eISSN: 2477-7986

Journal of Measurements, Electronics, Communications, and Systems *(Vol.05, Pg.07-14, December 2019)*

Dual Steganography in Digital Images with Spread Spectrum Insertion Method

Reza Ahmad Fauzan, Sofia Saidah*, Bambang Hidayat, Nor Kumalasari Caecar Pratiwi

School of Electrical Engineering, Telkom University, Indonesia

**Corresponding author: sofiasaidahsfi@telkomuniversity.ac.id*

Manuscript received 12 September 2018; revised 25 October 2018; accepted 29 November 2018

Abstract

This study aims to prove whether embedding a stego-image within another cover can be performed to deceive hackers or unauthorized people. In steganography, both concealing the fact that secret message is sent and its content are concerned. Dual steganography means to make unauthorized people think that the first cover is the real message. The first step is to embed the secret text message into the first cover image using Spread Spectrum (SS) method. After that, the resulting stego-image was transformed using the Discrete Wavelet Transform (DWT) method followed by the insertion process using the Singular Value Decomposition (SVD) method. The result of this study shows that the system can perform dual steganography with good imperceptibility. Parameters measured in the average of 35 dB of PSNR and 30 dB of SNR in the first embedding process; meanwhile, for the second process the system performed in the average of 41 dB of PSNR and 38 dB of SNR. Also, in the extraction process, BER measured close to 0. Although some basic attack scenarios such as Gaussian noise, Salt and Pepper noise, Low Pass Filter (LPF) and High Pass Filter (HPF) were performed in this research, more advanced attack scenarios can be discussed in future research; for instance, compression and geometric transform.

Keywords: DWT; Dual Steganography; SVD; Spread Spectrum.

DOI: 10.25124/jmecs.v5i1.2073

1. Introduction

Steganography is a practice of concealing information within other media, so the information can only be known and accessed by authorized people. In this digital era, that information can be text, image, audio or video. The fundamental principle of steganography is to exploit the weakness of human senses, both sight and hearing so that the inserted information is unlikely to notice. The study of steganography continues to increase in popularity, especially the one that used a digital image as a host or cover. In this study, the insertion process was somewhat different. The insertion process is carried out twice with the aim of deceiving unauthorized people [1].

In general, the dual steganography process is almost the same as steganography with a single insertion, which consists of the insertion and extraction process. The difference is that in dual steganography there are two insertion and extraction processes. Therefore, if steganography generally requires one cover, dual steganography requires two covers [2].

Dual steganography envelopes information to such a degree that it is invisible to a spectator. As identified by Makwana and Chudasama in [2], conduct an experiment of dual steganography using Least Significant Bit insertion method and Discrete Wavelet Transform method with image and video cover. Combining the work of two steganography techniques provides security for secret information but a single one can not guarantee absolute security data. Therefore to provide more security to the information at the time of communication over an unsecured channel a novel advance technique for data security is needed.

The advantage of steganography over traditional encryption is that in steganography the message is concealed. However, steganography is not secure enough, as it easy to recover the secret message if its existence is known [3]. So it requires an additional layer for security. Using spread spectrum image steganography it can be obtained due to the necessity that both the sender and receiver possess the same key. As identified and explained by Marvel, Boncelet, and Retter [4], the Spread Spectrum technique provides a method for concealing a digital signal within a cover image without increasing the size or dynamic range of the image. Additionally, the original image is not needed for extraction and slightly better robustness than Least Significant Bit insertion method.

The online version of this article can be found at: https://journals.telkomuniversity.ac.id/jmecs/article/view/2073

In steganography, there are two popular schemes that can be performed for image steganography which are spatial domain and transform domain. The transform domain is also known as the frequency domain. Transforming the image into the frequency domain allows embedding secret messages in the high-frequency sub-band to preserve unaltered to improve image quality. As explained by Chen and Lin in [5], Discrete Wavelet Transform is one of the simplest transformation methods that does not require a lot of computation resources.

