

# WATERMARKING METHOD OF REMOTE SENSING DATA USING STEGANOGRAPHY TECHNIQUE BASED ON LEAST SIGNIFICANT BIT HIDING

Destri Yanti Hutapea<sup>1</sup>, Octaviani Hutapea<sup>2</sup>

<sup>1</sup>Remote Sensing Technology and Data Center, LAPAN

<sup>2</sup>Gunadarma University

<sup>1</sup>e-mail: destri.yanti@lapan.go.id

Received: 7 November 2017; Revised: 5 June 2018 ; Approved: 22 June 2018

**Abstract.** Remote sensing satellite imagery is currently needed to support the needs of information in various fields. Distribution of remote sensing data to users is done through electronic media. Therefore, it is necessary to make security and identity on remote sensing satellite images so that its function is not misused. This paper describes a method of adding confidential information to medium resolution remote sensing satellite images to identify the image using steganography technique. Steganography with the Least Significant Bit (LSB) method is chosen because the insertion of confidential information on the image is performed on the rightmost bits in each byte of data, where the rightmost bit has the smallest value. The experiment was performed on three Landsat 8 images with different area on each composite band 4,3,2 (true color) and 6,5,3 (false color). Visually the data that has been inserted information does not change with the original data. Visually, the image that has been inserted with confidential information (or stego image) is the same as the original image. Both images cannot be distinguished on histogram analysis. The Mean Squared Error value of stego images of all three data less than 0.053 compared with the original image. This means that information security with steganographic techniques using the ideal LSB method is used on remote sensing satellite imagery.

Keywords: *Steganography, least significant bit, security.*

## 1 INTRODUCTION

In today's digital era, accessing and distributing digital information become much easier as the technology develops rapidly. The current information exchange is one of raster data, such as remote sensing satellite imagery, where the data is widely used by users to obtain information about natural resources, disaster, spatial and others. In addition, some satellite images of data commercial which is bounded by licenses in data usage. Therefore, it is necessary to secure the remote sensing imagery by giving

identification marks on the image in order to minimize the misuse of the images. Data exchange reciprocates a good example of applications that the using of encryption to maintain data confidentiality between senders and recipients (Ali *et al.* 2008). In this research, steganography is used to conceal information for security and giving the identification mark.

Steganography one of the methods to conceal confidential messages which safe and hard to detect by human vision. Messages can be in text, images, audio,

video with data quality maintained (Bhowmik 2016). The word Steganography comes from Greek, means closed or covered letter, which include the various ways of confidential communication mightly efficiently. Initially, this method involves the use of invisible inks, character settings, digital signatures, cluttered channels, and spread spectrum of communications. The insertion of confidential information has an important role in data communications (Fazli and Kiamini 2008). Data with steganographic algorithms must have security, capacity, transparency and robustness/strong elements (Nilizadeh and Nilchi 2016). There are two main processes in steganography, that are embedding and extracting the messages or information in media cover (Kadam *et al.* 2012). Embedding is the process of inserting messages or information into media cover, while extraction is the process of deciphering messages are hidden in the stego image. Messages that would be covered into an image require two files. First is the unmodified original image that will take in hand the covered message, called the cover image. The second file is the covered message information. A message can be either plain text, chipertext, other images, or anything that can be embedded into bit streams (Gupta *et al.* 2012). In this study shall examine the insertion of information on remote sensing image data using Least Significant Bit (LSB) method, particularly Landsat8 by not changing the value and content of the image significantly. LSB is worked by replacing the last bits in the digital image file with data bits in the data form of message that to be concealed (Akhtar *et al.* 2013). In the techniques of concealment, the LSB method is a modest and convenient method to be applied into systems that requires insertion of data

into images (Sitorus 2016). The insertion in the LSB of satellite images was done with the minimum change in the satellite images (Mobasheri and Jafarikouranturkish 2014).

