Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493)
Vol. 4 No. 1, 2019, pp. 28 – 38

Upload File Security on the Server Using LSB and Hill Cipher

Lekso Budi Handoko*[1]**, Chaerul Umam**[2]
Universitas Dian Nuswantoro, Jl. Imam Bonjol No. 207 Semarang, (024) 3517261
E-mail : handoko@dsn.dinus.ac.id[1]*, chaerul@dsn.dinus.ac.id*[2]
**Corresponding author*

Adelia Syifa Anindita[3]
Universitas Dian Nuswantoro, Jl. Imam Bonjol No. 207 Semarang, (024) 3517261
E-mail : ninditaasyf@gmail.com

Abstract – The rapid development of technology not only has a positive impact, but also can have a negative impact such as the development of cyber crime that can cause messages to be unsafe. Message security can be protected using cryptography to convert messages into secret passwords. Steganography is a technique of hiding messages by inserting messages into images that are used to increase message security. In this study, it discusses a combination of hill cipher and LSB algorithms to secure messages. The message used is a 3-bit grayscale image for steganography and text messages with 32, 64 and 128 characters for cryptography. The measuring instruments used in this study are MSE, PSNR, Entropy and travel time (CPU time). Test results prove an increase in security without too damaging the image. This is evidenced by the results of the MSE trial which has a value far below the value 1, the PSNR is> 65 dB with a range of entropy values of 5 to 7, and travel times are almost the same.

Keywords – Cryptography, Hill Cipher, LSB, Image

1. INTRODUCTION

Server, as one of the storage and data exchange places is very vulnerable to data manipulation. Most servers only use the security model by using access rights, login functions or using multiple passwords. This is considered insecure because there are various confidential data that need to be secured. Safeguarding data by applying cryptographic techniques is one option. It is known that cryptography can be used in both text and file media. On the other hand, large data sizes and various perliu file formats are considered in the selection of cryptographic algorithms.

According to Sangeeta in his research explained about simteric cryptographic techniques that are faster than asymmetric cryptography [1]. This is because simteris cryptography uses permutation and substitution calculations or a combination of the two. Some forms of symmetrical cryptographic algorithms are AES [2], DES. But the algorithm takes a long time with a long form of calculation. On the other hand, there are algorithms that are fast and safe because they only use substitution calculations, namely bit shifting [3]. Bit shifting is done by shifting to a certain shift. This process is also very fast, so it does not add to the workload on the server.

In this study the cryptographic algorithm used is Hill Cipher. According to [1], Hill Cipher is one of the symmetrical key algorithms that has several advantages in data encryption. Steganography is the science used to hide secret messages into a media without changing its shape. The secret message will be inserted in a digital image, so that no one knows that in the image there is a secret message. The steganography method used in this study is the Least Significant Beast (LSB) method. This Least Significant Beast (LSB) method is a method used in hiding secret messages by replacing the lowest bits of data on several pixel images with sequential data bits [4].

In this study, the author will use a merger of two algorithms, namely the Hill Cipher algorithm and the Least Significant Beast (LSB) method which is expected to improve data security or encoded messages. The message used in this study is character and image. The image used is 256 × 256, and 512 × 512 pixels, while the characters used are 32, 64, and 128 characters.

2. CONFIGURATION OF MOBILE ROBOT

2.1. Kirptografi

Cryptography is a science that discusses the encryption process where data will be encrypted by using an encryption key to be something that is difficult to recognize by someone who does not have a decryption key [2]. Encryption is the process of encoding messages from plaintext into ciphertext. While decryption is the process of returning messages from ciphertext to plaintext. This encryption and decryption can be used on messages that have been sent or for messages that have been stored.

2.2. Hill Cipher

Hill Cipher was created by Lester S. Hill in 1929 [1]. This method was created to produce ciphers (codes) that cannot be found by analyzing frequencies. Hill Cipher includes polyalphabetic cryptography which is classified as a block cipher, because the text messages to be processed are divided into several blocks of a certain size [3]. Each character in one block will affect the results of other characters in the process of encryption and decryption. Therefore, the same character in the initial block is not mapped to be the same character also in the final block.

The Hill Cipher algorithm is an algorithm that is difficult to solve because this algorithm uses matrix multiplication for encryption and decryption [4], besides when using a larger key matrix, the frequency for the hiding technique will also be higher. The following will be elaborated on the key matrix on Hill Cipher, as in (1).

$$Kunci = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{bmatrix} \qquad (1)$$

The encryption process in the Hill Cipher algorithm is carried out every plaintext block [1]. The plaintext is then converted to a decimal number before the text is divided into rows of blocks, such as A = 0, B = 1, C = 2, etc. as described below:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z
18	19	20	21	22	23	24	25

The Hill Cipher encryption process can be calculated using the following formula:

$C = K \times\ P\ mod\ 26$ (2)

Where:
C = Ciphertext (Result of encryption with Hill Cipher)
K = Key value in the form of matrix m x m
P = Plaintext is a decimal number

To return to the initial value, the decryption process is performed. This decryption process requires a key, the key used is the inverse of the key matrix. So that the key matrix is obtained using the following formula:

$K\ \times K^{-1}\ = 1$ (3)

While the decryption process on the Hill Cipher algorithm is obtained by using the following formula, as in (4).

