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

Text Insertion By Utilizing Masking Filtering Algorithms As Part of Text Message Security

[1]Doni El Rezen Purba, [2]Desinta Purba
[1,2]Informatics Engineering Study Program, Universitas Katolik Santo Thomas, Medan
Email : donielpurba11@gmail.com,desintapurba45@gmail.com

Keywords

Steganography
Masking
Filtering
Imagery

Abstract. for a secret message to be read and understood by a specific person only, a way is needed to hide the message, namely by steganography. Steganography is the concealment of secret messages in other media, such as images, audio, or video, so that the media inserted into the message looks as usual. Digital photos are one of the container media that are widely used for data hiding. However, when processing images such as compression, rotation, noise, and so on, confidential messages in the picture are prone to damage or loss. Then it takes the correct steganography method to hide secret messages into images to keep messages safe, not damaged even if the container image is manipulated, and the hidden message can be extracted again. on this thesis, applied masking method – filtering. Masking-filtering is included in the spatial domain. Message hiding is done by manipulating the luminance value of the image. Its use is applied to color or grayscale images. Masking serves as a tagging place on the picture that can be inserted message. Filtering passes a value to the marked section. the result is a stego image where the news is integrated with the container image, more robust to image processing when compared to methods that are also classified in the spatial domain, such as the least significant bit.

1. INTRODUCTION

Steganography is the science and complexity of secret housing messages (hiding messages) so that human senses do not detect the existence of messages. The word steganography comes from Greek which means "hidden writing" (closed writing). Steganography requires two properties: a container and confidential data to be hidden. Digital steganography uses digital media as a container, for example, images, sound, text, and video. Data security needs to be done because these data are very confidential. Confidential data that is hidden can also be in the form of images, sound, text, or videos. If you are a cryptographer, the data you use (ciphertext) is available; if you use cryptographic ciphertext, you will connect to a computer that cannot handle it.[1], [2].

Masking-filtering is included in the spatial domain. Message hiding is done by manipulating the luminance value of the image [3]. Its use is applied to color or grayscale images. Masking functions as marking of places in the picture where messages can be inserted while filtering passes the value to the significant part. This masking-filtering method is usually limited to images with 24-bit color or grayscale mode images. This method is similar to a watermark, where an image is marked (marking) to hide secret messages. This can be done, for example, by modifying the luminance levels of some parts of the image [4]. The masking method is much better than LSB because it allows for compression, cropping, and some other picture processing. The masking technique inserts information into certain significant areas so that the hidden message can be hidden more than just masking the level of noise in the image [5]. This makes masking better than LSB, for example, in pictures with the JPEG format, which are lossy compressed.

2. METHOD

2.1 Research Work Steps

The steps of research work by following the following activities:

Figure 1. Research Work Steps

Problem analysis is an activity to ascertain what will be solved against the object used as part

of the activity; object determination is an activity to choose the image used as an object to be inserted. The application of the selected method and following every step of the work that has been, the determination of the results is an activity to present the results found from the method.

2.2 Steganografi

According to Jonathan Cummins in hapsari much translation. Steganography is one way to hide confidential messages [6], [7]. In addition, cryptographic messages are hidden with "randomized" so that in some instances can easily invite suspicion, while on steganography, the news is "disguised" in a relatively "safe" form so that no fear occurs. Steganography can be used in various data forms, namely *image*, *audio*, and *video*[8].

2.3 Masking-Filtering

According to Susanti, this *masking* and *filtering* technique is usually limited to a 24-bit *color* images or *grayscale images.* This method is similar to watermarks, where an *image* is marked to hide secret messages. This can be done, for example, by modifying the luminance of some parts of the *image*[3], [9]–[11]. Although this method will change the look of *the image*, it is possible to do it in a certain way so that the human eye does not notice the difference. Because this method uses aspects of *the image* that are indeed visible directly, this method will be more "*robust*" against compression (especially *lossy* compression), *cropping*, and some other image *processing* when compared to modification methods lSb [12], [13].

3. RESULTS AND DISCUSSION

The masking process of the imagery is intended as a place tagging on the image to be inserted, while filtering aims to pass the value on the marked part. The system designed in this thesis consists of two main processes: insertion of messages and the process of extracting messages. The following is a simple example of inserting the letter "A" into a JPG file with six colors in the color palette.

