IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

INSERTING SECRET MESSAGES IN IMAGES USING THE STEGANOGRAPHY METHOD

Sugiyatno[1]

Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia[1]

Abstract: The importance of the level of security on digital media needs to be a special concern, especially when the information is sent. By using encryption or steganography methods where by inserting pieces of secret information in another media object. In steganography, data hiding or data embedding is known, which is data hiding that seems very familiar with encryption. However, data hiding in steganography and encryption is very different, where encryption performs data hiding by changing the arrangement of characters in the same media. While in steganography, data hiding is done by changing or exchanging some information that does not look important in the host media of the message carrier. With the method of using 24-bit Bitmap Digital Image media as input data for secret message carrier media. And the LSB (Least Significant Bit) method is by inserting secret message bits into low-level bits that have very little effect on the digital image visually that will be seen by the observer/reader of the message. So that the goal of inserting a secret message without being suspected by the observer / reader can be proven and the reading of the secret message can be read again after being inserted into the media.

Keywords: encryption, data hiding, embedding steganography.

I. INTRODUCTION

Computer networks and the Internet have experienced rapid development (Arifin, 2011). This technology is able to connect computers, so that they communicate with each other and exchange information. The form of information exchanged can be in the form of text data, images, moving images and sound. The development of technology affects the way of communication, if in the past communicating with letters through the post office, now services such as e-mail via the internet can send messages directly to the recipient faster and more economically. However, the public network is used by users around the world. Behind the benefits of technological development, there is a negative side, including the vulnerability of data theft.

By knowing the negative impact of technological developments, especially data theft, of course we must pay special attention to data security from sending to receiving data. Techniques commonly used to secure data to be sent can use encryption or steganography techniques (Kale et al., 2022). Steganography is a method to insert pieces of secret information in another media object.

In steganography, data hiding or data embedding is known, which is data hiding that seems very familiar with encryption (Singha & Sen, 2017). However, data hiding in steganography and encryption is very different, where encryption performs data hiding by changing the arrangement of characters in the same media (Kumar, n.d.).

Whereas in steganography, data hiding is done by changing or swapping some information that does not look important in the host media of the message carrier. By dividing the input data image media in frames, this technique is expected to insert secret information into one frame maximum of 1 bit so that the changes that occur are not visible(Sarkar, n.d.).

II. RESEARCH METHODOLOGY AND LITERATURE SURVEY

In this study, the authors used the waterfall method [8] with the following stages 1). Requirements Analysis and Definition, 2). Sytem and Software Design, 3). Implementation and Unit Testing, 4). Integration and System Testing, and 5). Operation and Maintenance(*SDLC-WATERFALL MODEL*, n.d.).

