International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 21 (2017) pp. 10999-11006

Comparative Analysis of Steganography Using LSB and Adaptive Method on GIF Image

Iman Teguh Fathurohman, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni

Departmen of Computer Engineering, Faculty of Electrical Engineering,
Telkom University, Bandung, Indonesia.

Abstract

Computer evolution and other supporting devices was already digital, has made digital data more widely used. On the other hand, the ease has raised issues around copyright and digital material ownership rights. The hidden message technique (steganography), is a technique that allows users to hide a message in another message. With such capabilities then copyright information such as the identity of an author, creation date, and others can be inserted or hidden into digital image specially gif image. In this research the steganography method using Least Significant Bit (LSB) and Adaptif which will be applied to gif image. Of these two methods will be compared how many characters from each method can be inserted in the gif image.

Keywords: Steganography, Least significant bit, Adaptive, and GIF Image.

INTRODUCTION

Fast development of information technology is currently supported by the importance of the need for obtaining information. It can be seen from the development of the network internet now is increasing rapidly. Information submitted is not just for everyone's information. Some of the information is only intended for certain people or certain agencies because it is so in the confidential information.

Along with the technological developments, threats to the security of the information needed are getting bigger, especially for the information kept secret. Various threats in cyberspace as hackers, crackers, and carder made people worry about the security of the information sent. It is this concern that makes a little stunted information delivery, while the information was very important to certain people.

The technique of concealing information that was quite famous is steganography. The technique reduces the disadvantages of cryptography which can easily give rise to suspicion. Steganography hiding secret information within other information so that the information can not be known by other people who are not in question.

This technique has a number of methods used to encrypt it. Among others is the LSB (Least Significant Bit) and adaptive.

The purpose of this research is to find out how much the number of characters that can be inserted on a gif image of the media using the LSB steganography method and adaptive.

The study has limits on the following issues:

1) Concealment of a secret message is done by the method of LSB (Least Significant Bit) and adaptive.
2) The file or secret message hidden in the form of a character or text.
3) The Image is used as the carrier's image or stego image of digital image with gif format.

BASIC THEORY

This basic theory section will focus discusses the history of steganography, steganography, steganography property and digital image.

A. History of Steganography

Such as cryptography, the use of steganography actually has been used centuries ago even before the term steganography itself appears. The word steganography (steganography) is derived from the Greece i.e. steganos which means hidden or veiled and grapho, meaning to write, so that more or less means "write posts that are hidden or veiled" (Sellars, 1996). This technique include the myriad methods of communication to hide secret messages. This method including ink that doesn't look, microdots, setting words, digital signatures, hidden line and spectrum of wide communication.

Here is an example of the use of steganography in the past :

1. Steganography has been known by the nation of Greece. Herodatus, ruler of Greece, sending secret messages by using the head of a slave or as media soldiers. In this case, the slave's hair is removed, and secret messages written on scalp slave. When the slave's hair grows, the slaves were sent the secret message behind her hair.
2. The Romans know steganography using an ink looks (invisible ink) to write a message. The ink is made from a mixture of fruit juice, milk, and vinegar. If the ink used to write then writing did not appear. Writing on paper can be

read by means of heating the paper.

3. The method used by the people of ancient Greece is by using a candle as the media hides their message. The message was written on a sheet, the sheet and will be covered with wax to hide messages that you have written. The receiving party will then remove the wax from the sheet to see the message conveyed by the sender.

B. Steganography

Steganography is the art of hiding messages. The goal of steganography is hiding communication for prevent third parties know about the existence of the message [1]. This is in contrast to cryptography, the art of secret messages, which are intended to make the message cannot be read by a third party but does not hide the existence of the secret communication. (Kessler, 2004). Steganography takes two properties, namely holding media and secret messages. Commonly used buffers media is an image, sound, video, or text. Hidden messages can be either an article, picture, list items, program code, or any other message. The advantage of steganography compared with cryptography is that the message sent is not attracting attention to the media holding which carries messages do not cause suspicion for third parties. This is in contrast to cryptography in which ciphertext raises the suspicion that the message is the message confidential. (Munir, 2006, pp.: 302).

