Journal of Engineering and Applied Sciences 14 (21): 7821-7827, 2019
ISSN: 1816-949X

Analysis of Steganography on PNG Image using Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)

Priyandanu Filzasavitra, Tito Waluyo Purboyo and Randy Erfa Saputra
Department of Computer Engineering, Faculty of Electrical Engineering,
Telkom University, Bandung, Indonesia
priyandanuf@student.telkomuniversity.ac.id

Abstract: As technology and information develop, we need to increase the attention to the system's security of the technology we use in our daily lives. For example, insertion of data and information we get from sharing media. Therefore, we can use steganography. Steganography is a technique of hiding data and information into a digital media such as text, images, video and sound. This study also discusses the method that will be used for the application of steganography with Portable Network Graphics (PNG) format. The method is Least Significant Bit (LSB). This study also discusses graphic image quality analysis using Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) method.

Key words: Steganography, LSB, PNG, PSNR, MSE, information develop

INTRODUCTION

In the era that has been using the internet, there are many ways to secure a secret message for communication such as watermarking, cryptography and steganography. Delivery of data or messages through the public such as the internet can be stolen or manipulated. Therefore, this knowledge must be developed in view of the many fatal internet crimes (Sari *et al*., 2017). One of them is steganography. Steganography is detected, if the secret information is known, the secret key is shared between sender and receiver. Steganography is an art or science used to hide secret messages, so that, the existence of messages can't be detected by the human senses. Broadly speaking steganography method consists of 2 main parts (Akhtar *et al*., 2017), namely the process of data hiding (hidden message) and the process of returning the data to the original form (reveal message). Both processes are done by using a secret key that will be used in the process to improve data security.

In general, digital images are stored as arrays in computer systems consisting of a limited number of elements. Each element has a specific location and value, known as pixels. In the case of 24-bit color images, each pixel includes three color components: red, green and blue. So, three bytes (24 bit) look at each pixel to show the intensity of this color. Media with or without information is called stego-media or media cover (Lee and Tsai, 2010). The media used is generally different from the media-media used to carry confidential information. The most common image media formats used in steganography are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) and Portable Network Graphics (PNG) (Rohayah, 2015). So, the function of steganography is as techniques hide messages using other media, so that, confidential information can't be seen clearly. Steganography can also be done in domain space (Patel and Meena, 2016).

Lots of studies that discuss how to use steganography by using various methods contained in steganography. The media to be used is the picture. The method to be used in this research is by using Least Significant Bit (LSB) method. Based on the background of this problem, steganography with LSB method is needed because the existence of a secret message is known only to the sender and recipient of the message (Singh and Sharma, 2016). So, the main purpose of this research is to know the comparison of images before and after inserted a secret message and evaluate a picture quality before and after message inserted by using the method of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).

MATERIALS AND METHODS

Steganography: Steganography comes from Greek which consists of the steganos word which means is hidden and

Corresponding Author: Priyandanu Filzasavitra, Department of Computer Engineering, Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia, priyandanuf@student.telkomuniversity.ac.id

graphien which mean is writing (Rohayah *et al*., 2015). So, it can be interpreted to be a hidden text. So, it can be concluded that steganography is a science that studies the technique of developing secret messages in other messages, so that, others will not know that there is a secret message in the message they read (Zhou *et al*., 2016).

The process concealment of data on the method of steganography is one part that plays an important role in the overall process where in this study, data hiding which is the core of the steganography method is done. In the process of concealment of this data is required accuracy in the calculation of color bits and bits of data because if there is little error on the calculation it will result in damage data sent, so that, data will not be restored into the original form. In addition, the measure of success in the steganography method is also influenced by the process of data hiding where the results of the process of hiding the data in the form of stego-image must resemble the original image (cover image), so that, no suspicion from others who see it. In addition, the data efficiency factor also needs to be considered in the concealment of data in relation to the comparison of the amount of data that is hidden with the quality of the resulting stego-image (the larger the data is hidden the lower the resulting stego-image quality). The amount of data that can be generated by the steganography method generally, reaches about 5-10% of the digital image file size (Juarez-Sandoval *et al*., 2017).

