© 2018 IJSRST | Volume 4 | Issue 11 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : https://doi.org/10.32628/IJSRST18401112

Implementation of LSB Steganography on Embedding Messages in Digital Image

Randi Rian Putra[1], Meika Sari[2], Andysah Putera Utama Siahaan[1], Muhammad Iqbal[1]
[1]Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
[2]Degree Student, Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

ABSTRACT

The development of information technology today, makes it easier for perpetrators of computer crime, by abusing technology to support its activities, where their activities significantly disrupt someone's privacy. In this paper the insertion of text messages with the least significant bit method. Therefore the administrator needs a system or application that is safe so that it can make it difficult for computer criminals to carry out their activities, and help technology users regarding securing the accessed data bit, which is expected to increase the security of a secret text message. To increase the security of the data to be stored, the data stored is embedded in other media. Least Significant Bit is one method that can be used to hide confidential data on images or media. With this method, the confidentiality of information will be more secure.

Keywords : LSB, Steganography, Embedding, Stego-Image, Vessel Image, Hiding, Security

I. INTRODUCTION

Steganography is a technique of embedding messages in other media so that the existence of the secret message cannot be known [1]–[3]. In contrast to cryptography which conceals the meaning of the message but the existence of the message persists, steganography conceals by covering or hiding messages [4]. Steganography in the world of digitalization has been widely applied to send messages or confidential information. Not only that steganography is also often used for archiving activities where digital data is hidden into other digital files that are more general so as not to attract the attention of those who want to steal information [5]. Steganography along with its development has given birth to a variety of different techniques and methods. In digital multimedia files such as digital images, the most commonly used steganography method is the Least Significant Bit (LSB) method. LSB method is one method of steganography in spatial domain techniques [6]. The LSB method changes the value of the last bit color component with the message bit to be hidden to produce an image that is similar to the original. This method can be developed in hiding secret messages [7].

II. THEORIES

2.1 Digital Image

In general, digital images are 2-dimensional images compiled by digital data in the form of an array containing real or complex values represented by a specific row of bits. An image can be defined as a function of f (x, y) sized M lines and N columns, with x and y are spatial coordinates, and amplitude f at the coordinate point (x, y) is called the intensity or gray level of the image at that point. Digital images are formed by a collection of points called pixels (picture element). Each pixel is described as a small box. Each

pixel has position coordinates. The coordinate system used to declare digital images is shown in the following figure.

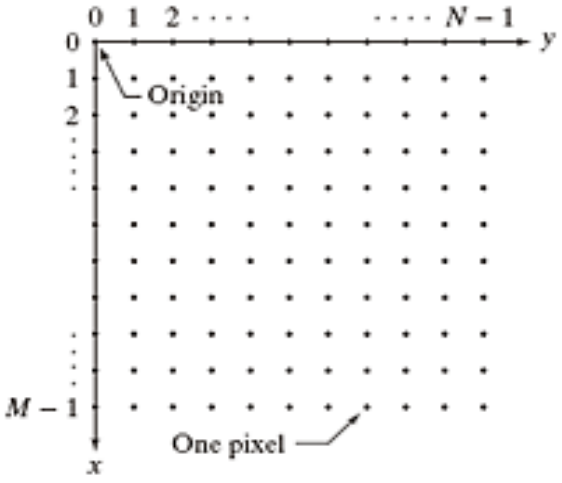

Figure 1. Digital Image Illustration

Figure 1 describes the coordinate system that follows the scanning principle on a standard TV screen. A pixel has coordinates (x, y) in this case:

- x states the position of the column;
- y represents the row position;
- the upper-left corner pixel has coordinates (0, 0) and the pixels in the lower-right corner have coordinates (N-1, M-1).

There are many ways to store digital images in memory. The storage method determines the type of digital image that is formed. The digital image formats that are widely used are Binary Imagery, Grayscale Image, and Color Image.

2.2 Digital Image Processing

Image processing is a discipline that studies things related to improving image quality (contrast enhancement, color transformation, image restoration), image transformation (rotation, translation, scale, geometric transformation), selection of feature images that optimal for the purpose of analysis, the process of withdrawing information or description of objects or the introduction of objects contained in the image, do compression or reduction of data for the purpose of data storage, data transmission, and data processing time. Input from image processing is an image, while the output is the image produced by processing.

Digital image processing is widely used by various fields ranging from security, health, education and other fields. The following are some of the objectives of digital image processing activities.

- Improve image quality regarding radiometric aspects (contrast enhancement, color transformation, image restoration) and from geometric aspects (rotation, translation, scale, geometric transformation).
- Conducting the process of withdrawing information or description of objects or the introduction of objects contained in the image.
- Perform data compression or reduction for data storage, data transmission, and data processing time.

2.3 Steganography

Steganography is the science and art of invisible communication. Steganography is a word derived from Greek words, such as "stegos" which means "cover-up" and "grafia" which means writing which is defined with "writing covered." Steganography is different from cryptography where cryptography aims to keep the content or information from the message confidential while steganography aims to keep the existence of the message confidential [8]–[10]. The original message is hidden on a carrier media where changes that occur on the carrier media are not visible to others. One of the advantages of steganography is where the message is transmitted or sent without being known by other parties which for the other party is seen as the carrier media [11]–[13].

