Jurnal Mantik, 5 (3) (2021) 1825-1832

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

Steganography Text Message Using LSB and DCT Methods

Bayu Angga Wijaya[1], Adrian Julio Manalu[2], Bayu Andreas Tarigan[3], Lovely Septian Silitonga[4]

[1234] Fakultas Teknologi dan Ilmu Komputer,
[1234] Universitas Prima Indonesia, Jl. Sekip Simp. Sikambing, Kec. Medan Petisah, Kota Medan, Sumatera Utara 20111, Indonesia

E-mail : bayuanggawijaya@unprimdn.ac.id[1], adrianmanalu04@gmail.com[2], bayuandreas995@gmail.com[3], tianvely@gmail.com[4]

ARTICLEINFO

Article History:

Received: September 11, 2021
Revised: October 14, 2021
Accepted: November 02, 2021

Keywords:

Steganography,
LSB,
DCT,
Message,
PSNR,
MSE

ABSTRACT

Advances in human thinking patterns make people realize that information technology is an important part of civilization. In line with the development of information technology, many parties are not responsible for committing crimes such as theft and falsification of information from data. These problems can be overcome using a variety of methods and techniques, one of which is steganography. Steganography is a technique of hiding confidential data in a digital (media) container so that the existence of the secret data is difficult to know by irresponsible people or parties. The purpose of this study is to provide a solution to the problem of hiding messages into images using two different steganographic methods, namely LSB and DCT, then both methods will be tested for their efficiency. In this study, it was concluded that the PSNR value for LSB steganography was 8.887, and the MSE value was 104.85. On the other hand, DCT Steganography got a PSNR of 83,728, and an MSE value of 0.0592. From the PSNR and MSE test results, it can be concluded that the better image quality comes from DCT Steganography, this is because, in processing DCT images, the author must convert the images first, then can encode, but this conversion is not done on the LSB method.

1. Introduction

Advances in human thinking patterns create people who are aware that information technology is an important part of civilization. In line with the development of information technology, there are also many parties who are not responsible for committing crimes such as theft and falsification of information from a data. These problems can be overcome using a variety of methods and techniques, one of which is stenography.

Stenography is a technique of hiding secret data in digital (media) containers so that the existence of the secret data is difficult to know by irresponsible people or parties (Aji, 2020), Stenography technique itself has many methods that can be used as needed, such as LSB (Least Significant Bit Mask and Filtering), compression and transformation, DCT (Discrete Cosine Transform) and DFT (Discrete Fourier Transform) methods. Based on research by Novani, Si, Ii, & Maliki, n.d.(2019) who combined the FFT (Fast Fourier Transform) and LSB (Least Significant Bit Mask and Filtering) methods. The results of this research are the data files that are used as containers are divided into blocks. After that the container data block is transformed into the frequency domain using the FFT (Fast Fourier Transform) method then the data or message that you want to insert into each container data block is inserted using the LSB (Least Significant Bit) method. After the entire block is inserted, then it is inverted again with FFT.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Based on the data described above, in this study the researcher will try to replace the FFT (Fast Fourier Transform) method in the research of Novani, Si, II, & Maliki, nd(2019), with the DCT (Discrete Cosine Transform) method, and comparing its efficiency and performance with the LSB (Least Significant Bit Mask and Filtering) method, the DCT method is used because the frequency adjustment is simpler than the FFT method for image media. So the title of the research that the author adopted is "Stenography of text messages using LSB and DCT methods".

2. Methods

This research methodology is divided into two parts, namely :

2.1 System Development Model

a. Analysis

Analysis is the stage of analyzing the things that are needed in the implementation of making applications. At this stage, the collection of reference materials on the LSB and DCT methods will be carried out. Then perform an analysis of the calculation of the text message insertion process using the LSB method which works by changing the redundant bits of the cover image which have no significant effect on the bits of the secret message. Meanwhile, DCT works by converting data from spatial form to frequency form, then processing frequency data, and converting it into spatial form using the inversion of the relevant method.

b. Design

This stage is the design of the user interface (User Interface). The design will be using Matlab software.

c. Coding

The stage of data translation or problem-solving that has been designed into a particular programming language. The programming language used in making this application is Java.

d. Testing

At this stage, the author will test the application, then record the test results that may experience problems or errors.

e. Maintenance

Maintenance is the final stage where the finished application changes, and adjustments from errors that appear during testing.

2.2 Design Program

This design is an overview of the software work system that will be made later. The design of this software consists of the design of UML (Unified Modeling Language) which consists of use case diagrams, and activity diagrams, and the design of Flowcharts (Flowcharts).

a. Usecase Diagram

Use case diagram is a picture or representation of the interaction that occurs between the system and its environment (user) [1]. The main purpose of this use case diagram is to explain the features or capabilities possessed by the user.

