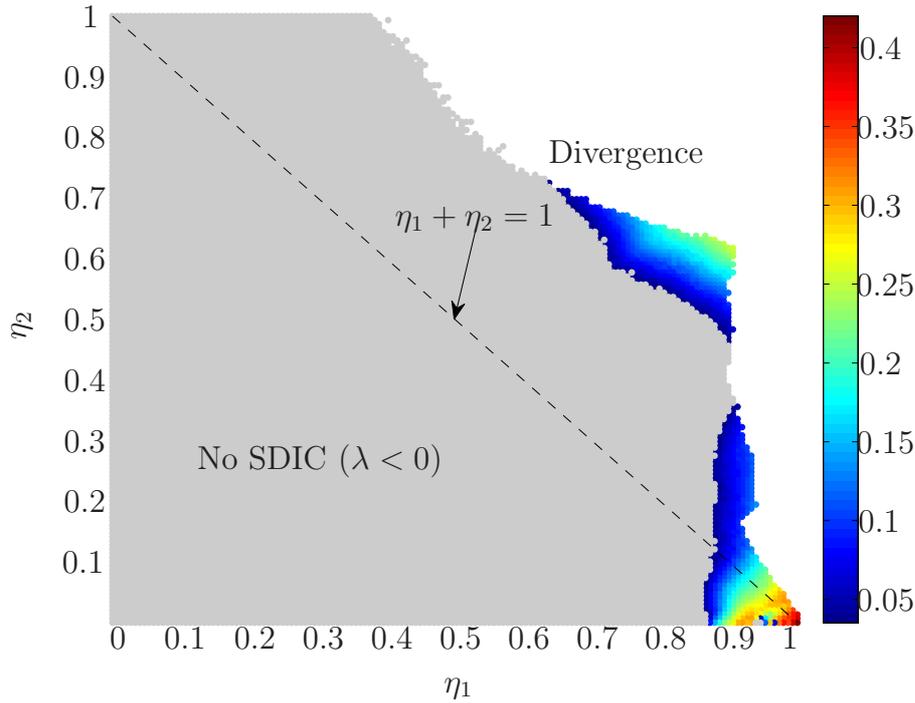


Fig. 3 Maximum Lyapunov exponent λ obtained when using (8) as a function of η_1 and η_2 .

4 Equalization Algorithm

To obtain a stochastic gradient algorithm to adapt the equalizer in the scheme of Figure 1, we define the instantaneous cost-function

$$\hat{J}(n) = e^2(n) = [m(n - \Delta) - \hat{m}(n)]^2.$$

Computing the gradient of $\hat{J}(n)$ with respect to the coefficient vector $\mathbf{w}(n-1)$, we obtain

$$\nabla_{\mathbf{w}} \hat{J}(n) = 2e(n) \frac{\partial e(n)}{\partial \mathbf{w}(n-1)} = -2e(n) \frac{\partial \hat{m}(n)}{\partial \mathbf{w}(n-1)}. \quad (10)$$

Since the output of the equalizer is $\hat{s}(n) = \mathbf{r}^T(n)\mathbf{w}(n-1)$, the recovery message (9) can be rewritten as

$$\hat{m}(n) = \frac{\eta_1 \hat{x}_1(n) - \mathbf{r}^T(n)\mathbf{w}(n-1)}{\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]} - 1. \quad (11)$$

Assuming that $\hat{x}_1(n)$ does not depend on $\mathbf{w}(n-1)$, we get¹

$$\nabla_{\mathbf{w}} \hat{J}(n) = 2 \frac{e(n)}{\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]} \mathbf{r}(n). \quad (12)$$

Thus, the update equation of the chaotic² least mean-square (cLMS₊) algorithm for the encoding (8) is given by

$$\mathbf{w}(n) = \mathbf{w}(n-1) - \mu \frac{e(n)}{\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]} \mathbf{r}(n). \quad (13)$$

To obtain a normalized version of cLMS₊, we first define the *a posteriori* error as

$$e_p(n) = m(n - \Delta) - \frac{\eta_1 \hat{x}_1(n) - \mathbf{r}^T(n)\mathbf{w}(n)}{\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]} + 1. \quad (14)$$

Using (13), $e_p(n)$ can be rewritten as

$$e_p(n) = e(n) \left[1 - \mu(n) \frac{\|\mathbf{r}(n)\|^2}{\eta_2^2(n)} \right]. \quad (15)$$

To enforce $e_p(n) = 0$ at each iteration n , we must select

$$\mu(n) = \frac{\eta_2^2(n)}{\|\mathbf{r}(n)\|^2}. \quad (16)$$

Introducing a fixed step-size $\tilde{\mu}$ to control the rate of convergence and a regularization factor δ to prevent division by zero in $\mu(n)$, and replacing the resulting

¹ In fact, $\hat{x}_1(n)$ depends on $\mathbf{w}(n-1)$. However, considering this dependence, we need to use some other assumptions to derive the equalization algorithm. Furthermore, the resulting algorithm is more complicated and the achievable performance is similar to that of the algorithm derived here.