$D =\ K^{-1}\ \times C$ (4)

where D is Plaintext before the encryption process is performed.

2.3. Steganography

Steganography is a method for hiding secret messages in digital media, so that third parties will not know that a message has been inserted in the media. Steganography requires two properties, namely placeholders and secret messages that will be hidden [5]. The steganography method uses digital media as placeholders, such as sound, text, video and images.

In general, there are 2 processes in the steganography method, namely the embedding process which is used to hide messages into the cover-object and extraction processes for message extraction from stego-objects [6] which will later require a secret key so that only authorized users can hide and message extraction [7].

2.4. Least Significant Bit (LSB)

Least Significant Bit (LSB) is a steganography method on the spatial domain that conceals messages by changing bits in the image segment with secret message bits including the easiest and simplest steganography method to implement [8]. This method uses digital imagery as covertext. Digital images used are 1 bit (binary), 3 bits (grayscale), and 24 bits (color). LSB must have an imperceptibility value, the image can reach the limits of the Human Visual System (HVS) which is above 40 dBhis study, the image used for the LSB method is a grayscale image with a size of 3 bits. A grayscale image is an image whose pixel intensity value is based on the degree of gray. Many colors depend on the number of bits provided in memory to accommodate the needs of each color. The greater the number of color bits provided in the memory, the smoother the color gradation that will be formed [9]. In addition, grayscale is also called monochromatic, because it has no other color than the variation in intensity of black and white. An image that is made grayscale will look different when compared to a colored image. To hide an image in LSB every byte of 3 bits, it can store 1 byte in each pixel.

Changes from the inserted image cannot be seen significantly with visible eyes [10]. However, this change can be proven by means of testing using measuring instruments such as Peak Signal Noisy to Ratio (PSNR) and Entropy from the resulting image.

3. RESULTS AND DISCUSSION

In this study measurements were made on stego images using PSNR and MSE. PSNR is a comparison between the maximum value of a signal as measured by the amount of noise that affects the signal. In general, PSNR is measured using decibel (dB) units.

In general, the greater the PSNR value, the higher the level of similarity between the inserted image and the original image. Inserted images have good quality images with PSNR levels above 40 dB. PSNR is also used to measure the comparison of the quality of the original image before and after the message is inserted. In determining PSNR, the value of Mean Square Error (MSE) must be determined beforehand. MSE is an error value from the result of the average square between the original image and the stego-image. MSE testing is said to be good if it has a low value. To calculate the MSE value use the following equation:

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} | (I(i,j) - K(i,j))^2 | \qquad (5)$$

$$PSNR = 20 \log \left(\frac{MAX}{\sqrt{MSE}} \right) \qquad (6)$$

Where:
M and N = Dimensions of the image
i and j = coordinates of a point in the image
I (i, j) = insertion image (stego-image)
K (, j) = Original image (cover image)
MAX = The biggest pixel value in the entire image

Tests are performed on the encryption and insertion of messages. To be able to understand the two processes of Hill Cipher-LSB, we can see the two processes given in Figure 1 and Figure 2. The process of encryption and insertion of messages can be described in Figure 1, while the extraction process and decryption process can be described in Figure 2.

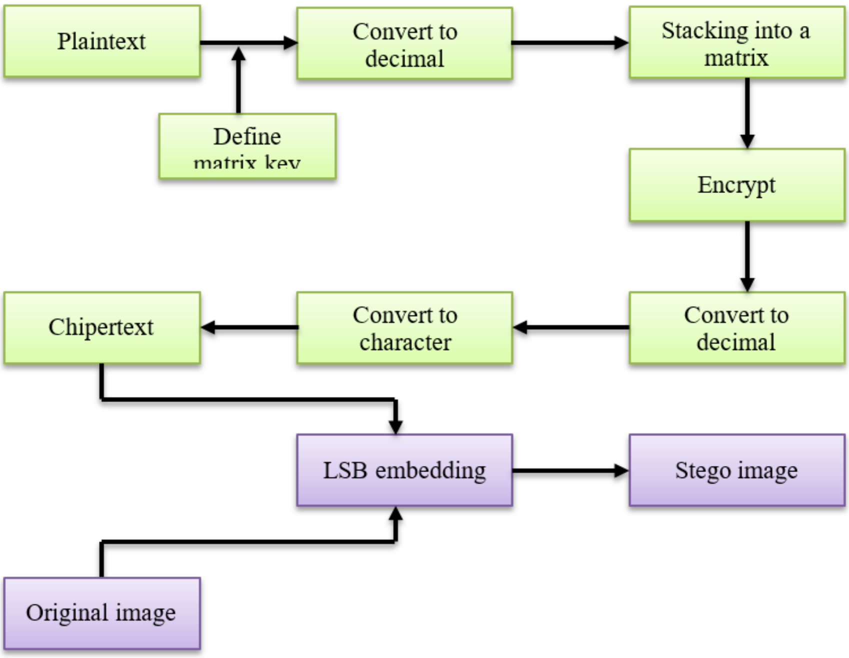


Figure 1. Encryption and embedding process.

