Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493)
Vol. 8 No. 3, November 2023, pp. 287 – 297
DOI:

Encryption of Information on Brain Tumor Images Using Vigenere Cipher Algorithm and Least Significant Bits

Renol Burjulius*[1], **Dini Rohmayani**[2]
[1]Jurusan Teknik Informatika, Politeknik Negeri Indramayu, Jl. Lohbener Lama 08 Indramayu-Jawa Barat
[2]Program Studi Teknik Informatika Politeknik TEDC Bandung, Jl. Pesantren, No. 2, Cibabat, Cimahi Utara, Kota Cimahi, Jawa Barat
E-mail : burjuliusrenol@gmail.com[1], dinirohmayani@poltektedc.ac.id[2]*
**Corresponding author*

Sonty Lena[3]
[3]Jurusan Teknik Informatika, Politeknik Negeri Indramayu, Jl. Lohbener Lama 08 Indramayu-Jawa Barat
E-mail : sontylena18@gmail.com[3]

Abstract - Cryptography is a branch of existing methods in mathematics which has the goal of being able to maintain the confidentiality of the information contained in the data so that the information is not known by parties who have no interest. Confidentiality of this information is important so that the information sent is not misused irresponsibly. Vigenere Cipher is a method used for cryptography. Vigenere Cipher works by using a tabula recta table where the table contains an alphabet arranged based on the Caesar Cipher shift. In this study, the Vigenere Chiper algorithm will be used to encrypt information into 25 brain tumor images. In the tests carried out on 25 images, the best MSE obtained was 1.541e-05, while the best PSNR was 48.1219, for the best SSIM it was 0.99995, then for the BER value, all images obtained a BER value of 0 and also for the entropy of the best steganography image, which was 6.8204.

Keywords - Brain Tumor Images, Vigenere Cipher Algorithm, Least Significant Bits

1. INTRODUCTION

Brain tumor is a disease that can be categorized as very deadly. Suta et. al [1], stated that brain tumor disease occurs due to the growth of brain cells which are usually abnormal which appear in the brain or around the brain. This growth of brain cells usually occurs abnormally and is also uncontrollable. Noreen [2], stated that brain tumors are one of the most dangerous types of cancer that can affect children to adults.

Image processing is a science that studies how images can be formed, processed and analyzed. In image processing, identification or transformation of the pixel processing results in the image can also be carried out. Grayscale image is an image that has a gray base color. Gunnam et. al [3], stated that a grayscale image is an image that only has one color channel.

Cryptography is a technique or method used to protect the confidentiality of information sent or embedded in images. Salim et. al [5] stated that in the digital world, there are many risks that threaten the confidentiality of the data sent. Abu-Faraj, et. al [4], argued that protecting confidential data can be done using cryptography, which will be encrypted when sending data and decrypted when receiving data. In the process of data encryption or cryptography, the algorithm or method that can be used is the vigenere cipher. In the encryption and decryption process, the Vigenere cipher uses a key. Boussif et. al [6], suggested that for data encryption and decryption the Vigenere cipher algorithm operates on each pixel. Qowi et. al [7], confirmed that the Vigenere cipher uses a key in the form of characters to encrypt information.

Steganography is a way to hide a message on a medium, so that the message sent cannot be directly seen or found through visuals. Subramanian et. al [8], argued that image steganography is a process for hiding information in an image. Dhawan et. al [9], argued that in the steganographic method, people can only see cover data (images) while secret data cannot be seen by humans and remains veiled. The algorithm commonly used for the steganography method is the LSB or Least Significant Bit algorithm. Pramanic et. al [10], suggested that LSB is used to hide the ciphertext in an image. Sharma et. al [11], confirmed that in the LSB steganography process, data will be hidden into the least significant bits of the image.

Research conducted by Voleti et. al [12], discusses ways to perform steganography on good images so that data is not properly encrypted using the refinement technique of the LSB technique and the Vigenere cipher algorithm. The purpose of this study is to explain how good steganography algorithms and techniques are so that they can run efficiently and also in this study to discuss the best techniques that can be used to carry out the steganography process. The results of this study are that LSB can hide data well and the steganography process can run well on 24 types of image media including BMP, GIF and PNG and data can be reappeared properly using the Vigenere cipher algorithm.

