Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493)
Vol. 3 No. 1, August 2018, pp. 28 – 38

Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit

Kas Raygaputra Ilaga*[1], **Christy Atika Sari**[2]
Universitas Dian Nuswantoro / Informatics Engineering Department, Jalan Imam Bonjol 207 Semarang, (+6224) 3517261/ (+6224) 3569684
E-mail : kas.rayga2012@gmail.com[1], christy.atika.sari@dsn.dinus.ac.id*[2]
**Corresponding author*

Abstract - The development of the digital world in the field of information technology is so rapid that making the exchange of information easy and fast. Such information may be general or specific. In general information there is no problem for the public, but specific information can not be free in the public. The main problem of the specific information is security, how the information is safe. To overcome these problems can be solved using cryptography and steganography. Cryptography is a technique for securing specific (secret) information from uninvolved parties, but the outcome is much different from the original information. While steganography is a technique to secure or hide the secret information on a digital object such as sound, image, vidio that applied results as seen the original information. In this paper be used a combination of ECB Mode cryptographic method and LSB steganographic method on a digital image. The measurement method uses Peak Signal to Noise Ratio and Mean Square Error to determine the quality of the stego image. The proposed cryptographic and steganographic methods are excellent for digital image encryption of RGB and Grayscale type since the resulting image (stego image) looks like the original image, with the best stego-image proof with MSE is 0.00013, PSNR is 87.00141, SSIM is 1 shows excellent results.

Keywords - Cryptography, Steganography, ECB Mode (Electronic Code Book), LSB (Least Significant Bit), Image Cryptography.

1. INTRODUCTION

Information and communication technology is currently growing rapidly, so it can send in large numbers and easily through the internet network [1], in terms of this security of cryptography and steganography is needed for all matters relating to information. According to [2], information equality is a matter of concern as it relates directly to one's privacy. Along with the increased importance, many methods have been made. The method is based on the systematic processing of mathematical operations as its foundation.

Cryptography and steganography are the solution to the problem in this case. Cryptography is a technique for securing an information into encoded information (encrypted), the information must be decrypted first to know the original information. Steganography is a technique for hiding information on digital media such as image, video, sound as suggested by [3]. Steganography is flexible and visibility is easy to set up, the point is that hidden information can not be detected directly without being extracted as proposed [4].

Information security is a main problem in this case. In cryptography, the security is not good enough because the encryption (ciphertext) is easily recognizable which allows the uninvolved party to try to pierce, therefore in this paper we use additional Steganography that

melimiki better security because the information (stego-file) is not clearly visible difference with the original information.

In this paper have been organized as follows. Section 2 discusses the details of the encryption and decryption system in cryptography using ECB Mode and embedding and extraction methods on steganography using the LSB method. In Section 3 the outputs of the methods are summarized in the table, and the descriptions. In Section 4 we conclude.

2. RESEARCH METHOD

2.1 Cryptography

Cryptography is a technique with science-based mathematical operations that learn about securing information so that no one knows other than the intended party [5]. Kriptografi memenuhi kebutuhan umum suatu pertukaran informasi yaitu, confidentiality, data integrity, authenticity, non-repudentiation.

Cryptography has components, which are plaintext, key, ciphertext. [6] Plaintext is the original information to be secured. A key is a secret code used to secure plaintext. Ciphertext is encoded information which is the result of the security process. Cryptography has two systems, which are encryption and decryption.

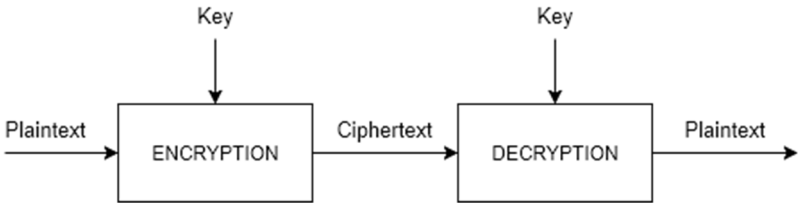


Figure 1. Cryptography Flow

Encryption is the process of securing information by making the information become unreadable directly without being decrypted first. Encryption is the process of encoding plaintext with key to ciphertext, ciphertext can vary because it depends on algorithm, plaintext and key. Decryption is the process of reading encoded information with the key requirement must be right to know the original information (plaintext).