According to a (Rinaldi, 2006), there are a few things needed to hide a message that is :

1. Insertion Algorithm (Embeding Algorithm). This algorithm is used to insert a hidden message in a data which will be sent. The insertion process is protected by a key-word so that only people who know the key-word is that can read messages hidden.
2. Detector Function. This Detector function is to restore hidden messages.
3. The Carrier Document. Is the document that serves as the medium used to insert information. This document can be in the form of files such as audio files, video or image (picture).
4. Key Is a keyword which feed into the document useful and used as the verification process when the information will be shown or described.
5. Secret Message/Plaintext is a secret message that will feed into the carrier's document. It is this message that does not want to look and read by people who are not interested.

According to a (Rinaldi, 2006), there are some things that must be owned by a hidden message that is:

1. The hidden message of Robustness and inserted in the data should not change any other information on the data. A hidden message that is said to be strong if the message is only detected by equipment that is trusted and the message cannot be modified or deleted.
2. A hidden message Undetectability shouldn't be detected by people who are not interested. A hidden message is not detected (undetectability) If messages are hidden have the same model. For example, if a component using Steganographic methods sound on digital data for inserting secret messages (messages that are hidden), then those should not have a difference with other sounds on digital data submitted.
3. This concept of Invisibility using the weakness of men, the weakness of the system of vision and hearing loss in humans. A secret message is said to be invisible if the average of the five senses of human beings cannot distinguish a message containing confidential data and data that does not have a secret message when sent.
4. Security A secret message that inserted is said to be safe if the secret message can not be changed or removed when the secret message read.
5. Secure Black-Box Public Detector the detector which is a message that is applied on a hardware (hardware). The device can not be disassembled again in hardware. The secret key to read the hidden message will be saved on the black-box and the key cannot be replaced or deleted. With the presence of black-box it, must be able to withstand the attacks from outside parties to retrieve the secret key or remove the information contained therein.
6. Secure Public Detector Is a more powerful detector concept of all detectors are known by the general public. This detector is present on an application that has a high level of technology. This application can filter out images that have special signs, display information from creator for each image and others.

Steganography scheme can be formulated as follows [10] :

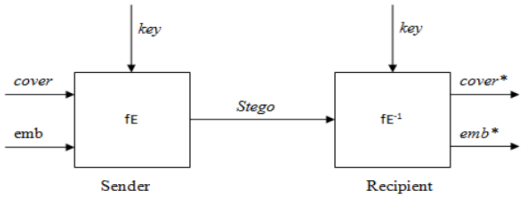

Figure 2.1. Schematic Process Steganography

Where,

fE = function steganography "embedding"

fE-1 = function steganography "extracting"

cover = data on the emb will be hidden

EMB = message will be inserted

Key = fE parameter

stego = cover data with the message that has been inserted.

C. Steganography Property

The following properties contained in the steganography is :

1. Embedded message (hidden text) is the file to be hidden. The file can be a text, video, audio or image.
2. Cover (cover text) Object is a file used as containers to hide the embedded message
3. The Stego Object (stegotext) is a file container that's been given message embedded message
4. Key Stego is the key that is used to insert the message and mengekstrasikan message from the stegotext.

D. Digital Image

This digital image section will focus discusses the Digital Image Representation, Image Histogram, and GIF Image.

1. Digital Image Representation

Digital images can be represented as a matrix of f (x, y) which indexes the rows and columns to identify a point on the image and value of the matrix element is the degree of colour at that point (pixel) [7]. Pixel also represents the contribution of the file size of the image. The values of the intensity of the pixels in the image are mapped to specific bit. The digital image can be defined as a function of two variables, f (x, y) where x and y are the coordinates of the space while the value of f at any given coordinates (x, y) declaring the brightness and image colour information. Digital image shaped matrix size MxN, where M and N high States declare the width of the image.

$$f(x,y)=\begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix}$$

Figure 2.2. Digital Image Matrix Representation [15]

2. Image Histogram

The image histogram is a graph that illustrates the spread of values of the intensity of the pixels of an image. This graph can be used as bookmark levels of brightness and the contrast of the image. On the graph, x-axis (basis) indicates the degree of colour and Y axis (ordinate) shows the frequency of occurrence of the point. When i gray stated level on an image then the probability of i stated:

$$Hi = \frac{Ni}{n} \qquad i = 0,1, \dots \dots L-1 \qquad (1)$$

Description

Hi = Histogram value

Ni = number of pixels that have a gray's degree of i

N = total number of pixels in the image

The information obtained from the Histogram Area is:

- Peak histogram → intensity pixel of the most prominent.
- The width of the peak → range of contrast.
- Over-exposed (too bright) and underexposed (too dark) has a narrow range of contrast.
- A good image of the filling area of the degree of grayish fully and evenly on each pixel intensity values

