VOL. 14, NO. 15, AUGUST 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ANALYSIS AND IMPLEMENTATION OF STEGANOGRAPHY ON JPEG IMAGE USING LSB METHOD AND F5 WITH AES CRYPTOGRAPHY

Danny Adiyan Z. and Tito Waluyo Purboyo
Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia
E-Mail: dannyadiyan@gmail.com

ABSTRACT

Steganography is a technique used to hide information on a medium. Media that can be used in the form of text, image files, audio and video files. In its use the insertion of messages or information is done by making small changes to the media. In this research will be done image steganography implementation using LSB and F5 method. To strengthen information security, this research also used one of cryptography method that is AES-128. From the steganography image results will be calculated the value of MSE and PSNR to determine the quality of the image, and also the results of steganographic images will be tested using salt and pepper noise to see the quality of the image after being given noise.

Keywords: steganography, JPEG, least significant bit, F5 algorithm, MSE, PSNR.

INTRODUCTION

Information Technology is growing rapidly. Includes the most frequently used information or messaging exchange today. As technology develops, many people are always trying to commit crimes such as theft of information that is not their right.

Humans are social beings who always communicate with each other. Many ways and forms of communication made by humans. Everyone has their own interests to communicate and sometimes they want to exchange confidential information.

To overcome the problems of human needs in exchanging confidential information, one way that can be used is steganography. Steganography is a technique for hiding / inserting information on a media (cover media). The media used can be image files, text files, audio files and video files [1]. Image Steganography takes advantage of the human eye's weakness in seeing an image.

Steganography is the art of writing or hide a message in a way, that besides the sender and the receiver that no other party can know or be aware of the existence of an information or a confidential message. The word steganography comes from the Greek word steganos which means hidden and graphein which means to write [2].

Here are some commonly used steganography techniques:

a) Subsitution technique, by making changes to certain pixels in an image.
b) Transform Domain Techniques, by storing confidential information through space transformation.
c) Spread Spectrum, in this technique the secret information is stored and distributed at a certain frequency.
d) Statistical Techniques, in this technique the data is inserted through the conversion of statistical information on the files used. Files are used to form blocks, where block blocks store pixel information containing secret messages.
e) Distortion Techniques, this technique hides information based on signal distortion.
f) Cover Generation Techniques, this technique hides secret messages that match the image cover [3].

In steganography, existence of information can not be seen visually and cover media quality has not changed significantly. The advantage of steganography is that a secret message does not attract the attention of others.

illustration of steganography in general, can be seen in Figure-1.

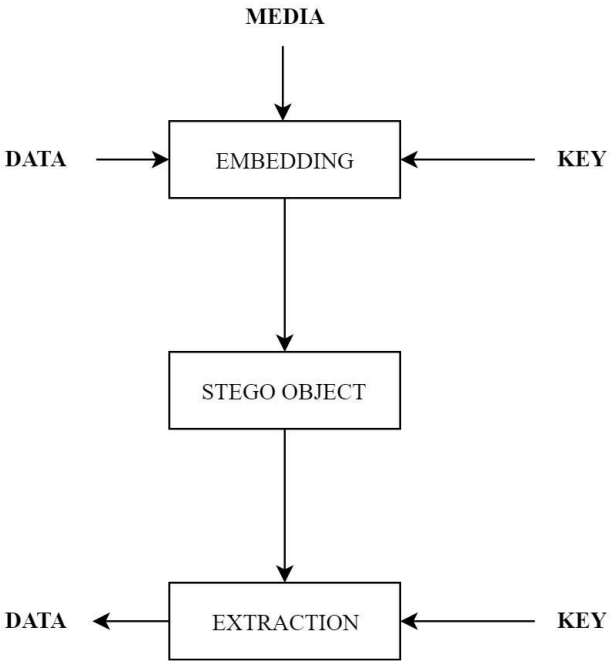


Figure-1. Steganography Process.

This paper will discuss about steganography in image. image to be used is JPEG image. JPEG is one of the compression methods used in bitmap files. Bitmap is a file that has a large size, which makes the bitmap becomes

less practical in the exchange of data / information. JPEG compression scheme making the file size smaller and more practical.

The Information file in this steganography process, used a .txt file. This information file before inserted in an image will be encrypted using AES-128.

AES is a symmetry cryptographic algorithm. This algorithm uses the same key during encryption and decryption, its input and output are blocks with a certain number of bits. AES has a standard block size, which is 128, 192, and 256 bits. With each block size will determine the number of processes passed in the process of encryption and decryption [4].

Table-1. AES Block Size.

