Robustness of Steganography Image Method Using Dynamic Management Position of Least Significant Bit (LSB)

R. Rizal Isnanto
Dept. of Computer Engineering
Universitas Diponegoro
Semarang, Indonesia
rizal_isnanto@yahoo.com

Risma Septiana
Dept of Computer Engineering
Universitas Diponegoro
Semarang, Indonesia
rismaseptiana@live.undip.ac.id

Ahmad Fashiha Hastawan
Information and Technology
Engineering Pedagogics
Universitas Negeri Semarang
Semarang, Indonesia
ahmad.fashiha@mail.unnes.ac.id

***Abstract*— Steganography is used to hide information in the process of data communication. The data that can be hidden are either the texts or images. Hiding image in an image means that the pixel values of the secret image will be embedded in an image called cover image. The challenge is that the cover image should not be damaged even if the embedding process changes the pixel values. Steganography methods have various ways to embed a secret message hidden. This research will use one of the methods called the Least Significant Bit (LSB) and the method will be combined with a dynamic management position of placement of the message. The aim of combining method is to make the robustness method that can be implemented using various size and type of hidden images as the secret message. The robustness method will ensure that the embedded process result called stego-image should be reversible correctly. Measurement of damaging image uses the parameters of similarity image quality that are Mean Square Error, Peak Signal to Noise Ratio and Root Mean Square Error. The result shows good quality of similarity image and the method can recover the secret image from the image cover.**

Keywords—Data Communication, Steganography, Images Least Significan Bit (LSB), Stego-Image, Image Quality, Secret message

I. INTRODUCTION

Data communication technology is the tremendous demand to be improved in the digital era. One of the challenges to be improved is a security issue. The data should be unreadable by an unauthorized receiver. Two sciences widely used to protect data are Cryptography and Steganography. Both sciences have different ways to hide information. Cryptography focuses on encrypting data by destructing the original data. Steganography hides an original data in a data cover. So, the original data will be a data embedded. Steganography is regularly designed better than cryptography because it will keep the consistency of the data form. So, it does not attract the suspicion from secret images hidden [1].

The data that can be hidden are either texts or images, but the data storage cover is usually an image. Saving text in an image will not cause deformation of the cover image. Saving image in an image means two images must be blended. Pixel values of two images will be combined. The challenge is that the changing of pixel values should be invisible from human eyes.

Some previous researches use one of the steganography methods that modify the Least Significant Bit (LSB) [2]. Researchers in [3][4] explains that changing LSB value will not erase the information in an image. Both types of research show that the result of the steganography process will keep the integrity of the image. [5] uses the quality of image measurement to analyze the integrity of the image. The parameters used are MSE (Mean Square Error), and PSNR (Peak Signal to Noise Ratio). The best result is showed by the lower value of MSE and the higher value of PSNR. Besides that, the rate of hiding process can be measured by counting the time to embed an image. The [6] explains the two halftone images can be used as image cover to hide a data. Using new conjugate property improved the hiding process rate. That research using a 24-bit cover image to hide a text. The future result must try to use the image as the hidden message.

Two requisites of a good steganography method for saving the image in an image are stego-image damage should be limited and the secret image should be reversible. The [7] explains explain the output image as a steganography result has to have a small change in pixel value to minimize the data damage. Both [8] and [9] explain that reversible data is an important challenge in the encryption and decryption process. The encryption process should not cause data damage.

This research will use a modification of the LSB method to save a secret image. LSB method is modified by adding the dynamic management placement of pixel value position. This method not only embeds the pixel values of the secret image but also embeds the size of the secret image. A dynamic management position is used to shift the pixel values in the embedding process, so the placement of the size and secret image can be organized in the cover image appropriately. The aim of the size image saving is to simplify the reversible process to recover the secret image. The purpose method will ensure limited data damage and the data should be reversible. Measurement of data damage will use the parameters of image quality that are MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio) and RMSE (Root Mean Square Error).

II. METHODOLOGY

A. Steganography

Steganography is an art of science to hide the secret message. Hiding method uses some media as a cover to save the message, such as image, audio, text, video, etc. The message is not only a text but also another digital data

such as an image. The unauthorized receiver can see only the data appeared from the cover image and cannot realize that there is a secret message saved [10].