² We use the term *chaotic* for the algorithms derived here only for distinguishing them from the original versions of LMS and normalized LMS (NLMS) algorithms (see, e.g., [22]). The use of this term does not imply a chaotic behavior of the algorithms. The subscript + is used here to distinguish this algorithm from that of [18], which uses the product as encoding function and thus, denoted with the subscript \times .

step size in (13), we obtain the update equation of the chaotic normalized LMS (cNLMS₊) algorithm, i.e.,

$$\mathbf{w}(n) = \mathbf{w}(n-1) - \frac{\tilde{\mu}\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]}{\delta + \|\mathbf{r}(n)\|^2} e(n) \mathbf{r}(n). \quad (17)$$

We should notice that an error in the sign of $\eta_1 \hat{x}_1(n)$ only causes an error in the decoded message when $m(n) = 1$. In this case, replacing $\hat{m}(n) = 1$ in (9), we obtain

$$\text{sign}[\eta_1 \hat{x}_1(n)] = \frac{\eta_1 \hat{x}_1(n) - \hat{s}(n)}{2\eta_2}. \quad (18)$$

Thus, replacing (18) with the opposite sign in (9), the recovered message would be

$$\hat{m}(n) = \frac{-2[\eta_1 \hat{x}_1(n) - \hat{s}(n)]}{\eta_1 \hat{x}_1(n) - \hat{s}(n)} - 1 = -3. \quad (19)$$

Therefore, we can identify when an error occurs in the estimate of $\text{sign}[\eta_1 \hat{x}_1(n)]$ by using the estimate of the message, which should be equal to 1, but is decoded as -3 . To circumvent this problem, when $\hat{m}(n)$ is decoded in the interval $-3.5 < \hat{m}(n) < -2.5$, we make $\hat{m}(n) \leftarrow \hat{m}(n) + 4$.

In order to ensure the stability of the algorithm and to avoid wrong estimates when $\hat{x}_1(n)$ is too large, we introduce a bound for $\hat{x}_1(n)$, i.e., if $|\hat{x}_1(n)| > X$, we simply make $\hat{x}_1(n) \leftarrow X \text{sign}[\hat{x}_1(n)]$, where X is a positive constant. We do not observe performance degradation in different simulation scenarios, when we used $X = 100$. The proposed algorithm is summarized in Table 1.

4.1 Stability conditions

Using (11), the update equation of cNLMS₊ can be rewritten as

$$\begin{aligned} \mathbf{w}(n) = & \left[\mathbf{I} - \frac{\tilde{\mu}}{\delta + \|\mathbf{r}(n)\|^2} \mathbf{r}(n) \mathbf{r}^T(n) \right] \mathbf{w}(n-1) \\ & - \tilde{\mu} \eta_2 \text{sign}[\eta_1 \hat{x}_1(n)] m(n - \Delta) \frac{\mathbf{r}(n)}{\delta + \|\mathbf{r}(n)\|^2} \\ & + \tilde{\mu} \eta_1 \hat{x}_1(n) \frac{\mathbf{r}(n)}{\delta + \|\mathbf{r}(n)\|^2} \\ & - \tilde{\mu} \eta_2 \text{sign}[\eta_1 \hat{x}_1(n)] \frac{\mathbf{r}(n)}{\delta + \|\mathbf{r}(n)\|^2}. \end{aligned} \quad (20)$$

where \mathbf{I} is the identity matrix with dimensions $M \times M$. The matrix between brackets has $M - 1$ eigenvalues equal to one and one eigenvalue equal to [22]

$$\lambda_1 = 1 - \tilde{\mu} \frac{\mathbf{r}^T(n) \mathbf{r}(n)}{\delta + \|\mathbf{r}(n)\|^2}.$$

Table 1 Summary of cNLMS₊ for the Hénon map.

