VOL. 14, NO. 6, MARCH 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ANALYSIS AND IMPLEMENTATION OF STEGANOGRAPHY ON JPEG USING LSB AND SPREAD SPECTRUM METHOD

Jordy A Bagaskara and Tito Waluyo Purboyo
Faculty of Electrical Engineering, Telkom University, Bandung, Indonesia
Email: titowaluyo@gmail.com

ABSTRACT

Information is a message in the form of a utterance or phrase that can consist of symbols, or meanings that can be interpreted from a message or a collection of messages. Steganography is a technique that can be used to hide information on a media. In the digital era, the media used can be audio, image, or video. In its use, the concealment of messages is done by making small changes to a digital medium so as not to attract the attention of other people or attackers. In general, the concealment of a data or message on the image media is a technique that is often used in the implementation of steganography. In the use of image media, steganography can be implemented with existing methods; in this journal will be implemented Least Significant Bit (LSB) and Spread Spectrum method, which will further determine the analysis of image quality and comparison of both methods.

Keywords: steganography, JPEG image, least significant bit, spread spectrum.

INTRODUCTION

Information Technology has now grown rapidly in helping human activities. Delivery of data and information as a message more easily done mainly through the internet. But not always the use of the Internet in sharing information can be said to be safe, sometimes there are parties who do not have the authority over any information by deliberately stealing, damaging or disturbing the existence of such information.

Therefore, efforts are made to ensure the confidentiality and security of a data can be guaranteed when sent through the internet. Cryptography is a technique for hiding or communicating safely, but in its use this technique reaps some of the issues of legality and ease of reading the frequently used cryptographic patterns.

Steganography is a technique for hiding information in a cover media such as image, audio or video files [1]. There are some steganography techniques which can be used in image such as Least Significant Bit Substitution, Transform Domain Technique, Spread Spectrum, Statistical Technique, F5, Distortion Technique, and Cover Generation [4].

Least Significant Bit is a method that is done by replacing less meaningful data bits with bits of secret messages, while Spread Spectrum [10] is a method that randomly scrambles the message in its insertion. Thus, a steganographic application of the image will be created using both methods and analyzing the differences that occur in the steganographic image.

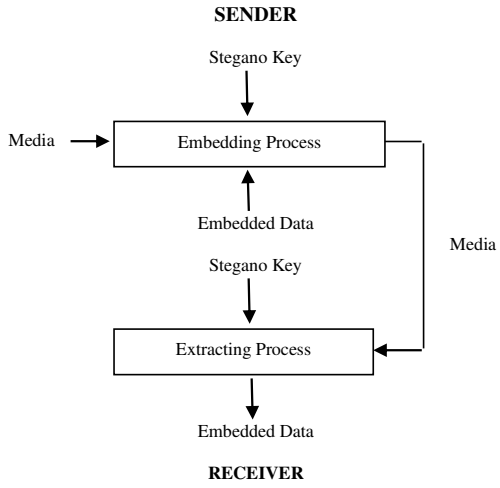


Figure-1. Steganography process.

METHOD

This study will compare two steganography methods, namely LSB and Spread Spectrum method. LSB is the most common and easy-to-apply steganography method in drawing. Data hiding is done by replacing some data bits inside binary data with bits of secret data. In the order of bits in a byte (1byte = 8bit), there is the most Significant Bit and the least significant bit (Least Significant Bit).

The LSB bit is an easily replaceable bit, because in its implementation, when an example image has a blue color, the change does not mean that it only changes the byte value one higher or one lower than the previous value and will not be visible by sight humans because the changes are too small.

If a lossy compression format is used, hidden secret messages may be lost. If a 24 bit color image is used as a cover, a bit of each RGB component can be used so that 3 bits can be stored on each pixel. An 800 x 600 pixel resolution image can be used to hide 1,440,000 bits (180,000 bytes) of confidential data [7].

Spread Spectrum is a technique that includes cover-image as noise and as pseudo- nise into the cover-image. Values can be added to the cover object by transmitting with added value. This value must be transmitted below the level of noise that values are added to it. This means that capacity is determined by the cover-object. While the inserted value can be a real number, in practice, it is difficult to insert and extract the real value of a single bit of data. To be able to transmit more than one bit, the cover-object is divided into small sections, called sub-cover objects.