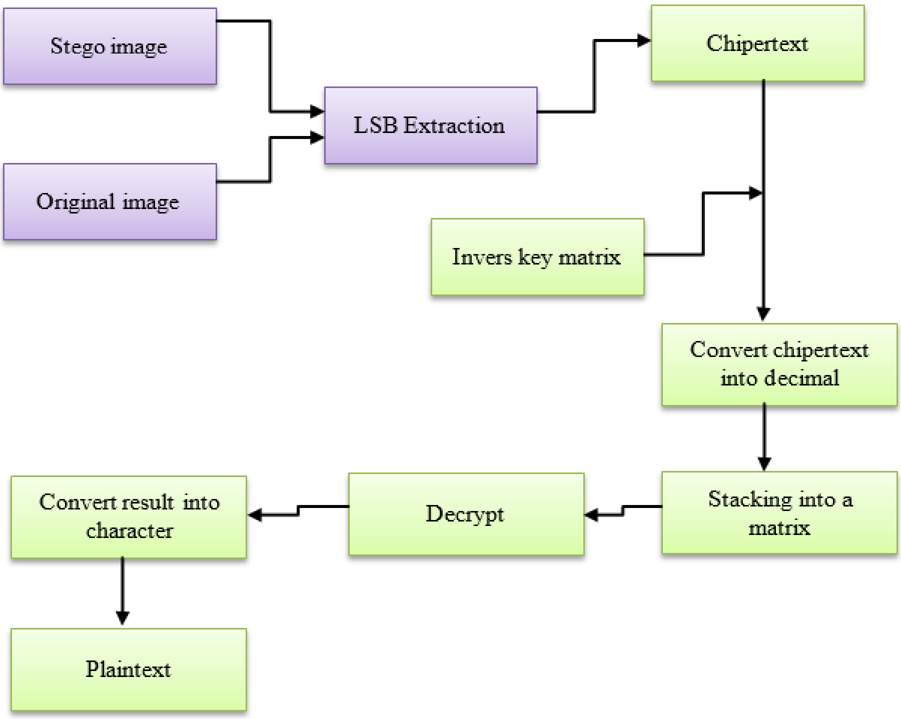


Figure 2. Extraction and decryption process.

This study using two types of digital image sizes, namely with a size of 256 × 256 pixels and 512 × 512 pixels with tiff format. The digital image is a grayscale image that has been widely used in various studies. This study aims to facilitate the comparison process for further research. The following is a sample of grayscale images that can be seen in Figure 3 and Figure 4.

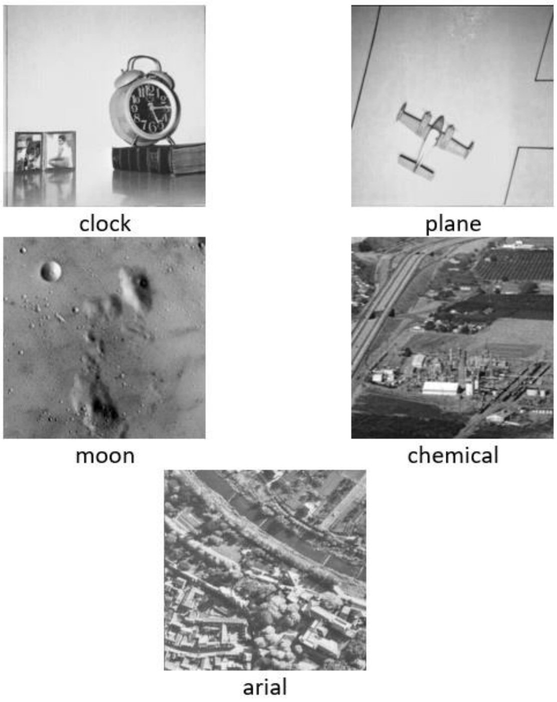


Figure 3. Image dataset in size 256x256 pixels.

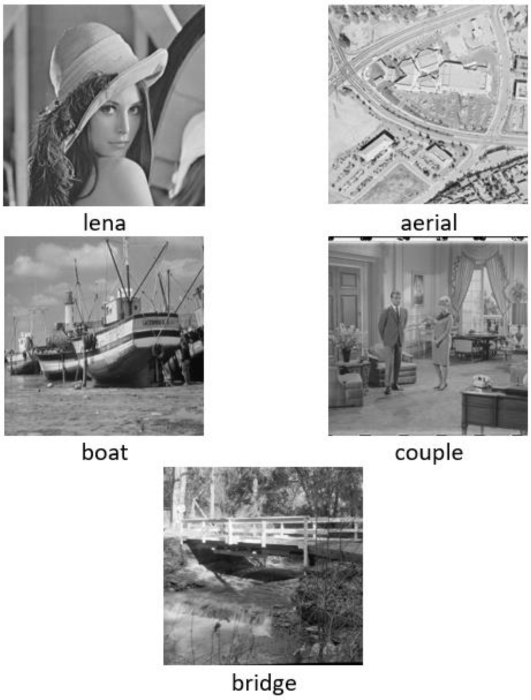


Figure 4. Image dataset in size 512x512 pixels.