Initialize the algorithm by setting: $\mathbf{w}(-1) = \mathbf{0}$, $\hat{\mathbf{x}}(0) = [0, 1 \ -0, 1]^T$ $\mathbf{A} = \begin{bmatrix} 0 & 1 \\ \beta & 0 \end{bmatrix}$, $\mathbf{b} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ α, β : parameters of Hénon map; $0 < \tilde{\mu} < 2$ δ : small positive constant; X : large positive constant η_1 e η_2 : parameters of the decoding function
For $n = 0, 1, 2, 3 \dots$, compute: $\hat{s}(n) = \mathbf{r}^T(n)\mathbf{w}(n-1)$ if $ \hat{x}_1(n) > X$ $\hat{x}_1(n) \leftarrow X \text{sign}[\hat{x}_1(n)]$ end $\hat{m}(n) = \frac{\eta_1 \hat{x}_1(n) - \hat{s}(n)}{\eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]} - 1$ $e(n) = m(n - \Delta) - \hat{m}(n)$ if $-3.5 < \hat{m}(n) < -2.5$ $\hat{m}(n) \leftarrow \hat{m}(n) + 4$ end $\mathbf{w}(n) = \mathbf{w}(n-1) - \frac{\tilde{\mu} \eta_2 \text{sign}[\eta_1 \hat{x}_1(n)]}{\delta + \ \mathbf{r}(n)\ ^2} e(n) \mathbf{r}(n)$ $\hat{\mathbf{x}}(n+1) = \mathbf{A} \hat{\mathbf{x}}(n) + \mathbf{b} + \begin{bmatrix} -\alpha \hat{s}^2(n) \\ 0 \end{bmatrix}$ end

Noticing that

$$0 \leq \frac{\mathbf{r}^T(n)\mathbf{r}(n)}{\delta + \|\mathbf{r}(n)\|^2} < 1,$$

and for $\|\mathbf{r}(n)\|^2 \gg \delta$, $\mathbf{r}^T(n)\mathbf{r}(n)/(\delta + \|\mathbf{r}(n)\|^2) \approx 1$, in order to ensure $|\lambda_1| < 1$, we must choose $\tilde{\mu}$ in the interval

$$0 < \tilde{\mu} < 2. \quad (21)$$

The norms of the second, third, and fourth terms on the right side of (20) are bounded, i.e.,

$$0 \leq \tilde{\mu} \eta_2 |\text{sign}[\eta_1 \hat{x}_1(n)]| |m(n - \Delta)| \frac{\|\mathbf{r}(n)\|}{\delta + \|\mathbf{r}(n)\|^2} \leq \tilde{\mu} \eta_2 \frac{\sqrt{\delta}}{2\delta} < \infty, \quad (22)$$

$$0 \leq \tilde{\mu} \eta_1 |\hat{x}_1(n)| \frac{\|\mathbf{r}(n)\|}{\delta + \|\mathbf{r}(n)\|^2} \leq \tilde{\mu} \eta_1 X \frac{\sqrt{\delta}}{2\delta} < \infty, \quad (23)$$

and

$$0 \leq \tilde{\mu} \eta_2 |\text{sign}[\eta_1 \hat{x}_1(n)]| \frac{\|\mathbf{r}(n)\|}{\delta + \|\mathbf{r}(n)\|^2} \leq \tilde{\mu} \eta_2 \frac{\sqrt{\delta}}{2\delta} < \infty. \quad (24)$$

Therefore, using (deterministic) exponential stability results for the LMS algorithm [24], we conclude that cNLMS₊ is stable in a robust sense if $\tilde{\mu}$ is chosen in the interval (21).

5 Switching Algorithm

Although the chaos-based communication systems may provide some interesting features such as security, it is well-known that they are much more sensitive to imperfections in the communication channel than conventional systems such as binary phase-shift keying (BPSK) [6, 11]. In this section, we present a scheme that allows the communication system to switch from chaos-based operation and conventional BPSK operation [6] based on the communication channel conditions.

To control the operation mode of the system, we introduce the parameters $\gamma_1(n)$ and $\gamma_2(n)$ in the encoding function (8), making

$$s(n) = \gamma_1(n) \{ \eta_1 x_1(n) - \eta_2 [m(n) + 1] \text{sign}[\eta_1 x_1(n)] \} + \gamma_2(n) m(n). \quad (25)$$

This way, when $\gamma_1(n) = 1$ and $\gamma_2(n) = 0$, (25) falls back to (8) and the system works just like the previously presented chaos-based communication system. However, when $\gamma_1(n) = 0$ and $\gamma_2(n) = 1$, $s(n) = m(n)$ and, assuming $m(n) \in \{+1, -1\}$, a BPSK system is obtained.

