JSCE (Journal of System and Computer Engineering)
Vol.7, No.1, January 2026, pp. 101-115
ISSN (online): 2723-1240
DOI : https://doi.org/10.61628/jsce.v7i1.2471

Performance Optimization of Image Cryptography for Copyright Protection on High-Resolution Images Using the Hill Cipher with Flexible Matrix Keys

Miftakhul Rohman[a]; Abd. Charis Fauzan[b,*] ; Veradella Yuelisa Mafula[c]

Department of Computer Science, Universitas Nahdlatul Ulama Blitar, Indonesia
[a]miftakhulrohman@unublitar.ac.id ,[b]abdcharis@unublitar.ac.id, [c]veradella@unublitar.ac.id
** Corresponding author*

Article history: Received: December 16, 2025; Revised: January 06, 2026; Published: January 30, 2026;

Abstract

The increasing use of high-resolution digital images has raised serious concerns regarding copyright protection and unauthorized distribution. Image cryptography is one of the effective approaches to safeguard visual data by transforming images into unintelligible forms. The Hill Cipher algorithm, which is based on matrix operations, has potential for image encryption; however, its application to high-resolution images often suffers from high computational cost. This study proposes a performance optimization of image cryptography for copyright protection by exploiting the flexibility of matrix key sizes in the Hill Cipher algorithm. The optimization focuses on improving computational efficiency without modifying the fundamental cryptographic mechanism. Experiments were conducted on high-resolution images using different matrix key sizes (2×2, 3×3, and 4×4). Performance was evaluated in terms of encryption and decryption time, while security robustness was assessed using Entropy, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). The experimental results demonstrate that increasing the matrix key size significantly reduces the total computation time, achieving up to nearly 50% performance improvement, while maintaining high security levels. The encrypted images exhibit entropy values close to the ideal level, NPCR values above 99%, and stable UACI values, indicating strong randomness and diffusion properties. These findings confirm that the proposed optimization improves computational performance without compromising cryptographic security. Therefore, the optimized Hill Cipher remains effective and suitable for copyright protection of high-resolution images.

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

1. Introduction

The rapid advancement of information and communication technology has enabled humans to communicate and exchange data in a very short time. However, this convenience is accompanied by significant challenges related to data security, particularly in the protection of digital image copyrights that are widely distributed on the internet (Siahaan, 2016). Digital images, which consist of two-dimensional visual representations generated through sampling processes, are highly vulnerable to misuse and copyright infringement due to their ease of duplication, distribution, and modification (Alfina, 2019). Many digital images contain valuable information associated with intellectual property rights and therefore should not be altered or disseminated without proper authorization (Freddy et al., 2017). As the volume of digital images circulating on online platforms continues to increase, protecting copyright becomes increasingly complex, underscoring the urgent need for effective security mechanisms.

The importance of this research lies in addressing the growing problem of copyright violations involving digital images, many of which occur without the awareness of internet users (Wang et al., 2020). This situation highlights the necessity of robust cryptographic approaches capable of safeguarding digital images with economic and intellectual value. One approach that can be applied is image-based cryptography, particularly image cryptography, which transforms digital images into unreadable forms unless the correct key is provided. This process involves encryption and decryption stages, ensuring that only authorized users are able to access the original image content (Donni et al., 2018).

Among classical cryptographic techniques, the Hill Cipher algorithm, introduced by Lester S. Hill in 1929, has attracted attention due to its matrix-based encryption mechanism (Ginting, 2020). Hill Cipher employs square matrices as cryptographic keys to perform linear transformations during encryption and decryption, providing stronger security than simple substitution-based methods (Agarwal et al., 2010). Its ability to encrypt data in blocks rather than character by character enhances diffusion and confidentiality. Previous studies have demonstrated the feasibility of applying Hill Cipher to digital image encryption, particularly using a 2×2 matrix key configuration (Dwitiyanti & Satria Setiawan, 2021). Nevertheless, this conventional configuration presents limitations in terms of flexibility and scalability, especially when applied to high-resolution images.

Several researchers have explored the application of Hill Cipher within the context of image cryptography for image security. Yang et al. (2012) demonstrated the effectiveness of Hill Cipher-based image cryptography for secure image transmission and emphasized the potential benefits of matrix-based encryption. Ranti et al. (2024) further highlighted the importance of cryptographic techniques, including Hill Cipher, in protecting digital images and suggested that larger and flexible matrix keys could enhance security. Mahmoud and Chefranov (2014) reviewed various Hill Cipher-based encryption schemes and concluded that the use of flexible matrix key sizes could provide a more robust and customizable approach for image protection. Additional studies by Firmanto et al. (2021) and Alfina (2019) have also reinforced the relevance of Hill Cipher in image cryptography, while indicating opportunities for further improvement in both security and efficiency.