Least Significant Bit (LSB): This method is very popular and the simplest of other methods to image. This method also has the lowest difficulty level and requires high capacity (Akhtar *et al*., 2017). LSB does not affect the human senses though because the comparison of images that have not been inserted with the already inserted almost invisible (Arora *et al*., 2016). Although, the LSB method is considered very good, the hidden data capacity is still low because of only one bit per pixel only. The LSB method is not difficult because of the ease of retrieving secret messages because the data is always hidden from any stego-image (Joshi *et al*. 2016).

LSB can be implemented more easily but it has a very serious security problem because there is a statistical difference between the modified part and the unmodified part of the stego-image (Zhang *et al*., 2006). Sahu and Swain (2016) proposed that LSB technique can give higher embedding capacity when extended up to 4 LSB planes. Therefore, this method allows very high transparency (Juarez-Sandoval *et al*., 2017). How to use this method we can use a four-pixel image as an example:

123 = 01111011
107 = 01101011
111 = 01101111
97 = 01100001

If the number 8 as the word you want inserted then the number can be changed into 4 bits into 1000. Then, the bits are inserted into the last bit that is already available as an example:

01111011
01101010
01101110
01100000

So, it can be seen binary difference before inserted words with already inserted.

Portable Network Graphics (PNG): PNG is one image storage. This format was introduced as a replacement for other image formats that is GIF. The PNG format uses a lossless compression method to display 24-bit images or solid colors on online media. This format supports transparency inside the alpha channel. The PNG format is very well used in online documents and has better color support when printed than GIF format. However, the PNG color will be placed in the in design document as a RGB bitmap image, so, it can only be printed as a composite image rather than a separation image (Lee and Tsai, 2010). The PNG format has several advantages:

- Image transparency
- Setting the light or darkness of an image
- Progressively displays the image

In addition, the PNG format has a better compression factor than the GIF format (Wang *et al*., 2016). Broadly speaking, the PNG format has the following features:

- Instead of GIF and TIFF formats
- Open format, efficient, free and lossless type compression
- Three color modes, namely: palette (8 bits), grayscale (16 bits), Truecolor (48 bits)
- Support for profile color, gamma and metadata
- Has a transparency feature and full support for alpha channel
- Extensive support for software manipulating graphics and web browsers

For the purposes of image processing, although, the PNG format can be an alternative during image processing

because this format in addition does not remove part of the image being processed (so, repeated storage of images will not degrade image quality) but JPEG format is still a better choice. Netscape 4.04 and MSIE 4.0 adds support for PNG browser files on web pages instead of replacing JPG but to replace GIF for graphics. For non-web and non-graphics use, PNG will compete with TIF. Most PNG image program support, so, the basic compatibility is not a problem. You may like PNG.

Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE): Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) are the most commonly used parameters to measure the quality of two images in steganography. PSNR can be said to be the similarity between the two images and the MSE is the reciprocal (Joshi *et al*., 2016). In each PSNR calculation, it is usually measured in decibels. To determine PSNR, MSE (Mean Square Error) must be determined first. MSE is the mean squared error value between the original image and the manipulation image. In the case of steganography, the MSE is the mean squared error value between the original image (cover-image) and the image of the insertion (stego-image). PSNR can be defined by formula:

$$PSNR = 10\log_{10}\left[\frac{I^2}{MSE}\right] \quad (1)$$

Where:
MSE = Mean Square Error value obtained
I^2 = The maximum value of the image pixels used

Before searching for PSNR value, then searched for the value of MSE. MSE can be defined by formula:

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

Where:
M = The No. of lines on the cover image
N = The No. of columns on the cover image
X_{ij} = The intensity of the cover image
Y_{ij} = The intensity of the stego-image

RESULTS AND DISCUSSION

LSB methods: In this chapter, discuss the results of experiments with the LSB method is to take the example using PNG image format with the size of 3×3 pixels. By taking the example image is a picture of watermelon.

In Fig. 1, it describes that in this study the research is using a watermelon image with different dimension.