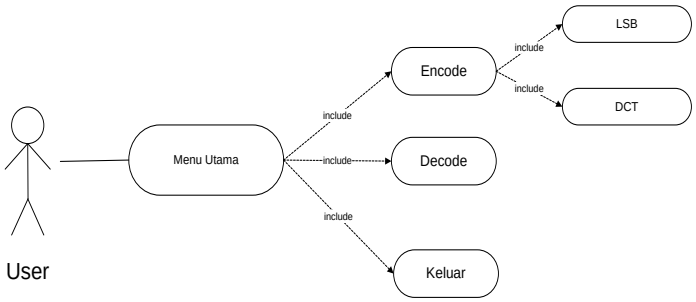


Fig. 1 Use Case Diagram

b. Activity Diagram

Making an application is also inseparable from the role of activity diagrams as an explanation of the workflow of the software created, activity diagrams serve to make it easier for users to understand the workflow of software made in visual form.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

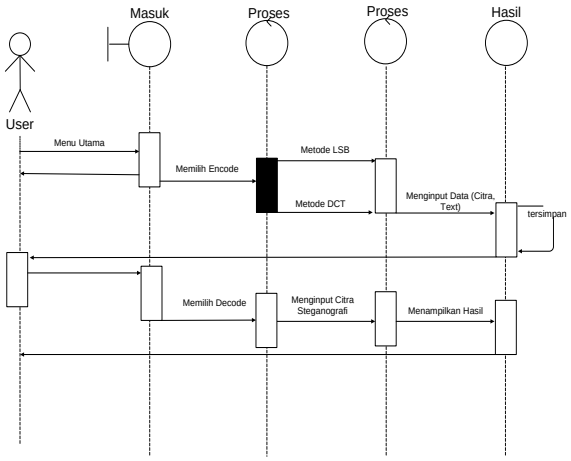


Fig. 2 Activity Diagram

c. Flowchart

The steps and sequence of making software are then presented in the form of graphs and arrows called flowcharts. The flowchart is expected to show the flow of user interaction with the software better.

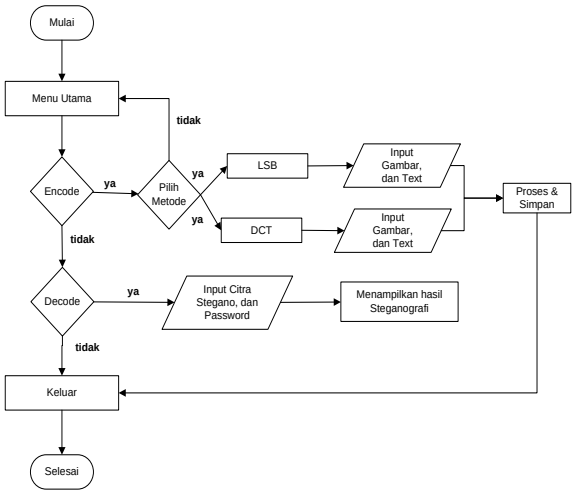


Fig. 3 Activity Diagram

3. Result and Analysis

3.1 Testing Lsb Method

a. Cover Image Input

In Picture 4 you can see the display program with LSB method, in this research the image used as the container is kualanamu.png.

Fig. 4 Cover Image

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

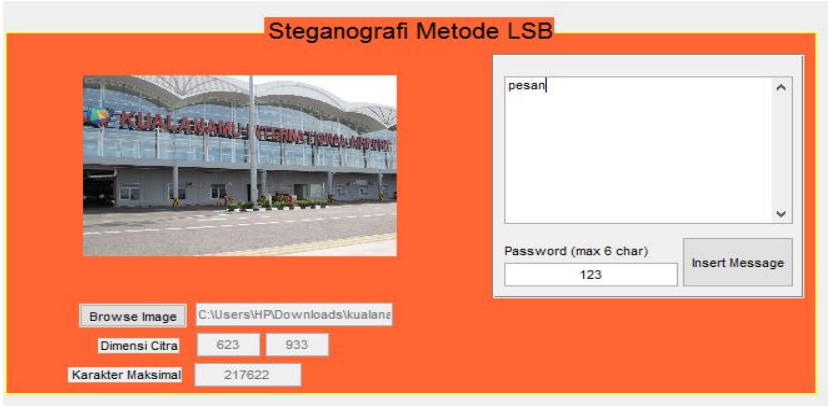


Fig. 5 Input Picture

b. Saving Steganography Image

After user input the image, he must input the password, and the message content that he want to insert inside the picture, As the example, we use "pesan" as the message content, and "123" as the password. After that the user must press the "Insert Message" button on the screen, and automatically the program or aplication will display "save file" window. Save the steganografi file with "SteganoLSB" as the name of file.

c. LSB method processing

Processing LSB method done by removing the smallest bits from the image, then replaced with the smallest bit of the inserted text or message. The first step is to change each character of the message that is inserted into a binary number.

