Technique of Hiding Information in Image using Least Significant Bit

[1] **Hermansyah,** [2] **Andysah Putera Utama Siahaan**
Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1] hermansyah@pancabudi.ac.id, [2] andiesiahaan@gmail.com

Abstract: *Information hiding is very important because a lot of data theft occurs which can result in significant losses. Data security can be done by hiding information into a media. This media can be in the form of images or sounds. There are several concealment techniques in the picture. In this study, we will discuss the hiding of information in a 24-bit color image which consits of 3 x 8-bit. The method used is Least Significant Bit (LSB). This method is used to insert messages into the 24-bit color image insertion media on every 1 of the most significant bits of each image color. The layers used are Red, Green, and Blue. This method has a small MSE and does not appear to differ if the image is seen directly with the eye. The results of the research show that MSE calculation is not so much different from the original image. Peak Signal to Noise ratio (PSNR) for each image inserted with the maximum message size can produce an average value above 40 dB. This LSB method is excellent to use to provide information in the form of images.*

Keywords: *steganography, LSB, data hiding, algorithm.*

1. INTRODUCTION:

Securing information is needed since there is a lot of theft and manipulation of data that can result in significant losses to users. The security and confidentiality of data on computer networks are now essential and continues to be a threat from wild parties. Technological advances in the field of computer networks can quickly change and retrieve these data without being detected by the owner. Information is something that needs security. Besides that, the problem is copyright; a copyrighted work must be protected so that there is no misuse or recognition of work because it can harm the owner [1]. One of the means to secure a copyrighted work is on digital data such as photographs that are by using watermarking techniques, with watermarking identity in a digital data can be hidden so that it can be used as an identification mark that is not detected, such as author data or copyright information [2]. However, if the identity of a copyrighted work is easily detected, then the information can be misused so that the data in the form of a message of copyright information needs to be secured again. Least Significant Bit is a method of inserting a message bit on the last bit of a meaningless bit, or that has the least value, that means it will only give a change in the value of one higher or one lower [3]. This slight change cannot be clearly distinguished and in the implementation of the concept of steganography because it does not change the appearance of the image. This method is very easy to implement. However, LSB has the disadvantage that the data is inserted in the image not as much as other methods such as BPCS [4]. It is expected that this method can help users to secure information that will be sent safely. LSB can also be given a key to extract; the system will ask for a password to ensure that the person who is extracting is the right person.

2. THEORIES:

2.1 Steganography

Steganography is a technique to hide personal information with something that results will look like other standard information [5]–[7]. Media used is generally a different medium with confidential information carrier media, where this is the function of steganography technique, which is a disguise technique using other media different so that confidential information in the first media is not visible [8]. Steganography comes from the Greek language which means "hidden writing." Used in various forms for thousands of years. In the 5th century BC, Histaiacus shaved the head of a slave and then wrote a message on his head and let the hair grow to cover the written message. To read the message the messenge, the hair must be shaved back. Technological developments also bring changes to the steganography of both techniques and media used [9]–[11]. At present, the development of information insertion is shown in the following figure.