3. GIF Image

Graphics Interchange Format or often abbreviated GIF is an image file format that was introduced by CompuServe in 1987 to replace the DIB format is only capable of displaying images with black and white only. The GIF file format is one of the most frequently encountered images in the digital world. This occurs because the format is relatively small-sized. For example for the same image, a file with a GIF format can be smaller if compared to the JPG format. This is because the GIF files using only 256 colour palette. So obviously the file size will be smaller. However the 256 colour palette of 256 colours just not absolutely certain. The colour can be chosen from the 24-bit RGB colour palette or it can be inferred that the files with GIF format will get rid of the colour palette is not required and take only 256 colour palette as needed [5].

GIF uses Lossless Compression methods, to make the file size as small as possible. Lossless Compression is a compression does not reduce the quality on the images, but it can minimize the magnitude of the number of files, so there is no data on the disappearances when done compression.

However the format instead of GIF format does not have the drawbacks. The result of the number of colours that only 256 colours just so the format is rarely used for photographic images. Because it's often the image using colour photography that is more than 256 colours. So if the photographic image is represented in the GIF format will experience a decline in the lot of qualities.

STEGANOGRAPHY TECHNIQUES

This steganography techniques section will focus discusses the methods of least significant bit and adaptive method.

A. Methods of Least Significant Bit (LSB)

The simplest approach is to hide the data in the image file is called insertion of Least Significant Bit (LSB). The insertion of the least significant bit (LSB) is a common approach to embed information in media images. Least significant bit (in other words, the 8th bit) some or all of the bytes in an image is converted into a bit of a secret message [11]. When using the 24-bit images, bits of each colour component red, green and blue can be used, as each is shown in the form of bytes. In other words, a person can save 3 bits per pixel. Images with 800 × 600 pixels can save a total amount of 1,440 million bits or 180,000 byte data inserted. In existing methods, it takes the binary representation of the data that will be hidden by the method of LSB. For example, suppose we have three adjacent pixels (nine bytes) with an RGB code follows:

11110101	00010110	10101010
11000100	11111001	00000001
00000001	11110001	00011101

The message will be inserted is the character "Y", which is the value of binary is "01011001", then the resulting image will result in the order of the bits as follows:

11110100	00010111	10101010
11000101	11111001	00000000
00000000	11110001	00011101

The method of this already very common LSB, so a lot of people already know. By using this method, an intruder can easily destroy a message that is in the image. By changing the values of the existing pixels of all the LSB be the value "0" or "1", then the message is corrupted. The destruction of this message just changes a little image quality, i.e. in the range of 1 or-1 on each pixel position.

B. Adaptive Method

Steganography information by means of the insertion of the LSB is performed on a bit-the most insignificant bits of a pixel image so as not to cause a difference in sensing with the human eye. However, steganography does not have enough resilience and easily damaged when facing the digital image processing operations carried out, such as lowpass filtering.

Therefore, to create more robust against attacks steganography, steganography preferably implanted on bit-bit more significant. This has led to a kind of trade-offs because the stylish image steganography produced will look a lot of distortion and contrary to the needs of the unseen by the eye senses. To qualify the solidity and transparency, then inserted steganography adaptively by modifying the intensity of certain pixels as much as possible and

In the process, the adaptive method utilizing sensitivity of human vision system by modifying the level of intensity of the pixels of a digital image block adaptively. In addition to maintaining the level of transparency of steganography in digital imagery, this technique is also reliable in the face of digital image processing in general like cropping, scaling, rotation, low-pass filtering or lossy compression.

The technique of insertion of messages on steganography techniques in penyisipannya can be categorized into two categories, namely:

1) The technique of Adaptive Process message insertion of non technique non adapative not correlating feature on media insertion with a message that will be inserted, in the case of images. An example is on the insertion with the LSB method inserts a message bit-bit randomly in the media insertion.

2) The technique of adaptive process of insertion of messages on Adaptive technique modification media insertion process that occurs at the insertion of the message be correlated with features and image content. This technique of analyzing and selecting pixels that will be inserted into a message, and the pixels which will be pasted depends by the media insertion. An example of this technique can avoid the areas in the image that has the same color (solid color) and so this technique will select pixel based on parity of pixels that will be inserted into the message is compared to the value of the parity of the message will be inserted.

