



# DINCON 2011

## 10<sup>a</sup> Conferência Brasileira de Dinâmica, Controle e Aplicações

### 28 de agosto a 1<sup>o</sup> de setembro de 2011



## SISTEMA DE COMUNICAÇÃO DIGITAL USANDO SINAIS CAÓTICOS EM CANAIS DE BANDA LIMITADA

*Rodrigo T. Fontes<sup>1</sup>, Marcio Eisenkraft<sup>2</sup>, Luiz H. A. Monteiro<sup>3</sup>*

<sup>1</sup>UNIBAN Brasil, São Paulo, Brasil, fontesrt@gmail.com

<sup>2</sup>Centro de Engenharia, Modelagem e Ciências Sociais Aplicadas, Universidade Federal do ABC, Santo André, Brasil, marcio.eisenkraft@ufabc.edu.br

<sup>3</sup>Escola de Engenharia da Universidade Presbiteriana Mackenzie e Escola Politécnica da Universidade de São Paulo, São Paulo, Brasil, luizm@mackenzie.br, luizm@usp.br

**Resumo:** Neste trabalho, avalia-se o desempenho de um sistema de comunicação baseado em sincronismo caótico que transporta mensagens binárias. Averigua-se o desempenho desse sistema em termos de taxas de erro de bit. Estas taxas possibilitam compará-lo quantitativamente com outros sistemas de comunicação digitais tanto convencionais quanto baseados em caos.

**Palavras-chave:** Caos, sincronismo, sistemas de comunicação.

### 1. INTRODUÇÃO

A proteção dos dados transmitidos em sistemas de comunicação tem sido estudada em diversas áreas da Engenharia de Telecomunicações [1]. Os sinais caóticos, por apresentarem como características determinismo, aperiodicidade e sensibilidade às condições iniciais, mostram-se adequados para a utilização em aplicações que requerem este tipo de segurança, devido à sua dificuldade de predição, a serem confundíveis com o ruído no canal e a poderem apresentar espectro de Fourier plano. Além disso, como sinais caóticos, em geral, são de banda larga, representam uma alternativa para sistemas que empregam técnicas de espalhamento espectral [2].

Diante destas possibilidades, nos últimos anos surgiram muitos artigos propondo sistemas de comunicação que empregam sinais caóticos [3]. Dentre eles, os baseados em *sincronização caótica* [4] parecem promissores, em particular, a *modulação caótica* [5, 6]. Neste sistema, a mensagem é combinada com uma variável de estado do mestre, aplicando-se uma função de codificação, a fim de modificar a dinâmica do mestre. Este sinal caótico é então transmitido e a mensagem é recuperada no escravo usando uma função de decodificação.

Como os sinais caóticos, em geral, ocupam uma larga

faixa de frequências [2], a sincronização caótica pode ser seriamente comprometida quando o canal de comunicação impõe limitações de largura de banda. Devido à natureza não-linear dos sistemas envolvidos, se qualquer componente espectral for minimamente afetada na transmissão, a sincronização caótica e a recuperação da mensagem no receptor podem ser severamente prejudicadas, como mostram as simulações numéricas relatadas em [7–9].

Uma possível solução para este problema para sistemas de tempo discreto foi proposta em [8, 9]. Os sistemas de comunicação apresentados nestes artigos foram simulados com mensagens analógicas, como senóides ou sinais de áudio. No presente artigo revisita-se esta solução, mas utilizando-se sequências binárias como sinais transmitidos. Desta forma, podem-se fazer análises quantitativas de desempenho em termos de Taxa de Erro de Bit (BER - *Bit Error Rate*) e comparações com outros sistemas de comunicação digitais baseados em caos e mesmo sistemas convencionais [1].

Apresenta-se o artigo da seguinte forma: na Seção 2 revisita-se o sistema proposto em [8, 9]. A seguir, na Seção 3, mostram-se resultados de simulações destes sistemas considerando mensagens digitais. Por fim na Seção 4, listam-se algumas conclusões.