When the sub-cover-object averaged (tile) this method is said to use direct-ended spread spectrum steganography. When the sub-cover-object consists of separate points distributed throughout the cover object, in this case the cover-image, this method is called the frequency-hopping spread spectrum steganography. This method requires a thorough search process of the cover-object to get the carrier (which will be inserted information) and maximize the use of data contained within the cover-object. [9]

Mean Square Error (MSE) is the error value between the original image and the manipulation image. MSE is used to perform the process of Peak Signal to Noise Ratio (PSNR) is the ratio between the maximum value of the signal as measured by the amount of noise that affects the signal

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}||I(i,j) - K(i,j)||^2$$

PSNR is usually measured in decibels (dB). PSNR is used to know the quality comparison of cover image before and after inserted message.

$$PSNR = 10.log_{10}\left(\frac{MAX^2}{MSE}\right)$$

EXPERIMENT SETUP

The simulation tool and another simulation environment can be seen in Table-1.

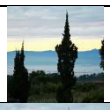
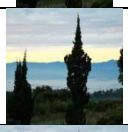
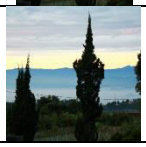
Table-1. Simulation setup.

Simulation tool	Matlab R2016a 9.0.0
OS	Windows 8.1 Pro
CPU	Intel core i3-3217U
RAM	4 Gb
Supporting Tools	Photoshop CC 2016, Microsoft Excel, Notepad ++

Steganography testing using JPEG image format with 3 categories Testing Media that still categorized will use 2 method that is Least Significant Bit and Spread Spectrum.

Test Media 1 uses the same JPEG image, but has different resolutions starting at 200 x 200 pixels, 400 x 400 pixels, 600 x 600 pixels, 800 x 800 pixels and 1000 x 1000 pixels as shown in Table 2.

Table-2. Test media 1.

No	JPEG image	Image resolution	Image name
1.		200 x 200	E1_2.jpg
2.		400 x 400	E1_4.jpg
3.		600 x 600	E1_6.jpg
4.		800 x 800	E1_8.jpg
5.		1000 x 1000	E1_10.jpg

Testing Media 2 uses different JPEG images and has different resolutions starting from 200 x 200 pixels, 400 x 400 pixels, 600 x 600 pixels, 800 x 800 and 1000 x 1000 pixels as shown in Table-3.

Table-3. Test media 2.

No	JPEG Image	Image Resolution	Image Name
1.		200 x 200	E2_Sea.jpg
2.		400 x 400	E2_Udon.jpg
3.		600 x 600	E2_Cat.jpg
4.		800 x 800	E2_Japan.jpg
5.		1000 x 1000	E2_Flower.jpg

RESULT

Simulation 1: LSB & spread spectrum test media 1

In simulation 1, testing is done on Test Media 1 by comparing the use of LSB and Spread Spectrum methods. With the insertion of a 12 bytes secret message "jordyardianbagaskara". The value of MSE and PSNR will be obtained, and then will be seen which method has the best steganography quality.

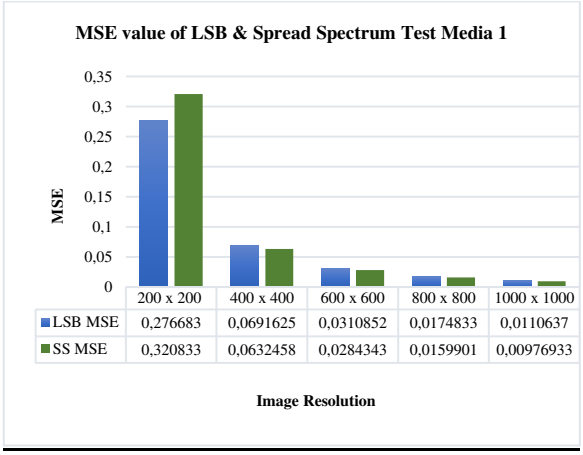


Figure-2. MSE of LSB & spread spectrum test media 1.

The value of MSE in Figure-2 using Test Media 1 shows that the use of LSB method has decreased MSE value, starting at 200 x 200 image with value 0,276683 until image 1000 x 1000 with value 0, 0110637. In the use of Spread Spectrum method, MSE value also decreased in image 200 x 200 with value 0,320833 until image 1000 x 1000 with value 0, 00976933.