2.2 ECB Mode (Electronic Code Book)

ECB Mode is included in Block Cipher Mode of Operations. This cryptographic method has a simple operation. Information will be divided into independent plaintext blocks. Encryption method on ECB Mode runs on binary numbers. Plaintext will be divided into plaintext blocks according to the key length. Each block is independent so it got more secure. However if it got error, there is not happen for other blocks. Because in this case it have many pixels to do then ECB Mode is better for many blocks because the repetitive blocks will not happen often. In the blocks are performed bit xor operations with the same key. From the result of bit xor operation is performed bit shit left 1 bit operation called ciphertext. Decryption starts from ciphertext which the process is opposite as encryption, but in bit shift operation it uses bit shift right 1 bit.

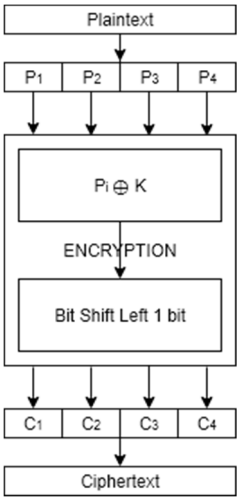


Figure 2. Electronic Code Book (ECB) Mode Encryption

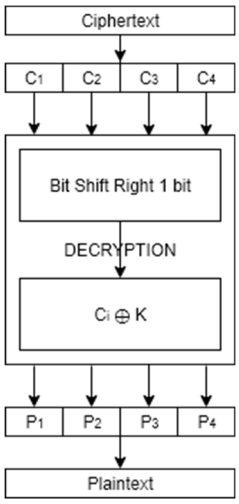


Figure 3. Electronic Code Book (ECB) Mode Decryption

Following are the ECB Formula:

Encryption: $C_i = E(P_i, K)$ (1)

Decryption: $P_i = D(C_i, K)$ (2)

Where:

C_i = Ciphertext Block to i,

P_i = Plaintext Block to i,

K = Key,

E = Encryption,

D = Decryption.

2.3 Steganography

Steganography is the development of cryptography that reduces the original information difference with the results of its information because to avoid hacking. Steganography can be implemented in all digital media. Steganography is also more flexible and visibility can be arranged [7].

Steganography has several different components with cryptography. Because in this paper, its applied in digital image therefore its component are cover-image, payload, stego-image. Cover image is the original image to be inserted (embedding). Payload is information that will be embedded on the original image. The payload form is a binary number. In steganography key is optional. Steganography has two systems, which are embedding and extraction.

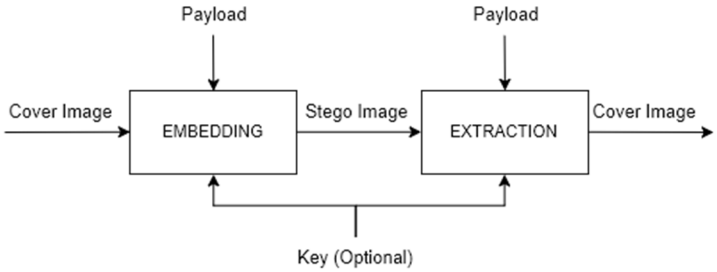


Figure 4. Steganography Flow

Embedding is the process of hiding information (payload) by inserting it on the cover image [4] by making the information becomes can not be seen directly because the stego image is very similar to the cover image, it must be extracted first. Extraction is the process of issuing embedded information with the key requirement must be right to know the original information.

2.4 Least Significant Bit (LSB)

Least Significant Bits (LSB) is one of the steganography methods. LSB is the smallest bit value. The position is the lowest bit or right-most bit in binary integer. This method, [8]replaces the right-most bit in the original data with each bit of input data that increment continuously.

