Criação de Chaves Criptográficas Usando Entropia de Pixels de Imagens

Artur Steinbrecher Bujes
UDC
Foz do Iguaçu, Brasil
artursteinbrecher@outlook.com

Luciano Santos Cardoso
UDC
Foz do Iguaçu, Brasil
luciano.cardoso@udc.edu.br

Alessandra Bussador
UDC
Foz do Iguaçu, Brasil
alessandra@udc.edu.br

***Abstract*—The security of digital systems depends on the robustness of cryptographic keys. Traditional approaches to key generation, often based on pseudo-random algorithms, may present vulnerabilities due to predictable patterns or low entropy. This work seeks to analyze the feasibility of using pixel variations in digital images as a source of entropy for generating cryptographic keys. A Python prototype is planned to be developed to capture frames from video cameras, process pixel values into hexadecimal sequences, and apply cryptographic functions. Preliminary analysis indicate that visual randomness provides high entropy and resistance to brute-force attacks, suggesting an accessible solution for digital security .**

***Keywords*—Cryptography; Entropy; Security.**

***Resumo*—A segurança digital depende fortemente da robustez das chaves criptográficas. Métodos tradicionais de geração de chaves, baseados em algoritmos pseudoaleatórios, podem apresentar vulnerabilidades devido a padrões previsíveis ou baixa entropia. Este trabalho busca analisar a viabilidade de utilizar variações de pixels em imagens digitais como fonte de entropia para geração de chaves criptográficas. Planeja-se desenvolver um protótipo em Python capaz de capturar quadros de vídeo, processar os valores dos pixels em sequências hexadecimais e aplicar funções criptográficas. As análises preliminares indicam que a aleatoriedade visual oferece alta entropia e resistência a ataques de força bruta, sugerindo uma solução acessível para segurança digital.**

***Palavras-chave*—Criptografia; Entropia; Segurança.**

I. Introdução

A segurança da informação depende de forma crítica da geração de chaves criptográficas capazes de resistir a ataques sofisticados. Contudo, métodos tradicionais de geração de chaves frequentemente utilizam algoritmos determinísticos ou pseudoaleatórios que podem apresentar padrões previsíveis, reduzindo a entropia e expondo vulnerabilidades exploradas por atacantes [1].

Nesse cenário, cresce a necessidade de buscar novas fontes de aleatoriedade que possam reforçar a segurança dos sistemas digitais. Enquanto alguns métodos utilizam dispositivos ou técnicas específicas para gerar dados imprevisíveis, a utilização de imagens digitais ainda é pouco explorada de forma acessível, apesar da ampla disponibilidade de câmeras em computadores e celulares atuais.

Este trabalho propõe a utilização da variabilidade natural de pixels em imagens digitais como fonte de entropia. Tal abordagem combina acessibilidade tecnológica, escalabilidade e aplicabilidade prática, contribuindo para mitigar uma das principais fragilidades atuais: a previsibilidade na geração de chaves criptográficas.

II. Fundamentação Teórica

A. Segurança da Informação e Criptografia

A segurança da informação constitui um dos pilares fundamentais das sociedades digitais, sendo responsável por garantir que dados sensíveis possam ser transmitidos, processados e armazenados de forma segura. Essa segurança é tradicionalmente representada pelo tríplice CID (Confidencialidade, Integridade, Disponibilidade), que também inclui a autenticidade, a auditabilidade e a legalidade da informação [2].

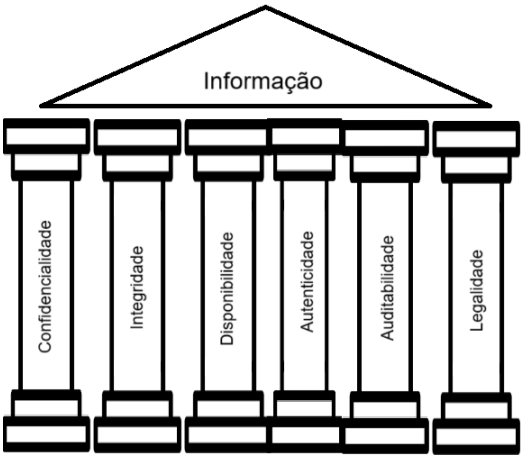

Fig. 1. Pilares da Informação

Nesse contexto, a criptografia emerge como ferramenta central para proteção de dados. Por meio da aplicação de algoritmos matemáticos, a criptografia converte informações em formatos cifrados, tornando-os inteligíveis apenas para aqueles que detêm a chave correta [2]. Essa técnica é amplamente empregada em áreas críticas, como autenticação de usuários, transações financeiras, comunicações militares e protocolos de rede.

