# An Implementation of MMS Steganography With The LSB Method

Dian Ahkam Sani[1]*, Mohammad Zoqi Sarwani[2], Muhamad Agus Setiawan[3]
[1,2,3]Universitas Merdeka Pasuruan, Pasuruan, 67129, Indonesia
[1]dianahkam@unmerpas.ac.id*; [2]zoqi.sarwani@unmerpas.ac.id; [3]Akhmadagussetia@gmail.com
*Corresponding Author

**ABSTRACT**

Around the world, the internet (interconnection network) has developed into one of the most popular data communication media. With a variety of illegal information retrieval techniques that are developing, many people are trying to access information that is not their right. Various techniques to protect confidential information from unauthorized persons have been carried out to secure important data. Steganography is a science and art for writing hidden messages so that no other party knows the existence of the message. The three results of tests conducted by the LSB method can be used to hide messages into images. The first test was successful by writing a message that less than 31 characters stored in the picture, the second succeeded in writing a message equal to 31 characters stored in the picture, the third failed to write a message of more than 31 characters stored in the picture.

Keywords: *Steganography*, *mobile*, *Least Significant Bit* (LSB).

| Article History | | |
|---|---|---|
| Received : June, 05th 2020 | Revised : June, 23rd 2020 | Accepted : June, 30th 2020 |

## I. INTRODUCTION

Security is an important thing that must be done to maintain very important information in technological development. Safety is a condition free from danger, where this term can be used concerning crime, accidents, and others. Security can not be described if not in a situation of fear. In the context of information and communication technology, security is one of the important aspects that need to be considered.

The application of steganography is not only used for sending confidential data. However, steganography can also be used to secure personal data stored on data storage media, such as hard disk, flash disk, and CD (Compact Disk). Similar to sending confidential data, the application of steganography also aims to protect data from other people's disturbances. The purpose of the disturbance can be in the form of reading, editing, and deleting data [1]. In this study, the researcher makes analysis and designs a steganographic application to be the solution to the security problem. By using this technique, we can hide information data in the Multimedia Message Sevice (MMS) or digital media that we have.

Multimedia Message Service (MMS) is a service provided by cellular phones to its users to communicate through sending short messages containing text and multimedia. MMS is very popular, aside from its low cost, the message sent can be received by the recipient well and quickly. Communication via MMS is not a point-to-point communication, but messages sent through MMS do not reach the destination directly, but first to the server on the MMS network and then delivered to the recipient of the message. On the MMS network, message security is very much threatened to be read by others. Security is needed so that the contents of messages sent via MMS are maintained and can only be read by those who have the right to read them. The solution offered is securing messages on MMS with Steganography [2].

The first study conducted by [3] entitled "Analysis and design of Steganography applications in digital images using the LSB method". Research conducted testing and testing analysis of this StegoImage application that aims to determine the level of success of the application in achieving the desired results and objectives. From the results of system testing conducted, the StegoImage application successfully implemented a steganography technique that uses the LSB algorithm to secure the message that a file can be inserted into an image file and retrieved from the image file.

The third study was conducted by [2] entitled "Implementation of Steganography Schemes with the Select Least Significant Bits (SSLB) Method on Encrypted Messages for MMS Delivery" The system built is a steganography system that can be an alternative to secure messages in the Multimedia Message Service (MMS) facility. The process of inserting messages on the system: insert original messages, insert compressed messages, insert encrypted messages, insert compressed and encrypted messages.

The fifth study was conducted by [4] entitled "Text Message Steganography Technique Using the Least Significant Bit Method and the Linear Congruential Generator Algorithm". The Least Significant Bit (LSB) method is used to insert messages into the 24-bit color image insertion (cover image) media on each of the two most significant bits of each color image (Red, Green, and Blue) so that each pixel of the color image can hold 6-bit text message. In determining the location of the pixel of the color image that the message will insert, a pseudo-random number generator, the Linear Congruential Generator (LCG) is used.

DOI: 10.25139/ijair.v2i1.2653

The experimental results show the calculation of Peak Signal to Noise ratio (PSNR) for each image that is inserted with the maximum message size (stegoimage), resulting in values above 40 dB. PSNR calculation is used to determine the comparison of image quality before and after the message is inserted.

Therefore, an application that can secure messages by using the above method will be designed so that the hidden information data can be saved into digital media that we have.

## II. METHOD

Inserting messages into covertext media is called encoding in Fig.1, while message extraction from stegotext is called decoding. Both of these processes may require a secret key (called stegokey) so that only authorized parties can insert messages and extract messages [11].

