Least Significant Bit Comparison between 1-bit and 2-bit Insertion

[1] Ressi Dwitias Sari, [2] Andysah Putera Utama Siahaan
Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1] ressy15@gmail.com, [2]andiesiahaan@gmail.com

Abstract: *Steganography can be used to secure secret messages. Steganography works by hiding valuable information in an accommodating medium. The media used is an image. In inserting information into a media, there are several techniques that can be used. The technique used is Least Significant Bit (LSB). It works by manipulating the last bit on each pixel. This bit will be replaced by a row of bits in the information. Each character in the information consists of 8 bits. And each bit will be inserted in each pixel in the image. A character needs 8 pixels to store information. The pixel sequence is RGBRGBRG. This study discusses insertion comparisons if carried out with 1-bit and 2-bit. Both image results will be tested for feasibility. MSE and PSNR will be applied and compared to the original image. MSE and PSNR test results say that 1-bit LSB is superior in terms of the image while 2-bit LSB is superior in terms of information size. For small information, it is better to use 1-bit LSB and large information will be inserted using 2-bit LSB.*

Key Words: *steganography, LSB, data hiding, algorithm.*

1. INTRODUCTION:

Steganography is the art and science of communication that is not visible. The word Steganography comes from the Greek word "Stegos" which means cover and "Grafia" which means to write. It can be interpreted as "hidden writing". The purpose of steganography is to hide data from wild parties. Usually, messages will be hidden in a media. This media is in the form of pictures, articles, sounds or other types [1]. The method often used to secure confidential messages from irresponsible people is to use cryptography and steganography. A cryptographic method is a process of changing the sequence of characters in the plaintext into an obscure character. However, the application of cryptographic techniques also still has weaknesses. Weakness arises from the suspicion that the information is confidential and does not take the form of an obscure character. Another method is steganography. This method is one technique used to hide secret messages on other objects such as color images [2][3]. Steganography technique is done by exchanging certain bits of digital image collection messages with secret message bits that will be hidden. The Least Significant Bit (LSB) method is the most common method used to hide secret messages into image media. The use of this method can be modified so that the use of the last bit can be added. Several methods can be applied to LSB such as 1-bit and 2-bit insertion [4].

Method Least Signification Bit (LSB) is a method that is easy to understand in the process of image insertion. The process of insertion and extraction of this method is also relatively fast because it uses only the last bit of the pixel. The LSB method inserts a message into the cover image on the smallest bit. The difference between the bits in the original image and the stego will not be too noticeable to the person who views the image. For 1-bit LSBs, the inserted bits are the 8th bit for each pixel, changing the decimal value from each pixel to one level higher or lower than the original pixel. Sometimes pixels do not change, or corresponding pixels before insertion occurs. As for the 2-bit LSB method, the inserted bits are the 7th bit and the 8th bit for each pixel. The change in values in the last two bits is between zero and three from the level of the original image. It is expected that by doing this test, it can be determined which bits are suitable for use in some instances based on the MSE and PSNR values obtained.

2. THEORIES:

2.1 Steganography

Steganography is the art and science of writing or hiding hidden messages in a way so that in addition to the sender and the recipient, no one knows or realizes that there is a secret message [5]–[7]. Instead, cryptography disguises the meaning of a message but does not hide that there is a message. For example, the sender starts with an ordinary image file, then sets the color of each 100th pixel to adjust an inner letter alphabet (the change is so smooth that no one is aware of it if he does not pay attention to it). 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, something messages can be hidden using ink that is not visible between visible lines [8]. Steganography techniques include many communication methods to hide secret messages (text or images) in other files that contain text, images, and even audio without showing the characteristics of real change orseen in the quali ty and structure of the original file. This method includes invisible ink, microdots, word settings, digital signatures, hidden paths, and full spectrum communication. The purpose of steganography is to conceal or hide the existence of a hidden message or information.

In practice mostly solved 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. In the method of steganography, this method is advantageous if used in the way of computer steganography because many digital file formats can be used as media to hide messages [9].