### 2. COMUNICAÇÃO USANDO SINAIS CAÓTICOS EM CANAIS DE BANDA LIMITADA

O método de sincronização mestre-escravo de Wu e Chua [5], adaptado para sistemas de tempo discreto, propõe que o sistema mestre seja descrito pela equação

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

enquanto o sistema escravo, que é dependente de  $\mathbf{x}[n]$ , seja escrito como

$$\mathbf{y}[n+1] = \mathbf{A}\mathbf{y}[n] + \mathbf{b} + \mathbf{f}(\mathbf{x}[n]) \quad (2)$$

em que  $n \in \mathbb{N}$ ,  $\{\mathbf{x}[n], \mathbf{y}[n]\} \subset \mathbb{R}^K$ ,  $\mathbf{x}[n] = [x_1[n], x_2[n], \dots, x_K[n]]^T$ ,  $\mathbf{y}[n] = [y_1[n], y_2[n], \dots, y_K[n]]^T$  e a matriz  $A_{K \times K}$  e o vetor  $\mathbf{b}_{K \times 1}$  são constantes. A função  $\mathbf{f}(\cdot)$  de  $\mathbb{R}^K \rightarrow \mathbb{R}^K$  é não-linear.

O sincronismo é alcançado quando a equação da dinâmica de erro

$$\mathbf{e}(n) \triangleq \mathbf{x}[n] - \mathbf{y}[n] = A\mathbf{e}[n] \quad (3)$$

tende a zero com a evolução de  $n$ . Para isso, basta que os autovalores de  $A$  satisfaçam [10]

$$|\lambda_i| < 1, 1 \leq i \leq K. \quad (4)$$

Um sistema de comunicação baseado nas Eqs.(1,2) foi proposto em [8] considerando que  $\mathbf{f}$  depende unicamente da componente  $x_1$  de  $\mathbf{x}$ . Desta forma  $\mathbf{f}(\mathbf{x}(n)) = [f(x_1(n)), 0, \dots, 0]^T$ . Para este sistema, a mensagem  $m[n]$  é codificada pelo sinal  $x_1[n]$  por meio da função  $c(\cdot, \cdot)$ , gerando o sinal transmitido  $s[n] = c(x_1[n], m[n])$ .

O canal de transmissão do sistema de comunicação é modelado por um sistema linear com resposta em frequência  $H_c(\omega)$ . O sinal  $r[n]$  na saída do canal é descrito por  $r[n] = s[n] * h_c[n]$  sendo  $h_c[n]$  a resposta ao impulso do canal e “\*” a integral de convolução [11]. A mensagem recuperada  $m'[n]$  é decodificada no escravo por meio da função  $d = c^{-1}$ ,  $m'[n] = d(y_1[n], r[n])$ , sendo  $y_1$  a primeira componente de  $\mathbf{y}$ . O objetivo é que o sistema mestre-escravo gere um sinal recuperado tal que  $m'[n] = m[n]$ .

Para o sistema de sincronismo utilizado, o transmissor e o receptor são modelados por

$$\mathbf{x}[n+1] = A\mathbf{x}[n] + \mathbf{b} + \mathbf{f}(s[n]) \quad (5)$$

$$\mathbf{y}[n+1] = A\mathbf{y}[n] + \mathbf{b} + \mathbf{f}(r[n]). \quad (6)$$

A diferença entre as Eqs.(1,2) e as Eqs.(5,6) está apenas nos argumentos de  $\mathbf{f}$ .

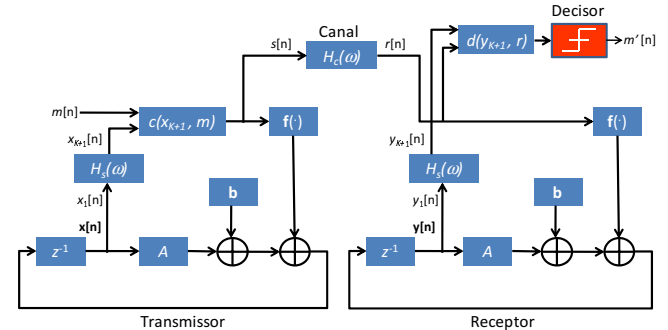
Para a condição de canal ideal, i.e.,  $H_c(\omega) = 1$  e  $s[n] = r[n]$ , a dinâmica do erro de sincronismo continua sendo descrita pela Eq.(3). Assim, se a condição (4) permanece válida,  $\mathbf{y}[n] \rightarrow \mathbf{x}[n]$  e, em particular,  $y_1[n] \rightarrow x_1[n]$ , e desta forma  $m'[n] \rightarrow d(x_1[n], c(x_1[n], m[n])) = m[n]$ . Quando os parâmetros do sistema mestre-escravo estão casados e o canal é ideal, a mensagem  $m[n]$  é completamente recuperada sem degradação, após um curto período transitório.

