STMIK AKAKOM YOGYAKARTA
Code for Life

ISRITI 2018

IEEE
IEEE Conference Number #45367

ISRITI2018 proceeding

International Seminar on Research of Information Technology and Intelligent Systems 2018

"Opportunities and Trends on The Decentralized System & Future of Internet"

Yogyakarta-Indonesia, 21-22 November 2018

www.isriti.akakom.ac.id

Organized by :

STMIK AKAKOM YOGYAKARTA Code for Life

IRSI Indonesia Researcher & Scientist Institute

IEEE INDONESIA SECTION

Supported by :

EDAS

IEEE Advancing Technology for Humanity

IEEE Xplore Digital Library

IEEE Xplore® Digital Library

Image Watermarking using Triple Transform (DCT-DWT-SVD) to Improve Copyright Protection Performance

Adli Azhar Arrasyid
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
Email: azharasr@gmail.com

De Rosal Ignatius Moses Setiadi
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
Email: moses@dsn.dinus.ac.id

M. Arief Soeleman
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
Email: arief22208@gmail.com

Christy Atika Sari
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
Email: atika.sari@dsn.dinus.ac.id

Eko Hari Rachmawanto
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
Email: eko.hari@dsn.dinus.ac.id

***Abstract*— One popular security technique used to protect copyright ownership in digital images is image watermarking. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are techniques that are widely studied in the development of watermarking methods. The combination of the two transformations successfully proved to be able to survive well from attacks. But the problem that often arises in the methods used in watermarking is contradictory imperceptibility and robustness. Singular Value Decomposition (SVD) can optimize the robustness and imperceptibility aspects. So in this research watermarking technique is proposed with a combination of the DCT-DWT-SVD method with the aim of optimizing robustness and imperceptibility. The stages that differentiate in this study are the DCT process that is carried out before DWT, while the SVD transformation is done last both in the host and watermark images. It was proven from the results of the experiment that the proposed method was able to withstand various attacks as evidenced by robustness measurements using NC and imperceptibility measurements as evidenced by satisfactory PSNR and MSE results.**

Keywords—Copyright Protection, DCT, DWT, SVD Transformation Domain

I. INTRODUCTION

Currently security in processing digital image data is needed. Along with the advancement of technology, crime in the security of digital copyright is also increasingly sophisticated. Therefore many of the creative works of people who are recognized for their ownership and distributed in cyberspace through the internet need to be protected. Watermarking is a solution that can overcome the data security problem. Watermarking is the technology of inserting secret messages on images, sounds, text, videos and other multimedia data with certain algorithms [1]. The inserted watermark is the owner's logo, serial number or certain information that indicates ownership.

There are two watermarking techniques based on their domain, ie spatial and frequency. Many studies use domain transforms into watermarking methods because transform domains have better imperceptibility and robustness than spatial domains [2] [3]. Imperceptibility is the watermark insertion characteristic not detected by the sight of the human eye so as not to cause suspicion [4]. While robustness is the watermark's resistance to image manipulation. Research on transform domains has been done with a variety of different transformation algorithms DWT, DCT, and SVD. Where each method has advantages and disadvantages.

To improve watermarking performance, many studies combine two methods of transformation, the performance in question is an increase in imperceptibility and robustness simultaneously. As in the study [4] proposed a combination of the DWT-DCT method, research [5] proposed a combination of DCT-DWT, and research [6] proposed a combination of DCT-SVD. But in this study the level of imperceptibility and robustness is still not optimal. So this research proposes a combination of three transformation methods, namely DCT, DWT and SVD.

II. LITERATUR RIEVIEW

Imperceptibility and robustness are the most important things from a watermarking algorithm. The meaning of Imperceptibility is done not to detect human senses, while robustness means resistance to attack or image manipulation [7]. In this study, discussed issues related to the conflict imperceptibility and robustness to the insertion strategy in a transform domain watermarking DCT, DWT and SVD.

