Image Steganography Using Combine of Discrete Wavelet Transform and Singular Value Decomposition for More Robustness and Higher Peak Signal Noise Ratio

Adam Nevriyanto [1st]
Department of Computer Engineering
Faculty of Computer Science
Indralaya, Palembang, Indonesia

Sutarno Sutarno [2nd]
Department of Computer Engineering
Faculty of Computer Science
Indralaya, Palembang, Indonesia

Erwin Erwin*
Department of Computer Engineering
Faculty of Computer Science
Indralaya, Palembang, Indonesia
*Corresponding authour: erwin@gmail.com

Sri Desy Siswanti [3rd]
Department of Computer Engineering
Faculty of Computer Science
Indralaya, Palembang, Indonesia

***Abstract*-----This paper presents an image technique Discrete Wavelet Transform and Singular Value Decomposition for image steganography. We are using a text file and convert into an image as watermark and embed watermarks into the cover image. We evaluate performance and compare this method with other methods like Least Significant Bit, Discrete Cosine Transform, and Discrete Wavelet Transform using Peak Signal Noise Ratio and Mean Squared Error. The result of this experiment showed that combine of Discrete Wavelet Transform and Singular Value Decomposition performance is better than the Least Significant Bit, Discrete Cosine Transform, and Discrete Wavelet Transform. The result of Peak Signal Noise Ratio obtained from Discrete Wavelet Transform and Singular Value Decomposition method is 57.0519 and 56.9520 while the result of Mean Squared Error is 0.1282 and 0.1311. Future work for this research is to add the encryption method on the data to be entered so that if there is an attack then the encryption method can secure the data becomes more secure.**

***Keywords*— Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Image Steganography, Peak Signal Noise Ratio (PSNR), Mean Squared Error (MSE)**

I. INTRODUCTION

Hiding information is a very important topic in the field of information security. As a major branch of information, steganography is an art hidden communication, which is where the intention is to transmit a secret message with embedded is an object, such as image, audio, and video. Two of the most important objectives and the capacity of steganography is not detected, which is a good steganography to embed as many loads with minimal distortion[1],

Steganography techniques that there are two approaches, spatial domain and frequency domain. Mechanical Least Significant Bit (LSB) is included in the category of the spatial domain.[2]filed LSB insertion method whereby data hiding techniques using the last bit of the cover image that cannot be known with the naked eye. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) categorized the frequency domain.[3] Has done a survey analysis on a variety of steganography techniques include DCT and DWT.

Data hiding can be effectively performed in the frequency domain. Steganography is for securing image using DCT [Discrete Cosine Transform] is a widely used method. DCT allows an image into three frequency bands, namely the Low-frequency band (FL), the High-frequency band (FH) and Mid-frequency band (FM).

DCT changes the image into three frequency bands, they are the Low-frequency band (LFB), the High-frequency band (HFB), and the Mid-frequency band (MFB)[3]. DWT separating into 4 blocks, the first is low-low (LL), second is low-high (LH), third is high-low (HL), and the last, high-high (HH). In DWT's application, high-frequency components are separated from the low-frequency component that will help to achieve a place to insert a message into an image[4],[5]mentioned advantages in DWT algorithms for steganography application is processing time

and capacity while the DCT algorithm is better in image quality.

The problems come from the third algorithm lies in the measurement of the PSNR and MSE on image steganography in which the proposed method will make the image steganography be better especially for DWT algorithm. The method proposed in this study is the method of steganography DWT and Singular Value Decomposition (SVD). This technique is a development technique that is related to the frequency DWT Haar-DWT domain where the SVD will outline the cover image and the secret image that will improve the performance of steganography. SVD is applied to the sub-bands are high then watermark 1 and 2 are to be decomposed by the SVD watermark so that the data will be inserted into smaller ones

A good Steganography application must have high payload capacity, data must not be perceptible to the viewer and the hidden information should be successfully obtain at the receiver.

II. RELATED WORKS

In a study by S. Chandran and B. Khoushik [6], have been done comparison method of LSB, DCT, and DWT for the application of steganography, in which the performance of the DCT method is better than both methods. They have investigated performance by comparing the quality of stego image and cover image. The lack of methods of this methods is diverse. For the lack of LSB method is of invisibility and robustness, for DCT method is in robustness, whereas DWT method has small PSNR value and MSE is big enough.

Neeta Deshpande, et al. (2006) has proposed a technique Least Significant Bit (LSB) in which to hide data using the last bit of the cover image cannot be known by the unaided human eye[2]. This technique lack in robustness, invisibility and has a very small payload.

