Application Of Hiding Messages With Cryptographic Algorithm Modification of Caesar Cipher and Hill Cipher

Rini Wijayanti*[1], Siska Febriani[2], Dony Ariyus[3]
[1,2,3]Magister Teknik Informatika Universitas AMIKOM Yogyakarta
E-mail: *[1]**riniwijayanti12@gmail.com**, [2]siska17feb@gmail.com,[3]dony.a@amikom.ac.id

Abstrak

Dalam era teknologi informasi saat ini, diperlukan cara untuk mengamankan pesan dengan baik. Pengamanan pesan bertujuan untuk menghindari adanya penyusup dalam komunikasi, karena pesan yang dikirim bersifat rahasia. Yang hanya dapat diakses oleh orang yang memiliki kepentingan saja. Salah satu cara untuk mengamankan pesan yaitu dengan metode kriptografi. Ada banyak sekali algoritma kriptografi yang dapat digunakan, seperti Caesar Cipher dan Hill Cipher. Kedua algoritma ini merupakan algoritma kriptografi golongan simetris, karena kunci yang digunakan dalam proses enkripsi dan dekripsi menggunakan kunci yang sama. Untuk memberikan tingkat keamanan ganda, maka dilakukan modifikasi kedua algoritma tersebut. Caesar Cipher dilakukan proses konversi menjadi bilangan biner, dan melakukan operasi XOR dengan pergeseran kunci sebagai proses enkripsi. Sedangkan dalam Hill Cipher dilakukan modfikasi dengan menggunakan beberapa kode Bank Daerah sebagai kunci untuk proses enkripsi dan dekripsi pesan. Proses terakhir untuk mendapatkan hasil akhir ciphertext yaitu dengan melakukan permutasi dengan rumus yang dimodifikasi, yang disesuaikan dengan kebutuhan. Hasil dari penelitian ini adalah sebuah kombinasi algoritma yang dapat digunakan untuk mengamankan pesan yang dikirim kepada penerima. Proses pengujian dilakukan dengan membandingkan besaran ukuran file gambar asli yang digunakan dengan besaran ukuran file hasil serta jumlah karakter yang dapat ditampung.

Kata Kunci—Pengamanan Pesan, Kriptografi, Caesar Cipher, Hill Cipher, Permutasi

Abstract

In the current of information technology, we need a way to properly secure message. Message seurity aims to avoid intruders in communication, because the messages sent are confidential. Which can only be accessed by people who have interests. One way to secure messages is by the cryptographic method. There are many cryptograpic algorithms that can be used, such as Caesar Cipher and Hill Cipher. Both of these algorithms are symetric group cryptographic algorithms, because the keys used in the encryption and decryption process use the same key. To provide a double level security, both algorithm modifications were made. Caesar Cipher carried out the conversion process into binary numbers, and carried out XOR operations by shifting keys as an encryption process. Whereas in the Hill Cipher modification is done by using some Regional Bank codes as a key for message encryption and decryption process. The final process to get the ciphertext end result is to do permutations with a modified formula, which is adjusted to needs. The result of this study are a combination of algorithms that can be used to secure messages sent tp recipients. The testing process is done by comparing the size of the original image file used with the size of the resulting file size and the number of characters that can be accommodated.

Keywords—*Message Security, Cryptography, Caesar Cipher, Hill Cipher, Permutation*

1. INTRODUCTION

Security in delivering a secret message is one factor that must be considered both from the sender and recipient of the message. With the existence of good security it will minimize the intruders entered in communication. One way to secure data or messages is to use cryptographic techniques. Cryptography is one of the fields of science that studies how to convey messages in secret without being known by unauthorized parties [1]. Cryptography is also a way to secure a message when the message is sent from the sender to the recipient with a different place [2].

Based on the keys used, cryptography is divided into three types, namely symmetric algorithm and asymmetric algorithm [2]. The difference between symmetric and asymmetric algorithms lies in the keys used during the encryption and decryption process, where the symmetric algorithm uses the same key, whereas the asymmetric algorithm uses different keys.