Fig 1. Ilustration of saving secret message in an image media[10]

B. Least Significant Bit (LSB) Method

LSB is one of the steganography methods. It has some rule to determine the pixel values changing of the cover image. There are some rules used in the LSB method [10]:

1. The message that will be saved should be a sequence of binary values.
2. The embedding message starts from the right sequence called MSB (Most Significant Bit). The followed rules:
   - If message_bit = 1 and intensity of image cover = odd or If message_bit = 0 and intensity of image cover = even, intensity of stego-image = intensity of image cover.
   - If message_bit = 1 and intensity of image cover = even, intensity of stego-image = intensity of image cover + 1
   - If message_bit = 0 and intensity of image cover = odd, intensity of stego-image = intensity of image cover-1
3. Save the Stego image

C. Proposed Method

This research will used improvement of LSB method. This method not only uses the pixel values of the secret image but also the size of the image. The size of the image will be saved in the cover image common with the pixel values of secret image. The algorithm of this method can be explained:

1. Determine the number of pixels in the cover that used to save the size of the image. In this research will use 24 pixels (start from the right sequence).
2. The image will be embedded in a cover image should have a lower size than the cover image. The equation to represent the size is

   Cover size - 24 > embedded size

3. Fill out the 24 bit with the height and width of the size form image embedded. Then, apply the LSB method to hide the image
4. Pixel values of the secret image will be blended with the pixel values of the cover image. Shift the position of the secret message to the 25^{th} pixel of the cover image.
5. Amount of pixel size that will be used to save the secret image can be explained by the equation

   The size for secret image = Cover size - 24

6. The size of the secret image can change dynamically and it will affect the position of the secret image in the cover image.
7. Management position will organize the placement of the size and the pixel values of the secret image.

D. Image Quality

Measurement of image quality can use three parameters that are MSE (Mean Square Error), PSNR (Peak Signal To Noise Ratio) and RMSE (Root Mean Square Error).

1. Mean Square Error (MSE)

   MSE can be measured using the equation 1 [10]:

$$MSE = \frac{\sum_{X}^{M}\sum_{Y}^{N}[f1(x,y) - f2(x,y)]^2}{MxN} \quad (1)$$

   MSE is used to measure the quality of a new image. If the values become lower, the quality is better because the new image has good similarity value with the original image.

2. Peak Signal To Noise Ratio (PSNR)

   PSNR can be measured using the equation 2[10]:

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}} \quad (2)$$

   If the values of PSNR become higher, the changing of intensity in an image can be unseen using human vision.

3. Root Mean Square Error (RMSE)

   RMSE can be measured using the equation 3[10]:

$$RMSE = \sqrt{\frac{\sum_{X}^{M}\sum_{Y}^{N}[f1(x,y) - f2(x,y)]^2}{MxN}} \quad (3)$$

III. Result And Discussion

A. Image Cover and Image Embedded

Steganography process uses two images, that is image as a cover and a secret message called image embedded. This research uses human photos that will save a secret image. Image covers are seen in Figure 2.

Image Cover 1	Image Cover 2	Image Cover 3

Fig. 2 Various of Images Cover

Figure 2 shows three images that is used as cover. The images are 24 bits grayscale image. Images cover will be a cover to carry the secret message. This research considers three secret message called Image Embedded. The various images are seen in Figure 3.

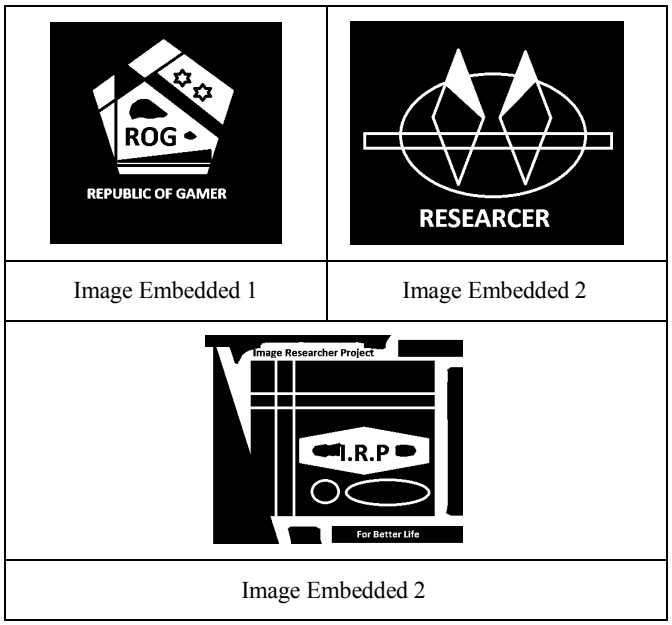

Fig 3 Various of Images Embedded

Figure 3 shows three images that will be embedded in the cover image. The images are 2 bits images. Each image has a different size and intensity formation. The differences are applied to test the dinamic changing position when the embedded processing is running.

