JSCE (Journal of System and Computer Engineering)
Vol.6, No.1, January 2025, pp. 101-116
ISSN (online): 2723-1240
DOI : https://doi.org/10.61628/jsce.v6i1.1634

Hill Cipher-Based Visual Cryptography for Copyright Protection of Images Using Flexible Matrix Keys

Veradella Yuelisa Mafula[1,a,*]; Abd. Charis Fauzan[2,b]; Tito Prabowo[3,c]; Muhammad Rizky Ramadhan[4,d]

[12,3,4]Department of Computer Science, Universitas Nahdlatul Ulama Blitar, Indonesia
[a]veradella@unublitar.ac.id, [b]abdcharis@unublitar.ac.id,[c]titoprabowo@unublitar.ac.id, [c]muhrizky0@gmail.com
** Corresponding author*

Abstract

The widespread distribution of digital images on the internet has diminished the copyright protection associated with them. In some cases, copyrighted and economically valuable digital images should not be modified or distributed without permission, as altering the original image can harm its owner. This violation is common, but many internet users are unaware of it. The goal of this research is to protect intellectual property rights of digital images using visual cryptography based on the Hill Cipher algorithm with matrix key flexibility. Hill Cipher is chosen for its ability to encrypt data in blocks, making it more secure than classical cryptographic algorithms that encrypt data individually. Visual cryptography is used to secure digital images through encryption and decryption. Encryption scrambles the image, while decryption restores it. The research method involves collecting digital image datasets, preprocessing, Hill Cipher encryption, and decryption. Key flexibility includes matrix keys of 2x2, 3x3, and 4x4 to enhance security. This research has demonstrated the effectiveness of the Hill Cipher algorithm in protecting digital images through encryption and decryption processes with flexible matrix keys of size 2x2 and 3x3. The results of the experiments, including encryption and decryption using both matrix sizes, have been thoroughly analyzed with respect to various cryptographic metrics: histogram analysis, energy, entropy, and running time.

Keywords—*Copyright Protection, Cryptography, Flexible Matrix Keys, Hill Cipher*

1. Introduction

The rapid advancement of information and communication technology enables humans to communicate and exchange data in a very short period. However, behind this convenience lies a major issue related to data security, particularly regarding the protection of digital image copyrights that are widely distributed on the internet (Siahaan, 2016). Digital images, which consist of two-dimensional pictures generated through sampling processes, are vulnerable to misuse and copyright infringement due to the ease of distribution and uncontrolled modification (Alfina, 2019). Digital images often contain valuable information related to intellectual property rights, which should not be modified or distributed without permission (Freddy et al., 2017). As the number of images circulating on the internet increases, protecting copyright becomes increasingly difficult, highlighting the need for an effective mechanism to safeguard these works.

The urgency of this research lies in the importance of protecting digital image copyrights to ensure that intellectual works remain secure, especially in the face of widespread copyright

violations that often go unnoticed by many internet users (Wang et al., 2020). This situation demonstrates the need for a stronger approach to protect digital images with economic value and copyright. One method that can be employed to secure digital images is visual cryptography, which transforms images into unreadable forms without the correct key. This cryptographic process involves encryption and decryption, ensuring that only authorized parties can access the digital image in its original form (Donni et al., 2018).

This study proposes the use of the Hill Cipher algorithm for digital image encryption, a classical cryptographic method first introduced by Lester S. Hill in 1929 (Ginting, 2020). Hill Cipher uses a square matrix as the key to perform matrix multiplication during the encryption and decryption processes, enhancing security compared to other cryptographic methods that use simple substitution (Agarwal et al., 2010). The main advantage of Hill Cipher lies in its ability to encrypt data blocks simultaneously, rather than character by character, which strengthens data confidentiality. Previous research by Dwitiyanti & Satria Setiawan, (2021) has demonstrated the effectiveness of using a 2x2 matrix key for digital image encryption; however, there is room for improvement, particularly in terms of flexibility and algorithm complexity. Previous research by Yang et al., (2012) demonstrated the use of Hill Cipher-based visual cryptography for secure image transmission, showcasing how matrix-based encryption methods could enhance image security. The study highlighted the potential of Hill Cipher in encrypting pixel values of images, but also suggested that its complexity could be improved by considering flexible matrix sizes. Similarly, (Ranti et al., 2024) conducted a survey on visual cryptography, underlining the importance of cryptographic techniques like Hill Cipher in the protection of digital images. Their research also explored how the application of larger matrix keys could improve the overall security of the encrypted image. In addition, Mahmoud & Chefranov (2014) reviewed various Hill Cipher-based encryption methods, focusing on their ability to secure images, especially when combined with visual cryptography for copyright protection. They concluded that incorporating flexible matrix key sizes in the encryption algorithm could provide a more customizable and robust approach to image protection. These studies, along with others such as Firmanto et al., (2021) and (Alfina, 2019), have paved the way for further improvements in Hill Cipher-based encryption techniques, specifically highlighting the role of flexible matrix key sizes in enhancing security and efficiency.

This research highlights the flexibility of the matrix key as a new scientific contribution. Hill Cipher traditionally uses a 2x2 matrix key, which, although effective, is limited in terms of complexity. Therefore, this study introduces the use of a 3x3 matrix key, which can increase the complexity and pixel distribution of the image, thereby improving encryption security. This flexibility allows users to select a security level that aligns with the sensitivity of the encrypted information. For instance, for more sensitive images, the use of a 3x3 matrix would provide a more secure encryption. This modification is expected to enhance the security and complexity of visual cryptography, making the Hill Cipher algorithm more adaptable to the specific needs of users in securing digital images.