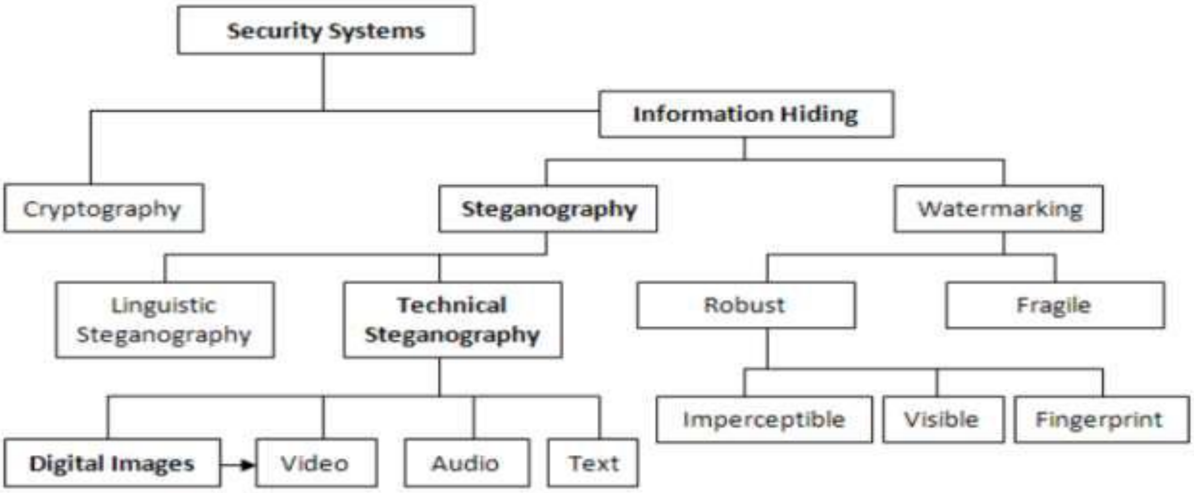

Figure 1. The focus of the discipline of information insertion

In general, steganographic messages appear in other forms such as pictures, articles, shopping lists, or other messages. This written message is writing that covers or covers. For example, a message can be hidden using ink that is not visible between visible lines. Steganography techniques include many communication methods to hide the secret message in other files containing text, images, and even audio without showing the characteristics of real or visible changes in the quality and structure of the original file. This method includes invisible ink, microdots, word settings, digital signatures, hidden paths, and excellent spectrum communication. The purpose of steganography is to conceal or hide the existence of a hidden message or information. In practice, most messages are hidden by making slight changes to other digital data whose contents will not attract the attention of potential attackers, for example an image that looks harmless. This change depends on the key and the message to hide. The person who receives the image can then deduce the hidden information by replacing the correct key into the algorithm used.

2.2 Least Significant Bit

LSB is a technique commonly used in encryption and decryption of confidential information. The workings of the LSB method are changing the redundant bit cover image which has no significant effect on the bits of the secret message. The following figure shows the mechanism of the LSB method on 8-bit images using 4-bit LSB.

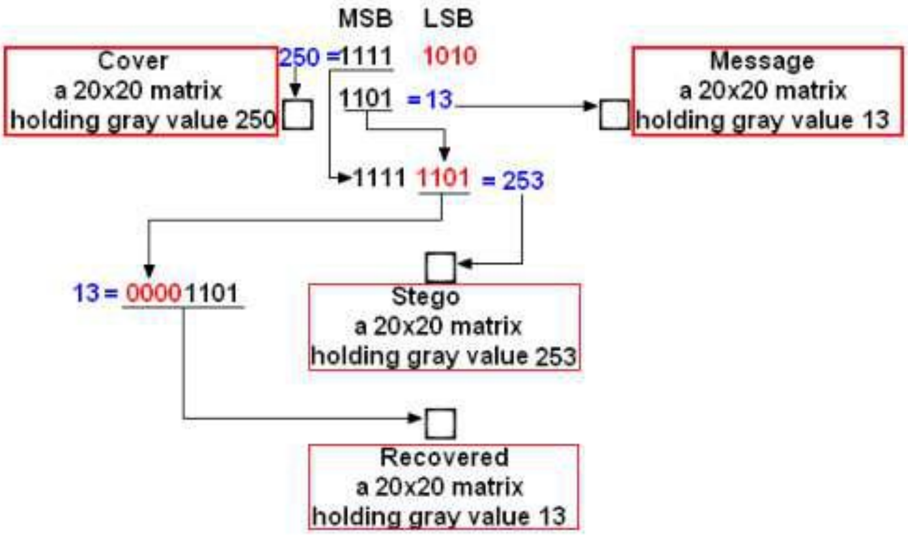

Figure 2. LSB mechanism

Figure 2 shows the application of LSB using pixel-based image media with 8-bit (gray value). Each pixel consisting of 8-bit is divided into two parts, 4-bit MSB (the most significant bit) and 4 bits LSB (least significant bit). The LSB section is converted to the value of the message to be inserted. After being spiked with a secret message, each pixel is rebuilt into a complete image resembling the original image media. The advantages of LSB are less suspicious in human eyes, easy to implement, and high perpetual transparency. LSB deficiencies include robustness, and sensitivity to filtering, as well as scaling, rotation, adding noise to the image, and cropping can damage secret messages [12].

