Jurnal Mantik
Volume 4, Number 3, Nov 2020, pp.1663-1670 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik

Comparative Analysis of Five Modulus an Pictorial Block Algorithms For Data Hiding in Digital Images

Syandi Nainggolan [1], Yennimar [2]

[1,2]Teknik Informatika, Universitas Prima Indonesia, Jl. Sekip Sei Kambing Medan 20111, Indonesia

Email : syandi.nainggolan44@gmail.com

ARTICLE INFO

Article history:
Received: 12/07/2020
Revised: 22/08/2020
Accepted: 30/09/2020

Keywords:
digital images, secret messages, steganography, Five Modulus, Pictorial Block.

ABSTRACT

Steganography is an art and science that studies invisible communication from confidential data on a multimedia carrier such as image, audio and video files. The most popular steganography method is the LSB (Least Significant Bit) method. However, the LSB method is very vulnerable to attack by using basic image processing operations. In 2013, Jassim applied the Five Modulus method in the steganography process. Five Modulus method will solve a digital image into a set of image sub-blocks called windows with size n x n. A secret message will be inserted in that window. According to Jassim, the smaller the window size, the more secret messages that can be inserted into the image. Meanwhile, in the Pictorial Block steganography algorithm, the secret information will be stored in a grayscale digital image file and converted to ASCII values and the length of the information will be calculated. After that, the digital image will be divided into 2n x 2n blocks using the block truncation coding (BTC) algorithm. Then, the block will be converted to binary format and incorporate the original information on its decomposition matrix. The pictorial block steganography algorithm uses the BTC algorithm to convert the grayscale input image block into a binary image block so that the secret information bit insertion operation can be performed. The resulting steganography software can hide confidential data into a digital image. The secret data stored in the stego image can be extracted out in the extraction process.

1. Introduction

Information security is one of the most important factors of information and communication technology because of the rapid development of the Web and copyright. Cryptography was created as a technique to secure the confidentiality of information. However, it is sometimes necessary so that the other party is not aware that information is confidential. For that, the steganographic method can be applied.

Steganography is the science of engineering or the art of hiding secret messages in other messages so that the existence of these secret messages cannot be accessed by other people who do not have the authority (Nizirwan Anwar, 2018). This technique will modify the multimedia carrier in an invisible way so that there is no known secret message attachment process and the location of the secret message is unknown. The steganography method will secure confidential data by hiding it on a media. Two requirements that must be met by the steganography method are the undetectability of the stego image and the ability to store secret information efficiently. The most popular steganography method is the LSB (Least Significant Bit) method (Nizirwan Anwar, 2018). However, the LSB method is very vulnerable to attack by using basic image processing operations. Jassim introduced the Five Modulus method which is applied to compress images (Jassim, 2012). The basic idea of this method is that neighboring pixels are usually related. Therefore, for a grayscale image, the neighbors of a pixel tend to be similar to that pixel. Then, in 2013, Jassim applied the Five Modulus method in the steganography process. Five Modulus method will solve a digital image into a set of image sub-blocks called windows with size n x n. A secret message will be inserted in that window. According to Jassim, the smaller the window size, the more secret messages that can be inserted into the image. The selection of the Five Modulus method is to hide files with the consideration that the Five Modulus method has a higher level of security when compared to the LSB method where the data will be stored randomly according to the data value so that other parties will have difficulty determining the position of secret data in the image.

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

Another algorithm that can be used is the Pictorial Block algorithm. In this algorithm, the secret information will be stored in a grayscale digital image file and converted to the form of ASCII values and the length of the information will be calculated. After that, the digital image will be divided into 2n x 2n blocks using the block truncation coding (BTC) algorithm. Then, the block will be converted to binary format and incorporate the original information on its decomposition matrix. The steganography pictorial block algorithm uses the BTC algorithm to convert the grayscale input image block into a binary image block so that the secret information bit insertion operation can be performed. The main concept of secret hiding is based on the approach of attaching confidential data to the cover media using a key. (Mondal, et. Al., 2012)

Based on the description above, the author is interested in comparing the Five Modulus and Pictorial Block steganography algorithms to secure secret files by hiding them in a digital image. The software created also provides facilities for attacking or adding noise to the stego image and image comparison process, so it is hoped that the software can provide an overview of the performance and performance of the Five Modulus and Pictorial Block steganography algorithms.

