USO DO MAPA CAÓTICO PWLCM PARA A CIFRAGEM DE IMAGENS

JOÃO INÁCIO MOREIRA BEZERRA[1]; ALEXANDRE MOLTER;[3]
VINÍCIUS VALDUGA DE ALMEIDA CAMARGO[3]
[1]Universidade Federal de Pelotas – jimbezerra@inf.ufpel.edu.br
[3]Universidade Federal de Pelotas – alexandre.molter@ufpel.com.br
[3]Universidade Federal de Pelotas – vvacamargo@inf.ufpel.edu.br

1. INTRODUÇÃO

Nas últimas décadas, em virtude dos avanços tecnológicos, a maioria das comunicações ocorre em redes públicas, como é o caso da internet (MURILLO-ESCOBAR et al., 2015), aumentando a importância da criptografia, pois os arquivos transmitidos estão propensos a sofrerem ataques. O formato de arquivo mais utilizado atualmente são imagens, e por isso, os algoritmos criptográficos devem ser construídos focados na cifragem de imagens (FAN et al., 2018).

Algoritmos tradicionais, de chave privada, como o DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*) e IDEA (*International Data Encryption Algorithm*) foram desenvolvidos focados na cifragem de textos (CHAI et al., 2019) e não são adequados para a cifragem de imagens pelas seguintes razões:

- Alta correlação entre pixeis adjacentes;
- Alto consumo de potência;
- Tamanho dos arquivos.

Nesse contexto, a Teoria do Caos aparece como uma alternativa promissora para a criptografia, atraindo considerável interesse de pesquisadores (MURILLO-ESCOBAR et al., 2015; CHAI et al., 2019; MOREIRA BEZERRA et al. 2021.), em virtude de características da Teoria do Caos que se relacionam com a criptografia, como mostra a Tabela 1 abaixo.

Propriedade Caótica	Propriedade Criptográfica	Descrição
Ergodicidade	Confusão	A saída é uniforme independentemente da entrada
Sensibilidade às Condições Iniciais	Difusão	Uma pequena mudança na entrada gera uma mudança significativa na saída.
Dinâmicas determinísticas	Pseudo-aleatoriedade randômica	Um processo determinístico pode gerar comportamento pseudo-aleatório.
Estruturas complexas	Complexidade de Algoritmos	Um processo simples computacionalmente possui alta complexidade teórica.

Tabela 1: Relação entre as propriedades da Teoria do Caos e da Criptografia (ALVAREZ; LI, 2006).

Para a aplicação da Teoria do Caos na criptografia, é necessário prestar atenção nas características dos sistemas, em especial se é de tempo discreto ou contínuo, para minimizar o consumo de tempo das simulações computacionais, de forma com que seja possível seu uso em aplicações de tempo real. Além disso, o sistema caótico utilizado necessita ser robusto, ou seja, apresentar comportamento caótico independentemente do valor do parâmetro. Neste trabalho, é apresentado o *Piecewise Linear Chaotic Map* (PWLCM) como opção para a criptografia com caos, mostrando que ele é robusto, por meio dos expoentes de Lyapunov, e que possui baixo consumo de tempo, ao realizar a comparação do consumo de tempo nas iterações do PWLCM e na resolução numérica de um sistema tempo contínuo.

2. METODOLOGIA

Neste trabalho, é realizada a comparação entre o tempo necessário para iterar um sistema de tempo discreto e resolver numericamente um sistema de tempo contínuo. O sistema de tempo discreto é o *Piecewise Linear Chaotic Map* (PWLCM), apresentado por ALVAREZ (2006), que é definido por:

$$f(x_n) = x_{n+1} = \begin{cases} \dfrac{x_n}{p}, x_n \in (0, p) \\ \dfrac{1 - x_n}{1 - p}, x_n \in (p, 1) \end{cases}$$

em que x_n é a variável do sistema e p é o parâmetro de controle.

Para verificar se um sistema é caótico, usam-se Expoentes de Lyapunov, que para um sistema de tempo discreto é dado pela equação abaixo, e para o sistema ser caótico, é necessário que $\lambda > 0$.

$$\lambda = \lim_{n \to \infty} \left| \frac{1}{n} \sum_{i=0}^{n-1} \ln(|f'(x_i)|) \right|$$

Quanto ao sistema de tempo contínuo, o sistema de Lorenz (1963) é utilizado, um sistema tri-dimensional, que é dado pelas seguintes equações:

$$\begin{cases} \dot{X} = \sigma(Y - X), \\ \dot{Y} = -XZ + \rho X - Y, \\ \dot{Z} = XY - \beta Z. \end{cases}$$

Em que X, Y e Z são as variáveis do sistema enquanto α, β e ρ são os parâmetros do sistema. Para os efeitos da comparação do tempo das iterações do sistema de tempo discreto com o tempo para resolver numericamente o sistema de tempo contínuo, para o PWLCM será usado $p = 0{,}3$, enquanto para o sistema de Lorenz, tem-se $\sigma = 10, \beta = \frac{8}{3}, \rho = 48$.

3. RESULTADOS E DISCUSSÃO

O primeiro requisito para um sistema caótico ser usado para aplicações criptográficas é a robustez, ou seja, há a necessidade do sistema ser caótico independente dos seus parâmetros de controle, como é *p* no PWLCM. Na Figura 1 abaixo, calcula-se os expoentes de Lyapunov para $p \in (0{,}1)$ no PWLCM, e como para todos os valores de *p*, $\lambda > 0$, o requisito de robustez é satisfeito.

