PROC. INTERNAT. CONF. SCI. ENGIN. ISSN 2597-5250
Volume 3, April 2020 | Pages: 201-205 E-ISSN 2598-232X

Analysis of Least Significant Bit Method Using Sequential Encoding-Decoding in Steganography Digital Image

Nurmi Hidayasari[1,*], Febi Yanto[2]
[1]Informatics Engineering Departement, UII Yogyakarta,
[2]Informatics Engineering Departement, Faculty of Science and Technology, UIN SUSKA Riau
Email*: 16917219@students.uii.ac.id

Abstract. The method of steganography commonly used to hide data or information is Least Significant Bit (LSB) method. One of the relevant research is LSB using sequential Encoding - Decoding by David Pipkorn and Preston Weisbrot. In this research, an analysis of the LSB method using Sequential Encoding - Decoding by doing some testing. The tests are on the aspect of message security using tools StegSpy and enhanced LSB algorithm, testing on image quality by calculating the Peak Signal to Noise Ratio (PSNR) value and see the image histogram, testing on robustness of message by doing some image processing operations on stego image, like cropping, rotating, and etc, and then testing on capacity to check size of cover image and stego image and calculates the maximum size of data that can be hidden. From the testing process, we know that there are deficiencies in the aspects of security, robustness and capacity of a message. And then in this research we try to change the location of messages that are hidden in the image bits, which previous research used the 8th bit of each bytes, changed to the 7th bit. To be able to correct deficiencies in the security aspect. After repairing and testing like before, obtained better results in the security aspect. This can be seen from the image of the enhanced LSB algorithm process, the message is not detected, but unfortunately the image quality is reduced, with the low PSNR value generated.

Keywords: Enhanced LSB, Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR), Sequential Encoding-decoding, Steganography

INTRODUCTION

Steganography is a way to collect data or information in a media (image, audio, video, etc.). The method that is widely used in steganography is the Least Significant Bit (LSB) method (Andrian, 2013; Pipkorn and Weisbrot, 2012; Puncuna, 2010). LSB or Least Significant Bit is the right most bit in a byte. Called LSB, because this bit is a bit that has no big effect. In a byte consists of 4-LSB and 4-MSB (Most Significant Bit). The process of inserting bits with the LSB method is to change the last bits of the byte with message bits.

One of the studies on LSB is "Steganography-Hidden Message" by David Pipkorn and Preston Weisbrot (2012), using two techniques in the LSB method, namely insertion techniques (sequential) and random. The good steganography has the following criteria (Munir, 2004) that are:

1. Fidelity, that is, the quality of the container image does not change much after the message is inserted, other people do not know if there is a secret message in the image.
2. Robustness, i.e. the hidden data must be resistant to various image processing operations (cropping, rotate, etc.).
3. Recovery, i.e. the hidden data must be revealed again (extracted).

Other criteria are (Gutub, 2010):

1. Capacity, i.e. the capacity of the original image and stego image does not change.
2. Invisibility, which is the insertion does not cause suspicion from others or tappers. This relates to data security.

This study will analyze the LSB method with the sequential techniques they use, by conducting several tests using several aspects of steganography, namely aspects of security, quality, resilience and capacity. From the test results will be improved, with the aim that the existing methods become better.

MATERIALS AND METHODS

Sequential encoding – decoding method

LSB method uses Sequential encoding-decoding is the insertion of messages in sequence. Pipkorn and Weisbrot (2012) developed the sequential technique to be more complicated than other sequential techniques. The message is inserted sequentially with the RGBBGRRG channel pattern, the insertion flow can be seen in the image below (Figure 1).

The process of encoding and decoding messages in general can be seen in Figures 2 and 3.

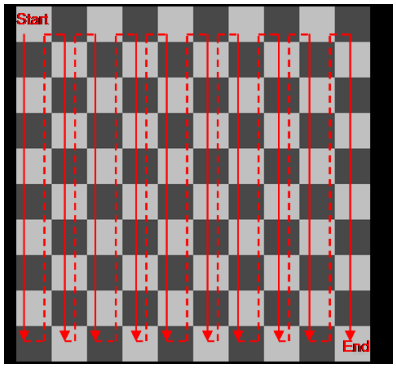


Figure 1. Sequential encode (Pipkorn & Weisbrot, 2012).

