http://ejournal.seaninstitute.or.id/index.php/InfoSains
Jurnal Info Sains : Informatikan dan Sains, Volume 11, No 01 Maret 2021
E-ISSN.2797-7889, P-ISSN.2089-3329

Steganography Formation by utilizing Enhanced Least Significant Bit Algorithm

[1]Pristiwanto, [2]Abdul Halim Hasugian
[1]Informatics Engineering Study Program, Universitas Budi Darma
[2]Faculty of Science and Technology, Universitas Islam Negeri Sumatera
Email : wanto97@gmail.com[1], abdulhasugian12@gmail.com[2]

Keywords

Steganography
Enhanced Least Significant Bit.

Abstract. Steganography is the science and art of hiding secret messages in other messages so that the existence of those messages cannot be known. The letter sent does not attract attention with steganography, and the container media does not arouse suspicion. Steganography requires two properties, namely container media and secret messages. The LSB method (least significant bit)is the simplest and easiest steganography method to implement. An example of implementing this method is to use a digital image as a cover text. Each pixel in the image is 1 (one) to 3 (three) bytes in size. Pda bit arrangement in a byte (1 byte = 8 bits), there are the most significant bits (MSB) and the least significant bits (LSB). For example, on 11010010 bytes, the first bit from the right is the MSB bit, and the last bit from the right is the LSB bit. The matching bit is replaced with the message bit is the LSB bit, because the modification only changes the byte value to one higher or one lower than the previous value.

1. INTRODUCTION

The rapid advancement of technology at this time makes it easy for everyone to convey information to others. However, the ease obtained in sharing information (messages) does not mean guaranteeing the security of the transmission to the destination. Certain parties likely want to know the content of the letter sent. Therefore, one way that the message is conveyed is unknown or attracts the attention of others is to use the technique of hiding the message (steganography)[1].

Steganography is the science and art of hiding secret messages in other messages so that the existence of those messages cannot be known. With steganography, the message sent does not attract attention and the container media does not arouse suspicion. Steganography requires two properties, namely container media and secret messages[2]. The LSB method (least *significant bit)*is the simplest and easiest steganography method to implement. An example of implementing this method is to use a digital image as a *covertext*. Each *pixel* in the image is 1 (one) to 3 (three) bytes in size[3]. Pda bit arrangement in a byte (1 byte = 8 bits), there are the most significant *bits* (MSB) and the least significant bits (LSB). For example on 11010010 bytes, the first bit from the right is the MSB bit and the last bit from the right is the LSB bit[4]. The matching bit is replaced with the message bit is the LSB bit, because the modification only changes the byte value to one higher or one lower than the previous value. For example, the bytes in the image give a perception of red color, then the change of one bit LSB only changes the perception of red color is not very striking. The human eye cannot distinguish the small changes that occur in the image[5].

To make *hidden text* untraceable, message bits do not replace sequential *bytes*. However, a randomly selected byte order is determined. For example, if 50 bytes and 6 bits of data are hidden, LSB will replace the chosen bytes randomly, bytes number 36, 5, 21, 10, 18, 49. In 8-bit images that are 256 x 256 pixels there are 65536 pixels, each pixel is 1 byte so that it can only be inserted 1 bit on each pixel. In a 24-bit image measuring 256 x 256 pixels, one pixel is 3 bytes (or 1 byte for each component R, G, B), so we can insert as much as 65536 x 3 bits = 196608 bits or 24576 bytes.

2. METHOD

2.1 Steganalysis

Steganalysis is an art and science to detect the presence or absence of hidden messages in an object. Steganalysis can be done in 2 (two) ways, namely subjective methods and statistical methods. Personal methods involve the human sense of vision to observe the suspected part of the image, which is also called *a visual attack*. One of the optical steganalysis techniques is *the enhanced LSB* method. This method displays the last bits of an image and uses the last bits of an image[6].

While the statistical method involves mathematical analysis of an image to find the difference between the original image and the picture that has been inserted message, although *stegoimage* is identical to its *cover image* when viewed using the human sense of vision, *stegoimage* often shows impressive statistics that distinguish it from its *cover image.* The purpose of statistical steganalysis is to expose this unusuality so that the difference between *stegoimage* and *cover image* can be known[7][8].

2.2 Enhanced LSB

This *LSB enhanced* algorithm was put forward by Andreas Westfield and Andreas Pfitzmann. The basic idea of this algorithm is luminance *values.* The LSB in an image is not entirely random, but still depicts the shape of the picture[9]. The primary process of the *LSB enhanced* method is to change the entire bit value to 1 if the LSB value of a byte is 1, and instead change the whole bit to 0 if the LSB of that byte is 0. Each pixel has three components namely *red, green* and *blue.* Each piece is presented by one byte, each byte has a bit of LSB. If the LSB bit is 1 then all bits in the byte are replaced with bit 1 so that the byte value is 11111111 (binary) or 255 (decimal). Whereas, if the LSB bit is 0, then all bits in the byte are replaced with 0 bits so that the byte value is 00000000 (binary) or 0 (decimal). After the filtering process, the image in the image not inserted by the message will approach the original image[10]. While the part of the image containing the secret message will become corrupted after filtering. Thus from the images produced after filtering, the human sense of vision can easily distinguish between images that do not contain secret messages and images containing secret messages.

3. RESULT AND DISCUSSION

3.1 System Analysis

The steganalysis method used in detecting secret messages inserted with *the least significant bit* (LSB) method is the enhanced least considerable *bit* method. This method utilizes the human sense of vision to recognize steganographic image objects with dominant color differences. This method will change the entire bit value of a pixel byte according to the pixel's last bit value. Here's an algorithm of the LSB *enhanced* steganalysis method.