Block Size	AES - 128	AES - 192	AES - 256
Key Length	4	6	8
Key Size	4	4	4
Round	10	12	14

The input and key data blocks are operated in the form of arrays. Each member of the array before producing the chipertext output is called the state. Broadly, each state will go through 4 processes, namely:

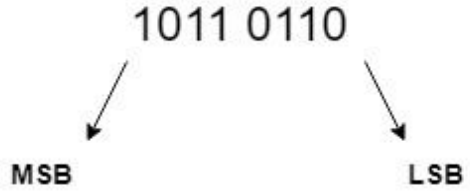
a. Add Round Key
b. Sub Bytes
c. Shift Rows
d. Mix Columns

In this simulation Encryption only affects the file to be inserted.

METHOD

In this paper, steganography method used is LSB (Least Significant Bit) and F5.

Least Significant Bit is a method often used in steganography techniques [5]. LSB exploits the last bit of a pixel by increasing or decreasing 1 value. When the LSB value changes, the changes that occur in the pixel are not very meaningful. The steganography technique of the image utilizes the weakness of the human eye to see small changes in an image. The resolution and color depth of an image affects the size of the information that can be inserted.



The insertion process on LSB method can be seen in the following illustration:

A 3x3 pixel RGB image will be inserted an information is character 'd'.

d = 0110 0100

	Red	
11011010	11001010	01101011
10010101	10110100	10011011
11100010	11011011	11101001
	Green	
11011010	11001010	01101011
10011101	10110100	10011011
11110010	11011010	11101201
	Blue	
11011010	11001010	01101011
10010101	10110110	10011011
11100010	11011011	11101001

Then the byte of character 'd' will be inserted on the lsb of each pixel in the image.

	Red	
1101101**0**	1100101**0**	0110101**0**
1001010**1**	1011010**0**	1001101**0**
1110001**1**	1101101**1**	11101001
	Green	
11011010	11001010	01101011
10011101	10110100	10011011
11110010	11011010	11101201
	Blue	
11011010	11001010	01101011
10010101	10110110	10011011
11100010	11011011	11101001

F5 is a steganography method performed during the JPEG encoding process. The process can be seen on Figure-2.

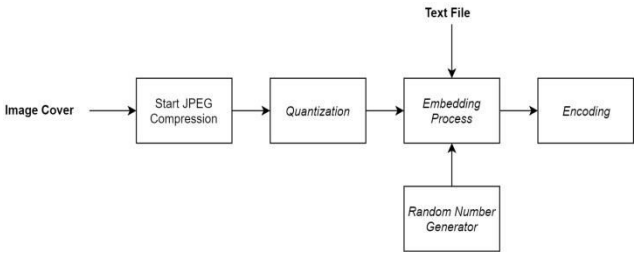


Figure-2. F5 Steganography.

Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) are used to compare the results of image processing with original images that have similarities between the two images.

Mean Square Error (MSE) is the sigma of the number of errors between the result image processing with the original image.

$$MSE = \frac{1}{(N \times M)^2} \sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} - Y_{ij})^2 \quad (1)$$

Peak Signal to Noise Ratio (PSNR) is a comparison between image quality of reconstruction with original image. The term Peak Signal to Noise Ratio (PSNR) is a term in engineering, which expresses the comparison between the maximum possible signal strength of a digital signal with the noise power affecting the correctness of the signal [6].

$$PSNR = 10 \log_{10} [\frac{I^2}{MSE}] \quad (2)$$

RESULTS

Simulation 1: The simulations use the LSB method on five different images and different resolution sizes, 200 x 200 pixels, 400 x 400 pixels, 600 x 600 pixels, 800 x 800 pixels, 1000 x 1000 pixels with 12 characters of message/ data. The test result can be seen on Table-2.

Table-2. MSE and PSNR Value from Simulation 1.

File Name	Resolution (pixel)	Message Size	MSE	PSNR (dB)
daun.jpg	200 x 200	12 Char	0,00318333	73,102
roof.jpg	400 x 400		0,0008	79,099
tree.jpg	600 x 600		0,000374	82,4012
cat.jpg	800 x 800		0,000189	85,3647
rooftelu.jpg	1000 x 1000		0,000133	86,8923

From Table-2 we can see the result of the simulation. Simulation is done to see the effect of image and resolution to the quality of stego image produced. Image quality can be seen from the value of MSE and PSNR obtained. The greater the resolution of a cover image, the better the resulting steganography image quality.

Simulation 2: The simulation use the LSB method on the same five images and the same resolution size is 600 x 450 with the number of message characters that is 14 characters, 12 characters, 10 characters, 8 characters, 6 characters. Obtained test results as in Table-3.

Table-3. MSE and PSNR Value from Simulation 2.