2. Method

This research follows a structured process aimed at enhancing the security of digital images through encryption and decryption techniques. First, the digital image is pre-processed to prepare it for encryption, which may involve resizing or normalizing the image. Next, Hill Cipher encryption is applied with the flexibility of using either a 2x2 or 3x3 matrix key, ensuring that the image is securely transformed into an unreadable format. The encrypted image data is then generated. For decryption, the corresponding Hill Cipher decryption process is applied, using the appropriate matrix key (2x2 or 3x3), to recover the original image data (Azhar, 2017). Finally, the decrypted image is analyzed, focusing on evaluating the image quality and cryptographic performance by examining metrics such as histogram, energy, entropy, and processing time for both encryption and decryption. These stages collectively

ensure the effectiveness and efficiency of the proposed encryption method for protecting digital image copyrights. The research process in the form of a flowchart is presented in Figure 1.

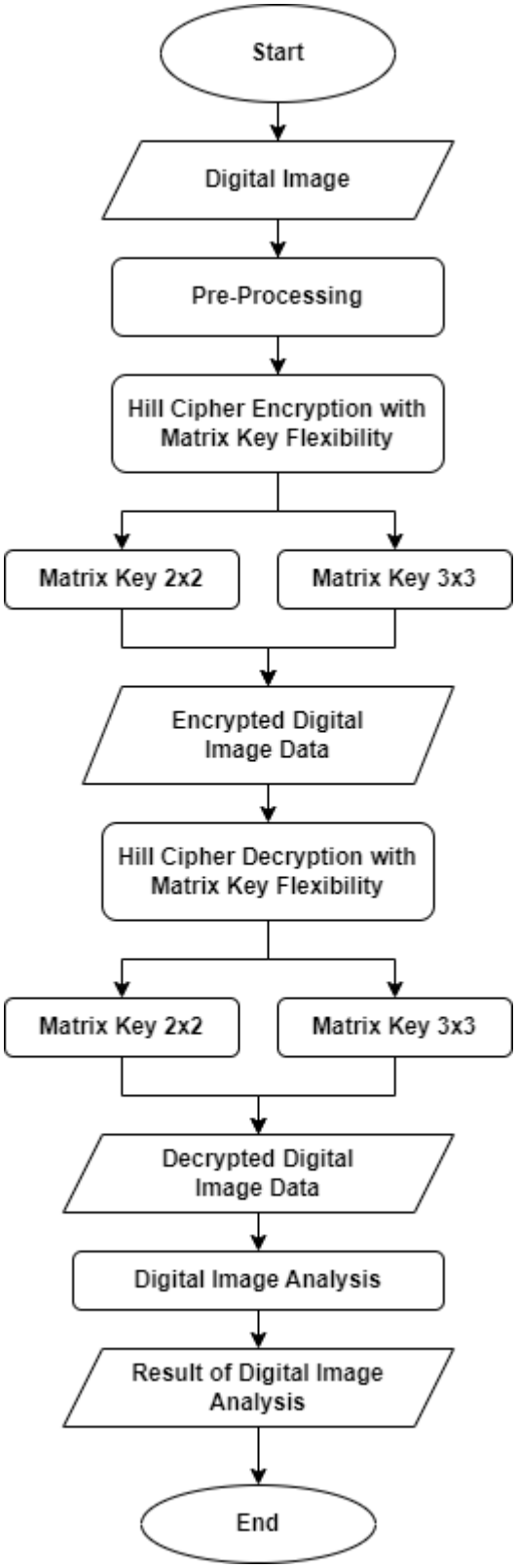

Figure 1. Flowchart of Research

2.1 Image Data Collecting

The data used in this research consists of digital image files captured by a DSLR camera. The images are limited to colored images with three channels (RGB), specifically photos taken from the footage of the film "Botoh," obtained directly by one of the crew members. These images are chosen as samples of digital images with copyright protection, meaning they cannot be used freely. The images are then utilized as subjects for testing the implementation of the Hill Cipher algorithm in image encryption using flexible matrix keys, namely 2x2 or 3x3 keys.

2.2 Pre-Processing

In the data preprocessing stage, the image used is processed to prepare it for encryption algorithm application. The first step is to extract the color components from the digital image. A colored image consists of three primary color channels: red, green, and blue, often abbreviated as RGB. Each color in the image has a numerical value between 0 and 255, which represents the intensity of that color. For example, in each pixel located at a specific coordinate, there is an RGB value that represents the intensity of red, green, and blue at that pixel. For instance, in a pixel located at coordinate (0,0), there may be an RGB value of (205, 167, 182), meaning the red value is 205, green is 167, and blue is 182.

Next, the following step is to extract data for each pixel in the image. This process involves separating the intensity values of the three color channels for each pixel, one by one. For example, in a 6x3 pixel image, each pixel at a specific coordinate will have separate RGB values. After separating the color components, the data is then used for the next process, which is applying the Hill Cipher algorithm to encrypt the image. By dividing the image based on different color components, the Hill Cipher algorithm processes each color channel separately.

2.3 Hill Cipher Encryption

Hill Cipher is a classical cryptography method that uses matrix algebra to encrypt a message (Supiyanto & Mandowen, 2021). The basic principle of Hill Cipher is to use a key matrix to perform matrix multiplication on the data to be encrypted. Only the party with the correct key can decrypt the data to return it to its original form (Serdano et al., 2019).

2.3.1 Encryption using 2x2 Key Matrix

$$K = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad (1)$$

Suppose we have a 2x2 key matrix K. Where a, b, c, and d are values in the key matrix. The message to be encrypted (for example, a digital image or text) needs to be converted into numerical representation. In the case of an image, this involves converting pixel values into numbers. For text, each letter can be translated to a number based on its position in the alphabet, such as A=0, B=1, C=2, and so on. For example, suppose the message to be encrypted is the pair [p1, p2], which represents two consecutive characters in the message (Mfungo et al., 2023). The encryption is performed by multiplying the key matrix K with the message vector P, under modulo 256:

$$C = K\ x\ P\ (mod\ 256) \quad (2)$$

Where C is the encrypted message. Mathematically:

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \mod 256 \quad (3)$$

This results in an encrypted vector C = [c1, c2], which represents the encrypted message.

