Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 8, No. 4, November, Pp. 751-758

Discrete cosine transform and singular value decomposition based on canny edge detection for image watermarking

Erna Zuni Astuti[1], Christy Atika Sari*[1], Eko Hari Rachmawanto[1], Yani Parti Astuti[1], Harwinanda Oktaridha[1], Folasade Olubusola Isinkaye[2]
University of Dian Nuswantoro, Semarang, Indonesia[1]
Ekiti State University, Ado Ekiti, Nigeria[2]

Article Info

Keywords:
Image Watermarking, Discrete Cosine Transform, Singular Value Decomposition, Canny Edge Detection, Grayscale

Article history:
Received: June 26, 2023
Accepted: September 11, 2023
Published: November 30, 2023

Cite:
E. Z. Astuti, C. A. Sari, E. H. Rachmawanto, Y. P. Astuti, H. Oktaridha, and F. O. Isinkaye, "Discrete Cosine Transform and Singular Value Decomposition Based on Canny Edge Detection for Image Watermarking ", KINETIK, vol. 8, no. 4`, Nov. 2023. https://doi.org/10.22219/kinetik.v8i4.1768

*Corresponding author.
Christy Atika Sari
E-mail address:
christy.atika.sari@dsn.dinus.ac.id

Abstract

The development of an increasingly sophisticated internet allows for the distribution of digital images that can be done easily. However, with the development of increasingly sophisticated internet networks, it becomes an opportunity for some irresponsible people to misuse digital images, such as taking copyrights, modification and duplicating digital images. Watermarking is an information embedding technique to show ownership descriptions that can be conveyed into text, video, audio, and digital images. There are 2 groups of watermarking based on their working domain, namely the spatial domain and the transformation domain. In this study, three domain transformation techniques were used, namely Singular Value Descomposition (SVD), Discrete Cosine Transform (DCT) and Canny Edge Detection Techniques. The proposed attacks are rotation, gaussian blurness, salt and pepper, histogram equalization, and cropping. The results of the experiment after inserting the watermark image were measured by the Peak Signal to Noise Ratio (PSNR). The results of the image robustness test were measured by the Correlation Coefficient (Corr) and Normalized Correlation (NC). The analysis and experimental results show that the results of image extraction are good with PSNR values from watermarked images above 50dB and Corr values reaching 0.95. The NC value obtained is also high, reaching 0.98. Some of the extracted images are of fairly good quality and are similar with the original image.

1. Introduction

The development of increasingly sophisticated internet networks allows people to buy goods online with the distribution of digital images that can be done easily. However, this caused some issues such as copyright protection and proof of legal ownership [1]–[4]. Over the years, watermarking technology has gained prominence and emerged as a solution to the problem of ownership and authenticity of digital data for examples: audio, video, and images [5]–[9]. Misuse of images by some irresponsible people includes taking other people's copyrights, modification and duplicating digital images.

Watermarking [10]–[14] is a technique of embedding information, capable of showing ownership depictions or tracking submissions, into text, digital images, video, or audio. Insertion of information must be detected or extracted again. Discrete Cosine Transform (DCT) [15]–[18] is used to convert images in the spatial domain into the frequency domain. DCT divides the image into different frequencies namely low, mid, and high-frequency bands. This method is stronger against attacks [19]. The image is divided into several different blocks and then DCT is applied to each block. The proposed method, namely Singular Value Decomposition (SVD) does not change the image significantly and it has also been found that insertion of images with modified values from Singular Value Decomposition (SVD) has less effect on the quality of the watermark image display [20], [21]. Watermarking can also be considered as a covert communication method. Secret data or images can be watermarked onto the original image using a key and can be sent to the recipient. The recipient can only extract the watermarked image with the help of the real key. The proposed watermarking algorithm is a non-blind watermarking algorithm that is strong enough because it has good quality. From the experimental results it was observed that the proposed watermarking algorithm has resistance to attacks compared to the existing DCT and SVD methods and the visual quality of the extraction results is good. Our proposed method had been DCT and SVD-based Canny Edge Detection where to insert a watermark. The combination of the three watermark methods can increase the resistance of the watermarked image from various attacks without reducing the quality of the original image. Here, we tested the proposed method using several calculations such as Peak Signal to Noise Ratio (PSNR), Correlation, Normalized Correlation, and several images processing attacks.

