File Hiding Application On Digital Images With Five Modulus Method

Roby Alfian[1], Arpan[2], Sri Wahyuni[3]
Computer System Study Program , Fakulty Of Science And Technologi ,
Pembangunan Panca Budi Medan 20122, North sumatera, Indonesia
Email: [1]Robyalfiannn@gmail.com , [2] ersevent@pancabudi.ac.id , [3] yuke@dosen.pancabudi.ac.id

Abstract

Article Info

Received : 29 November 2021
Revised : 22 December 2021
Accepted : 28 December 2021

Steganography is an art and study of 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 using basic image processing operations. In 2013, Jassim applied the Five Modulus method in the steganography process. The Five Modulus method will solve a digital image into a set of image subblocks called n x n sizes. Secret messages will be inserted in the window. According to Jassim, the smaller the window size, the more secret messages can be inserted into the image. The resulting steganography software can hide confidential data into a digital image. Secret data stored in the stego image can be extracted out in the extraction process.

Keywords : Digital Image, Secret Message, Steganography, Five Modulus Method, Attachment, Extraction

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, sometimes it is necessary to keep the other party from knowing that information is being kept confidential. For this reason, the steganography method can be applied.

The steganographic method will secure confidential data by hiding it in a media. Two requirements that must be met by the steganographic method are the undetectable nature of the stego image and the ability to efficiently store confidential information. The most popular steganographic method is the LSB (Least Significant Bit) method (Nizirwan Anwar, 2018). However, the LSB method is very vulnerable to attacks using basic image processing operations. Jassim introduced the Five Modulus method which was applied to compress images (Jassim, 2012). The basic idea of this method is that neighboring pixels are usually related. Therefore, for grayscale images, the neighbors of a pixel tend to be similar to those pixels. Then, in 2013, Jassim applied the Five Modulus method in the steganography process. The Five Modulus method will break a digital image into a set of image subblocks called windows with a size of n x n. The secret message will be inserted in the 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 perform file hiding 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 the secret data in the image.

Based on the description above, the author is interested in applying the Five Modulus steganography algorithm to secure secret files by hiding them in a digital image. The author chose the Five Modulus steganography algorithm with the consideration that this algorithm is able to produce stego images with good quality and easy to implement in practice because it uses a simple modulus operation. The software made also provides facilities for attacking or adding noise to the stego image and the image comparison process, so it is hoped that the software can provide an overview of the performance and performance of the Five Modulus steganography algorithm.

Image is a representation (picture), resemblance, or imitation of an object. The image as the output of a data recording system can be optical in the form of photos, analog in the form of video signals such as images on a television monitor, or digital which can be directly stored on a storage medium. Digital image is an image that is expressed discretely (not continuous), both for its coordinate position and color. Thus, a digital image can be described as a matrix, where the row index and column index of the matrix represent the position of a point in the image and the value of the matrix elements represents the color of the image at that point. In a digital image which is expressed as a matrix arrangement like this, the matrix elements are also referred to as pixels which come from the word picture element. Image can also be defined as a function of two variables, f(x,y), where x and y are spatial coordinates while the value of f(x,y) is the intensity of the image at those coordinates (Fuad&Melita, 2012).

In a binary image each point has a value of 0 or 1, each representing a certain color. For example, black is worth 0 and white is worth 1, in the standard image displayed on a computer screen, this binary value is related to the presence or absence of light fired by the electron gun contained in the computer monitor. The number 0 represents no light, thus the color represented is black. For number 1 there is light, so the color represented is white (Jalaluddin&Melita, 2012).

The number of colors depends on the number of bits provided in memory to accommodate this color requirement. The larger the number of color bits available in memory, the smoother the color gradation is. In the color image, each point has a specific color which is a combination of three basic colors, namely: red, green, blue. This image format is often referred to as an RGB (red-green-blue) image. Each basic color has its own intensity with a maximum value of 255 (8 bits). Thus each point in the color image takes 3 bytes. The number of possible color combinations for this image format is 224 or more than 16 million colors, thus it is considered to include all existing colors, this is why this format is called true color (Jalaluddin&Melita, 2012).