The insertion of information with steganographic techniques using the LSB method becomes a very important research in LAPAN. This research supports the role of LAPAN in Law/Act Number 21 Year of 2013 regarding outer Space. LAPAN has to collect, store, process and distribute the data through the National Remote Sensing Data Bank or Bank Data Penginderaan Jauh Nasional (BDPJN) by establishing a data network in the national spatial data network system. Withal the insertion of information into the remote sensing image shall support the security of data as well as the identity of the remote sensing image data acquisition of LAPAN's results/proceeds.

## **2 MATERIALS AND METHODOLOGY**

### **2.1 Data and Tools**

The medium resolution Landsat 8 data with 16 bit resolution was used in this study. Landsat 8 satellite imagery is equipped with two sensors which the results of the development of the sensors contained in satellites in the previous Landsat program. Both sensors are Operational Land Manager (OLI) which consists of 9 bands and Thermal Infrared Sensors (TIRS) which consists of 2 bands. In this study, three samples of Landsat 8 scenes with composite band 4,3,2 (true color) and 6,5,3 (false color) were used for the experiment as in Table 2-1. These three Landsat8 data are selected because they have a minimum cloud percentage, it will make easier to perform visual analysis. The confidential information which inserted is a LAPAN logo image in JPG format. It has 25 KB size and 480x328 dimension.

Table 2-1: Input Data (Original Image)

No	Scene Id	Location	Composite band	Size (Dimension)
1	LC81130 60201635 9RPI00	Goron- talo	4,3,2 (True Color) & 6,5,3 (False Color)	345 MB (7591 x776 1)
2	LC81220 65201707 2RPI00	Jawa Barat	4,3,2 (True Color) & 6,5,3 (False Color)	347 MB (7621 x778 1)
3	LO81100 62201705 2RPI00	Pulau Buru, Kepu- lauan Maluku	4,3,2 (True Color) & 6,5,3 (False Color)	344 MB (7591 x774 1)

The insertion of confidential information on Landsat 8 image using Matlab R2013b software by method of translating LSB. This is the plot of process insertion information to information extraction with LSB's method.

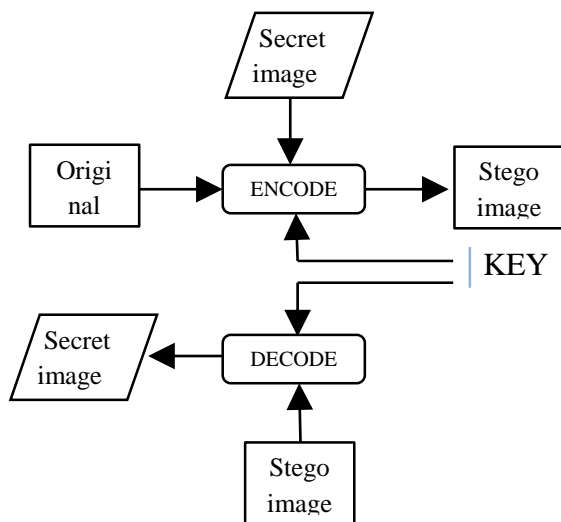


Figure 2-1: Flowchart of Steganograph Process

In the original image's encoding process is inserted with the secret image and produced a stego image. It can be extracted with the description key that has defined in the application and generates a secret image. The process of extraction is a decoding process. In case, the secret image of the decoding is the

same as the secret image during the encoding process, it means that the insertion process of the information is successful/worked and the image would be undamaged/intact.

## 2.2 Method of Least Significant Bit Hiding

The Least Significant Bit (LSB) hiding method is one of the watermarking methods on Red, Green, Blue (RGB) image. The method is performed by inserting the information on the rightmost bits of each RGB's element. The rightmost bit is simply inflected change in RGB value 1 of 256. The alteration might not be detected with the naked eyes. However, by a computer, for instance using the method of LSB Enhanced, it might be detected whether the image contains of watermark or not.