Entre os principais modelos, destacam-se:

- **Criptografia simétrica:** a mesma chave é utilizada para cifrar e decifrar os dados. Efetiva em desempenho, porém apresenta riscos no compartilhamento seguro da chave.
- **Criptografia assimétrica:** utiliza pares de chaves pública e privada. Mais segura para distribuição, porém exige maior capacidade computacional.

B. Vulnerabilidades na Geração de Chaves

Embora os algoritmos criptográficos modernos sejam reconhecidamente seguros, a robustez de um sistema depende em grande parte da qualidade das chaves utilizadas. Geradores pseudoaleatórios, frequentemente embutidos em softwares de propósito geral, podem apresentar padrões previsíveis e falhas estatísticas que reduzem o nível de entropia [3]. Esse cenário facilita a exploração por meio de ataques de força bruta, análise de frequência ou predição estatística.

De acordo com o relatório OWASP Top 10:2021, falhas criptográficas constituem uma das principais vulnerabilidades exploradas por atacantes em ambientes digitais [1].

C. Entropia e Aleatoriedade

O conceito de entropia, conforme proposto por Claude Shannon, refere-se ao grau de imprevisibilidade ou desordem de um conjunto de dados. No âmbito da segurança digital, quanto maior a entropia associada a uma chave criptográfica, maior sua resistência a ataques [4].

Pesquisas recentes demonstram que geradores quânticos podem atingir níveis de entropia elevados, compatíveis com aplicações críticas em segurança [4], [6]. Contudo, a necessidade de hardware especializado e os custos ainda representam barreiras à implementação em larga escala [7].

D. Imagens Digitais como Fonte de Entropia

O uso de imagens digitais surge como alternativa promissora e acessível para geração de chaves criptográficas. Cada pixel em uma imagem pode ser representado por valores numéricos correspondentes à intensidade de cor em canais RGB. Pequenas variações ambientais (luminosidade, ruído do sensor, movimento) alteram significativamente esses valores, produzindo uma fonte de variabilidade natural.

Quando representados em sequências hexadecimais e processados, os pixels podem ser utilizados como sementes de alta entropia para geração de chaves. Estudos em processamento digital de imagens e esteganografia já exploraram a aleatoriedade contida em padrões visuais, sugerindo que a imprevisibilidade do ambiente visual pode ser explorada em segurança digital [8], [9].

Além disso, a ampla disponibilidade de câmeras em dispositivos como smartphones, notebooks e sistemas embarcados torna essa abordagem escalável e de baixo custo.

E. Técnicas de Reforço da Aleatoriedade

Embora os pixels forneçam variabilidade inicial, é necessário aplicar técnicas de aumento de entropia para eliminar padrões residuais. Funções hash criptográficas, como SHA-256 e BLAKE2, permitem transformar a entrada visual em saídas de alta imprevisibilidade, com distribuição estatística uniforme. Operações adicionais, como XOR bit a bit e deslocamentos binários, também podem contribuir para reduzir correlações e aumentar a segurança [5].

Fig. 2. Funcionamento da Função Hash

III. Metodologia

A pesquisa será conduzida em caráter exploratório e experimental, tendo como foco a construção e validação de um protótipo computacional para geração de chaves criptográficas a partir da entropia de pixels de imagens digitais. Planeja-se estruturar o trabalho em cinco etapas principais:

A. Coleta e Pré-processamento das Imagens

Pretende-se realizar a captura de imagens digitais por meio de câmeras convencionais (webcams e dispositivos móveis), em frente a uma parede branca com diferentes condições de iluminação. A escolha desses dispositivos se justifica pela ampla disponibilidade e baixo custo, favorecendo a replicabilidade da solução. As imagens serão processadas em tempo real com a biblioteca OpenCV, considerando resoluções médias (ex.: 640x480 pixels) para balancear diversidade de dados e desempenho computacional.

B. Extração e Conversão dos Pixels

Planeja-se decompor os quadros capturados em matrizes RGB, de modo que cada pixel seja representado por valores numéricos correspondentes às intensidades das cores primárias, utilizando a biblioteca Pillow. Esses valores serão representados em sequências hexadecimais e, posteriormente, em cadeias binárias. Essa transformação permitirá que a variabilidade natural dos pixels seja utilizada como fonte de entropia.

C. Aumento da Entropia

Nesta etapa, pretende-se aplicar funções hash criptográficas (SHA-256, BLAKE2) via PyCryptodome, além de operações matemáticas (XOR bit a bit, deslocamentos binários) para eliminar padrões residuais. O processamento deverá assegurar que as chaves geradas apresentem distribuição estatística próxima à aleatoriedade ideal.