2. Research Method

2.1 Watermarking

Digital watermarking [22] is the process of hiding information in the form of digital content such as images, text, audio, and video using embedding and extracting process as shown in Figure 1. Basically, watermarking is a method of embedding some confidential information and additional information on the cover image which can then be extracted or detected for various purposes such as authentication, owner identification, copyright protection, and so on. Sometimes the scaling factor is also used for embedding a watermark on the cover image [16].

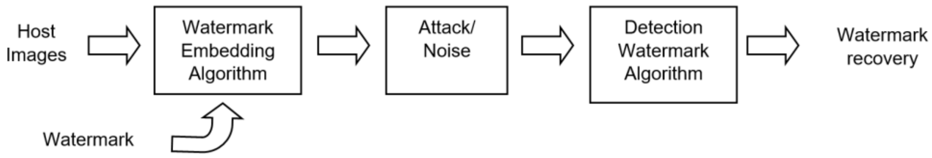


Figure 1. Digital Watermarking Scheme

Digital watermarking [23]–[25] is used for digital content security and to protect data from illegal users and provide ownership rights over digital data. A good watermarking technique has 4 important factors to determine quality:

- Robustness: a measure of the strength of the watermark on image modification and manipulation efforts such as compression, filtering, rotation, scaling, cropping and others.
- Imperceptibility: the quality of the host image cannot be damaged by the presence of a watermark.
- Capacity: this includes the techniques that make it possible to embed most of the information.
- Blind-watermarking: watermark extraction from the watermarked image without the original image is preferred, because it is impossible to utilize the original image.

2.2 Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) [15] is a transformation function that changes the image from the spatial domain to the frequency domain which makes signal analysis simple as shown in Equation 1, Equation 2, and Equation 3. DCT watermarking is applied using the direct application of the transformation to the entire image [26]. DCT is used in many standard image, audio, and compression methods [27]. It has shown advantages in reducing the redundancy of various signals. The way DCT works is as follows:

1. The original image is broken into 8x8 blocks.
2. Each block is transformed using 63 DCT coefficients.
3. Each coefficient can be quantized which may lose data.
4. The small coefficient is close to 0.
5. Using huffman can shorten the process of a compressed coefficient array.
6. The decompression process has been carried out using inverse DCT (IDCT).

$$F(u,v) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(u)C(v)f(i,j)\cos\left[\frac{\pi(2i+1)u}{2N}\right] * \cos\left[\frac{\pi(2i+1)u}{2N}\right] \tag{1}$$

$$f(i,j) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(u)C(v)F(u,v)\cos\left[\frac{\pi(2i+1)u}{2N}\right] * \cos\left[\frac{\pi(2i+1)u}{2N}\right] \tag{2}$$

$$C(u), C(v) = \begin{cases} \sqrt{1/N}, u,v = 0 \\ \sqrt{2/N}, u,v = 1,2,\dots.N-1 \end{cases} \tag{3}$$

2.3 Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is one of the most useful linear algebra tools with several applications for multimedia [12], [28]. The inherent properties of SVD from the point of view of image processing applications that are popularly used are: The singular value is stable, that is, any changes to it do not affect the image quality; The singular value is able to represent the algebraic properties inherent in digital images; SVD maintains one-away and non-symmetric properties which are not found in DCT and DFT; The size of the matrix can be square or rectangular; and The singular value is known to be immutable against some common attacks such as JPEG compression, adding noise (Low Pass Filter), rotation, scalling and cropping. The initial idea of the research was to find the original SVD image and then modify the singular value to insert a watermark. With matrix A(m,n); 1 <m <M, 1 < n < N, can be decomposed into the product of the three matrices given by the following Equation 4, where U and V are orthogonal matrices UTU = I, VTV = I and S = diag(λ1,λ2,........λr). The entry diagonal of S is called the singular value of A, the U column is called the left singular vector of A, and the V column is called the right singular vector of A. This decomposition is known as the SVD of A, and can be written as shown in the following Equation 5, Where r is the rank matrix A. Note that each singular value determines the luminance of the image layer while the corresponding singular vector pair determines the geometry of the image layer. An important feature of SVD watermarking is that the modified singular value changes very little for most types of attacks such as transpose, flip, scaling, rotation, and translation.

