

Codificação de imagens usando sinais caóticos

Eugênio G. Sabatini, Magno T. M. Silva e Marcio Eisencraft

Resumo— Sistemas de comunicação baseados em caos (SCBCs) podem ser utilizados em aplicações que requerem segurança, como a codificação de uma imagem. Neste artigo, uma imagem é codificada por um SCBC e a qualidade dessa codificação é avaliada utilizando-se o erro quadrático médio percentual (%MSE). Os resultados obtidos mostram que é possível realizar a codificação de uma imagem com segurança, escolhendo-se os parâmetros adequados.

Palavras-Chave— Sinais caóticos, codificação, imagens, segurança.

Abstract— Chaos-based communication systems (CBCSs) can be used in applications that require security, such as image coding. In this paper, we code an image using a CBCS and assess the quality of this coding by measuring the percentage mean square error (%MSE). The obtained results show that the image coding with this system is secure, when the adequate parameters are selected.

Keywords— Chaotic signals, coding, images, security.

I. INTRODUÇÃO

Sinais caóticos são determinísticos, aperiódicos e possuem dependência sensível às condições iniciais [1]. Assim, eles podem ser utilizados em aplicações em que se deseja dificultar a detecção de uma mensagem [3], [4].

Neste artigo, uma imagem é codificada utilizando o sistema binário proposto em [5]. Neste sistema a mensagem é misturada a uma variável de estado de um gerador de sinais caóticos utilizando-se uma função invertível. Para comparar a imagem codificada com a imagem original, utiliza-se o erro quadrático médio percentual (%MSE) [6].

II. FORMULAÇÃO DO PROBLEMA

Na Figura 1, é apresentado o diagrama de blocos do codificador do sistema utilizado, descrito por [5]

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

em que $\mathbf{x}(n) \in \mathbb{R}^K$, \mathbf{A} é uma matriz constante $K \times K$, \mathbf{b} é um vetor constante $K \times 1$, $\mathbf{f}(\cdot)$ é uma função $\mathbb{R}^K \rightarrow \mathbb{R}^K$ geralmente não linear e $s(n)$ é o sinal codificado. A matriz \mathbf{A} é importante para a solução do problema porque seus autovalores λ_i devem satisfazer $|\lambda_i| < 1$, $1 \leq i \leq K$ para que ocorra sincronismo caótico [5]. A codificação é feita por meio da função $c(\cdot, \cdot)$, ou seja,

$$s(n) = c(x_1(n), m(n)), \quad (2)$$

em que $x_1(n)$ é a primeira componente de $\mathbf{x}(n)$ e $m(n) \in \{-1; +1\}$ é a mensagem binária a ser codificada. A mensagem

Eugênio G. Sabatini, Magno T. M. Silva e Marcio Eisencraft, Escola Politécnica da USP, São Paulo, SP, e-mails: {eugenio.sabatini, magno.silva, marcioft}@usp.br. Este trabalho foi parcialmente financiado pelo CNPq (119671/2019-0, 304715/2017-4, 311039/2019-7), FAPESP (2017/20378-9) e CAPES (código de financiamento 001).

$m(n)$ é gerada a partir da conversão de uma imagem $N \times N$ em um vetor $1 \times N^2$. A decodificação é feita utilizando o mesmo mapa da codificação e a função inversa de $c(\cdot, \cdot)$ [5].

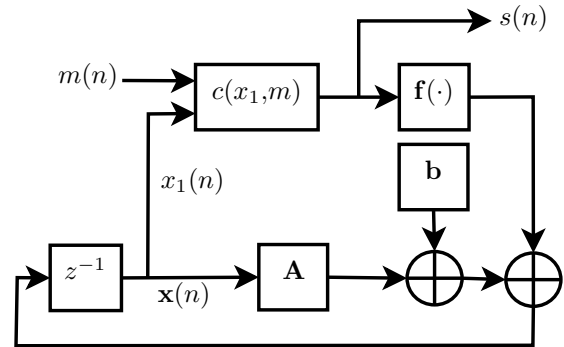


Fig. 1. Transmissor do sistema de comunicação utilizado.