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

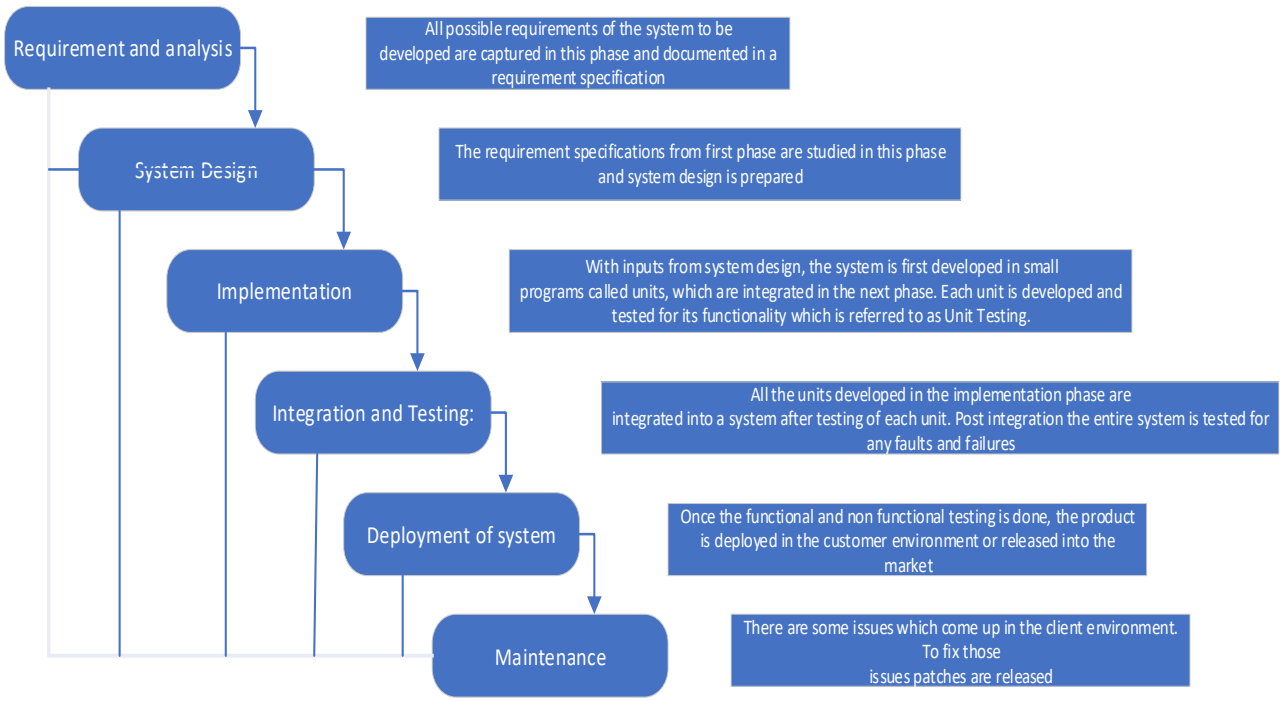

Fig 1. Research method (Dalcher, 2015)

Steganography is a technique of hiding secret data in digital media so that the existence of the secret data is unknown to people. Steganography requires two properties: the container and the secret data to be hidden. Digital steganography uses digital media as a container, such as images, sound (audio) text, and video (Harahap et al., 2019).

Steganography can be used as a way to replace one-way hash values (i.e. the user takes a variable length input and creates a static length output of type string to verify that no changes were made to the original input variable) (Akmal et al., 2023). In addition, steganography can be used as tag-notes for online images and to maintain the confidentiality of valuable information. To keep data from sabotage, thieves, or from unauthorized parties. Unfortunately, steganography can also be used for illegal reasons. For example, if someone has stolen data, they can hide the stolen archive into another archive and send it out without raising anyone's suspicion because it looks like a normal email or archive. Also, someone who likes to save pornography, or store it on a hard disk, they can hide their bad hobby through steganography. For example, if someone has stolen data, they can hide the stolen file into another file and send it out without raising anyone's suspicion because it looks like a normal email or file. In addition, someone who likes to save pornography, or save it on a hard disk, they can hide their bad hobby through steganography. Similarly, with the issue of terrorism, steganography can be used by terrorists to disguise their communications from outsiders..

Image Steganography Method

1. Least Significant Bit Insertion

The way to hide a message is by utilizing Least-Significant Bit (LSB) (Hernandes & Sartika, 2019). This method requires a condition, if compression is carried out on the stego, a lossless compression format must be used, because this method uses bits in each pixel in the image. If a lossy compression format is used, the secret message that is hidden may be lost. If a 24bit color image is used as the cover, a bit from each of the Red, Green, and Blue components can be used so that 3 bits are stored at each pixel. An 800 x 600 pixel image can be used to hide 1,440,000bits (180,000 bytes) of secret data. For example, below are 3 pixels of a 24 bit color image:
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
if it is desired to hide character A (10000001b) is generated:
(00100111 11101000 11001000)
(**00100110** 11001000 **11101000**)
(11001000 00100111 11101001)

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

It can be seen that only 3bits need to be changed to hide the A character. This change in LSB will be too small to be detected by the human eye so that the message can be effectively hidden. If an 8bit color image is used as a cover, only 1bit of each color pixel can be modified so the selection of the image must be done very carefully, because the change in LSB can cause a change in the color displayed in the image. It would be better if the image is a grayscale image because color changes will be more difficult to detect by the human eye. The message extraction process can be easily done by extracting the LSB from each pixel in the stego sequentially and writing it to the output file that will contain the message. The drawback of the LSB modification method is that it requires a relatively large "storage area". Another drawback is that the resulting stego cannot be compressed with a lossy compression format.

