

Análise Espectral de um Mapa Caótico Baseado na Função Tangente Hiperbólica

Carlos E. C. Souza, Daniel P. B. Chaves e Cecilio Pimentel

Resumo— Este trabalho generaliza o mapa caótico introduzido pelos autores recentemente com a adição de dois novos parâmetros de controle. O expoente de Lyapunov é empregado para analisar a dinâmica caótica do mapa proposto. As características espectrais de sinais caóticos gerados por este mapa em função das variáveis de controle também são investigadas. O mapa proposto pode ser aplicado em sistemas de comunicação baseados em dinâmica simbólica com vantagens sobre os sistemas atuais baseados em mapas lineares por partes.

Palavras-Chave— Comunicação caótica, sistemas dinâmicos, mapas iterativos, expoente de Lyapunov, densidade espectral de potência.

Abstract— This work generalizes the chaotic map recently introduced by the authors with the addition of two new control parameters. The Lyapunov exponent is employed to analyze the chaotic dynamics of the proposed map. The spectral characteristics of chaotic signals generated by this map as a function of the control parameters are also investigated. The proposed map can be used in symbolic dynamics based communication systems with advantages over current approaches based on piecewise linear maps.

Keywords— Chaotic communication, dynamical systems, iterative maps, Lyapunov exponent, power spectral density.

I. INTRODUÇÃO

Sinais caóticos são conhecidos por sua irregularidade, aperiodicidade, descorrelação e espectro faixa larga [1]. Apesar disso, podem ser gerados por sistemas dinâmicos determinísticos simples [2], o que motiva sua aplicação em criptografia [3], geração de números aleatórios [4], marca d'água [5], comunicação [6], modelamento de sistemas [7].

A reconhecida propriedade de descorrelação e larga faixa espectral os torna candidatos potenciais para implementação de sistemas de comunicação com espalhamento espectral [1], [2]. Tal sistema oferece vantagens como robustez a múltiplos percursos e baixa probabilidade de interceptação [8]. Além disso, o comportamento errático do sinal caótico propicia segurança à informação na camada física do sistema. Como há uma gama de sistemas caóticos de fácil construção, inclusive através de circuitos eletrônicos, podemos considerá-los para implementação de sistemas de baixo custo [3], [6].

As técnicas abordadas na literatura para implementação de esquemas de comunicação empregando sistemas caóticos são baseadas essencialmente em dois métodos. No primeiro, os símbolos de informação são codificados em uma sequência caótica gerada pela iteração direta do mapa caótico [9], [10],

enquanto o segundo utiliza a iteração reversa em conjunto com a dinâmica simbólica das órbitas [11].

Duas características do segundo método merecem destaque, que surgem como contraponto aos desafios tipicamente encontrados na implementação dos sistemas de comunicação baseados em caos. Esse método é capaz de minimizar os problemas relacionados à amplificação de erro e precisão de truncamento encontrados no primeiro método. Se implementado com um mapa adequado, pode-se estabelecer um compromisso entre desempenho e segurança da informação. Nesse contexto, um sistema baseado em um mapa linear por partes foi proposto em [12], com um parâmetro de controle que permite alterar o comprimento de uma região de guarda, propiciando maior ou menor imunidade ao ruído. Outros sistemas de comunicação baseados em caos foram propostos baseados neste mapa que possui uma região que nunca é visitada [13], [14], [15]. Isso restringe a dinâmica do sistema caótico em função do comprimento dessa região, o que induz invariavelmente um compromisso entre desempenho e segurança. Essa limitação foi eliminada com o mapa caótico proposto pelos autores em [16]. Este mapa, denominado de *tanh*, é baseado na função tangente hiperbólica e permite a indução de uma região de guarda sem degradar o caos, quando quantificado pelo valor do expoente de Lyapunov.

Este trabalho apresenta um novo mapa caótico baseado na função tangente hiperbólica, denominado de mapa *stanh*, que é uma generalização do mapa *tanh* proposto pelo autores em [16]. O mapa *stanh* é obtido pela adição de dois novos parâmetros de controle relacionados à paridade e à simetria do mapa. Inicialmente, estuda-se o expoente de Lyapunov do mapa proposto. Em seguida, mostraremos que os novos parâmetros podem ser utilizados para a obtenção de diferentes características espectrais dos sinais gerados pelo mapa.