Para a condição de canal não-ideal, i.e.,  $H_c(\omega) \neq 1$ , o sincronismo não é mais atingido e como consequência  $m'[n] \not\rightarrow m[n]$ . Note-se que, devido à não-linearidade do transmissor e do receptor, se qualquer componente espectral for atenuada ou filtrada pelo canal de transmissão, então todas as componentes espectrais do receptor são potencialmente afetadas.

Em [8, 9] propõe-se restabelecer o sincronismo do sistema para condição de canal limitado em banda ajustando o espectro do sinal caótico transmitido, de acordo com as características do canal.

O diagrama de blocos do sistema proposto é mostrado na Figura 1. Porém, em [8, 9], utilizaram-se mensagens analógicas, que podem assumir valores contínuos a cada instante

$n$ . No presente trabalho, estuda-se o comportamento deste sistema para mensagens digitais binárias  $m[n]$  que a cada  $n$  assume 1 ou  $-1$ . Assim, com esta informação a mais, acrescenta-se um *decisor* com limiar em 0 à saída de  $d$  como mostrado em destaque na Figura 1.



**Figura 1 – Diagrama de blocos do sistema de comunicação com inserção de filtros com resposta em frequência  $H_s(\omega)$ .**

Considera-se  $H_s(\omega)$  um filtro de Resposta ao Impulso Finita (FIR - *Finite Impulse Response*) [11] de ordem  $N$  tendo como sinal de entrada  $x_1$ . A saída de  $H_s(\omega)$ , escrita como  $x_{k+1}[n]$ , é determinada por  $x_{k+1}[n] = \sum_{j=1}^{N+1} c_j x_1[n-j+1]$  em que  $c_1, c_2, \dots, c_{N+1}$  são os coeficientes do filtro. O sinal transmitido  $s[n]$  é obtido por  $s[n] = c(x_{k+1}[n], m[n])$ . Um filtro idêntico à  $H_s(\omega)$  é colocado no receptor tendo como sinal de entrada  $y_1$ . A saída do filtro no receptor é  $y_{k+1}[n] = \sum_{j=1}^{N+1} c_j y_1[n-j+1]$  e desta forma  $m'[n] = d(y_{k+1}[n], r[n])$ . A dimensão do sistema de equações de diferenças que descreve o conjunto mestre-escravo neste modelo tem ordem  $2(K+N)$ .

Assim como em [9], considera-se nas simulações o mapa bidimensional de Hénon [12]:

$$x_1[n+1] = 1 - \alpha x_1^2[n] + x_2[n] \quad (7)$$

$$x_2[n+1] = \beta x_1[n]. \quad (8)$$

em que  $\alpha$  e  $\beta$  são constantes. Para este sistema, mostra-se em [9] que a condição da Eq.(4) é mantida independentemente dos coeficientes  $c_1, c_2, \dots, c_{N+1}$  para  $\beta < 1$ .

Uma questão que ainda está em aberto é quais as condições que os coeficientes dos filtros devem satisfazer de forma que os sinais gerados no mestre continuem caóticos e o sistema não divirja. Alguns resultados neste sentido são discutidos em [9]. Na próxima seção, são apresentadas e discutidas simulações deste sistema considerando-se mensagens digitais.