2.3.2 Encryption using 3x3 Key Matrix

If a 3x3 key matrix is used, the process is similar but with more components. Suppose we have a 3x3 key matrix K where a, b, c, d, e, f, g, h, and i are values in the key matrix.

$$K = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \quad (4)$$

Similar to the 2x2 case, the message is split into blocks of three elements for encryption. For example, the message to be encrypted could be the block [p1, p2, p3], representing three consecutive characters. The encryption is performed by multiplying the key matrix K with the message vector P and taking the modulo 256:

$$C = K \, x \, P \, (mod \, 256) \quad (5)$$

For each message block P (3x1), the encryption is computed as:

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \times \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \mod 256 \quad (6)$$

The result is an encrypted vector C = [c1, c2, c3], which represents the encrypted message.

2.4 Hill Cipher Decryption

Hill Cipher decryption involves reversing the encryption process by using the inverse of the encryption key matrix (J. I. Sari et al., 2017). In this research, the decryption process operates modulo 256, which ensures that the values remain within the valid range of pixel values (0 to 255). Below is a step-by-step explanation of how decryption works for both 2x2 and 3x3 matrices with modulo 256.

2.4.1 Decryption with 2x2 Matrix Key

To decrypt the image, we first need the inverse of the key matrix used during encryption (Acharya et al., 2010). If the encryption matrix is denoted as K, the decryption matrix is the inverse of K, denoted as K^{-1}. For a 2x2 matrix K:

$$K = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \quad (7)$$

The inverse of matrix K modulo 256 is given by:

$$K^{-1} = \frac{1}{\det(K)} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \mod 256 \tag{8}$$

Where det(K) is the determinant of matrix K, calculated as:

$$\det(K) = ad - bc \tag{9}$$

To ensure that the inverse exists, det(K) must be coprime with 256 (i.e., gcd(det(K), 256) = 1). Next, we calculate the modular inverse of det(K) modulo 256 using the Extended Euclidean Algorithm. If the modular inverse of det(K) exists, we multiply it with the matrix of cofactors to obtain the inverse matrix.

$$K^{-1} = \det(K)^{-1} \times \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \mod 256 \tag{10}$$

Once the inverse key matrix K^{-1} is computed, we apply it to the encrypted image data (ciphertext) blocks. Given a ciphertext block C = [C1 C2], the decrypted image block P = [P1 P2] is calculated as:

$$P = K^{-1} \times C \mod 256 \tag{11}$$

2.4.2 Decryption with 3x3 Matrix Key

For a 3x3 matrix key, the decryption process follows similar steps but involves a larger matrix (N. D. Sari & Arius, 2020). Let the encryption matrix be:

$$K = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \tag{12}$$

The inverse of a 3x3 matrix K modulo 256 is calculated by:

$$K^{-1} = \frac{1}{\det(K)} \cdot \text{adj}(K) \mod 256 \tag{13}$$

Where det(K) is the determinant of K and adj(K) is the adjugate matrix of K.
The determinant of matrix K is computed as:

$$\det(K) = a(ei - fh) - b(di - fg) + c(dh - eg) \tag{14}$$

The adjugate matrix adj(K) is the transpose of the cofactor matrix. Each cofactor corresponds to the determinant of a 2x2 submatrix. Once the determinant is calculated, we check if det(K) is coprime with 256. If it is, we compute the modular inverse of det(K) modulo 256.

The inverse matrix K^(-1) is then calculated by multiplying det(K)^(-1) with adj(K) modulo 256:

$$K^{-1} = \det(K)^{-1} \times \text{adj}(K) \mod 256 \quad (15)$$

Once we have K^(-1), the decrypted image data is obtained by applying the inverse matrix to the ciphertext blocks. Given a ciphertext block C = [C1 C2 C3], the decrypted block P = [P1 P2 P3] is calculated as:

$$P = K^{-1} \times C \mod 256 \quad (16)$$

2.5 Image Analysis

The final step is the analysis of the results by comparing the original digital image (plain image) with the encrypted digital image (cipher image). Several aspects are considered by the author as testing parameters. These parameters serve as benchmarks to evaluate the effectiveness of using the Hill Cipher algorithm as a digital image encryption process. The following parameters are used in the evaluation (Kadir & Susanto, 2013):

2.5.1 Histogram

The histogram shows the color distribution of a digital image. A histogram that produces an even color distribution can be considered as an indicator of a good encryption algorithm. The main determining factor is that the histogram of the encrypted image (cipher image) must differ significantly from the histogram of the plain image. The RGB values range from 0 to 255 for each red, green, and blue color channel.

2.5.2 Energy (uniformity)

Energy (uniformity) indicates the relationship between two variables. With the two variables being the plain image and cipher image, the algorithm is considered good if it produces energy (uniformity) close to zero. The energy descriptor is a measure of the pixel intensity distribution over the grayscale range. Its definition is given by the following equation:

$$energy = \sum_{i=0}^{L-1}[p(i)]^2 \quad (17)$$

2.5.3 Entropi Entropy (image complexity)

Entropi Entropy (image complexity) and energy tend to be inversely related. Entropy measures the uncertainty of information. The higher the entropy value (image complexity), the more uncertain the information. In the context of a cipher image, the higher the entropy (image complexity), the better the encryption algorithm. Entropy provides a measure of the complexity of a digital image and is calculated using the following equation:

$$entropy = -\sum_{i=0}^{L-1} p(i)\ \log_2(p(i)) \quad (18)$$

2.5.4 Process Time

The process time is used to calculate and analyze the encryption and decryption times when using the Hill Cipher algorithm with 2x2 and 3x3 matrix keys. The time unit used for

measuring the encryption and decryption process is milliseconds, and the file types used for input data (plain image) are .jpg and .png formats.

