USO DE UM MAPA CAÓTICO DE ESPAÇO DISCRETO PARA A CIFRAGEM DE IMAGENS

JOÃO INÁCIO MOREIRA BEZERRA[1]; ALEXANDRE MOLTER;[2]
VINÍCIUS VALDUGA DE ALMEIDA CAMARGO [2]
RAFAEL IANKOWSKI SOARES[2]
[1]*Universidade Federal de Pelotas – jimbezerra@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – alexandre.molter@ufpel.com.br*
[2]*Universidade Federal de Pelotas – vvacamargo@inf.ufpel.edu.br*
[2]*Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br*

1. INTRODUÇÃO

Nas últimas décadas, em virtude dos avanços tecnológicos, o uso de dispositivos de Internet das Coisas (IoT) vem crescendo de forma exponencial. (SHAFIQUE, 2020). Estes dispositivos estão conectados à Internet, que é um canal não seguro, de forma que os arquivos a serem transmitidos estão propensos a sofrerem ataques. A criptografia é a ciência que justamente estuda como proteger arquivos transmitidos em redes públicas de ataques por partes não autorizadas, então neste contexto sua importância é aumentada. Os arquivos mais transmitidos são imagens, de forma que um cifrador deve ser otimizado para a cifragem de imagens.

O algoritmo de criptografia simétrica mais utilizado é o AES (*Advanced Encryption Standard*), que é otimizado para a cifragem de textos (CHAI et al., 2019), não sendo otimizado para a cifragem de imagens pelas seguintes razões:

- alta correlação entre *pixels* adjacentes;
- alto consumo de potência;
- tamanho dos arquivos.

A Teoria do Caos atrai atenção significante dos pesquisadores (CHAI et al., 2019; TEH, 2019; LAMBIC, 2020; TALHAOUI, 2021), em virtude de apresentar propriedades semelhantes à criptografia, tais como à sensibilidade às condições iniciais, ergodicidade, dinâmicas determinísticas e a possibilidade de obtenção de comportamento matemático complexo com implementações de baixo custo computacional. Cada arquivo de imagem é uma matriz bi-dimensional, no caso de imagens em preto e branco, e tridimensional, no caso de mensagens coloridas, e cada elemento da matriz é denominado um *pixel* da imagem. A cifragem de imagens é baseada em uma arquitetura de permutação-difusão, sendo que na permutação os *pixels* são embaralhados, enquanto na difusão seus valores são trocados por intermédio de uma função. Na criptografia com caos, em geral, sequências caóticas são geradas para a realização destas operações.

Na maioria dos trabalhos de criptografia caótica propostos na literatura, o desempenho em termos de *throughput,* que é a taxa de transmissão do cifrados em *Megabytes* (MB) por segundo, é adequado para imagens de baixa qualidade, mas insuficiente para a transmissão de imagens de alta definição. Isso se dá em virtude de fatores como a realização de operações de permutação e difusão separadas ou acesso a memória ineficiente, contudo, o principal motivo é o uso da aritmética de ponto flutuante (TEH, 2019), a qual possui um alto custo computacional se comparada à aritmética de ponto fixo. de forma com que o destaque teórico da criptografia com caos ainda não se transformou em destaque prático na comunidade criptográfica. Além disso, mapas caóticos implementados com aritmética de ponto flutuante apresentam efeito transiente (BEZERRA, 2021,

TALHAOUI, 2021), que significa que um número de iterações de um mapa deve ser aplicado antes da dinâmica caótica aparecer, e degradação dinâmica (LAMBIC, 2021), pois os valores decimais, representados pela aritmética de ponto flutuante, são representados por conjuntos binários finitos na máquina, com uma representação que não é exata, implicando que ao longo de um número alto de iterações do mapa, a dinâmica caótica é perdida, havendo a necessidade de transformações para lidar com este problema.

Com um mapa caótico implementado com a aritmética de ponto fixo, nem o efeito transiente nem a degradação dinâmica estão presentes. Em virtude disso, este trabalho apresenta um mapa de tempo e espaço discreto, ou seja, um mapa que apresenta apenas valores inteiros, como opção para gerar as sequências caóticas na cifragem de imagens de alta definição.

2. METODOLOGIA

Neste trabalho, é realizada a comparação entre o tempo necessário para iterar um sistema de espaço contínuo, representado por valores reais, que é o *Piecewise Linear Chaotic Map* (PWLCM), ou Mapa Linear Caótico Definido por Partes, apresentado por ALVAREZ(2006), com o sistema de espaço discreto, representado por valores inteiros, proposto por LAMBIC(2020).

O PWLCM é definido de acordo com a equação (1) que segue:

$$f(x_n) = x_{n+1} = \frac{x_n}{p}, x_n \in (0, p]; \ \frac{1-x_n}{1-p}, x_n \in (p, 1), \quad (1)$$

em que x_n é a variável do sistema e p é o parâmetro de controle. Em virtude da imagem ser composta por números inteiros, cada valor do mapa caótico precisa ser transformado para inteiro, de acordo com a função (2) que segue:

$$h(x_n) = [2^{33} \times x_n] mod\ 256. \quad (2)$$

Além disso, a perturbação pela equação (3) é aplicada a cada 100 valores do PWLCM, para anular o efeito da degradação dinâmica:

$$p = (p + x_n)\ mod\ 1. \quad (3)$$

A definição do mapa de tempo discreto, considerando a implementação de 32 *bits,* é dada pela equação (4) que segue.

$$f(x_n) = x_{n+1} = (z << (z\%32)) | (z >> (32 - z\%32)), \quad (4)$$

$$z = (2^{-16} x_n + 1) \times (x_n \%2^{16} + 1) + 1.$$

Nesta definição, x_n é a variável do sistema, e não há variável de controle. Embora sem parâmetro de controle, o estudo do comportamento do mapa realizado por LAMBIC(2020) mostrou que o mapa não apresenta pontos fixos, e assim o mapa apresenta comportamento caótico independentemente de qual for sua condição inicial. Além disso, como cada pixel possui *8 bits*, enquanto cada valor caótico possui *32 bits*, o número de iterações do mapa caótico necessário para gerar as sequência de permutação e difusão é apenas um quarto do valor necessário para o PWLCM.