Este artigo está dividido em seis seções. Na Seção II é apresentada uma breve introdução aos conceitos de modulação via dinâmica simbólica. Na Seção III é introduzido o mapa *stanh*. Na Seção IV é feito um estudo do comportamento caótico do mapa *stanh*. Na Seção V é realizada uma investigação das características espectrais do mapa *stanh* e, finalmente, na Seção VI são apresentadas as conclusões deste trabalho.

II. MODULAÇÃO VIA DINÂMICA SIMBÓLICA

No início da década de 90 foi introduzido o conceito de controle de caos [17], que propõe a intervenção controlada na dinâmica do sistema caótico autônomo através de pequenas perturbações na sua órbita. Os mesmos autores propuseram em [9] a aplicação dessa técnica para transmissão, onde sequências binárias são mapeadas univocamente em órbitas do sistema caótico.

Técnicas de modulação de sistemas caóticos usando dinâmica simbólica foram propostas inicialmente em [9], [18]. O princípio básico consiste em criar um particionamento do espaço de fase do sistema dinâmico e atribuir um símbolo distinto a cada região da partição. Desta forma uma sequência de informação é transformada em uma sequência de símbolos que representa a dinâmica da visitação da órbita no espaço de fase. Por exemplo, no caso de sequências binárias, o particionamento é realizado em duas regiões: a uma delas é atribuído o símbolo 0 e à outra o símbolo 1. Uma forma de definir um particionamento ideal é utilizando seções de Poincaré do mapa [18].

Para utilizar mapas caóticos em sistemas de comunicações, deve-se obter uma série temporal a partir da aplicação iterativa do mapa. Dado um mapa unidimensional $f(x)$, tem-se uma série temporal através da iteração

$$x_n = f(x_{n-1}), n = 1, 2, \dots \quad (1)$$

Dada uma condição inicial x_0 , constrói-se a sequência $\{x_i\}_{i=0}^{\infty} = \{x_0, f(x_0), f^2(x_0), \dots\}$, que é denominada órbita de x_0 por f . Aplicações sucessivas do mapa estão associadas a sucessões de cruzamentos da órbita com uma seção de Poincaré adequada, cujas regiões do particionamento induzido são rotulados adequadamente, de forma a garantir às órbitas sequências únicas de símbolos, ou equivalentemente, sequências código únicas. Interpretando essas sequências como símbolos de informação, empregando controle de caos, ela pode ser modulada em uma órbita ou série temporal caótica.

Para ilustrar esse método, vamos introduzir o mapa modificado de Bernoulli [12]. A função $f(x)$ é definida sobre um intervalo limitado \mathbb{H} tal que $f(\mathbb{H}) = \mathbb{H}$, de forma que \mathbb{H} é invariante por f . Este mapa é linear por partes e induz um particionamento de \mathbb{H} em três subintervalos I_0 , I_1 e I_2 , sendo definido por

$$f(x) = \begin{cases} \frac{2x+(1+p)}{1-p}, & -1 \leq x \leq -p \quad (I_0) \\ \frac{x}{p}, & -p \leq x \leq p \quad (I_1) \\ \frac{2x-(1+p)}{1-p}, & p \leq x \leq 1. \quad (I_2) \end{cases} \quad (2)$$

A modulação caótica baseada na iteração direta do mapa em (2) apresenta dois inconvenientes: amplificação de erro e erro de quantização [12]. Para contornar estes problemas é utilizado a iteração reversa, por meio do mapa de Bernoulli modificado inverso

$$f_s^{-1}(x) = \begin{cases} \frac{(1-p)x-(1+p)}{2}, & s = 0 \quad (I_0) \\ px, & s = 1, \quad (I_1) \\ \frac{(1-p)x+(1+p)}{2}, & s = 2, \quad (I_2) \end{cases} \quad (3)$$