Table 1
Table Picture

Character	ASCII	Biner
P	70	01110000
E	65	01100101
S	73	01110011
A	61	01100001
N	6E	01101110

Table 2
Table Binary Image

00010000	000001001	000001001	000001001	000001001	000001001	000001001	000001001
00111000	00110100	00110100	00110110	00110101	00110110	00110110	00110110
00111000	00110100	00110100	00110110	00110110	00110110	00110110	00110110
00111000	00110100	00110100	00110111	00110110	00110110	00110110	00110110
00111001	00110101	00110100	00110110	00110110	00110110	00110110	00110110

d. Binary insertion

The last step is to insert the binary value of the hidden message into the binary value of the image, by ignoring or deleting the smallest bit value from the image, and replacing it with the smallest bit value of the hidden message.

Table 3
Insertion Data

0	1	1	1	0	0	0	0
0	1	1	0	0	1	0	1
0	1	1	1	0	0	1	1
0	1	1	0	0	0	0	1
0	1	1	0	1	1	1	0

Table 4
Result of LSB Method

0001000**0**	000001001	000001001	000001001	000001000	000001000	000001000	000001000
0011100**0**	0011010**1**	0011010**1**	0011011**0**	0011010**0**	0011011**1**	0011011**0**	0011011**1**
0011100**0**	0011010**1**	0011010**1**	0011011**1**	0011011**0**	0011011**0**	0011011**1**	0011011**1**

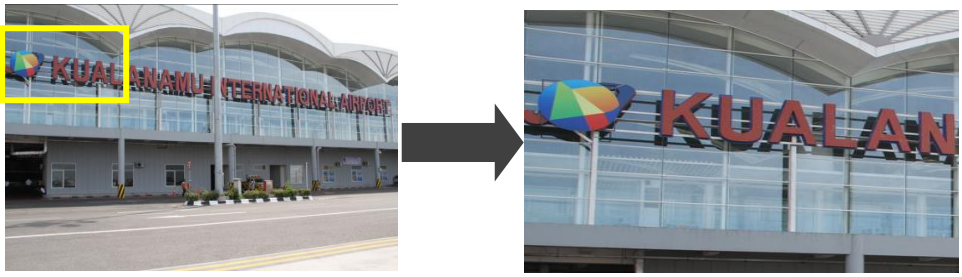
Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

00111000	00110101	00110101	00110110	00110110	00110110	00110110	00110110	001101101
00111000	00110101	00110101	00110110	00110111	00110111	00110111	00110110	

It can be seen in the LSB steganography table above that the smallest binary value is in the far-right position, and that value is then the smallest binary value of the message. The image of "Kualanamu" will not change much, the LSB method steganography only changes the binary value of the image because of the changes.

3.2 Testing Dct Method

a. The first step is to divide the “kualanamu” image into several blocks, and each block is divided into 8×8 pixel.



(1) (2)

Fig. 6 divide the original image (1), become 8×8 block pixel(2)

This block division is done because basically, every image consists of a collection of pixels r, g, b which are arranged in such a way as to form an image. The pixel division is useful to make it easier to calculate each pixel block that composes it.

b. The next step is count the value of matrix DCT by using this formula :

$$T(i,j) = \begin{cases} \frac{1}{\sqrt{N}} & jika\ i = 0 \\ \sqrt{\frac{2}{N}} \cos\frac{(2j+1)i\pi}{2N} & jika\ i \neq 0 \end{cases}$$

Then find the value of matrix C by using this formula :

$$C_{(i,j)} = round\ \frac{D_{ij}}{Q_{ij}}$$

Where “round” is the value result of the division to the nearest integer.

117	114	141	139	118	135	117	125
128	128	128	128	128	128	128	128
75	144	139	198	173	122	152	181
123	127	132	130	128	128	128	128
128	128	128	128	128	128	128	128
125	132	128	128	128	128	102	128
128	128	128	128	134	128	128	128
128	128	128	128	128	128	128	128

Fig. 7 Matrix C

c. The next step is zigzag compression scanning. This zigzag scan serves to sort the C matrix values in a zigzag manner, then convert them to binary data.