1) Check the last bit of each byte of data.
2) If the last bit is 0, change all bits of that byte to 0. And if the last bit is 1, then change all bits of that data byte to 1.
3) After the bit change process, pay attention to the image to determine if the image contains a secret message.
4) An example of implementing this *enhanced* LSB method is for example, there is a 6 x 8 pixel image. The following are bits of data on the image.

Table 1. Bit 6 x 8 Pixel Image Data

0000000	0000000	0000001	0000001	0000001	0000001	0000001	0000001
0000000	0000000	0000001	0000001	0000001	0000001	0000001	0000001
0000000	0000000	0000001	0000000	0000001	0000001	0000001	0000001
0000001	0000001	0000001	0000010	0000010	0000011	0000011	0000011
0000001	0000001	0000001	0000010	0000010	0000011	0000011	0000011
0000001	0000001	0000001	0000010	0000010	0000011	0000011	0000011

Then this image will be inserted text in the form of the word "*secret*" using the LSB method. The term "*secret*" which willbe inserted first will be represented in binary form as follows.

Table 2. ASCII Code Characters On The Word "Secret”

Karakter	ASCII	Heksadesimal	Biner
S	115	73	0111011
E	101	65	01100101
C	99	63	01100011
R	114	72	01110010
E	99	63	01100011
T	116	74	01110100

Then the word "*secret*" will be the following data:

Table 3. Bit Data Word "secret"

0	1	1	1	0	0	1	1
0	1	1	0	0	1	0	1
0	1	1	0	0	0	1	1
0	1	1	1	0	0	1	0
0	1	1	0	0	0	1	1
0	1	1	1	0	1	0	0

Then, each bit of the word*"secret"* constituent character will be archived at the last bit of each byte of the image. Then the changes of bits every byte on the picture are as follows.

Table 4. Bit Data ImageTableInserted in Message

0000000	0000001	0000001	0000001	000000	0000000	0000001	0000001
0000000	0000001	0000001	0000000	0000000	0000001	0000000	0000001
0000000	0000001	0000001	0000000	0000000	0000000	0000001	0000001
0000000	0000001	0000011	0000011	0000010	0000010	0000011	0000010
0000000	0000001	0000011	0000010	0000010	0000010	0000011	0000011
0000000	0000001	0000011	0000011	0000010	0000011	0000010	0000010

Once the LSB result image is obtained, steganalysis can be done by applying *the enhanced* LSB method. This method is used by replacing each bit of the image byte according to the LSB bit that has been replaced with that secret message bit. The following is the bit value of the image that has been steganalysis process.

Table 5. Bit ImageRy Data Steganalisis Results

0000000	11111111	11111111	11111111	0000000	0000000	11111111	11111111
0000000	11111111	11111111	0000000	0000000	0000000	0000000	11111111
0000000	11111111	11111111	0000000	0000000	0000000	11111111	11111111
0000000	11111111	11111111	11111111	0000000	0000000	11111111	0000000
0000000	11111111	11111111	0000010	0000000	0000000	11111111	11111111
0000000	11111111	11111111	11111111	0000000	11111111	0000000	0000000

4. CONCLUSION

After completing the design of the steganalysis application with *the enhanced least significant bit* method, it is concluded how the *enhanced* LSB method works are to change the value of each bit on a *byte pixel* of bitmap image data to 0 or 255 according to the LSB bit value that has been replaced with the message bit on the digital image. The image inserted with a secret message is almost the same as the original image, so it is difficult to distinguish the naked eye from humans. Steganalysis images can be analyzed by the human sense of vision to ascertain that the image contains a secret message. Inserted secret messages can be extracted so that the message's contents can be known to the user.

REFERENCE

[1] U. A. Anti, A. H. Kridalaksana, and D. M. Khairina, “Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF),” *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 12, no. 2, p. 104, 2017, doi: 10.30872/jim.v12i2.658.

[2] S. G. Supratman, “Steganografi Dengan Menggunakan Metode Lsb Dan Algoritma Hill Cipher,” *Buffer Inform.*, vol. 1, no. 1, pp. 38–45, 2017, doi: 10.25134/buffer.v1i1.582.

[3] Bakir and Hozairi, “Implementasi Metode Least Significant Bit (LSB) Dengan Enkripsi Cipher Caesar Pada Steganografi Menggunakan Image Processing,” pp. 75–81, 2018.

[4] N. Laila and A. S. R. Sinaga, “Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra,” *Sci. Comput. Sci. Informatics J.*, vol. 1, no. 2, p. 47, 2019, doi: 10.22487/j26204118.2018.v1.i2.11221.

[5] A. A. Fikhri and H. Hendrawaty, “Implementasi Steganografi Text To Image Menggunakan Metode One Bit Least Significant Bit Berbasis Android,” *J. Infomedia*, vol. 3, no. 1, pp. 10–17, 2018, doi: 10.30811/jim.v3i1.623.

[6] T. K. Watimena, “Keamanan Data Menggunakan Metode Lsb Dan Enkripsi Vigenere,” *J. Teknol. Inf. Unika St. Thomas*, vol. 4, no. 1, pp. 13–22, 2020.

[7] E. Nirmala, “Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android,” *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 36, 2020, doi: 10.32493/informatika.v5i1.4646.

[8] L. P. Malese, “Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (Lsb).,” vol. 11, no. 1, pp. 1–5, 2020, doi: 10.31234/osf.io/8g39h.

[9] A. Hafiz, “Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb),” *J. Cendikia*, vol. 17, no. 1, pp. 194–198, 2019.

[10] D. Novianto and Y. Setiawan, “Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES),” *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019, doi: 10.36982/jig.v9i2.561.