que é um conjunto de mapas de contração sobre \mathbb{H} . A modulação caótica de uma sequência finita de símbolos $s_n s_{n+1} \dots s_{M-1}$ é feita iterando (3) a partir de uma dada condição final x_N . Essa abordagem é considerada em diversos cenários de comunicação caótica [12], [13], [14]. O procedimento é mapear o bit de informação 0 para $s = 0$ e o bit de informação 1 para $s = 2$. Desta forma, a região interna I_1 (para $s = 1$) nunca é visitada e é interpretada como uma região de guarda que garante uma distância mínima entre as sequências transmitidas. A largura da região de guarda

depende do parâmetro p , tornando o sistema mais robusto ao ruído quando p aumenta. Entretanto, o sistema se torna mais previsível, diminuindo a segurança para aplicações criptográficas. Outro inconveniente deste mapa é o enfraquecimento das propriedades caóticas ao diminuir os graus de liberdade do sistema a partir da proibição da ocorrência de valores na região I_1 .

Este problema é contornado com o mapa caótico baseado na função tangente hiperbólica, denominado de tanh, introduzido em [16]. Este mapa tem um parâmetro de controle que pode ser convenientemente escolhido para manter uma região com pouca probabilidade de visitação (que pode ser interpretada como uma região de guarda) sem a necessidade de alterar a dinâmica do sistema com a proibição de visitação de regiões do mapa original. Por outro lado o mapa tanh possui pouca flexibilidade espectral. Isto pode ser um inconveniente em aplicações nas quais se precisa de sinais com potência concentrada em uma faixa específica do espectro. Na próxima seção definiremos um novo mapa, denominado de stanh, que é baseado no mapa tanh com a introdução de dois novos parâmetros de controle. O novo mapa mantém as vantagens de ter uma região de guarda natural, como no mapa tanh, sem comprometer a flexibilidade espectral do mapa.

III. O MAPA STANH

O mapa stanh $f : [-1, 1] \rightarrow [-1, 1]$ é definido por

$$f(x) = \begin{cases} e \cdot \tanh\left[\frac{r}{1+\alpha} \cdot (x+1)\right] - 1, & x < \alpha \\ (-1)^b \cdot [e \cdot \tanh\left[-\frac{r}{1-\alpha} \cdot (x-1)\right] - 1], & x \geq \alpha. \end{cases} \quad (4)$$

O fator de escala e é dado por

$$e = \frac{2}{\tanh(r)} \quad (5)$$

e os parâmetros de controle são especificados pela tripla (b, r, α) . O parâmetro b define a simetria do mapa stanh e pode assumir os valores 0 ou 1. No caso em que $b = 0$, o mapa stanh possui simetria par e é denominado *e-stanh* e no caso de $b = 1$ a simetria é ímpar e o mapa é denominado *o-stanh*.

O parâmetro r controla a largura da região de guarda do mapa stanh e pode assumir valores reais maiores que zero. Neste trabalho, assumiremos que r está definido no intervalo $(0, 10]$. Para o mapa stanh a região de guarda é a região central do mapa que tem uma baixa taxa de ocupação.

O parâmetro α está relacionado com o deslocamento do eixo de simetria, isto é, desloca o eixo central do mapa stanh, localizado em $x = 0$, para a direita, com valores positivos de α e para a esquerda com valores negativos deste parâmetro. No limite em que $r \rightarrow 0$ e $\alpha = 0$, o mapa e-stanh tende ao mapa da tenda e o mapa o-stanh tende ao mapa de Bernoulli. A Fig. 1 ilustra o mapa e-stanh para um valor fixo de r , $r = 3$, e para três valores do parâmetro α . Uma figura similar para o mapa o-stanh é mostrada na Fig. 2.

A modulação de sinais caóticos gerados pelo mapa stanh é feita por iteração reversa, em que o mapa stanh inverso é dado

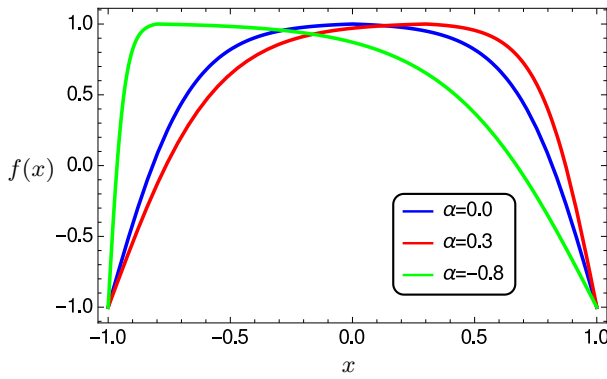


Fig. 1. Mapa e-stanh ($b = 0$) para três valores de α , $\alpha = 0; 0,3; -0,8$. $r = 3$.