This study continues and extends previous research on Hill Cipher-based image cryptography for copyright protection, which focused on the feasibility and security aspects of using flexible matrix keys in image encryption (Mafula, 2025). Building upon that foundation, the present research shifts the focus toward performance optimization, particularly in the context of high-resolution images, where computational efficiency becomes a critical factor. While earlier work demonstrated that flexible matrix keys can enhance security, this study investigates how variations in matrix key size influence computational performance without compromising cryptographic strength. However, when such cryptographic schemes are applied to high-resolution images, computational efficiency becomes an equally important concern.

Despite extensive studies on Hill Cipher–based image cryptography, most existing research primarily focuses on enhancing cryptographic security, such as improving diffusion, randomness, or resistance to attacks. However, relatively limited attention has been given to computational efficiency, particularly when the algorithm is applied to high-resolution images. As image resolution increases, the computational cost of block-based encryption algorithms becomes a critical challenge, especially for practical copyright protection systems that require both security and efficiency. Consequently, there is a research gap regarding how algorithmic parameters of the Hill Cipher can be leveraged to optimize performance without degrading cryptographic robustness.

Based on the identified research gap, this study formulates the following research questions: (1) How does matrix key size influence the computational performance of Hill Cipher–based image cryptography when applied to high-resolution images? and (2) Does performance optimization through matrix key size flexibility affect cryptographic robustness as measured by entropy, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI)? These questions aim to systematically examine the relationship between efficiency and security in block-based image cryptography.

This study contributes to image cryptography research by demonstrating that matrix key size flexibility in the Hill Cipher can be effectively utilized as a performance optimization strategy for high-resolution images. Unlike prior studies that predominantly emphasize security enhancement, this work provides a systematic analysis of the trade-off between computational efficiency and cryptographic robustness. The experimental results show that larger matrix key sizes significantly reduce processing time while maintaining stable entropy, NPCR, and UACI values. These findings confirm that matrix key flexibility enables efficient high-resolution image protection without degrading cryptographic strength, thereby enhancing the practical applicability of the Hill Cipher for copyright protection.

2. Method

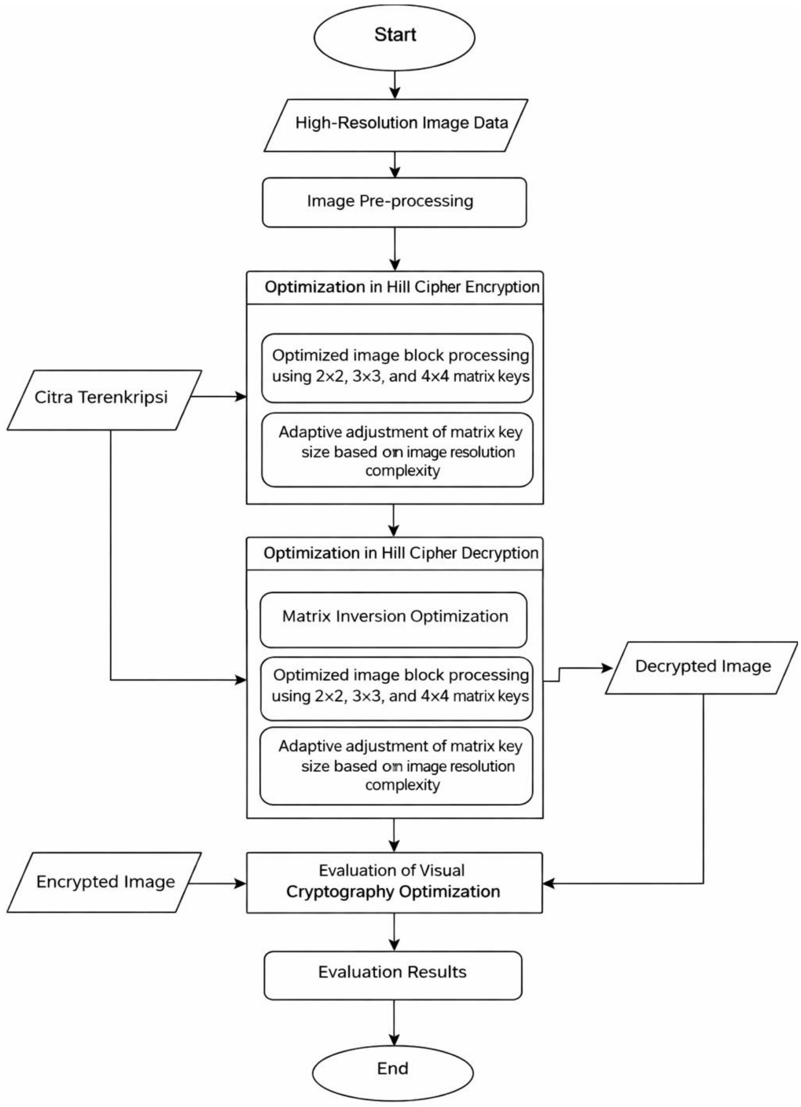
Start
High-Resolution Image Data
Image Pre-processing
Optimization in Hill Cipher Encryption
Optimized image block processing using 2×2, 3×3, and 4×4 matrix keys
Adaptive adjustment of matrix key size based on image resolution complexity
Citra Terenkripsi
Optimization in Hill Cipher Decryption
Matrix Inversion Optimization
Optimized image block processing using 2×2, 3×3, and 4×4 matrix keys
Adaptive adjustment of matrix key size based on image resolution complexity
Decrypted Image
Encrypted Image
Evaluation of Visual Cryptography Optimization
Evaluation Results
End