The symmetric algorithm is a classic algorithm, which emphasizes the security of the secret key used for the encryption and decryption process [2]. The sender of the message must first inform the recipient of the message about the key that is used so that the recipient can carry out the decryption process and know the contents of the message. The key function (key) in this algorithm is not only used for the encryption process, but also functions as an authentication [1]. One of the cryptographic algorithms belonging to the symmetric algorithm is the Hill Cipher. The Hill Cipher algorithm is included in the polyalphabet group, where each character has the possibility of more than one type of alphabet character by using the substitution method [2] [3]. Hill Cipher in 1929 was discovered by Lester S. Hill [2]. Hill Ciher's algorithm uses modulo arithmetic, which technique uses a square matrix which is run as an encryption and decryption key [4].

Research in the field of cryptography has been conducted by previous researchers, such as that conducted by Muhammad Hasanudi et al. Research conducted using the Hill Cipher cryptographic algorithm by combining one of the steganographic methods, namely Least Significant Bit [5]. This research conducts secret message security twice, namely security using the Hill Cipher and then the results of the ciphertext are inserted into the media image, thus providing multiple security in delivering messages.

Subsequently the research was carried out by Muhammad Hilman in 2018, this study modified the Hill Cipher algorithm [6]. Modifications made by this researcher are, changing the key (key) used for the encryption and decryption process using the circulatory method. This method serves to make a combination of public and private keys so as to produce a primary key that will be used in the next decryption encryption process. Subsequent research was conducted by Selviana Yunita, et al. This study aims to provide alternative choices of cryptographic algorithms in terms of data encryption speed and complexity in deciphering passwords [7]. This study uses a combination of Hill Cipher and Twofish cryptographic algorithms in decrypting encryption. The encryption and decryption process in this research is very dependent on the size of the file size, because the size of the file size will affect the speed and number of data processing to be processed. Finally, the research conducted by Pratiwi Rachmadi, this study conducted data encryption and decryption carried out using the Hill Cipher method with a modification of the ATM PIN (Personal Identifier Number) used as a key [8]. The message encoding process is done using the Hill Cipher method with a 6 digit ATM PIN number provided by the Bank to its customers. The implementation uses ASCII characters to provide the possibility of more characters being covered, i.e. it is not limited to only 26 letters of the alphabet.

Based on research related to message encryption and decryption, applied research will be carried out with the modification of the Hill Cipher algorithm by using several Regional Bank Codes as the key to encrypting and decrypting. In addition, this study also conducted a combination of two cryptographic algorithms namely Hill Cipher and Caesar Cipher. The combination of these algorithms aims to provide double security in the delivery of messages, so that a kripanalis does not easily find out the original message. The other purpose of this study is also to provide an alternative choice of algorithm for securing messages. The results of this

study are in the form of an application with the PHP programming language using the Hill Ciper key modification method.

2. RESEARCH METHOD

The method used in this study is a combination of Caesar Cipher and Hill Cipher cryptographic algorithms. This study also modified the Hill Cipher algorithm with the key of the Regional Bank Code.

2.1. Research Flow

The flow of research is a description of the research to be conducted, to find out the flow of research can be seen in Figure 1.