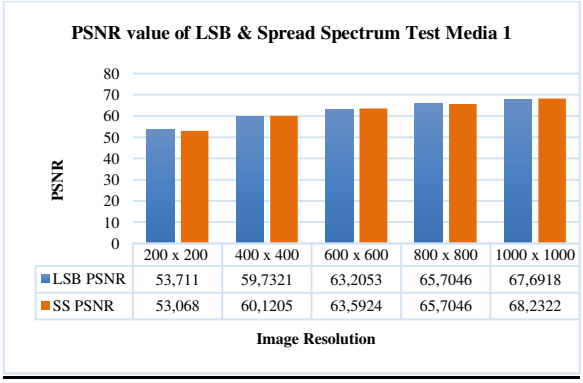


Figure-3. PSNR of LSB & spread spectrum test media 1.

The value of PSNR in Figure-3 using Test Media 1 shows that the use of LSB method has an MSE value that increases, starting with 200 x 200 image with value 53,711 dB up to 1000 x 1000 image with value 67,6918 dB. In the use of Spread Spectrum method, MSE value also decreased in image 200 x 200 with value 53,068 dB up to image 1000 x 1000 with value 68, 2322 dB.

Table-4. LSB processing time test media 1.

Name	Resolution	Embedding	Extracting
E1_2.jpg	200 x 200	0.311336	0.301203
E1_4.jpg	400 x 400	0.842315	0.883317
E1_6.jpg	600 x 600	1.820414	1.751754
E1_8.jpg	800 x 800	2.918946	3.077969
E1_10.jpg	1000 x 1000	4.707057	4.510795

Table-5. Spread spectrum processing time test media 1.

Name	Resolution	Embedding	Extracting
E1_2.jpg	200 x 200	0.280073	0.301213
E1_4.jpg	400 x 400	0.842315	0.883317
E1_6.jpg	600 x 600	1.820414	1.751754
E1_8.jpg	800 x 800	2.918946	3.077969
E1_10.jpg	1000 x 1000	4.707057	4.510795

Simulation 2: LSB & spread spectrum test media 2

In simulation 2, testing is done on Test Media 2 by comparing the use of LSB and Spread Spectrum methods. With the insertion of a 12 bytes secret message "jordyardianbagaskara". The value of MSE and PSNR will be obtained, and then will be seen which method has the best steganography quality.

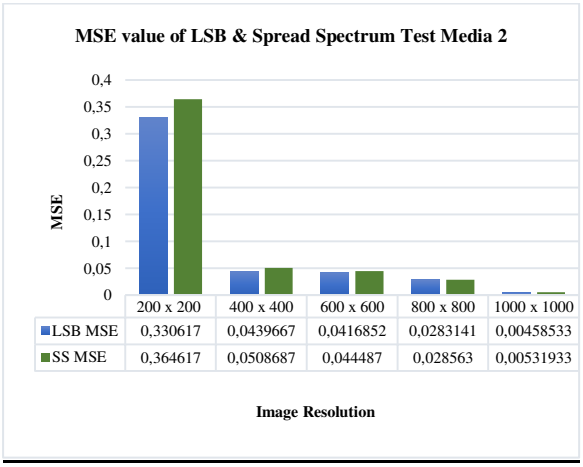


Figure-4. MSE of LSB & spread spectrum test media 2.

The next study was done on Test Media 2. The results obtained as in Figure-4 where the MSE value in different images. On the use of the LSB method, the image resolution 200 x 200 is worth 0.330617 with decreasing values up to 1000 x 1000 resolution worth 0.00458533.

In the use of Spread Spectrum method, the value of MSE image resolution 200 x 200 worth 0.364617 decreased up to 1000 x 1000 resolution image worth 0.00531933.

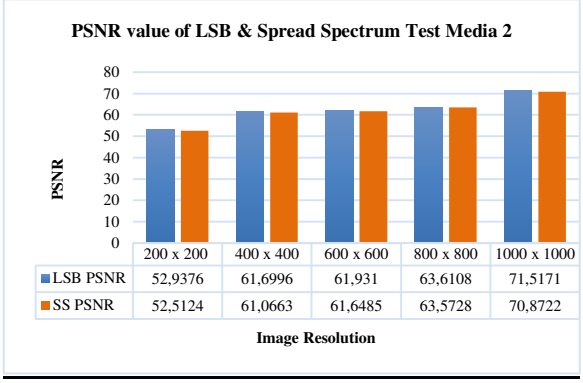


Figure-5. PSNR of LSB & spread spectrum test media 2.

