

## Digital watermarking image using three-level discrete wavelet transform under attacking noise

Lita Lidyawati<sup>1</sup>, Arsyad Ramadhan Darlis<sup>1</sup>, Lucia Jambola<sup>1</sup>, Lisa Kristiana<sup>2</sup>, Rea Ramada Jayandanu<sup>1</sup>

<sup>1</sup>Department of Electrical Engineering, Institut Teknologi Nasional Bandung, Bandung, West Java, Indonesia

<sup>2</sup>Department of Informatics Engineering, Institut Teknologi Nasional Bandung, Bandung, West Java, Indonesia

---

### Article Info

#### Article history:

Received Jul 20, 2021

Revised Oct 10, 2021

Accepted Jan 13, 2022

---

#### Keywords:

Blurring

Gaussian

Grayscale

Salt and pepper

---

### ABSTRACT

The authentication, identification, and copyright protection can be obtained by constructing the digital image watermarking technique. Watermark robustness and imperceptibility account for the capability of the hidden watermark to survive the manipulation. The proposed paper is a robust algorithm for digital image watermarking with 3-level discrete wavelet transform (DWT) with some attacks method. The 3-level DWT method was used constants  $\alpha=0.01$  and  $0.03$  as a function of how depth the watermark inserts to the host image in the insertion and extraction process. The algorithm was evaluated using 8 bits per pixel (bpp) grayscale,  $1024 \times 1024$  pixels for the host image, and  $256 \times 256$  pixels for the watermark image. The method is also implemented some experimental with attacks such as gaussian, salt and pepper, blurring, and compression. The algorithm is relatively acceptable of good quality, achieves low-value mean squared error (MSE), high peak signals to noise ratio (PSNR), and structural similarity index metric (SSIM) value approach to 1. It is found that the highest image quality measurements by using  $\alpha=0.03$  with the attacking method of salt and pepper yield  $MSE=0.01$ ,  $PSNR=45.6$  dB and  $SSIM=0.95$ , respectively.

*This is an open access article under the [CC BY-SA](#) license.*



---

### Corresponding Author:

Lita Lidyawati

Department of Electrical Engineering, Institut Teknologi Nasional Bandung

PKH Mustopha 23, Bandung 40123, West Java, Indonesia

Email: [lita@itenas.ac.id](mailto:lita@itenas.ac.id)

---

## 1. INTRODUCTION

In the digital world, a watermark can be applied as a pattern of bits inserted into a digital platform to identify the creator. The identification or modification can be avoided by embedding and scattering the bits into an image. Robust watermark is designed to resist arbitrary, malicious attacks such as gaussian, salt and pepper, blurring, and compression [1]. A digital watermarking system comprises three basic aspects: the generation of the watermark, the embedded process, and the extraction of the watermark. The imperceptibility and robustness are required in digital watermarking through the analysis of the image host and the embedded point selection [2].

The implementation of the digital watermarking method can be divided into spatial domain and frequency domain. The watermark signals are superposed on the signal space directly and over spatial domain digital watermarking while the spread spectrum in the frequency-domain digital watermarking is applied to hide the watermark information. Some techniques are based on image transformations, such as discrete cosine transform (DCT), discrete wavelet transforms (DWT), discrete fourier transform (DFT), or fast fourier transform (FFT) [3].

The multiresolution decomposition of signals and images is the main idea of the wavelet transform because a higher resolution is required in a small object, and a low resolution is suitable for larger objects [4].

Several studies have been carried out in the field of watermarking. In 2015, Abdullah *et al.* [5] proposed the robust DCT method for securing iris. This paper explained the security of biometric traits and presented the integrity of the iris image protection using a demographic text as a watermark. The watermark text will be embedded in the middle band frequency of the iris image. The three middle band coefficients pairs of DCT will be interchanged. The results showed that this method scheme yielded a robust algorithm against malicious attacks. However, the resolution of the image host and watermark image was not discussed.

In 2015, Jain and Jain [6] focused on combining different transform domain techniques. The method was used a hybrid 3-level DWT-FFT. Laur *et al.* [7] proposed a non-blind color image with robustness and imperceptibility image watermarking algorithm. Furthermore, Mulya and Utama [8] developed fast fourier transform to insert and extract the watermark in the LSB frequency domain on the audio files. The result showed the extracted watermark had a good performance in robustness and imperceptibility. In another case, Rajawat and Tomar [9] proposed the combination between digital watermarking and tampering detection to improve image security. The result yielded good PSNR, which achieved 55%. Viadya and Mouli [10] applied the scaling and embedding factors as namely the adaptive method. This project aims to preserve the ownership rights from piracy of digital data. The statistical evaluation denoted the efficacy of the method.