Figure 1. Flowchart of Research

The research procedure is summarized and illustrated in the form of a flowchart, as presented in Figure 1. This research adopts a structured experimental approach to optimize the computational performance of image cryptography for copyright protection using the Hill Cipher algorithm. The method consists of several sequential stages designed to evaluate both performance efficiency and cryptographic security. First, the digital image is prepared as input data. The image is converted into a suitable format for processing by transforming it into RGB channels and reshaping pixel values into vectors. This preparation ensures compatibility with the matrix-based operations required by the Hill Cipher algorithm. Next, the encryption process is performed using the Hill Cipher with flexible matrix key sizes, namely 2×2, 3×3, and 4×4. For each configuration, a random invertible matrix modulo 256 is generated as the encryption key. The image data are then encrypted in block form using matrix multiplication, producing a cipher image that is visually unreadable.

The encryption time is recorded to evaluate computational performance. Following the encryption stage, the decryption process is carried out using the corresponding inverse matrix key for each key size. The decryption aims to reconstruct the original image accurately from the encrypted data. The decryption time is also measured to assess the overall computational cost of the cryptographic process. To evaluate the effectiveness of the proposed optimization, the encrypted images are analyzed using several cryptographic metrics. Entropy is used to measure the randomness of the encrypted image, while Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are employed to assess pixel sensitivity and diffusion characteristics. In addition, the total computation time, consisting of encryption and decryption time, is analyzed to quantify performance improvement across different matrix key sizes.

All experiments were conducted using high-resolution color images with resolutions ranging from approximately 3000×2000 to 6000×4000 pixels. The experimental environment consisted of a workstation equipped with an Intel Core i7 processor, 8 GB RAM, and a Windows-based operating system. The Hill Cipher algorithm was implemented in Python. A total of three representative high-resolution images from the MIT–Adobe FiveK dataset were used for each matrix key size configuration, and each experiment was repeated to ensure consistency and reliability of performance measurements. These images were selected to represent diverse visual characteristics and resolutions commonly used in copyright-sensitive digital content.

2.1 Image Data Collecting

The data used in this research were obtained from the MIT–Adobe FiveK dataset, which consists of 5,000 high-resolution RAW images captured using professional DSLR cameras. The dataset provides color images with three RGB channels and is widely recognized as a benchmark dataset for image processing and computer vision research due to its high visual quality and diverse content.

In this study, a subset of images was selected as representative samples from the MIT–Adobe FiveK dataset to serve as input data. The selected images represent high-resolution digital images with potential copyright value, making them suitable for evaluating image cryptography techniques. These sample images were used to test the implementation of the Hill Cipher algorithm for image encryption and decryption.

To analyze both computational performance and cryptographic security, the selected sample images were encrypted and decrypted using flexible matrix key sizes, namely 2×2, 3×3, and 4×4. The use of sampled images from the MIT–Adobe FiveK dataset ensures that the experimental evaluation reflects realistic copyright protection scenarios, particularly for high-resolution images that require a balance between strong security and efficient computational processing.

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*

$$K = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \tag{1}$$

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:

$$C = \ K\,x\,P\ (mod\ 256) \tag{2}$$

Where C is the encrypted message. Mathematically:

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

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.