2. RESEARCH METHOD

Explaining research chronological, including research design, research procedure (in the form of algorithms, Pseudocode or other), how to test and data acquisition [1], [3]. The description of the course of research should be supported references, so the explanation can be accepted scientifically [2], [4].

2.1. Data

Brain tumor is a disease that can be considered very deadly. Suta et. al [1], suggested that brain tumor disease occurs due to the growth of brain cells which are usually abnormal which appear in the brain or around the brain. This growth of brain cells usually occurs abnormally and is also uncontrollable. Magnetic resonance imaging (MRI) is an examination technique that uses radio waves along with magnetic technology to determine the patient's condition. This technique is used to scan the internal cavities of the human body which cannot be directly seen by the human eye.In the research conducted this time, the dataset that will be used is brain tumor images with a total of 25 images. The image used is a combination of 3 types of tumors in the brain, namely glioma, meningioma and pituitary tumors. Where all the images are of type *.jpg and the size of the image is resized in the dimensions of 512 * 152 pixels. The image used in this study has a grayscale color space, so there is no need to transform it into a grayscale image so that the message insertion process can be carried out using the LSB steganography method or technique. The test that will be carried out is on each image one by one a secret message is inserted and the changes that occur in the image will be analyzed.

2.2. Vigenere cipher

Vigenere cipher is an algorithm for cryptography or data security. Qowi et. al [7], confirmed that the Vigenere cipher uses a key in the form of characters to encrypt information.

In the process, the text is converted into a ciphertext through an encryption process and to return the information, a key and a decryption method will be used [13]. There are 2 techniques or methods that can be used from the vigenere cipher, namely techniques using numbers and techniques using letters. In the technique of using numbers, the Vigenere Cipher algorithm uses the concept of substitution to replace letters into numbers. As for the technique of using letters, in its implementation it uses table tabula recta. Tabula recta is a 26 * 26 matrix consisting of letters of the alphabet to encrypt and decrypt data. Apart from using the tabula recta table, there is also a variation of the Vigenere cipher algorithm, namely using modulo 256. By using the modulus 256 method, the number of characters used can be up to 256 characters [14]. The Vigenere cipher with modulo 256 is a modification of the traditional Vigenere Cipher algorithm, to be able to encrypt or decrypt using ASCII characters. ASCII is a character encoding in a computer where the representation of each character is an integer from 0 to 255. Pujeri et.al [15], suggested that ASCII characters are used as plain text and the results can be converted into ciphertext with cryptographic methods. Apart from using the tabula recta table, there is also a variation of the Vigenere cipher algorithm, namely using modulo 256. By using the modulus 256 method, the number of characters used can be up to 256 characters [14]. The Vigenere cipher with modulo 256 is a modification of the traditional Vigenere Cipher algorithm, to be able to encrypt or decrypt using ASCII characters. ASCII is a character encoding in a computer where the representation of each character is an integer from 0 to 255. Pujeri et.al [15], suggested that ASCII characters are used as plain text and the results can be converted into ciphertext with cryptographic methods.

Enkripsi Vigenere Cipher (mod 256):

$$E[x] = (Z[x] + Y[x \, mod \, n]) \, mod \, 256 \tag{1}$$

Dekripsi Vigenere Cipher (mod 256):

$$D[x] = (E[x] + Y[x \, mod \, n] + 256) \, mod \, 256 \tag{2}$$

2.3. Least Significant Bit (LSB)

LSB is a technique used to embed or unify messages sent with a media, in this study, the media used is an image. LSB is used to hide the ciphertext in an image [10]. Gutub et. al [16], stated that in the process, LSB uses very insignificant bits or the last bit, for these bits can be ignored so that information security can be carried out.

2.4. Workflow

In the process of performing cryptography with the Vigenere cipher algorithm and using the LSB steganography technique, this study will use MATLAB version R2022a. In the cryptographic process, encryption will be carried out from plain text (the information provided) using the Vigenere cipher algorithm together with the user input key. After the encryption process is carried out, a steganography process is carried out using the LSB algorithm to insert the encrypted message into the image or image. After the steganography process, the message that has been combined with the image will be returned by taking the least significant numBits. Then, after obtaining insignificant numBits, a decryption process will be carried out using the Vigenere cipher algorithm to be able to see the embedded message. For process workflows or workflow processes can be seen in the image below.