2. Literature Review

2.1. Steganography

As a part of information security "Steganography" is a wellknown concept, literally which signifies the meaning "covered writing". Steganography imposes the secret information within a cover object termed as stego-medium to escape detection and to retain the original information with minimum distortion. This stego-medium appears like a non-secret file in the network and manages to avoid drawing the attention towards itself as a content of security (Sourabh Chandra and Smita Paira, 2019).

Steganography is the art and science of writing hidden messages or hiding messages in a way so that apart from the sender and the recipient, no one knows or realizes that there is a secret message (it does not appear that there is a hidden message).

2.2. Five Modulus Method

Basically, Five Modulus Method (FMM) was founded as a method for image compression. The basic idea behind FMM is to transform the whole image into multiples of five. Since the human eye does not differentiate between the original image and the transformed FMM image. It is known that, for each of the R, G, and B arrays in the color image are consist of pixel values varying from 0 to 255. The main impression of FMM is to transform the whole pixels inside the image into numbers divisible by five. Steganography algorithms concentrate on introducing as small deformation in the cover image as possible. It is clear that the FMM transformation does not affect the Human Visual System (HVS).

The new pixel value in the k×k window will be a multiple of five as: 0, 5, 10, 20, …, 100, 105, …, 200, 205, 210, …, 250, 255. Hence, the values that are not divisible by 5 are distinct inside k×k block. Now, the good thing is that by dividing the new values by 5. A new range of values will be constructed as: 0, 1, 2, 3, …, 51. Since 0÷5=0, 5÷5=1, 10÷5=2, …, 250÷5=50, 255÷5=51. Hence, the new range is consisting of 52 distinct values (Firas A. Jassim, 2014).

The steganography technique is based on the FMM transformation. Therefore, all the pixels inside the FMM images are all multiples of 5 only. Basically, the original pixel values are in the range 0 to 255 for each of the Red, Green, and Blue arrays. After the FMM transform, the new range is still 0 to 255 but with multiples of 5 only, i.e. 0, 5, 10, 15, …, 255. The FMM method will be applied for both the cover and the stego images. Now, if we divide the new range by 5 we can get a simpler range that is 0, 1, 2, …51, i.e. 0÷5=0, 255÷5=51. The model of the proposed stegosystem could be introduced as a scheme in figure (1).

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

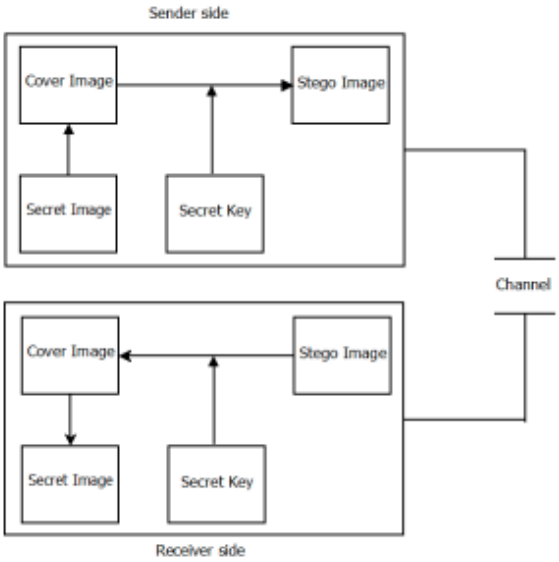

Fig 1. The Model of FMM Steganography Method (Firas A. Jassim, 2014)