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

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:

$$C = \ K \, x \, P \ (mod\ 256) \tag{5}$$

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

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

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:

$$K = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \tag{7}$$

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:

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

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:

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

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:

$$P = K^{-1} \times C \mod 256 \tag{16}$$

2.5 Performance Optimization

From a computational perspective, increasing the matrix key size reduces the total number of block operations required to process a high-resolution image. Since the Hill Cipher encrypts data in fixed-size blocks, larger matrix keys result in fewer block iterations over the same image dimension. Consequently, the frequency of matrix multiplication operations is reduced, which directly lowers computational overhead. This characteristic makes matrix key size a critical parameter for optimizing algorithmic complexity in block-based image cryptography.

Performance optimization in this study is conducted through a systematic evaluation of matrix key size flexibility to improve the computational efficiency of the Hill Cipher algorithm for high-resolution image cryptography. The optimization is performed at the implementation level and does not alter the fundamental mathematical structure of the Hill Cipher algorithm. The primary objective of this method is to identify a configuration that achieves efficient computation while preserving cryptographic security. The optimization process involves applying the Hill Cipher algorithm to the same set of sample images using different matrix key sizes, namely 2×2, 3×3, and 4×4. For each configuration, the image data are processed in block form, where the block size is determined by the dimension of the selected matrix key. This approach enables a consistent comparison of computational behavior across different key size configurations. During the encryption and decryption stages, the encryption time and decryption time are measured for each image and each matrix key size. These measurements are used to calculate the total computation time, which serves as the primary indicator for evaluating computational efficiency in the optimization process.

In addition to performance measurement, the optimization method incorporates an evaluation of cryptographic security to ensure that efficiency improvements do not compromise the strength of the encryption scheme. Security assessment is carried out using Entropy, Number of Pixel Change Rate (NPCR), and Unified Average Changing Intensity (UACI). These metrics are computed for each encrypted image and each key size configuration to assess randomness, pixel sensitivity, and diffusion characteristics. The determination of the optimal configuration is based on a joint evaluation framework, where computational efficiency indicators and cryptographic security metrics are analyzed together. A matrix key configuration is considered optimal if it provides improved computational efficiency while maintaining acceptable levels of entropy, NPCR, and UACI. This method ensures that the optimization process balances performance enhancement with the security requirements of image cryptography for copyright protection.

3. Results And Discussion

3.1 Visual Encryption and Decryption Results

Figure X illustrates a representative example of the encryption and decryption process using a sample image from the MIT–Adobe FiveK dataset. The figure presents three stages: the original image, the encrypted image, and the decrypted image.

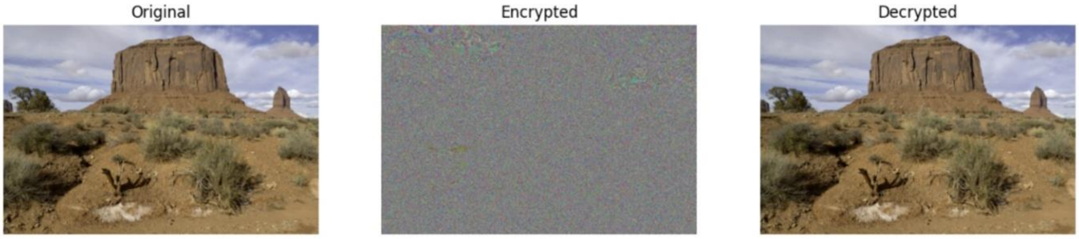

Figure 2. Example of the encryption and decryption

The encrypted image appears as a visually random and noise-like pattern, in which no recognizable structure, texture, or semantic information from the original image can be observed. This indicates that the Hill Cipher algorithm effectively obscures visual content, fulfilling the primary requirement of image cryptography for copyright protection. The transformation demonstrates strong confusion and diffusion properties, making the encrypted image unsuitable for unauthorized visual interpretation.

The decrypted image shows a successful reconstruction of the original image, with no visible distortion or loss of visual information. This confirms that the encryption–decryption process is reversible and that the inverse matrix computation is correctly applied. The ability to fully recover the original image validates the correctness and reliability of the proposed cryptographic implementation.

3.2 Effect of Matrix Key Flexibility on Image cryptography

The Table 1 presents the effect of matrix key flexibility on the performance and security characteristics of image cryptography using the Hill Cipher algorithm. The results demonstrate that varying the matrix key size (2×2, 3×3, and 4×4) has a direct impact on both computational efficiency and cryptographic robustness.