To decode the message considering (25) and assuming $\gamma_1(n)$ and $\gamma_2(n)$ are known at the receiver,

$$\hat{m}(n) = \frac{\gamma_1(n) \{ \eta_1 \hat{x}_1(n) - \eta_2 \text{sign}[\eta_1 \hat{x}_1(n)] \} - \hat{s}(n)}{\gamma_1(n) \eta_2 \text{sign}[\eta_1 \hat{x}_1(n)] - \gamma_2(n)}. \quad (26)$$

Following the steps presented in Section 4, it is possible to obtain the equalizer coefficient update equation, given by

$$\mathbf{w}(n) = \mathbf{w}(n-1) - \frac{\tilde{\mu} \{ \gamma_1(n) \eta_2 \text{sign}[\eta_1 \hat{x}_1(n)] - \gamma_2(n) \}}{\delta + \|\mathbf{r}(n)\|^2} e(n) \mathbf{r}(n). \quad (27)$$

As it can be noticed, when $\gamma_1(n) = 1$ and $\gamma_2(n) = 0$, (27) falls back to (17) and when $\gamma_1(n) = 0$ and $\gamma_2(n) = 1$, the conventional NLMS algorithm is obtained.

When using BPSK, to maintain the mean power of $s(n)$ equal to the power of the chaotic signal, $\gamma_2(n)$ is adjusted. Since the mean power of $s(n)$ is approximately equal to 0.415 when chaos is used ($\gamma_1(n) = 1$ and $\gamma_2(n) = 0$), considering $m(n) \in \{+1, -1\}$, it is possible to obtain the same power for BPSK using $\gamma_1(n) = 0$ and $\gamma_2(n) = \sqrt{0.415}$. This is the equivalent of a conventional BPSK system with an attenuation factor of $\gamma_2(n)$.

To make the system practical for transmitting an actual message, besides switching between the chaotic regime and BPSK, we also consider the switching between the training (T) mode and the decision-directed (DD) mode. In this way, the system may operate in four different modes, listed in Table 2.

Table 2 Operation modes of the switching algorithm.

Number	Modulation	Training or decision-directed
1	BPSK	T
2	Chaotic	T
3	Chaotic	DD
4	BPSK	DD

The overall communication system with the switching scheme is depicted in Figure 4. For each block of L samples, the switching is triggered based on thresholds applied to the estimate of the mean square error (MSE), i.e.,

$$\text{MSE}(n_0) = \frac{1}{L} \sum_{k=n_0}^{n_0+L-1} e^2(k),$$

with $n_0 = 0, L, 2L, \dots$, accordingly to the flowchart shown in Figure 5. The switching algorithm prioritize the use of the chaotic regime whenever possible and falls back to BPSK when the communication channel condition is poor.

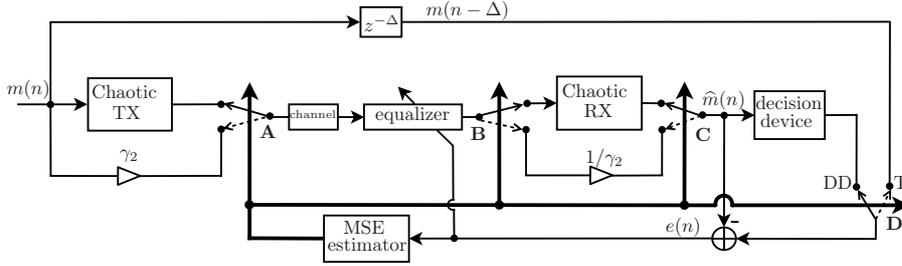


Fig. 4 Communication system with an equalizer and a switching scheme between conventional and chaos-based communication.

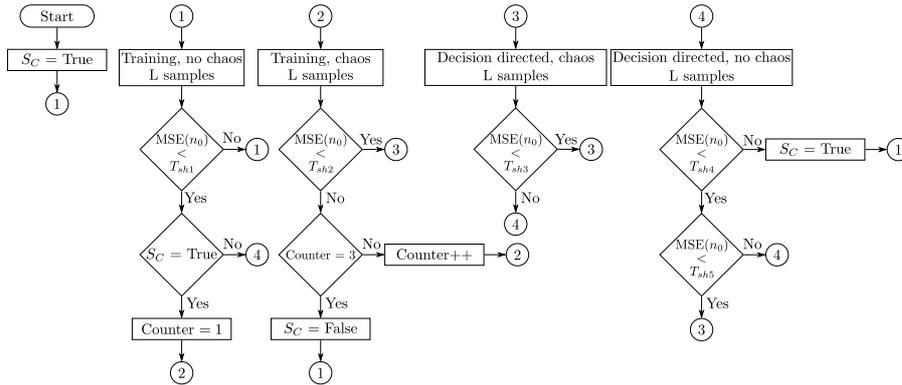


Fig. 5 Flowchart of the switching scheme between operation modes. $T_{sh1} \dots T_{sh5}$ are MSE thresholds that trigger the switching between the operation modes.