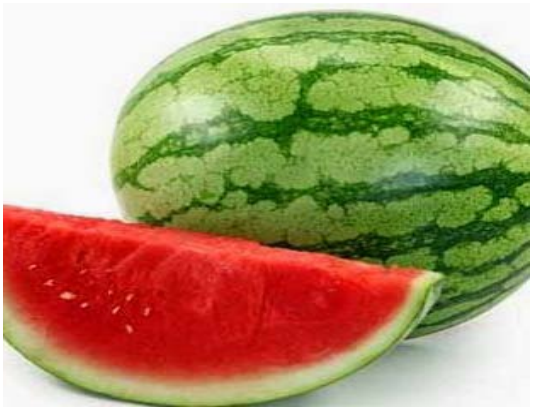

Fig. 1: Experiment with watermelon image

Once it is converted first into a 3×3 pixel form. Then see the RGB value in the image that has been converted into 3×3 pixels. Then after getting its RGB value, the next step to change the value of RGB is still in the form of decimal into the binary. So, we can get the value from this example:

Red value before being converted into binary:

254	158	197
249	92	114
255	230	209

Red value after being converted into binary:

11111110	10011110	11000101
11111001	01011100	01110010
11111111	11100110	11010001

Green value before being converted into binary:

255	195	193
113	72	96
70	47	177

Green value after being converted into binary:

11111111	11000011	11000001
01110001	01001000	01100000
01000110	00010111	10110001

Blue value before being converted into binary:

251	156	166
192	0	48
153	90	192

Blue value after being converted into binary:

11111011	10011100	10100110
11000000	00000000	00110000
10011001	01011010	11000000

After all values are obtained and converted into binary, then the next step is to calculate how many letters can be inserted into the 3x3 pixel image. By the way the result of 3×3 is 9 then multiplied 3. Why multiply 3 because the number of RGB colors is 3 then the result is 27 bits. After that, divided by 8 because the binary amounted to 8. The results obtained amounted to 3.37. So, the letters that can be inserted into the 3×3 pixel image are approximately 3 letters. The next step is to select the 3 letters "DAN". Subsequently the letters are converted into American Standard Code for Information Interchange (ASCII) values in binary form:

D = 68 converted into binary: 01000100
A = 65 converted into binary: 01000001
N = 78 converted into binary: 01001110

After obtained, next step is entering all the binaries of the letter into the RGB value that has been converted into binary. The rules in entering the binary is to start from the left and then go to the right and so on. By entering the last digit of the bit in the RGB value:
Red binary value after inserted:

1111111**0**	1001111**0**	1100010**0**
1111100**1**	0101110**0**	0111001**1**
1111111**0**	1110011**1**	1101000**1**

Red decimal value after inserted:

254	158	196
249	92	115
254	231	209

Green binary value after inserted:

1111111**1**	1100001**0**	1100000**0**
0111000**0**	0100100**0**	0110000**0**
0100011**0**	0001011**1**	1011000**1**

Green decimal value after inserted:

255	194	192
112	72	96
70	47	177

Blue binary value after inserted:

1111101**0**	1001110**1**	1010011**0**
1100000**0**	0000000**0**	0011000**1**
1001100**1**	0101101**0**	1100000**0**

Blue decimal value after inserted:

250	157	166
192	0	49
153	90	192

Then get the value on the experiment above. So, the remaining 2 values are not filled with the value of the letter "DAN".

PSNR and MSE methods: In this experiment, watermelon images of 3×3 pixels are used. To calculate with the formula PSNR and MSE, the first step that must be done is to compare the cover image with stego-image as below:

Red value before in steganography:

243	128	155
211	110	58
199	193	185

Red value after in steganography:

242	128	154
211	110	59
198	193	185

Green value before in steganography:

255	195	193
113	72	96
70	47	177

Green value after in steganography:

255	194	192
112	72	96
70	47	177

Blue value before in steganography

255	101	122
95	4	5
58	41	158

Blue value after steganography:

254	101	122
94	4	5
59	40	158

The next step is to use the MSE formula by reducing one by one the value of the cover image (X_{ij}) with the stego-image value (Y_{ij}). Having obtained the difference in the value of the cover image with stego-image and then lifted 2. After that summed the results of previous operations. Then divided by the number of rows and columns of the image is 3×3 and the following results are obtained:

$$MSE = \frac{1}{(3\times3)^2}(243-242)^2+(128-128)^2+(155-154)^2+(211-211)^2+(110-110)^2+(58-59)^2+(199-198)^2+(193-193)^2+(185-185)^2+(255-255)^2+(195-194)^2+(193-192)^2+(113-112)^2+(72-72)^2+(96-96)^2+(70-70)^2+(47-47)^2+(177-177)^2+(255-254)^2+(101-101)^2+(122-122)^2+(122-122)^2+(95-94)^2+(4-4)^2+(5-5)^2+(58-59)^2+(41-40)^2+(158-158)^2$$

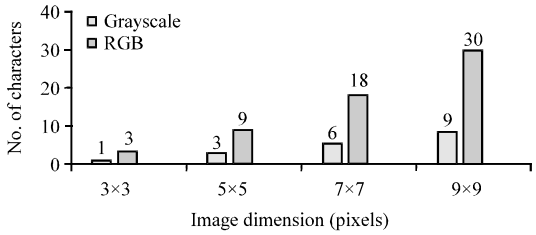

Fig. 2: No. of characters can be inserted in RGB and grayscale image

$$MSE = \frac{1}{(3\times3)^2}(1)^2+(0)^2+(1)^2+(0)^2+(0)^2+(-1)^2+(1)^2+(0)^2+(0)^2+(0)^2+(1)^2+(1)^2+(1)^2+(0)^2+(0)^2+(0)^2+(0)^2+(0)^2+(1)^2+(0)^2+(0)^2+(0)^2+(1)^2+(0)^2+(0)^2+(-1)^2+(1)^2+(0)^2$$

$$MSE = \frac{11}{(3\times3)^2}$$

$$MSE = 0.135$$

Having obtained the results of its MSE, then enter the value of MSE into the PSNR formula and obtained the following results:

$$PSNR = 10\log_{10}\left[\frac{255^2}{0.135}\right]$$

$$PSNR = 56.827$$

After input formula, the results obtained from PSNR and MSE. The value of PSNR = 56.827 and the value of MSE = 0.135.

Analysis: In this study will discuss the analysis and discussion of the experiments and discussions that have been tried. Gained graphs from the experimental results. Here are the graphic results obtained:

In Fig. 2, it describes the number of characters that can be inserted into an RGB and grayscale image. the graph increases because if the size of the image dimension increases, then the number of characters that can also be inserted in the RGB and grayscale image. In Fig. 3, it describes how much of the maximum text size can be inserted in RGB imagery. Each image size increases, the maximum text size increases as well. In Fig. 4, it explains the comparison between the original RGB image and the RGB image after the steganography. On the graph does not change in image size. At Fig. 5, it explains how much

of the maximum text size can be inserted in grayscale imagery. Can be seen that the graph increases because if the image size increases, then the maximum text size also increases. In Fig. 6, it describes the comparison between real image and stego-image in grayscale. can be seen no change in image size.

Overall experiment result data: In Table 1, it describes the overall data comparison obtained from the experiment. From the data that the size of the original image with the size of the image already in Steganography not change at all. In Table 2, it describes the overall data of PSNR is increased and MSE is stable. In Table 2 and Fig. 7, it describes the overall data of PSNR and MSE obtained from several dimensions of the image dimension. From the picture, it can be concluded that if the pixels are bigger,