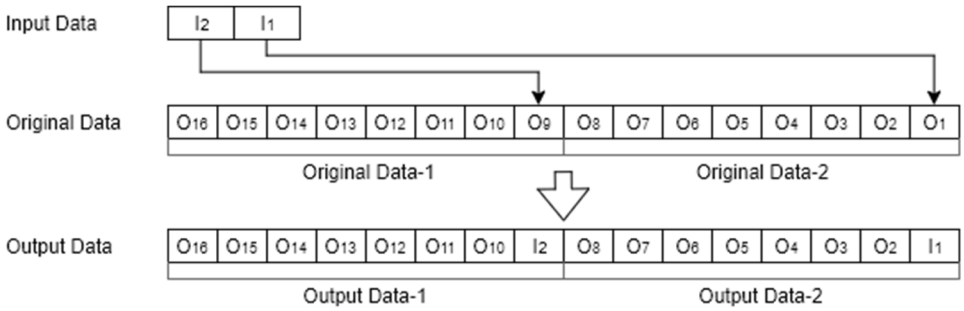


Figure 5. Least Bit Significant (LSB) Embedding

2.5 Proposed Method

Proposed cryptographic and steganographic methods using ECB Mode and LSB. For the more clear and detailed methods are shown in Figs. 6 and 7.

2.5.1 *Encryption and Embedding Algorithm*

Visualization encryption and embedding information in ECB-LSB shown in Fig. 6.

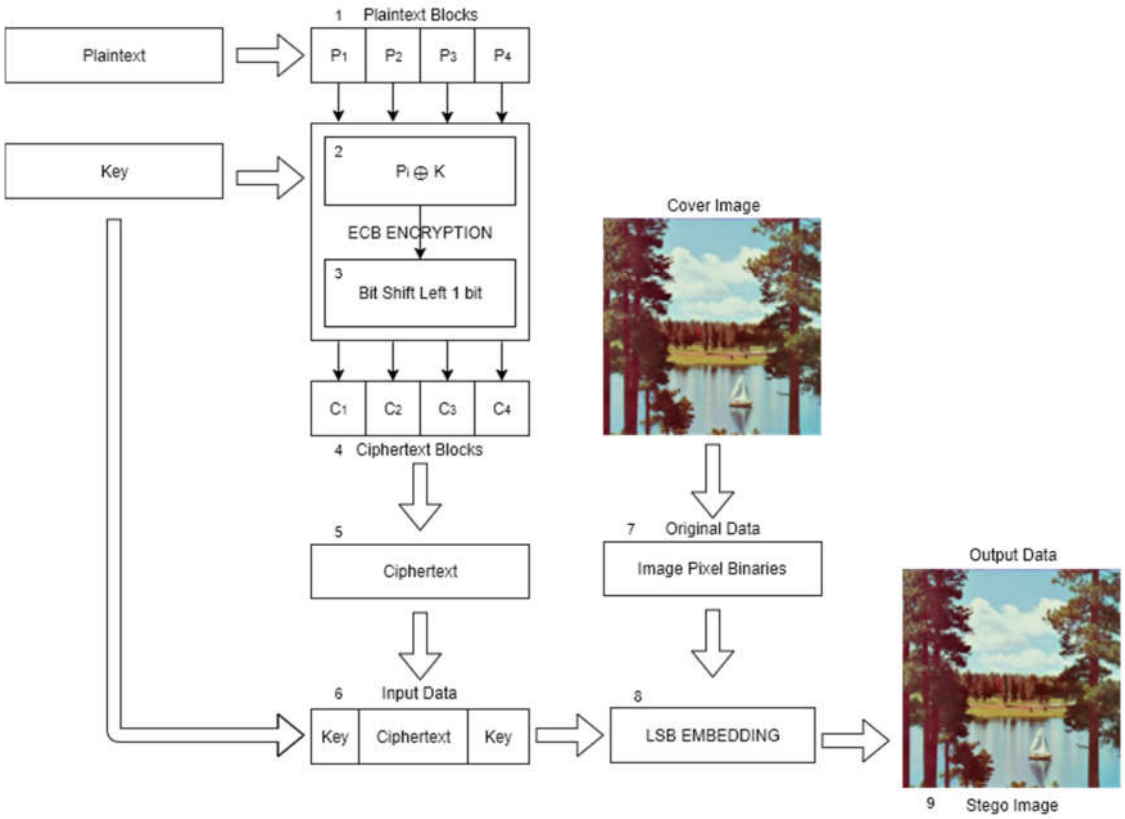


Figure 6. Encryption and Embedding ECB-LSB Visualization

Explanation of the encryption and embedding visualization in Fig. 6:

Encryption:

1. Divides plaintext into several independent blocks that each block of length corresponds to the key length.
2. Perform a bit xor operation on each plaintext block with a key.
3. Perform a bit shift left operation 1 bit on each plaintext block.
4. Obtain ciphertext blocks from all encrypted plaintext blocks ECB Mode.
5. Merge all ciphertext blocks into a ciphertext unity.