Table 1. Effect of Matrix Key Flexibility on Image cryptography

Image	**Key Size**	**Total Time (s)**	**Entropy Cipher**	**NPCR (%)**	**UACI (%)**
dec_demo.png	2×2	21.57	7.97	99.33	29.42
dec_demo.png	3×3	14.30	7.99	99.49	29.54
dec_demo.png	4×4	10.80	7.98	99.45	29.68
enc_demo.png	2×2	21.98	8.00	98.17	33.25
enc_demo.png	3×3	14.06	7.99	99.53	33.55
enc_demo.png	4×4	10.74	8.00	99.60	33.44
a0001	2×2	21.58	7.93	99.47	29.33
a0001	3×3	14.20	7.99	99.43	29.46
a0001	4×4	10.84	7.97	99.59	29.85

From a computational perspective, Table 1 shows that increasing the matrix key size consistently reduces the total processing time for all tested images. This behavior is attributed to the block-based processing mechanism of the Hill Cipher, where larger matrix keys correspond to larger pixel blocks. As a result, the number of block operations required to process a high-resolution image is reduced, leading to improved computational efficiency. This trend is consistently observed across different images, indicating that matrix key flexibility is an effective approach for optimizing performance in image cryptography.

In terms of cryptographic security, the entropy values reported in Table 1 remain close to the ideal level for all matrix key configurations. This indicates that the encrypted images exhibit a high degree of randomness regardless of the selected key size. The stability of entropy values suggests that increasing the matrix key size does not reduce the ability of the Hill Cipher to obscure visual information within the encrypted image.

Furthermore, the NPCR values in Table 1 are consistently high across all matrix key sizes, indicating that a large proportion of pixels in the encrypted images differ from those in the original images. This reflects strong sensitivity to pixel changes and confirms that the encryption process provides effective diffusion, which is essential for resisting differential attacks in image cryptography applications.

Similarly, the UACI values remain within an acceptable and stable range for all configurations. This indicates that the average intensity difference between the original and encrypted images is sufficiently high, demonstrating strong intensity diffusion across the image.

The consistency of UACI values further confirms that matrix key flexibility does not compromise the diffusion strength of the encryption process.

3.3 Performance Optimization Analysis

3.3.1 Time Performance Based on Matrix Key Size

As illustrated in Figure 3, the total computation time of the Hill Cipher algorithm is strongly influenced by the matrix key size. The graph shows a clear decreasing trend in average total processing time as the matrix key size increases from 2×2 to 4×4, indicating an improvement in computational efficiency.

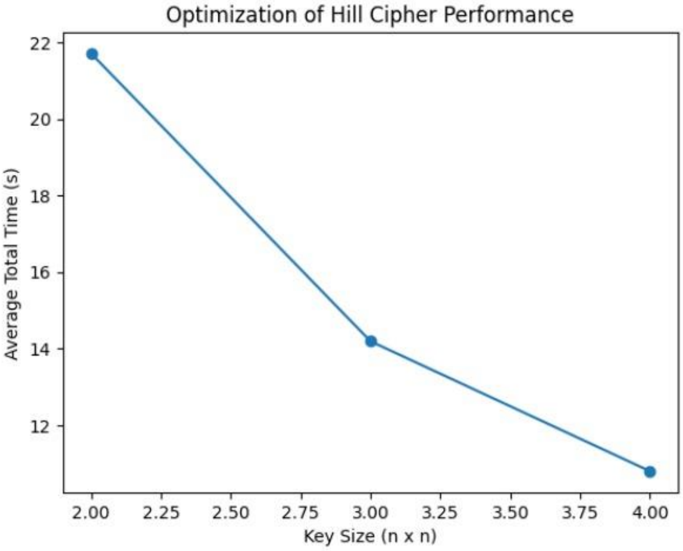

Figure 3. *Time Performance Based on Matrix Key Size*

For the 2×2 matrix key, the computation time is the highest. This occurs because the image must be divided into a large number of small pixel blocks, resulting in frequent matrix multiplication operations during both encryption and decryption. The high number of block-processing iterations increases computational overhead and leads to longer processing time.

When the matrix key size is increased to 3×3, the image is processed using larger pixel blocks. This reduces the number of block operations required to process the entire high-resolution image, thereby lowering the total computation time. A further reduction in computation time is observed when using the 4×4 matrix key, where the image is processed with even larger blocks, minimizing block iteration frequency.