$$A = USVT \tag{4}$$

$$A \ = \ \lambda 1U1V1T \ + \ \lambda 2U2V2T + \ldots\ldots\ldots + \lambda rUrVrT \tag{5}$$

2.4 Canny Edge Detection

The canny edge detection algorithm was developed to improve existing edge detection methods. The first and most obvious is the low error rate: it is important that edges occurring in the image are not missed and that there is no response to non-edges [29], [30]. The second criterion is that the edge points are well allocated. In other words, the distance between the edge pixels as found by the detector and the actual edges is the least. The third criterion is to have only one reaction to one side. This was implemented because the second and first criteria were not large enough to eliminate the possibility of multiple reactions from an edge. The gradient array is now reduced with Hysteresis to trace along the remaining unstressed pixels. The edge of the canny follows two threshold values. If the magnitude is below the first threshold, it is set to zero (made borderless). If the magnitude is above a high threshold, an edge will be created. And if the magnitude is between two thresholds, then the threshold will be zero unless there is a path from this pixel to the gradient pixel above the low threshold value.

2.5 Data Collection

This research has been done using 12 images in 512x512 pixels and grayscale as host images as shown in Figure 2, and another image as shown in Figure 3 is message image in 128x128 pixels grayscale.

Figure 2. Sample of Host Images

Figure 3. Message Image

2.6 Evaluation Method

MSE is the average squared error value between the original image and the manipulated image. PSNR is a calculation of image quality measurement by comparing the quality between the reconstructed image and the original image. To calculate the PSNR, we must first calculate the MSE (Mean Square Error) of the reconstructed image. The relationship between the MSE and PSNR values is that the smaller the PSNR value, the greater the MSE value as shown in Equation 6 and Equation 7. Calculation of the degree of similarity between the original watermark image and the extracted watermark image quantitatively as shown in Equation 8. Normalized Correlation (NC) is used to compare the original watermark with the extracted watermark by measuring the cosine angle of the two vectors. The NC shows the level of resilience in the image. If the NC value is high, then the level of image similarity is also high. The NC value has a value range from 0 to 1. The higher the NC value, the more similar the image is, as shown in Equation 9.

$$MSE = \frac{\sum[f(i,j) - F(i,j)]^2}{N^2} \tag{6}$$

$$PSNR = 20 \ * \log 10 \ (\frac{MAXi}{\sqrt{MSE}}) \tag{7}$$

$$CC = \frac{\sum(x-\overline{x})(y-\overline{y})}{\sqrt{\sum(x-\overline{x})^2\sqrt{\sum(y-\overline{y})^2}}} \quad (8)$$

$$NC = \frac{\sum_i \sum_j w_{ij} w_{ij}}{\sum_i \sum_j [w_{ij}]^2} \quad (9)$$

2.7 Proposed Method

The embedding stage is the stage of inserting a message into a container media that aims to hide a secret message so that it is not visible to the human senses or noticed by other people. At this stage, a host grayscale image measuring 512x512 pixels was used and the image to be inserted is a matrix block which final results is a binary image as shown in Figure 4. Figure 5 is an illustration of the message disclosure technique from a watermarked image which will display the secret message contained in the image file.