Embedding:

6. Insert key that same as before on encryption between ciphertext as input data.
7. Convert the cover image into image pixel binaries as the original data.
8. LSB Embedding on each bit of input data on original data with initial random pixel position.
9. The result is a stego image that contains ciphertext (secret information).

2.5.2 *Extraction and Decryption Algorithm*

Visualization extraction and decryption information in ECB-LSB shown in Fig. 7.

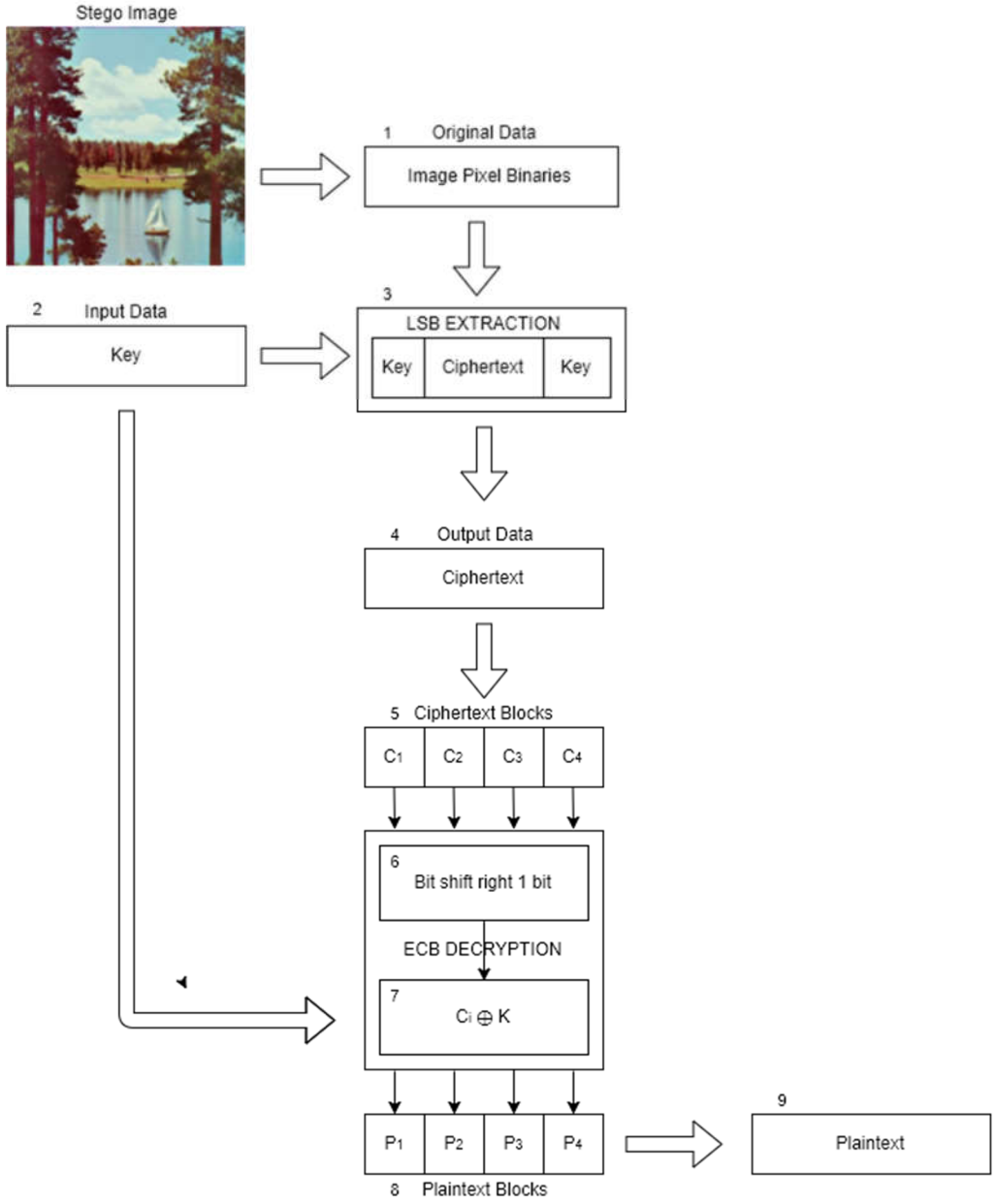


Figure 7. Exctraction and Decryption LSB-ECB Visualization

Explanation of the extraction and decryption visualization in Fig. 7:

Extraction:

1. Convert stego image into image pixel binaries as original data.
2. Prepare key as input data. (Key is a sign, there are 2 places key which are between the ciphertext)
3. LSB Extraction on each bit input data in original data by searching and comparing key as pixel sign beginning and end of a ciphertext (secret information).
4. Obtain the ciphertext from the extraction results.

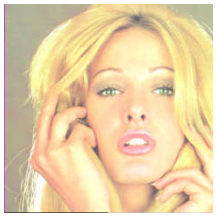
Decryption:

5. Divide the ciphertext into several independent blocks that each block of length corresponds to the key length.
6. Perform a bit shift right operation 1 bit on each ciphertext block.
7. Perform a bit xor operation on each ciphertext block with a key.
8. Obtain plaintext blocks from all deciphered ciphertext blocks ECB Mode.
9. Merge all plaintext blocks into a plaintext unity.

3. RESULTS AND DISCUSSION

In this paper be used 5 RGB Natural Images and 5 Grayscale Medical Images with 3 sizes (256 * 256), (384 * 384), (512 * 512) and tiff format. For Natural Images obtained from http://sipi.usc.edu/database/ and Medical Images obtained from https://medpix.nlm.nih.gov/. Below are the images used in this paper using RGB natural and medical images as shows below.
Grayscale Natural Images:


4.2.01


4.2.02


4.2.04


4.2.06

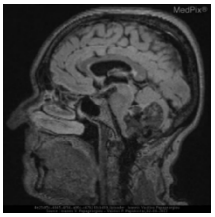

house

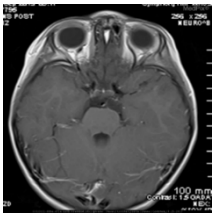
Grayscale Medical Images:


synpic18143


synpic32955


synpic33254


synpic57239


