# Implementation of a Combination of Hill Cipher and Least Significance Bit Steganography for Evaluation Digital Image Quality

**[1]Redo Osi Putra, 2*Juju Jumadi, 3Ockhy Jey Fhiter.W**

[1] Student, Informatics Study Program, Faculty of Computer Science, Dehasen University, Bengkulu
Jl. Siti Khadijah No. 562, North Bengkulu (Tel. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail:redho.oziputra123@gmail.com
[2,3,]Permanent Lecturer, Informatics Study Program, Faculty of Computer Science, Dehasen University, Bengkulu
Jl. Meranti Raya No. 32 Bengkulu City 38228 Tel. (0736) 22027, 26957 Fax. (0736) 341139;
e-mail:Joemadhie.2019@gmail.com,Ockhy@unived.ac.id

(Received: November 2025, Revised: February 2026, Accepted: April 2026)

***Abstract****-This study implements a combination of Hill Cipher and Least Significant Bit (LSB) steganography to improve data security and evaluate digital image quality. The Hill Cipher is used to encrypt text with a 2×2 key matrix, while LSB inserts the encrypted message into the least significant bits of the BMP image. The research method used is applied research with stages of analysis, design, implementation, and testing. The test results show that the integration of these two methods maintains image quality with a low Mean Square Error (MSE) value (0.0001–2.9424) and high Peak Signal-to-Noise Ratio (PSNR) (83.6554–103.4438 dB), indicating visually undetectable changes. The simulations prove the effectiveness of the system in securing data without significant image degradation. The conclusion of this study is that the combination of Hill Cipher and LSB steganography is effective in securing data without significantly compromising image quality. This study also provides an alternative solution for data security by using hybrid cryptography and steganography techniques.*

***Keywords: Hill Cipher, LSB Steganography, Data Security, Image Quality, MSE, PSNR.***

***Essence****-This study implements a combination of Hill Cipher and Least Significant Bit (LSB) steganography to improve data security and evaluate digital image quality. Hill Cipher is used for text encryption with a 2×2 key matrix, while LSB embeds an encrypted message into the lowest bit of a BMP image. The research method used is applied research with stages of analysis, design, implementation, and testing. The test results show that the integration of these two methods maintains image quality with low Mean Square Error (MSE) values (0.0001–2.9424) and high Peak Signal-to-Noise Ratio (PSNR) (83.6554–103.4438 dB), indicating changes that are not visually detectable. Simulations prove the effectiveness of the system in securing data without significant image degradation. The conclusion of this study is that the combination of Hill Cipher and LSB steganography is effective in securing data without significantly sacrificing image quality. This study also provides an alternative solution for data security by utilizing cryptography and steganography techniques in a hybrid manner.*

***Keywords :Hill Cipher, LSB Steganography, Data Security, Image Quality, MSE, PSNR***

## I. INTRODUCTION

The rapid development of digital technology has increased the need for reliable data security systems, especially in the exchange of confidential information through image media. Cryptography and steganography are two primary approaches frequently used to protect data. Cryptography is one technique that can be used to secure information. Cryptography has two common stages: encryption and decryption. Encryption is the process of converting an original message into ciphertext, while decryption is the process of converting an encrypted message into a readable and understandable one.(Ridho et al., 2022).*Hill cipher*which is a polyalphabetic cipher can be categorized as a block cipher, because the text to be processed is divided into blocks of a certain size. Each character in a block will influence the other characters in the encryption and decryption process, so that the same character is not mapped to the same character.(Ramadani, 2020). On the other hand, LSB (Least Significant Bit) steganography is known as a simple method for hiding messages in images, but it is vulnerable to statistical detection if the pixel modification is too obvious (Kumar & Sharma, 2023). The LSB steganography technique utilizes the least significant bits of an image to store secret messages. In this case, images of fish or the sea can be used as a medium for storing secret messages. The secret message will be hidden in bits that do not


P-ISSN1858-2680
E-ISSN2723-4673

significantly affect the image quality so that the message cannot be detected by the human eye. Evaluation of image quality after the message embedding process is crucial to ensure that the changes that occur are not visually detected. According to Kumar & Sharma (2023), the use of MSE (Mean Square Error) and PSNR (Peak Signal-to-Noise Ratio) can provide an objective measure of image degradation due to message embedding. However, their research only focused on LSB optimization without involving cryptography. This research will adopt a similar approach but in a hybrid context, namely by measuring MSE and PSNR on images that have gone through the Hill Cipher encryption process and LSB embedding.