Transformation is the technique of converting a domain signal to a frequency signal. DCT is a transformation technique in digital image processing which is usually done by dividing a sub block of 8x8 pixels. The results of the transformation process of the 8x8 sub block produce 64 coefficients which include 63 AC coefficients and 1 DC coefficient [8], as can be seen in figure 1.

DC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC
AC	AC	AC	AC	AC	AC	AC	AC

Fig. 1. DCT Transformation Reuslts

DWT transformation is a watermarking technique that has good characteristics in human vision systems. In the watermarking technique, there are important steps, namely the selection of the subband resulting from the DWT transformation [9]. Subband selection will greatly affect the results of the watermarking method. DWT divides the image into four sub-bands namely LL, LH, HL and HH as shown in Figure 2. Each subband, ie LL contains a low frequency coefficient, LH and HL which contains an intermediate frequency coefficient and HH which contains a high frequency coefficient [10].

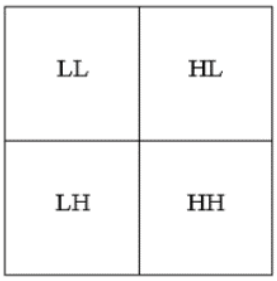


Fig. 2. DWT transformation Results

SVD is a mathematical approach to dividing the image matrix into three elements, namely one sigular element and two unary elements. Watermark is typically embedded in a singular element to provide robustness and imperceptibility [11]. Of the three matrices resulting from the SVD process, one of them has singular values from the original matrix. What is meant by the singular value here is the distance between a matrix and the set of singular matrices. These singular values will later be useful for a matrix which is a transformation from a vector node to another vector space or a different dimension [12]. Where SVD can be calculated by the formula (1).

$$F = U\ x\ S\ x\ V^t \qquad (1)$$

Where, a F matrix with size $m * n$, U is the Singular vector from matrix F and this vector is orthogonal, a S diagonal vector which stores a Singular value from Singular correspondence vector, V^t Singular vector from the orthogonal F matrix.

As the research that has been done [4]implements watermarking on the transform domain with the DWT-DCT method by utilizing the advantages of DWT, the watermark is inserted in the HL subband from the original image transformed with DWT to 3 levels and then applied to 4x4 DCT blocks on the DWT. The results show high imperceptibility and good robustness tested by JPEG compression, salt & peppers, additive random noise..

In the research [5], it was proposed a combination of DCT-DWT technique on 8x8 sub block by collecting DC value of 1.1 coefficient then transformed to DWT. Produces good imperceptibility that shows the watermark that is inserted is not known by the human eye, but only resistant to JPEG Compression attacks not with other attacks.

While in the study [13] the watermarking technique on images using SVD is homomorphic based on DWT domain. The LL sub-band is extracted using a homomorphic transformation for each RGB color. The watermark is inserted with the SVD on the reflectance component of the LL sub-band. Produces watermarked images resistant to attack.

In the study [14] a combination of DCT-DWT-SVD techniques to improve the resistance of watermark images from certain attacks without degrading images and embedding on diagonal sub-bands by selecting the HH sub-band. The result after several attacks on the watermarked image proved to be resistant after being tested with PSNR and SSIM values.

Based on the above research methods on watermarking techniques such as DWT-DCT, DCT-DWT, DCT-SVD and DWT-SVD which still get problems with imperceptibility and robustness. The study proposes to combine these three methods, namely DCT-DWT-SVD degan aim to resolve the issue.

III. PROPOSED METHOD

In this section, discuss the method proposed in this study. There are two main schemes in watermarking, namely embedding watermark and watermark extraction. For host images using grayscale images and watermarks using binary imagery. This will explain the stages of embedding and extraction.