synpic59562

All cover images inserted information with the proposed method. To measure the results of the method using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and SSIM. MSE is how close the regression line is on the set of points by measuring the mean of the square of the error or deviation, measuring the distance from point to line regression and squaring it. According to [9], Differences occur due to randomness or because the estimator does not take into account information that can produce more accurate estimates. The smaller the MSE value of an image the better the quality. MSE is given by Equation (3).

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \sum_{k=0}^{2} \|g(i,j,k) - f(i,j,k)\|^2 \quad (3)$$

Where:
M, N = Number of columns and rows in pixels,
f(i, j, k) = Original image (cover-image),

g(i, j, k) = Result image (stego-image).

PSNR is a function that measures the quality of reconstructed images. Function It is often used in watermarking image to indicate Imperceptibility. Imperceptibility means that the perceived quality of the host image should not be distorted by the watermark. A higher PSNR would indicate that the reconstruction is of higher quality [9]. PSNR is given by Equation (4).

$$PSNR_{dB} = 10 \log 10 \left(\frac{{MAX_f}^2}{\sqrt{MSE}}\right) \quad (4)$$

Where:
MAX_f = The maximum pixel value of the image,
MSE = Mean Square Error.

The structural similarity (SSIM) index is a method for predicting the perceived quality of digital television and cinematic pictures, as well as other kinds of digital images and videos. It also use for measuring between two images [10]. It designed to improve on traditional method like PSNR and MSE. SSIM is given by Equation (5).

$$SSIM(x, y) = \frac{(2\,\mu_x\mu_y + C_1)(2\,\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (5)$$

Where:
x = Signal of original image (cover-image),
y = Signal of result image (stego-image),
μx, μy = The local means,
σx, σy, σxy = Standard deviations,
C1, C2 = Constant C is included to avoid instantability when $\mu_x^2 + \mu_y^2$ is very close to zero.