## II. LITERATURE REVIEW

Encryption isThe process of using a specific algorithm to convert data or information into a format that is almost unidentifiable as the original information. Plaintext is information or messages sent in an easily readable or original format.(Ziliwu, Maslan, & Kremer, 2022).

### Basics of Cryptography

Cryptography is a science that studies how to keep data or messages safe when sent, from sender to recipient without experiencing interference from third parties. The principles underlying cryptography are:

a. *Secrecy*(confidentiality), a service used to protect the contents of information from anyone except those who have the authority or secret key to open or delete encrypted information.
b. *Authentication,*This relates to identification or recognition, both of the system as a whole and of the information itself. Two communicating parties must identify themselves. Information sent through a channel must be authenticated for authenticity, data content, time of delivery, and so on.

Access rights to a file or other facility in an information processing system are still another area where cryptographic ideas have been applied.

Decryption is the opposite of encryption because its purpose is to return a coded message or false information to its original form. The process of restoring the contents of a coded message requires the use of a pre-prepared code. The process of converting a message's contents from plaintext to ciphertext is called encryption, and the process of returning the text from ciphertext to plaintext is called decryption. (Ziliwu, Maslan, & Kremer, 2022).

### Hill Cipher Cryptography

A cryptographic algorithm, or cipher, often referred to as a code, is a mathematical function used for encryption and decryption. There are two types of cryptographic algorithms: symmetric algorithms and asymmetric algorithms. The Hill cipher, a polyalphabetic cipher, can be categorized as a block cipher because the text to be processed is divided into blocks of a certain size. Each character in a block influences the other characters in the encryption and decryption process, so that the same character is not mapped to the same character.(Ramadani, 2020).

Steganography is an alternative solution for securing important and private information. The term steganography comes from the Greek words steganos, meaning disguise or concealment, and graphein, meaning writing. Thus, steganography can be defined as the art of hiding messages within other data without altering the underlying data, so that the underlying data appears nearly identical before and after the concealment process.(Wibisono, Waluyo, & Ujianto, 2020).

## III. RESEARCH METHODOLOGY

### Research methods

In conducting this research, the author used an applied research method. Applied research is


P-ISSN1858-2680
E-ISSN2723-4673

conducted with regard to practical realities, the application, and development of knowledge generated by basic research in real life. Applied research serves to find solutions to specific problems. The primary goal of applied research is problem-solving so that the research results can be utilized for the benefit of humanity, both individually and collectively, as well as for industrial or political purposes, rather than solely for scientific insight.

In carrying out this applied research there are 5 (five) steps, including:

a. Do something that is needed, studied, measured, and checked for weaknesses.
b. Finding one of the weaknesses obtained is selected for research.
c. Seeking and providing solutions in problem solving
d. Then modifications are made so that the solution can be implemented.
e. The solution is maintained and placed in a single unit so that it becomes a permanent part of a system.

**Method of collecting data**

The data collection methods that the author used in this research are as follows:

Observation

In collecting data through observation, the author observed and analyzed the stages or steps of Hill Cipher cryptography and steganography.LSB on digital image objects.

Literature review

The method by which the writer studies and searches for data from books and references related to the problem being written about.

## IV. RESULTS AND DISCUSSION

### A. Application Results

The implementation application of Least Significance Bit (LSB) steganography and Hill Cipher cryptography for data security was built according to the analysis and design as described in the previous chapter, namely the research methodology chapter, so in this section will be presented the results of the application built using the design that has been done in the previous chapter. The LSB steganography and Hill Cipher cryptography application successfully inserted a message into an image object without changing the color significantly and strengthened with the Hill Cipher cryptographic key. This Hill Cipher algorithm is difficult to solve because it uses matrix multiplication. Apart from these advantages, the Hill Cipher algorithm also has disadvantages, one of which is that it cannot restore messages that use spaces because the Hill Cipher formula table only contains AZ. while the disadvantage of LSB is the number of inserted message characters is limited, so the size of the image must adjust the size of the message. In this chapter, a discussion will be carried out on the results of the system built, the system's functionality and an analysis of the system's performance based on the output results produced by the system.