In 2016, Kaur [11] proposed DCT, DWT, FFT, and SVD techniques with a new integrated watermarking technique. The input cover image will be used the DCT technique while further action will be performed by FFT and will be followed by DWT to arrange the sub-bands. In 2016, Muldakar and Shenvi [12] this project aimed to combine DWT-DCT transformation in low frequency watermarking. The wavelets coefficients modifying is selected the DWT sub-band of a host image after two levels of DWT decomposition and block-based DCT transform. The method can solve the processing and geometric attacks. Furthermore, Ansari *et al.* proposed a remarkable solution to a false-positive problem that arises in SVD based approach. Firstly, the host image is employed by the IWT, and SVD contributes to achieving a high value of robustness. The watermark embedding will be used the singular values. The optimization with artificial bee colony will help to improve the quality of watermarking [13].

In 2016, Haribabu *et al.* [14] presented the wavelet transform in HIS color space. Firstly, the coefficients of one-level wavelet are generated by (LL, LH, HL, HH) to the intensity component of HSI color space cover image. This method gave an improvement in peak signal-noise ratio and mean square error. In 2016, Al Shaikh *et al.* [15] provided the CT scan image watermarking based on wavelet transform. In the extraction process contributes to the improvement of watermark robustness and efficiency against several attacks. In 2017, Roy and Pal [16] delivered his proposed method by applying geometric transformation attack and geometric transformation attack, and JPEG compression attack to the multiple watermark data. In another way, Saqib and Naaz [17] delivered the issue about the types of watermarking.

While durakovic explored the DOE aspects and provided state-of-the-art of its application. It discussed conceptualizing, planning and conducting experiments, and analyzing and interpreting data [18]. Parah *et al.* [19] evaluated the spatial locations which are robust to image processing and geometric attacks. The pseudorandom address vector (PAV) determined the location of the least significant bit (LSB) to embed the watermark data. In 2018, Barnouti *et al.* [20] proposed the DWT and DCT for embedding and extracting copyright protection. In 2019, Aqel *et al.* [21] proposed a different level of sub-bands in DWT to evaluate its performance. The method can be used to overcome such kinds of illegal activities in the digital image by implementing different levels in watermarking that is low-level (LL), low- high (LH), high-low (HL), High-high (HH), and the SVD on image to reach the robustness, and imperceptibility.

Mohammed *et al.* [22] presented a technique that hides the RGB color element and provides robust image watermarking. The discrete wavelet transform and a dual intermediate significant bit (DISB) will integrate into one process. The method has a PSNR of 101.97 and NCC of 0.9780. In 2017, Jing [23] delivered a digital image watermarking algorithm which is based on DCT transform and Arnold scrambling. The algorithm can be well applied with the quality factor 70% and NC equal to 1.

In this study, we have proposed a scheme of digital watermarking image using 3 level DWT with some attacks. These DWT scheme use the parameter  $\alpha$  as a function to show how depth the watermark image inserts to the host image with the result that the robustness and imperceptibility can obtain the best performance.

## 2. METHOD

The proposed algorithm performs wavelet transform on images. The image will be decomposed into sub-images of different bands. Furthermore, the process will continue in the coefficients of sub-images. The diagram of the primary decomposition of the image is shown in Figure 1. An image is decomposed into 4 sub-images with  $\frac{1}{4}$  times to the whole image which comprised: the  $LL_1$  as the low-frequency sub-image; the  $HL_1$  as a horizontal component; the  $LH_1$  as a vertical component, and the  $HH_1$  as a diagonal component. The

DWT filtering will perform the low-frequency part to be decomposed and achieves an n-level decomposition. The schematic diagram of the DWT filtering is shown in Figure 2.