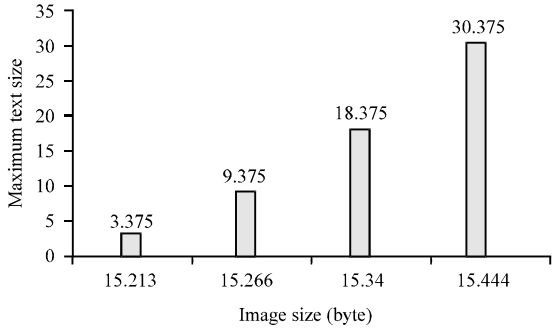

Fig. 3: Maximum text size on RGB image

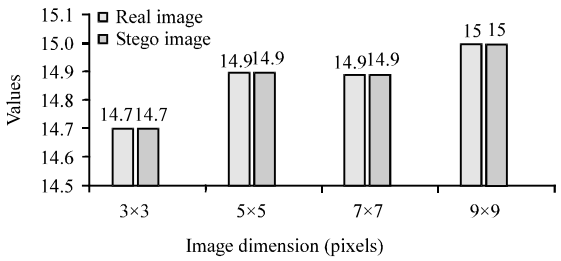

Fig. 4: Comparison between real image and stego-image in RGB

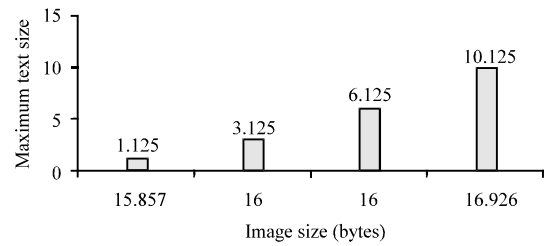

Fig. 5 : Maximum text size on grayscale image

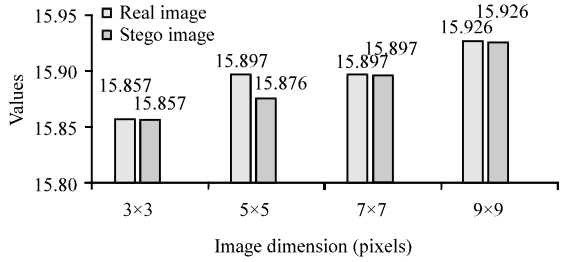

Fig. 6 : The comparison between real image and stego-image in grayscale

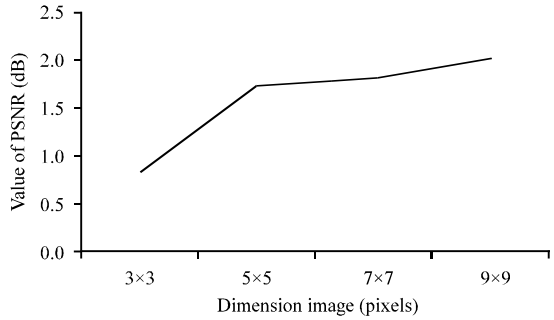

Fig. 7 : Dimension image and value of PSNR

Table 1: Overall data of the experiment

Images size (pixels)	Types of image	No. of character	Maximum character size (bytes)	Cover image size (bytes)	Stego-image size (bytes)
3×3	RGB	3	3.3750	15.213	15.213
5×5	RGB	9	9.3750	15.266	15.266
7×7	RGB	18	18.3750	15.340	15.340
9×9	RGB	30	30.3750	15.444	15.444
3×3	Grayscale	1	1.1250	15.857	15.857
5×5	Grayscale	3	3.1250	15.876	15.876
7×7	Grayscale	6	6.1250	15.897	15.897
9×9	Grayscale	10	10.1250	15.926	15.926

Table 2: Overall data of PSNR and MSE

Dimension image	Size of cover image	Size of stego-image	Size of character	MSE	PSNR
3×3	15.213	15.213	3	0.1480	0.829
5×5	15.266	15.266	3	0.0192	1.717
7×7	15.340	15.340	3	0.0110	1.811
9×9	15.444	15.444	3	0.0134	2.011

then the bigger the value of PSNR. And if the MSE value is getting smaller, the greater value of PSNR. MSE values close to zero have a high degree of similarity.