The next study was done on Test Media 2. The results obtained as in Figure-4 where the PSNR value in different images. On the use of the LSB method, the image resolution 200 x 200 is worth 52, 9376 dB with increasing values up to 1000 x 1000 resolution worth 71, 5171 dB.

In the use of Spread Spectrum method, the value of MSE image resolution 200 x 200 worth 52, 5124 dB increased up to 1000 x 1000 resolution image worth 70, 8722 dB.

Table-6. LSB processing time test media 2.

Name	Resolution	Embedding	Extracting
E2_Sea.jpg	200 x 200	0.0523561	0.415751
E2_Udon.jpg	400 x 400	0.939633	0.893195
E2_Cat.jpg	600 x 600	1.90677	1.989578
E2_Japan.jpg	800 x 800	3.194962	3.123429
E2_Flower.jpg	1000 x 1000	4.918038	5.354542

Table-7. Spread spectrum processing time test media 2.

Name	Resolution	Embedding	Extracting
E2_Sea.jpg	200 x 200	0.353575	0.332451
E2_Udon.jpg	400 x 400	0.885494	0.984221
E2_Cat.jpg	600 x 600	1.867196	1.866532
E2_Japan.jpg	800 x 800	3.324791	3.068917
E2_Flower.jpg	1000 x 1000	4.962142	4.922915

Thus it can be seen that the value of MSE will determine the value of the PSNR image, where as the MSE value decreases on the image also the value of PSNR will increase.

As a reference that a good MSE value will be worth close to 0, and the PSNR score will be above 40 dB. Thus the test on Test Media 1 experienced success where both methods showed the value of MSE approaching 0 and the value of PSNR above 40 dB.

CONCLUSION AND FUTURE WORK

In testing the image size, image size used as a container medium (original image) is very influential for the steganography process. The larger the size of the original image resolution to eat will be the more number of pixels that can be processed and can increase the time of the image process.

In testing the image quality, image size used as container media (original image) is very influential for changes in the value of MSE and PSNR. The smaller the resolution of the image, the image changes will be more visible, while the greater the image resolution of the container, the image changes will be less visible.

In testing the message size, the size of the messages used may affect the processing time of the image. The larger the message size used in the embedding and extracting process, the greater the time it takes because more and more processes are done by the program.

In testing the message size, the message size used may affect the quality of the steganographic image. The larger the message size used in the process, the more pixel bits will be changed thus increasing the MSE value and the decreasing value of PSNR.

REFERENCES

[1] Cox Ingenar J. 2008. Digital Watermarking and Steganography. Burlington, Morgan Kaufmann Publisher.

[2] Fridrich Jessica; M. Goljan; D. Soukai. 2014. Seaching for the Stego Key. Proceedings of SPIE, Electronic Imaging, Security, Steganograohy, and Watermarking of Multimedia Contents. 5306: 70-82.

[3] Haines, Richard F.; Chuang, Sherry L. 1 July 1992. The effects of video compression on acceptability of images for monitoring life sciences experiments (Technical report). NASA. NASA-TP-3239, A-92040, NAS 1.60:3239. Retrieved 13 March 2016. The JPEG still-image compression levels, even with the large range of 5:1 to 120:1 in this study, yielded equally high levels of acceptability.

[4] 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.

[5] Hakim Muhammad. 2016. Studi dan Implementasi Metode LSB dengan Preprocessing Kompresi Data dan Ekspansi Wadah.

[6] Hamilton. 1992. Eric JPEG File Interchange Format Version 1.02 C-Cube Microsystems 1778 McCarthy Blvd. September 1.

[7] 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.

[8] Pranoto Budi. 2017. Steganografi Pada Citra Digital Menggunakan Metode Spread Spectrum Dan Metode Least Significant Bit (LSB) Modification. Fakultas Sains dan Teknologi. Universitas Islam Negeri Sultar Syarif Kasim. Riau Pekanbaru. Accessed on 18-09.

[9] Trithemius Johannes. 2017. Polygraphiae (cf. p. 71f). German. Digitale Sammlungen. Accessed on 18-09.

[10] 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.