



Steganography Implementation of Insertion of Confidential Data on Digital Image Media with Bit-Plane Complexity Segmentation Method and Vigenere Cipher Extended Encryption Method

Kelvin Dharma Kusumah, Jeanny Pragantha and
Novario Jaya Perdana

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

July 25, 2022

STEGANOGRAPHY IMPLEMENTATION OF INSERTION OF CONFIDENTIAL DATA ON DIGITAL IMAGE MEDIA WITH BIT-PLANE COMPLEXITY SEGMENTATION METHOD AND VIGENERE CIPHER EXTENDED ENCRYPTION METHOD

Kelvin Dharma Kusumah¹, Jeanny Pragantha², Novario Jaya Perdana³

^{1,2} *Computer Science Department, Faculty of Information Technology*

³ *Information System, Faculty of Information Technology*

Tarumanagara University

^{a)} *kelvin.535180071@stu.untar.ac.id*

^{b)} *jeannyp@fti.untar.ac.id*

^{c)} *novariojp@fti.untar.ac.id*

Abstract Sending confidential messages through the internet is very vulnerable to theft, many irresponsible parties try to get information from these messages for personal gain. So that the secret message can only be read and understood by certain parties, a way is needed to hide the message, namely with steganography. Steganography is a technique to hide messages in media such as text, images, audio and video so that the media that is inserted looks like normal. Bit-Plane Complexity Segmentation (BPCS) is a steganographic method used in message embedding. This method has a large message insertion capacity. The insertion is done by replacing the complex bit-plane with a secret message block. In this final project, a software is developed that applies the steganography method with the BPCS method on uncompressed images. In addition, tests were conducted to analyze the suitability of the BPCS method on uncompressed images. The final result obtained is a software capable of handling message insertion. The conclusion of this research is that the BPCS algorithm is proven to be able to solve the problem of inserting messages into image media.

Keyword: *Steganography, Bit Plane Complexity Segmentation, BMP.*

INTRODUCTION

Data security is needed by all parties today, especially with the faster internet network that makes information processing very easy for all circles, information exchanged is very diverse, it can be in the form of text data, images, video or, audio. especially with the increasingly fast internet network, making information distribution very easy for all circles to do [1]. With the rapid development of the internet today, it must be followed by an increase in data security.

“Steganography is the art and science of writing hidden messages or hiding messages in a way so that apart from the sender and the recipient, no one knows or realizes that there is a secret message” [2]. The advantage of steganography over cryptography is that the message will be inserted on a medium by making slight changes to the media that the message will insert without changing the external appearance of the media, so that using steganography will not attract attention and cause suspicion for third parties, because the message will be stored in a medium as a container and the output result of the data is exactly the same as the original data [3].

Seeing this problem, the final project of the topic on steganography was proposed using the bitplane complexity segmentation method. The function of this application is to insert text data can be in the form of files or in the form of text written directly, into color images in BMP format without changing or damaging the appearance of the image, for the output of this program is a file that has been inserted by the sender before, which will be accepted by the recipient of the image the difference between this application

and the existing design is that in this design it adds a method of encrypting message data before being inserted using vigenere cipher.

THEORITICAL BASIS AND METHOD

Bit-Plane Complexity Segmentation

Bit-plane complexity segmentation (BPCS) is one of the steganographic techniques introduced by Eiji Kawaguchi and Richard O. Eason in 1997. Eiji Kawaguchi and R. O. Eason introduced this BPCS technique to be used in uncompressed color imagery documents in the BMP format. First the imagery document is divided into segments that are 8x8 pixels in size per segment, each pixel block has 8 bit-planes, from each bit-plane block is composed of 8x8 pixels or composed of 64bit per block [9]. The process of dividing an 8x8 pixel segment into an 8 bit plane is known as the process of bit slicing. In an 8-bit image document, each segment will have an 8 bit plane representing the pixels from which each bit originates. The representation of these eight bit planes is the PBC system (Pure Binary Code). The insertion process is carried out on the bit plane using the CGC (Canonical Gray Code) system, because the bit slicing process in the CGC tends to be better than in the PBC [4].

Informative Region dan Noise-Like Region

The complexity of a binary image is a change in the black and white color of a binary image, if the color change occurs a lot then it can be said that the image has a high complexity value [5], the complexity value is calculated by the formula (1).

$$\alpha = \frac{k}{n} \dots\dots (1)$$

Where k is the sum of the black-and-white color changes and n is the maximum possible color change in the image.