Abdallah, Hadhoud, and Shaalan in [6] explained that using Singular Value Decomposition approach in the embedding process of steganography can maintain a good fidelity. Additionally, the result showed that the combination of iterations and redundancy can provide large error reduction.

This paper seeks a good performance combining Spread Spectrum, Discrete Wavelet Transform and Singular Value Decomposition in dual steganography system so it will be able to deceive unauthorized parties. Although [2] resulted a good stego-data, it requires a relatively big size of the cover. This paper offers an alternative that requires a smaller size of cover. Additionally, since this dual steganography system uses the Spread Spectrum instead of Least Significant Bit insertion method, it provides a better error reduction.

2. Research Method

2.1 Discrete Wavelet Transform (DWT)

Discrete Wavelet Transform uses filters to analyze and reconstruct the signals [5,7]. DWT was produced and delivered by S. Mallat in 1989 which utilized the wavelet decomposition of transformed low pass filters (averaging) and high pass (differencing) filters. Filters generally serve to separate the signals in different frequency ranges. The spatial domain signal generated by DWT is obtained by filtering signals using LPF and HPF as shown in the Fig. 1, this procedure is known as Mallat Tree decomposition [8].

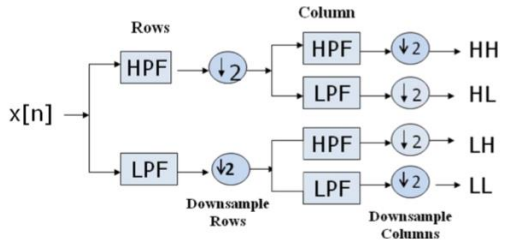

Fig. 1. Two Dimension (2D) of Discrete Wavelet Transform System

An input signal denoted by $x[n]$, where n is an integer number. At each level, HPF produces the detailed information or detailed coefficient, denoted as $d[n]$, while the LPF produces approximate coefficient, denoted as $a[n]$. Data input is passed through a set of LPF and HPF. The output of a high pass and low pass filter has a down sample of 2. DWT of an image represents the sum of multiple wavelets. The human eye is less sensitive to high frequency details [9]. On DWT 2 levels, it takes two operations.

Similar to DWT, which can be explained using filter theory, reconstruction can also be done using IDWT. The process is actually just the opposite of DWT process. The DWT coefficient is done by up sample which will automatically double the length of each decomposition signal. Then the signal is convoluted with a reconstruction scale filter (reconstruction scale filters are only genuine scale filters that have been turned left to right). These results are then added together to be returned to the original signal form [10].

2.2 Spread Spectrum Image Steganography

The basic concept of this insertion method is to insert narrowband information signals into wideband noise and then add the noise into the cover image. The added noise is like noise that occurs during the image acquisition process. If the noise occurs at a low level, it will not be easily detected by the human visual sense or computer analysis without using the original image [4].

In the Spread Spectrum method, the text message is converted into binary form and the message is multiplied by pseudorandom noise to produce information noise.

On the receiving side, the *stego-image* is received by the recipient who has the same key, namely the same pseudorandom noise to extract the received message.

2.3 Singular Value Decomposition

Singular Value Decomposition (SVD) of a A matrix is a factorization of A matrix into three matrices. The three matrices are $A = USV^T$, where is U and V are orthogonal matrix and S is a diagonal matrix with positive real numbers [6,11]. The matrices of U, S and V are defined by the equation (1):

$$A^T A = VS^T U^T USV^T \quad (1)$$

Due to U is an orthogonal matrix,$U^T U = 1$, so the equation (1) becomes:

$$A^T A = VS^T SV^T \quad (2)$$

Further, the equation (3) and (4) is also simplified as the equation (2):

$$AA^T = USV^T VS^T U^T \quad (3)$$

$$AA^T = USS^T U^T \quad (4)$$

It can be seen that the $A^TA = VS^TSV^T$ is a diagonalized equation, as well as $AA^T = USS^TU^T$, then S^TS and SS^T are eigenvalues for each eigenvectors V and U. So to get the U, S and V matrices it is necessary to find eigenvalue and vector Eigen from A^TA and AA^T [12,13].