Accredited “Rank 4”(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

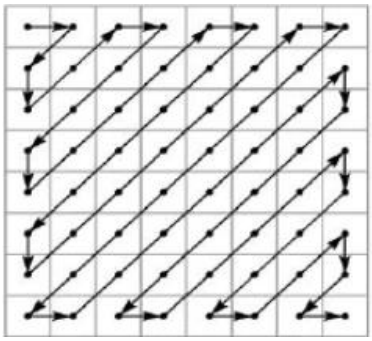


Fig. 8 Zigzag Scanning

d. The last step is the data decompression process, which is converting the compressed data into recognizable data. To decompress this data, the following equation is needed

$R = Q_{ij} \times C_{ij}$ become N, and the equation

$N = round\ (T^t.R.T) + 128$ so the result is :

117	114	141	139	118	135	117	125
128	128	128	128	128	128	128	128
75	144	139	198	173	122	152	181
123	127	132	130	128	128	128	128
128	128	128	128	128	128	128	128
125	132	128	128	128	128	102	128
128	128	128	128	134	128	128	128
128	128	128	128	128	128	128	128

Fig. 9 Matrix

e. This following picture is the result of processing image program with DCT method.

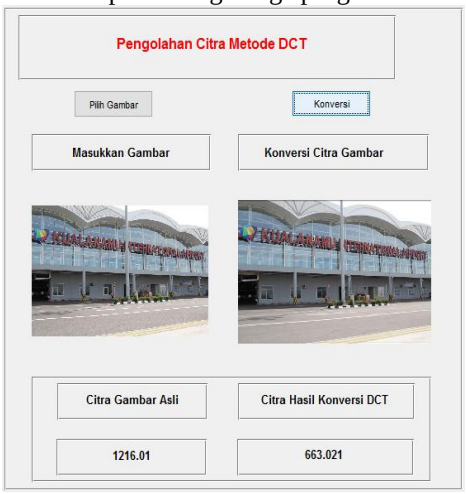


Fig. 10 DCT Processing Program

At first glance, there is no difference between the original image and the DCT processed image. But it can be seen that there are differences in size, and color composition stored in the DCT image processing.

f. The next step is to process the encoding message into images that have been converted with the previous DCT program.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

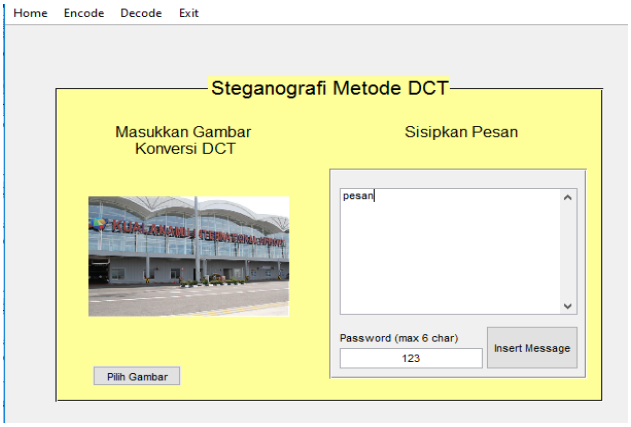


Fig. 11 Encoding Program with DCT

3.3 Decoding Steganography Lsb and Dct

Decoding is the last step on this program, this step give the user an ability to read the hidden message inside the picture. It works by converting a binary data set that has been inserted, and converted into readable data.

a. For example the author will try to decode the message that was inserted before into an image with LSB method, the file name is "SteganoLSB".

Fig. 12 Decode Program Desplay

b. Decode results from Steganography files with LSB Method

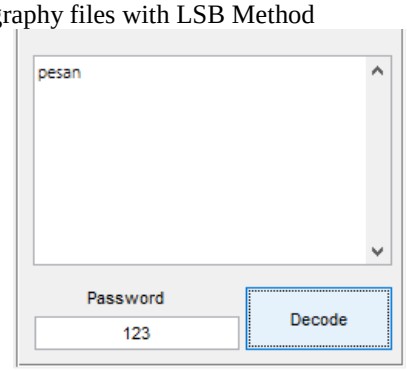


Fig 13 Result of Decoding

3.4 PSNR and MSE Analytics

PSNR and MSE measurement is needed to determine the quality of LSB and DCT steganography images value. And the following result is :

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Table 5
PSNR, and MSE measurement results