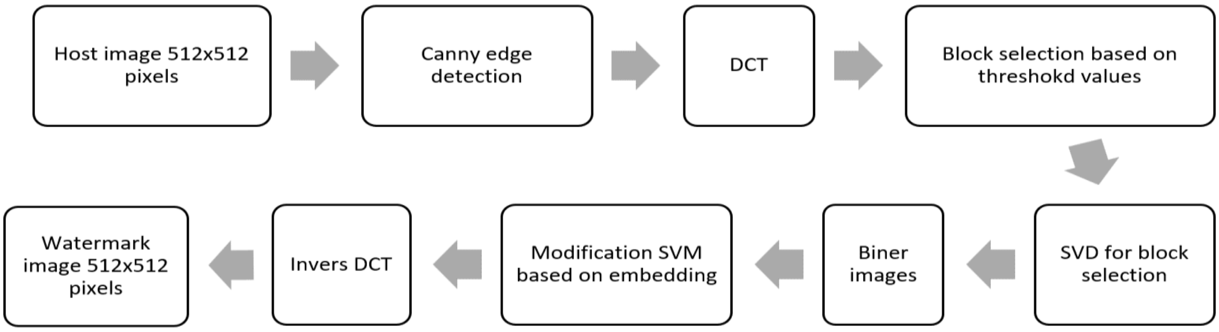


Figure 4. Embedding using DCT-VSD

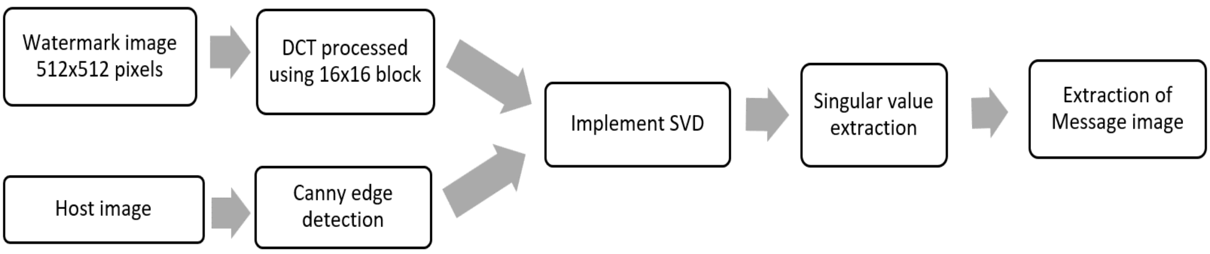


Figure 5. Extracting using DCT-VSD

3. Results and Discussion

Measurement of image quality resulting from watermarked images is obtained from the PSNR (Peak Signal Noise Ratio) value. PSNR measures image quality by comparing the quality of the watermarked image to the original image. PSNR measurement can be seen in the formula (section 2.5). The results of the research are in the form of matrix blocks, namely binary images and tested using the value of scaling factor (α) = 0.2, 0.4, 0.6, and 0.8. Based on Table 1, a low alpha value results in a higher PSNR value and a high alpha value result in a lower PSNR value. From Table 1, it can be seen that the higher the alpha value, the lower the quality of the watermarked image shown in diagram 1. The 12 images used have a satisfactory PSNR value because they have a PSNR value of more than 50dB. The crowd image has the highest PSNR value, namely at an alpha 0.2 value of 71.9127dB. To test the resilience of watermarked images using 5 attacks, namely rotation, salt and pepper, gaussian blurness, histogram equalization, and cropping.

Table 2 measures the Correlation Coefficient and Normalized Correlation on watermarked images that have previously been attacked. Corr and NC have values ranging from 0 to 1. The higher the value, the higher the similarity of the image. Table 2 shows that the Zelda image has a high Corr value, which is close to 1 for each scaling factor (α) value of the measurement, indicating that the relationship between the two variables is quite strong. The Corr value in the Zelda image with α=0.4 is close to 1 with a value of 0.9515. Whereas, the NC value close to 1 indicates that the resulting image extraction is similar to the original image. This shows that the image extraction has good quality and resistance to attack, and had secured the image properly. The dollar image has a high NC value in 0.9887 at α=0.2 close to 1.

Table 1. PSNR of Watermark without Image Processing Attacks

Images	Scalling factors (α)			
	α=0.2	α=0.4	α=0.6	α=0.8
Barbara	71.4484	64.0841	59.4134	56.2661
Bridge	71.2755	62.6668	57.9407	54.8106
Clown	70.6186	63.0467	58.4691	55.2218
Couple	70.7513	62.0508	58.0405	54.8343
Crowd	71.9127	64.3730	59.5678	56.5952
Dollar	70.1506	61.9749	55.7257	52.0271
Girlface	68.4246	61.3222	56.5564	53.5108
House	71.2202	64.5043	60.5966	56.8195
Man	70.6376	63.9856	58.7588	56.2768
Tank2	68.1265	59.0847	54.8865	51.2019
Trucks	70.1300	62.1945	57.1576	54.0079
Zelda	65.7261	58.7531	53.6659	50.3970

Table 2. Sample Correlation Value and Normalized Correlation after Salt and Peppers Attack