2.4 Design Model System

In general, the insertion process with dual steganography is as follows. In this study, dual steganography will be implemented using two covers in the form of images so that in this system there are two insertion processes and also two extraction processes as shown in the Fig. 2.

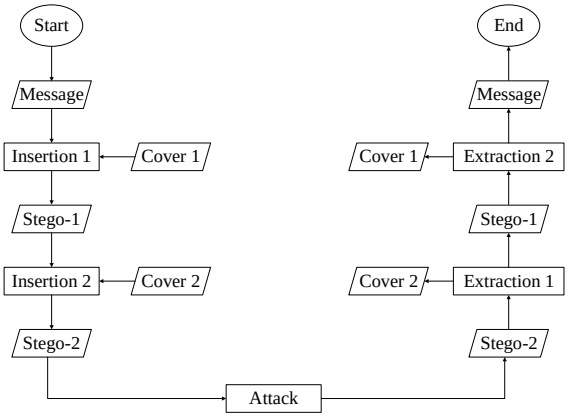

Fig. 2. General System Diagram

2.5 First Insertion Process

The first insertion process is carried out using the Spread Spectrum method explained by the Fig. 3 below. Secret messages in text form are converted into ASCII binary numbers, then binary secret messages are encoded. The result of coding a secret message is in the form of a black and white image that represents the bits $'1'$ and $'0'$ as shown in the Fig. 4.

The purpose of this coding process is to spread every bit of a secret message into a certain area of the image so that the message is not easily lost because it has backup data that is spread over the area. The area of the distribution is determined depending on the number of messages to be inserted. The more messages that will be inserted, the wider the area of distribution will be smaller and vice versa. In this system for the image cover size of 400×400 pixels, three conditions are determined:

K = 50 pixel for $x < 64\ bit$

K = 25 pixel for $64\ bit < x < 256\ bit$

K = 16 pixel for $256\ bit < x < 625\ bit$

Where K is length of the spread box in pixels and x is number of messages in bit.

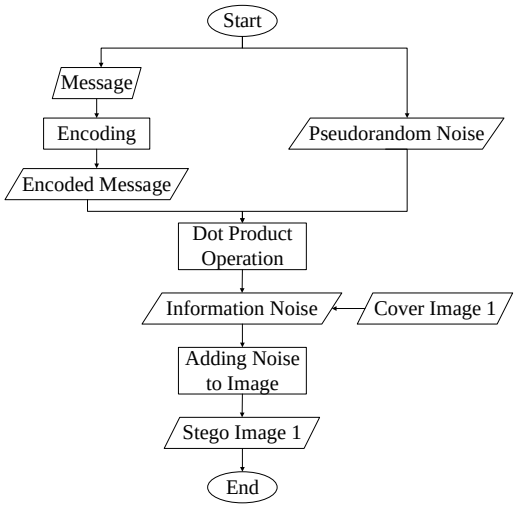

Fig. 3. System Diagram at First Insertion

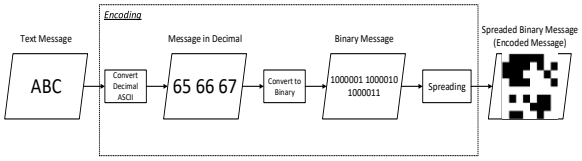

Fig. 4. Coding Process

2.6 Second Insertion Process

In the second insertion process, the first insertion *stego-image* is then made to change the domain first from the spatial domain to the frequency domain using a Discrete Wavelet Transform (DWT) then insertion using the Singular Value Decomposition (SVD) method. The *stego-image* generated through the first insertion process enters the second insertion process. SVD is done on *stego-image* to produce a Singular Value from the *stego-image*. Taken one layer on the second cover image, in this system the second layer or green layer is taken, then transformed into the frequency domain using the DWT 1 level method, resulting in 4 sub band namely LL (Low Low), LH (Low High), HL (High Low) and HH (High High). Then the HH sub band is taken to do the SVD process and produce a Singular Value from the sub band.