B. Image Embedding Process

The method used to embed the image is LSB method. Before applying the method, the process is initiated by embedding the image size to the cover image. The initialization process makes the reversible process easier. Adding the image size and embedding the secret message will change the pixel values in the cover image. Embedding Process of the image can be explained in Figure 4.

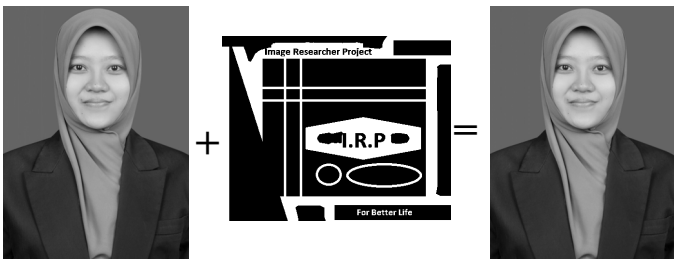

Fig 4 Process of Making Stego Image

Figure 4 shows the process of making Stego-Image. Although the visualization of a cover is almost equal to stego-image. Both Images has a different intensity. The differences can be shown in the histogram value as seen in Figure 5 and Figure 6

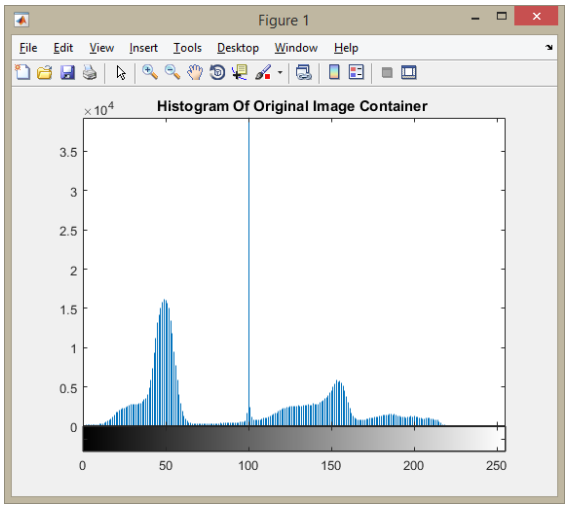

Fig 5 Histogram of Cover Image

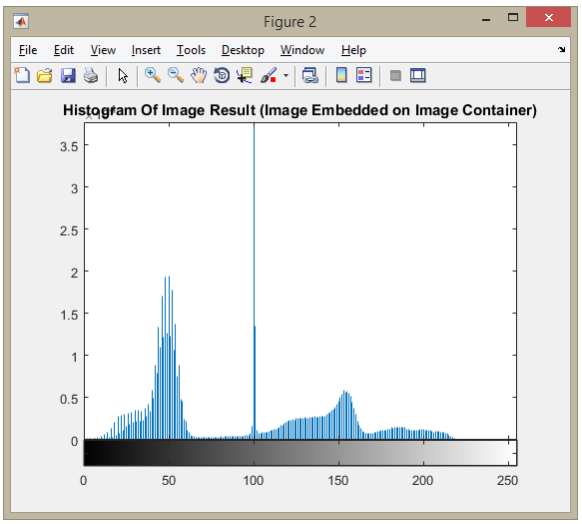

Fig 6 Histogram of Stego Image

The comparison result from two histograms above is the stego image histogram has additional pixel values from the image embedded. The value is shown from the overlapping color of the graph. It does not affect the image damage. So, the visualization is still the same.

C. Image Quality Result

Image quality measurement can be started by comparing the size of the original cover image and stego-image. The results are explained in Table 1.

Table 1. Comparison the size of cover image and the steganography result

No	Size Pixel Image Cover	Size Data Image Cover (KB)	Size Pixel Image Result	Size Data Stego-Image (KB)
1	918 x 1200	206	918 x 1200	211
2	918 x 1200	206	918 x 1200	212
3	918 x 1200	206	918 x 1200	216
4	751 X 1024	261	751 X 1024	266
5	751 X 1024	261	751 X 1024	268
6	751 X 1024	261	751 X 1024	271
7	1260 x 1890	660	1260 x 1890	666
8	1260 x 1890	660	1260 x 1890	666
9	1260 x 1890	660	1260 x 1890	669

Table 1 shows the result of an embedded process from three images to three cover images. There are nine variations. From the nine values, the size of each image does not change. But, the size of saving memory increases around 6-10 KB. Furthermore, measurement of similarity value from Stego-Image uses three values those are MSE, PSNR, and RMSE as shown in Table 2.