The insertion of the LSB is conferred by modifying the last bit in a byte of data. The bit which is replaced/substituted simply caused a change of mark one byte higher or lower (Nilizadeh and Nilchi 2016). For instance, the changed of data is green, therefore the alteration in the LSB may only cause slight modifications that the human eye does not detect. As we know for 24 bit bitmap files, each pixel on the image consist of arrangements of red, green and blue (RGB), and it's composed of 8 bit (byte) number from 0 to 255 or with a binary format 00000000 to 11111111. Thus/therefore, every 24 bit bitmap pixel we might insert 3 bits of data. For instance, the letter A we could insert in 3 pixels, example of the original raster data as follows:

```

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
    
```

Meanwhile the binary representation of the letter A is 10000011. By inserting it in the pixel data above it may be generated:

```

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001001 00100111 11101001)
    
```

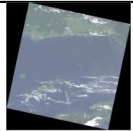
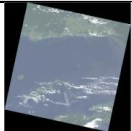
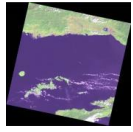
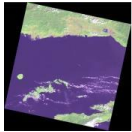
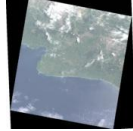
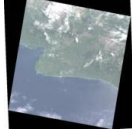


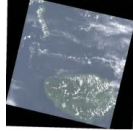
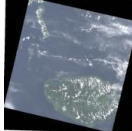


Selected from nine bytes, there are four bytes with a low bit difference. These changes shall not be differentiated by the human eyes. In this method only half of the low bit data become different, if it is needed, it could be used second or even third low bits. The size of data that would be concealed depends on the size of the container data. For instance, in the 8-bit image file size 256x256 pixels, there is 65536 pixels, each pixel measured 1 byte. Since it's converted to 24-bit image, the bitmap data size becomes  $65536 \times 3 = 196608$  bytes (Bhowmik 2016). Since that each byte could only stealth one bit in its LSB, so that the size of the data to be concealed in the maximum image is  $196608/8 = 24576$  bytes. The size of this data should be reduced by the length of the filename, seeing that the concealment of confidential data is not simply hiding the contents of the data, but also the name of the file.

**3 RESULTS AND DISCUSSION**  
**3.1 Encode and Decode Process**

In this process, the insertion of a secret image on Landsat 8 image in TIF format is performed. The inserted secret image is the LAPAN logo in a JPG data format. The result of Stego image is Landsat8 image in TIF format. Comparison of the original image with an image that has been inserted information on the encode process are in Table 3-1. From the information insertion process on the three Landsat 8 imagery data with true color and false color band combinations above, there is no color difference between the original image and the image of the information insertion. The inserted secret image is also not visually visible on the stego image. After the data is successfully inserted, the next step is the extraction (decode) of the stego.

The decoding is a stego image extraction process to produce the inserted secret image. In this study, the inserted image is parsed again, whether the inserted information can still be read and recognized as the initial insertion or not. From this experiment, it is found that the decoded information is the same as the image inserted in the Landsat 8 image. It means that the inserted information is not damaged after the process of insertion (encoding) and decoding.

Table 3-1: Results of steganographic trials

No	Scene id	Composite band	Original Image	Stego Image
1.	LC81130602016359RP100	4,3,2 (True Color)		
2.		6,5,3 (False Color)		
3.	LC81220652017072RP100	4,3,2 (True Color)		
4.		6,5,3 (False Color)		
5.	LO81100622017052RPI00	4,3,2 (True Color)		
6.		6,5,3 (False Color)		

**3.3 Histogram Analysis**

The histogram is a graph showing the number of the intensity values in an image. Histogram analysis is necessary to observe the similarity of histogram values on two different images (Lakshmi *et al.* 2016).