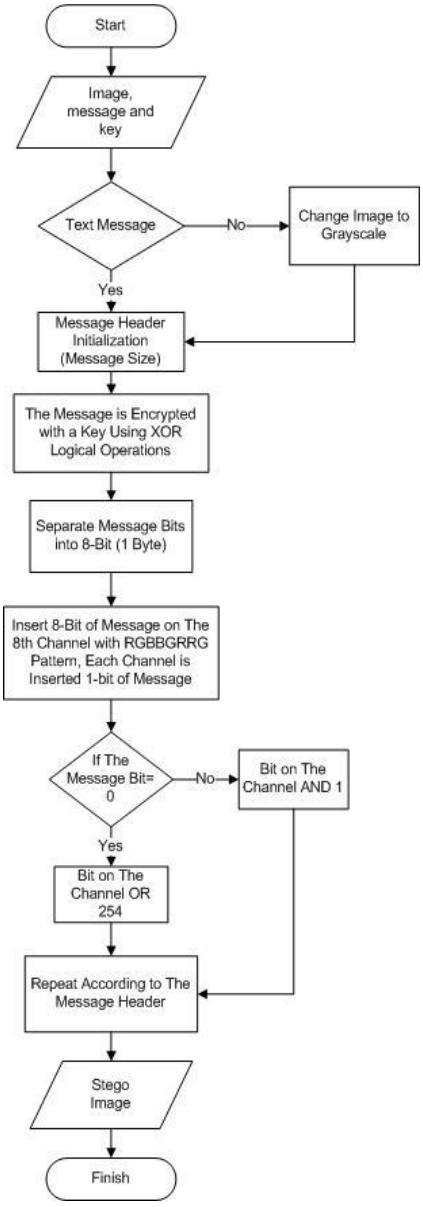


Figure 2. Sequential encode process.

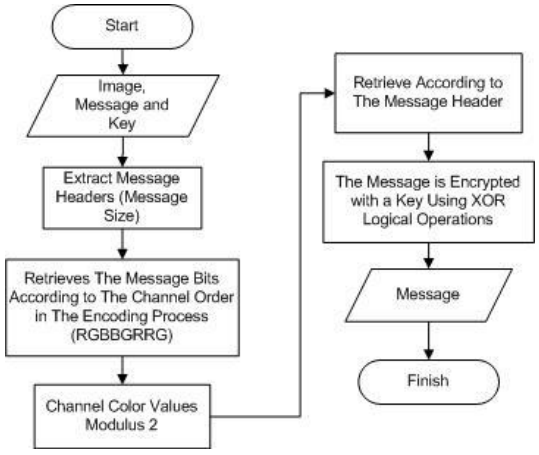


Figure 3. Sequential decode process.

Testing on digital image steganography

Tests on digital images that have been inserted messages are needed in a study to prove the level of success of the research that has been done. Tests that will be carried out in this study include several aspects or criteria, which are as follows:

1. Message security

Testing on this security aspect uses two ways, namely by using the tools StegSpy2.1 and the enhanced LSB algorithm. The explanation is as follows:

a). StegSpy Tools: These tools are tools that can detect data or information that is inserted on a media (image and audio). It looks as follows:

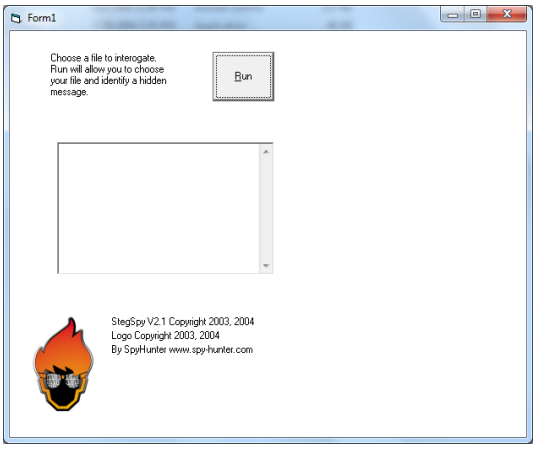


Figure 4. Display of StegSpy Tools.

b). Enhanced LSB Algorithm: This algorithm is a technique to detect messages visually. The main process of the enhanced LSB algorithm is to replace the value of all bits to 1 bit if the LSB of a byte is 1 and replace all the bits to 0 if the LSB of a byte is 0 (Sinaga, 2008). The process can be seen in the flowchart below:

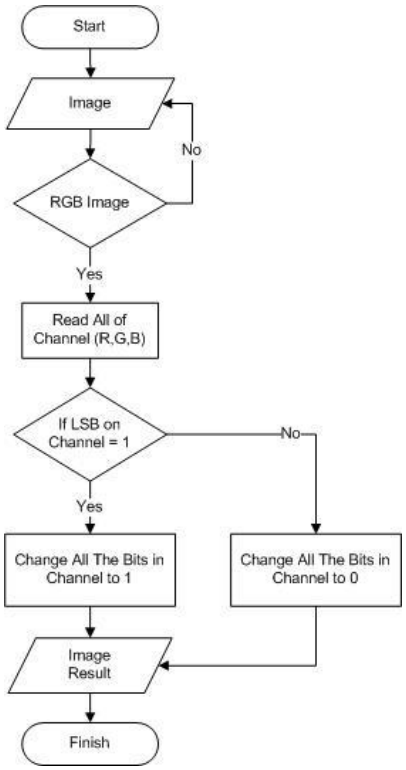


Figure 5. Process enhanced LSB algorithm.