Images	Scalling factors (α) Correlation Value				Scalling factors (α) Correlation Value			
	α=0.2	α=0.4	α=0.6	α=0.8	α=0.2	α=0.4	α=0.6	α=0.8
Barbara	0.8094	0.8047	0.8140	0.7668	0.9601	0.8578	0.8639	0.8338
Bridge	0.8422	0.8670	0.8107	0.7793	0.9505	0.8999	0.8618	0.8416
Clown	0.8385	0.8922	0.8079	0.8112	0.9848	0.9178	0.8600	0.8621
Couple	0.8865	0.9154	0.7830	0.7774	0.9821	0.9346	0.8439	0.8404
Crowd	0.8117	0.8032	0.7701	0.7434	0.9606	0.8572	0.8358	0.8196
Dollar	0.8293	0.8149	0.7572	0.6381	0.9887	0.8645	0.8279	0.7609
Girlface	0.8264	0.8651	0.8383	0.7567	0.9521	0.8985	0.8801	0.8276
House	0.7720	0.8042	0.6633	0.5978	0.9831	0.8575	0.7742	0.7408
Man	0.8108	0.8458	0.7645	0.7064	0.9557	0.8852	0.8324	0.7979
Tank2	0.9279	0.8751	0.8741	0.8670	0.9698	0.9055	0.9049	0.8999
Trucks	0.9047	0.8870	0.8270	0.8340	0.9627	0.9140	0.8725	0.8772
Zelda	0.9466	0.9515	0.9052	0.8571	0.9855	0.9618	0.9272	0.8929

Table 3. PSNR of Watermark using Salt and Peppers Attack

Images	Scalling factors (α)			
	α=0.2	α=0.4	α=0.6	α=0.8
Barbara	43.2564	43.2249	43.1674	43.1166
Bridge	44.8960	44.8591	44.7968	44.7293
Clown	48.1519	48.0981	47.9831	47.8801
Couple	44.6650	44.6386	44.5947	44.5154
Crowd	47.5997	47.5449	47.4387	47.3601
Dollar	40.6851	40.6575	40.6244	40.5871
Girlface	47.6065	47.5425	47.4574	47.3552
House	43.4848	43.4604	43.4077	43.3586
Man	46.8263	46.7629	46.6947	46.5986
Tank2	46.3356	46.2878	46.2216	46.1371
Trucks	46.2267	46.1649	46.1115	46.0354
Zelda	47.4500	47.4022	47.2989	47.2105

PSNR is used to measure image quality by comparing the quality between the watermarked image and the original image. The following tables show the quality of the watermarked image after being attacked as shown in Table 3 to Table 6 using rotation, salt and peppers, gaussian blurness, and histogram equalization. After the rotation attack in the table above, it shows that the PSNR value is not good because the results of the attack on several images show PSNR results is less than 30dB. The lowest PSNR value was the dollar image with a value of α=0.8 of 28.0059 dB and the highest PSNR value was the clown image of 33.7333 dB at a value of α=0.2. The salt and pepper attack measurements as shown in Table 3 indicates satisfactory results with a PSNR value above 40dB in each test with a different alpha value. In the clown image, each alpha value has a PSNR value above 45dB, the highest PSNR value in this image is on testing the value of α = 0.2 with a value of 48.1519 dB. The gaussian blurness attack measurement above has a proper PSNR value because it has a PSNR value exceeding 40dB, with a PSNR value of 49.7898 dB in a clown image with a value of α=0.2 as shown in Table 4. Giving a histogram equalization attack produces a decent PSNR value because in this attack the PSNR value produced by all images is 43 dB with the largest PSNR value in the barbara image being 43.3298 dB with a value of α = 0.2. After giving the proposed watermarking attack in Table 5, the PSNR value is quite satisfactory for the Gaussian blurness attack. The gaussian blurness attack has a high attack value of 49 dB. In an attack that has a low PSNR value, namely rotation, with a PSNR value unable to reach 40dB.

Table 4. PSNR of Watermark using Gaussian Blurness Attack

Images	Scalling factors (α)			
	α=0.2	α=0.4	α=0.6	α=0.8
Barbara	43.9175	43.8804	43.8294	43.7653
Bridge	45.7437	45.7018	45.6428	45.5681
Clown	49.7898	49.7147	49.6053	49.4642
Couple	45.4046	45.3644	45.3052	45.2273
Crowd	49.0639	49.0019	48.9199	48.8247
Dollar	41.1379	41.1171	41.0862	41.0480
Girlface	48.9123	48.8421	48.7401	48.6090
House	44.3037	44.2751	44.2326	44.1782
Man	48.0856	48.0219	47.9313	47.8125
Tank2	47.2747	47.2235	47.1462	47.0475
Trucks	47.2085	47.1566	47.0812	46.9831
Zelda	48.6054	48.5409	48.4461	48.3235