The Five Modulus Method (FMM) was first introduced by Jassim (2012). The basic idea of FMM is based on the concept that a common characteristic in most images is that neighboring pixels are interconnected. Therefore, in a 2-dimensional image, the neighbors of a pixel are almost the same as the original pixel. Therefore, FMM will divide an image into blocks of size k x k pixels.

The FMM transformation does not affect the human visual system (HVS). The algorithm introduced is referred to as ST-FMM which is referred to as Steganography by the Five Modulus Method. Therefore, all pixels in the FMM image are multiples of 5, so values that are not divisible by 5 will differ in k x k blocks. As is known, the standard ASCII code consists of 128 characters. But most of the 95 characters used in binary coding can be extracted from common ASCII codes. (Jassim, 2013)

2. Method

2.1 Method Of Collecting Data

To obtain the data or information needed to complete the research of this thesis, the authors collect data through the Library Research method. The author collects information through books, as well as other reference materials related to steganography, especially those related to the Five Modulus algorithm.

2.2 System Modeling

The designed system can be modeled using tools in the form of use case diagrams as shown in the following figure:

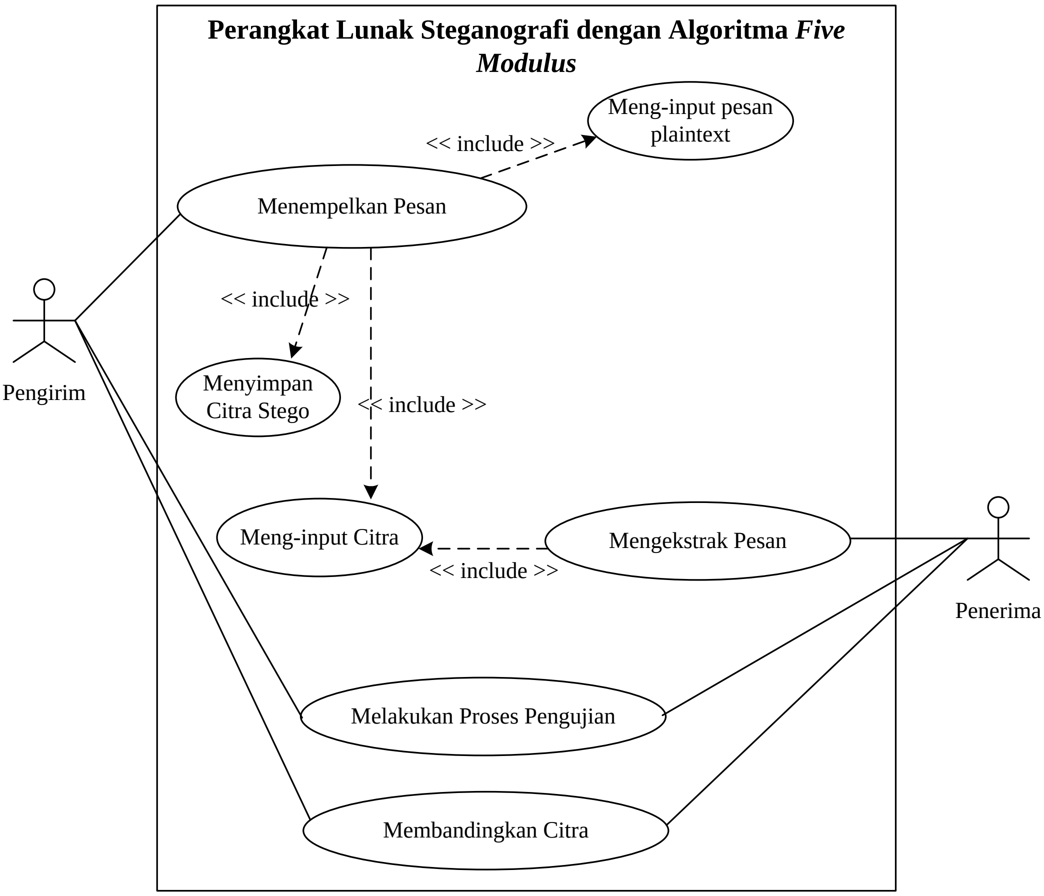


Figure 1. Drawing use case diagram of the system

2.3 Proces Analysis Method Five Modulus

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

1. The pasting process can be described using an activity diagram as shown in the following figure:

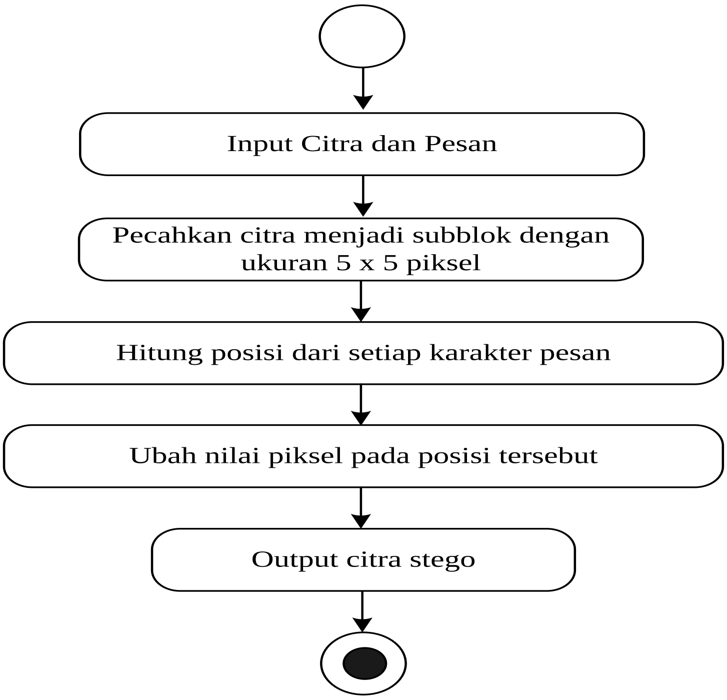

Input Citra dan Pesan
Pecahkan citra menjadi subblok dengan ukuran 5 x 5 piksel
Hitung posisi dari setiap karakter pesan
Ubah nilai piksel pada posisi tersebut
Output citra stego

