ALGORITMO DE CIFRAGEM DE IMAGENS PARA APLICAÇÕES IOT BASEADO EM MAPAS CAÓTICOS

GUSTAVO DA SILVA MACHADO[1]; JOÃO INÁCIO MOREIRA BEZERRA[2]; RAFAEL IANKOWSKI SOARES[3]; VINÍCIUS VALDUGA DE ALMEIDA CAMARGO[4]

[1]Universidade Federal de Pelotas– gdsmachado@inf.ufpel.edu.br
[2]Universidade Federal de Pelotas – jimbezerra@inf.ufpel.edu.br
[3]Universidade Federal de Pelotas – rafael.soares@inf.ufpel.edu.br
[4]Universidade Federal de Pelotas – vvacamargo@inf.ufpel.edu.br

1. INTRODUÇÃO

Atualmente cada vez mais é gerado e transmitido mídias digitais pela internet, tais como arquivos e imagens, assim necessitando de formas mais eficientes de criptografia para a segurança dos dados, e com o crescimento do desenvolvimento da Internet das Coisas (IoT), tal necessidade também se torna relevante no cenário de dispositivos de baixo custo e desempenho.

Um dos algoritmos mais tradicionais de criptografia é o Advanced Encryption Standard (AES), no entanto, ele não foi desenvolvido e otimizado com foco para cifragem de imagens (TALHAOUI, 2021), os quais representam 70% dos dados transmitidos por IoT (ARAB, 2019), (BEZERRA, 2021). Dessa forma, algoritmos baseados na teoria do caos e suas propriedades tais como sensibilidade às condições iniciais e comportamento pseudo-aleatório complexo, foram tornando-se relevantes para algoritmos de cifragem de imagens (TRUJILLO-TOLEDO, 2021), (BEZERRA, 2021), (TALHAOUI, 2021), (WANG, 2021), (ZHANG, 2020).

A arquitetura dos algoritmos de cifragem de imagens baseados na teoria do caos é normalmente baseada na permutação-difusão dos pixels da imagem (WANG, 2021), (ZHANG, 2020), (PATRO, 2019), (LIU, 2020), onde na permutação, os pixels são embaralhados pela imagem, e na difusão o valor dos pixels são alterados. O algoritmo proposto neste trabalho também utiliza a ideia de permutação-difusão, a qual ocorre simultaneamente, e operando sobre blocos de 4 pixels por vez em comparação ao acesso individual de pixels, assim diminuindo drasticamente o acesso a memória, que é uma das principais preocupações em aplicações de IoT (HAFSA, 2021), (ELSAFTY, 2020).

2. METODOLOGIA

O algoritmo proposto foi construído utilizando o mapa caótico tenda, representado pela equação (1), onde x e p, respectivamente variável de estado e controle, pertencem ao intervalo (0,1).

$$x_{N+1} = F(x_n) = \begin{cases} x_N/p, & x_N \in (0, p), \\ (1-x_N)/(1-p), & x_{nN} \in (p, 1) \end{cases} \quad (1)$$

O processo de permutação e difusão utiliza inteiros positivos, por esse fato, os valores caóticos gerados pela equação (1) são convertidos de reais para inteiros pela equação (2), onde V é o maior inteiro positivo que queremos que os valores caóticos assumam.

E para evitar degradação dinâmica dos valores caóticos,uma preocupação proveniente da precisão finita de 64 bits da Raspberry Pi 3 (LI, 2018), a cada 1000 iterações do mapa, perturbações da equação (3) são aplicadas. Testes NIST foram aplicados após as perturbações, confirmando que elas são eficientes em fazer o mapa caótico ser resistente a degradações dinâmicas.

$$h(x) = [(2^{33})*x] \bmod V, \quad (2)$$

$$p = \mathrm{mod}(p + x(i), 1). \quad (3)$$

O processo de cifragem para imagens em escala cinza é feito em blocos, recebendo uma imagem M x N, então o algoritmo divide a imagem em blocos de 4 pixels com o objetivo de reduzir tanto o acesso à memória, quanto para utilizar menos interações do mapa caótico. Esse processo utiliza dois mapas caóticos baseados na equação (1): xP, para as operações de permutação e xD, para as operações de difusão.

Dessa forma, as chaves secretas utilizadas são xP0 e pP, para o mapa Xp e xD0 e pD para o mapa xD, além da função SHA-256, que é utilizada para criar dependência entre a imagem original e as sequências caóticas e um valor de 32 bits Cin utilizado na operação de difusão.

O procedimento de cifragem pode ser dividido em 7 etapas:

Etapa 1: A imagem original é carregada.

Etapa 2: A função SHA-256 é aplicada, gerando a sequência S de 256 bits.

Etapa 3: As chaves secretas são perturbadas utilizando-se da sequência S gerada na etapa 2.

Etapa 4: A imagem é dividida em blocos de 4 pixels, sendo o número de blocos Nb = (M x N) / 4.

Etapa 5: Para evitar efeitos transientes, 50 interações de cada mapa são resolvidas (BEZERRA, 2021).