Below is shown stego image and results in analysis table insertion and description:
RGB Natural Images:

Table 1. Analysis results of encryption, embedding, decryption, extraction an information on verious images within size 512 * 512 using ECB-LSB

Cover Image	PLAINTEXT	KEY	CIPHERTEXT	MSE	PSNR	SSIM	TOTAL TIME (second)
4.2.01.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00014	86.63419	1	67
4.2.02.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00019	85.26898	1	73
4.2.04.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00015	86.29560	1	35
4.2.06.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00015	86.40556	1	10
house.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00015	86.33195	1	70

According to result in Table 1, the average MSE is 0.00016, the average PSNR is 86.18725, the average SSIM is 1 which can be concluded that the quality of stego-image quality is good.

Table 2. Analysis results of encryption, embedding, decryption, extraction an information on verious images within size 384 * 384 using ECB-LSB

Cover Image	PLAINTEXT	KEY	CIPHERTEXT	MSE	PSNR	SSIM	TOTAL TIME (second)
4.2.01.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00026	83.94406	1	46
4.2.02.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00026	82.71343	1	39
4.2.04.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00027	83.86982	1	50
4.2.06.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00030	83.38290	1	48
house.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00029	83.51654	1	44

Table 2 was illustrated a value of the average MSE is 0.00028, the average PSNR is 83.48535, the average SSIM is 1 which can be concluded that the quality of stego-image quality is good.

Table 3. Analysis results of encryption, embedding, decryption, extraction an information on verious images within size 256 * 256 using ECB-LSB

Cover Image	PLAINTEXT	KEY	CIPHERTEXT	MSE	PSNR	SSIM	TOTAL TIME (second)
4.2.01.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00063	80.16776	1	13
4.2.02.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00077	79.24838	1	21
4.2.04.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00069	79.76348	1	4
4.2.06.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00068	79.79577	1	11
house.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00053	80.89648	1	23

Based on the data in Table 3 that the average MSE is 0.00066, the average PSNR is 79.97437, the average SSIM is 1 which can be concluded that the quality of stego-image quality is good. Whereas the data in Table 1, Table 2 and Table 3 shown the average MSE is 0.00037, the average PSNR is 83.21566, the average SSIM is 1 which can be concluded that the stego-image quality will be better if the image size is bigger with evidence that the best result is 4.2.01.tiff with size 512 * 512 obtained MSE is 0.00014, PSNR is 86.63419, SSIM is 1. Several results using grayscale medical images has been shown in Table 4 until Table 6.

Table 4. Analysis results of encryption, embedding, decryption, extraction an information on verious images within size 512 * 512 using ECB-LSB

Cover Image	PLAINTEXT	KEY	CIPHERTEXT	MSE	PSNR	SSIM	TOTAL TIME (second)
synpic18143.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00013	87.00141	1	90
synpic32955.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00015	86.48044	1	11
synpic33254.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00016	86.18836	1	17
synpic57239.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00016	86.18836	1	16
synpic59562.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00018	85.65727	1	69

Compared with Table 3, inside of Table 4 a result of several images in 512x512 pixels shown an average value of MSE is 0.00016, the average PSNR is 86.30317, the average SSIM is 1 which can be concluded that the quality of stego-image quality is good.

Table 5. Analysis results of encryption, embedding, decryption, extraction an information on verious images within size 384 * 384 using ECB-LSB

Cover Image	PLAINTEXT	KEY	CIPHERTEXT	MSE	PSNR	SSIM	TOTAL TIME (second)
synpic18143.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00029	83.48274	1	7
synpic32955.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00025	84.21438	1	33
synpic33254.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00028	83.68959	1	58
synpic57239.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00031	83.25325	1	59
synpic59562.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00031	83.25325	1	50

Based on the data in table 5 that the average MSE is 0.00029, the average PSNR is 83.57864, the average SSIM is 1 which can be concluded that the quality of stego-image quality is good.