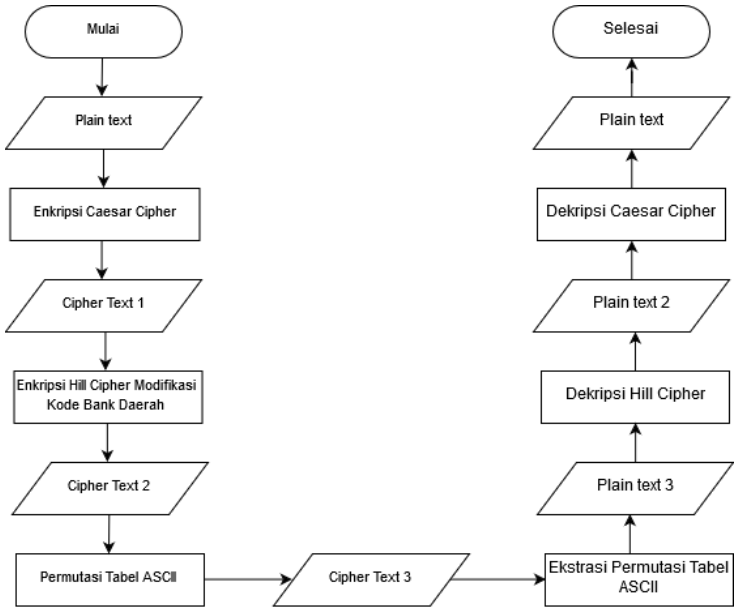

Figure 1. Research Flow

The first stage of encryption will be carried out using the Caesar Cipher algorithm, in this algorithm a key is needed to be used for both encryption and decryption processes. The first process is done by changing each character in the plaintext to decimal in the ASCII table and then encrypting it by shifting the character of the number of keys used. After the Caesar Cipher encryption process is completed, the results of the ciphertext phase 1 will be used as a plaintext for the next stage of encryption, by encrypting using the Hill Cipher method with the modification of the Regional Bank code used as a key. After the encryption process using the Hill Cipher method is complete, permutations are performed using the ASCII table so that the ciphertext results are safer so it is difficult to solve.

To make permutations with the ASCII table a modification of the permutation mathematical formula is made to suit the research needs. To encrypt the formula used is formula (1), whereas to decrypt it using mathematical formulas (2).

$$p = n - r \quad \text{..... (1)}$$
$$r = p - r \quad \text{..... (2)}$$

$p = permutation$ $n = number\ of\ ASCII$ $r = character - n$

2.2. Regional Bank Code

Modification of the Hill Cipher key uses several Regional Bank Codes to carry out the encryption and decryption process. Regional Bank Codes used in this study are shown in table 1 below:

Table 1. List of Regional Bank Codes

No	Regional Bank Code	Modification	Description of the Regional Bank Code
1	112	1121	Bank DIY
2	113	1131	Bank Jateng
3	133	1331	Bank Bengkulu
4	131	1311	Bank Maluku Malut

To do the encryption using the Hill Cipher the key used is adjusted to the number of keys in the Caesar Cipher encryption. The key used will loop as needed.

3. RESULTS AND DISCUSSION

3.1 Encryption Process

In this encryption process, first do the plaintext encryption using the Caesar Cipher method, then the Caesar Cipher ciphertext results will be encrypted again using the Hill Cipher method.

3.1.1. Caesar Cipher

The encryption process using the Caesar Cipher makes modifications that is changing the plaintext to an 8-bit binary number, then performs the key shift of the number of keys used right, then XOR arithmetic operations are carried out, but when the number of plaintext characters is odd, an additional character will be added to the end of the character. For example the plaintext used is "BLESSING" having an even number of characters, so no additional characters are needed. With a Caesar Cipher key is 3. In the process, Caesar Cipher encryption is changing the plaintext with the substitution method according to the number of keys used. The first thing to do is to change each plaintext character to ASCII decimal numbers, as shown in table 2 below:

Table 2. ASCII Plaintext Decimal Numbers

B	E	R	K	A	H
66	69	82	75	65	72

The second step is to convert the plaintext decimal number into an 8-bit binary number.

Plaintext = BERKAH
Binary = 010000100100010101010010010010110100000101001000

The third stage, performs the first encryption process, which is to shift 3 bits to the right by XOR operations. The results are as follows:

Plaintext	01000010	01000101	01010010	01001011	01000001	01001000
Result	00101000	01011000	00101010	00111001	00011000	00001001 ⊕
	01101010	00011101	01111000	01110010	01011001	01000001

The results of the XOR operation are then converted to decimal form, the results can be seen in table 3, and this is the ciphertext generated in the Caesar Cipher encryption process.

