Cifra De Hill Aplicada Em Imagens

João Kennedy Souza Soares[1], Rafael José Braga Coelho[2]

Instituto Federal do Norte de Minas Gerais (IFNMG) – Campus Montes Claros
Village do Lago I - Rua Dois – 39404-058 – Montes Claros – MG – Brasil

Abstract. This paper presents an image encryption method combining the Hill cipher with an additional transformation to enhance security. It uses a 4x4 key matrix in a modular field of 256, with the inverse calculated using the Gauss-Jordan method. The additional transformation conceals visual patterns, complicating cryptanalysis. Implemented in Python and tested on various images, the method proves effective in recovering the original image.

Resumo. Este artigo apresenta um método de criptografia de imagens que combina a cifra de Hill com uma transformação adicional para aumentar a segurança. A técnica utiliza uma matriz-chave 4x4 em um campo modular de 256, com a inversa calculada pelo método de Gauss-Jordan. A transformação adicional oculta padrões visuais, dificultando a análise da imagem criptografada. O algoritmo foi implementado em Python e testado com imagens de diferentes tamanhos, demonstrando eficácia na recuperação da imagem original.

Palavras–chave: Cifra de Hill, Transformação Adicional, Inversa Modular.

1. Introdução

Com o avanço tecnológico e o aumento da troca de informações digitais, a proteção de dados tornou-se essencial devido à crescente frequência de ataques cibernéticos. Nesse contexto, a criptografia de imagens é fundamental para proteger informações sensíveis em áreas como vigilância e armazenamento seguro. Este trabalho propõe um método de criptografia de imagens que combina a cifra de Hill com uma transformação adicional para melhorar a segurança. Sendo assim, a técnica utiliza uma matriz-chave 4x4, definida em um campo modular, cuja a inversa é calculada pelo método de Gauss-Jordan, permitindo que a mesma matriz seja usada tanto para criptografar quanto para descriptografia.

Além disso, uma transformação adicional baseada em uma equação matemática e multiplicada pela matriz chave, assim aumentando a complexidade do sistema e dificultando a recuperação de traços da imagem original sem a chave correta. Contudo, o algoritmo foi implementado em Python e testado em imagens de diferentes dimensões, ajustadas para o tamanho do bloco da matriz-chave. Desse modo, os resultados demonstram a eficácia oferecendo uma solução prática e segura para a proteção de dados visuais digitais.

2. Metodologia

2.1 Estrutura da Cifra de Hill

A cifra de Hill é uma técnica de criptografia simétrica baseada na multiplicação de blocos de dados por uma matriz-chave, onde a principal vantagem dessa abordagem é a sua robustez matemática, derivada das operações com matrizes e álgebra linear, neste presente trabalho a cifra de Hill é aplicada diretamente sobre as imagens, sendo cada bloco de pixels da imagem tratado como um vetor a ser transformado pela matriz-chave.

Seja P um bloco de dados de imagem com dimensões compatíveis com a matriz chave A, onde o M é o módulo de 256 para representar os valores dos pixels, o processo de criptografia pode ser expresso pela seguinte equação:

$$C = (A \cdot P) \, mod \, M$$

2.2 Matrizes e o Cálculo da Inversa Modular

Uma característica fundamental da cifra de Hill aplicada a imagens é a necessidade de que a matriz-chave A seja invertível no campo modular. Para garantir a descriptografia correta, a matriz A deve possuir uma inversa modular A^{-1}, tal que:

$$A.A^{-1} \equiv I \, mod \, M$$

Onde I é a matriz identidade. A inversa modular é calculada pelo método de Gauss-Jordan adaptado para operações modulares. Nesse processo, a matriz A é aumentada com a matriz identidade I formando $[A|I]$. Em seguida, aplica-se a eliminação gaussiana para escalonar a matriz A, usando operações modulares como multiplicação de linhas por inversos modulares e subtração de múltiplos de linhas. Ao final, a matriz identidade à esquerda é transformada na matriz inversa A^{-1}, que é usada para a descriptografia da imagem.