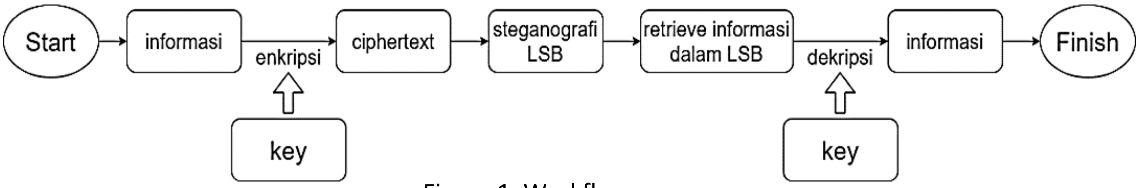


Figure 1. Workflow process

The data used in this study is data obtained from the Kaggle.com website. After the data has been prepared and filtered as many as 25 data, cryptographic processes can be carried out with the Vigenere cipher algorithm and steganography with LSB. The following are the stages of the process carried out.

a. Brain tumor image reading
b. Prepare information data to be sent along with the key to be used
c. Carry out the process of encrypting the information data to be sent using the Vigenere cipher algorithm and the key that has been input. From this process will be generated in the form of ciphertext or text from the results of information encryption.
d. After obtaining the ciphertext, the ciphertext data is inserted or embedded into the image or image that has been read using the LSB or Least Significant Bit Technique.
e. After the image contains encryption or ciphertext information, the information is returned by taking numBits at insignificant bit values.
f. Then after getting back the ciphertext in the form of a character, a decryption process is carried out using the Vigenere cipher algorithm and the key that was used earlier, so that the ciphertext will become information data that is input or sent.

2.5. Testing

To see how the performance of the results of encryption and decryption using the Vigenere cipher algorithm and to see a comparison of images after the steganography process using the Least Significant Bit method, this study will use several test metrics. The test metrics used in this study are MSE, PSNR, SSIM, BER, Histogram and entropy. These metrics were obtained from the results of cryptographic testing with the Vigenere cipher and steganography with LSB.

Mean Squared Error (MSE) is a metric used to measure the difference between the original image and the reconstructed image. Sarah et. al [17], stated that the closer the value is to 0, the more the reconstructed image will match the original image.

$$MSE = \frac{1}{x}\sum_{y=1}^{x}(Z_y - Q_y)^2 \tag{3}$$

Peak Signal to Noise Ratio (PSNR) is a method used to measure the quality of image reconstruction. PSNR in image processing is used to be able to evaluate whether the reconstructed image can have similarities with the original image by also taking into account the error rate generated by the image compression process. Setiadi [18], stated that the PSNR results were obtained from the results of calculations using logarithms on the MSE of the image.

$$PSNR = 10 * \log_{10}(\frac{Piksel^2}{MSE}) \tag{4}$$

Structural Similarity Index (SSIM) is a method used to evaluate the quality of the reconstructed image, whether the reconstructed image is similar to the original image by considering the structural similarity between the reconstructed image and the original image. Nilsson et. al [19], stated that to calculate SSIM, it is not fixated on any color space, because color input has never been defined before.

$$SSIM\ (M,N) = \frac{(2 * \ \mu M * \ \mu Y + C_1) * \ (2 * \ \sigma MN \ + \ C_2)}{(\mu^2 M \ + \ \mu^2 N \ + \ C_1) * \ (\sigma^2 M \ + \ \sigma^2 N \ + \ C_2)} \tag{4}$$

Bit Error Rate (BER) is a metric used to measure errors that exist after the image compression or decompression stages are performed. Usually errors occur because bit information is lost during the compression process to reduce file size but when you want to decompress it, the bit information cannot be restored. Ko et. al [20], stated that the smaller the BER value, the better the quality of the compressed or reconstructed image

.

$$BER = \frac{Different\ bits}{Total\ of\ bits} \tag{5}$$

The histogram is a visualization that is used to be able to show the color difference between the original image and the resulting image of the steganography process. Salem et. al [21], stated that the Histogram is a tool to increase the contrast in an image. The way to increase the contrast is to restore the lost contrast by redistributing the brightness values of the image but can produce traces that are processed on the image.