III. SIMULAÇÕES E RESULTADOS

Para as simulações foram utilizados três mapas como geradores de sinais caóticos (GSC), sendo eles:

- 1) Mapa quadrático [7], escrito na forma (1) como

$$\mathbf{x}(n+1) = 1 - 2s^2(n); \quad (3)$$

- 2) Mapa de Hénon 2D [8], escrito na forma (1) como

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

com $\alpha = 1,4$ e $\beta = 0,3$;

- 3) Mapa de Hénon 3D [5], escrito na forma (1) como

$$\mathbf{x}(n+1) = \begin{bmatrix} 0 & 0 & 1 \\ -\beta & 0 & 0 \\ \beta & 1 & 0 \end{bmatrix} \mathbf{x}(n) + \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} \alpha s^2(n) \\ 0 \\ 0 \end{bmatrix}, \quad (5)$$

com $\alpha = 1,07$ e $\beta = 0,3$.

Para codificar o sinal foram utilizadas duas funções

$$c^{(1)}(x_1(n), m(n)) = (1 - \gamma)x_1(n) + \gamma m(n) \quad (6)$$

$$c^{(2)}(x_1(n), m(n)) = m(n)x_1(n), \quad (7)$$

sendo $0 < \gamma \leq 1$ uma constante.

Como medida de qualidade da codificação utilizou-se o %MSE definido como [6]

$$\%MSE \triangleq \frac{\sum [a\hat{f}(x,y) - f(x,y)]^2}{\sum f^2(x,y)} \times 100, \quad (8)$$

sendo

$$a = \frac{\sum f(x,y)\hat{f}(x,y)}{\sum \hat{f}^2(x,y)}, \quad (9)$$

f é a imagem original, \hat{f} é a imagem codificada e os somatórios são tomados sobre todos os pontos (x,y) da imagem.

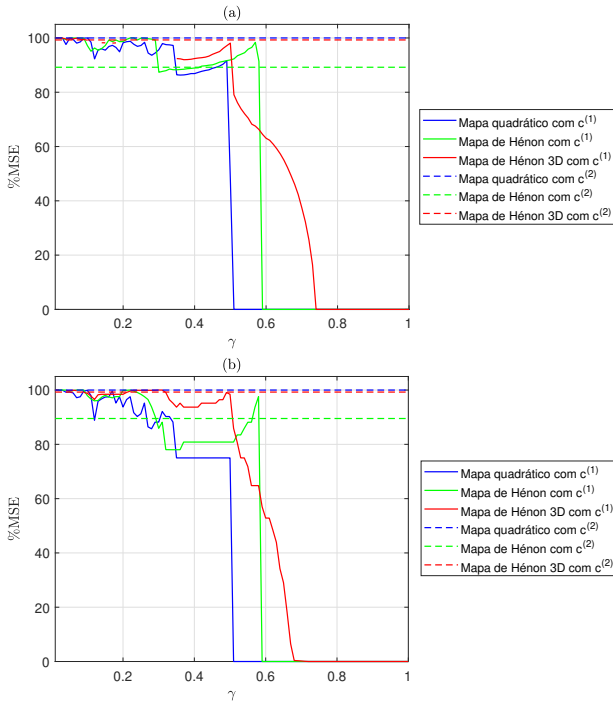


Fig. 2. Valores de %MSE em função do parâmetro γ de (7). (a) Valores calculados para a Figura 3a e (b) valores calculados para a Figura 4a.

Quanto maior o valor de %MSE, mais escondida está a imagem original na imagem codificada.

Para a transmissão, a imagem original é transformada em um vetor e seus níveis 0 e 1 são convertidos para -1 e 1, gerando assim a mensagem $m(n)$ a ser transmitida.

Nas Figuras 2a e 2b são apresentados os valores de %MSE calculados para as imagens em preto e branco Figuras 3a e 4a respectivamente, codificadas utilizando $c^{(1)}$ e $c^{(2)}$, para cada um dos três mapas em função de γ de $c^{(1)}$. Os valores de γ definem a influência da codificação caótica no sinal codificado $s(n)$, de forma que, quanto menor o valor de γ , maior é a influência do sinal caótico na imagem. A função $c^{(2)}$ não depende do valor de γ e, por isso, os valores de %MSE para essa função são constantes. Pode-se perceber que para a codificação $c^{(1)}$ e $\gamma < 0,5$ é possível obter valores elevados (> 90) de %MSE para os três mapas e a imagem original está pouco visível na imagem codificada. Em contrapartida, para $\gamma > 0,6$ nos mapas quadrático e de Hénon 2D, e para $\gamma > 0,75$ no mapa de Hénon 3D, %MSE ≈ 0 e a imagem original fica aparente na imagem codificada. Além disso, para $\gamma < 0,35$ não há valor de %MSE para o mapa de Hénon 3D devido à sua divergência [7].