6 Numerical Simulations

In all simulations, we consider the communication system using the Hénon map with parameters $\alpha = 1.4$ and $\beta = 0.3$. The state vectors were initialized

with $\mathbf{x}(0) = \mathbf{0}$ and $\hat{\mathbf{x}}(0) = [0.1 \ -0.1]^T$, respectively. Other initializations also allow equally good results in terms of synchronization when the equalizer mitigates reasonably well the ISI. Furthermore, we assume the transmission of a binary message $m(n) \in \{-1, +1\}$ and equalizers initialized as $\mathbf{w}(-1) = \mathbf{0}$. At first, we show some numerical results to compare the scheme proposed in Section 4, (without the switching algorithm and considering only the training mode) with that of [18], where the encoding function is given by (5) and a similar NLMS algorithm, denoted here as cNLMS_\times , was used to update the equalizer.

We first assume that the encoded sequence $s(n)$ is initially transmitted through Channel 1 with transfer function

$$H_1(z) = -0.005 + 0.009z^{-1} - 0.024z^{-2} + 0.850z^{-3} \\ - 0.218z^{-4} + 0.050z^{-5} - 0.016z^{-6},$$

which is changed abruptly at $n = 100 \times 10^3$ to Channel 2 with transfer function

$$H_2(z) = -0.004 + 0.030z^{-1} - 0.104z^{-2} + 0.520z^{-3} \\ + 0.273z^{-4} - 0.074z^{-5} + 0.020z^{-6}$$

in the absence of noise [18, 25]. Figs. 6-(a) and (b) show the evolution of the coefficients through the iterations for cNLMS_\times and cNLMS_+ respectively. For both channels and both algorithms, we considered equalizers with $M = 12$ coefficients and a delay of $\Delta = 7$ samples. We have adjusted the step sizes of the cNLMS_\times and cNLMS_+ algorithms in order to obtain a convergence rate approximately equal for both algorithms. As it can be noticed, in both cases and both channels, the equalizers converge to the Wiener solution indicated by the dashed lines. In Figure 6-(c), we consider the bit error rate (BER) as a performance measure to compare the results provided by cNLMS_\times and cNLMS_+ . For each point shown in this figure, we assumed an equalizer with fixed coefficients given by the values shown in Figs. 6-(a) and (b) and measured the BER of the systems after the transmission of 10^5 samples of a binary message. We can observe that, for Channel 1, both systems, using (5) or (8) provide similar results in terms of BER after the convergence of the equalizers. However, after the abrupt channel variation (for Channel 2), the system that encodes the message using (8) performs better than the system that uses (5). This indicates that the system that uses (8) to encode the message may be more robust to ISI than the system that uses (5). Despite the interesting features of chaos-based operation, we can notice it is more susceptible to ISI than a conventional communication system, since we have a considerable level of BER even in the absence of noise. Hence, it is interesting to consider a switching scheme to allow communication even when the channel condition is poor.

Assuming the transmission of the encoded sequence through Channel 3 with transfer function