The trend shown in Figure 3 confirms that matrix key flexibility directly contributes to performance optimization. Larger matrix keys improve computational efficiency by reducing the number of block-based operations inherent to the Hill Cipher algorithm. This result demonstrates that performance optimization in Hill Cipher–based image cryptography is largely determined by block-processing behavior. Based on the experimental results, increasing the matrix key size from 2×2 to 4×4 reduces the total computation time from approximately 21.6 seconds to 10.8 seconds, corresponding to a performance improvement of nearly 50%.

3.3.2 Entropy Analysis

As shown in Figure 4, the entropy values of the encrypted images remain consistently close to the ideal entropy level across different matrix key sizes. This indicates that the encrypted images exhibit a high degree of randomness, regardless of whether a 2×2, 3×3, or 4×4 matrix key is applied. The trend in Figure 4 demonstrates that variations in matrix key size do not introduce significant fluctuations in entropy.

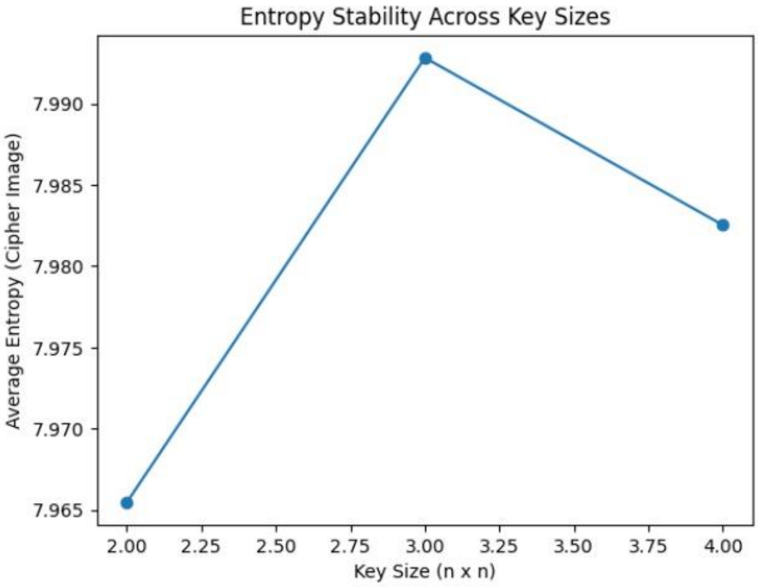

Figure 4. Entrpy Analysis

This stability suggests that the Hill Cipher algorithm maintains strong randomness properties even when larger matrix keys are used. Consequently, the encrypted images do not reveal recognizable visual patterns or statistical structures that could be exploited by unauthorized parties. From a performance optimization perspective, this result is particularly important. Although larger matrix keys are employed to reduce computational time, the entropy values remain stable and close to the ideal level. This confirms that the optimization strategy based on matrix key flexibility does not compromise encryption randomness. Therefore, the proposed approach successfully improves computational efficiency while preserving the core security requirement of image cryptography, namely the effective obfuscation of visual information from the original images.

3.3.3 NPCR Analysis

As illustrated in Figure 5, the NPCR values obtained from the experiments remain consistently high across all tested matrix key sizes. The NPCR results, which range between approximately 98.17% and 99.60%, indicate that a very large proportion of pixels in the encrypted images differ from those in the original images.

These high NPCR values demonstrate that the Hill Cipher algorithm exhibits strong sensitivity to pixel-level changes. Even a minimal variation in the input image results in widespread changes throughout the encrypted image. This property is essential for image cryptography, as it prevents attackers from exploiting statistical similarities between the original and encrypted images. From a performance optimization perspective, the trend shown in Figure 5 confirms that increasing the matrix key size does not reduce diffusion strength. Although larger matrix keys reduce the number of block-processing operations and improve computational efficiency, the NPCR values remain high and stable. This indicates that the optimization strategy preserves the ability of the encryption algorithm to alter nearly all pixel values, thereby maintaining strong resistance to differential attacks while achieving improved processing performance.