### B. System Discussion

In the Least Significance Bit (LSB) steganography and Hill Cipher cryptography security applications, there are several interfaces designed to make it easier for users to use or run these applications. The interfaces are as follows:

**1. *Interface*Main course**

*Interface*The main menu is the interface that first appears when the system is run. On this interface there are selection buttons, namely the "Insert and Encryption" button which is used to enter the Insert and Encryption interface, the "Extract and Decryption" button is used to enter the Extract and Decryption interface, the "MSE and PNSR Testing"


P-ISSN1858-2680
E-ISSN2723-4673

button is used, and the "Exit" button is used to exit the system. Display on the main menu form


**Figure 1. Application Main Menu**

## 2. Insert and Encryption Interface

*Interface*The Insert and Encryption interface will be displayed if the user selects the "Insert and Encryption" button. In general, this interface's main function is to insert a message into a digital image object and then encrypt it using the Hill Cipher algorithm. The Insert and Encryption implementation shows how the developed system can insert and encrypt messages into input image objects using the LSB and Hill Cipher techniques.

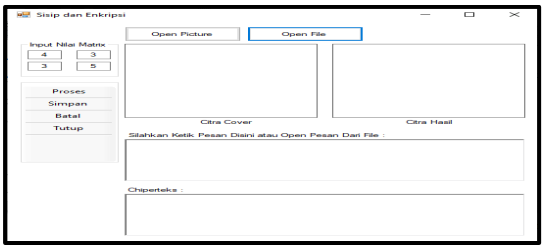



**Figure 2. Insert and Encryption Interface**

In figure 2. userClick the open picture button to select the image you want to insert a message into.

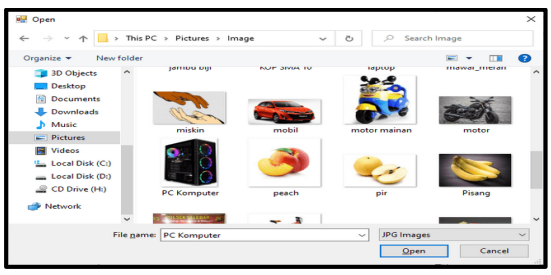



**Figure 3. Explorer Dialog Box**

Select the file to insert the message and encrypt it, for example a motorbike file, then an image like the following will appear.


**Figure 4. Selected Image File**

From figure 4, enter the matrix value in the column provided, then type or select open message from file, then the following results will appear:

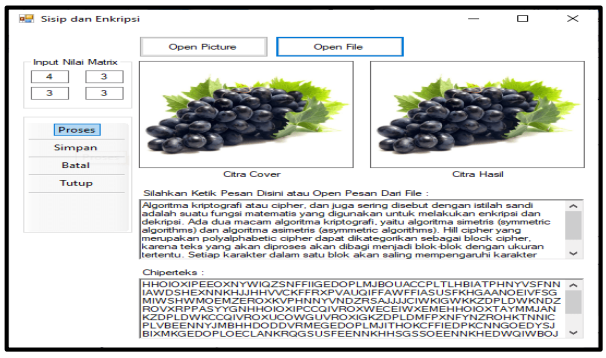



**Figure 5. Results of the Insertion and Encryption Process**

## 3. Extract and Decrypt Interface

Interface implementationextract and decrypt shows that the functionextract and decryptowned by the system can run well where the system is able to extract and decrypt messages contained in the image.

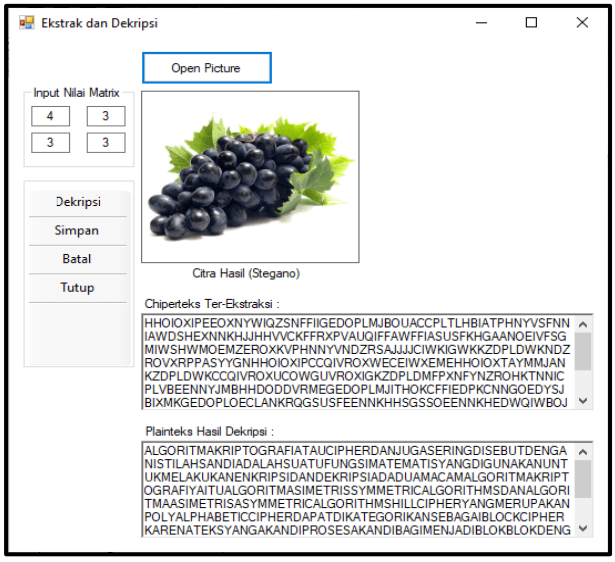



**Figure 6. Extract and Decrypt Interface**


P-ISSN1858-2680
E-ISSN2723-4673

### 4. MSE and PNSR Test Interface

Image testing is performed by inserting, extracting, encrypting, and decrypting. Several bitmap images are used as test images.