3. Results And Discussion

3.1 Hill Cipher-Based Visual Cryptography

In this research, the Hill Cipher algorithm was successfully applied to encrypt and decrypt digital images using flexible matrix keys of sizes 2x2 and 3x3. The encryption and decryption processes were implemented through the development of a desktop application created using Java programming with the NetBeans 8.2 IDE. The application was designed to handle digital images, applying the Hill Cipher algorithm to protect images, particularly for copyright protection. The encryption process begins with preprocessing the digital image, where the image is separated into three color channels: Red, Green, and Blue (RGB). Each of these color channels is represented as a matrix, with each matrix entry corresponding to the pixel intensity values of that color. Once the image is divided into its color channels, the Hill Cipher algorithm is applied by multiplying these matrices with the encryption key (either a 2x2 or 3x3 matrix). This results in an encrypted version of the image, known as the cipher image, with pixel values transformed using modular arithmetic (modulo 256) to ensure that they remain within the acceptable range for RGB values (0–255). For the decryption process, the inverse of the encryption matrix is calculated. The cipher image is then multiplied by this inverse matrix using the same modular arithmetic approach, effectively recovering the original image (the plain image). The use of flexible matrix keys (2x2 and 3x3) provides varying levels of encryption strength, with the 3x3 matrix offering higher security due to its increased complexity. The Java-based desktop application allows users to easily perform these encryption and decryption operations, demonstrating the practicality and effectiveness of the Hill Cipher algorithm in protecting images, such as those with copyright, from unauthorized access.

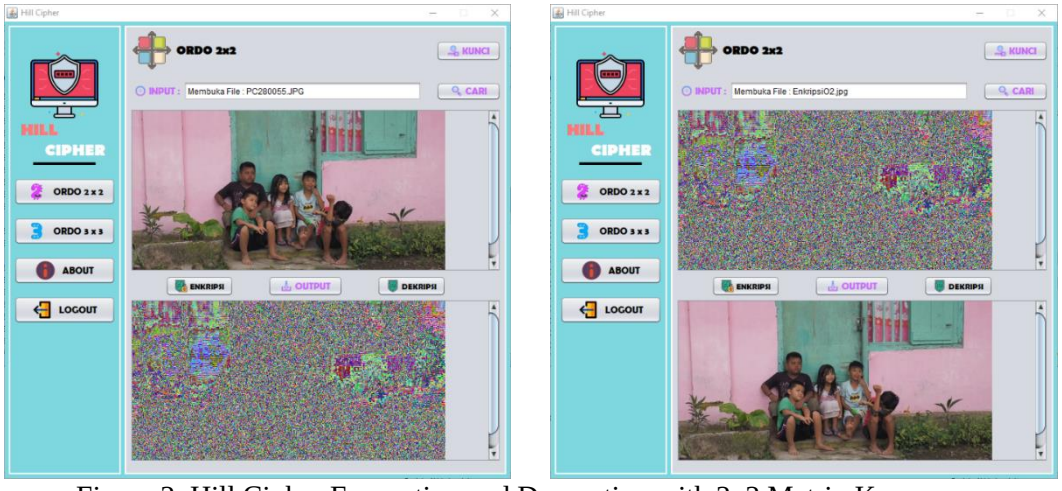

Figure 2. Hill Cipher Encryption and Decryption with 2x2 Matrix Key

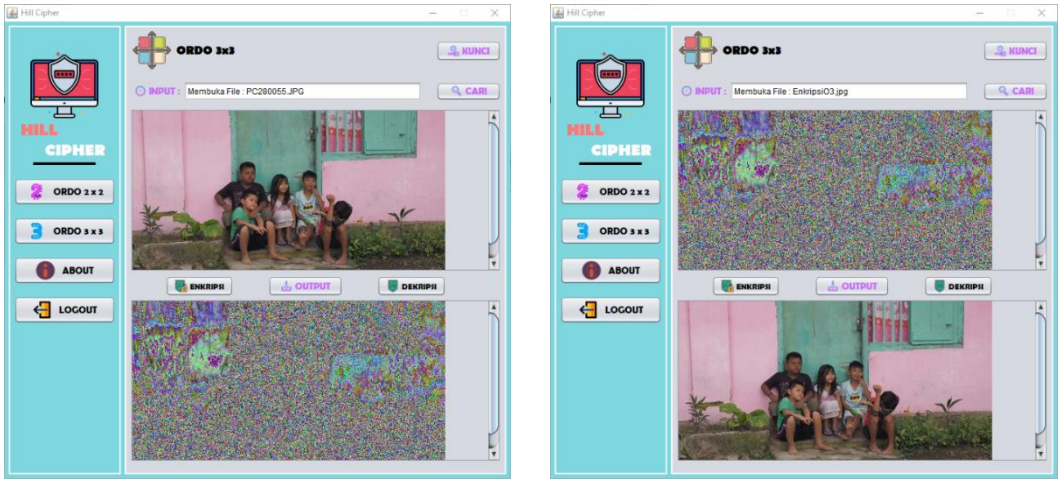

Figure 3. Hill Cipher Encryption and Decryption with 2x2 Matrix Key

Figure 2 illustrates the process of Hill Cipher encryption and decryption using a 2x2 matrix key, while Figure 3 presents the same process but with a 3x3 matrix key. These figures visually represent the stages of both encryption and decryption, highlighting the differences in the matrix sizes used for each key. In Figure 2, the image is encrypted by applying a 2x2 matrix key to the image's RGB components, resulting in the transformed cipher image. This matrix key is applied through matrix multiplication, where each pixel's RGB values are manipulated according to the values in the 2x2 matrix. For decryption, the inverse of the 2x2 matrix is used to recover the original image. In Figure 3, a more complex 3x3 matrix key is employed for encryption and decryption, providing a higher level of security due to its larger size and more complex calculations. The encryption and decryption processes are similar to those in Figure 2, but with the additional complexity introduced by the larger matrix. Using a 3x3 matrix enhances the algorithm's robustness against potential attacks, making it more suitable for applications requiring a higher level of security. These figures demonstrate how matrix size affects the encryption strength and computational complexity, as well as the practical application of Hill Cipher for digital image protection using flexible matrix keys.