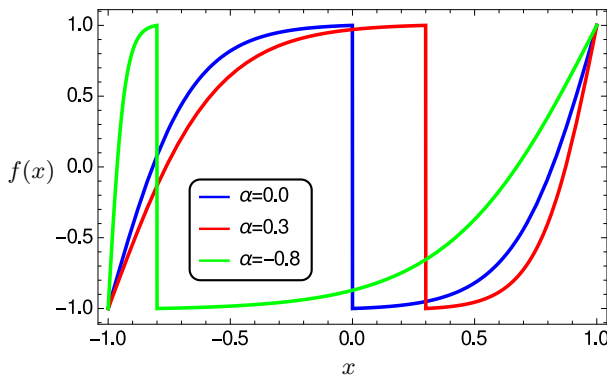


Fig. 2. Mapa o-stanh ($b = 1$) para três valores de α , $\alpha = 0; 0,3; -0,8$. $r = 3$.

por

$$f_s^{-1}(x) = \begin{cases} \frac{1+\alpha}{r} \tanh^{-1}\left(\frac{x+1}{e}\right) - 1, & s = 0 \quad (I_0) \\ -\frac{1-\alpha}{r} \tanh^{-1}\left(\frac{x+1}{be}\right) + 1, & s = 1. \quad (I_1) \end{cases} \quad (6)$$

A adequação desse mapa para aplicações em comunicação é estabelecida com relação às propriedades do sinal caótico. Uma das ferramentas para esta análise é investigar o expoente de Lyapunov do mapa, o que será analisado na próxima seção.

IV. COMPORTAMENTO CAÓTICO

O expoente de Lyapunov mede a taxa de separação entre duas trajetórias durante a evolução dinâmica do sistema. Duas órbitas infinitesimalmente próximas tendem a se afastar se o expoente de Lyapunov for positivo [1], [2], sendo um indicativo da presença de caos no sistema. O expoente de Lyapunov para um mapa discreto unidimensional é definido por [2]

$$\lambda = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln \left| \frac{d}{dx_i} f(x_i) \right|. \quad (7)$$

A Figura 3 ilustra o comportamento do expoente de Lyapunov versus o parâmetro α para o mapa o-stanh ($b = 1$) para três valores do parâmetro r . Um comportamento semelhante foi observado para o mapa e-stanh ($b = 0$). Observa-se nesta figura que o Lyapunov é positivo para o intervalo de parâmetros considerado. Quando r assume valores próximos

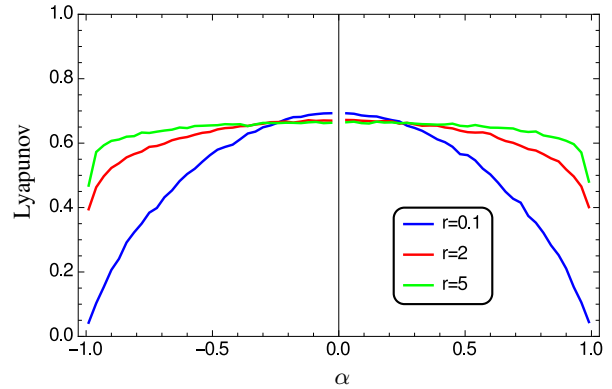


Fig. 3. Expoente de Lyapunov versus α para o mapa o-stanh para $r = 0, 1; 2; 5$.