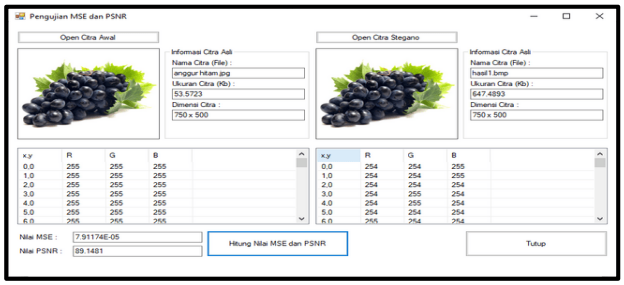
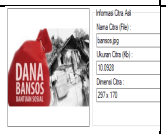



**Figure 7. MSE and PNSR Test Interface**

Figure 4.7 shows that the MSE and PNSR tests carried out by the system can run well, where the system is able to analyze basic information from the opened image, such as image size, image dimensions, MSE and PNSR values. Several images used as test images in this study can be seen in the following table: \

| No. | Initial Image Information | LSB and Hill Cipher Image Information | MSE value | PNSR Value |
|---|---|---|---|---|
| 1 |  |  | 7.9117 | 89.1481 |
| 2 |  |  | 0.0001 23142 | 87.2267 |
| 3 |  |  | 0.0001 01384 3 | 88.0711 |
| 4 |  |  | 1.5832 2 | 96.1354 |
| 5 |  |  | 0.0002 80246 5 | 83.6554 |
| |  |  | 2.9424 | 103.4438 |

**System Testing**

The testing carried out on this application is by using the black box technique, this black box technique is a testing technique that focuses on the output of the response results, or simply to find out whether there are errors or there are functions that do not work as expected.The purpose of this testing is to ensure that the software being built is of reliable quality, namely being able to present the basic analysis of the specifications, design, and coding of the software itself. The following is a table of black box testing.

**Table 2. Black Box Testing**

| Test Type | Test Description | Types of Testing |
|---|---|---|
| Open | Searching for image.bmp | *Black Box* |
| *Insert and Encryption* | Object insertion and encryption process | *Black Box* |
| Extract and Decrypt | Display message content again | *Black Box* |
| MSE and PNSR Testing | Testing the image value before and after inserting the message | *Black Box* |

| Case and Test Results Image.bmp | | | |
|---|---|---|---|
| **Input Data** | **Which are expected** | **Observation** | **Conclusion** |
| Enter image.bmp | Image can be processed | Image successfully processed | [x] accepted [ ] rejected |
| Insertion and encryption | Images can be inserted and encrypted | Image successfully inserted and encrypted | [x] accepted [ ] rejected |
| Extract and decrypt | Displays the inserted message | Message appears | [x] accepted [ ] rejected |
| MSE and PNSR Testing | Displays image object information before and after LSB and Hill Cipher processing. | Successfully displayed image information | [x] accepted [ ] rejected |

## V. CLOSING

### A. Conclusion

After conducting literature studies, designing, analyzing, implementing and testing the system, the following conclusions can be drawn:

1. Implementation of steganography with algorithms*Least Significance Bit*(LSB) and Hill Cipher algorithm cryptography on digital image objects can run well.


P-ISSN1858-2680
E-ISSN2723-4673

2. The application of steganography using the Least Significant Bit (LSB) method can be combined with Hill Cipher cryptography. This can be proven by successfully encrypting data and embedding it into an image without significantly reducing the quality of the original image, making it indistinguishable from the embedded message.
3. The image quality depends on the number of message characters or the size of the message file inserted in the image object.

**B. Suggestion**

The suggestions the author makes are expected to further improve the results obtained. Here are some suggestions from the author:

1. In the development of the next data security application, it can be developed by combining steganography and cryptography with other algorithms.
2. For further development, a file can be used, for example a file in docx format, which can be selected by the user.
3. To increase the level of security of data, other modern encryption methods can be used, such as the 64-bit AES algorithm, RSA and others, because the Hill Cipher method is still a classic method.

**BIBLIOGRAPHY**

[1]Alfina, O., & Harahap, F. (2019). UML Modeling of Decision Support System in Class Determination of Mentally Disabled Students. METHOMIKA: Journal of Informatics Management & Computerized Accounting, 143-150.

[2] Andhika, DI, Muharrom, M., Prayitno, E., & Siregar, J. (2022). Design and Construction of a Document Receiving System at PT. Reasuransi Indonesia Utama. JITEK (Journal of Informatics and Computer Technology), 136-145.

[3] Arianti, T., Fa'izi, A., Adam, S., & Wulandari, M. (2022). Designing a Library Information System Using UML (Unified Modeling Language) Diagrams. Journal of Applied Computer Science and Information (JIKTI), 19-25.