Binary Image Conjugation

The conjugation of a binary image P is another binary image that has a complexity value of one minus the value of complexity p. Suppose a black-and-white image P measuring 8x8 pixels has a white background color and a black foreground color. W is a pattern with all pixels in white and B is a pattern with all pixels in black. Wc and Bc are chessboard patterns, with pixels on the top left white on the Wc and black on Bc [6].

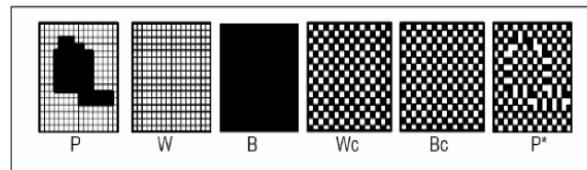


FIGURE 1 Conjugation on Binayu Image

To construct a P* conjugation from a P image, it can be done by the following formula, where " \oplus " signifies an exclusive OR operation [6].

$$P^* = P \oplus Wc \dots\dots (2)$$

Informative Region dan Noise-Like Region

A simple image is also called an informative image or an image that has bits that are not complex but contain important information from the image, while a complex image is called a noise-like region which contains complex bits and does not have important information from the image, therefore the insertion process can be done in the noise-like region. If a bit-plane has a complexity value that is smaller than the threshold ($\alpha \leq \alpha_0$) then the bit-plane is classified as an informative region and vice versa the bit-plan will be considered a noise-like region [7].

Vigenere Cipher

Vigenere Cipher is a classic cryptographic algorithm invented by Giovan Battista Bellaso in 1553, Vigenere Cipher is a method of development of the Caesar Cipher encryption method [8], mathematically the encryption-decryption function can be calculated by formulas (3) and (4):

$$\text{Encryption: } Ci = (Pi + Ki) \text{ mod } 26 \dots\dots (3)$$

$$\text{Decryption: } Pi = (Ci - Ki) \text{ mod } 26 \dots\dots (4)$$

Vigenere Cipher that will be used in this application is vigenere cipher extended where the description is not only for alphabet letters but also includes ASCII characters. The encryption-decryption function can be written in formulas (5) and (6):

$$\text{Enkripsi: } Ci = (Pi + Ki) \text{ mod } 256 \dots\dots (5)$$

$$\text{Dekripsi: } Pi = (Ci - Ki) \text{ mod } 256 \dots\dots (6)$$

PSNR AND MSE

PSNR (Peak Signal to Noise Ratio) is the value to determine the quality of the image resulting from steganography, to calculate the PSNR value will be calculated the Mean Square Error (MSE) value first, MSE is the average error difference value between the original image pixels and the steganographic image pixels. PSNR is measured in desible units (db), the greater the PSNR value produced by the image, the better the image quality, on the contrary, the smaller the PSNR value produced, the worse the image quality will be [9]. For the calculation of the values of MSE and PSNR is written in the formula (7):

$$MSE = \frac{1}{MN} \sum_{y=1}^M \sum_{x=1}^N [I(x,y) - I'(x,y)]^2 \dots\dots (10)$$

Where:

MSE = Mean Square Error value of steganographic imagery

M = Length of stego image (in pixels)

N = Width of stego image (in pixels)

I(x,y) = pixel value of the cover image

I'(x,y) = pixel value on stego image

After obtaining the MSE value, then the PSNR value can be calculated using the formula (8):

$$PSNR = 10 \log\left(\frac{MAXi^2}{MSE}\right) \dots\dots (11)$$

Where:

MSE = MSE value

MAXi = maximum value of the pixel image used.

TESTING AND RESULT

The implementation of application testing will be carried out when all the designed system programs have been completed to find out whether the application is running according to the criteria.

1. Testing the Effect of Thresholds on Message Insertion Capacity.
This test is carried out only looking at the maximum capacity of a digital image using all possible threshold values, table 1 shows the effect of the threshold on the message insertion capacity.