2. Image quality (fidelity)

This test is done by comparing the original image and stego image, by calculating the PSNR value and image histogram.

a). Peak Signal to Noise Ratio (PSNR): PSNR is the ratio between the maximum value of the measured signal and the amount of noise that affects the signal. To determine the PSNR you must first determine the average square value of the error (MSE-Mean Square Error). The formula is as follows:

$$MSE = \frac{1}{m\,n}\sum_{y=1}^{m} m \sum_{x=1}^{n} n\,[I(x,y) - I'(x,y)]^2 \quad (1)$$

$$PSNR = 10Log_{10}\left(\frac{255^2}{MSE}\right) \quad (2)$$

b). Image Histogram: An image histogram is a diagram that illustrates the color distribution of a digital image or illustrates the spread of pixel intensity values of an image. From a histogram, it can be seen the relative frequency of occurrence of intensity in the image, the brightness and contrast of an image.

3. Message robustness

Testing on this aspect is done by utilizing image processing operations with the help of tools that have been available, namely Photoshop.

4. Message capacity

Testing on this aspect is carried out to determine the original image capacity and stego image and calculate the maximum capacity of messages that can be inserted.

RESULTS AND DISCUSSION

Results

From the tests that have been done, the results of testing the LSB method using sequential encoding-decoding is this method of low security, because the message can still be detected with the enhanced LSB algorithm. In the aspect of image quality, this method does not damage the image quality, in the aspect of message durability, some messages cannot be extracted after an image processing operation. Then in the aspect of capacity, the original image and stego image do not experience a change in capacity, whereas for the maximum capacity of messages that can be inserted small.

Improvement

From the results of tests conducted previously, repairs will be made to improve its safety aspects. By changing the original image bit that will be changed by the message bit. Previously the 8th bit will be changed to the 7th bit. After repairs, testing is the same as the previous test.

Comparison of Results

After the repairs are done then testing the method after modification. The test results will be compared with the results of testing with the method before modification. This test will use the original image ‘lenna.bmp’ size 768 Kb and text message ‘message6.txt’ size 22.7 Kb, and image message boy.jpg ’size 12.8 Kb.

Table 1. Original Image and Message.

Original Image	Message	
	Text	Image
		
lenna.bmp	pesan6.txt	boy.jpg

Table 2. Comparison of the Results Testing Security Aspects.

StegSpy Tools				
	Text Message		**Image Message**	
Method	**Before Modification**	**After Modification**	**Before Modification**	**After Modification**
Results	Detected no messages	Detected no messages	Detected no messages	Detected no messages
***Enhanced* LSB Algorithm**				
	Text Message		**Image Message**	
Method	**Before Modification**	**After Modification**	**Before Modification**	**After Modification**
Results	Messages detected	Detected no messages	Messages detected	Detected no messages

Table 3. Comparison of MSE and PSNR values.

Secret Message	**Before Modification**		**After Modification**	
	MSE	**PSNR**	**MSE**	**PSNR**
Text	0.1182	57.4033	0.5513	50,7170
Image	0.1223	57.2567	0.4899	51.2300

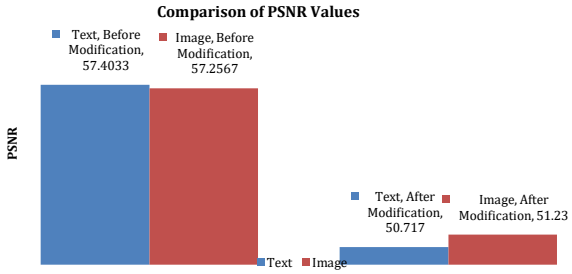


Figure 6. Comparison of PSNR values

Table 4. Comparison of Image Histogram for Red Channel.