2. Masking dan Filtering

Masking and filtering techniques are limited to 24bit color images or grayscale images. This method is similar to watermarking, where an image is marked to hide a secret message. This can be done by modifying the luminance of some parts of the image (Kumar, n.d.).

Although this method will change the appearance of the image, it is possible to do so in such a way that the human eye does not notice the difference. Since this method uses aspects of the image that are directly visible, it is more robust to compression (especially lossy compression), cropping, and other image processing, compared to the LSB modification method.

3. Transformation

This method for hiding messages in images is done by utilizing Discrete Cosine Transformation (DCT) and Wavelet Compression (Rosal et al., 2017). DCT is used, especially in JPEG compression, to transform consecutive 8x8 pixel blocks of the image into 64 DCT coefficients. Each DCT coefficient F(u,v) of an 8x8 pixel block image f(x,y) is calculated as follows:

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * cos\frac{(2x+1)u\pi}{16} cos\frac{2y+1)v\pi}{16}\right]$$

Where when x equals 0 and C(x) = 1 when x equals 1. After the coefficients are obtained, the quantization process is carried out as follows;

Where Q(u,v) is the 64-element quantization table. For example, here is a simple algorithm to hide a message in a JPEG image:

1: WHILE (masih ada data untuk di-embed) do
2: Ambil koefisien DCT selanjutnya dari cover images (DCT)
3: IF koefisien < nilai threshold then
4: Ambil bit selanjutnya dari pesan
5: Ganti bit koefisien DCT dengan bit pesan tersebut
6: END IF
7: Masukkan DCT ke stego (invers DCT)
8: END WHILE

Although images compressed with lossy compression will arouse suspicion because LSB changes will be clearly visible..

4. Wavelet Compression

It is a data compression method that is suitable for image, audio, and video compression. The goal is to store data in the smallest possible "space" in a file, the loss of certain information is expected, this compression is an example of lossy compression (Akmal et al., 2023). Just like DCT, wavelet compression is based on the frequency domain. The advantage of wavelet compression is that it is better at representing transient regions, such as star images in the night sky. That is, elements of transient data will be represented in a smaller amount of information than what happens with other transformations, such as the DCT. The disadvantage is that wavelet compression is not good for periodic and smooth data. The method performed in wavelet compression will be explained as follows. First of all, a wavelet transform is performed which will produce coefficients according to the number of pixels in the image as follows

$$[W\psi f](a,b) = \frac{1}{\sqrt{|a|}}\sum_{-\infty}^{\infty}\psi\left(\frac{x-b}{a}f(x)dx\right)$$

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

The wavelet coefficient cjk is obtained by

$$c_{jk} = [W\psi f](2^{-j}, k2^{-j})$$

Where a = 2-j is called binary dilation or dyadic dilation, and b = k2-j is called binary position or dyadic position. Once the wavelet coefficients are obtained, they can be compressed easily because the information is statistically concentrated in a few specific coefficients. This principle is called transform coding. After that, the coefficients are quantized, and then encoded with entropy encoding and/or run length encoding.

Here is a simple algorithm for hiding messages in images using wavelet compression:
Input: pesan, cover image
Output: stego
1: WHILE (masih ada data untuk di-embed) do
2: ambil koefisien wavelet selanjutnya dari cover image (wavelet transform)
3: IF koefisien < nilai threshold then
4: ambil bit selanjutnya dari pesan
5: ganti koefisien wavelet dengan bit pesan tersebut dan kompresi
6: END IF
7: masukkan DCT ke stego (invers wavelet transform)
8: END WHILE

The message extraction process uses the transformation method by transforming the stego to obtain the image transformation coefficient. Select the coefficient whose value is smaller than the threshold value. Extract the data bits corresponding to these coefficients and write them to the output file that will contain the message

Flowchart

The flowchart shown below is a flowchart of the standard LSB method for inserting secret data into other data.