1. The message to be inserted is "A," which, when converted into binary form based on ASCII encoding, returns a binary number: 01000001, where the binary value is obtained from converting A into a decimal form which is 65, and then the value 65 is converted to binary which returns = 01000001.
2. m=1010000012=32110
3. The number of color palettes is 6. 6!>321-1For insertion can be done
4. The color order in the image's color palette is:

Table 1. Image Color Order

0	1	2	3	4	5
Color A R G B 255 255 255	Color B R G B 254 221 236	Color C R G B 251 186 216	Color D R G B 255 255 251	Color E R G B 251 251 203	Color F R G B 251 214 235
16777215	15703724	16497368	16777211	16496075	16504555

The order of the color palette after being sorted by the values above is:

Table 2. Color Palette Arrangement

0	1	2	3	4	5
Color A	Color B	Color C	Color D	Color E	Col or F

5. Iteration of variable I from 1 to n: The color of the index to - (n-1) is moved to the index to - (m mod i), m=m/i
   For i=1
   5th index color moved
   to 0 m-321, m-321/1-
   321
   For i=2

The color of the 4th index is moved to the 1st index. m-321, m-321/2-160

For I =3

The color of the 3rd index is moved to the 1st index. m-160, m-160/3-53

For i=4

The color of the 2nd index is moved to the 1st index. m-53, m-53/4-53-13

For i=5

The color of the 1st index is moved to the 3rd index. m-13, m-13/5-2

For i=6

The color of the 0th index is moved to the 2nd index.

6. In the fifth stage, several colors occupy the same index. Any color that occupies the index that has been filled, then the color that previously occupied the index will shift once to the following index

Table 3. Color Based on Index

0	1	2	3	4	5
Color A					
Color A	Color D				
Color A	Color B	Color D			
Color A	Color F	Color B	Color D		
Color A	Color F	Color B	Color C	Color D	
Color A	Color F	Color E	Color B	Color C	Color D

7. This color palette sequence is then inserted back into the JPG image file to generate the image that has been inserted into the message.
8. A picture that has been inserted with Messages.

4. CONCLUSION

After conducting literature studies, analysis, design, implementation, and testing of the masking- filtering algorithm, it can be concluded that the insertion of text data into an image file so that others cannot know the data. This is due to differences in the color arrangement of the original image color and the stego image. The decoding process in the masking-filtering algorithm does not return the stego image to the original image.

REFERENCE

[1] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *J. Appl. Intell. Syst.*, vol. 3, no. 1, pp. 28–38, 2018.

[2] A. A. Mahesh and K. B. Raja, "Design of an efficient steganography model using lifting based

[3] DWT and Modified-LSB Method on FPGA," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 10, pp. 226–231, 2019.

[4] B. Williges, M. Dietz, V. Hohmann, and T. Jürgens, "Spatial Release From Masking in Simulated Cochlear Implant Users With and Without Access to Low-Frequency Acoustic Hearing," *Trends Hear.*, vol. 19, 2015, DOI: 10.1177/2331216515616940.

[5] S. Lanfranco, L. H. Mazzini, A. E. Dominguez, and J. L. Naguil, "Watermark detector based on stochastic resonance phenomenon," *IEEE Lat. Am. Trans.*, vol. 11, no. 1, pp. 396–401, 2013,

DOI: 10.1109/TLA.2013.6502836.

[6] M. Cem kasapbaşi and W. Elmasry, "New LSB-based color image steganography method to enhance the efficiency in payload capacity, security and integrity check," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 43, no. 5, 2018, DOI: 10.1007/s12046-018-0848-4.

[7] Sembiring Sandro, "Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End of File," *Pelita Inform. Budi Darma*, 2013.

[8] U. Amri, I. G. P. S. Wijaya, and F. Bimantoro, "Steganografi Menggunakan Metode Pencocokan LSB dan Karakter Non-Breaking Space Sebagai Penanda Pesan," *J. Comput. Sci. Informatics Eng.*, vol. 1, no. 1, p. 23, 2018, doi: 10.29303/jcosine.v1i1.18.

[9] M. F. Syawal, D. C. Fikriansyah, and N. Agani, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," *J. TICOM*, vol. 4, no. 3, pp. 91–99, 2016.

[10] G. Tarawneh *et al.*, "Invisible noise obscures visible signal in insect motion detection," *Sci. Rep.*, vol. 7, no. 1, 2017, doi: 10.1038/s41598-017-03732-7.

[11] R. L. Goldsworthy, L. A. Delhorne, L. D. Braida, and C. M. Reed, "Psychoacoustic and phoneme identification measures in cochlear-implant and normal-hearing listeners," *Trends Amplif.*, vol. 17, no. 1, pp. 27–44, 2013, doi: 10.1177/1084713813477244.

[12] T. M. Bücking, P. J. van den Berg, and S. Balaban, "Processing methods for photoacoustic Doppler flowmetry with a clinical ultrasound scanner," *J. Biomed. Opt.*, vol. 23, no. 2, p. 1, 2018, doi: 10.1117/1.jbo.23.2.026009.

[13] H. C. Rustamaji, M. Mariani, and B. Yuwono, "APLIKASI KOMPRESI DATA MENGGUNAKAN METODE HUFFMAN STATIK PADA PERANGKAT MOBILE BERBASIS ANDROID," *Telematika*, vol. 11, no. 1, 2015, doi: 10.31315/telematika.v11i1.311.

[14] A. P. U. Siahaan, "IMPLEMENTASI TEKNIK KOMPRESI TEKS HUFFMAN," *J. Inform.*, vol. 10, no. 2, 2016, doi: 10.26555/jifo.v10i2.a5070.