Since the reminder of each number that is not divisible by five is either 0, 1,2,3 or 4. The zero reminder means that it is divisible by 5 while 1, 2, 3, 4 reminders means the opposite. The determination of the suitable window size is based on two concepts. The first one is that the new range values are 0..51, i.e. 52 distinct values. The second one is that the reminders of numbers that are not divisible by five are 1, 2, 3, and 4. Since the selection of window is based on the square criterion which means k×k. Then, nearest number which can accommodate the 52 values is 64. But the square root of 64 is 8 which means 8×8 window size and that is large. Now, to reduce the large window size, the second concept which is the 1, 2, 3, and 4 reminders may be applied. Since the whole values are multiples of five, then each number that is not divisible by five will be inconsistent with the others inside window. Therefore, by dividing 64 by 4 we get 16. Subsequently, a 4×4 window size that contains 16 items will be suitable to accommodate the proposed algorithm. A 4×4 window could holds the 52 values by using a simple looping method (Firas A. Jassim, 2014).

2.3. Pictorial Block Steganography Algorithm

Considered a grayscale image first, where we can encrypt the original information. In this paper the original information first converted into its corresponding ASCII value and the length of information have been calculated. After using binary conversion we have divided the binary number into 8 bit block segment. The initial gray scale image (256×256 i.e. 28×28) first converted into block size of (8×8) using block truncation coding (BTC). Then we have converted it into binary format using binary conversion and merge the original information into the decomposed matrices by the following encryption algorithm. Now we have sent this coded image towards the receiver end. At receiver section the reverse technique is followed to decompose the image matrix to easily retrieve the original information by the following decryption algorithm (Anupam Mondal, Sudipta Sahana, Sainik Kumar Mahata, 2012).

a) Encryption Technique:

Step 1: Taken an input string of information is known as a plain text.
Step 2: Calculate the number of character without Space stored in a variable of PT.
Step 3: Convert the PT string to ASCII value character by character and convert those characters to equivalent binary bits.
Step 4: Divide the binary bits in several blocks where every block was considering n numbers of bit.
Step 5: After that we were taken a gray scale image with dimension 2n x 2n.
Step 6: Apply the partial Block Truncation Coding on this gray scale image with n x n size block matrix, where every block of this matrix size 2(n-p) x 2(n-p) (where, n= 2p).
Step 7: Convert this gray scale image to bit map image.
Step 8: After taking the 1st block of the PT, we have considered the following steps.
Step 9: Now 1st block 1st bit placed into 1st image block (0, 0 position), 1st block 2nd bit placed into 2nd image block (0, 0 position) and continue this procedure for 1st block of text with n time recursively. Next time for the rest of the text block we were considering next row of the image recursively with (0, 0 position).
Step 10: Convert the entire changed binary image to gray scale image.

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

Step 11: Forward this gray scale image along with the unique dimension of each logical decomposed matrix block to the receiver.

b) Decryption Technique:

Step 1: Convert the gray scale image to binary image (bit map image).
Step 2: Apply the partial Block Truncation Coding with this binary image with n x n size block matrix, where every block of this matrix size 2(n-p) x 2(n-p) (where, n= 2p).
Step 3: Then taken the binary value of the 1st position (0, 0) from every block (2(n-p) x 2(n-p)) row wise.
Step 4: Then divided those bits in several blocks with n numbers of bit.
Step 5: Convert the binary representation into equivalent decimal form block by block.
Step 6: If the decimal number is zero Discard the number Else Convert the decimal number (ASCII value) to character.
Step 7: These set of characters are the ultimate information was forwarded by the sender.