In 2012, one of the researchers has proposed combination technique with spatial domain and frequency domain[4], V. Saurabh Joshi, et al focus on increasing the capacity of hidden information while maintaining visual of the cover image. In these studies, obtained conclusions can help combine advantages and overcome some of the weaknesses of both domains and by using two-level DWT can gain greater capacity for data insertion for using frequency domain.

Algorithm SVD with various transformations such as DCT, DWT, and the DFT for the detection of image splicing[7] have been compared by Moghaddasi Z, et al. (2015), this paper shows the SVD-DCT has better detection value compared with SVD, SVD-DWT and SVD-DFT only with 25 dimensions. In the results, they say that the result is less than 80% and the reason is likely because of the differences between steganography and splicing operations.

Shallu Vohra, et al. (2017) shows that effectiveness method also checks against the different value of noise attack on stego image. The proposed steganography algorithms using LWT, DWT, DCT and SVD transformation that contributes more robust in comparison with many steganography algorithms. In this work, stego image is attacked by different types of noise but in future, we can test the effectiveness of these methods against other types of attacks such as cropping, rotational and resizing. But it must be improved using full band LWT-DCT-SVD and LWT-DWT-SVD and further can be extended to colour images and video processing[8].

In 2015, the proposed Hybrid DCT-DWT algorithm are to obtain further robustness of image steganography application by Anuradha Goswami et al.. The idea is to combined transform that joint transform eliminates the drawback of each other. Thus, we may get a good embedding data of steganography image method.

The proposed approach is imperceptible part of an image. In middle frequency coefficient set of the 3-level DWT transform of host image followed by block-level Discrete Cosine Transform and selected HH Discrete Wavelet Transform coefficient sets an image that was embedded. Their PSNR were robustness thus theirs has higher robustness to against visual attacks. But this research still needs more execute and calculate in many different types of attack[9].

There are many ways to compare quality in an image, for example by using the method of measurement Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) as he had done [5], [6], [10], [11], [12], [13], [14], [15], [16], [17] to analyze the image quality comparison.

In this paper will focus on a comparative analysis of performance and image quality of the original image steganography where the image will be measured based on the calculation of PSNR and MSE. With the addition of DWT, SVD algorithm will reduce the data is pasted on the image so as to make the data smaller and make the image quality of steganography not experienced many significant changes.

III. PROPOSED WORK

This is an additional method for DWT, where SVD will outline the cover image and secret image to improve the performance of image steganography. SVD is a matrix factorization of a real or complex matrix, with many useful applications in statistics and signal processing[18],

DWT used in this case is Haar-Discrete Wavelet Transform. Haar-DWT 2-stage process for processing image file. The first phase by scanning the pixels from left to right on the horizontal direction and do the addition and subtraction operation on neighbouring pixels to rows of pixels are exhausted. Low frequency obtained from the addition operation and high-frequency pixel obtained from the reduction operation.

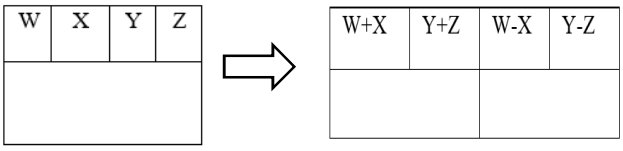


Fig. 1 The horizontal operation

The next stage by scanning pixels from top to bottom in the vertical direction, the same as the first step of adding and subtracting but the results still kept with the operating results of the addition of the above pixel and pixel reduction operation results stored inside of all the results of the calculations.

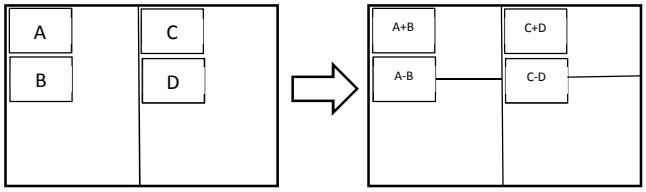


Fig. 2 The vertical operation

SVD is a matrix factorization technique that is generally used to produce low-rank approximation. The SVD transformation is a change of linear algebra for real or rectangular matrix factorization, such as image compression, noise reduction, and image watermarking[19]. Given an m × n matrix A with rank r, SVD on a matrix shown in equation (1)[20],

$$SVD(A) = U \times S \times V \tag{1}$$

Where U, S and V is the dimension of each m × m, m × n and n × n. U and V are two orthogonal matrices called left and right singular matrix, S is a diagonal matrix called the single matrix. With watermarking based, we can get that the methods are more robust against the usual image processing [19].

Algorithm:

Step 1: Read the cover image and text messages to be inserted.