No contexto da criptografia de imagens, o campo modular é $M = 256M$, que corresponde ao intervalo de valores de um pixel em uma imagem de 8 bits por canal (0 a 255). A inversa modular é então calculada como:

$$A^{-1}.C \equiv P \, mod \; 256$$

2.3 Transformação Adicional

A cifra de Hill é robusta, mas pode deixar traços visuais como áreas homogêneas ou bordas, que criptoanalistas podem explorar. Para aumentar a segurança, aplica-se uma transformação adicional não linear antes da cifra, que altera significativamente os valores dos pixels, dispersando-os de forma complexa e imprevisível. A transformação é definida pela função:

$$f(x, y) = A[x \,\%\, 4, \; y \,\%\, 4] \; * \; (x^2 + y^2 + 5x + 8y)$$

Na qual x e y são as coordenadas dos pixels e A é a matriz-chave 4x4. Essa transformação impede que padrões visuais, como gradientes ou regiões de cores semelhantes, permaneçam após a criptografia, dificultando a análise estatística e a reconstrução da imagem sem a chave correta. Desse modo, ao ajustar os valores RGB de cada pixel com base nessa

função, a transformação oculta os traços visuais da imagem original, combinando essa etapa com a cifra de Hill, obtém-se uma criptografia mais segura e eficaz.

2.4 Processo de Criptografia

O processo de criptografia inicia-se pela leitura da imagem e seu ajuste para que o número de linhas seja múltiplo do tamanho da matriz-chave que é de dimensão 4x4, após isso a imagem é processada em blocos de pixels, onde cada bloco de 4 linhas é criptografado separadamente usando a matriz-chave A. Desse modo, para cada canal de cor (R, G, B), o algoritmo aplica a cifra de Hill, multiplicando os blocos pela matriz A e obtendo os valores criptografados. Onde, C_R C_G e C_B são canais dada por cada equação:

$$C_R = (A \cdot P_R)\ mod\ 256$$

$$C_G = (A \cdot P_G)\ mod\ 256$$

$$C_B = (A \cdot P_B)\ mod\ 256$$

2.5 Processo de Descriptografia

O processo de descriptografia reverte as etapas da criptografia, restaurando a imagem original. Primeiramente, a imagem criptografada é lida e processada em blocos de 4x4 pixels, conforme a matriz-chave. Para cada bloco, aplica-se a inversa modular da matriz-chave A^{-1} usando o campo modular de 256, correspondente aos valores dos pixels em uma imagem de 8 bits, como mostrado abaixo:

$$P = (A^{-1} \cdot C)\ mod\ 256$$

Onde P é o bloco de pixels original, A^{-1} é a matriz inversa modular e C é o bloco criptografado. Esse procedimento é repetido para os três canais de cor (R, G, B). Em seguida, os blocos são recombinados para formar a imagem descriptografada. Por fim, é necessário remover a transformação adicional aplicada antes da criptografia para restaurar a imagem original.

2.6 Remoção da Transformação Adicional

Após a descriptografia dos blocos de pixels utilizando a inversa modular da matriz-chave, é necessário remover a transformação adicional que foi aplicada antes da criptografia para restaurar a imagem original. Desse modo, esse processo envolve subtrair a transformação dos valores de pixels descriptografados, onde $P(x, y)$ é o valor do pixel descriptografado, $T(x, y)$ é o valor da transformação aplicada previamente, e $P'(x, y)$ é o valor do pixel resultante após a remoção da transformação, o que resulta a seguinte fórmula seguinte fórmula:

$$P'(x, y) = (P(x, y) - T(x, y))\ mod\ 256$$

3. Resultados e Discussão

Os testes realizados em imagens de diferentes tamanhos demonstraram a eficácia do método proposto. Visto isso, para ilustrar os resultados, serão apresentadas quatro imagens principais: a imagem original, a imagem passo, a imagem criptografada, e a imagem após a descriptografia. Cada uma dessas etapas será discutida abaixo.