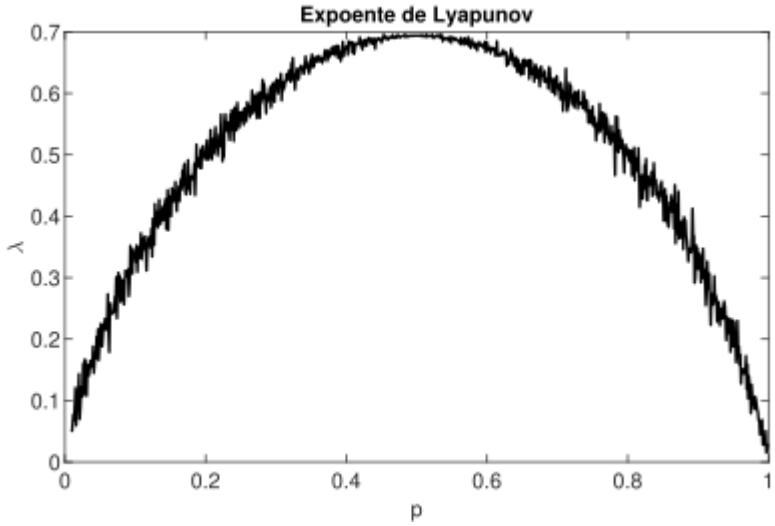

Figura 1: Expoentes de Lyapunov para o PWLCM.

Para um processo criptográfico ser eficiente, a solução das iterações do mapa ou sistema caótico precisa ser rápida. Na tabela 2, é exposto o tempo necessário para iterar o PWLCM, em função do número de iterações, e também o tempo necessário para resolver este mesmo número de iterações do sistema de Lorenz. Nesta tabela, mostra-se que iterar o PWLCM, um sistema de tempo discreto, é consideravelmente mais rápido do que resolver o sistema de Lorenz, um sistema de tempo contínuo, em virtude de não haver a necessidade do uso de métodos numéricos, tais como o método de Runge-Kutta de quarta ordem, que possui alto custo computacional e aumenta o tempo necessário para resolver o sistema.

Número de iterações	PWLCM	Sistema de Lorenz	4 conjuntos de iterações do PWLCM
256×256	0,0058s	0,88s	0,018s
$2 \times 256 \times 256$	0,0089s	1,40s	0,03s
512×512	0,01s	2,67s	0,04s
$2 \times 512 \times 512$	0,02s	5,61s	0,07s

Tabela 2: Comparação do tempo necessário para iterar o PWLCM como o tempo necessário para resolver o sistema de Lorenz.

No trabalho de CHEN et al. (2019), defende-se o uso de sistemas de ordem superior com o argumento de que como possui mais variáveis, mais sequências caóticas podem ser geradas em cada solução do sistema, assim minimizando o consumo de tempo. Contudo, na terceira coluna da tabela 2, mostra-se que o tempo necessário para iterar os 4 conjuntos de iterações separadas do PWLCM ainda é consideravelmente menor que o tempo necessário para resolver um sistema como o de Lorenz, de tempo contínuo.

No trabalho de MOREIRA BEZERRA (2021), o PWLCM foi usado para gerar as sequências caóticas, e o baixo tempo das iterações deste sistema fez com que

o cifrador proposto apresentasse *throughput* superior a outros trabalhos propostos na literatura. Ademais, a robustez deste mapa fez o cifrador passar todos os testes de segurança, e assim, ser seguro contra as mais variadas formas de ataque.

4. CONCLUSÕES

Neste trabalho, o contexto atual da criptografia, em que há a necessidade de novas estratégias pensando na cifragem de imagens, foi citado, considerando que a teoria do Caos fornece um caminho promissor, e apresentando o mapa caótico PWLCM como um sistema caótico que atende os requisitos criptográficos. O expoente de Lyapunov foi usado para mostrar que este mapa apresenta comportamento robusto, a além disso, foi feita a comparação entre o tempo necessário para iterar este sistema com a resolução numérica de um sistema de tempo contínuo, mostrando-se que sistemas de tempo discreto são mais rápidos, assim permitindo melhor performance e possibilitando ainda o seu uso em aplicações de tempo-real.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ALVAREZ, Gonzalo; LI, Shujun. Some basic cryptographic requirements for chaos-based cryptosystems. **International journal of bifurcation and chaos**, v. 16, n. 08, p. 2129-2151, 2006.

CHAI, Xiuli; FU, Xianglong; GAN, Zhihua; LU, Yang; CHEN, Yiran. A color image cryptosystem based on dynamic DNA encryption and chaos. **Signal Processing**, v. 155, p. 44-62, 2019.

FAN, Haiju; LI, Ming; LIU, Dong; AN, Kang. Cryptanalysis of a plaintext-related chaotic RGB image encryption scheme using total plain image characteristics. **Multimedia Tools and Applications**, v. 77, n. 15, p. 20103-20127, 2018.

LORENZ, Edward N. Deterministic nonperiodic flow. **Journal of atmospheric sciences**, v. 20, n. 2, p. 130-141, 1963.

MAY, Robert M. Simple mathematical models with very complicated dynamics. **The Theory of Chaotic Attractors**, p. 85-93, 2004.

MURILLO-ESCOBAR, Miguel Angel; CRUZ-HERNANDEZ, Cesar; ABUNDIZ-PEREZ, Fausto; LOPEZ-GUTIÉRREZ, Rosa Martha. A RGB image encryption algorithm based on total plain image characteristics and chaos. **Signal Processing**, v. 109, p. 119-131, 2015.

MOREIRA BEZERRA, João Inácio; MOLTER, Alexandre; CAMARGO, Vinícius Valduga de Almeida. A new efficient permutation-diffusion encryption algorithm based on a chaotic map. **Chaos, Solitons & Fractals.** v.151, 2021. https://doi.org/10.1016/j.chaos.2021.111235.