After that the Singular Value from the HH sub band is modified using the equation (5):

$$S_{stego} = S_{HH} + \left(S_{message} \times \alpha\right) \quad (5)$$

Where S_{stego} is modified singular value, S_{HH} is sub band HH of singular value, $S_{messages}$ is messages value if singular and α is embedding power (this system using $\alpha = 0.0002$).

Then the Singular Value from the HH sub band is reconstructed using the SVD inverse to the modified HH sub band. Then the DWT inversion process and the layer reconstruction process are carried out to produce the second *stego-image*. The Fig. 5. shows second insertion process.

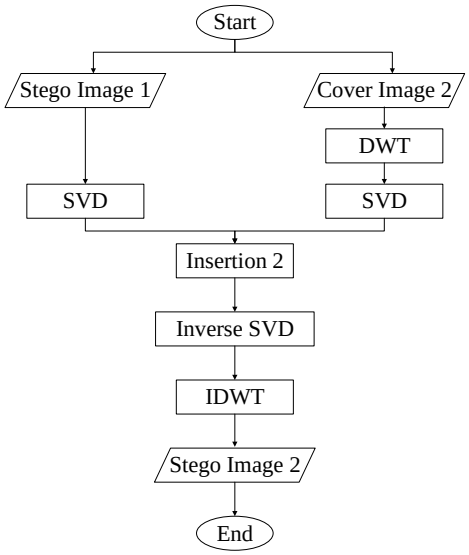

Fig. 5. System Diagram at Second Insertion

2.7 First Extraction Process

The first extraction process is simply as an opposite process of second insertion as shows as Fig. 6. below.

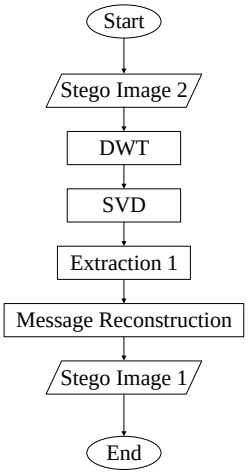

Fig. 6. System Diagram at First Extraction

The second layer from the second *stego-image* is transformed using DWT then HH subband is taken for the next SVD process[14]. In the SVD process, the extraction is performed using the equation (6):

$$S_{Message} = \frac{S_{extraction} - S_{HH}}{\alpha} \quad (6)$$

Subtraction of $S_{extraction}$, which is singular value of extracted HH sub band, by S_{HH}, which is singular value of the original HH sub band will be divided by defined embedding power, which represented by α. The result of this process is the singular value of the secret message itself represented by $S_{Message}$.

2.8 Second Extraction Process

In the second extraction process, the secret message can be obtained by performing the opposite process of the first insertion. The representation of the process should be as follows and shown in Fig. 7