3.2 Histogram Analysis

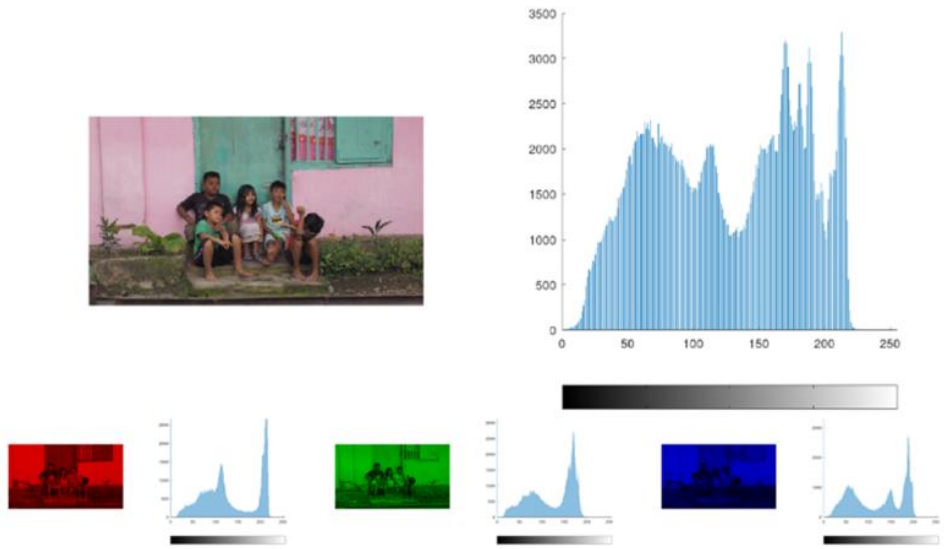

Figure 4. Histogram analysis for *plain image RGB*

The histogram shown in Figure 4 represents the plain image RGB histogram, where the frequency displayed indicates the relative intensity of each color channel in the image. The histogram for the red, green, and blue color channels all exhibit similar peak values, suggesting that the intensity distribution for each color is fairly uniform across the image. This implies that the plain image has a balanced and well-distributed intensity of colors, with no single color channel dominating the others. The peaks in the histogram correspond to the most common intensity values within each color channel. In this case, the uniformity of the peaks across the three channels indicates that the image's color composition is evenly distributed, with a moderate range of pixel intensities from 0 to 255 in each of the RGB components. This type of histogram is typical for a well-exposed and balanced image, where no particular color is overly saturated or lacking. This analysis is important in the context of image encryption because it serves as a baseline to compare with the encrypted cipher image histogram to evaluate how well the encryption process has scrambled the image's original color distribution.

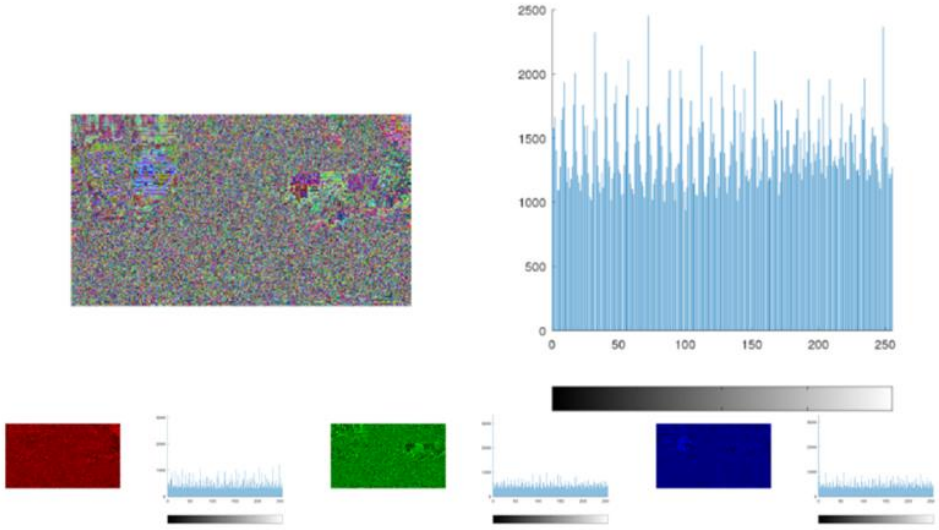

Figure 5. Histogram analysis for cipher image RGB 2x2 using 2x2 matrix key

Figure 5 presents the histogram of the cipher image RGB with a 2x2 matrix key. In this histogram, the frequency of color intensities is distributed evenly across the three color panels—red, green, and blue. The average intensity frequency, or the number of pixels, appears relatively lower when compared to the original plain image histogram. This even distribution suggests that the encryption process, using the Hill Cipher with a 2x2 matrix key, has successfully obscured the digital image by effectively scattering the pixel intensities across a broader range. The lower intensity frequencies in the histogram indicate that the encryption has significantly altered the original pixel values, making it difficult to deduce the original image. This is a key characteristic of a good encryption algorithm, as it ensures that the visual characteristics of the image, including its color distribution, are thoroughly scrambled. As a result, the encrypted cipher image is far less recognizable compared to the plain image, effectively protecting the image's content and confidentiality.