$$H_3(z) = 0.25 + z^{-1} + 0.25z^{-2}, \quad (28)$$

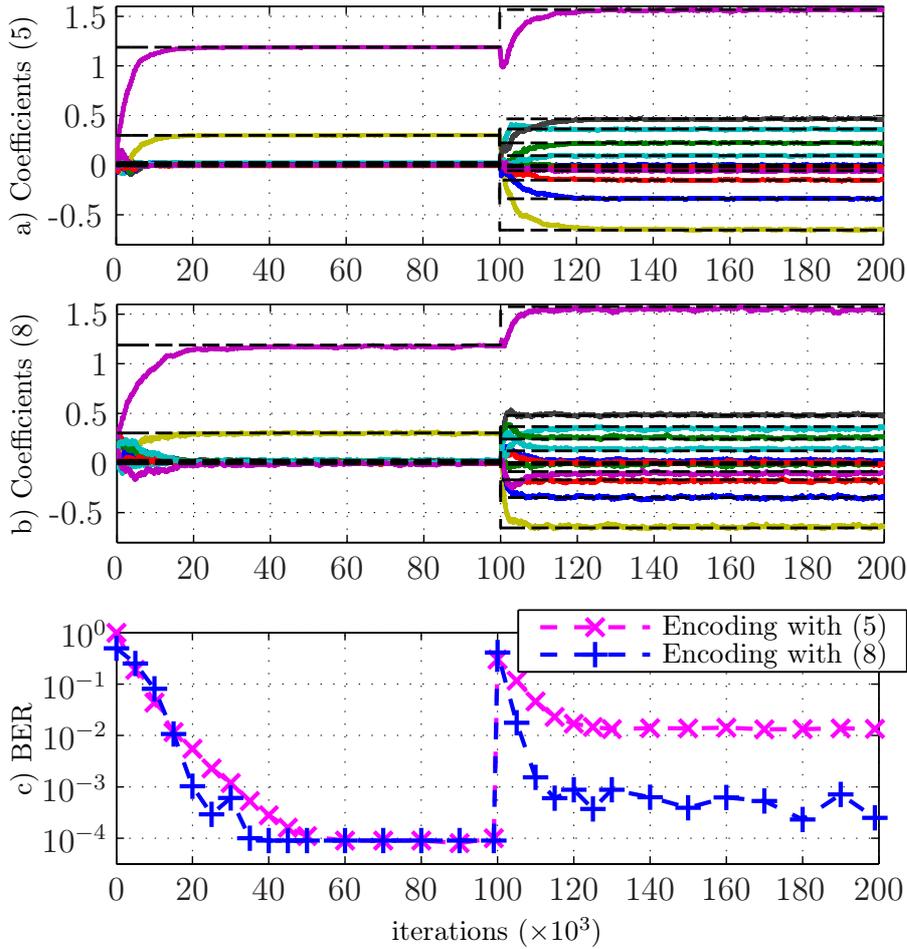


Fig. 6 Average of the $M = 12$ coefficients of (a) cNLMS_\times ($\tilde{\mu} = 0.01$, $\delta = 10^{-5}$, $\varepsilon = 0.1$, $X = 100$), (b) cNLMS_+ ($\tilde{\mu} = 0.02$, $\delta = 10^{-2}$, $\varepsilon = 0.1$, $X = 100$) and Wiener solution (dashed lines); (c) Bit error rate considering the equalizer coefficients are fixed for cNLMS_\times and cNLMS_+ ; abrupt variation from Channel 1 to Channel 2 at $n = 100 \times 10^3$ in the absence of noise.

we obtained BER curves as a function of signal-to-noise ratio (SNR), shown in Figure 7. As a performance reference to equalization in a dispersive and noisy scenario, considering that the message is encoded with (8), we included the BER curves obtained for the non-dispersive AWGN channel for the system shown in Figure 1 but without the equalizer. For comparison, we also included the curves obtained with Wiener's solution considering that the message is encoded with (5) and assuming a conventional system, without chaos. We can observe that the BER obtained by the system that uses (8) to encode the message and the cNMLS_+ algorithm is inferior than the optimal solution obtained with the system that uses (5) for SNRs from 30 dB to 60 dB. For

lower SNRs, ranging from 0 dB to 30 dB, the BER curves obtained using (8) or (5) to encode the message are similar. It is worth to notice that, for SNRs ranging from 20 dB to 60 dB, cNMLS₊ does not achieve the optimum performance, which is close to the one obtained for the non-dispersive AWGN channel. This is due to the step-size of the cNMLS₊ algorithm. It is possible to obtain results closer to the optimum solution using a smaller step-size but this would lead to a lower convergence rate.

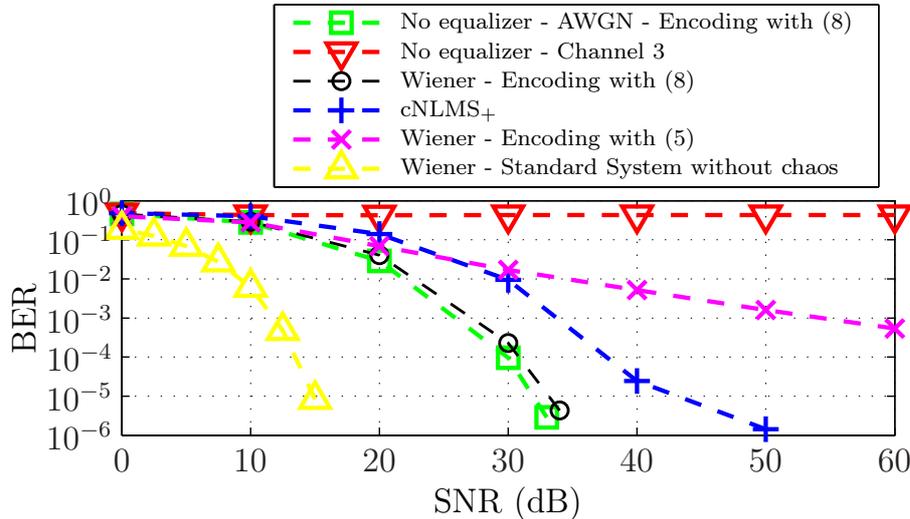


Fig. 7 Bit error rate as a function of SNR for the non-dispersive AWGN channel and for Channel 3; cNMLS₊ ($\tilde{\mu}=0.02$; $\delta=10^{-5}$), Wiener solution using (8), Wiener solution using (5) and Wiener solution for the standard system with $M = 21$; $\Delta = 11$.