By using the Hill Cipher algorithm, the data used for messages is an alphabetical character with range A - Z, where the character will be encrypted. Message encryption aims to hide a message into an image so that the message is difficult to recognize, so that it can improve security in a message. In this study using 32, 64, and 128 characters length. Message samples and encryption results can be seen in Figure 5.

Characters length	Plaintext	Chipertext
32	UNIVERSITASDIANUSWANTOROSEMARANG	ZEVQRIOFBJZWKZVXEZNARDVNCDCFFTFD
64	UNIVERSITASDIANUSWANTOROSEMARANGUDINUSPOLKEJAYAALMAMATERTEKNIS	ZEVQRIOFBJZWKZAAONIHSQXKARCZZCNAWTFPVXJCFUSRVHEXHMCFCFNLKWWLLRIL
128	UNIVERSITASDIANUSWANTOROSEMARANGUDINUSPOLKEJAYASELALUKAMPUSTERAKREDITASASIAPETINGGINYAPAKEDINURSASONGKOTEKNIKINFORMATIKASARJANAST	ZEVQRIOFBJZWKZAAONIHSQXKARCZZCNAWTFPVXJCFUSRVHEXCDRXZHGPVGONNLFTFEBOPCCJKZVFZNFDMNHZTOEFBOXMLGQBGVFDWJNLTCORXMTVPZFQORCJZCVHNNVE

Figure 5. A comparison between plaintext and chipertext.

From Figure 1, it can be seen if messages that have the same character length do not necessarily have the same encryption results. This is because encryption is affected by key values and key matrices in the message. From the three images, it can be seen that the results of encryption can also change the character value of the original message which will be used in the insertion process with the LSB algorithm. Changes from the encryption message value will also affect the LSB algorithm insertion process.

To determine the quality of the stego-image, a standard measuring instrument is needed, namely using PSNR, MSE, Entropy, and travel time (CPU time). The results of the inserted encryption do not appear to change significantly. This can be seen in table A and table B for digital dreams measuring 256 × 256 pixels and 512 × 512 pixels below.

Table 1. Result Comparison between original image and stego image in size 512x512 pixels