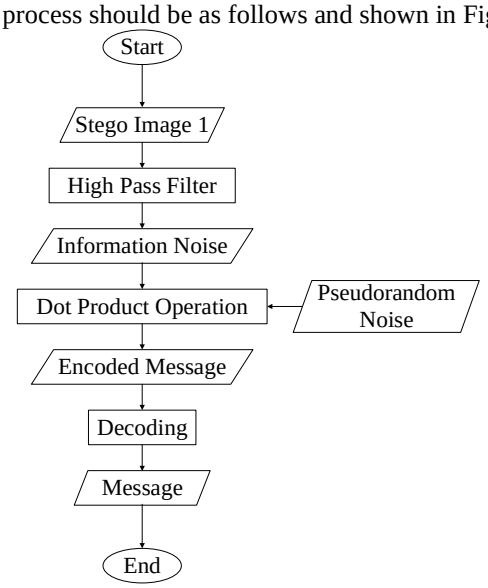

Fig. 7. System Diagram at Second Extraction

The first *stego-image* that is recovered through the first extraction process is then passed to the High Pass Filter to get the information noise. After that, the information noise is processed using dot product operation with the same pseudorandom-noise as the first insertion process, so that the secret message is coded [3]. The coded secret message is carried out the decoding process to get the secret message back in binary form. Decoding is done by averaging the gray intensity of pixels in one distribution area into one bit of binary number. For example, in an area the average distribution of colors is black, then that area represents the bit '0' and the white area represents the bit '1'. So we get a secret message in the form of binary numbers. After obtaining a secret message in the binary form then the conversion process is carried out back into text.

4. Result

The test scenarios that performed in this study use images from SIPI Image Database of USC University [15]. There are 5 greyscale images for cover 1 with .tiff format as shown on Figure 8-12 and RGB images on Figure 13-17 for cover 2. The resolution of the images are 400×400 pixel for cover 1, and 800×800 for cover 2.

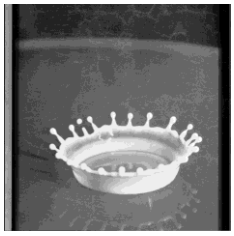

Fig. 8 Splash

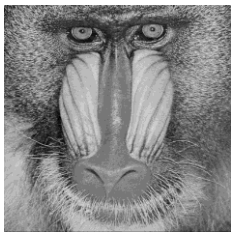

Fig. 9 Baboon

Fig. 10 Airplane

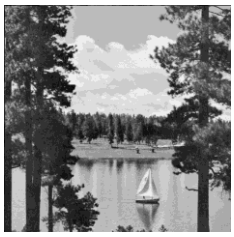

Fig. 11 Sailboat

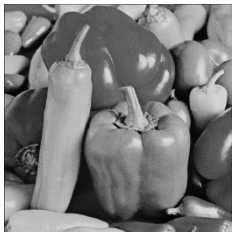

Fig. 12 Pepper

Fig. 13 Richmond

Fig. 14 Oakland

Fig. 15 San Diego

Fig. 16 Shreveport

Fig. 17 San Francisco

Table 1. Test Result Parameter for First Insertion with Spread Spectrum (SS) Method

	PSNR (dB)	SNR (dB)
Splash	35.720	28.830
Baboon	35.751	30.281
Airplane	35.756	32.969
Sailboat	35.755	30.622
Pepper	35.753	30.010

The results of the first insertion, which is shown on Table 1, are then transformed from the spatial domain to the frequency domain by using the Discrete

Wavelet Transform (DWT) method, followed by the insertion process using the Singular Value Decomposition (SVD) method.

The optimal results generated from dual steganography systems are shown on Table 2.

Table 2. Test Result Parameter for the Second Insertion

PNSR (dB)					
	Richmond	Oakland	San Diego	Shreveport	San Francisco
Splash	43.532	43.533	43.532	43.531	43.532
Baboon	42.122	42.111	42.120	42.112	42.111
Airplane	39.432	39.422	39.421	39.420	39.424
Sailboat	41.770	41.772	41.763	41.769	41.771
Pepper	42.380	42.389	42.387	42.386	42.388
SNR (dB)					
	Richmond	Oakland	San Diego	Shreveport	San Francisco
Splash	40.532	40.733	38.322	39.091	39.711
Baboon	38.971	39.312	36.910	37.688	38.292
Airplane	36.282	36.624	34.271	34.991	35.601
Sailboat	38.626	38.964	36.565	37.332	37.955
Pepper	39.232	39.571	37.177	37.944	38.566
SSIM					
	Richmond	Oakland	San Diego	Shreveport	San Francisco
Splash	0.994	0.998	0.991	0.996	0.998
Baboon	0.996	0.996	0.995	0.996	0.997
Airplane	0.995	0.994	0.998	0.999	0.997
Sailboat	0.990	0.991	0.991	0.992	0.995
Pepper	0.991	0.993	0.994	0.994	0.993
BER (%)					
	Richmond	Oakland	San Diego	Shreveport	San Francisco
Splash	0.000	0.000	0.000	0.000	0.000
Baboon	0.000	0.000	0.000	0.000	0.000
Airplane	0.000	0.000	0.000	0.000	0.000
Sailboat	0.000	0.000	0.000	0.000	0.000
Pepper	0.000	0.000	0.000	0.000	0.000

Figure 18-22 shows images result after insertion process. We can infer that there is no major different after the message was embedded within the cover images.