No	Citra Pengujian	Kapasitas maksimal media penyimpan pada Threshold				
		0,1	0.2	0.3	0.4	0.5
1	lglo.bmp (229 KB)	110632	75104	52520	35336	14304
2	Lion.bmp (450 KB)	333048	269120	222240	183568	85296
3	Grayscale-lena.bmp (117 KB)	121904	97280	74832	56240	23128
4	Mobile-phone.bmp (900 KB)	472728	371784	268176	181392	65512
5	Food-salmon.bmp (731 KB)	242520	173968	132464	101072	41952
6	Eiffel-tower.bmp (292 KB)	200064	165432	135456	105760	42944
7	person-holds-a-book.bmp (487 KB)	303496	242040	188008	141832	60600
8	img_5terre.bmp (703 KB)	540728	479600	411616	336992	150048
9	Buildings.bmp (731 KB)	560656	478488	399832	320920	135240
10	Lenna.bmp (768 KB)	516160	445384	371568	296688	128480

TABLE 1 The Effect of Thresholds on Message Insertion Capacity

2. Testing the Effect of Threshold Value on Stego Image quality.

This test is carried out by inserting a message into an image at different thresholds, by entering a message with a size of 20 KB, 40 KB and 80KB and then the PSNR value generated by the image will be calculated. Tables 2, 3, and 4 show the effect of the threshold value on the quality of the Stego Image.

No	Citra Pengujian	Nilai PSNR pada Threshold dengan Ukuran Pesan 20KB				
		0,1	0.2	0.3	0.4	0.5
1	Lenna.bmp (758 KB)	39 dB	43 dB	44 dB	46 dB	47 dB

TABLE 2 PSNR Value at Threshold with Message Size 20KB.

No	Citra Pengujian	Nilai PSNR pada Threshold dengan Ukuran Pesan 40B				
		0,1	0.2	0.3	0.4	0.5
1	Lenna.bmp (758 KB)	36 dB	39 dB	41 dB	42 dB	44 dB

TABLE 3 PSNR Value at Threshold with Message Size 40KB

No	Citra Pengujian	Nilai PSNR pada Threshold dengan Ukuran Pesan 80KB				
		0,1	0.2	0.3	0.4	0.5
1	Lenna.bmp (758 KB)	31 dB	35 dB	37 dB	39 dB	41 dB

TABLE 4 PSNR Value at Threshold with Message Size 80KB

3. Maximum of Insertable Message Character To Maintain Image Quality Testing

This test is carried out to find out the maximum limit of message characters that can be inserted into the image to maintain image quality. Table 15 shows the maximum testing of the character of the message inserted to maintain quality.

No	Citra Pengujian	pesan karakter yang disisipkan agar kualitas citra terjaga	
		25 %	30 %
1	Iglo.bmp (229 KB)	48 dB	47 dB
2	Lion.bmp (450 KB)	31 dB	31 dB
3	Grayscale-lena.bmp (117 KB)	38 dB	37 dB
4	Mobile-phone.bmp (900 KB)	43 dB	43 dB
5	Food-salmon.bmp (731 KB)	38 dB	37 dB
6	Eiffel-tower.bmp (292 KB)	24 dB	23 dB
7	person-holds-a-book.bmp (487 KB)	36 dB	35 dB
8	img_5terre.bmp (703 KB)	27 dB	25 dB
9	Buildings.bmp (731 KB)	29 dB	28 dB
10	Lenna.bmp (768 KB)	36 dB	36 dB

TABLE 5 Message Character Testing to Maintain Image Quality

4. Stego image quality testing

Stego image quality testing is carried out by inserting messages into ten test images of different sizes, then the PSNR value generated by the image will be seen which will affect the image quality. Table 6 shows the quality of the Stego Image results.

No	Citra Pengujian	Nilai PSNR dengan ukuran pesan			
		1 KB	10 KB	20 KB	40 KB
1	Iglo.bmp (229 KB)	61 dB	50 dB	46 dB	36 dB
2	Lion.bmp (450 KB)	58 dB	47 dB	38 dB	34 dB
3	Grayscale-lena.bmp (117 KB)	53 dB	50 dB	37 dB	29 dB
4	Mobile-phone.bmp (900 KB)	65 dB	55 dB	52 dB	45 dB
5	Food-salmon.bmp (731 KB)	65 dB	48 dB	42 dB	36 dB
6	Eiffel-tower.bmp (292 KB)	59 dB	45 dB	37 dB	33 dB
7	person-holds-a-book.bmp (487 KB)	56 dB	45 dB	41 dB	37 dB
8	img_5terre.bmp (703 KB)	65 dB	47 dB	38 dB	33 dB
9	Buildings.bmp (731 KB)	46 dB	39 dB	36 dB	32 dB
10	Lenna.bmp (768 KB)	59 dB	48 dB	44 dB	41 dB

TABLE 6 Stego Image Quality Testing

5. Visual Image Quality Testing

Visual image quality testing on steganographic images is carried out to see if there are differences in the visual appearance of the image before and after the insertion of the message. Table 8 shows the results of imagery quality visually.