The adaptive method is a method that uses the techniques of Adaptive insertion techniques as his message. This method has the advantage that is on a high level of security for steganography in palette-based images (palette – based image), GIF and PNG images. This method will analyze and select pixels that will not produce a great suspicion by the change of color values, for example, this method will avoid inserting a message in an area that has the same color in an image. On the image of the GIF, adaptive method is called because the insertion and modification of the pixel, this method will select

the colors available in the color table of the inserted image message. Because each GIF image has a color table content.

This method of message insertion capacity depends on the insertion of media, and in some cases, the capacity of a message that can be inserted in an image and in all insertion cannot be calculated before the insertion process began, but can still be conducted analysis about the maximum capacity of the inserted message using the adaptive method. The workings of the adaptive method on the insertion process begin with the selection of pixels that will be inserted by pseudo random messages. The process of inserting a message in Gif image using Adaptive method is as follows:

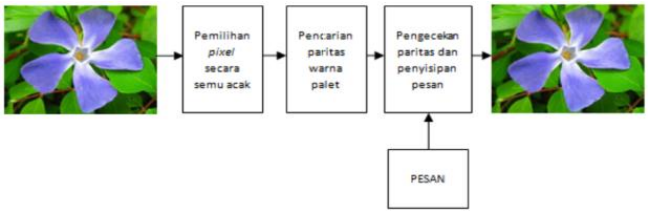

Figure 3.1. the concealment of messages with the adaptive method [15]

The pixel will be inserted a message selected at random from the set of all pixels in the image file. Then the colour palette will be determined the bit using parity equation R + G + B mod 2 [8]. After that held checking each pixel and compare the parity of each pixel with a bit of the message. If the resulting equation of bit, then the pixel is not modified and continues checking the next pixel. If a pixel Selection does not occur will be inserted randomly. A search of parity of colour palette. The selection of a pixel will be inserted randomly. Original image Stego-object messages 16 bit difference, then the color of the pixel in the modification by way of searching for the nearest neighbors of color have the same parity on the color palette.

If the modification process completes, then checking in continue on the next pixel. The procedure of inserting a message ensures that the collections of blocks on the original image and image files that are already on the modifications are identical. This allows the detection algorithms to restore messages from the parity of colour by way of performing a search on a the pixels in a pseudo random pattern similar to that of a pixel selection message will be inserted at the insertion process. The extraction process the messages which can be seen in Figure 3.2 is the opposite of the order in the process of inserting a message in GIF image. At first the story already inserted a message will be read and the pixel will be read and selected at random, using pseudo pseudo random pattern that is similar to the pattern at the time of insertion of the message. After pixel containing a message is identified, then the message can be inserted will be taken.

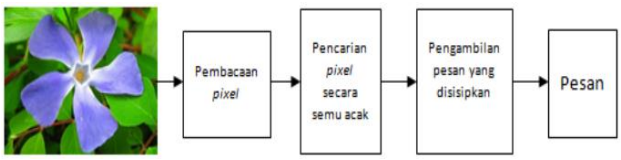

Figure 3.2. the message Extraction using adaptive method [15]

1. Pseudo Random Number Generator

The adaptive method in needed a pseudo random number generator stages to help choose which pixels will be inserted message. Random numbers in question is the number which is not easy in predictions by other parties. However, in practice it is very difficult to get a random number, because there is no computational procedure that can generate random numbers. Random numbers generated by the formula – a mathematical formula is a pseudo random number (pseudo) random numbers, because the resurrected can be repeated periodically.

2. Linear Congruential Generator (LCG)

Linear congruential Generator (LCG) or also called random number generators with congruent – lanjar is one of the oldest and random number generators are well known. LCG can be translated into the following equation :

$$Xn = (aXn - 1 + b) \bmod m \quad (2)$$

Description,

Xn : n random numbers from his series

Xn-1 : previous random numbers

a : multiplier

b : the value increments

m : modulo (a, b, and m are constants)

To start the random numbers it needed a number x 0 are in use as initial values (the bait). The first random number is generated subsequently became the next random number generation seeds. Number of random numbers that are not equal to each other is as much m. The greater the value of m, then the less likely generated repeated values.

3. Error Measurement

The measurement of the quality of the image has been inserted the message done subjectively and objectively. Subjective measurement done by visually sees the difference the shape and colour of the image has been inserted with that yet [9].