3. RESULT AND DISCUSSION

3.1 LSB Insertion Model

Storage of bits in LSB is performed with several 1-bit models in the last bit. The following are the steps carried out in the LSB modification process to insert messages in certain bits on the content of the three color elements.

Table 1. Bit storage on LSB

R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0
B	7	6	5	4	3	2	1	0
R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0
B	7	6	5	4	3	2	1	0
R	7	6	5	4	3	2	1	0
G	7	6	5	4	3	2	1	0

3.2 MSE and PSNR

The resulting image is in the form of information that has been inserted. The image will be calculated by the MSE and PSNR values to determine how well the image is after having information in it. The following is the formula used to calculate MSE and PSNR.

$$\mathrm{PSNR} = 10 \times \lg\left(\frac{255^2}{\mathrm{MSE}}\right)$$

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=1}^{N} \sum_{j=1}^{M} \left[I(i,j) - I'(i,j) \right]^2$$

3.3 LSB Test

This section will look at the results of the LSB steganography process in inserting information into the image. This process will produce an image with MSE and PSNR calculations. This test involves images with a size of 4 x 4 pixels. This image can hold as much as 16 x 3 = 48 bits. If converted to characters, it can accommodate as many as six characters for 1-bit usage. The following tests are carried out on this method.

Information:

233	207	232	211	196	227

The information will be stored in the image using 1-bit models. The following storage illustration is done. In this test, an image of 4 x 4 pixels will be taken to be set as stego-image. The capacity that can be accommodated by this image is 4 x 4 x 3 bits = 48 bits (6 characters) on the use of 1 bit.

Red			
65	58	187	190
222	171	203	63
246	101	32	89
192	151	36	11

Green			
87	176	149	241
223	74	221	68
205	204	143	53
125	130	167	60

Blue			
116	249	167	229
150	134	191	182
128	84	243	163
226	101	153	23

The information bits that will be inserted:

11101001	11001111	11101000	11010011	11000100	11100011

Stego-image result:

Red			
65	58	186	191
223	171	203	62
247	101	33	89
192	150	37	10

Green			
87	177	149	240
223	75	220	68
205	204	143	52
125	131	166	61

Blue			
117	248	167	228
151	135	191	182
128	84	243	162
226	101	152	23

$$\text{MSE} = \frac{24}{48} = 0.5$$

$$\text{PSNR} = 10 * Log10\left(\frac{249^2}{0.5}\right) = 50.93429$$

The results of the calculation above state that the six character information is still safe if hidden in an image measuring 4 x 4 pixels. It can be seen that the MSE (0.5) value is small and PSNR (50.93429) value is more than 40 dB. It means that the stego-image is safe to embed.

4. CONCLUSION:

From the results of previous experiments can be seen the ability of LSB in storing information is outstanding because the changes in bits that occur are only one pixel. It makes the image indistinguishable from the human eye. However, besides all that, LSB has weaknesses that can lead to information leakage. If the insertion type is known by using LSB, then information will be retrieved by merely extracting the last bit of each image. Because of this weakness, LSB should be equipped with cryptographic methods so that the information contained therein is more awake than before.

REFERENCES:

1. 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.
2. Y. Wang, “Robust watermarking in wavelet domain based on chaotic scrambling,” *Sens. Rev.*, vol. 31, no. 4, pp. 349–357, Sep. 2011.
3. 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.
4. S. Sun, “A New Information Hiding Method Based on Improved BPCS Steganography,” *Adv. Multimed.*, vol. 2015, pp. 1–7, 2015.
5. 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.
6. A. P. U. Siahaan, “Noise-Like Region Security Improvisation in BPCS Steganography.”
7. 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.
8. 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.
9. R. Rahim, H. Nurdiyanto, R. Hidayat, A. Saleh Ahmar, D. Siregar, A. P. Utama Siahaan, I. Faisal, S. Rahman, D. Suita, A. Zamsuri, D. Abdullah, D. Napitupulu, M. I. Setiawan, and S. Sriadhi, “Combination Base64 Algorithm and EOF Technique for Steganography,” in *Journal of Physics: Conference Series*, 2018, vol. 1007, no. 1.
10. 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.
11. 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.
12. 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/.