3. Methodology

The work process of the Five Modulus Method can be detailed as follows:

a) The embedding process can be described using an activity diagram as shown in the following figure:

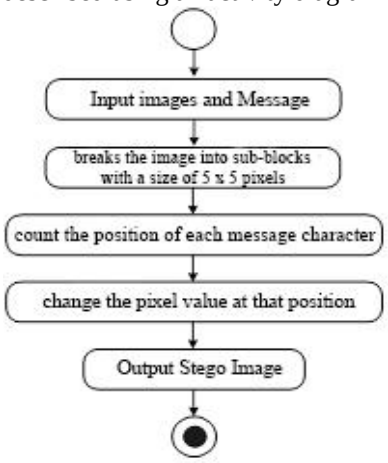

Fig 2. Activity Diagram of Embedding Process of FMM Steganography Method

b) The extraction process can be described using an activity diagram as shown in the following figure:

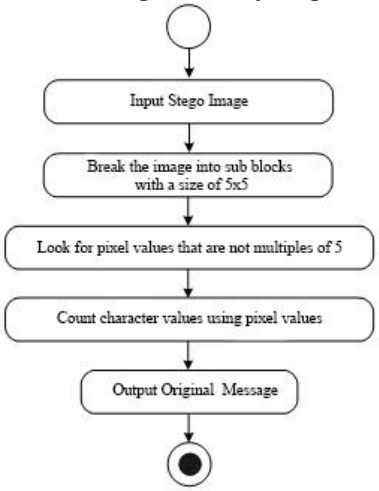

Fig 3. Activity Diagram of Extraction Process of FMM Steganography Method

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

The working process of the Pictorial Block method includes the process of embedding and extraction message. The work procedure of the message embedding process can be seen in figure below :

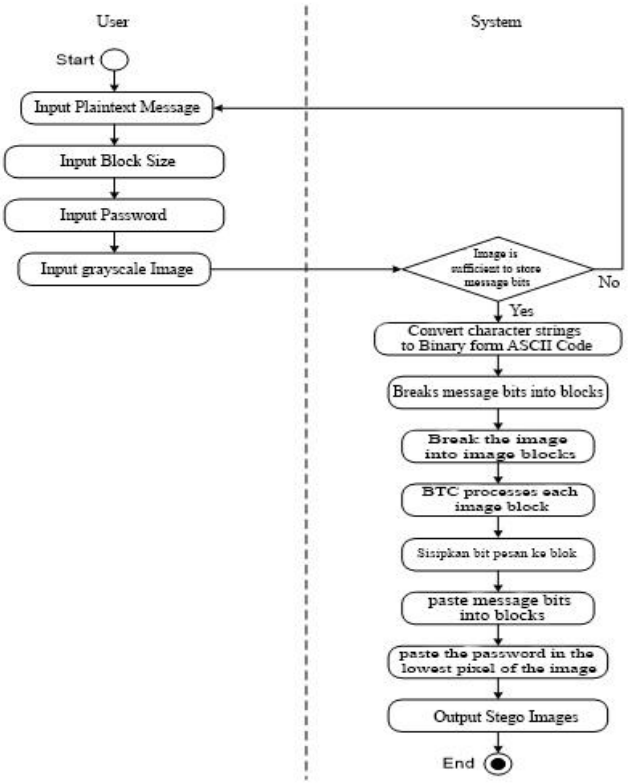

Fig 4. Activity Diagram of Embedding Process

The work procedure of the message extraction process can be seen in Figure 5 below:

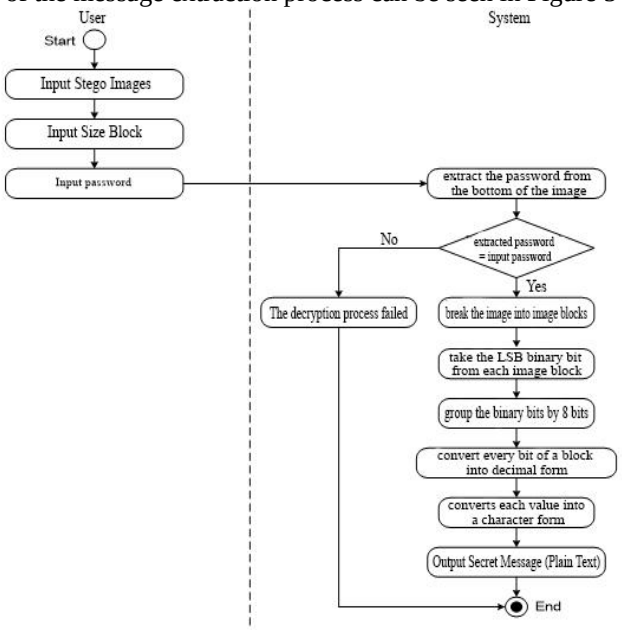

Fig 5. Activity Diagram of Message Extraction Process

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

4. Result and Testing

4.1. Result

In this main view, there are several menus that function to access the forms contained in the system. The following is the detailed of the menus contained in the system:

a) Message Embedding Sub Menu, which functions to embed confidential files into the cover image. The first step in the pasting process is selecting the cover image file to use. The trick is to click the '...' button, so the system will display the Open dialog box as shown in Figure 6:

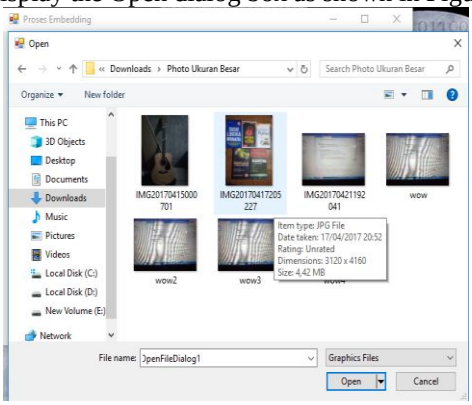

Fig 6. Display of Open Dialog Box

Select the desired image file. After that, click on the 'Open' button to open the image. After that, enter the secret message to be inserted. Suppose the secret message to be inserted is '0123456789'. After that, click on the 'Process' button so that the system will paste the secret file on the cover image. The display of the form after the pasting process can be seen in Figure 7:

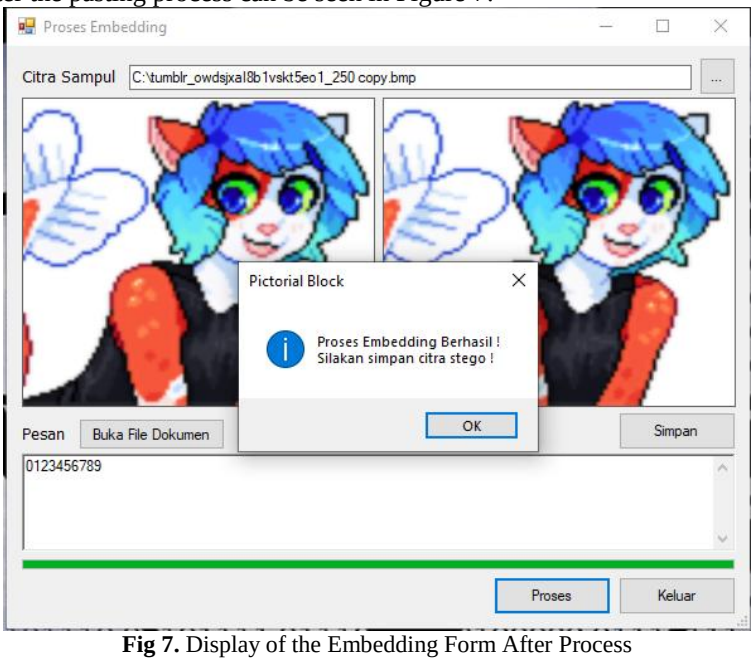

Fig 7. Display of the Embedding Form After Process

In the display process, this form shows the successful insertion of files into the steganographic image. After completing the message insertion process, please save the stego image that has been inserted with the message. Click the 'Save' button to save the stego image into a file. After that, the system will go to the Embedding form and click the 'Save' button to save the stego image.