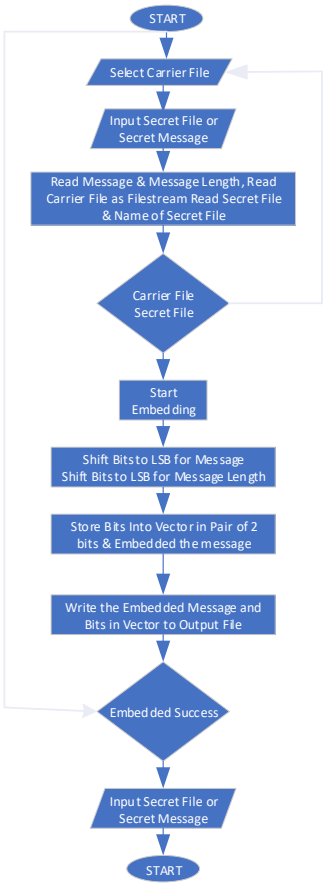

Fig. 2 LSB Method Diagram (Source Author 2024)

III. RESULT AND DISCUSSION

To form the unhiding stage, a useful function is needed to retrieve the data that has been inserted in the embedding process above in one piece..

Implementation of Retrieving Stage

To form the unhiding stage, a useful function is needed to retrieve the data that has been inserted in the embedding process above in one piece.

1. DecodeMessage function to retrieve the contents of the message inserted into a carrier file and displayed in a text box. The program language of decodeMessage insert message in a file can be written as follows:

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

```
1: //Sisipkan Pesan Dalam File
2: for(i=0; i<messageSize; i++)
3: byt=(byte) message.charAt(i);
4: byt&=0x7F;
5: for(j=6; j>=0; j-=2)
6: by=byt;
7: by=j;
8: by&=0x03;
9: byb=in.readByte(); //tulis ke output file
10: byb&=0xFC;
11: bybl=by;
12: out.writeByte(byb);
```

The program language of decodeMessage read message size can be written as follows:

```
1: //Baca Ukuran Pesan
2: for(i=14; i>=0; 1-=2)
3: by=in.readByte();
4: temp=(short)by;
5: temp&=0x0003;
6: temp=i;
7: messageSizel=temp;
8: //Baca Isi Pesan Yang Disampaikan
9: for(i=0; i<messageSize; i++)
10: by=0;
11: for(j=6; j>=0; j-=2)
12: byt=in.readByte();
13: byt&=0x03;
14: byt=j;
15: byl=byt;
16: mesg[i[=(char)(((char)by)&0x007F);
```

1. decodeFile serves to retrieve the file and the contents of the secret message file inserted into a carrier file and written to the hard disk. The decodeFile program can be written as follows:

```
1: //Baca isi file pesan rahasia
2: fileName=new char[messageSize];
3: for(i=0; i<messageSize; i++)
4: by=0;
5: for(j=6; j>=0; j-=2)
6: byt=in.readbyte();
7: byt&=0x03;
8: byt=j;
9: byl=byt;
10: by&=0x7F;
11: filrName[i]=(char) by;
```

2. Main Menu Form

This Main Menu Form is a form that provides an application program menu that can be accessed by users who have authority and have logged in..

Fig 3. Main Menu Form (Source Author 2024)

3. Write Message Form

This Write Message form will appear if the user presses the Write Message menu on the main menu form. This form functions to insert a secret message into the Image file

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

Fig 4 Compose Message Form (Source Author 2024)

4. Read Message Form

This Read Message form will appear if the user presses the Read Message button on the Main Menu. This Read Message form serves to separate the secret message from the image file as a carrier file. So that the secret message can be displayed and then can be read by the user

Fig 5. Read Message Form (Source Author 2024)

5. Testing and Analysis

Tests are expected to provide answers to the truth of various kinds of limitations, theories, or analysis that researchers want to do. Concealment of secret data into a digital image will change the quality of the image. The criteria that must be considered in data hiding are:

1. Fidelity. The quality of the container image does not change much. After the addition of secret data, the steganographic image is still visible. Observers do not know that the image contains secret data.
2. Robustness. The hidden data must be robust to various manipulation operations performed on the container image, such as changing contrast, sharpening, compression, rotation, image magnification, cropping, encryption and so on. If these image processing operations are performed on the container image, then the hidden data should not be damaged (still valid if extracted again).
3. Recovery. The hidden data must be able to be revealed again (reval). Since the purpose of steganography is data hiding, at any time the secret data in the container image must be recoverable for further use..