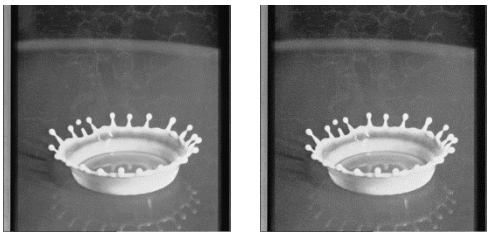

Fig. 18 Original Cover Image "Splash" (Left) and Stego-Image (Right)

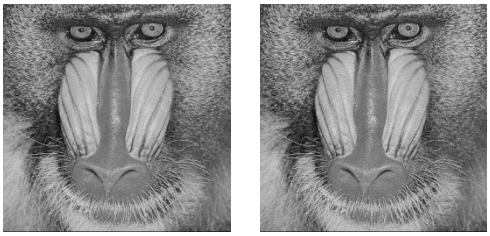

Fig. 19 Original Cover Image "Baboon" (Left) and Stego-Image (Right)

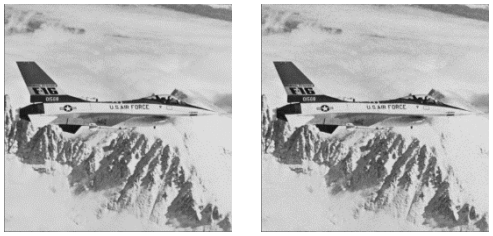

Fig. 20 Original Cover Image "Airplane" (Left) and Stego-Image (Right)

Fig. 21 Original Cover Image "Sailboat" (Left) and Stego-Image (Right)

Fig. 22 Original Cover Image "Pepper" (Left) and Stego-Image (Right)

Figure 23-27 shows the sample comparison between cover image 2 and *stego-image 2* on the second insertion process. The test resulted that the lowest value of PSNR 39.4 dB and the highest at 43.5 dB, also the lowest SNR at 34.2 dB and the highest at 40.5 dB. So, we can say that the difference in term of image quality is not significant. Average result of the parameters are 41.845 dB of PSNR, 37.971 dB of SNR, 0.995 of SSIM and 0% of BER.

4. Discussion

The purpose of this study is to prove whether dual steganography can be done. Test scenario results show good system performance so that if the right cover is used it can be used to deceive unauthorized parties. This system is also tested with basic attacks such as Gaussian noise, salt and pepper noise, LPF and HPF filters. The result shows that only LPF filters that can attack the system. The more advanced attacks such as compression and geometric transforms might be corrupting the message. The future work is needed to figure out how to make the system robust to those advanced attacks.

However, this system can be classified as semi-blinded steganography so it requires some information from the message and the cover in order to extract the secret message.

Nevertheless, semi-blinded steganography has an advantage in terms of robustness compared to the Least Significant Bit that conducted by Makwana and Chudasama in [2] which is blinded steganography.

5. Conclusion

The combination of spread spectrum, discrete wavelet transform, and singular value decomposition method on dual steganography maintains the secrecy of steganography. We show that the system can be used for semi-blinded steganography and has an advantage in terms of robustness parameter. We also shows that this method can be termed as a new successful technique of dual steganography.