Figure 2. Image activity diagram of the pasting proces

2. Ekstraction proces , can be described using an activity diagram as shown in the following figure :

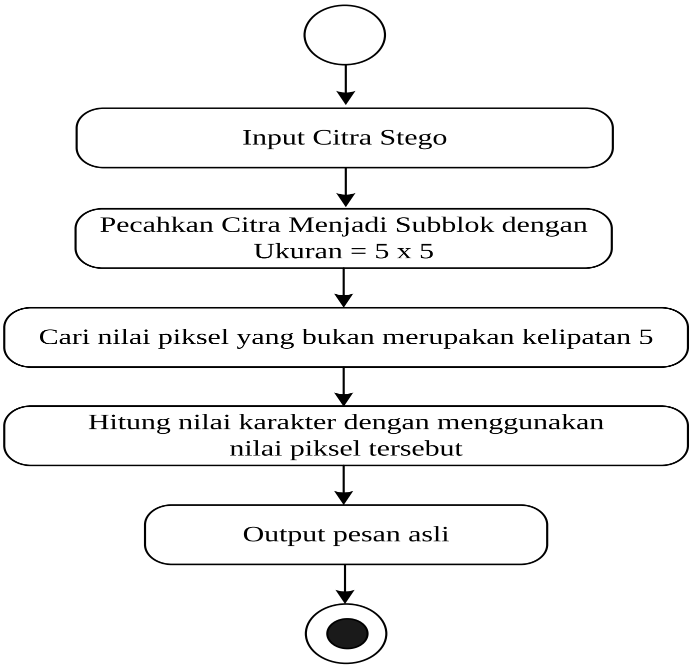

Input Citra Stego
Pecahkan Citra Menjadi Subblok dengan Ukuran = 5 x 5
Cari nilai piksel yang bukan merupakan kelipatan 5
Hitung nilai karakter dengan menggunakan nilai piksel tersebut
Output pesan asli

Figure 4. Drawing activity diagram of the extraction proses

3. Results And Discussion

3.1 Results

To use this software, run the file “Five modulus exe”, it will display the main screen of the program as shown in the picture:

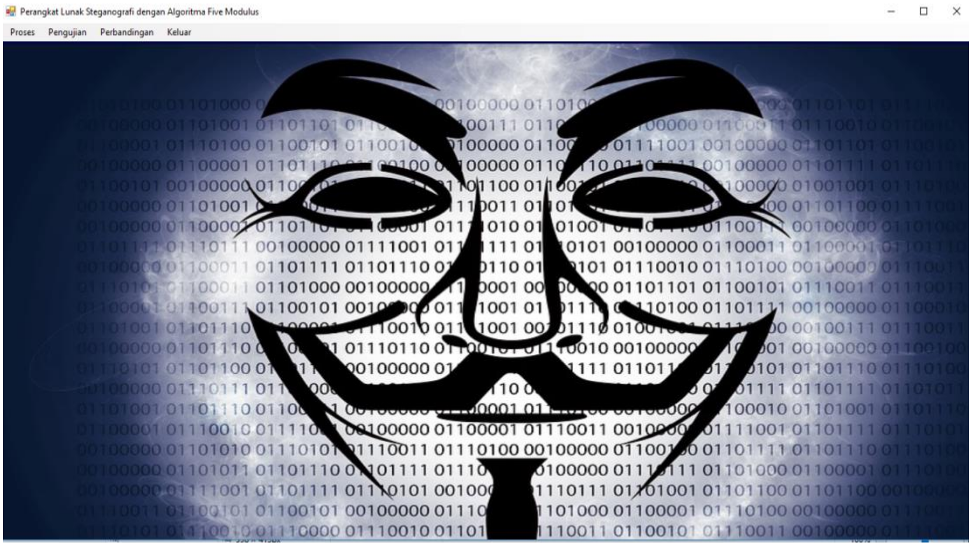


Figure 5. Main View Image

in this main view there are several menus that function to acces the forms contained in the system. The following are the details of the menu contained in the system :

A. Message attachment submenu , which server to carry out the process of pasting secret files into the cover image. The display of the attachment form can be seen in the image:

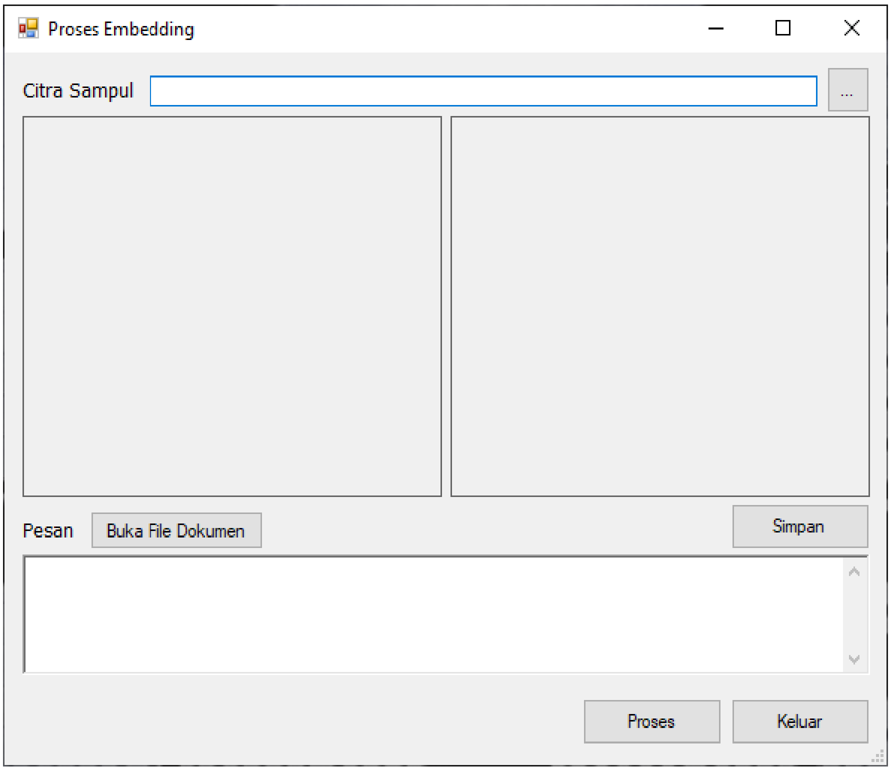
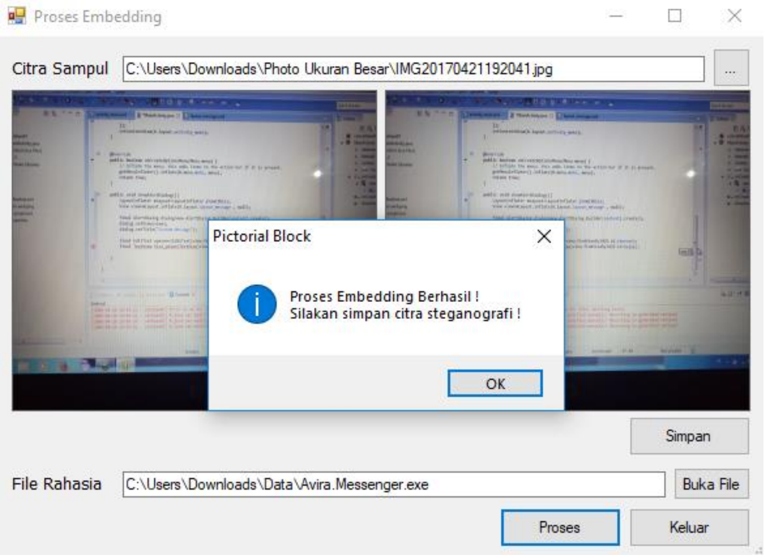


Figure 6. Attachment form display image



Citra Sampul C:\Users\Downloads\Photo Ukuran Besar\IMG20170421192041.jpg

Pictorial Block

Proses Embedding Berhasil !
Silakan simpan citra steganografi !

File Rahasia C:\Users\Downloads\Data\Avira.Messenger.exe

`

Figure 7. A picture of the display of the pasting form after the pasting process

File extraction sub menu, which function to perform the file extraction process from steganographic image. Extraction form display can be seen in the image:

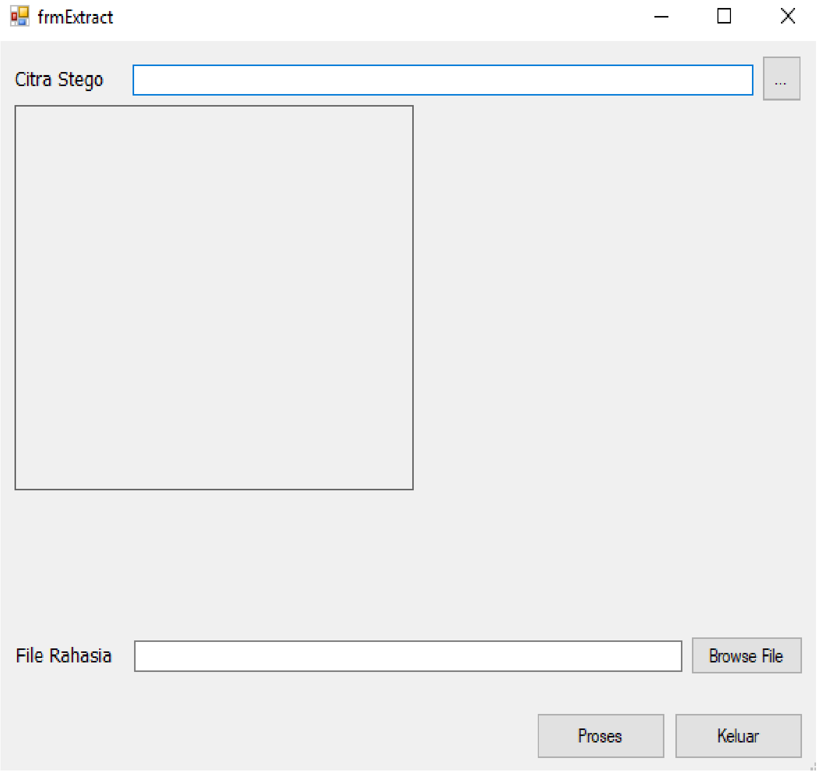
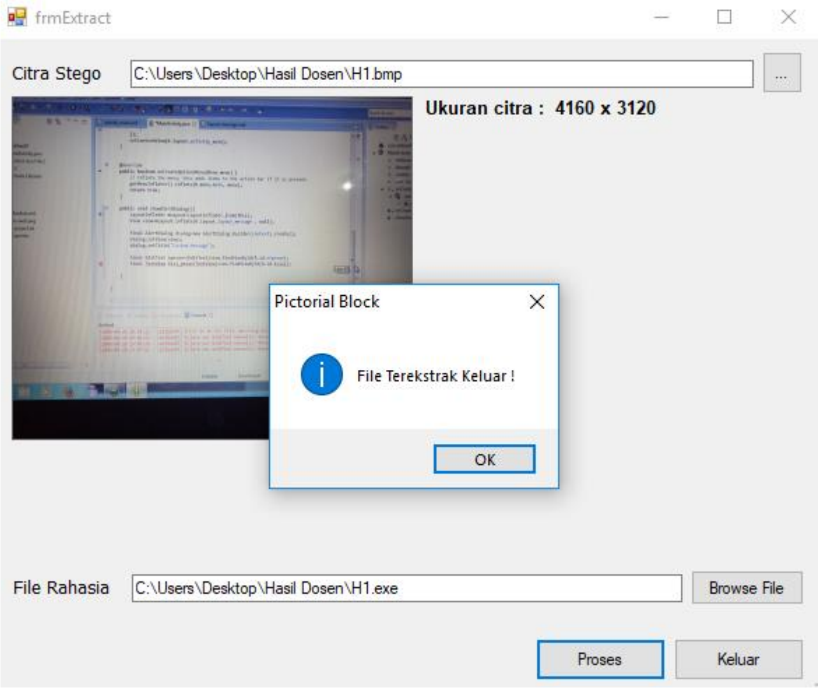


Figure 8. Image of the extraction form

Select the desired image file. After that, click the ‘Open’ button to open the image. After the image selestion process, the extraction form will look like the image below:



frmExtract

Citra Stego: C:\Users\Desktop\Hasil Dosen\H1.bmp

Ukuran citra : 4160 x 3120

Pictorial Block

File Terekstrak Keluar !

File Rahasia: C:\Users\Desktop\Hasil Dosen\H1.exe

Figure 9. Image of the original file insertion form display

3.2 Discussion

The implementation stage of an information system is the stage where the system that has been designed, explains the making of the system in accordance with the previous analysis and design. After the implementation stage is carried out, a system test is needed to prove that the application can run as expected.