Measuring objectively the human rate visualizations are used by calculating the value of PSNR (Peak Signal to Noise Ratio). PSNR values in units of decibels (dB) are counted according the equation:

$$\text{PSNR} = 10\ \log 10\left(\frac{\text{MAX}^2}{\text{MSE}}\right) \quad (3)$$

Where MSE values (Mean Square Error) obtained from the equations:

$$\text{MSE} = \frac{1}{\text{mn}}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|f(i,j) - g(i,j)\|^2 \quad (4)$$

Description:

f : represents the matrix data of our original image

g : represents the matrix data of our degraded image in question

m : represents the numbers of rows of pixels of the images and i represents the index of that row

n : represents the number of columns of pixels of the image and j represents the index of that column

MAX : the maximum signal value that exists in our original "known to be good" image

MSE equation requires two input images, and then looks for its value. After that calculated the value of PSNR. PSNR values are reasonable on the comparison of two image file is above 30 dB.

Because the image of the logo of the paste in the form of binary image format, then the measurement against attacks on stego images used calculation of Bit Error Rate (BER). The smaller the value the results of calculation of BER, then the better the quality of the resulting image. Calculation of the BER is calculated by the following equation:

$$\text{BER}\ (S, S') = \frac{\sum \text{Pi}}{\text{N}} \quad (5)$$

S is the original and S ' steganography is steganography extracted. N is the number of bits and the value of pi is defined as follows :

pi =1 for Si ≠ Si'

pi = 0 for Si = Si'

The test is said to be successful if each way, the obtained results using adaptive method that has been implemented in accordance with the following equation :

$$\text{P} = \frac{\text{m x n}}{8} \quad (6)$$

Where,

p : message size

m : length of the image size in pixels

n : size of image width in pixels

EXPERIMENTS AND RESULTS

This steganography techniques section will focus discusses the steganography method of least significant bit, steganography adaptive method and PSNR and MSE stego image.

A. Steganography Least Significant Bit (LSB) Method

In this study individually-focused on how much the maximum number of characters or the length of a message that can be inserted in gif image. The methods used to obtain the results of the use of manual calculations with formulas:

$$\text{P} = \frac{\text{m x n}}{8}$$

Retrieved data results from experiments that have been done before with to find out what the maximum number of characters that can be inserted on a gif image if taken five sample gif images with different image size in the following table :

Table 4.1. experimental results using the method of Least Significant bits (LSB)

Image Size	The Number Of Characters
4 x 4 pixel	2
6 x 6 pixel	3
8 x 8 pixel	8
10 x 10 pixel	12
12 x 12 pixel	18

B. Steganography Adaptive Method

In this study individually-focused on how much the maximum number of characters or the length of a message that can be inserted in gif image. The methods used to obtain the results of the use of manual calculations with formulas:

$$\text{P} = \frac{\text{m x n}}{8}$$

Retrieved data results from experiments that have been done before with to find out what the maximum number of characters that can be inserted on a gif image if taken five sample gif images with different image size in the following table:

Table 4.2. experimental results using the adaptive method

Image Size	The Number Of Characters
4 x 4 pixel	2
6 x 6 pixel	3
8 x 8 pixel	8
10 x 10 pixel	12
12 x 12 pixel	18

C. PSNR and MSE Stego Image

After doing the insertion on the sample image with each image

is inserted the characters ' S ' and ' K ', then the PSNR value can be obtained and the following MSE:

Table 4.3. PSNR and MSE values

Image Size	MSE	PSNR
4 x 4 pixel	0,3125	58,2338
6 x 6 pixel	0,166666667	63,69382862
8 x 8 pixel	0,09375	68,69137808
10 x 10 pixel	0,05	74,15140352
12 x 12 pixel	0,041666667	75,73502844

ANALYSIS AND DISCUSSION

From experimental results that steganography has been done before against gif image about how much the message maximum number of characters that can be inserted by the method of least significant bit (LSB) and the adaptive method, it can be seen by comparison the number of characters of both these methods in the following figure:

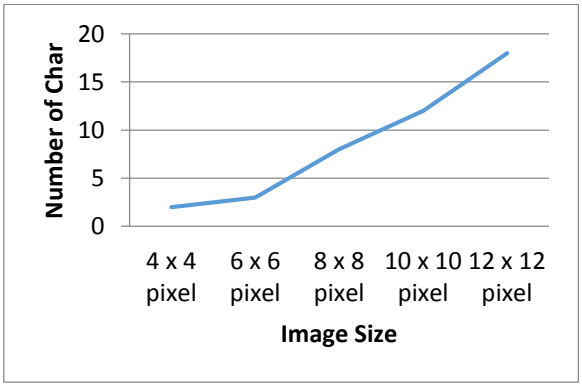

Figure 5. comparison chart the adaptive method with the LSB test

From the graph above it can be seen that the experimental results about a lot of the number of characters that can be inserted on a gif image produces the same results. This is because the formula that is used in the same two methods to produce the same value.