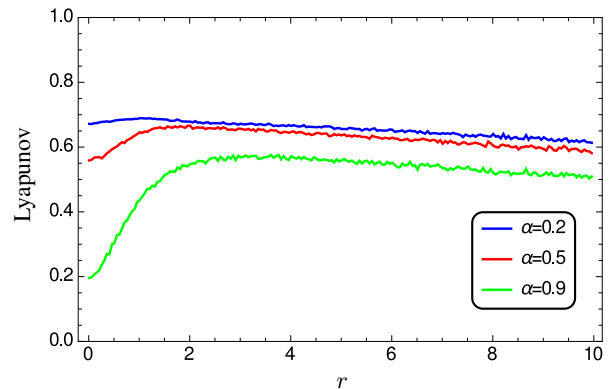


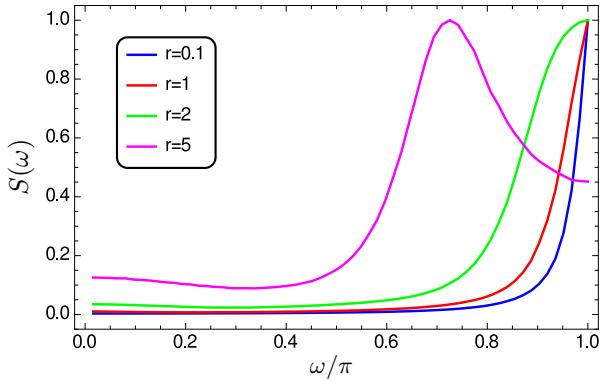
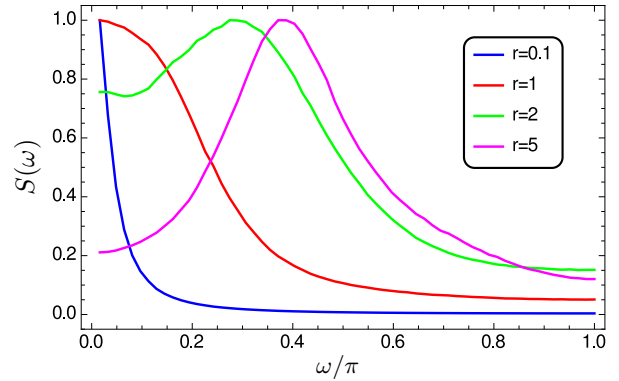
Fig. 4. Expoente de Lyapunov versus r para o mapa e-stanh para $\alpha = 0, 2; 0, 5; 0, 9$.

de zero, o expoente tende a zero nos extremos do intervalo de definição de α . Ao aumentarmos o valor de r , o expoente tem uma variação mais uniforme, indicando uma maior robustez do comportamento caótico à variação do parâmetro α . A Figura 4 mostra como o expoente varia em relação a r para três valores do parâmetro α . Para valores pequenos de r observa-se uma maior variação do expoente de Lyapunov com α . Esta variação diminui quando α é reduzido. Adicionalmente, para valores suficientemente elevados de r , independente do α , todas as curvas apresentam um decaimento linear com leve inclinação. Observa-se que esse estado é alcançado para valores cada vez menores de r quanto menor for o valor de α . Assim, o aumento do valor de r assegura um mapa com melhores propriedades caóticas, ou seja, um expoente de Lyapunov com pouca sensibilidade à variação dos outros parâmetros do mapa.

Como uma análise final das propriedades do mapa stanh, na próxima seção avaliaremos o comportamento da densidade espectral de potência (PSD) deste mapa com a variação dos seus parâmetros.

V. COMPORTAMENTO ESPECTRAL

O comportamento da PSD de sinais caóticos gerados por mapas lineares por partes é investigado em [19], [20]. Nesta seção, estenderemos esta análise para o mapa stanh utilizando simulações computacionais.


 Fig. 5. PSD do mapa e-stanh para $r = 0, 1; 2; 5$. $\alpha = -0.9$.

 Fig. 6. PSD do mapa e-stanh para $r = 0, 1; 2; 5$. $\alpha = 0.9$.