DOI : https://doi.org/10.61628/jsce.v7i1.2471

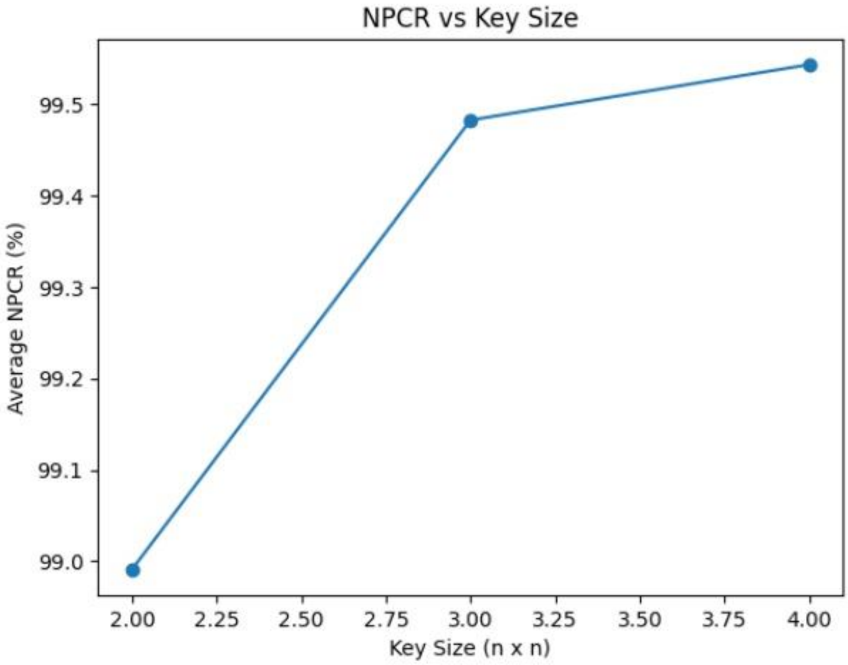

Figure 5. NPCR Analysis

3.3.4. UACI Analysis

As shown in Figure 6, the UACI values obtained from the experiments remain within a stable and acceptable range across all tested matrix key sizes. The recorded UACI values vary approximately between 29.33% and 33.55%, indicating that the average intensity difference between the original and encrypted images is sufficiently high.

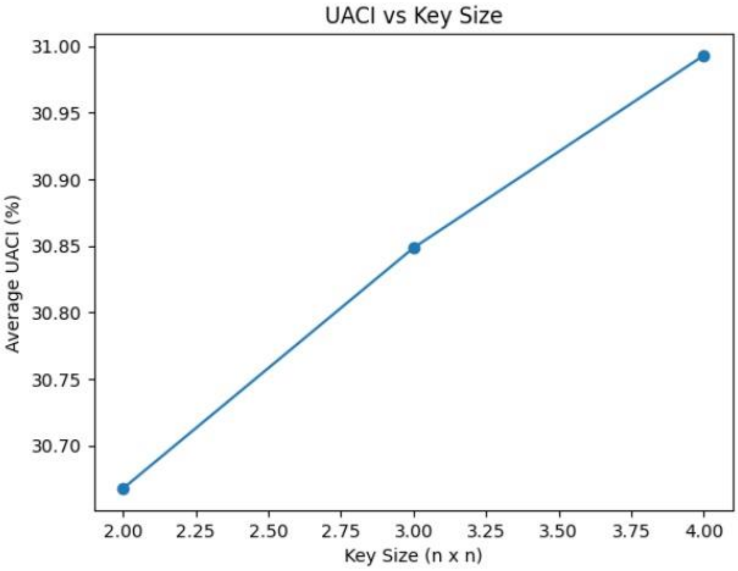

Figure 6. UACI Analysis

These UACI values demonstrate that the encryption process introduces substantial changes in pixel intensity throughout the image. A higher UACI value reflects stronger intensity diffusion, meaning that the encrypted image exhibits significant visual distortion compared to the original image. This property is essential in image cryptography, as it ensures that the encrypted image does not reveal meaningful visual information that could be exploited for unauthorized interpretation. From the perspective of performance optimization, the trend observed in Figure 6 confirms that increasing the matrix key size does not weaken intensity diffusion. Despite the reduction in the number of block-processing operations achieved through larger matrix keys, the UACI values remain stable and within the ideal range for secure image encryption. This indicates that the optimization strategy successfully improves computational efficiency while preserving the strength of pixel intensity diffusion, making it suitable for copyright protection applications involving high-resolution images.

3.4 Discussion

The results indicate that performance optimization in Hill Cipher–based image cryptography is primarily influenced by block-processing behavior rather than changes in cryptographic strength. Although larger matrix key sizes involve higher-dimensional matrix operations, the reduction in the number of processed blocks outweighs this computational overhead. As a result, a net performance gain is achieved. This phenomenon becomes particularly significant for high-resolution images, where block count dominates overall computational cost.