Step 2: Convert the text into a binary form and then convert the binary result once again in the binary image (secret image).

Step 3: Make the process of DWT the second image with the 2D Haar Discrete Wavelet Transform and get the matrix 4 sub-bands LL1, HL1, LH1, and HH1.

Step 4: Make the process of sub-bands SVD on high.

Step 5: Combine the three components of the matrix SVD and paste the image into the secret of the cover image.

Step 6: Write stego image.

Step 7: For the extraction process is performed by applying IDWT message and does the sequence in reverse.

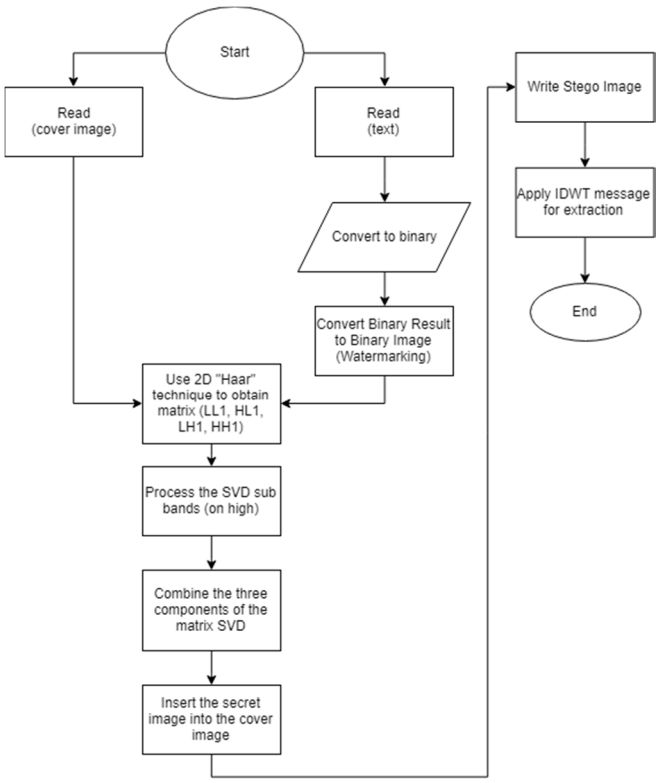


Fig.3 Flowchart of Watermarking and Extraction with DWT-SVD*

* do the sequence in reverse

IV. PERFORMANCE METRICS

In image processing applications, where an image is to be reconstructed the performance of the image processing algorithms need to be evaluated. Some metrics used to measure the efficiency of the image steganography is MSE and PSNR.

A. Mean Squared Error (MSE)

MSE value is obtained from the average intensity of original image's square f (x, y) and the resultant pixel image f '(x, y) can be written in the equation (2):

$$\text{MSE} = \frac{1}{XY}\sum_{y=0}^{Y-1}\sum_{x=0}^{X-1} e(y,x)^2 \tag{2}$$

Where, it is the difference error between the reference image and a distorted image $e(y,x)^2$

B. Peak Signal Noise Ratio (PSNR)

PSNR value is obtained from the pixel where it is difference of the reference image and the distorted image. All the pixel's SNR values are the most appropriate a max value that can be written in an equation (3):

$$PSNR = 10log\frac{p^2}{MSE} \tag{3}$$

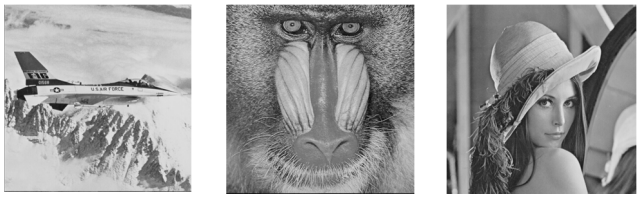
Where, p = 255, the 8-bit image

For optimal performance, values of MSE should be small and PSNR should be large.

V. RESULT AND DISCUSSION

The proposed method has been simulated using the MATLAB R2016a program on Windows 10 platform. A set of 8-bit grayscale images of size 512 × 512 are used as the cover image to form the stego image.

The cover image used for this study shows in fig. 4.



(a) (b) (c)

Fig. 4 (a) Jet. (b) Baboon. (c) Lena

For good performance of steganography image the PSNR and MSE values of stego image after embedding the message on every method are tabulated in table 1. For good steganography image, the value of PSNR at least must above 40 and the value of MSE should be close to 0. We take the reference of [6] and [21] for comparison with image baboon and jet, and for image lena, we used the reference of [22][23][24][8][9], which shows in table 1 and table 2.