Etapa 6: Nb sequências caóticas Xp e Xd são geradas, e então quantizadas pela equação (4).

$$hP(i) = [233 \times xP(i)] \bmod (Nb - i), \quad (4)$$

$$hD(i) = [2^{33} \times xD(i)] \bmod 2^{32}$$

Etapa 7: O processo simultâneo de permutação-difusão é executado. Ele é definido pela equação (5), sendo $E(-1) = Cin$ and $i \in [0, Nb - 1]$, e E sendo a imagem cifrada gerada.

$$B(i) \Leftrightarrow B(hP(i)), \quad (5)$$

$$E(i) = B(i) \oplus hD(i) \oplus E(i - 1).$$

O procedimento de decifragem é fundamentalmente o de cifragem invertido, com 2 diferenças: o valor da função SHA-256 é transferido no protocolo de troca de chaves, assim a etapa 2 não é executada; a etapa 7 é aplicada de forma inversa, isto é, do último bloco até o primeiro bloco da imagem.

Testes de segurança contra ataques estatísticos, diferenciais, de forma bruta, ruído, oclusão e informação escolhida foram executados, demonstrando a segurança do algoritmo proposto.

3. RESULTADOS E DISCUSSÃO

O algoritmo proposto foi executado em uma Raspberry Pi 3 Model B, a qual dispõe de uma CPU de 1.2 GHz e 1 GB de memória ram.

O tempo médio de cifragem de uma imagem com apenas um canal de cor (imagem preto e branco), de dimensões 256 x 256, com pixels de 8 bits, foi de 7.105 ms, o que corresponde a um throughput de 9,224 MB/s. Os resultados com testes com imagens de outros tamanhos são apresentados na tabela 1 a seguir.

E comparações com outros algoritmos caóticos de cifragem de imagem propostos na literatura são mostradas na tabela 2 a seguir, os quais evidenciam a superioridade do algoritmo proposto neste trabalho.

Tabela 1: Tempo computacional e throughput do algoritmo de cifragem.

Dimensão da Imagem	Tempo de cifragem (ms)	Throughput(MB/s)
256 x 256	7,105	9,224
512 x 512	29,78	8,803
1024 x 1024	140,579	7,459
2048 x 2048	638,277	6,571

Tabela 2: Comparação de throughput com outros algoritmos de cifragem propostos.

Trabalho	Dispositivo	Thoughput (MB/s)
Proposto	Raspberry Pi 3	9,224
(GARCÍA-GUERRERO, 2020)	MCU PIC 16F877A	1,600
(TRUJILLO-TOLEDO, 2021)	Raspberry Pi 4	1,320
(ZHANG, 2018)	QT interface	0,550

4. CONCLUSÕES

Este trabalho apresentou um algoritmo de cifragem de imagens caótico que utiliza permutação e difusão simultânea e o comparou com outros algoritmos de cifragem de imagens caóticos quando executado em plataformas de IoT, além de resultados demonstrando a segurança da arquitetura apresentada.

Assim, pelo seu baixo tempo de execução e alta segurança, o algoritmo proposto demonstra-se viável para cifragem de imagens em dispositivos IoT.

5. REFERÊNCIAS BIBLIOGRÁFICAS

TRUJILLO-TOLEDO, D. A. et al. Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. **Chaos, Solitons & Fractals**, v. 153, p. 111506, 2021.

ARAB, Alireza; ROSTAMI, Mohammad Javad; GHAVAMI, Behnam. An image encryption method based on chaos system and AES algorithm. **The Journal of Supercomputing**, v. 75, n. 10, p. 6663-6682, 2019.

BEZERRA, João Inácio Moreira; DE ALMEIDA CAMARGO, Vinícius Valduga; MOLTER, Alexandre. A new efficient permutation-diffusion encryption algorithm based on a chaotic map. **Chaos, Solitons & Fractals**, v. 151, p. 111235, 2021.

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.

WANG, Xingyuan; YANG, Jingjing; GUAN, Nana. High-sensitivity image encryption algorithm with random cross diffusion based on dynamically random coupled map lattice model. **Chaos, Solitons & Fractals**, v. 143, p. 110582, 2021.

ZHANG, Yong et al. Plaintext-related image encryption algorithm based on perceptron-like network. **Information Sciences**, v. 526, p. 180-202, 2020.

PATRO, K. Abhimanyu Kumar; ACHARYA, Bibhudendra. An efficient colour image encryption scheme based on 1-D chaotic maps. **Journal of Information Security and Applications**, v. 46, p. 23-41, 2019.

LIU, Lidong; LEI, Yuhang; WANG, Dan. A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation. **IEEE access**, v. 8, p. 27361-27374, 2020.

HAFSA, Amal et al. FPGA implementation of improved security approach for medical image encryption and decryption. **Scientific Programming**, v. 2021, 2021.

ELSAFTY, Abdulaziz H. et al. Enhanced hardware implementation of a mixed-order nonlinear chaotic system and speech encryption application. **AEU-International Journal of Electronics and Communications**, v. 125, p. 153347, 2020.

LI, Chengqing et al. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. **IEEE multimedia**, v. 25, n. 4, p. 46-56, 2018.

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.

ZHANG, Yong. Test and verification of AES used for image encryption. **3D Research**, v. 9, n. 1, p. 1-27, 2018.