Table 2. Comparison MSE, PSNR, & RMSE Image Result

No	MSE	PSNR	RMSE
1	0.0371	62.4404	0.1925
2	0.0400	62.1064	0.2001
3	0.0623	60.1867	0.2496
4	0.0607	60.2955	0.2465
5	0.0675	59.8399	0.2597
6	0.0937	58.4143	0.3061
7	0.0191	65.3302	0.1380
8	0.0210	64.9133	0.1448
9	0.0296	63.4108	0.1722

Nine various stego-images in Table 2 show the similarity value of image quality. If MSE value is lower, the quality of the image will be better. So, the image looks like the original image. The higher PSNR value causes the human visualization to see the same image even though the intensity has the different value. The RMSE values show the error correction from the Stego-Image.
The result explains that the various size and shape of the image as a secret message can be embedded in a various type of Cover Image with the similarity value close to the original image.

D. Image Recover Result

The stego-image should be reversible. Separation of the secret message from the cover image is the recover process. Initialization the size of the image is the first process. It will help to get all of the image intensity completely. The quality of Image can be measured as shown in table 3.

Table 3 of Image Embedded Extracted

Size Pixel of Image Embedded	Size Pixel of Image Extracted	MSE	PSNR	RMSE
389 x 372	389 x 372	0	Inf	0
474 x 383	474 x 383	0	Inf	0
474 x 383	474 x 383	0	Inf	0

Table 3 shows values of MSE, PSNR, and RMSE from the result of the recover process. Images recover results give value for MSE and RSME that is equal to 0 then give infinitive for PSNR value. The result shows that the image is the right secret message and the images still have good quality.

IV. CONCLUSSION

The proposed method provides dynamic placement of the pixel values in a cover image. Two main parts that would be embedded in this method were the size of the image and the pixel values. The method organizes the placement of the pixel values, so placement of the pixel values from the secret images embedded can be shifted after the placement process of the image size. The management position makes the robust dynamic placement of the embedding process. Various images with the various size and type can be embedded and recovered perfectly. The result shows good quality of similarity image and the method can recover the secret image from the image cover for various size and type of images

ACKNOWLEDGMENT

Authors have to thanks to Strategics Research Grant from Faculty of Engineering, Diponegoro Universirty, Semarang, Republic of Indonesia. This research was financially supported by The Faculty of Engineering, Diponegoro University, Indonesia
through Strategic Research Grant 2018

REFERENCES

[1] X.-W. Li, W.-X. Zhao, J. Wang, and Q.-H. Wang, "Multiple-image hiding using super resolution reconstruction in high-frequency domains," *Opt. Commun.*, vol. 404, pp. 147–154, Dec. 2017.

[2] R. Tavoli, M. Bakhshi, and F. Salehian, "A New Method for Text Hiding in the Image by Using LSB," *IJACSA (International Journal of Advanced Computer Science and Applications)*, vol. 7, no. 4, 2016.

[3] D. Rawat and V. Bhandari, "A steganography technique for hiding image in an image using lsb method for 24 bit color image," *Int. J. Comput. Appl.*, vol. 64, no. 20, 2013.

[4] C. B.S., P. K., and R. D., "Least Significant Bit algorithm for image steganography," *IJACT (International Journal Of Advance Computer Technology*, vol. 3, no. 4.

[5] Rojali and A. G. Salman, "Reversible Data Hiding Technique on Jpeg Image By Quad-Tree Segmentation and Histogram Shifting Method Based On Android," *Procedia Comput. Sci.*, vol. 59, pp. 530–539, 2015.

[6] H. Ding and Y. Yang, "Data hiding in color halftone images based on new conjugate property," *Comput. Electr. Eng.*, vol. 70, pp. 302–316, Aug. 2018.
[7] Manonmaniam Sundaranar University, India, R. R, M. D, Manonmaniam Sundaranar University, India, D. V. Krishnan, and Infosys Limited, India, "PIXEL PATTERN BASED STEGANOGRAPHY ON IMAGES," *ICTACT J. Image Video Process.*, vol. 5, no. 3, pp. 991–997, Feb. 2015.
[8] C.-F. Lee and Y.-L. Huang, "Reversible data hiding scheme based on dual stegano-images using orientation combinations," *Telecommun. Syst.*, vol. 52, no. 4, pp. 2237–2247, Apr. 2013.
[9] Z.-L. Liu and C.-M. Pun, "Reversible data-hiding in encrypted images by redundant space transfer," *Inf. Sci.*, vol. 433–434, pp. 188–203, Apr. 2018.
[10] P. N. Andono, T. Sutojo, and Muljono, *Pengolahan Citra Digital*, 1st ed. Yogyakarta: Andi, 2017.