All approaches in the field of steganography have a similarity, namely hiding secret messages on physical objects that are sent. The following figure is the

process of steganography where the image of the carrier is passed into the planting function which will then produce an image that contains a secret message. The steganography process is also usually able to use keys to increase security on hidden messages, which steganography process will be equipped with cryptographic processes as an additional process [14].

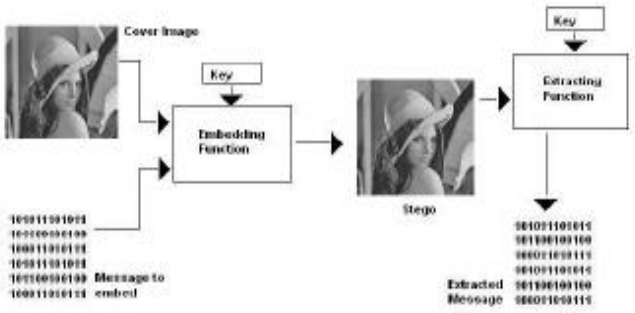

Figure 2. Steganography procedure

2.4 Least Significant Bit

Least Significant Bit (LSB) is a technique commonly used in the field of steganography. The LSB method works by replacing the least significant bit with the bits of information to be planted [15]. The following is an illustration of the process of planting information using LSB steganography on digital image media.

Embedding:

Pixel :
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Char : A
Decimal : 65
Bit : 01000001

Result :
(00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

Extracting:
Result :

(00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

Bit Extraction : 0 1 0 0 0 0 1 1
Decimal : 65
Char : A

The process of embedding or planting is done by replacing LSB bits in the image with bits of information character. The bits underlined as seen in the embedding process above are replacement bits obtained from the information character. The extraction process is done by taking LSB bits from each pixel and then reassembling them into information characters.

III. METHODOLOGY

3.1 LSB Analysis

How the LSB Method Works The working concept of the Least Significant Bit (LSB) method in inserting messages into image media is to modify the bits of each pixel of the image that becomes the cover (message container image). The last bit (least) of each pixel will be replaced with the bits of the message that will be hidden. The process of disclosure or retrieval of messages from within site is carried out by taking the pixel bits of the resulting image that are in the final position, then converted into characters. The main process in the LSB method is the embedding and extraction process. Embedding Process Based on LSB. The process of embedding a message on a cover that is used as a container is by selecting the cover image, reading the decimal cover value, converting it into the binary number, then entering the message, then the number of messages used as a key is combined with the message and key which is inserted into the cover image, after that the

message value is converted into binary numbers. If the total number of message messages can be accommodated in the cover image based on the calculation criteria for the number of pixels divided by 8 bits, a bit exchange process can be carried out. After the message is inserted in the cover, the results of the new binary cover values are converted back into decimal numbers and then mapped to stego-image.

As explained in the previous chapter, the function of steganography is to hide secret text messages in a container. What should be a concern is that in the process of modifying the changes that occur between the media and the results of the modifications must not be too striking. Changes that occur after a container image has been inserted by a secret message are not visible in plain view. Secret messages that will be inserted into the storage media are maintained, so a security technique is needed to make the secret message unreadable, so that not just anyone can retrieve the information contained in the container image object. Before the secret text is inserted into the image, the text is first encrypted, thus safeguarding the security of the secret message. For more details, see the following figure.

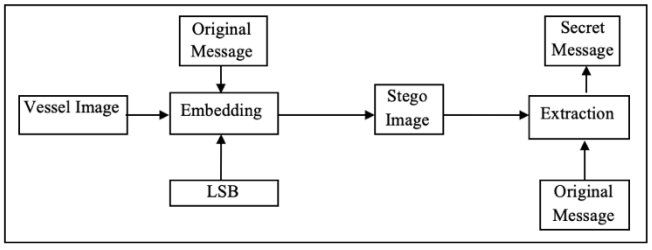

Figure 3. LSB Embedding Process

After generating an image that has been inserted a secret message, the file can be sent to the recipient, and only the legitimate recipient can retrieve the secret message contained in the image, of course, to extract the secret message extraction process is needed in the form of a detection algorithm and decryption that is owned by the legitimate recipient.

IV. RESULT AND DISCUSSION

There are two main processes in message insertion using the Least Significant Bit method, namely the embedding process and extraction process. The embedding process is the process of inserting a secret message into a media. While the extraction process is the process of retrieving secret messages from a media, in this system, the secret message used is in the form of text binary data which is text from the results of embedding techniques into the final bit values of the container media and the media used for message insertion is ".bmp" and ".jpg" image files.

The following is an example of text insertion using the Least Significant Bit method. There is one message that has been encrypted “AKU" which will be inserted in an image "hydrangeas.jpg."