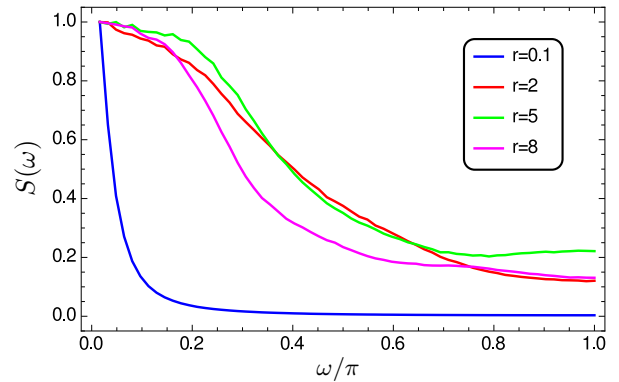
A partir de uma condição inicial x_0 é gerada uma órbita finita $\{x_i\}_{i=0}^{N-1}$ usando (1). Esta órbita, que é um sinal determinístico, pode ser considerada uma função amostral de um processo estocástico estacionário [19]. Assim, $\{x_i\}_{i=0}^{N-1}$ é uma sequência de variáveis aleatórias discretas indexadas pelo índice i tal que a média de x_i é $\eta = \mathbf{E}[x_i]$ e a função de autocorrelação (ACF) é dada por $R[m] = \mathbf{E}[x_i, x_{i+m}]$, onde a média é somada sobre todas as condições iniciais. Para as simulações numéricas da AFC foram empregadas órbitas de tamanho $N = 1024$ e um *ensemble* de 30.000 condições iniciais uniformemente distribuídas no intervalo $[-1, 1]$.

A PSD é a transformada de Fourier de tempo discreto da ACF, isto é,

$$S(\omega) = \sum_{m=-\infty}^{\infty} R[m]e^{-j\omega m}. \quad (8)$$

Nos mapas lineares por partes, é possível obter sinais caóticos de comportamento passa-baixa ou passa-faixa variando os parâmetros de controle do mapa [20], [19]. Para o mapa stanh podemos obter três tipos de comportamento: passa-baixa, passa-alta e passa-faixa.

A Figura 5 mostra o gráfico da PSD para alguns sinais caóticos gerados pelo mapa e-stanh para quatro valores de r e $\alpha = -0.9$. As curvas estão normalizadas para um valor máximo da PSD unitário. Quando r é pequeno, o sinal apresenta comportamento passa-alta sendo mais seletivo com valores menores de r . Aumentando o valor de r observa-se um aumento na faixa de passagem porém o expoente de Lyapunov também aumenta. Com isto, pode-se gerar sinais passa-alta com maior ocupação espectral e com maior robustez à propriedade caótica. Finalmente, para valores de r maiores que aproximadamente 5 a PSD assume um comportamento passa-faixa. Para valores positivos de α o sinal gerado pelo mapa e-stanh tem comportamento passa-baixa quando r é pequeno e passa-faixa quando r é maior que aproximadamente 5, conforme é ilustrado na Figura 6. Em suma, os comportamentos passa-baixa e passa-alta com faixa estreita do mapa e-stanh estão relacionados a valores pequenos de r em conjunto com α positivo (passa-baixa) ou α negativo (passa-alta). Com o aumento de r o mapa e-stanh gera comportamentos passa-faixa e quanto maior o valor de r , menor a dependência dos sinais em relação ao parâmetro α .


 Fig. 7. PSD do mapa o-stanh para $r = 0, 1; 2; 5; 8$. $\alpha = 0.9$.

O mapa o-stanh não possui a mesma variação espectral do mapa e-stanh. A Figura 7 mostra que o comportamento da PSD para o mapa o-stanh é passa-baixa com maior seletividade para valores pequenos de r . Observou-se (figura não mostrada) que este comportamento passa-baixa é invariante em relação ao sinal do parâmetro α .

VI. CONCLUSÕES

A partir da variação dos parâmetros de controle do mapa stanh é possível obter sinais caóticos com várias características espectrais. O conjunto de parâmetros (b, r, α) pode ser definido para gerar sinais caóticos com comportamentos espectrais passa-baixa, passa-alta ou passa-faixa. Além disso, no limite em que r tende a zero, obtemos os mapas da tenda ou o mapa de Bernoulli deslocado, de acordo com a paridade definida pelo parâmetro b .

A tangente hiperbólica pode ser realizada eletronicamente através de um par diferencial com transistor de junção bipolar [21]. Com a incorporação de um circuito periférico, como o *track-and-hold* [22] e fontes de corrente, um circuito que implementa o mapa stanh com $\alpha = 0$ e simetria par foi simulado em SPICE, apresentando comportamento condizente com a previsão teórica para a faixa testada de valores do parâmetro r . Dessa forma, o stanh é um candidato para aplicações em comunicações que envolvem transmissão de informação e geração de números aleatórios.