Table 5. PSNR of Watermark using Histogram Equalization Attack

Images	Scalling factors (α)			
	α=0.2	α=0.4	α=0.6	α=0.8
Barbara	43.3298	43.3268	43.3308	43.3275
Bridge	43.3209	43.3159	43.3245	43.3234
Clown	43.3166	43.3127	43.3057	43.3025
Couple	43.3190	43.3175	43.3293	43.3268
Crowd	43.3136	43.3116	43.3065	43.3153
Dollar	43.3224	43.3302	43.3542	43.3475
Girlface	43.3179	43.3178	43.2977	43.2982
House	43.3181	43.3334	43.3208	43.3202
Man	43.3106	43.3114	43.3102	43.3061
Tank2	43.3252	43.3357	43.3115	43.3213
Trucks	43.3070	43.3152	43.3125	43.3121
Zelda	43.3124	43.3093	43.3196	43.3084

Table 6. PSNR of Watermark using Several Attacks

Attaks	Scaling factor (α)			
	α = 0.2	α = 0.4	α = 0.6	α = 0.8
Rotation	31.5941	31.5568	31.5036	31.4371
Salt and Pepper	45.5986	45.5536	45.4830	45.4065
Gaussian Blurness	46.6206	46.5700	46.4971	46.4043
Histogram Equalization	43.3007	43.3198	43.3186	43.2949

Masurement of the average PSNR value in attacks at each alpha value is presented in Table 6. The table shows that the highest PSNR value is owned by a gaussian blurness attack with a PSNR value of α = 0.2 of 46.6202 dB. The attack that has the lowest PSNR value is the rotational attack α=0.8 which is 31.4371dB. To compare a visual proof based on the extracting result, message image has been illustrated in Table 7 and Table 8.

Table 7. Sample of Visual Extracting Message Image without attacks

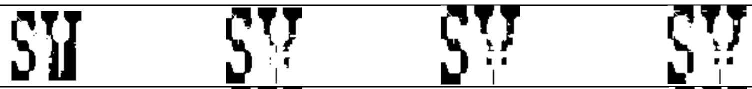
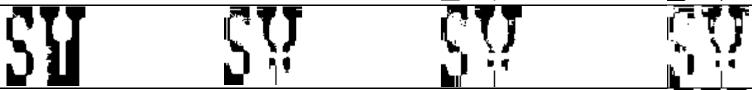
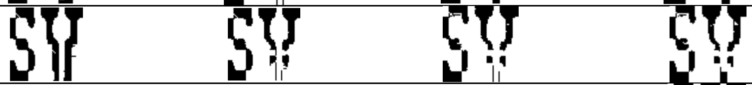
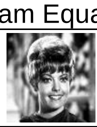
Images	Scalling Factor (α)			
	α=0.2	α=0.4	α=0.6	α=0.8
Barbara				
Bridge				
Clown				
Couple				
Crowd				
Dollar				
Girlface				
House				
Man				
Tank2				
Trucks				
Zelda				

Table 8. Visualization of Watermark Image using Several Images

Rotation	Salt and Pepper	Gaussian Blurness	Histogram Equalization	Cropping
				

4. Conclusion

Research using a combination of Canny Edge Detection techniques, Discrete Cosine Transform and Singular Value Decomposition has been proven to produce good resistance to watermarked images when viewed from a high PSNR above 50dB. The combination of these methods can also show a good level of similarity even though an attack has been given with values from NC and Correlation close to 1. In the attacks, the low MSE value and high PSNR value can be seen, so it can improve the image quality and there is not much change in the image. Inserting a watermark with a combination of Canny Edge Detection, Discrete Cosine Transform and Singular Value Decomposition techniques produces a watermarked image with good quality, so it does not raise suspicion when viewed by the human eye so that it can secure the message properly. From the results of binary image extraction, there are 12 images that have good quality. PSNR in several images after attacks has low value for example after rotation attack, the image can still be read by the human eye. Further research can be developed using the host or message image using its own image, applying this watermarking technique on other media, namely video, audio, and text. This research an be applied to RGB images with image formats such as .tiff, .jpg, .png and so on. It is expected that it can add attacks to provide more satisfactory image resistance results.