No	Citra Asli	Pesan	Stego Image
1	 iglo.bmp	Text 20 KB	 iglo.bmp (hasil pengujian)
2	 buildings.bmp	Text 20 KB	 buildings.bmp (hasil pengujian)
3	 eiffel-tower.bmp	Text 20 KB	 eiffel-tower.bmp (hasil pengujian)

TABLE 7 Stego Image Quality Testing

CONCLUSION

After all stages of testing on the steganography application have been completed, the following conclusions can be drawn:

From several tests that have been carried out, it was concluded that the greater the threshold value used, the better the image quality will be, from testing the maximum character of the message that can be read, it is concluded that the maximum message character that can be inserted so that the quality of the message will maintained is 30% of the maximum capacity of the image, then the larger the size of the message inserted, the quality of the image will decrease, in the visual case it is evident that there can be no visual distinction between the preceding image and the steganographic image, this indicates that the application has been made according to the criteria.

REFERENCES

- [1] Petrus, Johanes. "Implementasi Steganografi Pada Citra Dengan Metode Bit-Plane Complexity Segmentation Untuk Transformasi Data". Citec Journal. Vol. 2, No 3.
- [2] Kartono, Aan. "PENGERTIAN STEGANOGRAFI, JENIS-JENIS, DAN PRINSIP KERJA". <https://www.immersa-lab.com/pengertian-steganografi-jenis-jenis-dan-prinsip-kerja.htm>, 21 Februari 2022.
- [3] Z, Habibi. "Implementasi Metode Bit Plane Complexity Segmentation pada Citra Digital dalam Penyembunyian Pesan Rahasia". Jurnal Means. Vol. 3, No 2.
- [4] Widyanarko, Arya. "Implementasi Steganografi dengan Metode Bit-Plane Complexity Segmentation (BPCS) untuk Dokumen Citra Terkompresi". Bandung : Program Studi Teknik Informatika, Institut Teknologi Bandung. https://informatika.stei.itb.ac.id/~rinaldi.munir/TA/Makalah_TA%20Arya_Widyanarko.pdf
- [5] Munir, R, " Metode BPCS (Bit-Plane Complexity Segmentation)". Bandung: Program Studi Teknik Informatika ITB. <https://docplayer.info/58275901-Metode-bpcs-bit-plane-complexity-segmentation-oleh-dr-rinaldi-munir-program-studi-informatika-sekolah-teknik-elektro-dan-informatika-itb.html.pdf>.
- [6] Widyanarko, Arya. "Implementasi Steganografi dengan Metode Bit-Plane Complexity Segmentation (BPCS) untuk Dokumen Citra Terkompresi". Bandung : Program Studi Teknik Informatika, Institut

Teknologi Bandung.

https://informatika.stei.itb.ac.id/~rinaldi.munir/TA/Makalah_TA%20Arya_Widyanarko.pdf

- [7] Munir, “R. Metode BPCS (Bit-Plane Complexity Segmentation)”. Bandung: Program Studi Teknik Informatika ITB. <https://docplayer.info/58275901-Metode-bpcs-bit-plane-complexity-segmentation-oleh-dr-rinaldi-munir-program-studi-informatika-sekolah-teknik-elektro-dan-informatika-itb.html.pdf>.
- [8] Faruqi, Muhammad Iqbal, “Modifikasi Vigenere Chiper dengan Menggunakan Kunci Bergeser”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2009-2010/Makalah1/Makalah1_IF3058_2010_051.pdf, 1 Maret 2022.
- [9] Haruno Sajati. “Analisis Kualitas Perbaikan Menggunakan Metode Median Filter Dengan Penyeleksian Nilai Pixel”, Jurnal Ilmiah Bidang Teknologi. Vol 10, No 1.