Figure 4. Vessel Image of "hydrangeas"

Table 1. Binary Value of Original Message

Binary Value		
A	K	U
0	0	0
1	1	1
0	0	0
0	0	1
0	1	0
0	0	1
0	1	0
1	1	1

Table 2. Binary value of "hydrangeas.jpg"

00000001	00010100	00000000	00000001	00010100	00000000	00000001	00010100
00000001	00000000	00010011	00000000	00000000	00010011	00000000	00000000
00010101	00000000	00000000	00010110	00000001	00000000	00011000	00000000
00000000	00011010	00000000	00000001	00010100	00000000	00000000	00010011
00000000	00000000	00010011	00000000	00000000	00010110	00000001	00000000
00010110	00000001	00000000	00010110	00000001	00000010	00010101	00000010
00000000	00010011	00000000	00000001	00010011	00000011	00000000	00010001
00000001	00000000	00010001	00000001	00000000	00010000	00000000	00000000

Table 3. Binary image containing a secret message

00000000	00000001	00010010	00000000	00000000	00010010	00000000	00000001	A
00010100	00000001	00000000	00010110	00000001	00000000	00011001	00000001	K
00000000	00011011	00000000	00000001	00011000	00000001	00000000	00011001	U
00000000	00000000	00010101	00000000	00000000	00010011	00000000	00000000	-
00010011	00000000	00000000	00010111	00000001	00000000	00010111	00000001	-
00000000	00010111	00000001	00000010	00010101	00000010	00000000	00010011	-
00000000	00000000	00010011	00000011	00000000	00010001	00000001	00000000	-
00010001	00000001	00000000	00010001	00000000	00000000	00010001	00000000	-

At the end of each binary, the image has been inserted by a secret message marked with a Bold letter. The next step is the matrix will be mapped in the form of an RGB image and this image is called stego-image.

V. CONCLUSION

After the whole process is done, which starts with the literature study stage to software testing, then some conclusions can be drawn. Least Significant Bit steganography algorithm is done by replacing the hidden message bits in the last bit of each image pixel color component. This algorithm works well and fast.

The disadvantage of this algorithm is that the stego-image cannot hold too many characters because it only uses the last 1 bit of the vessel image. The advantages of this algorithm are the fast process, and the results of the image are not suspicious when seen by the eye. One image color component is only inserted one message bit so that the image size does not change. The processing time depends on the size of the information and the speed of the computer processor used.

VI. REFERENCES

[1] Hermansyah and A. P. U. Siahaan, "Technique of Hiding Information in Image using Least Significant Bit," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 67–70, 2018.

[2] R. D. Sari and A. P. U. Siahaan, "Least Significant Bit Comparison between 1-bit and 2-bit Insertion," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 110–113, 2018.

[3] S. Goel, S. Gupta, and N. Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions," 2015, pp. 105–112.

[4] Y. Wang, "Robust watermarking in wavelet domain based on chaotic scrambling," *Sens. Rev.*, vol. 31, no. 4, pp. 349–357, Sep. 2011.

[5] F. A. Al-Omari, O. D. Al-Khaleel, G. A. Rayyashi, and S. H. Ghwanmeh, "An innovative information hiding technique utilizing cumulative peak histogram regions," *J. Syst. Inf. Technol.*, vol. 14, no. 3, pp. 246–263, Aug. 2012.

[6] K. Kordov and B. Stoyanov, "Least Significant Bit Steganography using Hitzl-Zele Chaotic Map," *Int. J. Electron. Telecommun.*, vol. 63, no. 4, pp. 417–422, Nov. 2017.

[7] S. Sun, "A New Information Hiding Method Based on Improved BPCS Steganography," *Adv. Multimed.*, vol. 2015, pp. 1–7, 2015.

[8] R. Apau and C. Adomako, "Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones," *Int. J. Comput. Appl.*, vol. 164, no. 1, pp. 13–22, Apr. 2017.

[9] A. P. U. Siahaan, "Noise-Like Region Security Improvisation in BPCS Steganography."

[10] A. P. U. Siahaan, "Vernam Conjugated Manipulation of Bit-plane Complexity Segmentation," *Int. J. Secur. Its Appl.*, vol. 11, no. 9, pp. 1–12, Sep. 2017.

[11] R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," in *Journal of Physics: Conference Series*, 2018, vol. 1007, no. 1.

[12] W. Fitriani, R. Rahim, B. Oktaviana, and A. P. U. Siahaan, "Vernam Encypted Text in End of File Hiding Steganography Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 214–219, Jul. 2017.

[13] A. P. U. Siahaan, "High Complexity Bit-Plane Security Enchancement in BPCS Steganography," *Int. J. Comput. Appl.*, vol. 148, no. 3, pp. 17–22, 2016.

[14] S. Sajasi and A.-M. Eftekhari-Moghadam, "A high quality image hiding scheme based upon noise visibility function and an optimal chaotic based encryption method," in *2013 3rd Joint Conference of AI & Robotics and 5th RoboCup Iran Open International Symposium*, 2013, pp. 1–7.

[15] A. S. Girsang, "Steganografi Dengan Least Significant Bit (LSB)," *Binus University*, 2017. [Online]. Available: https://mti.binus.ac.id/2017/10/11/steganografi-dengan-least-significant-bit-lsb-2/.