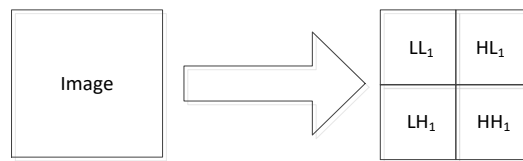


Figure 1. The diagram of a primary decomposition

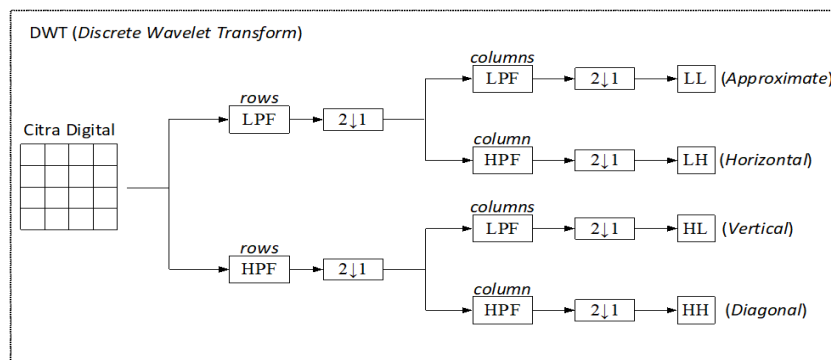


Figure 2. The schematic filtering of the DWT

The high and low-frequency components of the image can be extracted by the wavelet transform method. The watermark embedded in the higher frequency region and it is less influence on the original image which is yielding better transparency of the watermark. In two-dimensional applications of each level decomposition, the vertical direction of DWT will perform first and the second process is the horizontal direction. There are 4 sub-bands:  $LL_1$ ,  $LH_1$ ,  $HL_1$ , and  $HH_1$  [24]. In the embedding process, the intensity of each pixel will be multiplied by  $\alpha$  value. The high-intensity value affects the grayscale image more clearly. However, the higher  $\alpha$  value will be affected to the watermarked image is perceptible to the human sight. Thus,  $\sigma$  value is an important matter to the imperceptibility characteristic. In this experiment, we use  $\alpha=0.01$  and  $\alpha=0.03$ , thus we select the 2048x2048 pixels Lena grayscale image as original or host image and takes REA 256x256 pixels as the watermark image. Figure 3 shows the host image and the watermark image. Figure 3(a) shows the host image and Figure 3(b) points to the watermarking image



Figure 3. The simulation image for (a) host image and (b) the watermarking image

After embedding the watermarking image on the host image, we applied the attackers, such as gaussian, salt & pepper, and blurring. The next step is the process of extracting the watermark image from the watermarked image that has been attacked. After the extraction process, we measure the quality of extracted watermark images with the original watermark image. The quality will be performed by some

parameters, such as MSE, PSNR, and SSIM. Figure 4 shows the whole process of embedding, attacking, and extracting process.