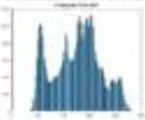
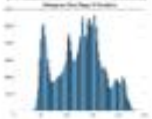
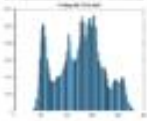
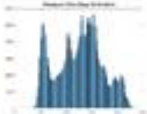
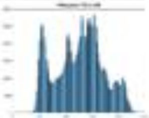
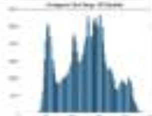
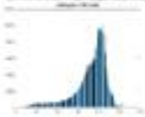
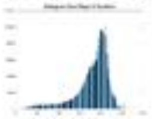
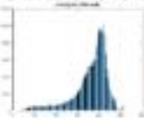
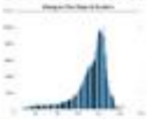
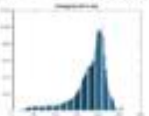
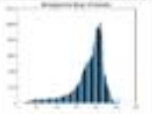
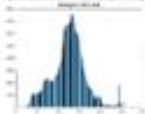
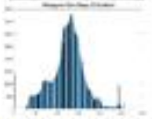
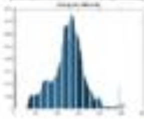
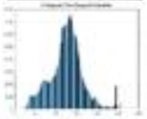
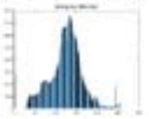
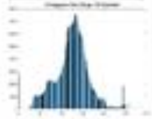
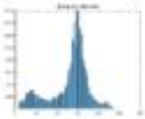
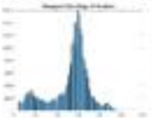
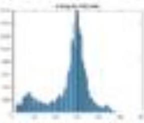
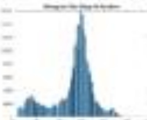
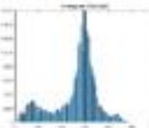
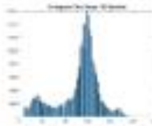
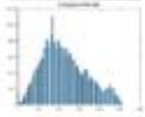
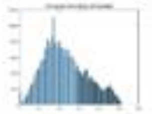
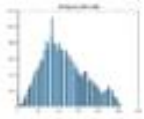
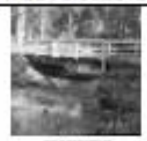
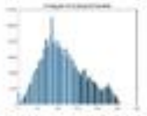
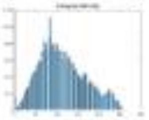
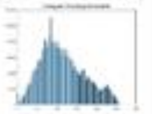
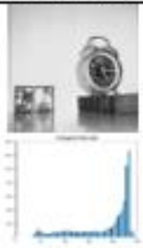
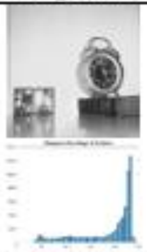
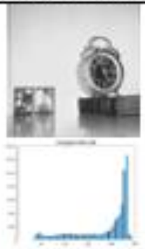
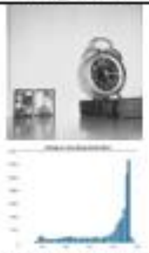
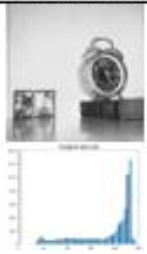
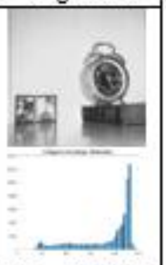
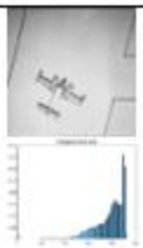
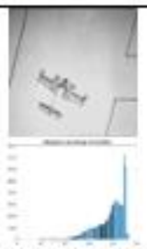
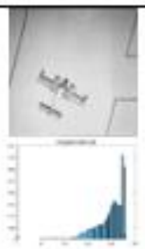
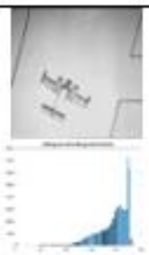
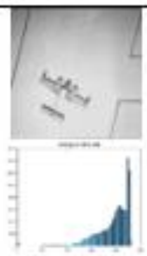
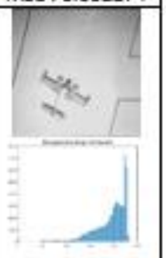
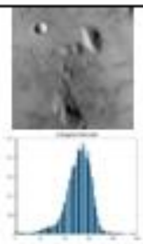
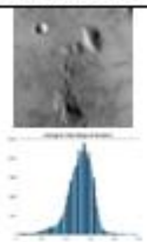
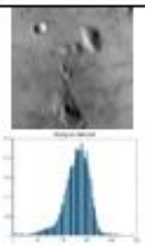
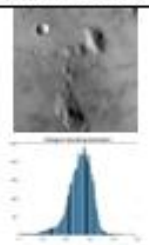
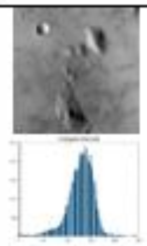
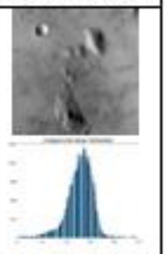
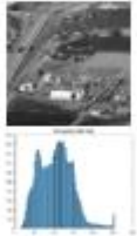
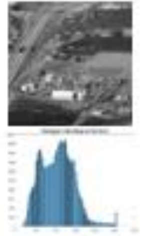
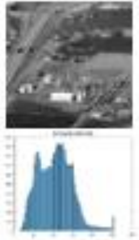
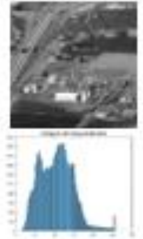
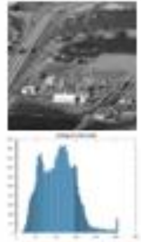
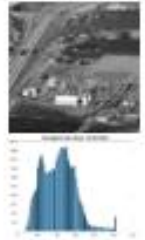
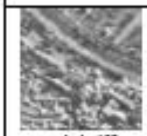
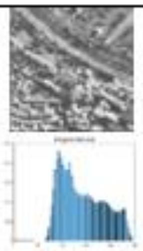
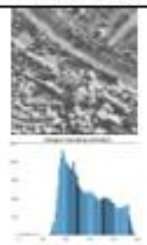
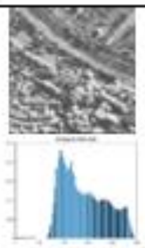
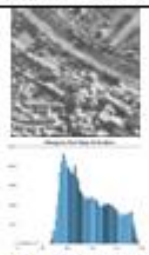
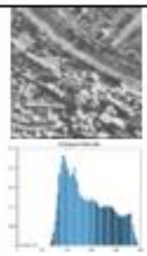
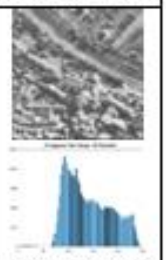
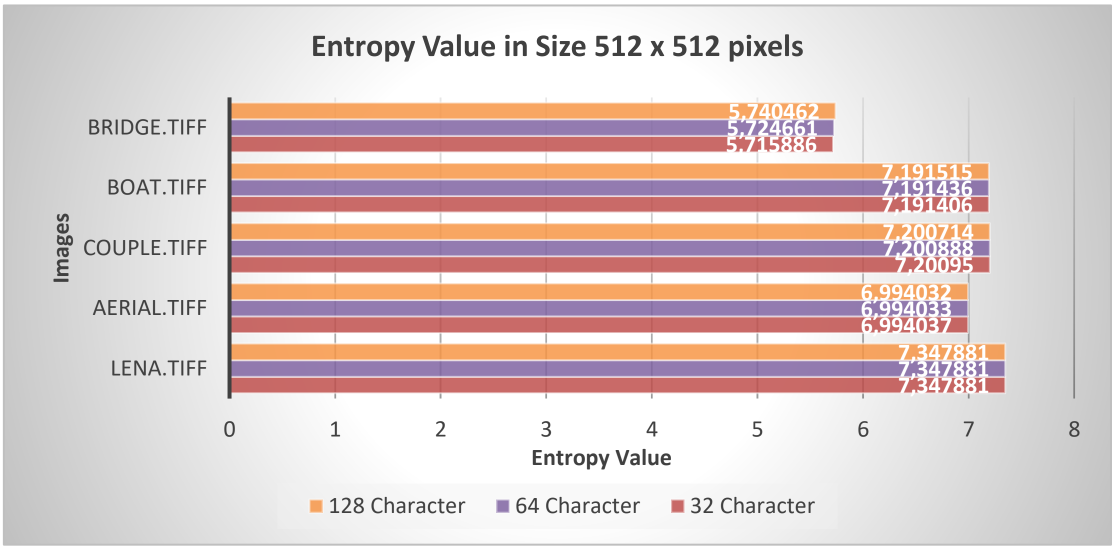
Original images	32 Characters		64 Characters		128 Characters	
	Original image	Stego imae	Original image	Stego imae	Original image	Stego imae
 lena.tiff	 	  PSNR : 77.282626 MSE : 0.001141	 	  PSNR : 77.282626 MSE : 0.001141	 	  PSNR : 4.286876 MSE : 0.002274
 aerial.tiff	 	  PSNR : 80.526433 MSE : 0.000576	 	  PSNR : 77.559491 MSE : 0.001141	 	  PSNR : 4.563740 MSE : 0.002274
 couple.tiff	 	  PSNR : 77.282626 MSE : 0.001141	 	  PSNR : 77.282626 MSE : 0.001141	 	  PSNR : 7.282626 MSE : 0.001141
 boat.tiff	 	  PSNR : 80.526433 MSE : 0.000576	 	  PSNR : 77.559491 MSE : 0.001141	 	  PSNR : 4.563740 MSE : 0.002274
 bridge.tiff	 	  PSNR : 80.526433 MSE : 0.000576	 	  PSNR : 77.559491 MSE : 0.001141	 	  PSNR : 4.563740 MSE : 0.002274