But in terms of the durability of the image quality better than does the adaptive method of least significant bit (LSB). In this case because the adaptive method utilizing the sensitivity of human vision system by modifying the level of intensity of the pixels of a digital image block adaptively. In addition to maintaining the level of transparency of steganography in digital imagery, this technique is also reliable in the face of digital image processing in general like cropping, scaling, rotation, low-pass filtering or lossy compression.

Results from Table 4.3 can be analyzed that the larger the size of a logo that will inserted then MSE values will be even greater, because of the increasingly troubled by media imagery modifications and insertion of bits is done, if comparing with the value of the initial media image.

In contrast to the value of PSNR. If more largest size of the logo is inserted, then the a small value of PSNR. Save the results of image media the initial value is inversely proportional to MSE values PSNR.

CONTRIBUTION

This research contributes to a form of steganography techniques suitable to use on gif image. because generally it's been an awful lot of steganography is applied to the digital image formats such as bmp, jpeg, or png. While the steganography is applied to the image as a gif is extremely rare. So this journal can give references or suggestions or good steganography method of suit against the gif image to be applied. In this study used methods of least significant bit (LSB) and adaptive method on the application of gif image. Of research results obtained by the maximum number of characters that can be inserted as well as value of PSNR and MSE which produces good value for a method of steganography is used. So it can be inferred that the least significant bit (LSB) method and also the adaptive method is very suited towards the application of steganography in gif image.

In the journal "Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm" this is only described steganography technique on jpeg RGB image [3]. So for gif image format is not explained in detail how steganography technique on image gif format.

In this journal described in detail about steganography techniques on gif imagery. Where steganography technique used by using two method that is least significant bit (LSB) and also Adaptive method. Both methods are usually applied only to jpeg, bmp, and png image formats. Therefore in this journal focus tehadap gif image.

CONCLUSION

Conclusions after conducting experiments and analysis as well as the discussion towards how much the number of characters that can be inserted on the application of steganography using method of least significant bit (LSB) and adaptive is the number of characters the maximum that can be pasted similar or the same value. This is the image object in because of use gif images is such that for the formula of finding the maximum number of characters the same no difference.

But in terms of the durability of the gif image itself better than the adaptive method on the method of least significant bit (LSB). This is due to the adaptive method utilizing sensitivity

of human vision system by modifying the level of intensity of the pixels of a digital image of the block being implanted on the significant bits.

REFERENCES

[1] N.F. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer Journal. 1998.

[2] Munir, Rinaldi, "Criptography", Bandung : Informatics. 2006.

[3] Nurhayati and S. S. Ahmad, "Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm," Cyber and IT Service Management, International Conference on, 2016.

[4] Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", IEEE Security and Privacy Journal, 2003.

[5] CompuServe, "Graphics Interchange FormatTM," Ohio: CompuServe Incorporate, 1989.

[6] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques Sign In or Purchase," Computer Communication and Informatics (ICCCI), 2014.

[7] Acharya, Tinku and Ray, K, Ajoy, "Image Processing Principles and Applications," A John Wiley & Sons, Inc., Publication.

[8] J. Fridrich, "A New Steganographic Method for Palette-Based Images," Center for Intellegent Systems, SUNY Binghamton, 1998.

[9] Pratt K, William. "Digital Image Processing Forth Edition," PixelSoft, Inc.Los Altos, California.

[10] Munir, Rinaldi, "Steganography dan Watermarking," Bandung: Institut Teknologi Bandung. 2004.

[11] P. Joseph and S. Vishnukumar, "A study on steganographic techniques," Communication Technologies (GCCT), 2015.

[12] Sumeet Kaur, Savina Bansal, R. K. Bansal, "Steganography and Classification of Image Steganography Techniques ", International Conference on Computing for Sustainable Global Development , IEEE, 2014.

[13] Sutaone, M.S., Khandare, M.V.,"Image based steganography using LSB insertion technique ", IET International Conference on Wireless, Mobile and Multimedia Networks, 2008.

[14] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, 2001.

[15] Deni Azhari, Tjokorda Agung, and Retno Novi Dayawati, "Analysis and Implementation of Adaptive Steganography on Digital Image", Telkom Institute of Technology.

[16] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, 1998.