TABLE 1. PSNR AND MSE MEASUREMENT RESULTS WITH IMAGE BABOON AND JET

No	METHOD	PSNR		MSE	
		Baboon	Jet	Baboon	Jet
1	LSB[6]	51.3214	50.9015	0.4834	0.5325
2	DCT[6]	53.2092	52.9532	0.3130	0.3320
3	DWT[6]	46.8262	46.7309	1.3610	1.3912
4	DCT with OTP Encryption[21]	51.1242	51.1242	0.5020	0.5020
5	Proposed Method	57.0519	56.9520	0.1282	0.1311

TABLE 2.PSNR MEASUREMENT RESULTS WITH IMAGE LENA

No	METHOD	PSNR
1	Novel DWT[22]	54.4378
2	IWT[23]	54.92
3	Block Matching DWT[24]	46.2412
4	Hybrid LWT-DWT-SVD[8]	46.5432
5	Hybrid DCT-DWT[9]	44
6	Proposed Method	58.020

For analysis graph of PSNR with image baboon a jet can be observed in figure 5 and for the image, lena shows in figure 6.

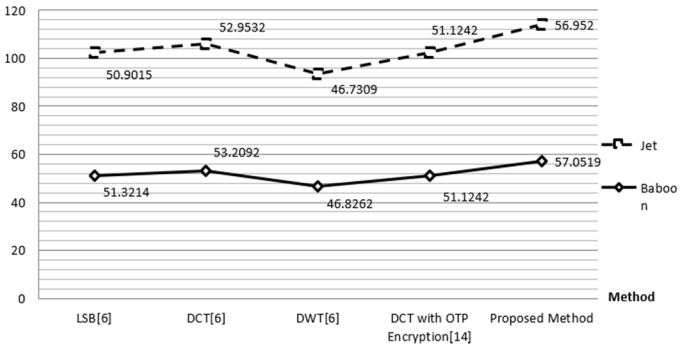


Fig. 5 Analysis a graph of PSNR of the proposed method and the other methods for image baboon and jet

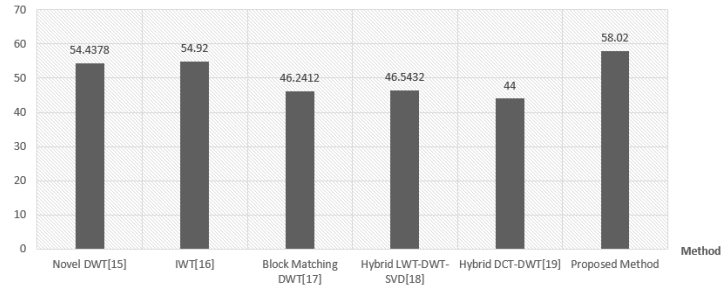


Fig. 6 Analysis a graph of PSNR of the proposed method and the other methods for image lena

In this work, the addition of the SVD method to the DWT can reduce significant image changes, for example, we can see from the PSNR value of the DWT method for the previous image of baboon 46.8262 rising to 57.0519. This shows that decomposing data by using the SVD method can make the inserted data smaller so it does not make large pixel changes and the value of MSE can be minimized so that it becomes 0.1282, it means the error is very low. Referring to each PSNR and MSE values in table 1 and table 2, we can see that the PSNR and MSE values of the DWT and SVD method have a better value. With the test results from the performance metrics where the PSNR value is 57.0519 and the MSE value is 0.1282, we can know the level of robustness and invisibility is better.

According to the results in table 1 and table 2, it is found that the proposed method has high PSNR values than another method, which means that the stego image quietly take after the original image in other words its robustness is better than any other methods and based on small MSE values can be said that the level of invisibility is high.

VI. CONCLUSIONS

In this study, we have successfully implemented algorithm DWT and SVD in an image so that the image of steganography. From the comparison above that PSNR and MSE values are compared to show DWT and SVD algorithm is better than LSB algorithm, DCT, and DWT. PSNR indicate the quality of an image already inserted data. Results PSNR for DWT and SVD method is higher than the third algorithm, so as the application of steganography is more suitable than the LSB algorithm, DCT, and DWT.

MSE measurement results on the DWT and SVD method is smaller than other methods. This indicates that even when the data has been entered, the image only changes small pixels. A good image steganography is more like the image before the data is inserted, in other words, the level of robustness and invisibility is high. Future work for this research is to add the encryption method on the data to be entered so that if there is an attack then the encryption method can secure the data becomes more secure.

REFERENCES

[1] Q. Shen, G. Liu, W. Liu, and Y. Dai, "Adaptive Image Steganography Based on Pixel Selection," pp. 623–627, 2015.