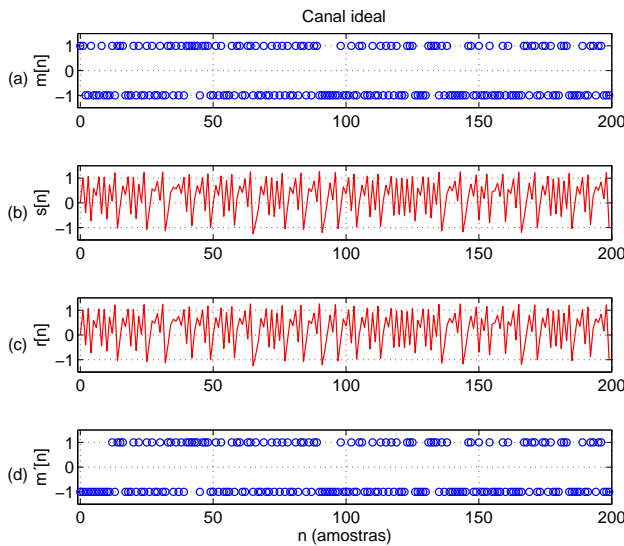
### 3. SIMULAÇÕES COMPUTACIONAIS

Nesta seção são mostrados os resultados obtidos simulando-se o sistema de comunicação descrito pelas Eqs.(5,6) e representado em diagrama de blocos na Figura 1. Os filtros  $H_c(\omega)$  e  $H_s(\omega)$ , utilizados nas simulações, são FIR passa-baixas de ordens  $N_c$  e  $N$ , respectivamente e projetados pelo método do janelamento da resposta ao impulso [11]. Possuem frequências de corte  $\omega_c$  e  $\omega_s$ , respectivamente. As frequências discretas, são dadas em radianos. Vale lembrar

que uma frequência discreta  $\omega = \pi$  do espectro de um sinal amostrado corresponde a metade da frequência de amostragem, ou frequência de Nyquist [11].

Considera-se que a mensagem  $m[n]$  é composta por uma sequência aleatória binária que assume 1 ou  $-1$  a cada instante  $n$ . Como função de codificação, considerou-se  $s[n] = c(x_{k+1}[n], m[n]) = x_{k+1}[n] + 0,001m[n]$  de forma que  $m'[n] = \text{sign}(d(x_{k+1}[n], r[n])) = \text{sign}(1000(r[n] - y_{k+1}[n]))$ . A função  $\text{sign}(z)$  retorna 1 para  $z \geq 0$  e  $-1$  para  $z < 0$ .

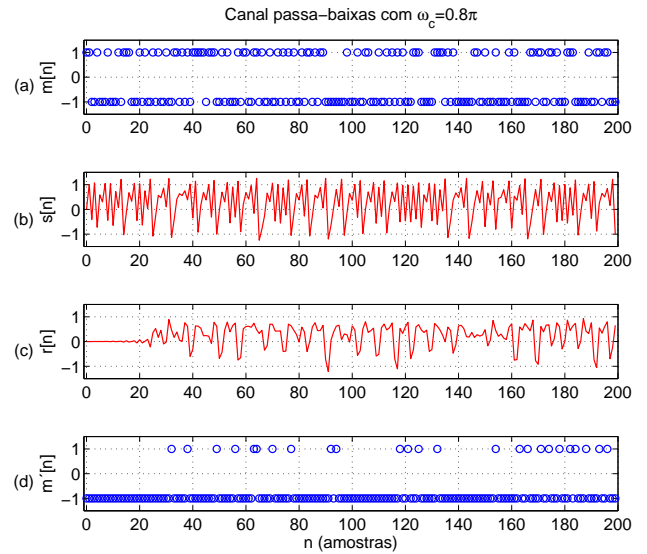
Na Figura 2, correspondente à condição de canal ideal, e na Figura 3, em que o canal é limitado em frequência, são mostrados os gráficos de realizações dos sinais  $m[n]$ ,  $s[n]$ ,  $r[n]$  e  $m'[n]$ , com  $\alpha = 1,4$  e  $\beta = 0,3$ . Nestes primeiros casos, desconsideraram-se os filtros nos laços de realimentação, ou seja,  $H_s(\omega) = 1$ .



**Figura 2 – Simulação do sistema de comunicação digital da Fig. 1 para o caso de canal ideal  $H_c(\omega) = H_s(\omega) = 1$ : a) mensagem  $m[n]$ , b) sinal transmitido  $s[n]$ , c) sinal recebido  $r[n] = s[n]$  e d) mensagem recuperada  $m'[n]$ .**