Figure 3-1: Comparison of RGB values and histogram between Original Image and Stego Image

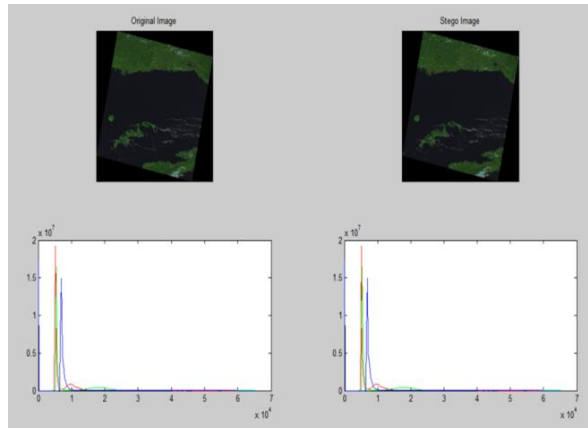


Table 3-2: Histogram of average digital number original image and stego image

No	Scene id	Composite band	Average histogram of the original image			Average digital number of stego image		
			R	G	B	R	G	B
1	LC81130	4,3,2 (True Color)	5087.40	6855.60	5442.00	5087.40	6855.60	5442.00
	6020163							
2	59RPI00	6,5,3 (False Color)	5087.40	6855.60	5442.00	5087.40	6855.60	5442.00
	LC81220							
3	6520170	4,3,2 (True Color)	5283.40	5905.00	6612.60	5283.40	5905.00	6612.60
	72RPI00							
3	LC81120	6,5,3 (False Color)	6539.20	9138.90	5905.00	6539.20	9138.90	5905.00
	6220170							
3	52RPI00	4,3,2 (True Color)	5427.80	6040.40	7137.00	5427.80	6040.40	7137.00
	LO81100							
		6,5,3 (False Color)	5286.40	6844.00	6040.40	5286.40	6844.00	6040.40

From the data in the above histogram, it could be calculated the average digital number of each color on all Landsat 8 data used. From the Table 3-2 above, it could be seen that the average of digital number in the original image is same as the stego image in each image data with certain band composite. It means, there is no alteration in the mark of the occurrence and the number of pixels between the original image and the inserted image.

### 3.4 Mean Squared Error

There are three parameters to evaluate the performance of steganography (Wu and Tsai 2003):

1. Load Capacity: This is defined as the maximum amount of data inserted into the image.
2. Robustness: This is the message's ability to persist even after performing operations such as compression, rotation, cutting and filtering etc.
3. Imperceptibility: This is defined as a stego-image quality and is measured by Mean Squared Error (MSE).

In this research, the performance evaluation of steganography image using imperceptibility parameter was measured by MSE. MSE is the mean squared error value between the original image (cover-

image) and the image of the insertion (stego-image). (Cheddad *et al.* 2010).

$$MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2 \quad 3-1$$

Where x and y are the coordinates of the image, M and N are the dimensions of the image, S<sub>xy</sub> represents the stego-image and C<sub>xy</sub> represents the cover-image.

Table 3-3: MSE between original image and stego image

No	Scene Id	Compo site band	MSE original image and stego image		
			R	G	B
1	LC81130602016359RPI00	4,3,2 (True Color)	0.0527	0.03	0.025
		6,5,3 (False Color)	0.0527	0.0325	0.0275
2	LC81220652017072RPI00	4,3,2 (True Color)	0.0524	0.052	0.048
		6,5,3 (False Color)	0.0524	0.052	0.048
3	LO81100622017052RPI00	4,3,2 (True Color)	0.0526	0.0522	0.049
		6,5,3 (False Color)	0.0527	0.0522	0.049

Table 3-3 shows the mean squared error value between the original image and the image of the insertion of information with the MSE value per RGB color. These values could be described in the following graph. Figure 3-2 shows the error value of each color, it is different for true color and false color composite. Red band for each color composite has the highest error value compared to green and blue. The mean squared error value each blue band of Landsat 8 scene has the lowest error value. Means that the lower the MSE results of digital image processing, the process of insertion of information the better.