b) File Extraction Sub Menu, which functions to extract files from steganographic images. The first step of the extraction process is to select the steganographic image file to be used. The trick is to click the '...' button, so the system will display the Open dialog box as shown in Figure 8:

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

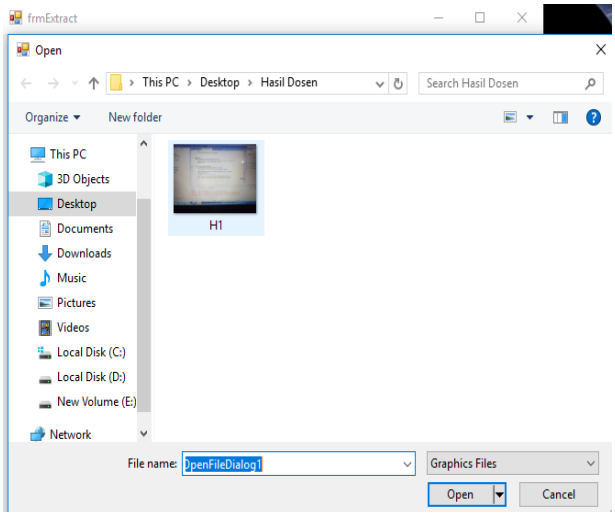

Fig 8. Display of Open Dialog Box

Select the desired image file. After that, click on the 'Open' button to open the image. After the image selection process, the Extraction form will look like Figure 9:

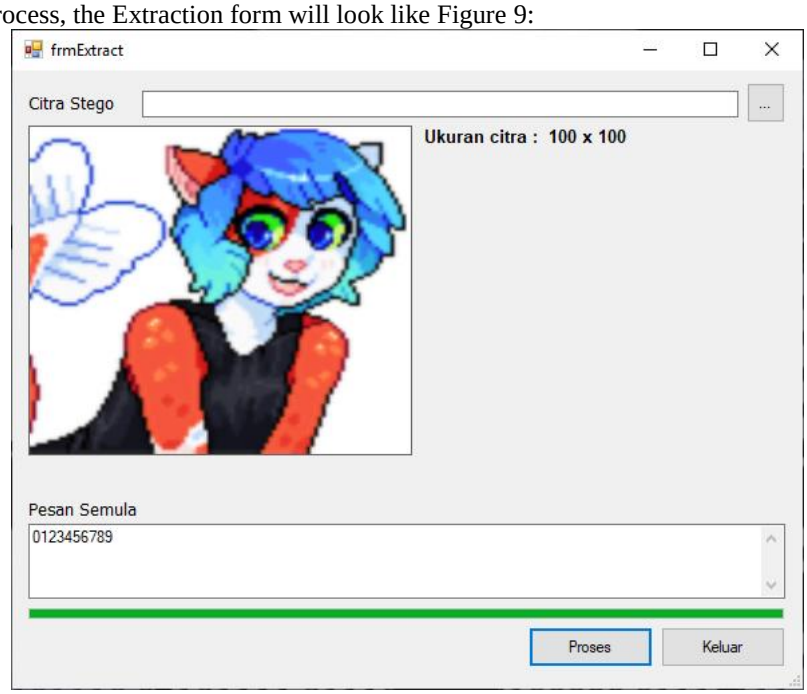

Fig 9. Display of the original file extraction form

After that, click the 'Process' button so that the system will display the results of the extraction process in the original textbox file and save it in the folder we want.