Nas Figuras 3 e 4 são apresentados exemplos de codificação das imagens apresentadas nas Figuras 3a e 4a, respectivamente, utilizando $c^{(1)}$ com $\gamma \in \{0,1; 0,4; 0,6\}$, $c^{(2)}$ e o mapa quadrático como GSC. Os resultados foram semelhantes, quando se utiliza $c^{(1)}$ com $\gamma = 0,1$ ou $c^{(2)}$, a imagem original fica escondida na imagem codificada. No entanto, quando se utiliza $c^{(1)}$ com $\gamma = 0,4$, aspectos da imagem original são encontrados na imagem codificada. Por fim, para $\gamma = 0,6$, a imagem codificada é similar à imagem original.

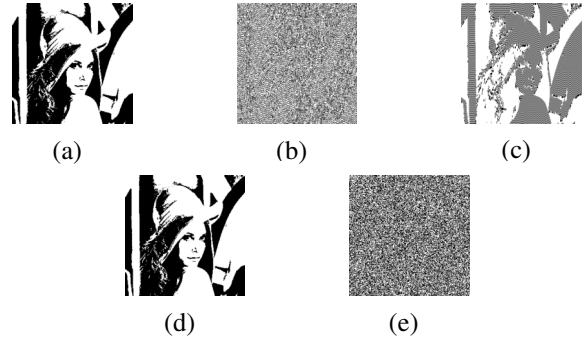


Fig. 3. (a) Imagem original, (b) imagem codificada com $c^{(1)}$ e $\gamma = 0,1$, (c) imagem codificada com $c^{(1)}$ e $\gamma = 0,4$, (d) imagem codificada com $c^{(1)}$ e $\gamma = 0,6$ e (e) imagem codificada com $c^{(2)}$.

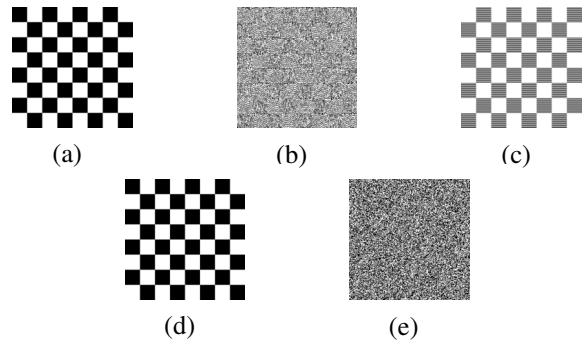


Fig. 4. (a) Imagem original, (b) imagem codificada com $c^{(1)}$ e $\gamma = 0,1$, (c) imagem codificada com $c^{(1)}$ e $\gamma = 0,4$, (d) imagem codificada com $c^{(1)}$ e $\gamma = 0,6$ e (e) imagem codificada com $c^{(2)}$.

IV. CONCLUSÕES

Com os resultados obtidos, pode-se concluir que é possível realizar a codificação de uma imagem utilizando o sistema de [5], que permite a recuperação perfeita da imagem original. Considerando a codificação $c^{(1)}$ com uma escolha adequada do parâmetro γ , pode ser difícil detectar a imagem a partir da imagem codificada. Considerando a codificação $c^{(2)}$, o mapa quadrático e o mapa de Hénon 3D são os mais eficazes em esconder a mensagem, com %MSE ≈ 100 .

REFERÊNCIAS

- [1] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos*. Textbooks in Mathematical Sciences, Springer New York, 2000.
- [2] W. M. Tam, F. C. M. Lau, and C. K. Tse, *Digital Communications with Chaos*. Elsevier Science, 2010.
- [3] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-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, pp. 343–346, nov 2005.
- [4] M. Feki, B. Robert, G. Gelle, and M. Colas, "Secure digital communication using discrete-time chaos synchronization," *Chaos, Solitons & Fractals*, vol. 18, pp. 881–890, nov 2003.
- [5] M. Eisencraft, R. D. Fanganiello, and L. A. Baccala, "Synchronization of discrete-time chaotic systems in bandlimited channels," *Mathematical Problems in Engineering*, vol. 2009, pp. 1–12, 2009.
- [6] D. Kundur and D. Hatzinakos, "Blind image deconvolution," *IEEE Signal Processing Magazine*, vol. 13, no. 3, pp. 43–64, 1996.
- [7] G. A. Abib and M. Eisencraft, "On the performance of a digital chaos-based communication system in noisy channels," in *Proc. IFAC MICNON, 2015, Saint Petersburg, Russia*, vol. 1, pp. 1–6.
- [8] M. Hénon, "A two-dimensional mapping with a strange attractor," *Communications in Mathematical Physics*, vol. 50, pp. 94–102, 1976.