Table 3. Binary to Decimal Conversions

Biner	01101010	00011101	01111000	01110010	01011001	01000001
Desimal	106	29	120	114	89	65

3.1.2. Hill Cipher

The next step encryption process uses the Hill Cipher method. The plaintext used in the encryption process is the result of the ciphertext in the previous Caesar Cipher encryption. Then do the encryption using Hill Cipher with the modification of the Regional Bank code key. The keys used in this encryption process include:

$$K1 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \qquad K2 = \begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix} \qquad K3 = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$$

The first step in encrypting in Hill Cipher is to divide the plaintext into blocks that are adjusted to the number of columns in the key matrix. Plaintext block division can be seen as follows:

Blok 1		**Blok 2**		**Blok 3**	
j	♦♦	x	r	Y	A
106	29	120	114	89	65

The next step is to encrypt the multiplication of plaintext blocks with a key.

a. Block 1 (BE)

$$C_{(j♦♦)} = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 106 \\ 29 \end{bmatrix} = \begin{bmatrix} 106 + 29 \\ 212 + 29 \end{bmatrix} = \begin{bmatrix} 135 \\ 241 \end{bmatrix} mod\ 255 = \begin{bmatrix} 135 \\ 241 \end{bmatrix}$$

b. Block 2 (RK)

$$C_{(xr)} = \begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 120 \\ 114 \end{bmatrix} = \begin{bmatrix} 120 + 114 \\ 360 + 114 \end{bmatrix} = \begin{bmatrix} 234 \\ 474 \end{bmatrix} mod\ 255 = \begin{bmatrix} 234 \\ 219 \end{bmatrix}$$

c. Block 3 (AH)

$$C_{(YA)} = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 89 \\ 65 \end{bmatrix} = \begin{bmatrix} 89 + 195 \\ 267 + 65 \end{bmatrix} = \begin{bmatrix} 284 \\ 332 \end{bmatrix} mod\ 255 = \begin{bmatrix} 29 \\ 77 \end{bmatrix}$$

3.1.3. Permutation

The stage after encrypting with the Caesar Cipher and Hill Cipher method is to continue the encryption process by performing permutation arithmetic operations in accordance with equation (1) for encryption.

a. Block 1 (BE) = $\begin{bmatrix}135\\241\end{bmatrix}$

$P_{(135)} = n - r$ $\quad$ $P_{(241)} = n - r$

$= 256 - 135$ $\quad$ $= 256 - 241$

$= 121$ $\quad$ $= 15$

b. Block 2 (RK) = $\begin{bmatrix}234\\219\end{bmatrix}$

$P_{(234)} = n - r$ $\quad$ $P_{(219)} = n - r$

$= 256 - 234$ $\quad$ $= 256 - 219$

$= 22$ $\quad$ $= 37$

c. Block 3 (AH) = $\begin{bmatrix}29\\77\end{bmatrix}$

$P_{(29)} = n - r$ $\quad$ $P_{(77)} = n - r$

$= 256 - 29$ $\quad$ $= 256 - 77$

$= 227$ $\quad$ $= 179$

3.2 Description

After the cipher text is obtained from the previous encryption results, if the recipient wants to know the true purpose of the message, the decryption process must be carried out through the decryption process which will be explained below:

The first step is to carry out permutation arithmetic operations using equation (2) on each existing character block.

a. Block 1 (BE) = $\begin{bmatrix}121\\15\end{bmatrix}$

$r_{(121)} = n - p$ $\quad$ $r_{(15)} = n - p$

$= 256 - 121$ $\quad$ $= 256 - 15$

$= 135$ $\quad$ $= 241$

b. Block 2 (RK) = $\begin{bmatrix}22\\37\end{bmatrix}$

$r_{(22)} = n - p$ $\quad$ $r_{(219)} = n - p$

$= 256 - 22$ $\quad$ $= 256 - 37$

$= 234$ $\quad$ $= 219$

c. Block 3 (AH) = $\begin{bmatrix}227\\179\end{bmatrix}$

$r_{(227)} = n - p$ $\quad$ $r_{(179)} = n - p$

$= 256 - 227$ $\quad$ $= 256 - 179$

$= 29$ $\quad$ $= 77$

The second step is to decrypt it using the Hill Cipher method in general by using a key modification of the Regional Bank Code.

