Journal of Engineering and Applied Sciences 14 (14): 4849-4852, 2019
ISSN: 1816-949X

Analysis of JPEG Image Steganography using Least Significant Bit Method

Jordy Ardian Bagaskara, Tito Waluyo Purboyo and Ratna Astuti Nugrahaeni
Department of Computer Engineering, Faculty of Electrical Engineering,
University of Telkom, Bandung, Indonesia

Abstract: The use of digital media as a means of information exchange is common in the present. There is certain information that can be called confidential information. Indicated by a person or a particular party to another party. In order to avoid any information leakage required a special technique in the delivery of this confidential information. Steganography is a technique that can protect this secret information. The meaning of steganography in Greek is the concealment of a writing or data. Secret messages can be hidden in media form such as text, image, audio and video. In use on imagery there is a method called Least Significant Bit (LSB). LSB is the basic method used. This method replaces the value of pixels in a digital image with secret data using ASCII value. Changes in the color of the image are not visible to the eye due to the replacement of small pixel values. In this study, we will discuss the use of steganography on JPEG image with LSB method. To determine whether messages can be well hidden and stego images still have good quality.

Key words: Steganography, JPEG image, least significant bit, image steganography, messages, hidden

INTRODUCTION

In modern times, the use of technology is becoming a common practice for humans, especially in the exchange of information. Information is a message in the form of speech or expression or expression can consist of symbols or meanings that can be interpreted from a message or a collection of messages.

An information may contain an important message and sometimes there is special information that is only shown for personal purposes need a special way in the delivery of such information, so that, the security and the interests of information can be delivered without any person or other party not authorized to know the specific information (Haines and Chuang, 1992).

Cryptography is a technique that has been done in ancient times (Egypt, CA 1900 BC) where found chipper text engraving or a technique of randomizing a message using a particular pattern, modern cryptography refers more to the mathematical theory and practice of computer science (Petitcolas *et al*., 1999).

Steganography is a special form of cryptography in which this technique conceals a file, message, image or video on other digital media in the form of other files, messages, images or video. First recorded in 1499 by Johannes Trithemius (Cox, 2008).

There are many algorithms used in steganography techniques this research uses one of the basic techniques, namely least significant bit to find out what pattern is the basis of this technique with the use of image media as the main media to know the results of message concealment, the level of security and the difference induced on the original image and steganographic image with the technique (Cox, 2008).

MATERIALS AND METHODS

Steganography: Steganography gives the advantage over cryptography that secret messages that are not attractive to itself as objects, information can not see visually and quality that does not significantly influence because of the application of steganography using Kerckhoffs principle (Fridrich *et al*., 2004). The steganography process is shown in Fig. 1:

- Media: Media on steganography can be either an image, audio or video
- Stegano key: The key used for determining the location or security of the media to be used
- Embedded data: Data to be hidden can be text, image or audio (Anonymous, 1986)

In the implementation there are two main processes, namely embedding and extracting. Embedding is the process of concealment of data on the media using the stegano key from this process will be generated stego-media.

Corresponding Author: Jordy Ardian Bagaskara, Department of Computer Engineering, Faculty of Electrical Engineering, University of Telkom, Bandung, Indonesia

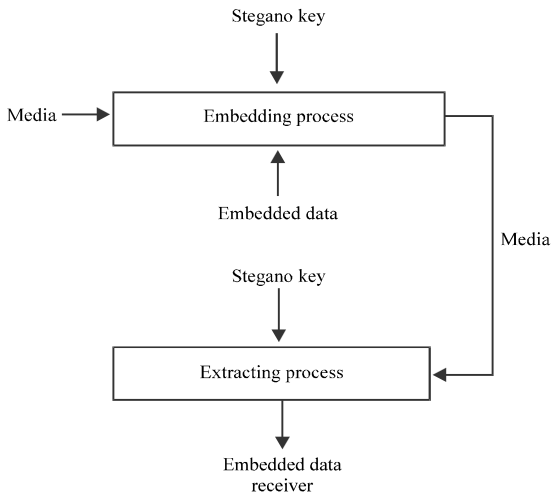

Fig. 1: Steganography process

In this study, the media used are images with JPEG format where the type of image is the most commonly used in this modern era (Hakim 2007; Pahati 2007). The second process is an extracting process where this process is a data retrieval that is contained in the stego-media, stegano key is required as the primary key to determine the location of the data, media and stegano keys must be the same as that used in the embedding process. In this study, the expected data is a text message contained in JPEG image media.