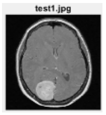
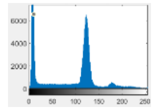
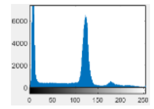
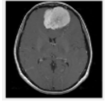
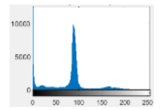
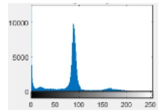
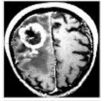
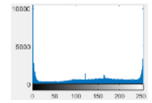
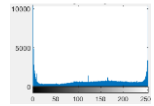
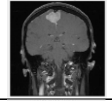
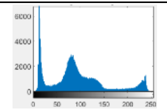
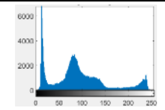
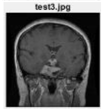
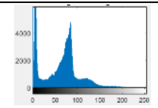
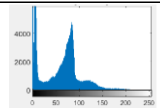
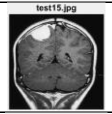
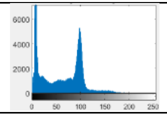
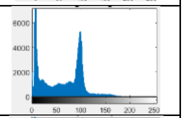
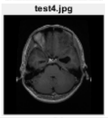
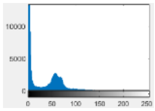
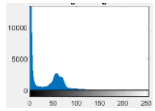
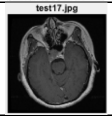
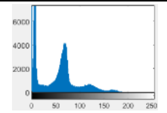
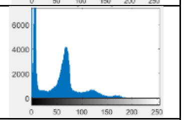
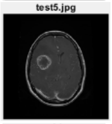
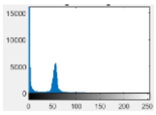
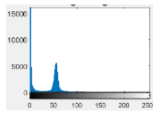
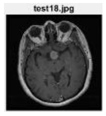
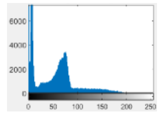
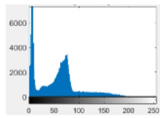
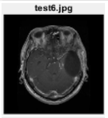
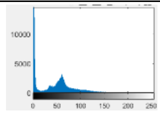
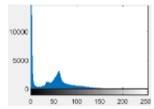
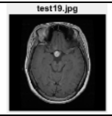
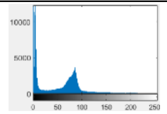
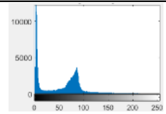
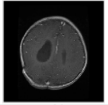
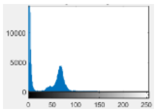
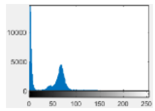
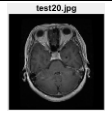
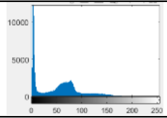
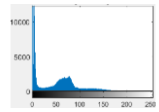
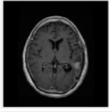
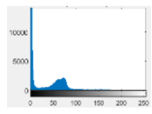
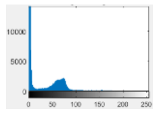
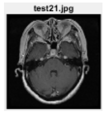
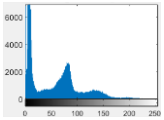
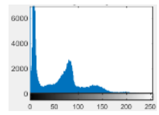
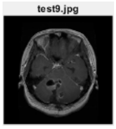
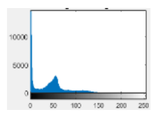
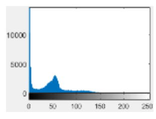
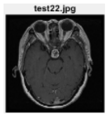
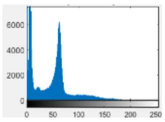
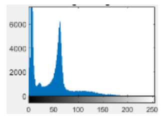
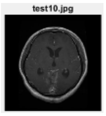
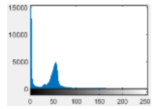
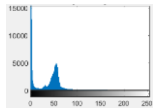
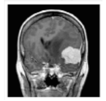
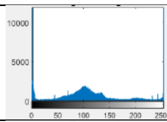
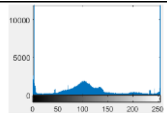
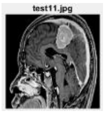
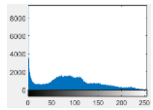
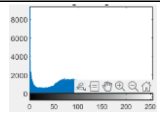
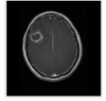
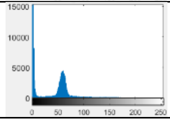
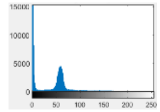
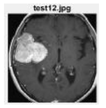
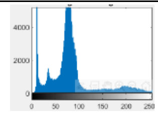
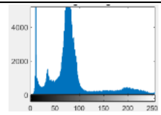
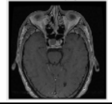
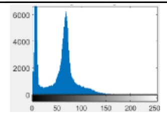
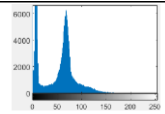
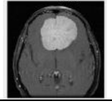
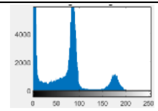
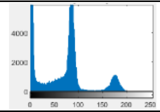
3. RESULTS AND DISCUSSION