References

[1] H.-J. Ko, C.-T. Huang, G. Horng, and S.-J. WANG, "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation," *Inf Sci (N Y)*, vol. 517, pp. 128–147, May 2020. https://doi.org/10.1016/j.ins.2019.11.005

[2] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "Robust SVD-based schemes for medical image watermarking," *Microprocess Microsyst*, vol. 84, p. 104134, Jul. 2021. https://doi.org/10.1016/j.micpro.2021.104134

[3] X. Wang, K. Hu, J. Hu, L. Du, A. T. S. Ho, and H. Qin, "Robust and blind image watermarking via circular embedding and bidimensional empirical mode decomposition," *Vis Comput*, vol. 36, no. 10–12, pp. 2201–2214, Oct. 2020. https://doi.org/10.1007/s00371-020-01909-2

[4] S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela, and H. Jelodar, "An intelligent and blind dual color image watermarking for authentication and copyright protection," *Applied Intelligence*, vol. 51, no. 3, pp. 1701–1732, Mar. 2021. https://doi.org/10.1007/s10489-020-01903-0

[5] X. Wang, D. Ma, K. Hu, J. Hu, and L. Du, "Mapping based Residual Convolution Neural Network for Non-embedding and Blind Image Watermarking," *Journal of Information Security and Applications*, vol. 59, p. 102820, Jun. 2021. https://doi.org/10.1016/j.jisa.2021.102820

[6] N. Hasan, M. S. Islam, W. Chen, M. A. Kabir, and S. Al-Ahmadi, "Encryption Based Image Watermarking Algorithm in 2DWT-DCT Domains," *Sensors*, vol. 21, no. 16, p. 5540, Aug. 2021. https://doi.org/10.3390/s21165540

[7] L. B. Handoko, Utariyanto, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and R. R. Ali, "An Analysis of Imperceptibility and Robustness Performance in CRT Image Watermarking based on Color Space Theory," *J Phys Conf Ser*, vol. 1501, no. 1, p. 012015, Mar. 2020. https://doi.org/10.1088/1742-6596/1501/1/012015

[8] X. Kang, Y. Chen, F. Zhao, and G. Lin, "Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain," *Soft comput*, vol. 24, no. 14, pp. 10561–10584, Jul. 2020. https://doi.org/10.1007/s00500-019-04563-6

[9] R. Sinhal, S. Sharma, I. A. Ansari, and V. Bajaj, "Multipurpose medical image watermarking for effective security solutions," *Multimed Tools Appl*, vol. 81, no. 10, pp. 14045–14063, Apr. 2022. https://doi.org/10.1007/s11042-022-12082-0

[10] C. A. Sari, Utariyanto, D. R. I. M. Setiadi, E. H. Rachmawanto, and M. K. Sarker, "Robust IHWT- CRT Image Watermarking using YCbCr Color Space," *J Phys Conf Ser*, vol. 1501, no. 1, p. 012014, Mar. 2020. https://doi.org/10.1088/1742-6596/1501/1/012014

[11] D. K. Mahto and A. K. Singh, "A survey of color image watermarking: State-of-the-art and research directions," *Computers & Electrical Engineering*, vol. 93, p. 107255, Jul. 2021. https://doi.org/10.1016/j.compeleceng.2021.107255

[12] P. Kadian, S. M. Arora, and N. Arora, "Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey," *Wirel Pers Commun*, vol. 118, no. 4, pp. 3225–3249, Jun. 2021. https://doi.org/10.1007/s11277-021-08177-w

[13] Y. A. Mekarsari, D. Setiadi, C. A. Sari, E. H. Rachmawanto, and Muljono, "Non-Blind RGB Image Watermarking Technique using 2-Level Discrete Wavelet Transform and Singular Value Decomposition," in *International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 623–627. https://doi.org/10.1109/ICOIACT.2018.8350793

[14] C. A. Sari, E. H. Rachmawanto, and D. Setiadi, "Robust and Imperceptible Image Watermarking by DC Coefficients Using Singular Value Decomposition," in *International Conference on Electrical Engineering, Computer Science and Informatics*, IEEE, 2017. https://doi.org/10.1109/EECSI.2017.8239107