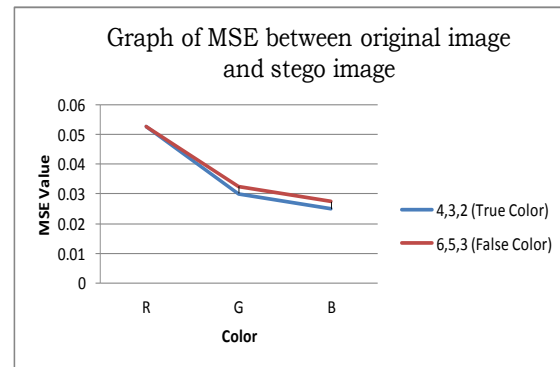


Figure 3-2: Graph of MSE between original image and stego image in scene LC81130602016359RPI00

#### 4 CONCLUSION

It can be concluded from this research that application of steganography could be done by inserting information into remote sensing image data with the Least Significant Bit (LSB) method. The result of encoded image is similar as the original image visually, the histogram analysis shows that the average digital number of each band from both images are same. The difference between the original and stego images in each band can be seen from the MSE values. The blue band images show the smallest MSE values compared to others. MSE values in the all three bands are less than 0.053. It means that the insertion of information using LSB method may be used on remote sensing images with very small changing on the image. This experiment was applied on the Landsat 8 image data, which should be applied for the insertion of information in distinct satellite imagery.

#### ACKNOWLEDGEMENTS

The author would like to thank Dr. Ir. Dodi Sudiana, M. Eng. and Dr. Rahmat Arief, M.Sc. for their guidances and directions so that this paper could be completed.

**REFERENCES**

- Akhtar N., Johri P., Khan S., (2013), Enhancing the security and quality of lsb based image steganography. Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013, 385-390.  
<https://doi.org/10.1109/CICN.2013.85>
- Ali M., Younes B., Jantan A., (2008), A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion. International Journal of Computer Science and Network Security, 8(6), 2-9.
- Bhowmik S., (2016), A New Approach in Color Image Steganography with High Level of Perceptibility and Security, 283-286.
- Cheddad A., Condell J., Curran K., *et al.*, 2010, Digital Image Steganography: Survey and Analysis of Current Methods. Signal Processing, Elsevier. Northern Ireland, UK.
- Fazli S., Kiamini M., (2008) A high performance steganographic method using JPEG and PSO algorithm. IEEE INMIC 2008: 12th IEEE International Multitopic Conference - Conference Proceedings, 100-105.  
<https://doi.org/10.1109/INMIC.2008.4777716>
- Gupta S., Goyal A., Bhushan B., (2012), Information Hiding Using Least Significant Bit Steganography and Cryptography. International Journal of Modern Education and Computer Science, 4(6), 27-34.  
<https://doi.org/10.5815/ijmecs.2012.06.04>
- Kadam K., Koshti A., Dunghav P., (2012), Steganography Using Least Significant Bit Algorithm. International Journal of Engineering Research and Applications, 2(3), 338-341.
- Lakshmi SB, Srinivas KS, Chandra MB, (2016), Steganography based information security with high embedding capacity. RAECE 2015 - Conference Proceedings, National Conference on Recent Advances in Electronics and Computer Engineering, 17-21.  
<https://doi.org/10.1109/RAECE.2015.7510218>
- Mobasheri MR, Jafarikouranturkish M., (2014), Steganography of Metadata in Satellite Images Using Insignificant Bits. 8thSASTech 2014 Symposium on Advances in Science & Technology-Commission-IV, 19-23.
- Nilizadeh A., Nilchi ARN, (2016), A novel steganography method based on matrix pattern and LSB algorithms in RGB images. 1st Conference on Swarm Intelligence and Evolutionary Computation, CSIEC 2016 - Proceedings, 154-159.  
<https://doi.org/10.1109/CSIEC.2016.7482107>
- Sitorus, Michael, (2015), Teknik Steganography dengan Metode Least Significant Bit (LSB). Jurnal Ilmiah Fakultas Teknik Limit's, 11(2), 54-61.
- Wu DC, Tsai WH, (2003), A steganographic method for images by pixel-value differencing, Pattern Recognit. Lett., 2003, 24, (910), pp. 1613-1626.