The advantages of steganography rather than cryptography are that the messages do not attract the attention of others. Encoded messages in cryptography are not hidden even if they cannot be solved; it will attract attention. Often, steganography and cryptography are used together to ensure the security of the secret message. Most steganography algorithms use a combination of types of techniques to perform a task in cloaking secret messages in a file envelope. A steganography program is needed to do the following things, find the excess bits in the file envelope that can be used to cover the secret message inside, choose some of them to be used in enveloping data and cloaking the data in bits selected before [10]–[12]. There are four types of steganography methods, such as [9]:

1. Least Significant Bit Insertion (LSB) The method used to hide messages on digital media is different. Examples of the message image file can be hidden by using a way to insert it on the low bit or the rightmost bit (LSB) on the pixel data that compose the file. As we know for 24-bit bitmap files, each pixel (dot) in the image consists of three red, green and blue (RGB) colors, each of which is composed of 8 bits from 0 to 255 or binary format 00000000 to 11111111. Thus in every pixel of a 24-bit bitmap file, it can be inserted by 3 bits of data. Disadvantages of LSB Inversion: can be deduced from the example of 8-bit pixels, using the LSB Insertion can drastically change the color constituents of pixels. It can show the real difference from the cover image to the stego image so that the sign shows the state of steganography. Color variations are less apparent with 24-bit images. However the file is enormous between 8 bits, and 24-bit images are vulnerable to image processing, such as cropping and compression.
2. Algorithms and Transformation A compression algorithm is a method of steganography by hiding data in a mathematical function. These two functions are Discrete Cosine Transformation (DCT) and Wavelet Transformation. The function of DCT and Wavelet is to transform data from one place (domain) to another. The DCT function is to transform data from a spatial domain to the frequency domain.
3. Redundant Pattern Encoding Redundant Pattern Encoding is drawing small messages on most images. The advantage of this method is that it can survive cropping, the disadvantage of not being able to draw a larger message.
4. Spread Spectrum Spread Spectrum steganography methods are scattered as messages that are encrypted through images. To read a message, the recipient requires an algorithm that is crypto-key and stego-key. This method is also still easy to attack, namely the destruction or destruction of compression and image processing.

2.2 Least Significant Bit

Steganography is a method of hiding information into the media while LSB is one method used to insert information into the media. The LSB method is done by modifying the last bits in the image in every byte of color in a pixel [13]. These LSB bits will be modified by replacing each last bit with the secret bits of information. After all bits of information has entered the last bit of the image, the information has been successfully hidden. When the secret information wants to be reopened, the LSB bits that are now available will be extracted one by one and then reassembled into complete information as before. Determination of LSB bits is done sequentially from the initial byte to the last byte according to the length of the secret data that will be hidden. Changing the LSB bit will change the byte value one higher or one lower than the pixel value in the image. It does not affect visual perception. [14].

3. METHODOLOGY:

The strength of steganography lies in the smoothness of the image in storing information. MSE and PSNR can measure this level of subtlety. MSE will calculate how far the image results from the original image while the PSNR will determine the feasibility of the image in decibels. The following is the formula used to determine MSE and PSNR.

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

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

4. RESULT AND DISCUSSION:

4.1 1-bit Least Significant Bit

1-bit storage will affect the last bit on the pixel. The following table is how information values in units of bits are stored in a row of pixels in the original image. This storage involves 3 pixels in the R-G-B-R-G-B-R-G sequence. The last pixel is only stored on the green layer. Each pixel has three color layers.

Table 1. 1-Bit storage on 1-bit 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

4.2 2-bit Least Significant Bit

2-Bit storage will affect the last two bits of the pixel. The following table is how information values in units of bits are stored in a row of pixels in the original image. This storage involves two pixels with the R-G-B-R sequence. The last pixel is only saved on the red layer. Each pixel has three color layers. Each layer will store 2 bits of information so that there are four layers that will be used as a placeholder.

Table 2. 2-Bit storage on 2-bit 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

4.3 Least Significant Bit Test

1-bit testing will be done by providing confidential information as much as six characters or 48 bits. The image used is 4 x 4-pixel dimension. Each pixel has three layers. The image can accommodate 4 x 4 x 3 = 48 bits. This size matches the information that will be inserted later. The following calculations and illustrations will illustrate how information is stored in the stego-image.