A. Embedding Method

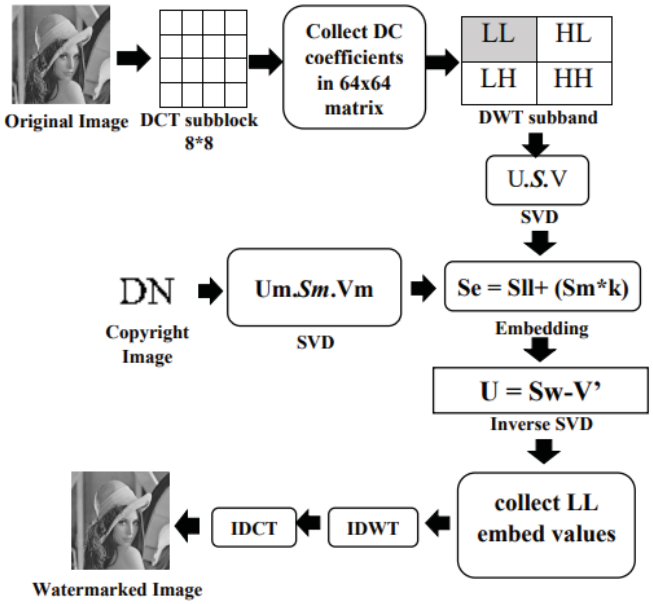


Fig. 3. Embedding Watermark Process

Based on Figure 3 the embedding process requires input in the form of a grayscale type host image, and a binary image for the watermark. Host image will be transformed with DCT followed by the last DWT and SVD. While the watermark image is transformed with the SVD before being pinned, in detail the embedding stage is as follows:

1. DCT transforms subblock 8x8.
2. Creating an empty matrix to collect DC coefficiency on coordinat (1,1).
3. DWT transforms sub-band LL.
4. SVD is transformed by taking matrix S (Singular).
5. SVD transforms an image using watermarking which takes only matrix S (Singular).
6. Singular massage is embedded on LL collection and continued to inver SVD.
7. LL collection has been modified, then it is recovered to each subblock.

8. Inverting DWT and DCT to subblock 8x8 that results watermarked grayscale image.

B. Extraction Method

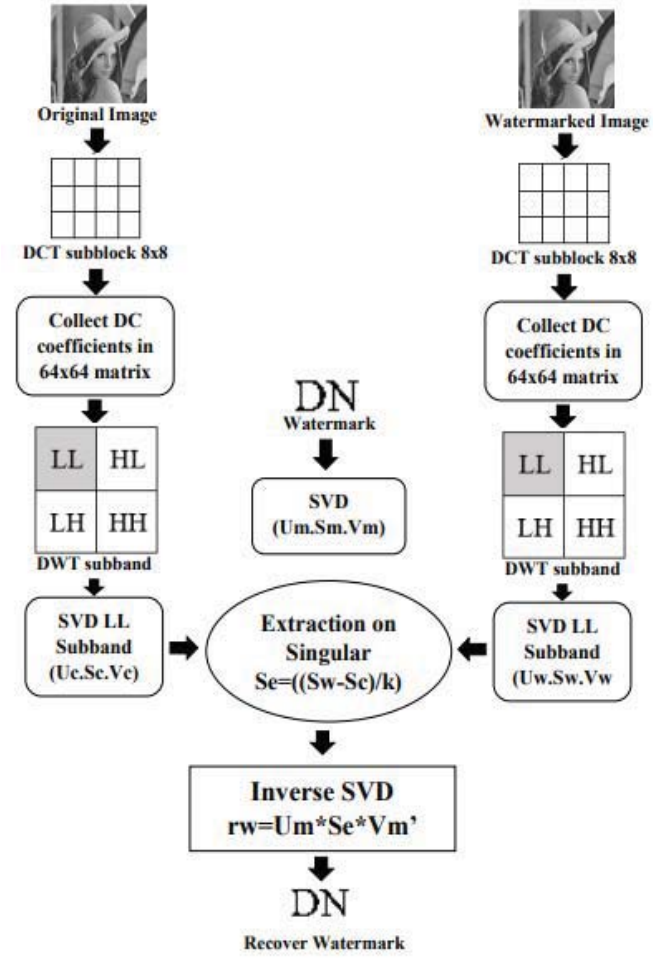


Fig. 4. Watermark Extraction

Based on Figure 4, the extraction process requires input in the form of host image and watermarked an image with grayscale type. Host image and the watermarked image will be transformed with DCT followed by DWT and finally SVD. The extraction results will produce the output of the watermark image obtained from the difference in value between the watermarked image and the original host image. In detail the extraction steps based on Figure 4 are as follows