3. RESULTADOS E DISCUSSÃO

Visando maximizar a efetividade do processo de geração das sequências caóticas, na Tabela 1, é realizada a comparação do tempo necessário para resolver as iterações do PWLCM, que é o mapa implementado com ponto

flutuante que apresenta melhor desempenho (MOREIRA BEZERRA et. al., 2021) com o tempo necessário para resolver as iterações do mapa de tempo discreto. As comparações foram realizadas para as implementações em linguagem C, em um sistema com Windows 11, 8 GB de RAM, e processador Intel Core de 11ª geração, e CPU de frequência entre 2.4 e 2.42 GHz.

Classificação da Imagem	Dimensão (*pixels*)	Tempo para resolver o PWLCM(s).	Tempo para resolver o mapa discreto(s).
SD	640 x 480 x 3	0,01	$< 10^{-6}$
HD	720 x 480 x 3	0,02	$< 10^{-6}$
Full HD	1920 x 1080 x 3	0,08	0,02
4K Ultra HD	3840 x 2160 x 3	0,31	0,05
Full Ultra HD	7680 x 4320 x 3	1,20	0,20

Tabela 1: Comparação do tempo necessário para iterar o PWLCM com o tempo necessário iterar o mapa discreto de LAMBIC (2020).

A tabela mostra que o uso do mapa discreto causa uma redução de aproximadamente seis vezes no tempo necessário para a geração das sequências caóticas, em virtude de as operações com ponto fixo serem menos custosas, a perturbação das sequências não serem necessárias, e o menor número de iterações necessário para gerar a sequência. Aproveitando este resultado, o cifrador de permutação-difusão simultânea proposto por MOREIRA BEZERRA (2021) que foi implementado com o uso do mapa discreto ao invés do PWLCM, com resultados resumidos a seguir.

- A implementação original (MOREIRA BEZERRA, 2021) teve um *throughput* de 9,36 MB/s, um pouco inferior ao *throughput* de 14,25 obtido por TALHAOUI (2021), embora este tenha usado uma máquina de desempenho superior.
- Com o mapa discreto, o *throughput* subiu para 220,3 MB/s, métrica 15,74 vezes superior à de TALHAOUI (2021), de forma que uma imagem Full Ultra HD pode ser cifrada em 0,45 segundos. Esse *throughput* é também 74 vezes superior à melhor implementação sequencial do AES, de Zhang (2018), que apresenta um *throughput* de aproximadamente 3 MB/s.
- Usando o mapa discreto, o cifrador também foi implementado em um dispositivo Raspberry Pi 3 Modelo B, apresentando um *throughput* de 18,67 MB/s, significativamente superior ao melhor resultado obtido anteriormente na literatura, de 1,60 MB/s por GARCIA-GUERRERO (2020). A implementação foi festa neste dispositivo em virtude de seu difundido uso em aplicações de baixo custo de Internet das Coisas.

4. CONCLUSÕES

Este trabalho apresentou o uso de um mapa discreto implementado com arquitetura de ponto fixo como melhor alternativa para a geração de sequências caóticas, que é a operação que consome mais tempo em um algoritmo criptográfico. Foi realizada a comparação do consumo de tempo deste mapa com o mapa PWLCM, implementado em uma arquitetura de ponto flutuante, e houve uma redução média de seis vezes no tempo necessário para gerar as sequências caóticas, o que causou um aumento ainda mais significativo no *throughput* do algoritmo criptográfico. Dessa forma, o cifrador apresentado por MOREIRA BEZERRA(2021) passa a ter a capacidade de transmissão de imagens Full Ultra HD em 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.

GARCÍA-GUERRERO, E. E. et al. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. **Chaos, Solitons & Fractals**, v. 133, p. 109646, 2020.

LAMBIĆ, Dragan. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. **Nonlinear Dynamics**, v. 100, n. 1, p. 699-711, 2020.

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.

MOREIRA BEZERRA, J. I. **Um novo algoritmo de criptografia de alto desempenho baseado em modelos caóticos**. 24 de nov de 2021. Dissertação. (Mestrado em Modelagem Matemática) - PPGMMat, UFPel.

SHAFIQUE, Kinza et al. Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. **Ieee Access**, v. 8, p. 23022-23040, 2020.

TALHAOUI, Mohamed Zakariya; WANG, Xingyuan. A new fractional one dimensional chaotic map and its application in high-speed image encryption. **Information Sciences**, v. 550, p. 13-26, 2021.

TEH, Je Sen; TAN, Kaijun; ALAWIDA, Moatsum. A chaos-based keyed hash function based on fixed point representation. **Cluster Computing**, v. 22, n. 2, p. 649-660, 2019.