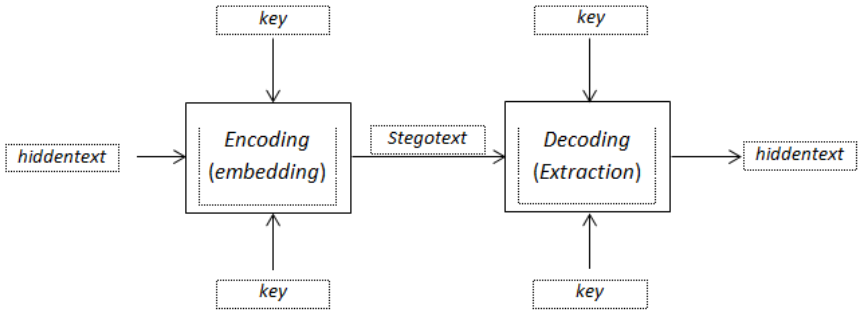



Fig. 1. Message insertion and extraction diagram

### A. *Steganography*

Data insertion techniques into covertex can be done in two kinds of domains:

1. Spatial (time) domain (spatial / time domain), this technique directly modifies the byte value of the covertext (the byte value can represent the intensity/color of the pixel or amplitude). Examples of methods classified as spatial domain techniques are the LSB method.
2. The domain of transform (transform domain) This technique directly modifies the transformation of the signal frequency. Examples of methods that fall into the frequency domain technique are spread spectrum [10].

### B. *Least Significant Bit* (LSB)

In the arrangement of bits in a byte (1 byte = 8 bits), there are the most significant bits (the most significant bit or MSB) and the least significant bits (the least significant bit or LSB). They are seen in Fig. 2, which illustrates an example of a binary value of 8 bits.


Fig. 2. most significant bit (MSB) dan least significant bit (LSB)

The right bit to replace is the LSB bit because the change only changes the byte value, one higher or one lower than the previous value. Suppose the byte represents red, then changing one LSB bit does not change the red color significantly, and the human eye cannot distinguish that very small change. Suppose there is an image with the pixel value as follows Fig.3.

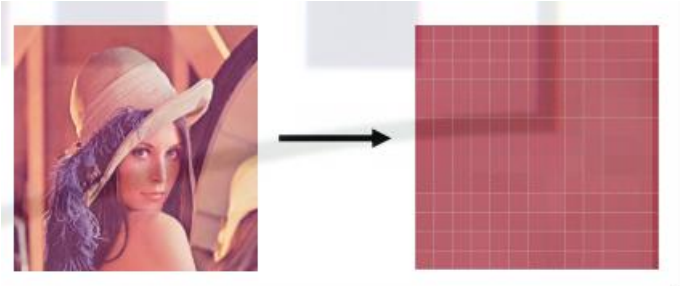


Fig. 3. Process Image File into Collection of Pixels

For example, we take the values of several pixels in the image above, where the pixel value is converted first into binary to insert a character “R” = 01010010, where 01010010 is the binary code for 82 which is the ASCII code “R” character.

DOI: 10.25139/ijair.v2i1.2653

(00100111 11101001 11001000)
(00100111 1100100011101001)
(11001000 0010011111101001)

*Image segment before inserting

(00100110 1110100111001000)
(00100111 1100100011101000)
(11001001 0010011011101001)

*Image segment after inserting "R"

Seen above is the change in the sample image data segment contained in the rightmost bits, after inserting 01010010 as hidden data, that the bit change only occurs on the far right side of the 8 bits that exist. Steganography with the LSB method is also only able to store information with a very limited size. For example, a 24-bit image (R = 8-bit, G = 8-bit, B = 8-bit) is used as a container to store 100-bit data, if each color component (RGB) is used one pixel to store confidential information. Therefore, each pixel is stored 3 bits of information, so that at least a container image of 34 pixels or equal to 34 x 3 x 8 = 816 bits (8 times) is needed. So a 24-bit image is used to store confidential information that can only hold a maximum size of 1/8 of the size of the container image [3].

### *C. Flowchart Use of Steganography Applications*

The flow of user application illustrated in Fig.4. Fig.4 explains the flow of the program using a mobile-based steganography application. It explains what information must be input to begin the process of extracting secret messages. The information must be complete; if incomplete, an error will appear to remind it. After all of the information is complete, the steganography program will use the LSB algorithm to retrieve the message bytes from the LSB image file so that the secret message can be read again. After the secret message can be read, the message extraction process has finished.