Table 2. Result Comparison between original image and stego image in size 256x256 pixels

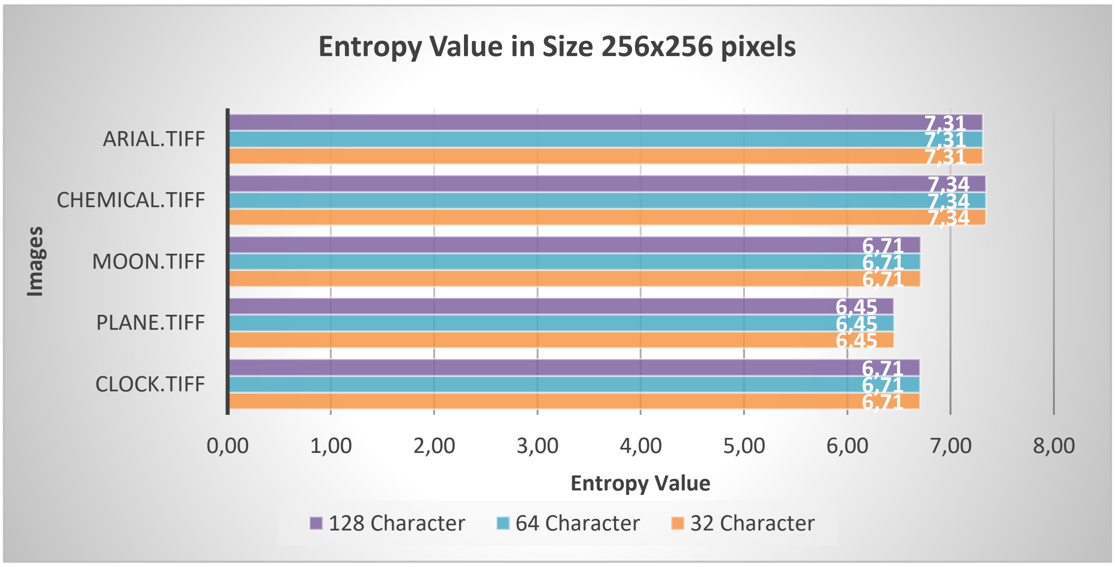
Original images	32 Characters		64 Characters		128 Characters	
	Original image	Stego imae	Original image	Stego imae	Original image	Stego imae
 clock.tiff		 PSNR : 74.193732 MSE : 0.002304		 PSNR : 77.282626 MSE : 0.001141		 PSNR : 4.286876 MSE : 0.002274
 plane.tiff		 PSNR : 73.684790 MSE : 0.002304		 PSNR : 70.717847 MSE : 0.004562		 PSNR : 7.722096 MSE : 0.009094
 moon.tiff		 PSNR : 74.299017 MSE : 0.002304		 PSNR : 71.332074 MSE : 0.004562		 PSNR : 8.336324 MSE : 0.009094
 chemical.tiff		 PSNR : 74.505833 MSE : 0.002304		 PSNR : 71.538891 MSE : 0.004562		 PSNR: 68.543140 MSE : 0.009094
 arial.tiff		 PSNR : 74.264063 MSE : 0.002304		 PSNR : 71.297121 MSE : 0.004562		 PSNR: 68.301370 MSE : 0.009094