Block 1

K = $\begin{bmatrix}1 & 1\\2 & 1\end{bmatrix}$

1) Calculate key matrix determinants

$$\det = (1 * 1) - (1 * 2) = 1 - 2 = -1$$

2) Looking for inverse modulo 〖-1〗 ^ (- 1) mod 255

$$K = 1 \Rightarrow\gg \frac{255(1) + 1}{-1} = \frac{256}{-1} = -256$$

3) Look for the key matrix inverse

$$K = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \quad K^{-1} = \begin{bmatrix} 1 & -1 \\ -2 & 1 \end{bmatrix}$$

4) Look for the key matrix *Hill Cipher*

$$-256 \begin{bmatrix} 1 & -1 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} -256 & 256 \\ 512 & -256 \end{bmatrix} mod\ 255$$
$$= \begin{bmatrix} 254 & 1 \\ 2 & 254 \end{bmatrix}$$

5) description

$$\begin{bmatrix} 254 & 1 \\ 2 & 254 \end{bmatrix} \begin{bmatrix} 135 \\ 241 \end{bmatrix} = \begin{bmatrix} 34.290 + 241 \\ 270 + 61.214 \end{bmatrix}$$
$$= \begin{bmatrix} 34.531 \\ 61.484 \end{bmatrix} mod\ 255$$
$$= \begin{bmatrix} 106 \\ 29 \end{bmatrix}$$

Block 2

K = $\begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix}$

1) Calculate key matrix determinants

$$\det = (1 * 1) - (1 * 3) = 1 - 3 = -2$$

2) Searching for invers modulo $-2^{-1}\ mod\ 255$

$$K = 1 \Rightarrow\gg \frac{255(1) + 1}{-2} = \frac{256}{-2} = -128$$

3) Searching the key matrix inverse

$$K = \begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix} \quad K^{-1} = \begin{bmatrix} 1 & -1 \\ -3 & 1 \end{bmatrix}$$

4) Searching the Hill Cipher key matrix

$$-128 \begin{bmatrix} 1 & -1 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -128 & 128 \\ 384 & -128 \end{bmatrix} mod\ 255$$
$$= \begin{bmatrix} 127 & 128 \\ 129 & 127 \end{bmatrix}$$

5) Decryption

$$\begin{bmatrix} 127 & 128 \\ 129 & 127 \end{bmatrix} \begin{bmatrix} 234 \\ 219 \end{bmatrix} = \begin{bmatrix} 29.718 + 28.032 \\ 30.186 + 27.813 \end{bmatrix}$$
$$= \begin{bmatrix} 57.750 \\ 57.999 \end{bmatrix} mod\ 255$$
$$= \begin{bmatrix} 120 \\ 114 \end{bmatrix}$$

Block 3

K = $\begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}$

1) Calculate key matrix determinants
$\det = (1 * 1) - (3 * 3) = 1 - 9 = -8$

2) Searching invers modulo $-2^{-1}\ mod\ 255$
$K = 1 \Rightarrow\gg \frac{255(1)+1}{-8} = \frac{256}{-8} = -32$

3) Seaaching Key invers matrik
$K = \begin{bmatrix} 1 & 3 \\ 3 & 1 \end{bmatrix}\ K^{-1} = \begin{bmatrix} 1 & -3 \\ -3 & 1 \end{bmatrix}$

4) Searching Key matrik *Hill Cipher*
$-32\begin{bmatrix} 1 & -3 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} -32 & 96 \\ 96 & -32 \end{bmatrix} mod\ 255$
$= \begin{bmatrix} 223 & 96 \\ 96 & 223 \end{bmatrix}$

5) Decryption
$\begin{bmatrix} 223 & 96 \\ 96 & 223 \end{bmatrix}\begin{bmatrix} 29 \\ 77 \end{bmatrix} = \begin{bmatrix} 6.467 + 7.392 \\ 2.784 + 17.171 \end{bmatrix}$
$= \begin{bmatrix} 13.859 \\ 19.955 \end{bmatrix} mod\ 255$
$= \begin{bmatrix} 89 \\ 65 \end{bmatrix}$

After the decryption process using the Hill Cipher is complete, the final decryption step is to use the Cesar Cipher. In this decryption used decimal numbers obtained in the previous process by changing in the form of 8-bit binary numbers. The next process is to perform an XOR arithmetic operation with the key used in the initial encryption process. For more details can be seen as follows:

Block 1 :

106 = 01101010
00101000 ⊕
01000010

29 = 00011101
01011000 ⊕
01000101

Block 2 :