Fig. 23 Original Cover Image "Richmond" (Left) and Stego-Image (Right)

Fig. 24 Original Cover Image "Oakland" (Left) and Stego-Image (Right)

Fig. 25 Original Cover Image "San Diego" (Left) and Stego-Image (Right)

Fig. 26 Original Cover Image "Shreveport" (Left) and Stego-Image (Right)

Fig. 27 Original Cover Image "San Francisco" (Left) and Stego-Image (Right)

Reference

[1]. X. Zhou, W. Gong, W. Fu and L. Jin, "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography," 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), pp. 1-4, 2016.

[2]. J. Makwana and S. Chudasama, "Dual Steganography: A New Hiding Technique for Digital Communication," International Journal of Advanced Research in Electrical, Electronic and Instrumentation Engineering, vol. V, no. 4, pp. 3184-3188, 2016.

[3]. J. Kulkarni, K. Nair and M. Warde, "Secure Semi-Blind Steganography using Chaotic Transform," International Conference on Computing for Sustainable Global Development, pp. 2669-2673, 2016.

[4]. L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread Spectrum Image Steganography," IEEE Transactions on Image Processing, vol. VIII, no. 8, pp. 1075-1083, 1999.

[5]. P.-Y. Chen and H.-J. Lin, "A DWT Based Approach for Image Steganography," International Journal of Applied Science and Engineering, vol. IV, no. 5, pp. 275-290, 2006.

[6]. H. A. Abdallah, M. M. Hadhoud and A. A. Shaalan, "An Efficient SVD Image Steganographic Approach," Computer Engineering & Systems, pp. 257-262, 2009.

[7]. A. Zakaria dan R. Munir, "Steganografi Citra Digital Menggunakan Teknik Discrete Wavelet Transform pada Ruang Warna CIELab," 2015.

[8]. B. Gupta Banik and S. K. Bandyopadhyay, "A DWT Method for Image Steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. III, no. 6, pp. 983-989, 2013.

[9]. N. F. Johnson, Z. Durie and S. Jajodia, Information Hiding: Steganography and Watermarking - Attacks and Countermeasures, New York: Kluwer Academic Publishers, 2001.

[10]. H. Olkkonen, Discrete Wavelet Transforms: Algorithms and Applications, Rijeka: InTech, 2011.

[11]. E. Biglieri and K. Yao, "Some Properties of Singular Value Decomposition and Their Applications to Digital Signal Processing," Signal Processing 18, pp. 277-289, 1989.

[12]. Y. Zeng and Y.-C. Liang, "Eigenvalue-Based Spectrum Sensing Algorithms for Cognitive Radio," IEEE Transactions on Communications, vol. 57, no. 6, pp. 1784-1793, 2009.

[13]. K. S. Babu, K. B. Raja, U. M. Rao, R. K. A, V. K. R and L. M. Patnaik, "Robust and High Capacity Image Steganography using SVD," IET-UK International Conference on Information and Communication Technology in Electrical Sciences, pp. 718-723, 2007.

[14]. K. Nair, K. Asher and J. Joshi, "Implementing Semi-Blind Image Steganography with Improved Concealment," International Journal of Computer Applications, vol. 4, pp. 14-19, 2015.

[15]. USC University of California, "USC-SIPI Image Database," USC Viterbi School of Engineering, 1977. [Online]. Available: http://sipi.usc.edu/database/. [Accessed 27 August 2019].

Reza Ahmad Fauzan received bachelor degree on Telecommunication Engineering study program at Telkom University. His area of expertise is information signal processing

Bambang Hidayat received bachelor degree at ITB and received master and doctoral degree Universite De Rennes I france. He was a founder of Telkom University at 1989 and he is working as a lecturer. The area of expertise is information signal processing, especially in image and audio processing.

Sofia Saidah received bachelor and master degrees in Telecommunications Engineering at telkom university. Currently working as a lecturer at Telecomunication Engineering of Telkom University. The area of expertise is information signal, image and audio processing.

Nor Kumalasari Caecar Pratiwi received bachelor degrees from Telkom University and received master degree at ITB. Currently she is a lecturer at Telecomunication Engineering of Telkom University. Her expertise is information signal processing and image processing.