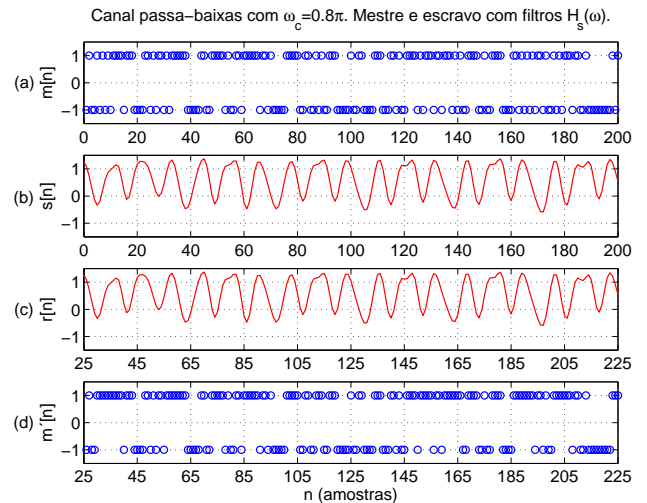
Para a condição de canal ideal de transmissão da Figura 2, a mensagem  $m[n]$  é recuperada perfeitamente, ou seja  $m'[n] = m[n]$ , a menos de um transitório necessário para o sistema mestre-escravo sincronizar, o que leva cerca de 20 amostras. Já para o caso da Figura 3, o canal de transmissão é modelado como um filtro de ordem  $N_c = 50$  e frequência de corte  $\omega_c = 0,8\pi$ . Neste caso, a mensagem  $m'[n]$  recuperada é bem diferente da mensagem transmitida, ou seja, a limitação de banda do canal de transmissão afeta drasticamente o sincronismo do sistema mestre-escravo.

Na Figura 4 é mostrado o desempenho do sistema perante o mesmo canal utilizado na simulação da Figura 3, porém, agora inserindo-se filtros  $H_s(\omega)$  de ordem  $N = 30$  e frequência de corte  $\omega_s = 0,4\pi$  no transmissor e no receptor. Neste caso, tomou-se  $\alpha = 0,9$  e  $\beta = 0,3$  como em [9]. Para estes parâmetros, os sinais gerados são caóticos, mesmo com a inclusão de  $H_s(\omega)$ , e o sistema mestre não diverge. Observa-se que, neste caso, o número de erros na obtenção



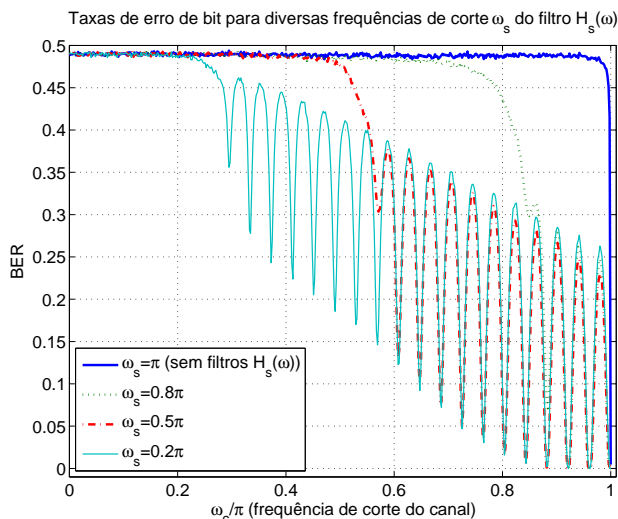
**Figura 3 – Simulação do sistema de comunicação digital da Fig. 1 para  $\omega_c = 0,8\pi$  e  $H_s(\omega) = 1$ : a) mensagem  $m[n]$ , b) sinal transmitido  $s[n]$ , c) sinal recebido  $r[n]$  e d) mensagem recuperada  $m'[n]$ .**

de  $m'[n]$  é significativamente menor, ainda que não nulo. As escalas foram ajustadas de forma a poder-se comparar  $m[n]$  e  $m'[n]$  descontando-se o efeito do atraso do canal, da ordem de  $\frac{N_c}{2} = 25$ .



**Figura 4 – Simulação do sistema de comunicação digital da Fig. 1 para  $\omega_c = 0,8\pi$  e  $\omega_s = 0,4\pi$ : a) mensagem  $m[n]$ , b) sinal transmitido  $s[n]$ , c) sinal recebido  $r[n]$  e d) mensagem recuperada  $m'[n]$ .**

Para avaliar o desempenho do sistema proposto, mede-se a BER no receptor, quando varia-se a frequência de corte do canal  $\omega_c$  para alguns valores da frequência de corte  $\omega_s$  dos filtros usados no transmissor e receptor. Os resultados estão mostrados na Figura 5 e foram obtidos considerando-se a transmissão de 100000 bits para cada valor de  $\omega_c$ ,  $\alpha = 0,9$ ,  $\beta = 0,3$ ,  $N = 30$ ,  $N_c = 50$ , e 500 valores diferentes de  $\omega_c$  entre  $0,0001\pi$  e  $0,9999\pi$ .



**Figura 5** – Taxa de erro de bit do sistema de comunicação variando-se os valores de  $\omega_c$  para valores fixos de  $\omega_s$ .