1. Applying DCT to transform the real image to subblock 8x8 and continued by transforming DWT to be altered into subblock 8x8. Then, taking the first pixel group, LL.
2. At the same time, applying IDCT to transform watermarked image to subblock 8x8 and followed by IDWT transformation to be altered into subblock 8x8. Then, taking the first pixel group, LL.
3. Collecting LL pixel taken by original image transformation and watremarked image into subblock 32x32.
4. Collecting LL pixel taken from original image transformation and watermarked image to be transformed by SVD.
5. Singular Extraction value from other chosen frequency.
6. Transforming SVD on watermark by choosing matrix S which is a diagonal matrix.
7. Inverting SVD from extraction and transformed SVD on watermark to recover the image.

IV. Experiment and Results

In this study the proposed method was tested on a grayscale image measuring 512x512 as a host image, and for a watermark image using a binary image measuring 32x32. For the testing process in this study using MATLAB R2015a. The host image used and the output watermarked image of the proposed method are shown in Figure 5, while the watermark image is shown in Figure 6.

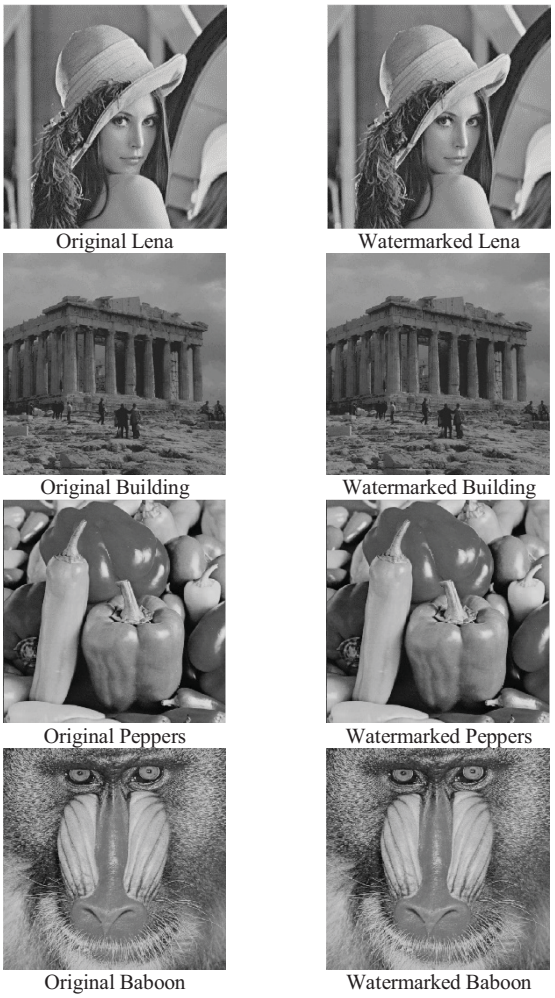


Fig. 5. Original Host Image used and Watermarked Image results

Fig. 6. Zoomed watermark image

Based on Figure 5, visually the watermarked image results are very identical with the original host image. The human eye should not be able to see the difference between the host image and the watermarked image. Then the visual quality of the image needs to be measured by standard measuring

instruments, namely PSNR and MSE. MSE is calculated by calculating the value of the host image with a watermarked image. While the PSNR value is calculated from the logarithm value of MSE [15]. Formula (2) is used to calculate MSE, so to calculate the PSNR the formula is used (3).

$$MSE = \frac{1}{ST}\sum_{s=1}^{S-1}\sum_{t=0}^{T-1}\left(H(s,t) - Hr(s,t)\right)^2 \quad (2)$$

$$PSNR = 10\log 10\frac{255^2}{\sqrt{MSE}} \quad (3)$$

For the extraction process, the original host image is needed to be compared with the watermarked image to reproduce the watermark that is inserted in the cover image. The technique is called non-blind watermarking technique. To measure the quality of the recovered watermark image using NC calculations [11].