[2] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB steganography and its evaluation for various bits," *2006 1st Int. Conf. Digit. Inf. Manag. ICDIM*, vol. 872, pp. 173–178, 2006.

[3] G. S. Rajput, "Analytic Survey on Various Techniques of Image Steganography," vol. 132, no. 1, pp. 42–45.

[4] S. V.Joshi, A. A. Bokil, N. A. Jain, and D. Koshti, "Image Steganography Combination of Spatial and Frequency Domain," *Int. J. Comput. Appl.*, vol. 53, no. 5, pp. 25–29, 2012.

[5] J. Desai, H. S, and S. SR, "Comparison Between DCT and DWT Steganography Algorithms .," vol. 24, no. 24, pp. 51–55, 2014.

[6] S. Chandran and B. Khoushik, "Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography," *IEEE Int. Conf. Electr. Electron. Signals, Commun. Optim.*, vol. 15, no. 978-1-4799-7678–2, pp. 2–6, 2015.

[7] Z. Moghaddasi, H. A. Jalab, and R. M. Noor, "A comparison study on SVD-based features in different transforms for image splicing detection," *2015 IEEE Int. Conf. Consum. Electron. - Taiwan, ICCE-TW 2015*, no. 3, pp. 13–14, 2015.

[8] S. Vohra and B. B. Kumar, "Image Steganography Using Hybrid Method LWT-DWT-SVD," pp. 16274–16285, 2017.

[9] A. Goswami and S. Khandelwal, "Hybrid DCT-DWT Digital Image Steganography," *Int. J. Adv. Res. Comput. Commun. Eng. Vol.*, vol. 5, no. 6, pp. 228–233, 2016.

[10] A. Kaur, "Image Steganography using Discrete Wavelet Transformation and Artificial Bee Colony Optimization," vol. 1, no. September, pp. 4–5, 2015.

[11] M. Gunjal and J. Jha, "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm," *Int. J. Comput. Trends Technol.*, vol. 11, no. 4, pp. 144–150, 2014.

[12] Erwin, A. Nevriyanto, and D. Purnamasari, "Image enhancement using the image sharpening, contrast enhancement, and Standard Median Filter (Noise Removal) with pixel-based and human visual system-based measurements," in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, 2017, pp. 114–119.

[13] Erwin, Saparudin, and M. Fachrurrozi, "Segmentation and classification models validation area mapping of peat lands as initial value of Fuzzy Kohonen Clustering Network," in *IAES International Conference on Electrical Engineering, Computer Science and Informatics IOP Publishing*, 2017.

[14] Saparudin, Erwin, and M. Fachrurrozi, "Tongue Segmentation Using Active Contour Model," in *IAES International Conference on Electrical Engineering, Computer Science and Informatics IOP Publishing*, 2017, pp. 1–6.

[15] M. Fachrurrozi, Erwin, Saparudin, and Mardiana, "Multi-object face recognition using Content Based Image Retrieval (CBIR)," in *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)*, 2017, pp. 193–197.

[16] Erwin, M. Fachrurrozi, A. Fiqih, B. R. Saputra, R. Algani, and A. Primanita, "Content based image retrieval for multi-objects fruits recognition using k-means and k-nearest neighbor," in *2017 International Conference on Data and Software Engineering (ICoDSE)*, 2017, pp. 1–6.

[17] M. Fachrurrozi *et al.*, "The grouping of facial images using agglomerative hierarchical clustering to improve the CBIR based face recognition system," in *2017 International Conference on Data and Software Engineering (ICoDSE)*, 2017, pp. 1–6.

[18] J. P. Dsouza and D. Naik, "Visible Light Communication using White LEDs for Indoor Wireless Data Transmission," *Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng.*, vol. 3, no. 1, pp. 86–89, 2015.

[19] M. Makhloghi, F. Akhlaghian, and H. Danyali, "Robust Digital Image Watermarking Using Singular Value Decomposition," *Transform*, pp. 219–224, 2011.

[20] P. Chouksey and P. Patel, "Secret Key Steganography technique based on three-layered DWT and SVD algorithm," vol. 35, no. 9, pp. 440–445, 2016.

[21] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017.

[22] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 612–618, 2015.

[23] M. Vijay and V. Vigneshkumar, "Image Steganography Method Using Integer Wavelet Transform," *Int. J. Innov. Res. Sci. Eng. Technol.*, vol. 3, no. 3, pp. 1207–1211, 2014.

[24] J. Kim, H. Park, and J. Il Park, "Image steganography based on block matching in DWT domain," *IEEE Int. Symp. Broadband Multimed. Syst. Broadcast. BMSB*, no. 4, 2017.