Table 3. Information that will be inserted in the image in byte and binary form

C1	C2	C3	C4	C5	C6
233	207	232	211	196	227
11101001	11001111	11101000	11010011	11000100	11100011

Table 4. Pixel rows from the original image before insertion

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

Table 4 illustrates the pixel array for each of Red, Green, and Blue. The total pixel used is 16 x 3 = 48 pixels.

Table 5. The pixel results after insertion in the last bits

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

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

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

Table 6. The pixel results after insertion in the last two bits

Red	67	57	187	190	223	171	201	62	246	101	32	89	192	151	36	11
Green	86	179	151	242	221	75	220	68	205	204	143	53	125	130	167	60
Blue	118	248	167	228	148	132	191	183	128	84	243	163	226	101	153	23

MSE $= \frac{59}{48}$
$= 1.229167$

PSNR $= 10 * Log10\left(\frac{249^2}{1.229167}\right)$
$= 47.02788$

The results of the comparison of MSE and PSNR values can be seen in Tables 5 and 6. Test results show that the application of 1-bit on LSB is better than 2-bit. This can be seen from the 1-bit MSE value smaller than 2-bit MSE. 1-bit PSNR is also larger than 2-bit PSNR. It shows the insertion of six characters in a 4 x 4 image gets more positive values on the 1-bit LSB model.

5. CONCLUSION:

LSB testing has got different results on 1-bit and 2-bit models. The use of bits affects the smoothness of the image on the stego-image. Looking at the results of MSE and PSNR calculations in both image testing, 1-bit LSB is much better than 2-bit. It happens because the MSE value is 1-bit smaller than MSE on 2-bit. Image smoothness can be measured with PSNR which shows the PSNR value on 1-bit LSB is greater than 2-bit LSB. Although the two PSNR values are already above 40 dB, this is not necessarily the case with other information patterns and stego-mages.

REFERENCES:

1. F. A. Al-Omari, O. D. Al-Khaleel, G. A. Rayyashi, dan S. H. Ghwanmeh, “An innovative information hiding technique utilizing cumulative peak histogram regions,” *J. Syst. Inf. Technol.*, vol. 14, no. 3, hal. 246–263, Agu 2012.
2. K. Kordov dan B. Stoyanov, “Least Significant Bit Steganography using Hitzl-Zele Chaotic Map,” *Int. J. Electron. Telecommun.*, vol. 63, no. 4, hal. 417–422, Nov 2017.
3. S. Sun, “A New Information Hiding Method Based on Improved BPCS Steganography,” *Adv. Multimed.*, vol. 2015, hal. 1–7, 2015.
4. Y. Wang, “Robust watermarking in wavelet domain based on chaotic scrambling,” *Sens. Rev.*, vol. 31, no. 4, hal. 349–357, Sep 2011.
5. R. Apau dan C. Adomako, “Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones,” *Int. J. Comput. Appl.*, vol. 164, no. 1, hal. 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, hal. 1–12, Sep 2017.
8. S. Sajasi dan 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, hal. 1–7.
9. A. Cokro, “Belajar Kriptografi dan Steganografi,” *Kumpulan Tutorial*, 2016. .
10. R. Rahim *et al.*, “Combination Base64 Algorithm and EOF Technique for Steganography,” in *Journal of Physics: Conference Series*, 2018, vol. 1007, no. 1.
11. W. Fitriani, R. Rahim, B. Oktaviana, dan A. P. U. Siahaan, “Vernam Encypted Text in End of File Hiding Steganography Technique,” *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, hal. 214–219, Jul 2017.
12. A. P. U. Siahaan, “High Complexity Bit-Plane Security Enchancement in BPCS Steganography,” *Int. J. Comput. Appl.*, vol. 148, no. 3, hal. 17–22, 2016.
13. Segi3Hijau, “Teknik Steganografi dengan Metode LSB,” 2012. [Daring]. Tersedia pada: https://segi3hijau.wordpress.com/2012/11/01/teknik-steganografi-dengan-metode-lsb/.
14. A. S. Girsang, “Steganografi Dengan Least Significant Bit (LSB),” *Binus University*, 2017.