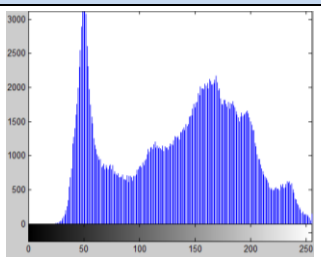
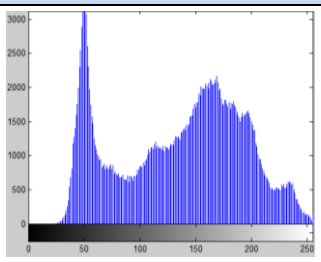
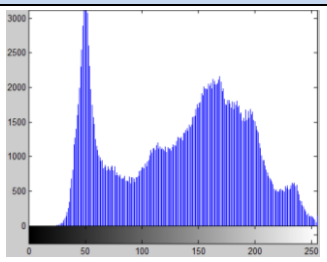
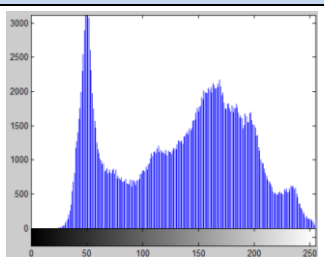
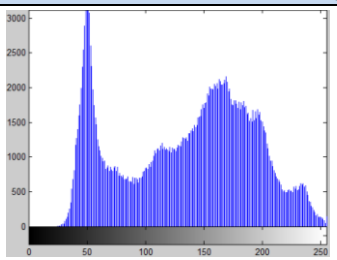
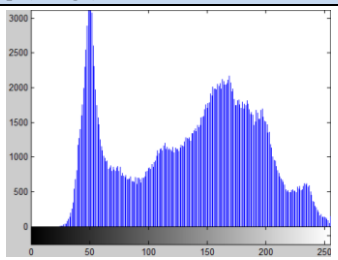
	Lenna.bmp	
		
	lenna_stego.bmp (Text)	
Red Channel		
	lenna_stego_filegbr.bmp (Image)	
		

Table 5. Comparison of Contents after Text Messages Cropping Some Percent.

Crop The Bottom	Difference in Message Content
±5%	±10%
±20%	±55%
±50%	±51%
±80%	100%
Crop The Right	**Difference in Message Content**
±5%	0%
±20%	0%
±50%	0%
±80%	100%

Table 6. Comparison of Results after the Stego Image Contrast is Changed.

Contrast Values	Percentage of Damage	
	Before Modification	After Modification
-4	Failed to extract	Failed to extract
-2	0%	0%
-1	0%	0%
1	0%	0%
2	0%	0%
4	Failed to extract	Failed to extract

Table 7. Comparison of Results After Stego Images on Rotate.

Rotate (°)	Percentage of Damage	
	Before Modification	After Modification
90° left	Failed to extract	Failed to extract
90° right	Failed to extract	Failed to extract
180°	Failed to extract	Failed to extract

Table 8. Comparison of Capacity Testing Results.

Original Image	Original Size (byte)	Message	Message Size (byte)	Stego Image Size (byte) – before modification	Stego Image Size (byte) – after modification
lenna.bmp	786.486	pesan6.txt	23.294	786.486	786.486
		boy.jpg	13.125	786.486	786.486

CONCLUSIONS

The following are some conclusions from this study:

1. Steganography with LSB method using Sequential encoding-decoding before modification has several disadvantages, namely:
   a. In terms of security, testing using the enhanced LSB algorithm on the stego image in the detection of hidden messages.
   b. The message that has been inserted is not fully resistant to image processing operations (cropping, changes in contrast and rotate values), some messages cannot be extracted again after changes are made to the stego image.
   c. The capacity of the original image and stego image does not change (still same).
   d. The size of the message that can be inserted is small, less than 10% of the container media size.
2. After changing the location of the message bit insertion, the existing techniques have become better in terms of message security. This can be seen from the image of the message security test results using the Enhanced LSB algorithm, in the detection of no messages. The original image and stego image there is no difference.
3. Because it only modifies the location of the bit insertion, this technique still has shortcomings. Both in terms of message durability and message capacity that can be inserted. Besides stego image after modification has decreased quality, can be seen from the PSNR values. Produce features that are incompatible with the test image.

REFERENCES

Andrian Y. 2013. Modifikasi Metode Least Significant Bit (LSB) pada Steganografi Citra Digital.

Gutub AAA. 2010. Pixel indicator technique for RGB image steganography. Journal of Emerging Technologies in Web Intelligence 2(1): 56–64. https://doi.org/10.4304/jetwi.2.1.56-64

Munir R. 2004. Steganografi dan Watermarking. Bahan Kuliah Ke-7 IF5054 Kriptografi Departemen Teknik Informatika Institut Teknologi Bandung.

Pipkorn D, Weisbrot P. 2012. Steganography-The Hidden Message. (Cs 534).

Puncuna I. 2010. Steganography, sebuah kata yang berasal dari bahasa Yunani yang berarti "tulisan rahasia" adalah sebuah metode penyembunyian pesan rahasia dalam pesan lainnya sehingga tidak bisa dideteksi atau dipecahkan oleh sembarang orang.

Sinaga YA. 2008. Program Steganalisis Metode LSB pada Citra dengan Enhanced LSB, Uji Chi-Square, dan RS-Analysis. [Thesis] Institut Teknologi Bandung, Bandung. [Indonesian]

THIS PAGE INTENTIONALLY LEFT BLANK