120 = 01111000
00101010 ⊕
01010010

114 = 01110010
00111001 ⊕
01001011

Block 3 :

89 = 01011001
00011000 ⊕
01000001

114 = 01000001
00001001 ⊕
01001000

The next process is to change the result of the binary XOR operation to a decimal number as below:

	Block 1		Block 2		Block 3	
Binary	01000010	01000101	01010010	01001011	01000001	01001000
Decimal	66	69	82	75	65	72
Chaacter	B	E	R	K	A	H

After the decryption process is done using the Caesar Cipher and Hill Cipher cryptographic

algorithms, then the text "BLESSING" is obtained, according to what was sent by the sender. When the encryption process uses a modification algorithm that is designed, then the message will be re-inserted in an image using the LSB (Least Significant Bit) steganography method.

3.3 Steganograf

Steganography is one type of method that is useful for hiding information on a media in the form of images, sound and video. The word stenography or steganography is one of the languages of the Greek language steganos which is "hidden / veiled" and graphein which is "writing". From these explanations it can be concluded that steganography is writing veiled writing. In steganography, there are two important specs that affect the results of the decryption, namely the container and confidential data that will be hidden. The Steganography Process is depicted in the image below

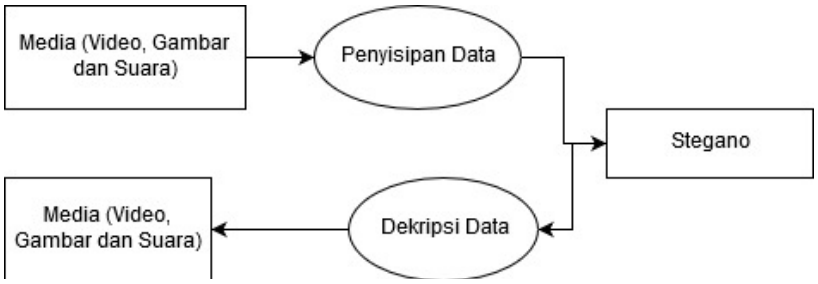

Figure 2. Steganography Process

3.4 LSB (Least Significant Bit)

The Least Significant Bit method is one method to hide messages in digital media by inserting the message. The size of data to hide depends on the size of the container data. For example, in an 8-bit image file measuring 256x256 pixels there are 65536 pixels, each pixel is 1 byte in size and each byte can only hide one bit in its LSB.

In the arrangement of bits in a byte (1 byte = 8 bits), there are the most significant bits (the most significant bit or MSB) and the least significant bits (the least significant bit or LSB). The right bit to replace is the LSB bit, because the change only changes the byte value one higher or one lower than the previous value. Suppose the byte says yellow, then changing one LSB bit does not change the yellow color significantly.

3.5 Algorithm implementation

To implement the algorithm that was designed before, implemented using the PHP programming language. For the encryption form in Figure 3 (a) and the decryption form.