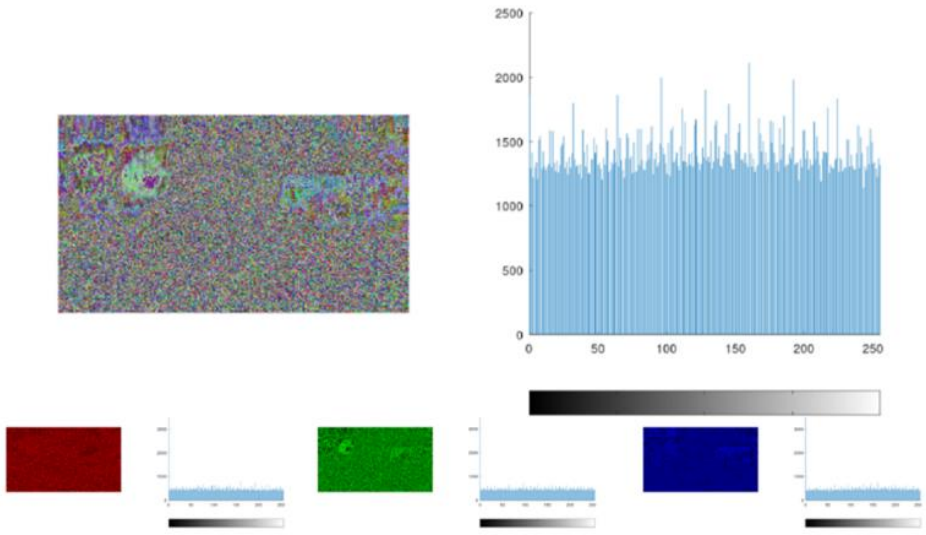

Figure 6. Histogram analysis for cipher image RGB 2x2 using 3x3 matrix key

Figure 6 shows the histogram of the cipher image RGB with a 3x3 matrix key. In this histogram, the distribution of color intensities is evenly spread across the red, green, and blue color channels. The average intensity frequency, or the number of pixels, is relatively lower in the cipher image with a 3x3 matrix key compared to the histogram of the cipher image with a 2x2 matrix key. This lower intensity frequency suggests that the encryption using the Hill Cipher with a 3x3 matrix key has further scrambled the pixel values more effectively than the 2x2 matrix, resulting in a more secure and less recognizable encrypted image. The even spread of pixel intensities across all color channels indicates that the encryption has thoroughly obscured the original image, making it harder to reverse-engineer and providing a stronger level of confidentiality and protection.

The analysis of the histograms for the 2x2 and 3x3 matrix key Hill Cipher encryption reveals important differences in the distribution of color intensities in the encrypted images. For the 2x2 matrix key, the histogram shows a more concentrated distribution of pixel intensities in each of the three color channels (red, green, and blue). Although the intensities are spread out, they are not as uniformly distributed, and there is a more noticeable peak in the histogram for each color channel. This suggests that while the encryption obscures the image, the frequency of certain intensity values is still relatively higher, making it easier to deduce patterns or hints of the original image. In other words, the encrypted image, while encrypted, may still retain some identifiable patterns or redundancies due to the relatively lower complexity of the 2x2 key matrix encryption. On the other hand, for the 3x3 matrix key, the histogram shows a much more even spread of pixel intensities across all three color channels. The frequency of pixel intensities is significantly lower compared to the 2x2 matrix encryption. This even distribution of pixel intensities indicates that the encryption is more effective at randomizing the image, making it harder to identify any pattern or correlation with the original image. The higher complexity of the 3x3 matrix key results in a more thorough scrambling of the pixel values, thereby providing a higher level of security and making it more difficult to reverse-engineer the encrypted image.

Statistically, the Hill Cipher encryption with a 3x3 matrix key is superior to the 2x2 matrix key due to the increased randomness and better distribution of pixel intensities. The more uniform histogram for the 3x3 cipher image demonstrates a greater level of image obfuscation, which makes the encryption process more robust and secure. This indicates

that the 3x3 matrix key provides a better safeguard for image data, making it more effective for use in protecting copyright or ensuring confidentiality in digital images.

3.3 Analysis of Energy

Table 1. Result of Energy

Images	***Result of Energy***
Plain image	0.4455
	0.4454
	0.4454
Cipher image using 2x2 matrix key	0.4467
	0.4470
	0.4469
Cipher image using 3x3 matrix key	0.4471
	0.4472
	0.4472

The energy analysis of the plain image and the encrypted images with 2x2 and 3x3 matrix keys reveals important insights into the effectiveness of the Hill Cipher encryption in terms of pixel intensity distribution. The plain image (original RGB image) shows moderate energy values across the three color channels, indicating a relatively uniform distribution of pixel intensities. This suggests that the original image has less complexity and its pixel values are relatively predictable. When the Hill Cipher encryption is applied with a 2x2 matrix key, the energy values for the cipher image slightly increase across all three color channels. This increase indicates that the encryption has successfully disrupted the regularity of the original image, introducing more variation and making the pixel intensities less predictable. This is an expected outcome for an effective encryption algorithm, as it should make the image harder to analyze or recognize. The energy values for the cipher image with the 3x3 matrix key show a further increase, suggesting that the 3x3 matrix key has a slightly stronger encryption effect than the 2x2 matrix key. This further increase in energy indicates a higher level of randomness and complexity in the pixel distribution, which makes the encrypted image even more secure and less susceptible to pattern recognition. Overall, the energy analysis demonstrates that both the 2x2 and 3x3 matrix keys effectively encrypt the image, with the 3x3 key providing a marginal improvement in terms of energy, reflecting slightly stronger encryption. The overall trend confirms that the Hill Cipher successfully obscures the original image data, with the 3x3 matrix key offering a slightly more secure form of encryption.