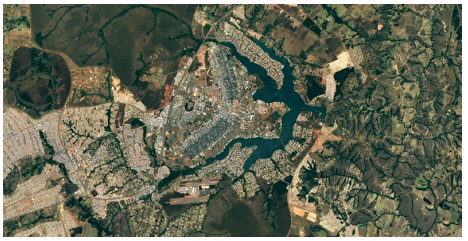

Figura 1. Original de Brasília

A imagem original é a base do processo. Ela contém os pixels organizados de acordo com suas respectivas cores (RGB). Essa imagem inicial, antes da aplicação da cifra de Hill, serve como referência para avaliar a qualidade do processo de criptografia e descriptografia.

$$A = \begin{bmatrix} 3 & 3 & 2 & 5 \\ 4 & 5 & 1 & 2 \\ 6 & 4 & 3 & 1 \\ 5 & 2 & 3 & 4 \end{bmatrix}$$

Matriz chave A tamanho 4 x 4 utilizada para cifrar a imagem.

Figura 2. Transformação

A transformação adicional foi aplicada nessa etapa na qual modifica os valores dos pixels de forma não linear, dispersando padrões visuais como visto anteriormente.

Figura 3. Criptografado

Após a aplicação da Cifra de Hill, os blocos de pixels da imagem original são transformados pela multiplicação com a matriz-chave A. Contudo, o resultado é uma imagem aparentemente sem sentido, onde os pixels foram reorganizados e misturados, tornando difícil identificar qualquer padrão visual ou traços da imagem original sem a chave correta.

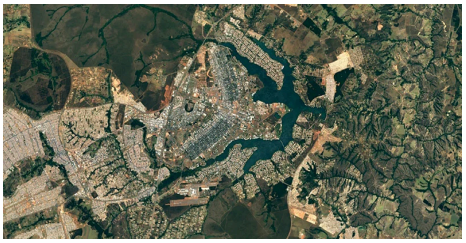

Figura 4. Descriptografado

Após a descriptografia, utilizando a inversa modular da matriz-chave A^{-1}, a imagem original é restaurada. No entanto, a transformação adicional os valores de pixel são inicialmente distorcidos e a remoção dessa transformação devolve os pixels ao seu estado original, recuperando a imagem. Em suma, a imagem descriptografada, após a remoção da transformação, é visualmente idêntica à imagem original onde pequenas diferenças podem existir devido à precisão numérica, mas não é perceptível mostrando a eficácia do algoritmo tanto em proteger os dados da imagem quanto em recuperá-los sem perda de qualidade.

4. Conclusão

Este presente trabalho, desenvolvido em Python, implementou com sucesso o método de Gauss-Jordan para calcular a inversa de matrizes, aplicando-o na criptografia de imagens através da Cifra de Hill, complementada por uma transformação não linear adicional. Diante disso, essa abordagem demonstrou ser eficaz na proteção de dados visuais, garantindo que a imagem criptografada seja completamente irreconhecível, ao mesmo tempo em que permite a recuperação exata da imagem original após o processo de descriptografia e remoção da transformação aplicada. Portanto, a técnica proposta se destaca como uma solução prática e robusta para a criptografia de imagens digitais, assegurando a integridade dos dados visuais.

5. Referências Bibliográfica

ACHARYA, B.; PANIGRAHY, S. K.; PATRA, S. K.; PANDA, G. *Advanced Hill Cipher Algorithm*. 2009. Disponível em: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=9272b0bdf894725ad25ed3df4e420eb83f3cd2d5. Acesso em: 1 set. 2024.

ANTON, H.; RORRES, C. *Álgebra Linear com Aplicaçõe*s. 10a. edição, Bookman, Porto Alegre, 2012.

HERWIG, C., Keeping Earth up to date and looking great. Google Blog, 2016. Disponível em: https://blog.google/products/earth/keeping-earth-up-to-date-and-looking/. Acesso em: 1 set. 2024.

PRERNA, U.; UROOJ, S.; KUMARI, M.; SHRIVASTAVA, J. N., *Image Encryption and Decryption using Modified Hill Cipher Technique*. International Journal of Information and Computation Technology, 2014. Disponível em: https://www.ripublication.com/irph/ijict_spl/ijictv4n17spl_20.pdf. Acesso em: 1 set. 2024.

SUPIYANTO; MANDOWEN, S. A., *Advanced Hill Cipher Algorithm for Security Image Data with the Involutory Key Matrix*. Journal of Physics: Conference Series, vol. 1899, no. 1, 2021, pp. 1-12. Disponível em: https://doi.org/10.1088/1742-6596/1899/1/012116. Acesso em: 1 set. 2024.