3.1. Testing of 25 images

In this study, the MATLAB R2022a software will be used to implement the program. The algorithm used in this study is the Vigenere cipher to carry out cryptographic processes and LSB to carry out steganographic processes on images. In the process carried out during cryptography, namely encryption and decryption of messages, while in the process carried out by steganography, it is combining the encrypted messages in the image used. After the cryptography and steganography processes have been carried out, we can see the results of the comparison between the original image and the resulting steganography image by using a histogram for visualization.

It can be seen in the table, that there does not appear to be a significant difference between the original image and the resulting steganography image. This can show that when using the steganography process the message into the image using LSB does not raise a big difference. Which means the message can be hidden properly in the image, so it is not visible to the naked eye. Besides being able to see the differences in the images, we can also see the values of MSE, PSNR, SSIM, BER and also the entropy of the images, both the original image and the resulting steganography image. The value of this metric can be used to see how the quality value of the image after the steganography process is carried out. In this study, messages that are cryptographically processed are strings with the words "Hello, World!" with the keyword 'SecretKey' and the message will be combined with the image with the LSB process. The result of the message when the encryption process is carried out is that it raises a ciphertext containing ÊÏÞÔ k¼èÅÑÇ and if decryption is carried out, the ciphertext will return to all messages namely "Hello, World!". The table for the tests carried out can be seen in Tabel 2.

Table 1. Testing Histogram

Original image	Histogram of original image	Histogram of stegano image	Original image	Histogram of original image	Histogram of stegano image
test1.jpg 			test14.jpg 		
test2.jpg 			test16.jpg 		
test3.jpg 			test15.jpg 		
test4.jpg 			test17.jpg 		
test5.jpg 			test18.jpg 		
test6.jpg 			test19.jpg 		
test7.jpg 			test20.jpg 		
test8.jpg 			test21.jpg 		
test9.jpg 			test22.jpg 		
test10.jpg 			test23.jpg 		
test11.jpg 			test24.jpg 		
test12.jpg 			test25.jpg 		
test13.jpg 					

In the next test, several images will be used to see if the given message length affects the quality value of the image. As well as seeing what values are affected when the longer the input string as information or keys.

Table 2. Testing Matrix MSE, PSNR, BER, Entropy

No	Images	Appearance					
		MSE	PSNR	SSIM	BER	Enttopy	
						Original image	Stego image
1	test1.jpg	1.7477e-05	47.5754	0.99986	0	6.2219	6.2221
2	test2.jpg	1.577e-05	48.0218	0.99995	0	6.383	6.3832
3	test3.jpg	1.8317e-05	47.3715	0.9997	0	6.5447	6.545
4	test4.jpg	1.8649e-05	47.2934	0.99945	0	4.9987	4.9993
5	test5.jpg	1.8649e-05	47.2934	0.99943	0	4.1631	4.1637
6	test6.jpg	1.8649e-05	47.2934	0.9996	0	5.0088	5.0093
7	test7.jpg	1.8649e-05	47.2934	0.99955	0	4.7474	4.748
8	test8.jpg	1.8649e-05	47.2934	0.99961	0	4.9158	4.9164
9	test9.jpg	1.8649e-05	47.2934	0.99956	0	5.0155	5.0161
10	test10.jpg	1.8649e-05	47.2934	0.99951	0	4.6458	4.6463
11	test11.jpg	1.8649e-05	47.2934	0.99985	0	6.7266	6.727
12	test12.jpg	1.6682e-05	47.7776	0.99979	0	6.778	6.7783
13	test13.jpg	1.8649e-05	47.2934	0.99978	0	6.4043	6.4046
14	test14.jpg	1.8649e-05	47.2934	0.99979	0	5.4002	5.4007
15	test15.jpg	1.541e-05	48.1219	0.99988	0	6.8202	6.8204
16	test16.jpg	1.7979e-05	47.4525	0.99971	0	6.3297	6.33
17	test17.jpg	1.8649e-05	47.2934	0.99969	0	6.1769	6.1773
18	test18.jpg	1.8649e-05	47.2934	0.99971	0	6.2389	6.2392
19	test19.jpg	1.8649e-05	47.2934	0.99973	0	5.4738	5.4742
20	test20.jpg	1.8649e-05	47.2934	0.9997	0	5.4942	5.4947
21	test21.jpg	1.8649e-05	47.2934	0.99976	0	6.3781	6.3784
22	test22.jpg	1.8649e-05	47.2934	0.99962	0	6.0403	6.0407
23	test23.jpg	1.6121e-05	47.926	0.99993	0	6.028	6.0283
24	test24.jpg	1.8649e-05	47.2934	0.99956	0	4.5212	4.5218
25	test25.jpg	1.8649e-05	47.2934	0.99956	0	6.1563	6.1568