Finally, we show an example to illustrate the switching scheme proposed in Section 5. We first assume that the encoded sequence $s(n)$ is initially transmitted through Channel 1, which is changed abruptly at $n = 150 \times 10^3$ to Channel 2 and changed back to Channel 1 at $n = 300 \times 10^3$, in the absence of noise [18, 25]. Figure 8 shows the errors in the recovered message (a), the squared error (b), and the operation mode of the communication system (c), according to Table 2. The switching is performed at each $L = 2000$ iterations based on the flowchart shown in Figure 5 with thresholds $T_{sh1} = -30$ dB, $T_{sh2} = -40$ dB, $T_{sh3} = -30$ dB, $T_{sh4} = -20$ dB, and $T_{sh5} = -35$ dB. For the first iterations, under Channel 1, we can observe that the system switches to chaotic modulation in decision-directed mode (number 3), after a brief transient. During this transient, there are some wrong estimations of $m(n)$ but after the switching algorithm stabilizes in State 3, the message is recovered. After the abrupt variation to Channel 2 at $n = 150 \times 10^3$, the algorithm switches to BPSK modulation in decision-directed mode (State 4), after a transient period. This is due to the fact that Channel 2 inserts more ISI than Channel 1, hindering the utilization of the chaotic modulation, as we can no-

tice by the squared error level. When the communication channel is changed back to Channel 1, at $n = 300 \times 10^3$, the algorithm switches back to chaotic modulation in decision-directed mode (State 3), after a transient period.

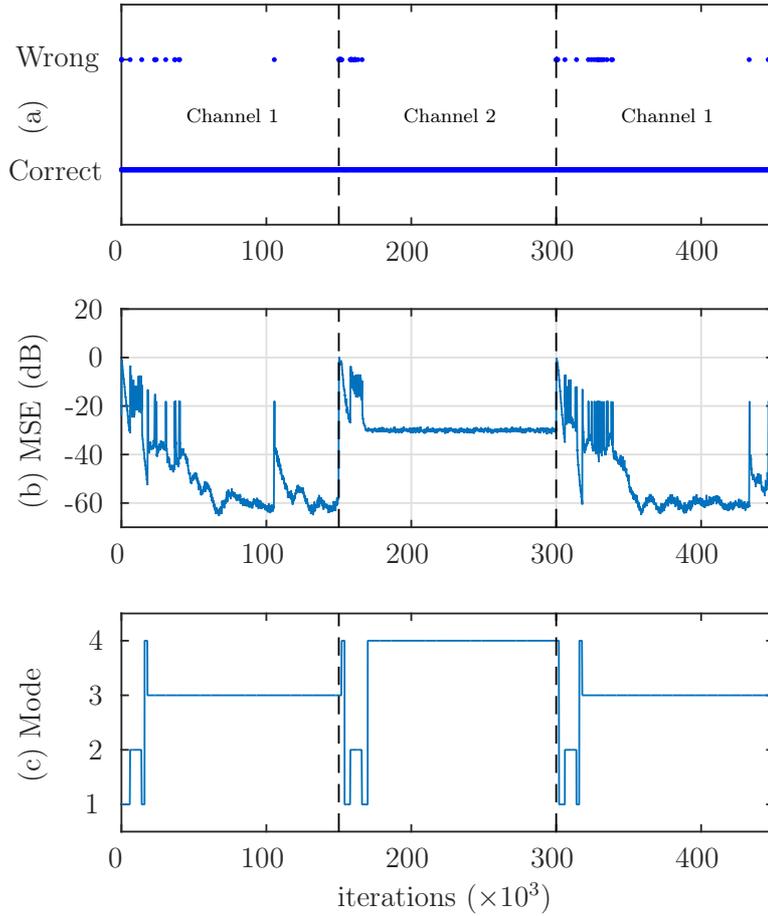


Fig. 8 (a) Errors in the recovered message, (b) squared error, and (c) operation mode according to Table 2 along iterations. Communication system using the Hénon map, cNLMS₊ ($\tilde{\mu} = 0.01$; $\delta = 10^{-2}$) and the switching scheme described in Section 5. Abrupt variation from Channel 1 to Channel 2 at $n = 150 \times 10^3$ and from Channel 2 back to Channel 1 at $n = 300 \times 10^3$; $M = 12$; $\Delta = 7$.

7 Conclusions

In this paper, we proposed a new encoding function that ensures the generation of chaotic signals and a supervised equalization scheme based on the NLMS algorithm for recovering a binary sequence in a CBCS. Moreover, we proposed an adaptive scheme that switches between the chaos-based communication system and the conventional one based on thresholds applied to the MSE. Simulations show that the proposed encoding and equalization algorithm outperforms the scheme of [18] in terms of BER for the same convergence rate and the switching scheme can successfully recover the transmitted sequence, using the CBCS or a conventional one, depending on the communication channel conditions.