Based on Table 1 and Table 2, it is evident that the results of steganography using 32, 64 and 128 characters did not change significantly. Therefore, the comparison between steganographic image results cannot be seen in plain view. In addition, in the two tables above it is evident that the insertion image with the number of characters results in a value of MSE that is far below the number 1. This indicates that the insertion image is not significantly damaged. In the table above, it can be seen that pixel size and the number of characters inserted will affect the value of MSE. The smaller the pixel size of the image and the more the number of characters the message is inserted, the greater the value of MSE. The image that has the highest MSE value is plane.tiff, moon.tiff, chemical.tiff, and arial.tiff with a size of 256 x 256 pixels and 128 characters insertion that has a value of 0.009094. While the image that has the lowest MSE value is aerial.tiff, boat.tiff, and bridge.tiff with a size of 512 x 512 pixels and a 32 character insertion that has a value of 0.000576.

The PSNR test results in the table above show that the image quality is very good because the PSNR value in each image is up to 65 dB. The PSNR value is also influenced by the maximum pixel value and MSE value. The smaller the maximum pixel value and the greater the MSE value, the smaller the PSNR value will be. The image that has the highest PSNR value is aerial.tiff, boat.tiff and bridge.tiff with a size of 512 x 512 pixels and a 32 character insertion that has a value of 80.526433 dB. While the image that has the lowest PSNR value is plane.tiff with a size of 256 x 256 pixels and insertion 128 character that has a value of 67.722096 dB.

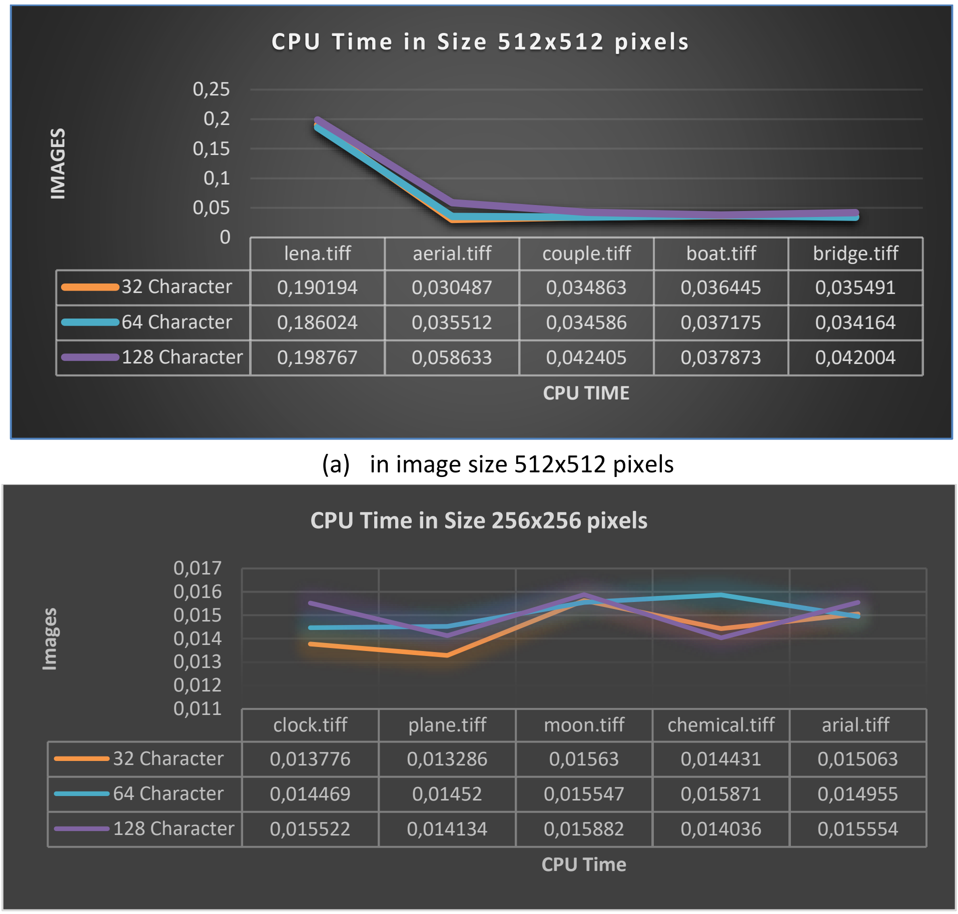


(a) in image size 512x512 pixels



(b) in image size 256x256 pixels

Figure 6. A comparison between entropy value in size 512 and 256 pixels.



	lena.tiff	aerial.tiff	couple.tiff	boat.tiff	bridge.tiff
32 Character	0,190194	0,030487	0,034863	0,036445	0,035491
64 Character	0,186024	0,035512	0,034586	0,037175	0,034164
128 Character	0,198767	0,058633	0,042405	0,037873	0,042004

(a) in image size 512x512 pixels

	clock.tiff	plane.tiff	moon.tiff	chemical.tiff	arial.tiff
32 Character	0,013776	0,013286	0,01563	0,014431	0,015063
64 Character	0,014469	0,01452	0,015547	0,015871	0,014955
128 Character	0,015522	0,014134	0,015882	0,014036	0,015554

(b) in image size 256x256 pixels

Figure 7. A comparison between CPU Time value in size 512 and 256 pixels.