Observa-se que, quando não são utilizados filtros no mestre e escravo, ou seja,  $\omega_s = \pi$ , qualquer frequência de corte do canal faz com que a BER se aproxime do limite superior de 0,5.

A utilização dos filtros no mestre e no escravo reduz efetivamente a BER para os valores de  $\omega_s$  usados quando  $\omega_c > \omega_s$ . Porém, é interessante notar que esta redução parece atingir um limite independentemente do filtro  $H_s(\omega)$  usado. Ou seja, a solução proposta em [8, 9], apesar de reduzir os valores da BER não é capaz de fazer os valores aproximarem-se de zero. Certamente serão necessárias aplicar outras técnicas em conjunto. Note-se que estes resultados não são facilmente observáveis nos trabalhos anteriores por utilizarem-se sinais analógicos.

Também é interessante notar que as curvas de BER na faixa em que os filtros  $H_s(\omega)$  são efetivos não é monotônica: elas oscilam com a resposta em frequência do canal. Como os filtros FIR que simulam o canal não são ideais, apresentam pequenas oscilações na faixa de passagem. Estas oscilações parecem já ser suficientes para influenciar o desempenho em termos de BER.

#### 4. CONCLUSÕES

Neste trabalho analisou-se o sistema de comunicação baseado em codificação caótica proposto em [8, 9] para mensagens digitais, obtendo-se como parâmetro de desempenho a BER.

Os resultados indicam que o uso dos filtros digitais no mestre e no escravo possibilita alcançar taxas de menores de BER, porém, ainda altas do ponto de vista de comunicações práticas e com comportamento sensível à variações do canal de transmissão. Assim, um longo caminho ainda é necessário para que estes sistemas de comunicação baseados em caos rivalizem com os convencionais em canais de banda limitada.

Como trabalhos futuros, pretende-se: (i) analisar, teoricamente e numericamente, as condições a serem satisfeitas pelos filtros para que os sinais gerados sejam caóticos e mi-

nimizar as variações da BER, (ii) comparar o desempenho deste sistema com outros em termos de BER e (iii) considerar a influência do ruído no canal.

#### AGRADECIMENTOS

Marcio Eisencraft e Luiz H. A. Monteiro agradecem o apoio do CNPq.

#### Referências

- [1] S. S. Haykin, *Communication systems*, 4th ed. New York: Wiley, 2000.
- [2] W. M. Tam, F. C. M. Lau, and C. K. Tse, *Digital Communications with Chaos: Multiple Access Techniques and Performance*. New York, NY, USA: Elsevier Science Inc., 2006.
- [3] M. Kennedy, G. Setti, and R. Rovatti, Eds., *Chaotic Electronics in Telecommunications*. Boca Raton, FL, USA: CRC Press, Inc., 2000.
- [4] L. M. Pecora and T. L. Carroll, “Synchronization in chaotic systems,” *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb 1990.
- [5] 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, 1993.
- [6] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. Mirasso, L. Pesquera, and K. Shore, “Chaos-based communications at high bit rates using commercial fibre-optic links,” *Nature*, vol. 438, no. 7066, pp. 343–346, 2005.
- [7] M. Eisencraft and M. Gerken, “Comunicação utilizando sinais caóticos: influência de ruído e limitação em banda,” in *Anais do XVIII Simpósio Brasileiro de Telecomunicações*, Gramado, Brasil, 2001, pp. 1–6, (in Portuguese).
- [8] DOI M. Eisencraft, R. D. Fanganiello, and L. A. Baccala, “Synchronization of discrete-time chaotic systems in bandlimited channels,” *Mathematical Problems in Engineering*, vol. 2009, 2009.
- [9] DOI M. Eisencraft, R. D. Fanganiello, and L. H. A. Monteiro, “Chaotic synchronization in discrete-time systems connected by bandlimited channels,” *Communications Letters, IEEE*, vol. PP, no. 99, pp. 1–3, 2011.
- [10] R. P. Agarwal, *Difference equations and inequalities: theory, methods, and applications*. New York: M. Dekker, 1992.
- [11] A. V. Oppenheim and R. W. Schaffer, *Discrete-Time Signal Processing*. Upper Saddle River, NJ, USA: Prentice Hall Press, 2009.
- [12] DOI M. Hénon, “A two-dimensional mapping with a strange attractor,” *Comm. Math. Phys.*, vol. 50, no. 1, pp. 69–77, 1976.