[15] E. H. Rachmawanto, D. R. I. M. Setiadi, C. A. Sari, and N. Rijati, "Imperceptible and secure image watermarking using DCT and random spread technique," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 4, p. 1750, Aug. 2019. http://doi.org/10.12928/telkomnika.v17i4.9227

[16] A. A. Arrasyid, D. Setiadi, M. A. Soeleman, C. A. Sari, and E. H. Rachmawanto, "Image Watermarking using Triple Transform (DCT-DWT-SVD) to Improve Copyright Protection Performance," in *International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2018, pp. 522–526. https://doi.org/10.1109/ISRITI.2018.8864461

[17] E. L. Lydia, J. S. Raj, R. Pandi Selvam, M. Elhoseny, and K. Shankar, "Application of discrete transforms with selective coefficients for blind image watermarking," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, Feb. 2021. https://doi.org/10.1002/ett.3771

[18] A. Susanto, D. Setiadi, E. H. Rachmawanto, I. U. Mulyono, and C. A. Sari, "An Improve Image Watermarking using Random Spread Technique and Discrete Cosine Transform," in *International Conference on Information and Communications Technology (ICOIACT*, 2019, pp. 168–173. https://doi.org/10.1109/ICOIACT46704.2019.8938498

[19] P. Garg and R. R. Kishore, "An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain," *Multimed Tools Appl*, vol. 81, no. 26, pp. 36947–36964, Nov. 2022. https://doi.org/10.1007/s11042-021-11237-9

[20] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Sci Int*, vol. 320, p. 110691, Mar. 2021. https://doi.org/10.1016/j.forsciint.2021.110691

[21] A. A. Mohammed, D. A. Salih, A. M. Saeed, and M. Q. Kheder, "An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique," *Multimed Tools Appl*, vol. 79, no. 43–44, pp. 32095–32118, Nov. 2020. https://doi.org/10.1007/s11042-020-09694-9

[22] Sunesh and R. R. Kishore, "A Novel and Efficient Blind Image Watermarking In Transform Domain," *Procedia Comput Sci*, vol. 167, pp. 1505–1514, 2020. https://doi.org/10.1016/j.procs.2020.03.361

[23] S. P. Vaidya, "Fingerprint-based robust medical image watermarking in hybrid transform," *Vis Comput*, vol. 39, no. 6, pp. 2245–2260, Jun. 2023. https://doi.org/10.1007/s00371-022-02406-4

[24] F. Kahlessenane, A. Khaldi, M. R. Kafi, and S. Euschi, "A color value differentiation scheme for blind digital image watermarking," *Multimed Tools Appl*, vol. 80, no. 13, pp. 19827–19844, May 2021. https://doi.org/10.1007/s11042-021-10713-6

[25] E. Kartikadarma, E. D. Udayanti, C. A. Sari, and M. Doheir, "A Comparison of Non Blind Image Watermarking Using Transformation Domain," *Scientific Journal of Informatics*, vol. 8, no. 1, 2021. https://doi.org/10.15294/sji.v8i1.28334

[26] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A robust blind medical image watermarking approach for telemedicine applications," *Cluster Comput*, vol. 24, no. 3, pp. 2069–2082, Sep. 2021. https://doi.org/10.1007/s10586-020-03215-x

[27] A. M. Cheema, S. M. Adnan, and Z. Mehmood, "A Novel Optimized Semi-Blind Scheme for Color Image Watermarking," *IEEE Access*, vol. 8, pp. 169525–169547, 2020. https://doi.org/10.1109/ACCESS.2020.3024181

[28] Z. Yuan, Q. Su, D. Liu, and X. Zhang, "A blind image watermarking scheme combining spatial domain and frequency domain," *Vis Comput*, vol. 37, no. 7, pp. 1867–1881, Jul. 2021. https://doi.org/10.1007/s00371-020-01945-y

[29] Z. Bin Faheem *et al.*, "Image Watermarking Using Least Significant Bit and Canny Edge Detection," *Sensors*, vol. 23, no. 3, p. 1210, Jan. 2023. https://doi.org/10.3390/s23031210

[30] S. Y. Chilkandi Mtech, M. Moodbidri, and N. U. Banu M Asst professor, "Digital Image Watermarking Based On Canny Edge Detection and Texture Block in DWT," *International Journal of Research and Engineering*, vol. 1, no. 4.