In Figure 6, the entropy test shows that the highest entropy value lies in the lena.tiff image with a size of 512 x 512 pixels which has an entropy value of 7.347888. While the image that has the lowest entropy is bridge.tiff with a size of 512 x 512 pixels which has an entropy value of 5.715885. In testing the travel time to insert the message character as given in Figure 7, it can be seen that the fastest travel time is in the chemical.tiff image that is equal to 0.014036 s with 128 characters insertion and measuring 256 × 256 pixels, while the travel time is late in the lena.tiff image which is 0.198767 s with 128 characters insert and measures 512 × 512 pixels. Therefore, it can be seen that travel time is influenced by the size of the image and memory capacity on the computer.

4. CONCLUSION

Based on the results of testing in message hiding on digital images by combining the Hill Cipher and Least Significant Bit (LSB) algorithms, it can be concluded that the process of hiding messages using the Hill Cipher algorithm in digital images can improve security and cannot be seen in plain view, because the results of steganography did not change after the insertion of text messages using the LSB method, so there was no significant change when the image before and after steganography. The combination of these two algorithms has been successfully applied to the gray 3-bit (Grayscale) image. The results of the merger between the Hill Cipher and LSB algorithms produce a very good image. The gray image used has a size of 256 × 256 pixels and 512 × 512 pixels. While the text messages used for the insertion process are 32, 64, and 128 characters. Based on the results of the comparison on the image it can be seen that the LSB method has advantages in the quality of stego images. It is evident that the PSNR value of each image is> 65 dB which is shown in Table 1 and Table 2. In addition, the PSNR value is also quite stable because all PSNR values produce values with very small differences or no more than 1 dB. The highest PSNR value is owned by aerial.tiff, boat.tiff, and bridge.tiff imagery at 80.526433 dB. The entropy value in the stego image is up to 5. The highest entropy value is owned by the lena.tiff image of 7.347888. While the travel time (CPU Time) generated in running these two algorithms is less than 1s. So that both of these algorithms can be used to increase the security of the message. In addition, both of these algorithms are proven to have the advantage of good image results using algorithms that are simple and fast in processing and have a high similarity to the original image.

REFERENCES

[1] D. Nofriansyah, S. Defit, G. W. Nurcahyo, G. Ganefri, R. Ridwan, A. S. Ahmar and R. Rahim, "A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm," *Journal of Physiscs : Conference Series,* vol. 954, 2018.

[2] Sangeeta and A. Kaur, "A Review on Symmetric Key Cryptography Algorithms," *International Journal of Advanced Research in Computer Science* , vol. 8, no. 4, pp. 358-361, 2017.

[3] A. Reddy, Vishnuvardhan and Madhuviswanatham, "A Modified Hill Cipher Based on Circulant Matrices," *Procedia Technology,* vol. 4, pp. 114-118, 2012.

[4] S. Sun and Y. Guo, "A Novel Image Steganography Based on Contourlet Transform and Hill Cipher," *Journal of Information Hiding and Multimedia Signal Processing,* vol. 6, no. 5, pp. 889-897, 2015.

[5] N. A. Abu, P. W. Adi and O. Mohd, "Robust Digital Image Steganography within Coefficient Difference on Integer Haar Wavelet Transform," *International Journal of Video&Image Processing and Network Security IJVIPNS-IJENS,* vol. XIV, no. 2, pp. 1-7, 2014.

[6] C. Irawan, D. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," Semarang, 2017.

[7] P. Malathi and T. Gireeshkumar, "Relating the embedding efficiency of LSB Steganography techniques in Spatial and Transform domains," *Procedia Computer Science,* vol. 93, p. 878 – 885, 2016.

[8] E. H. Rachmawanto, R. S. Amin, D. Setiadi and C. A. Sari, "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size," Semarang, 2017.

[9] E. J. Kusuma, C. A. Sari, E. H. Rachmawanto and D. Setiadi, "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography," *J. ICT Res. Appl,* vol. 12, no. 2, pp. 103-122, 2018.

[10] G. Swain, "A steganographic method combining LSB substitution and PVD in a block," *Procedia Computer Science,* vol. 85, p. 39 – 44, 2016.

[11] A. Devi, A. Sharma and A. Rangra, "A Review on DES, AES and Blowfish for Image Encryption & Decryption," *International Journal of Computer Science and Information Technologies,* vol. 6, no. 3, pp. 3034-3036, 2015.