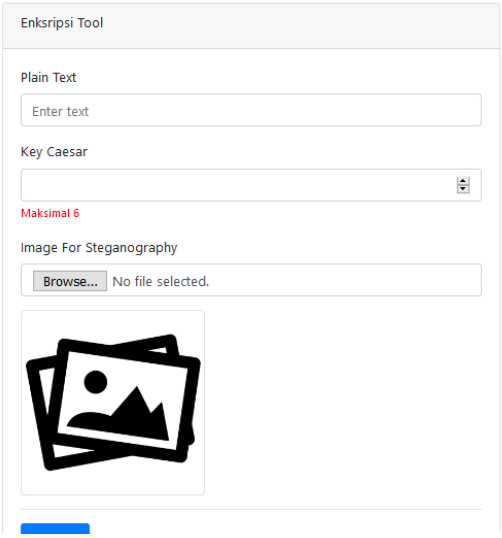

Figure 3 (a). Encryption Form

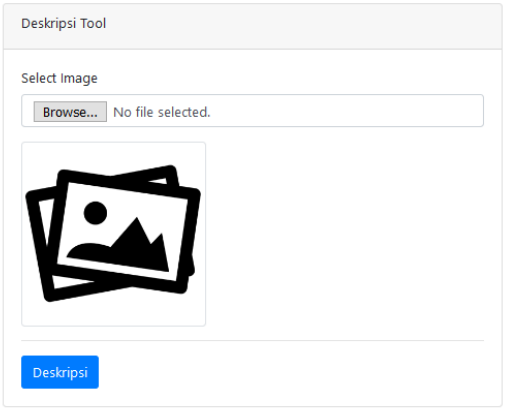

Figure 3 (b). Decryption Form

The trial process for encrypting and decrypting messages is done by conducting 7 attempts, using JPG format image files of various sizes. This test is conducted to determine the success of the system to carry out the encryption and decryption process. Testing is categorized based on the size of the initial and final file sizes after the encryption process. Tests carried out in this study are steganographic testing with LSB which obtains the test results as presented in table 4.

Table 4. Testing Results

No	Encryption Information				Embedd / Insertion Information		Process	
	Key	Number of Message Characters	Image Name	Image Format	Initial Size	Final Size	Encryption	Description
1	3	214	gado gado	JPG	120 KB	993 KB	Successful	Successful
2	4	558	gado gado	JPG	120 KB	994 KB	Successful	Successful
3	3	1362	karedok	JPG	32 KB	283 KB	Successful	Successful
4	4	1362	karedok	JPG	32 KB	283 KB	Successful	Successful
5	6	2384	lontong opor	JPG	22 KB	161 KB	Successful	Successful
6	3	3161	lontong opor	JPG	22 KB	-	Failed	Failed
7	3	3161	lotek	JPG	115 KB	628 KB	Successful	Failed

Table 4 above is the result of trials that have been carried out. Based on table 4, it can be seen that the image file size will affect the success rate of the application to perform the decryption encryption process, as well as affect the number of characters that can be accommodated.

The larger the size of the original image file, the greater the size of the encrypted file. Likewise, the larger the image file size, it will accommodate more characters but does not guarantee that the encryption and decryption process will run.

4. CONCLUSION

The conclusions obtained from this study are:

1. The size of the image file will affect the success of the system in accommodating the number of characters that will be carried out the encryption and decryption process. With a large image file size, the greater the number of characters that can be accommodated. But for the success of the application not all of the data processing is successful. This is because the original file size is too small to accommodate a large number of characters.
2. The number of characters used for the encryption and decryption process affects the size of the resulting file. The more the number of characters, the greater the size of the resulting file, and vice versa.

5. SUGGESTIONS

In subsequent studies, the Caesar Cipher and Hill Cipher modification algorithm can be implemented, using other programming languages. As well as optimizing the use of image sizes so that they can do the encryption and decryption process well and can produce file sizes that are not much different from the original size

REFERENCES

[1] E. Setyaningsih, *Kriptografi & Implementasinya Menggunakan MATLAB*. Yogyakarta: Andi Offset, 2015.
[2] D. Ariyus, *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu, 2006.
[3] D. Damara, J. T. Informatika, F. Tenik, and U. S. Tasikmalaya, "TEKNIK KEAMANAN MULTIMEDIA," Tasikmalaya, 2012.
[4] A. Karima, "Hill Cipher & Vigenere Cipher," Semarang, 2012.
[5] M. H. Hidayat, Y. A. Gerhana, and U. Syarifudin, "Kombinasi Algoritma Kriptografi Vigenere Cipher Dan Hill Cipher Untuk Penyandian Pesan Rahasia Pada Metode Steganografi," vol. 1, no. 1, pp. 1–8, 2018.
[6] M. H. Adiwibawa, R. Marwati, and R. Sispiyati, "Pengimplementasian modifikasi kriptografi hillcipher dengan matriks sirkulan," pp. 1–11.
[7] S. Yunita, P. Hasan, and D. Ariyus, "Modifikasi Algoritma Hill Cipher dan Twofish Menggunakan Kode Wilayah Telepon Hill Cipher and Twofish Algorithm Modification with Phone Region Code," vol. 9, no. 2, pp. 213–224, 2019.
[8] P. Rachmadi, "Penyandian Teks Dengan Metode Hill Chiper," *Progresif J. Ilm. Komput.*, vol. 13, no. 1, pp. 1681–1684, 2017.