CONCLUSION

Based on the experimental results using the LSB method that has been obtained, it can be concluded that: the larger the dimensions of RGB and grayscale images, the more characters that can be inserted into the image. The maximum text size will also increase if the image size also increases. The image size changed from RGB image into grayscale image is bigger than before. Data integrity on RGB image and grayscale image that has been inserted has not changed at all. If the letter bit is inserted into the RGB or grayscale image bits, then the value of the image bit does not change significantly. So that, the shape of the image does not look any color change at all. The capacity of digital images to accommodate files by 30% and more colors in digital images can accommodate more files. So, for more optimal testing you should use digital image with more variety of colors. If the dimensions of the image dimension increase, then also, the result of PSNR and MSE in the image.

REFERENCES

Akhtar, N., V. Ahamad and H. Javed, 2017. A compressed LSB steganography method. Proceedings of the 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), February 9-10, 2017, IEEE, Ghaziabad, India, ISBN:978-1-5090-6219-5, pp: 1-7.

Arora, A., M.P. Singh, P. Thakral and N. Jarwal, 2016. Image steganography using enhanced LSB substitution technique. Proceedings of the 4th International Conference on Parallel, Distributed and Grid Computing (PDGC'16), December 22-24, 2016, IEEE, Waknaghat, India, ISBN:978-1-5090-3670-7, pp: 386-389.

Joshi, K., R. Yadav and S. Allwadhi, 2016. PSNR and MSE based investigation of LSB. Proceedings of the 2016 International Conference onComputational Techniques in Information and Communication Technologies (ICCTICT), March 11-13, 2016, IEEE, New Delhi, India, ISBN:978-1-5090-0082-1, pp: 280-285.

Juarez-Sandoval, O., M. Cedillo-Hernandez, G. Sanchez-Perez, K. Toscano-Medina and H. Perez-Meana *et al*., 2017. Compact image steganalysis for LSB-matching steganography. Proceedings of the 2017 5th International Workshop on Biometrics and Forensics (IWBF), April 4-5, 2017, IEEE, Coventry, UK., ISBN:978-1-5090-5792-4, pp: 1-6.

Lee, C.W. and W.H. Tsai, 2010. A new Steganographic method based on information sharing via PNG images. Proceedings of the 2nd International Conference on Computer and Automation Engineering (ICCAE), February 26-28, 2010, IEEE, Singapore, Singapore, ISBN:978-1-4244-5569-0, pp: 807-811.

Patel, N. and S. Meena, 2016. LSB based image steganography using dynamic key cryptography. Proceedings of the 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), November 18-19, 2016, IEEE, Dehradun, India, ISBN:978-1-5090-4506-8, pp: 1-5.

Rohayah, S., G.W. Sasmito and O. Somantri, 2015. [Application of steganography for messaging of messages (In Indonesian)]. J. Inf., 9: 975-981.

Sahu, A.K. and G. Swain, 2016. A review on LSB substitution and PVD based image steganography techniques. Indonesian J. Electr. Eng. Comput. Sci., 2: 712-719.

Sari, W.S., E.H. Rachmawanto and C.A. Sari, 2017. A good performance OTP encryption image based on DCT-DWT steganography. Telkomnika, 15: 1987-1995.

Singh, Y.K. and S. Sharma, 2016. Image steganography on gray and color image using DCT enhancement and RSA with LSB method. Proceedings of the 2016 International Conference on Inventive Computation Technologies (ICICT) Vol. 3, August 26-27, 2016, IEEE, Coimbatore, India, ISBN:978-1-5090-1286-2, pp: 1-5.

Wang, F., W.L. Lyu and J.S. Pan, 2016. Robust image authentication scheme with self-repair capability for greyscale source document images via PNG format. IET. Image Process., 10: 971-978.

Zhang, T., Y. Zhang, X. Ping and M. Song, 2006. Detection of LSB steganography based on image smoothness. Proceedings of the 2006 IEEE International Conference on Multimedia and Expo, July 9-12, 2006, IEEE, Toronto, Ontario, Canada, pp: 1377-1380.

Zhou, X., W. Gong, W. Fu and L. Jin, 2016. An improved method for LSB based color image steganography combined with cryptography. Proceedings of the 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), June 26-29, 2016, IEEE, Okayama, Japan, ISBN:978-1-5090-0807-0, pp: 1-4.