$$NC = \frac{\sum_{i=1}^{H}\sum_{j=1}^{L} W(i,j)\ x\ W'(i,j)}{\sum_{i=1}^{H}\sum_{j=1}^{L}[W(i,j)]^2} \quad (4)$$

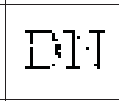
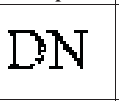
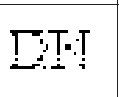
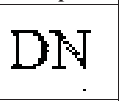
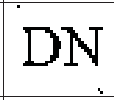
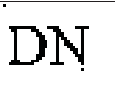
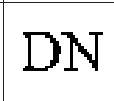
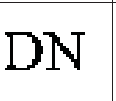
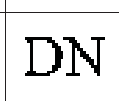
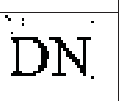
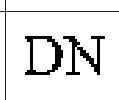
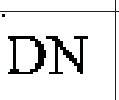
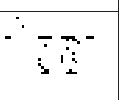
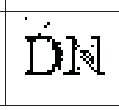
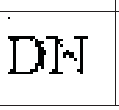
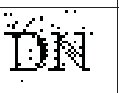
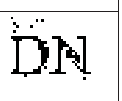
The results of measurement of PSNR and MSE and NC values of watermarked images without attack are presented in Table I.

TABLE I. PSNR, MSE AND NC RESULTS FROM PROPOSED METHOD

Image	PSNR (dB)	MSE	NC
Lena	43.1230	3.1680	1.0000
Building	43.0447	3.2256	1.0000
Peppers	43.3483	3.0078	1.0000
Baboon	43.2466	3.0791	1.0000

Based on Table I it appears that the imperceptibility value of the proposed method is excellent, this is inferred from the PSNR value which reaches 40dB [6].

TABLE II. RECOVER WATERMARK IMAGE RESULTS (WITH VRIOUS ATTACK)

Attack Type	Lena.bmp	Building. bmp	Peppers.tif	Baboon. bmp
Salt & pepper (0.01)				
Gaussian noise (0.005)				
JPEG Compression Q=50				
Filtering				
Unsharp				
Blurring				

In this study several attacks on watermarked images were carried out, including JPEG compression, salt & pepper, Gaussian noise, filtering, unsharp and blur. The recovered watermark image in the watermarked image that has been attacked is shown in Table II. If visually observed the results of recovering relative watermarked images throughout the whole can still be recovered properly, with the exception of the baboon image that is attacked with an unsharp filter resulting from image recovery seems difficult to read.

V. COMPARISON WITH THE PREVIOUS METHOD

In this section the proposed method will be compared with the previous method. Comparison seen from the PSNR and MSE values to determine the image quality that has been inserted by the watermark and find out the correlation of recover watermark image and original watermark image compared to NC value.

TABLE III. COMPARISON OF PSNR AND NC VALUES WITH PREVIOUS RESEARCH ON LENA IMAGES (WITHOUT ATTACK)

Method	PSNR	NC
Method [4]	38.4879 dB	0.8989
Method [5]	42.6950 dB	1.0000
Proposed Method	43.1230 dB	1.0000

Based on the comparative value of PSNR and NC in the image Lena image is shown in Table III appears that The proposed method is superior in every way

TABLE IV. COMPARISON OF NC RESULTS FROM RECOVER WATERMARK ON LENA IMAGE (WITH VRIOUS ATTACK)

Attack Type	Method [5]	Proposed Method
Salt&pepper 0.001	0.7844	0.9531
Gaussian noise 0.005	0.8825	1.0000
JPEG Compression quality 50%	1.0000	1.0000
Filtering	0.9812	1.0000
Unsharping	0.7694	0.9989
blurring	0.8777	0.9753

In Table IV, it appears that the results of the comparison of the proposed method are better compared to the methods that existed before. The NC value in the proposed method can increase significantly by adding SVD transformations.