D. Validação Estatística

Espera-se validar a qualidade das chaves por meio de duas abordagens:

- Cálculo da entropia de Shannon para quantificar o grau de imprevisibilidade;
- Aplicação da suíte NIST SP 800-22 para avaliação de aleatoriedade em contexto criptográfico.

Essas análises confirmarão a robustez estatística das sequências geradas e sua adequação para uso em segurança da informação.

E. Aplicação em Criptografia Simétrica

Planeja-se utilizar as chaves obtidas em algoritmos de criptografia simétrica (ex.: AES-256) para avaliar aplicabilidade prática, desempenho (tempo de processamento) e resistência a ataques de força bruta simulados.

F. Ferramentas e Ambiente de Desenvolvimento

O protótipo será implementado em Python, devido à sua versatilidade e disponibilidade de bibliotecas para manipulação de imagens, estatística e criptografia. Os testes serão realizados em máquinas com sistema operacional Windows para garantir consistência.

IV. Resultados Preliminares

O protótipo desenvolvido, baseado em captura de imagens por webcam, extrai blocos de bytes a partir de subconjuntos aleatórios de pixels e foi avaliado segundo métricas clássicas de entropia informacional. As análises incluíram entropia de Shannon, estimativas conservadoras de min-entropy, estabilidade temporal e sensibilidade a variações ambientais. Os resultados indicaram entropia média entre 6,1 e 7,2 bits por byte, com variação associada principalmente à iluminação e às características do sensor.

Em comparação, os geradores quânticos analisados por Jacak et al. [4] oferecem garantias físicas de imprevisibilidade e exibem valores superiores de min-entropy e estabilidade temporal. Esses dispositivos, quando devidamente calibrados, apresentam desempenho consistente em baterias estatísticas padronizadas (NIST SP 800-22), alcançando taxas de geração próximas a 1 Mb/s e elevadas margens de aleatoriedade.

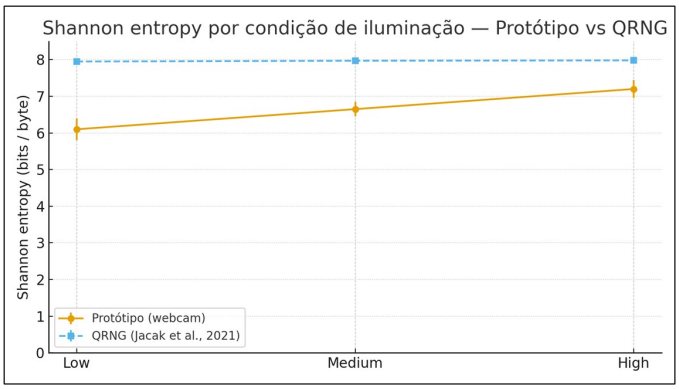

Fig. 3. Gráfico comparativo entre protótipo de geração de chaves criptográficas e Gerador de números verdadeiramente Aleatórios

V. Conclusão

O presente trabalho apresentou e discutiu uma abordagem para geração de chaves criptográficas baseada em variações de pixels de imagens digitais de forma acessível. Os resultados preliminares sugerem que a aleatoriedade visual é capaz de fornecer entropia suficiente para a criação de chaves seguras, resistentes a ataques baseados em análise estatística e compatíveis com padrões internacionais.

Agradecimentos

O autor agradece a sua universidade e ao seu professor orientador pelo suporte técnico e científico.

Referências

[1] OWASP. A02 Cryptographic Failures - OWASP Top 10:2021.
[2] Cleberton Junio Viana et al., “Criptografia e Segurança”, e-Locução, vol. 1, no. 22, 2022.
[3] Gonçalves, E. et al., “Usabilidade e Segurança nos Métodos de Geração de Senhas”, Mackenzie, 2023.
[4] Jacak, M. M. et al., “Quantum generators of random numbers”, *Scientific Reports*, 2021.
[5] Sivanandam, S.; Marimuthu, B.; Alzahrani, A. K., “Entropy Generation in Casson Fluid”, *Entropy*, 2024.
[6] Duda, C. K.; Meier, K. A.; Newell, R. T., “High Min-Entropy Quantum Random Number Generator”, *Entropy*, 2023.
[7] Abderrahmane, A. et al., “MHD Hybrid Nanofluid Mixed Convection Heat Transfer and Entropy Generation”, *Mathematics*, 2022.
[8] Alves, A. C. B.; Tamura, L. H. B.; Navarro, V. S., “IA no auxílio de pessoas daltônicas”, Mackenzie, 2023.
[9] Polachini, M. E., “Detecção de esteganografia em imagens utilizando aprendizado de máquina”, UNESP, 2022.