3.2 Testing 5 images with 16 information characters and 11 key characters

Informasi : TesinGDgn16char_
Key : IniKuncinya

Table 3. First test

No	Images	Appearance					
		MSE	PSNR	SSIM	MSE	Enttopy	
						Original image	Stego image
1	test1.jpg	1.7477e-05	47.4822	0.99986	0	6.2219	6.2221
2	test2.jpg	2.095e-05	46.7882	0.99993	0	6.383	6.3832
3	test3.jpg	1.8317e-05	47.2692	0.9997	0	6.5447	6.545
4	test4.jpg	1.9168e-05	47.1741	0.99943	0	4.9987	4.9993
5	test5.jpg	1.9168e-05	47.1741	0.99941	0	4.1631	4.1637

In the first test, the information sent is in the form of a 16-character string with the value 'TesinGDgn16char_' and the key used is an 11-character string with the value 'IniKey'. After the encryption process is carried out from the information and key provided with the Vigenere cipher algorithm, we get a ciphertext that has a value of ÓÓÜ´ãµ§ÐÜª¬ÖÊ½Ô. Just like the previous test, after getting the ciphertext, the steganography process will be carried out using the LSB method. After the steganography process, the results are in table 2. By using the string 'TesinGDgn16char_' and the key 'IniKuncinya', the MSE value of the steganographic image increases from the original image that was input and the previous test so that there is an increase in the difference between the original image and the resulting steganography image. The PSNR value drops from the previous test because the input string is getting longer, it can also increase the storage used. The SSIM in this test shows a change, which is lower than the previous test, because the longer the input string, the more pixels are used, which can cause changes in bits or pixels, which can cause differences in the original image with the steganography image. Meanwhile, the entopy of the steganography results remains the same, there is no change from the previous test. Which, there is no significant change in the value of the image randomness after the steganography process.

3.3 Testing 5 Images with 39 information characters and 19 key characters

Information : Testing with many B3R54MAAN Characters*_!
Key : thisKeyUsed1

Table 4. Second Testing

No	Images	Appearance					
		MSE	PSNR	SSIM	BER	Enttopy	
						Original image	Stgeo image
1	test1.jpg	6.9593e-05	41.5743	0.99944	0	6.2219	6.2228
2	test2.jpg	3.8563e-05	44.1383	0.99987	0	6.383	6.3838
3	test3.jpg	7.4525e-05	41.277	0.9988	0	6.5447	6.5457
4	test4.jpg	7.5572e-05	41.2164	0.99777	0	4.9987	5.0006
5	test5.jpg	7.5572e-05	41.2164	0.99768	0	4.1631	4.165