Table 6. Analysis results of encryption, embedding, decryption, extraction an information on verious images within size 256 * 256 using ECB-LSB

Cover Image	PLAINTEXT	KEY	CIPHERTEXT	MSE	PSNR	SSIM	TOTAL TIME (second)
synpic18143.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00065	80.02878	1	16
synpic32955.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00064	80.06311	1	25
synpic33254.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00064	80.09772	1	22
synpic57239.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00060	80.38496	1	25
synpic59562.tiff	Kas Raygaputra I	myData	L0n,L (<J" * >0ÈP	0.00063	80.16776	1	18

An experiment results of 256x256 pixels given by Table 5, which is the average MSE is 0.00063, the average PSNR is 80.14847, the average SSIM is 1 which can be concluded that the quality of stego-image quality is good. Based on the data in Table 4, Table 5, and Table 6 that the average MSE is 0.00036, the average PSNR is 83.34342, the average SSIM is 1 which can be concluded that the stego-image quality will be better if the image size is bigger with evidence that the best result is synpic18143.tiff with size 512 * 512 obtained MSE is 0.00013, PSNR is 87.00141, SSIM is 1.

4. CONCLUSION

In this paper combined ECB Mode cryptographic method with LSB steganographic method. The system works by encoding text-based information (ASCII) by converting the information into binary form using ECB Mode, then the result of encrypted information (ciphertext) is inserted using LSB on digital images of RGB and Grayscale types. Referring to the result of the obtained paper that the bigger the image size PSNR, MSE and SSIM is better for RGB and Grayscale image. The best result obtained is synpic18143.tiff with the grayscale image type, size 512 * 512 obtained MSE is 0.00013, PSNR is 87.00141, SSIM is 1. Therefore it will also make the information more secure.

5. FUTURE WORK

For future work, these methods can be combined with PVD (Pixel Value Differencing) stereographic methods, other cryptographic block cipher methods such as CBC Mode (Cipher Block Chaining), CFB (Cipher Feedback), or other methods.

REFERENCES

[1] M. A. B. Younes dan A. Jantan, "Image Encryption Using Block-Based Transformation Algorithm," *IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03,* 2008.

[2] Q. Huang dan W. Ouyang, "Protect Fragile Regions in Steganography LSB Embedding," *International Symposium on Knowledge Acquisition and Modeling,* vol. 3rd, 2010.

[3] N. Akhtar, V. Ahamad dan H. Javed, "A Compressed LSB Steganography Method," dalam *IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017)*, 2017.

[4] W. Jiang, . Z. Guo, K. Wang dan Y. Huang, "A Self-contained Steganography Combining LSB Substitution with MSB Matching," dalam *International Conference on Computer Science and Network Technology (ICCSNT)*, 2016.

[5] R. M, Y. R dan Dr.S.V.Sudha, "Trends of Cryptography Stepping from Ancient to Modern," dalam *IEEE International Conference on Innovations in Green Energy and Healthcare Technologies(ICIGEHT'17)*, 2017.

[6] D. Sharma, "Implementing Chi-Square Method and Even Mirroring for Cryptography of Speech Signal using Matlab," dalam *International Conference on Next Generation Computing Technologies (NGCT-2015)*, Dehradun, 2015.

[7] M.-Y. Wang, C.-P. Su, C.-L. Horng, .C.-W. Wu dan C.-T. Huang, "Single- and Multi-core Configurable AES Architectures for Flexible Security," *IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS,* vol. 18, no. 4, April 2010.

[8] B. Karthikeyan, A. Deepak, K. S. Subalakshmi, A. R. M. M dan V. Vaithiyanathan, "A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm," dalam *International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB17)*, 2017.

[9] D. R. I. M. Setiadi, E. H. Rachmawanto dan C. A. Sari, "Secure Image Steganography Algorithm Based on DCT," *Journal of Applied Intelligent System,* vol. 2, no. 1, pp. 1-11, 2017.

[10] Z. Wang, A. C. Bovik, H. R. Sheikh dan E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to," *IEEE TRANSACTIONS ON IMAGE PROCESSING,* vol. 13, no. 4, pp. 1-14, 2004.