References

1. G. Kolumban, M.P. Kennedy, and L.O. Chua, "The role of synchronization in digital communications using chaos. ii. chaotic modulation and chaotic synchronization," *IEEE Trans. Circuits Syst. I*, vol. 45, no. 11, pp. 1129–1140, Nov 1998.
2. M. P. Kennedy, G. Setti, and R. Rovatti, Eds., *Chaotic Electronics in Telecommunications*, CRC Press, Inc., Boca Raton, FL, USA, 2000.
3. G. Kolumbán, T. Krébesz, C. K. Tse, and F. C. M. Lau, "Basics of communications using chaos," in *Chaotic Signals in Digital Communications*, Marcio Eisencraft, Romis Attux, and Ricardo Suyama, Eds., chapter 4, pp. 111–141. CRC Press, Inc., 2013.
4. M. S. Baptista, E. E. Macau, C. Grebogi, Y. Lai, and E. Rosa, "Integrated chaotic communication scheme," *Phys. Rev. E*, vol. 62, pp. 4835–4845, Oct 2000.
5. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, 2005.
6. S. Haykin, *Communication systems*, Wiley, New York, 4th edition, 2001.
7. L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb. 1990.
8. K. M. Cuomo and A. V. Oppenheim, "Chaotic signals and systems for communications," in *Proc. IEEE Int. Conf. Acoustics, Speech, and Signal Process.*, Apr. 1993, vol. 3, pp. 137–140.
9. P. Stavroulakis, Ed., *Chaos Applications in Telecommunications*, CRC Press, Inc., Boca Raton, FL, USA, 2005.
10. K. T. Alligood, T. Sauer, and J. A. Yorke, *Chaos: An Introduction to Dynamical Systems*, Textbooks in Mathematical Sciences. Springer-Verlag, New York, 1997.
11. C. Williams, "Chaotic communications over radio channels," *IEEE Trans. Circuits Syst. I*, vol. 48, no. 12, pp. 1394–1404, Dec. 2001.
12. M. Eisencraft, R. Attux, and R. Suyama, Eds., *Chaotic Signals in Digital Communications*, CRC Press, Inc., 2013.
13. M. Eisencraft, R. D. Fanganiello, and L. A. Baccalá, "Synchronization of discrete-time chaotic systems in bandlimited channels," *Mathematical Problems in Engineering*, vol. 2009, pp. 1–12, 2009.
14. C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *International Journal of Bifurcation and Chaos*, vol. 3, no. 6, pp. 1619–1627, Dec. 1993.
15. R. Candido, M. Eisencraft, and M. T. M. Silva, "Channel equalization for synchronization of Ikeda maps," in *Proc. of 21st European Signal Processing Conference (EU-SIPCO'2013)*, Marrakesh, Marocco, 2013.
16. K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Optics Communications*, vol. 30, no. 2, pp. 257–261, 1979.

17. R. Candido, D. C. Soriano, M. T.M. Silva, and M. Eisencraft, "Do chaos-based communication systems really transmit chaotic signals?," *Signal Processing*, vol. 108, no. 0, pp. 412 – 420, 2015.
18. R. Candido, M. Eisencraft, and M. T. M. Silva, "Channel equalization for synchronization of chaotic maps," *Digital Signal Processing*, vol. 33, pp. 42 – 49, 2014.
19. M. Hénon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics*, vol. 50, pp. 69–77, 1976.
20. G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive mac protocol for multi-hop wireless networks," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, New York, NY, USA, 2001, MobiCom '01, pp. 236–251, ACM.
21. L. M. Pecora, T. L. Carroll, G. A. Johnson, D. J. Mar, and J. F. Heagy, "Fundamentals of synchronization in chaotic systems, concepts, and applications," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 7, no. 4, pp. 520–543, 1997.
22. A. H. Sayed, *Adaptive Filters*, John Wiley & Sons, NJ, 2008.
23. G. A. Abib, M. Eisencraft, and A. M. Batista, "Using coupled maps to improve synchronization performance," in *Chaotic Signals in Digital Communications*, M. Eisencraft, R. Attux, and R. Suyama, Eds. CRC Press, Inc., 2013.
24. W. A. Sethares, "Adaptive algorithms with nonlinear data and error functions," *IEEE Trans. Signal Process.*, vol. 40, no. 9, pp. 2199–2206, Sep. 1992.
25. G. Picchi and G. Prati, "Blind equalization and carrier recovery using a "stop-and-go" decision-directed algorithm," *IEEE Trans. Commun.*, vol. COM-35, pp. 877–887, Sep. 1987.