Least significant bit: Least Significant Bit (LSB) is one of the steganography techniques on image media which is the simplest and most basic technique this technique requires the pixel value of an image as the location of steganography determination (Jennings, 2004). With the known pixel value, LSB processes the final value of each existing pixel thereby changing the value of the small value end resulting in a change in the pixel color that is not very significant, especially for the direct view by the human eye in general (Bagaskara *et al*., 2017). Here is a brief illustration of the use of the LSB technique.

There are 3 pixel values in the image:

1110000**1**	1010001**0**	1101110**1**

The underlined value represents the least significant bit value. This value is used by the LSB technique by changing the last numbers on each pixel in the image used (Adiyan *et al*., 2018). Next explanation on how to conceal messages on LSB techniques. In the 4×4 image resolution the text of the message "x" is concealed:

"x" in binary = 01111000

Pixel value if 4×4 images:

10100010	11101101	10011111	10011100
11110110	10011100	10110010	11011101
11001100	11010001	11110000	11101111
10001111	10010001	11101010	11100000

Next, change each LSB to an existing pixel value until all binary values in "x" enter in the 4×4 image pixel value.

The result is:

1010001**0**	1110110**1**	10011111	10011100
1111011**1**	1001110**0**	10110010	11011101
1100110**1**	1101000**0**	11110000	11101111
1000111**1**	1001000**0**	11101010	11100000

Thus, the color of some pixels in the image has changed but on the result the change is not too significant because the pixel value changed is only the smallest value of the 4×4 resolution image.

RESULTS AND DISCUSSION

Embedding and extracting discussion

Cover image: This research uses four JPEG images with different file size and resolution. Starting from the smallest image with 88.7 kB file size and 750×652 resolution to the largest image with file size 982 kB and resolution 1984×1856. These images are used because it is a common image that is widely circulated on the internet (Table 1).

Embedding process: The program used in this study is MATLAB Version 9.0.0, the use of MATLAB intended for image processing to produce value and maximum results. In the embedding process a secret text message will hide the image. The images and messages used will vary to find out how successful they are. The overall results in this process can be seen in Table 2.

After the embedding process it is generated that all images can accommodate secret messages. Thus, the image used is of good quality. Color changes that occur

Table 1: Cover image, file size and resolution

Image	File size (kB)	Resolution
 cake.jpg	88.7	750×652
 udon.jpg	140	960×720
 shibuya.jpg	515	1600×900
 lake.jpg	982	1984×1856

Table 2: Cover image, message and result

Cover image	Message	Result
 cake.jpg	Text: "Never trust a man with no beard"	Accepted
 udon.jpg	Text: "Call 1-844-788"	Accepted
 shibuya.jpg	Text: "Go to blue coral club"	Accepted
 lake.jpg	Text: "Stage 4, at 4 PM"	Accepted

in the image is not too visible to the eye thus, generated stego-image of good quality. With the success of the embedding process, the resulting steganographic image with a secret message in it there is a change in image file size, Table 3 shows the size changes that occur in all 4 images.