In the second test, the information sent is in the form of a string of 39 characters with the value 'Testing With Many Characters B3R54MAAN*_!' and the key used is a string of 19 characters with the value 'thisKeyUsed1'. After the encryption process of the information and key provided with the Vigenere cipher algorithm, we get a ciphertext that has a value of ½ÓÜ¿ÞÜÊÎÕÜÏÏÃÏâÏÔkÀÏÕÊ¯ÝÌç£³£e¶¯ªÍ. Just like the previous test, after getting the ciphertext, the steganography process will be carried out using the LSB method. After the steganography process is carried out, the results are as shown in table 3. By using the string 'Testing With Many Characters B3R54MAAN*_!' and the key 'thisKunciUsed1', the MSE, PSNR, SSIM and entopy values of the steganographic image appear to show changes. The MSE value seems to increase from the original image and from the previous test, because the longer the string used, it will affect the differences between the original image and the resulting steganography image, the PSNR value also seems to decrease significantly from the previous test value because the input string is either key or as information is getting longer, thus increasing the storage used. Likewise with SSIM, there is a decrease because the more strings are input, the more pixels are used, so that this causes a difference in similarity between the original image and the resulting steganography image. Meanwhile, the entopy of the steganography result image also changes, as can be seen in the test results table 2, the entropy value of the steganography image is due to the increasing number of strings input as keys and information, it will add bits in pixels, so that entropy calculations are measured in pixel bits, resulting the value of non-randomness in the resulting steganography image increases. In the previous test, the entropy value was not affected because the keys used the same characters, namely only using lowercase and uppercase, whereas in this test, the entropy value changed due to additional numbers, so that the characters used were more varied than the previous 2 tests.

4. CONCLUSION

After testing by carrying out the cryptographic process using the Vigenere cipher algorithm, and the steganography process using the LSB algorithm, the test results are very good. It can be seen from testing using the message 'Hello, World!' and the keyword 'Secret key' for the image generated from the steganography process is very similar to the original image input. With this, the information sent is successfully hidden so that it cannot be seen by the human eye. In testing using the message 'Hello, World!' and the keyword 'Secret key' also obtained quite good test metric results, for the best MSE it obtained was 1.541e-05, while for the best PSNR it obtained 48.1219, for the best SSIM obtained for 0.99995, then for the BER value, all images get a BER value of 0 and also for the best steganography image entropy that is equal to 6.8204. Then by testing also using 5 images taken as samples using information as many as 16 characters and keywords as many as 11 characters, then it can be concluded that the MSE value has increased from the previous test. The best MSE value is 1.7477e-05. The PSNR value decreased from the previous test, the best PSNR value was 47.4822 and the SSIM value showed a change, which was lower than the previous test, so the best SSIM value was 0.99993. Meanwhile, the entopy of the steganography results remains the same, there is no change from the previous test. After that, in the next test using 5 images taken as samples using 39 characters of information and 19 characters of keywords, the results show that the values of MSE, PSNR, SSIM, The entropy of the steganographic image has a significant change compared to the value obtained in the test using the 5 previous images. The MSE value increased significantly, so that the best MSE value obtained was 3.8563e-05. The PSNR value also decreased significantly, for the best PSNR value, which was 44.1383. The SSIM value also shows a change from the previous test, so the best SSIM value is 0.99944. The entropy value of the steganography image also changes so that the best entropy value of the steganography image in this test is 6.5457. Judging from the results of the conclusions from the tests that have been carried out, then with this a final conclusion can be drawn, namely the longer and more characters used as keys, the better the entropy value or obscurity in the image, but this can lead to higher MSE values. the higher and the PSNR and SSIM values decreased.

For future research, it is expected to be able to add methods used in the cryptographic process, such as modifying the Vigenere cipher algorithm using a 95 * 95 matrix, or other methods, so that more tests can be given. Also for images that are used so that they can be preprocessed first, such as normalizing, whitening, etc., so as to get an entropy value that can be increased from this research. It is also hoped to be able to add other methods to be used as a comparative value from this study.

REFERENCES

[1] Suta, I. B. L. M., Sudarma, M., & Satya Kumara, I. N. (2020). Segmentasi Tumor Otak Berdasarkan Citra Magnetic Resonance Imaging Dengan Menggunakan Metode U-NET. *Majalah Ilmiah Teknologi Elektro*, *19*(2), 151. https://doi.org/10.24843/mite.2020.v19i02.p05

[2] Noreen, N., Palaniappan, S., Qayyum, A., Ahmad, I., Imran, M., & Shoaib, M. (2020). A Deep Learning Model Based on Concatenation Approach for the Diagnosis of Brain Tumor. *IEEE Access*, *8*, 55135–55144. https://doi.org/10.1109/ACCESS.2020.2978629

[3] A Deep Learning-based Approach for Colorization of Grayscale Images and Videos. (2023). *International Journal of Food and Nutritional Sciences*, *11*(12). https://doi.org/10.48047/ijfans/v11/i12/194