4.2. Testing

The testing process will be carried out using the MSE and PSNR methods to test the quality of the resulting stego image. The test results obtained can be detailed as follows:

Table 1
Testing Result

Cover Image Resolution	Five Modulus Method		Pictorial Block Steganography	
	MSE	PSNR	MSE	PSNR
200 x 200	0.8036	49.08	0.0493	61.20
300 x 300	0.7935	49.135	0.0336	62.8674
400 x 400	0.7931	49.1375	0.0282	63.6283
500 x 500	0.7918	49.1446	0.0225	64.6089
600 x 600	0.7875	49.1682	0.0168	65.8777

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

5. Conclusions

After completing this research, the author can get the following conclusions:

a) Pictorial Block Steganography Method has a better quality of stego image than Five Modulus Method.
b) Changes in the value of bits and the length of the extracted message size due to the process of adding noise are not seen from the amount of noise but from the replacement of the bits that are inserted into the message based on the test changing the pixel color.
c) The longer the text size and the block size, the less good the stego image quality is based on the PSNR and MSE testing.

6. References

[1] Ardhianto, E., Hadikurniawati, W., dan Budarso, Z, Implementasi Metode *Image Subtracting* dan Metode *Regionprops* untuk Mendeteksi Jumlah Objek Berwarna RGB pada *File Video*, Jurnal Teknologi Informasi DINAMIK Volume 18, No. 2, 91-100, 2013.
[2] Capah, S. N. A., Nasution, S. D., & Hondro, R. K, Penerapan Metode Median Filter Untuk Mereduksi, Jurnal Pelita Informatika, 17, 20–23, 2018.
[3] Erin Yuni Reva, Boko Susilo, Endina Putri Purwandari, Aplikasi *Watermark* Pada Citra Digital Menggunakan Kombinasi Metode *Discrete Cosine Transform*, *Discrete Wavelet Transform* dan *Singular Value Decomposition*, 2016.
[4] Jalaluddin & Melita, Pengolahan Citra Digital, 2012.
[5] Junaidi, Steganografi Audio (WAV) Menggunakan Metode LSB, *CCIT Journal*, *9*(2), 214-224, 2013.
[6] Munir, R., Pengantar Pengolahan Citra, PT. Elex Media Komputindo, Jakarta, 2014.
[7] Nafi'iyah, N., Algoritma Kohonen dalam Mengubah Citra Graylevel menjadi Citra Biner. JITIKA Vol. 9, No.2, 49-55, 2015.
[8] Nurcahyani dan Saptono, Identifikasi Kualitas Beras dengan Citra Digital, Scientific Journal of Informatics, Vol. 2 No. 1, Mei 2015, p-ISSN 2407-7658, http://journal.unnes.ac.id/nju/index.php/sji, e-ISSN 2460-0040, 2016.
[9] Nurul Fuad, Melita, Yuliana, "Analisa Perbandingan Metode Low- Pass Filter dengan Median Filter untuk Optimalisasi Kualitas Citra Digital", Magister Teknologi Informasi. Institut Saint Terapan & Teknologi Surabaya, 2012.
[10] Sembiring, Sanro, Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks pada Gambar dengan Metode End Of File, Medan, 2013.
[11] Sihombing, O., Zendrato, N., Laia, Y., Nababan, M., Sitanggang, D., Purba, W., ... & Siregar, S. (2018). Smart home design for electronic devices monitoring based wireless gateway network using cisco packet tracer. *JPhCS*, *1007*(1), 012021.
[12] Sitanggang, D., Siregar, S. D., Situmeang, S. M., Indra, E., Sagala, A. R., Sihombing, O., ... & Saragih, R. I. (2018, April). Application of forwardchaining method to diagnosis of onion plant diseases. In Journal of Physics: Conference Series (Vol. 1007, No. 1).
[13] Sulistiyanti dan Kris Sivam, Rancang Bangun Alat Identifikasi Jenis Daging dengan Pengolahan Citra Digital Menggunakan Python 2.7 dan Opencv Berbasis Raspberry Pi 3, Universitas Lampung, 2016.