The image file size change in Fig. 2 is caused by changes in some pixel values in the image, the file size tends to increase due to changes in the embedding process by the program and the desired result changes in

Table 3: Cover image size and stego image size

Image	Cover image size (kB)	Stego image size
 cake.jpg	89	787
 udon.jpg	140	1297
 shibuya.jpg	516	3339
 lake.jpg	982	7803

Table 4: MSE and PSNR

Image	MSE	PSNR (dB)
cake.jpg	0.0021	74.9850 dB
udon.jpg	0.0127	67.0982 dB
shibuya.jpg	0.0509	90.7199 dB
lake.jpg	0.0059	70.4270 dB

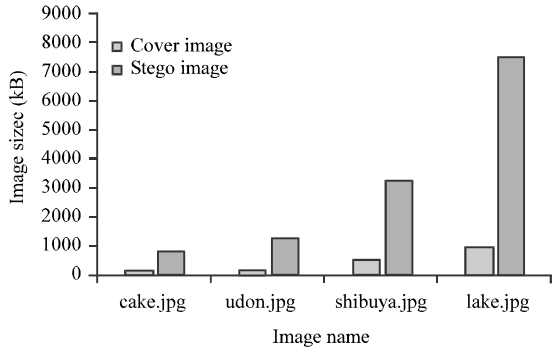

Fig. 2: Cover and stego file size comparison; Cover image size and stego image size

JPEG format, so, the program recalculates to produce the desired format. Table 4 shows the MSE and PSNR values of each image used (Table 3).

Extraction process: In the extraction process, the image that has been generated in the embedding process is checked to find out whether the message is actually hidden inside it and the overall text of the message is still of good quality with readability of all messages.

Table 5 shows that every secret message contained in all 4 images can be read and the message

Table 5: Stego-image, result and hidden message

Stego image	Result	Hidden message
 cake.jpg	Legible	Text: "Never trust a man with no beard"
 udon.jpg	Legible	Text: "Call 1-844-788"
 shibuya.jpg	Legible	Text: "Go to Blue Coral Club"
 lake.jpg	Legible	Text: "Stage 4, at 4 PM"

is still of good quality without any change to the text character. Thus the extracting process can be said to be successful.

CONCLUSION

From the analysis of steganography performed on JPEG image using LSB method, the following results are obtained. Embedding process is done on 4 JPEG image format with different file size, resolution and message. The process successfully executed. There are changes that occur in the 4 images, namely the file size where the file size tends to rise from the previous size this is due to changes in color and the process of calculating JPEG format. The extracting process is performed on all 4 images, resulting in the successful embedding process in which the message is successfully hidden and in extracting the message the message can be read properly without any character changes in the secret message.

REFERENCES

Adiyan, D.Z., T.W. Purboyo and R.A. Nugrahaeni, 2018. Implementation of secure steganography on jpeg image using LSB method. Intl. J. Appl. Eng. Res., 13: 442-448.

Anonymous, 1986. Four coded character set-7-bit American National Standard code for information interchange. American National Standard Instutute, New York, USA.

Bagaskara, J.A., T.W. Purboyo and R.A. Nugrahaeni, 2017. Analysis of JPEG image steganography using spread spectrum method. Intl. J. Appl. Eng. Res., 12: 13944-13950.

Cox, I., 2008. Digital Watermarking and Steganography. Morgan Kaufmann Publishers Inc., San Fransisco, USA.

Fridrich, J., M. Goljan and D. Soukal, 2004. Searching for the stego-key. Proceedings of the International Conference on Security, Steganography and Watermarking of Multimedia Contents VI Vol. 5306, June 22, 2004, SPIE, San Jose, California, USA., pp: 70-83.

Haines, R.F. and S.L. Chuang, 1992. The effects of video compression on acceptability of images for monitoring life sciences experiments. MCS Thesis, NASA, Washington, D.C., USA.

Hakim, M., 2007. [Study and implementation of steganography LSB method with preprocessing data compression and container expansion]. Master Thesis, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Bandung Institute of Technology, Bandung, Indonesia. (In Indonesian)

Jennings, T., 2004. An annotated history of some character codes or ASCII: American Standard Code for Information Infiltration. Am. Stand. Code Inf. Infiltr., 1: 1-11.

Pahati, O.J., 2007. Confounding carnivore: How to protect your online privacy. AlterNet Media, Washington, DC, USA.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.