The five modulus steganography method can hide the presence of secret information in a digital image by hiding the secret data bits into the color of each pixel of the digital image. This application of hiding file with the five modulus steganography method also provides a testing section on the software that can be carried out to test the level of toughness of the five modulus steganography algorithm against noise or attacks. Based on the result of tests carried out on the software, information can be obtained that the five modulus method is able to withstand attacks using basic image processing operation.

Finally, the file hiding application using the five modulus steganography method can also perform comparisons by calculating the mean squared errors (MSE) and peak signal to noise ratio (PSNR) values between the original image and the stego image along with the stego image that has been added noise and the stego image that has been added. Pixels have been removed

4. Conclusion

After completing the creation of this software, the author can draw several conclusions as follows. The application is designed to hide and display files back into a digital image using the five modulus method. The application can test the five modulus steganography algorithm so that it can know the level of thougness of the five modulus steganography algorithm against noise of attacks. The application can test the result of the comprarison of mean squared error (MSE) and peak signal to noise ratio (PSNR) between the original image and the stego image along with the stego image that has added noise and the stego image that has removed the pixels.The application can display the MSE and PNSR values on the original image and stego image by accessing the comparison form

Reference

1. Ardhianto, E., Hadikurniawati, W., dan Budarso, Z., (2013), Implementation of image subtracting method and regionprops method to detect number of RGB colored objects in video file, Journal of information technology DYNAMIC Volume 18, No. 2, 91-100.
2. Capah, S. N. A., Nasution, S. D., & Hondro, R. K., (2018), Application of the median filter method for reduction, Journal of informatics pelita, 17, 20–23.
3. Cun-Cun, (2014), Steganography application program design on media audio files with the direct sequence spread spectrum method, BINUS Jakarta
4. Erin Yuni Reva, Boko Susilo, Endina Putri Purwandari, (2016), Watermark application in digital image using a combination of discrete cosine transform, Discrete wavelet transfor and singular value decomposition methods,
5. Jalaluddin & Melita, (2012), Digital image processing.
6. Junaidi, (2013), Audio steganography (WAV) using the LSB metode method. *CCIT Journal*, *9*(2), 214-224.
7. Munir, R., (2014), Introduction to image processing, PT. Elex Media Komputindo, Jakarta
8. Nafi'iyah, N., (2015), Kohonen algorithm in converting graylevel image into binary images. JITIKA Vol. 9, No.2, 49-55.
9. Nurcahyani dan Saptono, (2016), Rice quality identification with digital image, 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.
10. Nurul Fuad, Melita, Yuliana, (2012), “Comprative analysis of the low-pass filter method with the median filter for aptimizing digital image quality”, Magister Teknologi Informasi. Institut Saint Terapan & Teknologi Surabaya
11. Priyanto, R., (2016), Can directly visual basic .Net 2008, C.V. Andi Offset, Yogyakarta.
12. Sadeli, M., (2016), Visual Basic.net 2008, Maxikom.
13. Sembiring, Sanro, (2013), Steganography application design to insert text messages in images with the end of file method, Medan.
14. Sulistiyanti dan Kris Sivam, (2016), Design and build a meat type identification tool with digital image processing using python 2.7 and opencv based on raspberry Pi 3, Universitas Lampung.
15. Supardi, Y., (2016), Microsoft visual basic 2008 for all living, PT. Elex Media Komputindo.
16. A. S. Sihotang and P. Indrayati, “3D Image Side Sharpening Using Fourier Phase Only Synthetis Method,” *J. Info Sains Inform. dan Sains*, vol. 10, no. 2, pp. 24–29, 2020.
17. J. Sihotang, “Analysis Of Shortest Path Determination By Utilizing Breadth First Search Algorithm,” *J. Info Sains Inform. dan Sains*, vol. 10, no. 2, pp. 1–5, 2020.