6. Retrieving Stage

In this stage, testing is only done within the scope of the data return process. Some inputs are required to start the data retrieval process. The required inputs include the following::

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

1. Retrieval of Carier Data

Retrieval of secret message carrier data can be done using the File Open menu. After the image is selected, we just need to press the Read Message button to separate the image with the secret message.

Fig 6 Carrier File to be Read (Source Author 2024)

2. Output Result of Retrieving Stage

To get the output of the retrieving stage, is to select the Read Message button. After selecting the Read Message button, the process will separate the message from the image.

Fig 7 Output Result Retrieve (Source Author 2024)

7. Results and Analysis

This section will discuss the analysis of the output results generated by the Application Program made in this thesis. The criteria that will be used to analyze the output results of the application program made. include:

Fidelity.	Robustness.	Recovery.
The output of the steganography application program will be analyzed from the quality of the container image after being filled with the secret message. A good result is that the container image after being filled by the secret message does not change much against the container image that has not been filled with the secret message. Or in other words, after the addition of the secret	The output of the steganography application will be analyzed for robustness against manipulation operations on the container image. Manipulation operations performed on the container image, such as changing contrast, sharpening, compression, rotation, image magnification, cropping,	The output of the steganography application program will be analyzed from the ability to reveal the secret message inserted in the container image. So that the secret message can be retrieved for other purposes..

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal & Refereed journal ⁜ Vol. 12, Issue 12, December 2023

DOI: 10.17148/IJARCCE.2023.121217

data, the steganographic image is still visible. Observers do not know that the image contains secret data.

The results of this analysis can be seen

in the image results below

Fig 8. File Carrier

Fig 9. Files Containing Messages

With contains a secret message that reads:

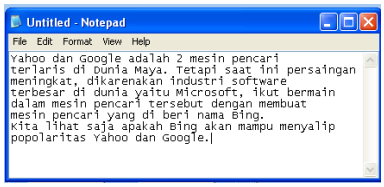

Fig 9. Message Inserted in the Carrier File above

In addition, it can also be seen in the picture below:

Fig 10 Uninserted Carrier File Message

It contains the following secret message:

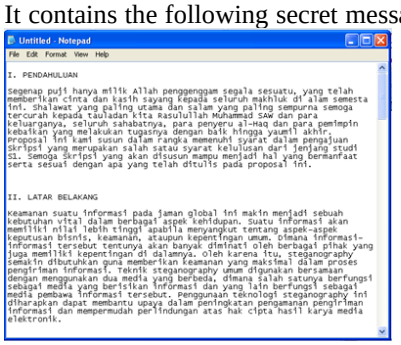

Figure 11. Message inserted in the Carrier File above

encryption and so on. The results are good if the container image of the image processing operation of the hidden data is not damaged. Experimental results on the container image using Adobe Photoshop.

Table 1 Robustness Test with Brightness Manipulation Operation

Nama File	Dimensi	Operasi Manipulasi	
fotoku rahasia bright 5	604x453	Brightness +5	Tidak Bis
fotoku rahasia bright 10	604x453	Brightness +10	Bisa Diba
fotoku rahasia bright 15	604x453	Brightness +15	Tidak Bis
fotoku rahasia bright 20	604x453	Brightness +20	Bisa Diba
fotoku rahasia bright 25	604x453	Brightness +25	Tidak Bis
fotoku rahasia bright-5	604x453	Brightness -5	Tidak Bis
fotoku rahasia bright -10	604x453	Brightness -10	Bisa Diba
fotoku rahasia bright -15	604x453	Brightness -15	Tidak Bis
fotoku rahasia bright -20	604x453	Brightness -20	Bisa Diba

Table 2 Robustness Test with Contrast Manipulation Operation

Nama File	Dimensi	Operasi Manipulasi	
y&g1 contrast 5	98x132	Contrast +5	Tidak B
y&g1 contrast 10	98x132	Contrast +10	Tidak B
y&g1 contrast 15	98x132	Contrast +15	Tidak B
y&g1 contrast 20	98x132	Contrast +20	Tidak B
y&g1 contrast 25	98x132	Contrast +25	Tidak B
y&g1 contrast -5	98x132	Contrast +5	Bisa Di
y&g1 contrast -10	98x132	Contrast +10	Tidak B
y&g1 contrast -15	98x132	Contrast +15	Tidak B
y&g1 contrast -20	98x132	Contrast +20	Bisa Di