This study focuses on performance optimization of image cryptography for copyright protection on high-resolution images by introducing flexible matrix key sizes in the Hill Cipher algorithm. The results summarized in Table X demonstrate a clear relationship between matrix key flexibility, computational efficiency, and cryptographic security, which directly supports the objective stated in the research title. From a performance perspective, the total computation time consistently decreases as the matrix key size increases from 2×2 to 4×4 across all tested images. This behavior confirms that matrix key flexibility plays a crucial role in optimizing computational performance for high-resolution image encryption. Larger matrix keys enable the algorithm to process the image using larger pixel blocks, thereby reducing the number of block-based operations required during encryption and decryption. As a result, the Hill Cipher becomes more suitable for handling high-resolution images, where computational efficiency is a critical factor in practical copyright protection systems.

In terms of cryptographic security, the entropy values of the encrypted images remain consistently close to the ideal level across all key sizes. This indicates that the increased computational efficiency achieved through larger matrix keys does not reduce the randomness of the encrypted images. The encrypted outputs maintain a high level of unpredictability, ensuring that visual patterns from the original images are effectively obscured. This finding is essential in image cryptography, as entropy directly reflects the algorithm's ability to prevent statistical and visual analysis attacks.

The NPCR results further reinforce the robustness of the proposed optimization strategy. High NPCR values across all key sizes indicate that nearly all pixel values change after encryption, demonstrating strong diffusion properties. Importantly, the diffusion strength remains stable even as the matrix key size increases, showing that performance optimization does not compromise resistance to differential attacks. This characteristic is particularly important for copyright protection, where unauthorized attempts to analyze or manipulate encrypted images must be effectively mitigated.

Similarly, the UACI values remain within an acceptable and stable range for all tested configurations. This indicates that the magnitude of pixel intensity changes between the original and encrypted images remains significant, regardless of the matrix key size used. The consistent UACI results confirm that visual distortion remains strong, ensuring that the encrypted images cannot be visually interpreted without proper decryption keys. The results presented in Table 1 demonstrate a strong correlation between the research title and the experimental findings. The use of flexible matrix keys in the Hill Cipher algorithm successfully optimizes computational performance while preserving essential cryptographic properties, including randomness, diffusion, and intensity variation. This balance between efficiency and security confirms that the proposed approach is well suited for copyright protection of high-resolution images, as it enables faster processing without sacrificing visual cryptographic strength.

Importantly, the experimental results confirm that performance improvement does not come at the cost of reduced security. Entropy, NPCR, and UACI values remain stable across all matrix key sizes, indicating that the proposed optimization strategy preserves randomness, diffusion, and intensity variation. This demonstrates that matrix key flexibility enables a favorable balance between computational efficiency and cryptographic robustness.

4. Conclusions

This research investigated the performance optimization of image cryptography for copyright protection on high-resolution images using the Hill Cipher algorithm with flexible matrix key sizes. The study demonstrated that matrix key flexibility plays a significant role in improving computational efficiency without compromising cryptographic security. The experimental results confirm that increasing the matrix key size reduces the total computation time required for encryption and decryption. This improvement is achieved by reducing the number of block-processing operations inherent to matrix-based cryptography, making the Hill Cipher more suitable for high-resolution image applications where processing speed is critical.

At the same time, the security evaluation shows that the optimized configurations maintain strong cryptographic properties. The encrypted images exhibit high entropy, indicating a high level of randomness, while consistently high NPCR and stable UACI values demonstrate strong pixel diffusion and significant intensity variation. These characteristics ensure that the encrypted images effectively obscure visual information and remain resistant to statistical and differential attacks. The findings confirm that the proposed performance optimization strategy based on flexible matrix key sizes, successfully balances efficiency and security. The Hill Cipher algorithm, when enhanced with matrix key flexibility, proves to be an effective and practical approach for image cryptography in copyright protection of high-resolution images. These findings suggest that flexible matrix key selection can be dynamically adapted based on image resolution and system constraints. Consequently, the optimized Hill Cipher is suitable for real-world applications such as copyright protection systems, digital content distribution platforms, and large-scale image repositories that require efficient and secure image encryption. Future work may explore adaptive key size selection or parallel processing techniques to further enhance performance in large-scale image protection systems.

Acknowledgements

The authors would like to express their sincere gratitude to the Ministry of Higher Education, Science, and Technology of the Republic of Indonesia for the financial support provided for this research. The authors also acknowledge the support and facilities provided by Universitas Nahdlatul Ulama Blitar, which greatly contributed to the successful completion of this research.

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*.

Mafula, V. Y., Fauzan, A. C., Prabowo, T., & Ramadhan, M. R. (2025). *Hill cipher-based visual cryptography for copyright protection of images using flexible matrix keys*. Journal of System and Computer Engineering, 6(1), 101–116.

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