REFERÊNCIAS

- [1] S. Strogatz, *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry, and Engineering*. Studies in Nonlinearity Series, Westview Press, 2001.
- [2] K. Alligood, T. Sauer, and J. Yorke, *Chaos: An Introduction to Dynamical Systems*. New York, NY, 1997.
- [3] L. Kocarev and S. Lian, *Chaos-based Cryptography: Theory, Algorithms and Applications*. Studies in Computational Intelligence, Springer, 2011.
- [4] T. Stojanovski and L. Kocarev, "Chaos-based random number generators-part I: analysis [cryptography]," *IEEE Trans. Circuits Syst. I Fundam. Theory Appl.*, vol. 48, pp. 281–288, Mar. 2001.
- [5] 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, p. 121, 2011.
- [6] P. Stavroulakis, *Chaos Applications in Telecommunications*. Taylor & Francis, 2005.
- [7] M. Hasler, G. Mazzini, M. Ogorzalek, R. Rovatti, and G. Setti, "Scanning the special issue - special issue on applications of nonlinear dynamics to electronic and information engineering," *Proc. IEEE*, vol. 90, pp. 631–640, May 2002.
- [8] F. Lau and C. Tse, *Chaos-Based Digital Communication Systems*. Engineering online library, Springer, 2010.
- [9] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, pp. 3031–3034, May 1993.
- [10] C. Williams, "Robust chaotic communications exploiting waveform diversity. Part 1: Correlation detection and implicit coding," *IET Communications*, vol. 2, pp. 1213–1222, Nov. 2008.
- [11] J. Schweizer and T. Schimming, "Symbolic dynamics for processing chaotic signals. I. Noise reduction of chaotic sequences," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 11, pp. 1269–1282, 2001.
- [12] D. Luengo and I. Santamaria, "Secure communications using OFDM with chaotic modulation in the subcarriers," in *IEEE Vehicular Technology Conference (VTC 2005-Spring)*, vol. 2, pp. 1022–1026 Vol. 2, May 2005.
- [13] G. Kaddoum, M. Vu, and F. Gagnon, "Chaotic symbolic dynamics modulation in MIMO systems," in *2012 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 157–160, May 2012.
- [14] G. Kaddoum, G. Gagnon, and F. Gagnon, "Spread spectrum communication system with sequence synchronization unit using chaotic symbolic dynamics modulation," *Int. J. Bifurcat. Chaos*, vol. 23, no. 02, pp. 1350019.1–1350019.14, 2013.
- [15] G. Kaddoum, F. Gagnon, and D. Couillard, "An enhanced spectral efficiency chaos-based symbolic dynamics transceiver design," in *Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on*, pp. 1–6, Dec 2012.
- [16] D. Chaves, C. Souza, and C. Pimentel, "A new map for chaotic communication," *International telecommunication Symposium (ITS 2014)*, pp. 1 – 5, August 2014.
- [17] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.*, vol. 64, pp. 1196–1199, Mar 1990.
- [18] B. Hao and W. Zheng, *Applied Symbolic Dynamics and Chaos*. Directions in chaos, World Scientific, 1998.
- [19] M. Eisencraft, D. Kato, and L. Monteiro, "Spectral properties of chaotic signals generated by the skew tent map," *Signal Processing*, vol. 90, no. 1, pp. 385 – 390, 2010.
- [20] M. Eisencraft and D. M. Kato, "Spectral properties of chaotic signals with applications in communications," *Nonlinear Analysis: Theory, Methods & Applications*, vol. 71, no. 12, pp. e2592 – e2599, 2009.
- [21] D. Pederson and K. Mayaram, *Analog Integrated Circuits for Communication: Principles, Simulation, and Design*. Kluwer Academic Publishers, 1991.
- [22] C.-C. Wang, J.-M. Huang, H.-C. Cheng, and R. Hu, "Switched-current 3-bit cmos 4.0-mhz wideband random signal generator," *Solid-State Circuits, IEEE Journal of*, vol. 40, pp. 1360–1365, June 2005.