# Encriptação de Imagem Utilizando Sinais Caóticos

**Rafael Alves da Costa***, **Marcio Eisencraft***
*Escola Politécnica da Universidade de São Paulo, São Paulo, Brasil
e-mail: rcosta@lcs.poli.usp.br

**Introdução:** Um sinal caótico é limitado em amplitude, aperiódico, determinístico e apresenta dependência sensível às condições iniciais (DSCI). Esta última característica implica que se o sistema gerador dos sinais for iniciado com condições iniciais ligeiramente diferentes, os sinais obtidos apresentarão valores completamente distintos após um curto período de tempo. A DSCI é uma característica que torna sinais caóticos fortes candidatos para aplicações em sistemas de comunicação seguros. Nesse trabalho, propõe-se a utilização de um gerador pseudo-aleatório que fornece uma sequência binária a partir um mapa linear por partes [1]. O mapa $f : [-1, 1[ \rightarrow [-1, 1[$ é definido como $s(n+1) = f(s(n))$ em que [1]

$$f(s) = \frac{2s - (\alpha_j + \alpha_{j-1})}{\alpha_j - \alpha_{j-1}}, \quad \text{com} \quad \alpha_{j-1} \leq s < \alpha_j \quad \text{e} \quad j = 1, 2 \ldots, r \geq 2. \tag{1}$$

Esse mapa é ergódico, gera órbitas no domínio $U = (-1, 1)$ e possui densidade invariante uniforme, ou seja, as amostras geradas pelo mapa são uniformemente distribuídas no intervalo $(-1, 1)$. Aplica-se essas ideias em um processo de encriptação de imagem.

**Métodos:** A imagem $I$ utilizada de tamanho $M \times N$ pixels é representada por 3 matrizes $M \times N$ contendo as componentes RGB. Cada elemento dessas matrizes é digitalizado utilizando-se 8 bits. Assim, cada matriz possui $M \times N \times 8$ bits. Utiliza-se o mapa caótico para se gerar uma órbita de comprimento $M \times N \times 8 + 10^3$. Descarta-se os $10^3$ primeiros pontos gerados pelo mapa na tentativa de eliminar o comportamento transitório e gera-se uma sequência de $M \times N \times 8$ de 0s e 1s tomando-se o sinal das amostras restantes. Realiza-se então a operação XOR entre a sequência pseudoaleatória gerada pelo mapa e cada uma das matrizes associadas com a imagem. Em seguida, cada vetor de pixels é reconstruído. Na recuperação da imagem realiza-se o processo inverso. Nota-se que a chaves de encriptação são a condição inicial e os parâmetros do mapa utilizado [1].

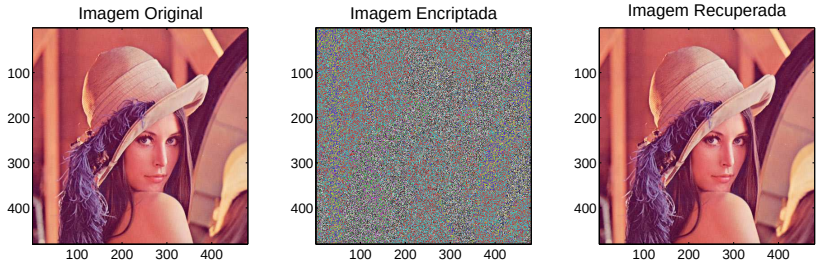


Figura 1 – Imagem Encriptada utilizando o modelo proposto

**Resultados:** Realizamos simulações com a condição inicial $s(0) = 0.731579999$ e parâmetros do mapa $\alpha_1 = -0.5$, $\alpha_2 = 0.001$, $\alpha_3 = 0.5$ como chaves de encriptação. Na Figura 1 temos a imagem original '*Lenna*' jpeg com $480 \times 480$ pixels, a imagem encriptada utilizando o algoritmo proposto e a imagem recuperada.

**Conclusão:** O algoritmo proposto realizou a encriptação conforme esperado, entretanto, estudos sobre o efeito de precisão finita na implementação do mapa, em sua condição inicial e parâmetros necessitam de mais estudos. Além disso, técnicas de embaralhamento dos pixels baseados na órbita caótica gerada podem ser implementadas para tornar a encriptação mais robusta como em [2]. Pretende-se em trabalhos futuros realizar testes estatísticos do gerador pseudo-aleatório e da imagem encriptada [2].

**Referências:** [1] Costa RA et al. Correlation and spectral properties of chaotic signals generated by a piecewise-linear map with multiple segments, Signal Processing, 2017. [2] Zhou Y, et al. A new 1d chaotic system for image encryption, Signal Processing, 2014.