Table 3 Robustness Test with Rotate Manipulation Operation

Nama File	Dimensi	Operasi Manipulasi	
fotoku rahasia 90 cw	604x453	Rotate 90 Clockwise	Tidak B
fotoku rahasia 180	604x453	Rotate 180	Tidak B
y&g1 90 cw	98x132	Rotate 90 Clockwise	Tidak B
y&g1 180	98x132	Rotate 180	Tidak B

The results of the analysis of the tests conducted with several container image files with several manipulation operations stated that the container image was unable to survive the manipulation operations performed on the container image. So the result is that most secret messages cannot be read in full after the container image has undergone manipulation operations. This is caused by the program being unable to read the fleck at the beginning of the container image which indicates that the container image contains a secret message. It can also be concluded that the application program built is still not perfect.

Fig.12 Container Image Containing Secret Message.

Figure 4.13 shows the container image being opened using this application

Figure 4.13 Reading the Secret Message from the Container Image..

So that the secret message is obtained which is inserted in the container image. The secret message read from the container image can be seen below::

Figure 4.14 Secret Message Reading Results

DOI: 10.17148/IJARCCE.2023.121217

CONCLUSION

The resulting output file experiences low noise because a block is only changed by a maximum of 1 bit. However, the noise that occurs will be more obvious if the inserted message is larger. The input file (Image file) and the output file have exactly the same number of bits, which means that the message insertion does not affect the amount of input and output data. So that the quality of the container image does not change much, meaning that the observer is not able to distinguish the results of the container image that does not contain a secret message and the container image that contains a secret message. The quality of the image file is determined by the size of the secret message file used and the size of the carrier file. The larger the size of the secret message file, the greater the noise generated. And the container image is not resistant to changes in the various manipulation operations performed on the container image, based on the research conducted.

ACKNOWLEDGMENT

The authors thank to Universitas Bhayangkara Jakarta Raya in supporting this research as internal research grant. Also, for the reviewers who have given the insightful comments.

REFERENCES

[1]. Akmal, R. A., Furqan, Mhd. F., & Kurniawan R, R. (2023). Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital. G-Tech: Jurnal Teknologi Terapan, 7(2), 543–553. https://doi.org/10.33379/gtech.v7i2.2300

[2]. Arifin, H. (2011). Kitab Suci Jaringan Komputer dan Koneksi Internet. Mediakom.

[3]. Dalcher, D. (2015). Going Beyond The Waterfall: Managing Scope Effectively Across the Project Life Cycle. In Project Management Journal (Vol. 46, Issue 1). https://doi.org/10.1002/pmj.21475

[4]. Harahap, R. H., Hasibuan, N. A., & Saputra, I. (2019). PENERAPAN METODE MODULUS FUNCTION (MF) UNTUK PENYISIPAN PESAN PADA CITRA DIGITAL. KOMIK (Konferensi Nasional Teknologi Informasi Dan Komputer), 3(1). https://doi.org/10.30865/komik.v3i1.1695

[5]. Kale, H., Keshattiwar, M., Patil, M., Shinde, A., & Mahale, P. P. (2022). MESSAGE TRANSFER USING STEGANOGRAPHY. International Research Journal of Engineering and Technology. www.irjet.net

[6]. Kumar, M. P. M. (n.d.). A reversible high embedding capacity data hiding technique for hiding secret data in images. http://sites.google.com/site/ijcsis/

[7]. Sarkar, T. (n.d.). Reversible and Irreversible Data Hiding Technique.

[8]. SDLC-WATERFALL MODEL. (n.d.). http://www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm

[9]. Singha, S., & Sen, M. (2017). Encoding algorithm using bit level encryption and decryption technique. 2016 International Conference on Computer, Electrical and Communication Engineering, ICCECE 2016, 160(2), 23–26. https://doi.org/10.1109/ICCECE.2016.8009584

BIOGRAPHY

Sugiyatno has published some papers about Network and Security. She is now a lecturer of Informatics department in Universitas Bhayangkara Jakarta Raya.