File Name	Resolution (pixel)	Message Size	MSE	PSNR (dB)
penampung.jpg	600 x 450	14 Char	0,000493827	81,1951
		12 Char	0,000483951	81,2828
		10 Char	0,000482185	82,2717
		8 Char	0,000283951	83,5984
		6 Char	0,000277778	83,6938

From Table-3 we can see the results of the simulation. The simulation is done to see the effect of message size on the resulting stego image quality. Image quality can be seen from the value of MSE and PSNR obtained. The smaller the message size the better the quality of the steganography image.

Simulation 3: The simulations use the F5 method on five different images and different resolution sizes, 200 x 200 pixels, 400 x 400 pixels, 600 x 600 pixels, 800 x 800 pixels, 1000 x 1000 pixels with 12 characters of message/ data. The test result can be seen on Table-4.

Table-4. MSE and PSNR Value from Simulation 3.

File Name	Resolution (pixel)	Message Size	MSE	PSNR (dB)
pancing.jpg	200 x 200	12 Char	0,00323333	73,0343
kucing.jpg	400 x 400		0,0007875	79,1683
mancing.jpg	600 x 600		0,000363889	82,5211
blackcat.jpg	800 x 800		0,000221354	84,6799
kucing2.jpg	1000 x 1000		0,000125333	87,1501

From Table-4 we can see the result of the simulation. Simulation is done to see the effect of image and resolution to the quality of stego image produced. Image quality can be seen from the value of MSE and PSNR obtained. The greater the resolution of a cover image, the better the resulting steganography image quality.

Simulation 4: The simulation use the F5 method on the same five images and the same resolution size is 600 x 450 with the number of message characters that is 14 characters, 12 characters, 10 characters, 8 characters, 6 characters. Obtained test results as in Table-5.

Table-5. MSE and PSNR Value from Simulation 4.

File Name	Resolution (pixel)	Message Size	MSE	PSNR (dB)
pemandangan.jpg	600 x 450	14 Char	0,00044321	81,6647
		12 Char	0,000440741	81,689
		10 Char	0,000431852	81,7808
		8 Char	0,000271605	83,7914
		6 Char	0,000267901	83,8511

From Table-5 we can see the results of the simulation. The simulation is done to see the effect of message size on the resulting stego image quality. Image quality can be seen from the value of MSE and PSNR obtained. The smaller the message size the better the quality of the steganography image.

CONCLUSIONS AND FUTURE WORK

In this paper, we perform steganography simulations using LSB and F5 methods. There have been 4 simulations of both methods. From the simulation results obtained, it can be concluded the resolution size of an image will affect the quality of steganography image. The greater the resolution of an image (with the same message size) the better quality of the steganography image. From the simulation results can also be concluded that the larger size of the message to be inserted in a cover image (the same image and resolution) will decrease the quality of the steganography image.

For the future work, it is expected that simulation can not only be done on RGB image but also on grayscale image, and expected to produce better steganography image quality.

REFERENCES

[1] I. Gede Arya Putra Dewangga, Tito Waluyo Purboyo, and Ratna Astuti Nugrahaeni. 2017. A new approach of data hiding in BMP image using LSB steganography and caesar vigenere cipher cryptography. International Journal of Applied Engineering Research. 12(21): 10626-10636.

[2] V. Aditya, Yogie, Andhika Pratama and Alfian Nurlifa. 2010. Studi Pustaka untuk Steganografi dengan beberapa metode. Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

[3] Bogy Oktavianto, Tito Waluyo Purboyo and Randy Erfa Saputra. 2017. A Proposed Method for Secure Steganography on PNG Image Using Spread Spectrum Method and Modified Encryption. International Journal of Applied Engineering Research. 12(21): 10570-10576.

[4] DAEMEN Joan; RIJMEN Vincent. 2013. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.

[5] Cox Ingemar J. 2008. Digital Watermarking and Steganography. Burlington, Morgan Kaufmann Publisher.

[6] Sutardi Sutardi and Muhammad Rezqy. 2015. Implementasi teknik visible watermarking dengan metode one-to-one mapping pada citra digital. DINAMIKA–Jurnal Ilmiah Teknik Mesin 7.1.

[7] Westfeld A. 2001. F5-a steganographic algorithm: High capacity despite better steganalysis. In 4th International Workshop on Information Hiding.

[8] Suhartono, Derwin, Afan Galih Salman and Christian Octavianus. 2012. Aplikasi Penyembunyian Pesan Pada Citra JPEG Dengan Algoritma F5 Dalam Perangkat Mobile Berbasis Android. Seminar Nasional Aplikasi Teknologi Informasi (SNATI).

[9] Aryfandy Febryan, Tito Waluyo Purboyo and Randy Erfa Saputra. 2017. Steganography Methods on Text, Audio, Image and Video: A Survey. International Journal of Applied Engineering Research. 12(21): 10485-10490.