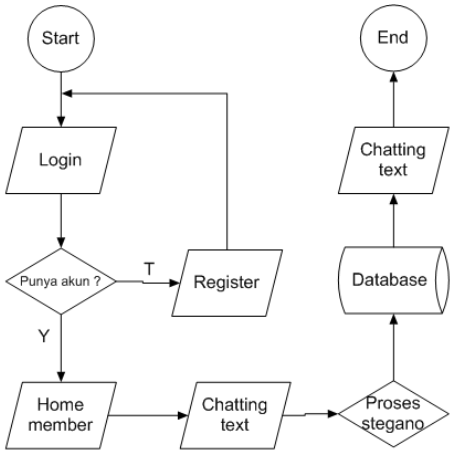



Fig. 4. Message Extraction Process Flowchart

### *D. Flowchart Message Extraction Process.*

In Fig.5 at this stage, or hidden files are separated from the storage media using steganography techniques with the LSB method, so it becomes a message file that can be read.

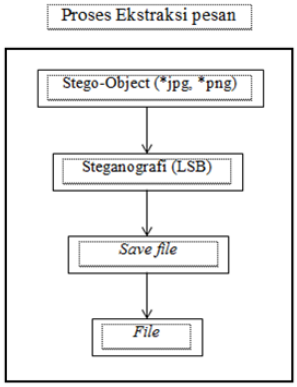



Fig. 5. *Message Extraction Process Flowchart*

DOI: 10.25139/ijair.v2i1.2653

## III. RESULT AND DISCUSSION

This chapter discusses a series of trials and evaluations of the applications. This test includes a system functional test consisting of character length testing and character type testing. The first test is a functional system that consists of several tests. Among them from each system test are in the following table I.

TABLE I
LONG TESTING CHARACTERS

| Procedure | Result | Information |
|---|---|---|
| Sending Messages Less Than 31 Characters | Application Can Receive and Extract hidden messages | Success |
| Sending a Message Equal To 31 Characters | Application Can Receive and Extract hidden messages | Success |
| Sending Message More Than 31 Characters | The application cannot accept and cannot extract hidden messages | Not Successful |

There are three conditions when testing when a user receives a message with a character length of less than 31, equal to 31, and more than 31 characters in table II. The result is that the message can be sent and encrypted if the character length is less than 31, and the character length is 31. While for the character length, more than 31 messages can still be sent, but the message cannot be extracted or failed to encode the message.

TABLE II
LONG TESTING CHARACTERS

| Procedure | Result | Information |
|---|---|---|
| Sending Message in the Form of Letters | Applications Can Receive and Encode hidden messages | Success |
| Send messages in the form of numbers | Applications Can Receive and Encode hidden messages | Success |
| Send a Message in the Form of a Symbol | Applications Can Receive and Encode hidden messages | Not Successful |

There are three conditions as seen in Table II, when testing with the procedure of sending messages in the form of letters, sending messages in the form of numbers and sending messages in the form of symbols, obtained the results that when users can send messages in the form of letters, numbers, and symbols and successfully decrypted. Either send only letter characters or letters with numbers or symbols together. Encoding testing on encrypted messages is performed on mobile android version 8.1.0 (Oreo) with a screen size of 1440 x 720 pixels or 5.99 inches shown in Fig.6 to the following image

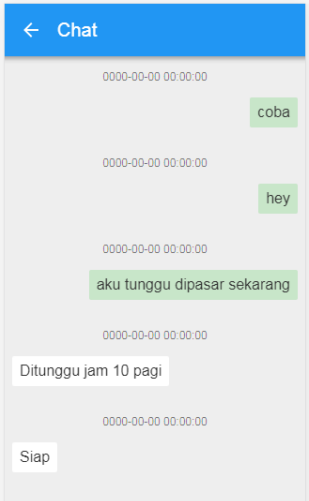
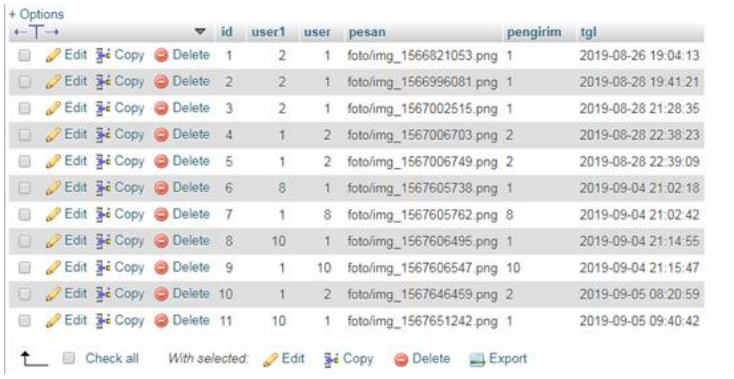



Fig. 1. Display Test Encrypted Message

Testing the chat_member table in the database above in Fig.7, it appears in the incoming message column in the form of an encrypted image. The image is beautiful, which will be extracted or decrypted in the computerization process of the application. And what appears will be the text on the chat page where the text has no more than 31 characters. Based on the application trials that have been done, the results show that the application can be installed and can be run later on testing application features such as registration, login, contact list, sending messages, displaying messages sent, and logging out to function properly and as expected.