[4] Ayumida, S., Azis, MS, & Fiano, ZG (2020). Implementation of Desktop-Based Payment Administration Program (Case Study: SMA Negeri 1 Cikampek). Interkom Journal: Journal of Scientific Publications in the Field of Information and Communication Technology, 72-83.

[5] Fauziah, RZ, Khudzaifah, M., & Herawati, E. (2024). Securing Text Messages Using Affine Cipher and Goldbach Code Algorithm. CyberSecurity and Digital Forensics, 1-6.

[6] Gunawan, I., & Sumarno. (2018). The Use of Least Significant Bit Steganography Cryptography Algorithm for Securing Text Messages and Video Data. J-Sakti (Journal of Computer Science and Informatics), 57-65.

[7] Haris, CA, & Ariyus, D. (2020). Combination and Modification of Vigenere Cipher and Hill Cipher Using Hybrid Postcode, Trigonometry, and Temperature Conversion Methods as Message Security. Mulawarman Informatics: Scientific Journal of Computer Science, 90-96.

[8] Hasibuan, YW, Isnarto, & Veronica, RB (2022). Design and Implementation of Hill Cipher Algorithm Cryptography Application in Decryption and Encryption of Bank Sampoerna Customer Financial Data Using ASCI Code. UNNES Journal of Mathematics, 45-68.

[9] Jumadi, J., Yupianti, & Sartika, D. (2021). Digital Image Processing for Object Identification Using the Hierarchical Agglomerative Clustering Method. Journal of Science and Technology, 148-156.

[10] Kumar, A., & Sharma, R. (2020). A Hybrid Approach for Secure Data Transmission Using AES and LSB Steganography. Journal of Information Security, 11(3), 45-60

[11] Limantoro, RR, & Kristiadi, DP (2021). Development of a Green Folder Data Collection Information System Using Object-Oriented Methods and Web-Based UML at TKHarvest Christian School. JOURNAL OF INFORMATION SYSTEMS AND TECHNOLOGY (SINTEK), 7-14.

[12] Lutfi, S., & Rosihan. (2018). Comparison of LSB (Least Significant Bit) and MSB (Most Significant Bit) Steganography Methods to Hide Confidential Information in Digital Images. JIKO (Journal of Informatics and Computers), 34-42.

[13] Muafi, Wijaya, A., & Aziz, VA (2020). Expert System for Diagnosing Eye Diseases in Humans Using the Forward Chaining Method. Journal of Computing and Information Technology, 43-49.

[14] Rahmatillah, SR, Tahir, M., Detina, HI, Darmasaputra, A., Laili, II, Aliy, Z., et al. (2024). Steganography: Data Security with the Least


P-ISSN1858-2680
E-ISSN2723-4673

Significant Bit Method Using Python. Journal of Information Systems and Information Technology (JURSISTEKNI), 439-447.
[15] Ramadani, S. (2020). HYBIRD Cryptosystem Hill Cipher Algorithm and Elgamal Algorithm on Image Security. METHOMIKA: Journal of Informatics Management & Accounting Computerization, 1-9.
[16] Ridho, A., Mutia, C., & Sinaga, AP (2022). Analysis of Encryption and Decryption of Cipher Text Using a Combination of Gronsfeld Cipher with Reverse Cipher. JTIK (Jurnal Teknik Informatika Kaputam), 87-94.
[17] Sutrisno, J., & Karnadi, V. (2021). English Learning Support Application Using Android-Based Song Media. COMASIE JOURNAL, 31-41.
[18] Syahril, M., & Jaya, H. (2019). Steganography Application for Customer Data Security at Standard Chartered Bank Using the Least Significant Bit and RC4 Methods. National Seminar on Science & Information Technology (SENSASI), 505-509.
[19] Syarif, M., & Nugraha, W. (2020). UML Diagram Modeling of Cash Payment System in E-Commerce Transactions. Kaputama Informatics Engineering Journal, 64-70.
[20] Wibisono, G., Waluyo, T., & Ujianto, E. (2020). Study of Steganography Methods in Spatial Domain. JTIK (Journal of Computer Science and Technology), 251-256.
[21] Yusup, I., Carudin, & Purnamasari, I. (2020). Implementation of Caesar Cipher Algorithm and Least Significant Bit Steganography for Document Files. JUTISI (Journal of Informatics Engineering and Information Systems), 434-441.
[22] Ziliwu, K., Maslan, A., & Kremer, H. (2022). Implementation of Caesar Cipher in Cryptographic Algorithms in Encrypting Whatsapp Messages. Comasie Journal, 117-125.


P-ISSN1858-2680
E-ISSN2723-4673