[4] Alqadi, Z., Abu-Faraj, M., & Alqadi, Z. A. (2021). Improving the Efficiency and Scalability of Standard Methods for Data Cryptography Analysis of Color Image Features Extraction using Texture Methods View Project Improving the Efficiency and Scalability of Standard Methods for Data Cryptography Mua'ad. *IJCSNS International Journal of Computer Science and Network Security*, *21*(12). https://doi.org/10.22937/IJCSNS.2021.21.12.61

[5] Salim, M. Z., Abboud, A. J., & Yildirim, R. (2022). A visual cryptography-based watermarking approach for the detection and localization of image forgery. *Electronics (Switzerland)*, *11*(1). https://doi.org/10.3390/electronics11010136

[6] Boussif, M., Aloui, N., & Cherif, A. (2020). Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher. *IET Image Processing*, *14*(6), 1209–1216. https://doi.org/10.1049/iet-ipr.2019.0042

[7] Qowi, Z., & Hudallah, N. (2021). Combining caesar cipher and hill cipher in the generating encryption key on the vigenere cipher algorithm. *Journal of Physics: Conference Series*, *1918*(4). https://doi.org/10.1088/1742-6596/1918/4/042009

[8] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*, *9*, 23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998

[9] Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. In *Information Security Journal* (Vol. 30, Issue 2, pp. 63–87). Bellwether Publishing, Ltd. https://doi.org/10.1080/19393555.2020.1801911

[10] Pramanik, S., Samanta, D., Dutta, S., Ghosh, R., Ghonge, M., & Pandey, D. (2020, December 30). Steganography using Improved LSB Approach and Asymmetric Cryptography. *Proceedings of IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation, ICATMRI 2020*. https://doi.org/10.1109/ICATMRI51801.2020.9398408

[11] Sharma, K., Aggarwal, A., Singhania, T., Gupta, D., & Khanna, A. (2019). Hiding Data in Images Using Cryptography and Deep Neural Network. *Journal of Artificial Intelligence and Systems*, *1*(1), 143–162. https://doi.org/10.33969/ais.2019.11009

[12] Voleti, L., Balajee, R. M., Vallepu, S. K., Bayoju, K., & Srinivas, D. (2021). A Secure Image Steganography Using Improved Lsb Technique and Vigenere Cipher Algorithm. *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, 1005–1010. https://doi.org/10.1109/ICAIS50930.2021.9395794

[13] Hameed, T. H., & Sadeeq, H. T. (2022). Modified Vigenère cipher algorithm based on new key generation method. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(2), 954–961. https://doi.org/10.11591/ijeecs.v28.i2.pp954-961

[14] V, B. K., J, B. D., B, C. K., & R Asst Professor, R. B. (2021). A CRYPTO SYSTEM USING VIGENERE AND POLYBIUS CIPHER. In *International Journal of Engineering Applied Sciences and Technology* (Vol. 6, Issue 2). http://www.ijeast.com

[15] Pujeri*, Dr. U., & Pujeri, Dr. R. (2020). Symmetric Encryption Algorithm using ASCII Values. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(5), 2355–2359. https://doi.org/10.35940/ijrte.E5980.018520

[16] Gutub, A., & Al-Shaarani, F. (2020). Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. *Arabian Journal for Science and Engineering*, *45*(4), 2631–2644. https://doi.org/10.1007/s13369-020-04413-w

[17] Sara, U., Akter, M., & Uddin, M. S. (2019). Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study. *Journal of Computer and Communications*, *07*(03), 8–18. https://doi.org/10.4236/jcc.2019.73002

[18] Setiadi, D. R. I. M. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*, *80*(6), 8423–8444. https://doi.org/10.1007/s11042-020-10035-z

[19] Nilsson, J., & Akenine-Möller, T. (2020). *Understanding SSIM*. http://arxiv.org/abs/2006.13846

[20] Ko, H. J., Huang, C. T., Horng, G., & WANG, S. J. (2020). Robust and blind image watermarking in DCT domain using inter-block coefficient correlation. *Information Sciences*, *517*, 128–147. https://doi.org/10.1016/j.ins.2019.11.005

[21] Salem, N., Malik, H., & Shams, A. (2019). Medical image enhancement based on histogram algorithms. *Procedia Computer Science*, *163*, 300–311. https://doi.org/10.1016/j.procs.2019.12.112