DOI: 10.25139/ijair.v2i1.2653



+ Options

| | id | user1 | user | pesan | pengirim | tgl |
|---|---|---|---|---|---|---|
| Edit Copy Delete | 1 | 2 | 1 | foto/img_1566821053.png | 1 | 2019-08-26 19:04:13 |
| Edit Copy Delete | 2 | 2 | 1 | foto/img_1566996081.png | 1 | 2019-08-28 19:41:21 |
| Edit Copy Delete | 3 | 2 | 1 | foto/img_1567002515.png | 1 | 2019-08-28 21:28:35 |
| Edit Copy Delete | 4 | 1 | 2 | foto/img_1567006703.png | 2 | 2019-08-28 22:38:23 |
| Edit Copy Delete | 5 | 1 | 2 | foto/img_1567006749.png | 2 | 2019-08-28 22:39:09 |
| Edit Copy Delete | 6 | 8 | 1 | foto/img_1567605738.png | 1 | 2019-09-04 21:02:18 |
| Edit Copy Delete | 7 | 1 | 8 | foto/img_1567605762.png | 8 | 2019-09-04 21:02:42 |
| Edit Copy Delete | 8 | 10 | 1 | foto/img_1567606495.png | 1 | 2019-09-04 21:14:55 |
| Edit Copy Delete | 9 | 1 | 10 | foto/img_1567606547.png | 10 | 2019-09-04 21:15:47 |
| Edit Copy Delete | 10 | 1 | 2 | foto/img_1567646459.png | 2 | 2019-09-05 08:20:59 |
| Edit Copy Delete | 11 | 10 | 1 | foto/img_1567651242.png | 1 | 2019-09-05 09:40:42 |

Check all With selected: Edit Copy Delete Export

Fig. 7. Display Test Message on the database

## IV. CONCLUSION

Based on the discussion and testing that has been done, it is concluded that the implementation of steganography applications in the form of text chat successfully implements steganographic techniques—the LSB algorithm in securing messages sent to the database so it cannot be read. The message sent to the database is in the form of an image format *png.

## REFERENCES

[1] Adiria, "Analisis dan perancangan aplikasi steganografi pada citra digital menggunakan metode LSB (Least Significant Bit)," pp. 1–264, 2010.
[2] D. Darwis, "Implementasi Teknik Steganografi Least Significant Bit (LSB) dan Kompresi untuk Pengamanan Data Pengiriman Surat Elektronik," vol. 10, no. 2, pp. 1–7, 2016.
[3] Ainurrizan, "Implementasi steganografi pada file image menggunakan teknik spread spectrum skripsi," 2014.
[4] E. H. Nurkifli and E. Winarko, "Implementasi Skema Steganografi Dengan Metode Select Least Significant Bits (SLSB) Pada Pesan Terenkripsi Untuk Pengiriman MMS," vol. 2012, no. SemnasIF, pp. 9–16, 2012.
[5] S. Syam and A. S. Wahyuningsih, "Pengolahan citra dan steganografi dengan metode LSB," no. April, pp. 31–35, 2014.
[6] E. R. Djuwitaningrum and M. Apriyani, "Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit dan Algoritma Linear Congruential Generator (Text Message Steganography Using Least Significant Bit Method and Linear Congruential Generator Algorithm)," *Endang*, vol. IV, no. November, pp. 79–85, 2016.
[7] L. Diyo and W. Yustanti, "RANCANG BANGUN E – VOTING BERBASIS WEBSITE DI UNIVERSITAS NEGERI SURABAYA," *Ranc. BANGUN E – VOTING Berbas. WEBSITE DI Univ. NEGERI SURABAYA*, vol. 6, pp. 72–81, 2016.
[8] D. Hamdani, "Security network - encrypt - decrypt," *Security network encrypt - decrypt*, 2013.
[9] A. A. Putra, *Buku Praktis Belajar Pemrograman Android*. 2012.
[10] Munir, Rinaldi. (2004). Pengolahan Citra Digital dengan Pendekatan Algoritmik. Bandung : Informatika.
[11] Munir, Rinaldi. (2006). Kriptografi. Bandung: Informatika.

DOI: 10.25139/ijair.v2i1.2653