3.4 Analysis of Entropy

Table 2. Result of Entropy

Images	***Result of Entropy***
Plain image	2.2955
	2.2862
	2.3190
Cipher image using 2x2 matrix key	2.4533
	2.4636
	2.4610
Cipher image using 3x3 matrix key	2.4700
	2.4707
	2.4698

The entropy analysis measures the complexity and unpredictability of an image, where higher entropy values indicate greater randomness and complexity. The results for the original image (plain image) and the cipher images with 2x2 and 3x3 matrix keys show how the Hill Cipher encryption impacts the information content and unpredictability of the image. Original Image (Plain Image): The entropy values for the original image range from 2.2862 to 2.3190 across the three RGB channels. These values reflect the level of uncertainty or randomness in the original image. Since entropy measures the unpredictability of pixel values, the relatively lower entropy values suggest that the original image has more predictable patterns, meaning it is easier to recognize or analyze. Images with lower entropy generally have more uniform or repetitive pixel structures.

After applying the Hill Cipher encryption with a 2x2 matrix key, the entropy values increase to 2.4533, 2.4636, and 2.4610 across the three color channels. This increase in entropy indicates that the encryption has successfully introduced more complexity and randomness into the image. The higher entropy values imply that the encrypted image is more unpredictable and has less structure or regularity than the plain image, making it more resistant to analysis or pattern recognition. The result demonstrates that the Hill Cipher encryption with a 2x2 matrix key effectively increases the image's unpredictability.

The entropy values for the cipher image encrypted with a 3x3 matrix key show an even greater increase, with values of 2.4700, 2.4707, and 2.4698. This suggests that the 3x3 matrix key produces an even more complex and unpredictable image compared to the 2x2 matrix key. The further increase in entropy reinforces the idea that the 3x3 key enhances the encryption, making the resulting cipher image harder to decipher and more resistant to attacks or analysis.

The entropy results clearly demonstrate the effectiveness of Hill Cipher encryption in enhancing the complexity of an image. Both the 2x2 and 3x3 matrix keys significantly increase the entropy values, making the encrypted images less predictable and more secure. However, the 3x3 matrix key provides slightly higher entropy, suggesting it offers a marginally better encryption in terms of increasing randomness and complexity. Higher entropy values in the cipher images indicate stronger encryption, and this trend further validates the use of Hill Cipher with matrix keys in digital image encryption.

3.5 Process Time

```
run:
MATRIKS ORDO 2x2
Waktu Enkripsi Kunci Ordo 2x2 : 67 milisecond
Determinan : 95
MultiPlikatif = 159
Invers Kunci Matriks [[135, 113], [175, 178]]
Waktu Dekripsi Kunci Ordo 2x2 : 45 milisecond
BUILD SUCCESSFUL (total time: 39 seconds)
```

Figure 7. Process time using 2x2 matrix key

```
run:
MATRIKS ORDO 3x3
Waktu Enkripsi Kunci Ordo 3x3 : 89 milisecond
Determinan : 193
MultiPlikatif = 65
Invers Kunci Matriks [[151, 249, 87], [122, 236, 219], [36, 119, 223]]
Waktu Dekripsi Kunci Ordo 3x3 : 59 milisecond
BUILD SUCCESSFUL (total time: 20 seconds)
```

Figure 8. Process time using 2x2 matrix key

Based on Figure 7 the encryption and decryption process for the 2x2 matrix key takes 45 milliseconds. This relatively quick processing time suggests that the Hill Cipher with a

2x2 key is computationally less demanding compared to the 3x3 matrix key. This lower processing time is expected because the 2x2 matrix involves fewer calculations, making it faster for encryption and decryption processes. However, this speed comes at the cost of lower security, as a 2x2 matrix is less complex and may be more vulnerable to cryptographic attacks. On the other hand, Figure 8 shows the encryption and decryption process for the 3x3 matrix key takes 59 milliseconds. The increase in running time is due to the higher computational complexity of the 3x3 matrix. A 3x3 matrix requires more operations (multiplications and matrix inversions) than a 2x2 matrix, which naturally results in a longer processing time. However, this increased processing time is justified by the enhanced security of the 3x3 key. With a larger matrix size, the Hill Cipher provides more robust encryption, making it harder to break or analyze.

4. Conclusions

This research has demonstrated the effectiveness of the Hill Cipher algorithm in protecting digital images through encryption and decryption processes with flexible matrix keys of size 2x2 and 3x3. The results of the experiments, including encryption and decryption using both matrix sizes, have been thoroughly analyzed with respect to various cryptographic metrics: histogram analysis, energy, entropy, and running time. Firstly, the histogram analysis revealed significant differences between the plain image and the cipher image. For both matrix sizes, the histogram of the encrypted image showed a uniform distribution of pixel intensities across the red, green, and blue channels, indicating effective image encryption. However, the 3x3 matrix encryption exhibited a more uniform spread compared to the 2x2 matrix, suggesting that it provides stronger protection by further disguising the original image's characteristics. Secondly, the energy analysis showed that both the 2x2 and 3x3 matrix encryptions led to similar energy values for the encrypted images, slightly differing from the plain image. This result indicates that the Hill Cipher algorithm effectively disturbs the image's intensity distribution, making the encrypted image appear more uniform. The 3x3 matrix, though slightly higher in energy, still displayed similar properties, reinforcing its reliability for cryptographic purposes. Moreover, the entropy analysis demonstrated a significant increase in complexity after encryption, with the 3x3 matrix producing higher entropy values than the 2x2 matrix. This higher entropy suggests that the 3x3 matrix encryption adds more uncertainty and unpredictability to the encrypted image, which is a desirable trait for secure cryptography, ensuring the image is more resistant to attacks. Finally, the running time analysis highlighted the trade-off between encryption strength and processing efficiency. The 2x2 matrix demonstrated faster processing times (45 milliseconds), while the 3x3 matrix took slightly longer (59 milliseconds). Despite the longer processing time, the 3x3 matrix provided stronger encryption, making it more suitable for applications requiring higher levels of security. In conclusion, the findings indicate that Hill Cipher-based visual cryptography, using flexible matrix keys of 2x2 and 3x3, is a viable approach for protecting copyrighted images. While the 2x2 matrix offers faster encryption and decryption, the 3x3 matrix provides enhanced security with marginally increased computational cost. This study contributes to the development of practical encryption systems for image protection, balancing security and performance to safeguard digital content effectively.