VI. CONCLUSION

In the previous study, the combination of DCT-DWT transformation was chosen by selecting the DC coefficient on DCT and LL subband on DWT as a place to fill. The results of this study proved to have good and robust imperceptibility against attacks, especially JPEG Compression. This study modifies the method proposed by the study [5] by adding SVD transformation. Based on the results of the experiment it was proved that the combination of three transformations (DCT-DWT-SVD) was able to increase imperceptibility and robustness values for various attacks such as salt & pepper, Gaussian noise, JPEG Compression, filtering, usharp and blurring.

REFERENCES

[1] D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto and C. A. Sari, "Fast and efficient image watermarking algorithm using discrete tchebichef transform," in *International Conference on Cyber and IT Service Management (CITSM)*, Denpasar, 2017.

[2] X. Li, X. Wang, A. Chen and L. Xiao, "A Simplified and Robust DCT-based Watermarking Algorithm," in *International Conference on Multimedia and Image Processing*, Shenzhen, 2017.

[3] U. Sudibyo, F. Eranisa, E. H. Rachmawanto, D. R. I. M. Setiadi and C. A. Sari, "A secure image watermarking using Chinese remainder theorem based on haar wavelet transform," in *International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, Semarang, 2017.

[4] Z.-Y. Meng, P.-P. Yu and G.-Q. Yu, "Copyright protection for digital image based on joint DWT-DCT transformation," in *International Conference on Wavelet Analysis and Pattern Recognition*, Xian, 2012.

[5] A. Winarno, D. R. I. M. Setiadi, A. A. Arrasyid, C. A. Sari and E. H. Rachmawanto, "Image Watermarking using Low Wavelet Subband based on 8×8 Sub-block DCT," in *International Seminar on Application for Technology of Information and Communication.*, Semarang, Indonesia, 2017.

[6] C. A. Sari, E. H. Rachmawanto and D. R. I. M. Setiadi, "Robust and Imperceptible Image Watermarking by DC Coefficients Using Singular Value Decomposition," in *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Yogyakarta, 2017.

[7] H. Tao, L. Chongmin, J. M. Zain and A. N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review," *Journal of Applied Research and Technology,* vol. Vol.1, pp. 122 - 138, 2014.

[8] M. N. M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari and S. Astuti, "An improved secure image hiding technique using PN-sequence based on DCT-OTP," in *International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, 2017.

[9] Y. AL-Nabhani, H. A. Jalab, A. Wahid and R. Md Noor, "Robust watermarking algorithm for digital images using discrete wavelet and probabilistic neural network," *Journal of King Saud University – Computer and Information Sciences,* pp. 393 - 401, 2015.

[10] N. Li, X. Zheng, Y. Zhao, H. Wu and S. Li, "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform," *International Symposium on Electronic Commerce and Security,* no. 978-0-7695-3258-5/08, pp. 942 - 945, 2008.

[11] N. Mohananthini and G. Yamuna, "Comparison of multiple watermarking techniques using genetic algorithms," *Journal of Electrical Systems and Information Technology,* vol. 3, no. 1, pp. 68 - 80, 2016.

[12] H. Zhang, C. Wang and X. Zhou, "Fragile Watermarking for Image Authentication Using the Characteristic of SVD," *Algorithms,* vol. 10, no. 1, pp. 1-12, 2017.

[13] K. A. Al-Afandy, E.-S. M. EL-Rabaie, F. E. Abd El-Samie, O. S. Faragallah and A. ELmhalawy, "Efficient Color Image Watermarking Using Homomorphic based SVD in DWT Domain," in *IEEE*, 2016.

[14] G. Kaur and G. Sidhu, "Image Watermarking Scheme Using Combined DCT-DWT-SVD Transforms," *Imperial Journal of Interdisciplinary Research,* vol. 2, no. 9, pp. 852-857, 2016.

[15] D. R. I. M. Setiadi and J. Jumanto, "An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection," *Cybernetics and Information Technologies,* vol. 18, no. 2, pp. 74-88, 2018.