SteganoLSB.bmp							
PSNR Red	PSNR Blue	PSNR Green	**PSNR Total**	MSE Red	MSE Blue	MSE Green	**MSE Total**
8.974	8.831	8.856	**8.887**	103.93	105.17	105.44	**104.85**
SteganoDCT.bmp							
PSNR Red	PSNR Blue	PSNR Green	**PSNR Total**	MSE Red	MSE Blue	MSE Green	**MSE Total**
84,263	84,651	82,268	**83,728**	**0,0558**	**0,05372**	**0,06817**	**0,0592**

In the measurement table above, it can be seen that the PSNR value of the Stegano LSB is 8.887 db, and the MSE is 104.85 db. While the PSNR of the Stegano DCT is 83,726db, and the MSE is 0.0592db. Good image quality is if the PNSR value is higher than the MSE value, it can be seen in SteganoLSB that the PSNR value is smaller than the MSE value, while in SteganoDCT the PSNR value is greater than the MSE value.

4. Conclusions

Based on the results of the LSB (Least Significant Bit) Steganography Test, and the DCT (Discrete Cosine Transform) Method Steganography, it can be concluded that this research was successfully completed with a desktop-based steganography program that runs well. Files with the *.bmp extension are better than other file extensions in inserting messages into image images. LSB Steganography process is more efficient than DCT Steganography because LSB Steganography is basically used specifically to insert messages, while DCT Steganography is basically an image conversion method. From the PSNR and MSE table data in table 5, it can be concluded that the better image quality comes from DCT Steganography.

5. References

[1] Aji, I. B. 2020. Citra Hasil Dari Steganografi Discrete Cosine. Citisee, 1–9.
Basuki, R. S., and Maranggani, E. N. (2011). Installing Pesan Rahasia Di Dalam Suatu Gambar Dengan Metode Least Critical Bit Addition (Lsb). Course Nasional Teknologi Informasi and Komunikasi Terapan 2011 (Semantik 2011), 2011(Semantik), 2–7.

[2] D. A. N., Hersaputra, Y.,Sarjana, G. 2020. Pemanfaatan Metode Altered Least Huge Bit dan Teknik Adjustment Reshape Transposisi untuk Steganografi. Pendidikan, K., Kebudayaan, D. A. N., Tinggi, S., Informatika, M., Komputer.

[3] Jamasoka, S. 2012. Perbandingan Steganografi pada Citra Gambar Designs Exchange Organization dengan Algoritma Gifshuffle dan Metode Least Critical Bit. Kriptografi, (13509080).

[4] Nirmala, E. 2020. Penerapan Steganografi Document Gambar Menggunakan Metode Least Huge Bit (LSB) dan Algoritma Kriptografi Progressed Encryption Standard (AES) Berbasis Android. Jurnal Informatika Universitas Pamulang, 5(1), 36.

[5] Novani, P. I. S., Si, S., Ii, P., and Maliki, I. (n.d.). Steganografi Pada Media Video Computerized Dengan Menggunakan Metode Fft (Quick Fourier Change) Dan Lsb (Least Critical Bit) Oleh : Rizki Ayus Gusmayuda Fakultas Teknik dan Ilmu Komputer Jurusan Teknik Informatika Universitas Komputer Indonesia Abstra.

[6] Pradita, R., and Nurhaida, I. 2020. Implementasi Steganografi Video dengan Menggunakan Metode Egypt, Least Critical Bit (LSB) dan Least Huge Bit (LSB) Fibonacci Edge Pixel. Jurnal Telekomunikasi Dan Komputer, 10(1), 25.

[7] Rekursif, J., Ardiansyah, H., Susilo, B., and Erlansari, A. (2017). Penerapan Metode Dct (Discrete Cosine Change) Pada Aplikasi Penyembunyian. Jurnal Rekursif, 5(1), 66–74.

[8] Santiko, I. 2016. Implementasi Model Steganografi Dalam Mengelola Kerahasiaan Informasi Dengan Metode LSB (Least Critical Bit). Citisee, 44–52.

[9] Widyawati, L., Riadi, I., and Prayudi, Y. (2020). Near Investigation of Picture Steganography utilizing SLT, DCT and SLT-DCT Calculation. MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer, 20(1), 169–182.

[10] Wijaya, B. A., Nugraha, A., Juandry, J., Okinawa, J. and Kinoto, J. (2020) "Film Recommendation System with Social-Union Algorithm: Film Recommendation System with Social-Union Algorithm", *Jurnal Mantik*, 4(2), pp. 1278-1284. doi: 10.35335/mantik.Vol4.2020.932.pp1278-1284.

[11] Wijaya, B. A. 2018. The steganographic video analysis uses combination of discrete cosine transform and discrete wavelet transform algorithms. *J. Phys.: Conf. Ser.* **1116** 022046

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.