Acknowledgements

The authors would like to express their sincere gratitude to the Ministry of Education, Science, and Technology of the Republic of Indonesia for their generous funding of this research through the PDP Scheme. This financial support has played a crucial role in the successful completion of this study, and the authors are deeply appreciative of the opportunity to contribute to the field of visual cryptography and the protection of digital image copyrights.

References

Acharya, B., Panigrahy, S. K., Patra, S. K., & Panda, G. (2010). Image Encryption Using Advanced Hill Cipher Algorithm. *ACEEE International Journal on Signal and Image Processing*, *1*(1).

Agarwal, G., Chaudhary, M., & Singh, S. (2010). Image Encryption using the Standard Hill Cipher. *International Journal of Advanced Research in Compter Science*, *1*(4), 74–76.

Alfina, O. (2019). Enkripsi Data Citra untuk Model Warna RGB dan Treshold Menggunakan Algoritma Hill Cipher. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *4*(1), 175–178. https://doi.org/10.30743/infotekjar.v4i1.1675

Azhar, W. Y. (2017). *KRIPTANALISIS HILL CIPHER TERHADAP KNOWN PLAINTEXT ATTACK MENGGUNAKAN METODE DETERMINAN MATRIKS BERBASIS ANDROID*. *8*(2), 579–592.

Donni, M., Siahaan, L., Putera, A., & Siahaan, U. (2018). Application of Hill Cipher Algorithm in Securing Text Messages. *INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD*, *4*(10), 55–59.

Dwitiyanti, N., & Satria Setiawan, H. (2021). *APLIKASI OPERASI MATRIKS PADA PERANCANGAN SIMULASI METODE HILL CIPHER MENGGUNAKAN MICROSOFT EXCEL*. *6*(1), 41–49.

Firmanto, B., Putri, D., Ningrum, K., Bramanto, A., & Putra, W. (2021). Perbandingan Hasil Performa Optimasi Transposisi Hill Cipher dan Vigenere Cipher pada Citra Digital. *SMARTICS Journal*, *7*(2), 65–71.

Freddy, J., Siahaan, O., Widodo, A. P., Ilmu, J., Informatika, K., Sains, F., Diponegoro, U., & Cipher, A. H. (2017). Kriptografi Teks dan Citra dengan Menggunakan Algoritma Hill Cipher pada Perangkat Android. *Jurnal Masyarakat Informatika*, *8*(1), 9–15.

Ginting, V. S. (2020). Penerapan Algoritma Vigenere Cipher dan Hill Cipher Menggunakan Satuan Massa. *Jurnal Teknologi Informasi*, *4*(2), 241–246. https://doi.org/10.36294/jurti.v4i2.1365

Kadir, A., & Susanto, A. (2013). *Teori dan Aplikasi Pengolahan Citra*.

Mahmoud, A., & Chefranov, A. (2014). *Hill Cipher Modification based on Pseudo-Random Eigenvalues*. *516*(2), 505–516.

Mfungo, D. E., Fu, X., Wang, X., & Xian, Y. (2023). Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map. *Applied Sciences (Switzerland)*, *13*(6). https://doi.org/10.3390/app13064034

Ranti, D., Fauzi, A., Pita, M., & Sitompul, U. (2024). Digital Image Security Analysis using Hill Cipher and AES Algorithm. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, *4*(1).

Sari, J. I., Sihotang, H. T., & Informatika, T. (2017). Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma Hill Cipher Dan Metode Least Significant Bit (LSB). *Jurnal Mantik Penusa*, *1*(2), 1–8.

Sari, N. D., & Arius, D. (2020). Modifikasi Algoritma Hill Cipher dengan Tabel Periodik Unsur Kimia Menggunakan Kode Nomor Operator Seluler di Indonesia. *Jurnal Teknologi Informasi*, *4*(2), 202–207. https://doi.org/10.36294/jurti.v4i2.1339

Serdano, A., Zarlis, M., Sawaluddin, & Hartama, D. (2019). Pengamanan Pesan Menggunakan Algoritma Hill Cipher Dalam Keamanan Komputer. *Jurnal Mahajana Informasi*, *4*(2), 1–5.

Siahaan, A. P. U. (2016). Genetic Algorithm in Hill Cipher Encryption. *American International Journal of Research in Science, Technology, Engineering & Mathematics*, 84–89.

Supiyanto, & Mandowen, S. A. (2021). Advanced hill cipher algorithm for security image data with the involutory key matrix. *Journal of Physics: Conference Series*, *1899*(1). https://doi.org/10.1088/1742-6596/1899/1/012116

Wang, R., Fung, B. C. M., & Zhu, Y. (2020). Heterogeneous data release for cluster analysis with differential privacy. *Knowledge-Based Systems*, *201–202*, 106047.

https://doi.org/10.1016/j.knosys.2020.106047
Yang, Q., Lou, J., Liu, S., & Diao, A. (2012). A Secure Image Encryption Algorithm Based on Hill Cipher System. *Bulletin of Electrical Engineering and Informatics*, *1*(1), 51–60. https://doi.org/10.12928/eei.v1i1.55