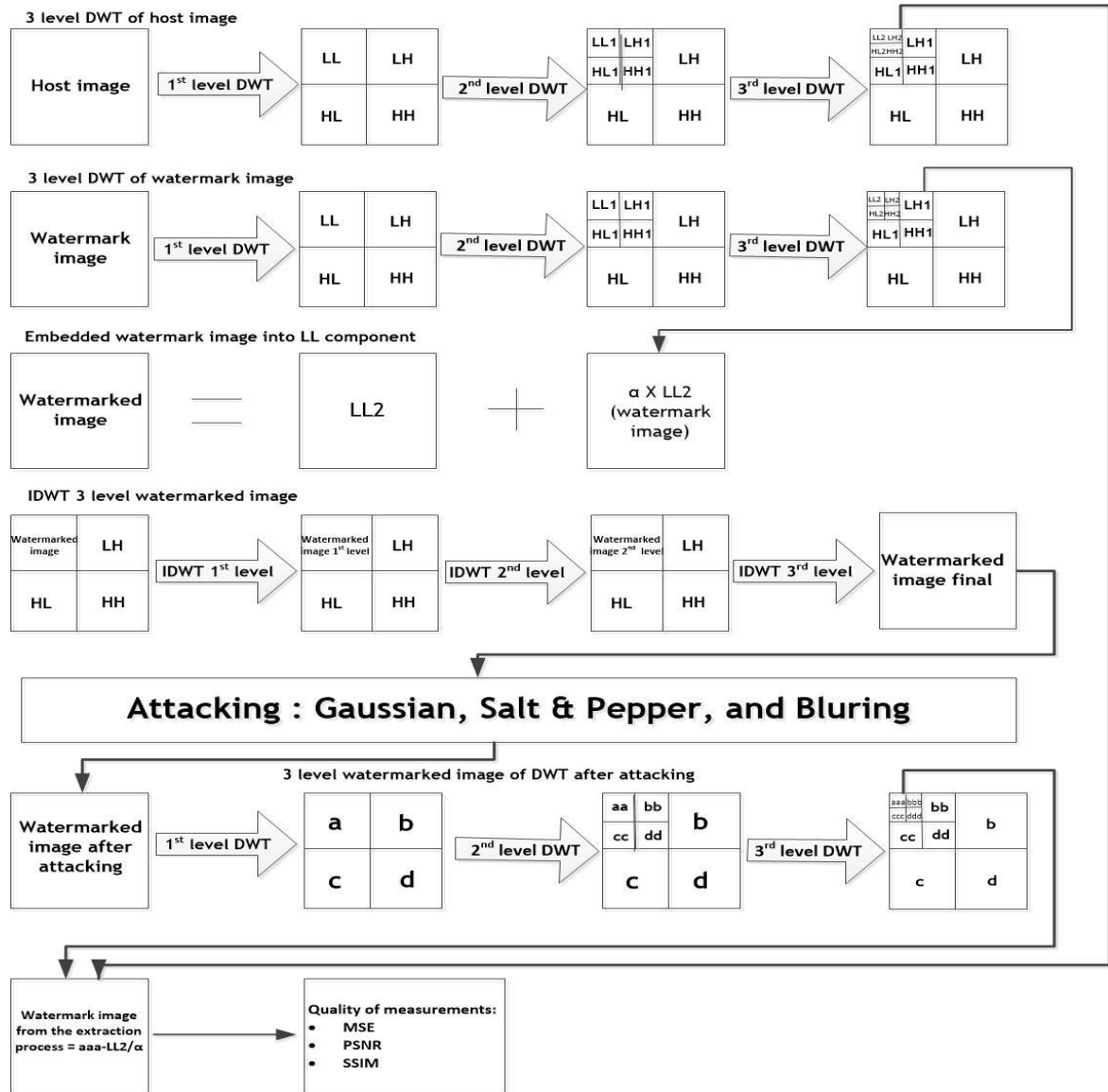


Figure 4. The embedding, attacking, and extracting process

Attacks on the watermarked image can be interpreted as providing interference or disability from an image that causes the image to become unclear, blurring, grainy, and so on. These attacks serve to test the performance of the proposed scheme. Gaussian noise is the disturbance that is distributed to every pixel in the image with a normal distribution (Gaussian). Noise density depends on the probability density function (pdf). One of the causes of this noise is the error of image transmission. The amount of noise is determined by the mean and variance value. The mean value is 0 while the variance value is 0.01. Thus, the image is added Gaussian noise with mean equal to 1 and variance equal to 0.01. Figure 5 shows the effect of the watermarked image which attack by gaussian noise.

Moreover, salt & pepper noise is a common noise in a digital image. This noise has black spots with a value of 0 and a white spot with a value of 255 on the grayscale image. The addition of noise into the image is applied randomly. Grayscale image added noise salt & pepper with a density equal to 0.01. Figure 6 shows the effect of additional salt & pepper noise. The further attack of this experiment is blurring noise. Blurring is a noise that provides a blurred effect on the image. The level of image blur can be adjusted by blurring parameters. Figure 7 provides the image with blurring noise.



Figure 5. The watermarked image under gaussian noise



Figure 6. The watermarked image salt & pepper noise

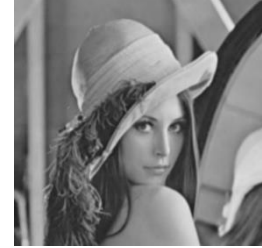


Figure 7. The watermarked image with blurring noise

To test the performance of the proposed scheme, several benchmarking criteria have been used, such as MSE, PSNR, and SSIM. The mean square value of pixel difference value of original image and distorted image can be calculated as a mean squared error (MSE). The size of the mean square value can determine the image distortion degree. A function could be written to (1).

$$MSE = \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [x(i, j) - \hat{x}(i, j)]^2 \tag{1}$$

Furthermore, the peak signal-to-noise ratio (PSNR) measures the quality of the watermarked image in comparison to the original image (host). It is a standard way of measuring image fidelity. Referring to the watermarking requirements, robustness in the watermarking system must have a PSNR value above 20 dB [10]. The PSNR is defined as:

$$PSNR = 10 \log \left[ \frac{I_{MAX}^2}{MSE} \right] \tag{2}$$

Where  $I_{MAX}$  is the maximum gray level of the image. In this case,  $I_{MAX}$  has a maximum value of 255. The main problem with the previous two criteria is that they are not similar to what similarity means to the human visual system (HVS). Structural similarity (SSIM) is a function defined as (3) which overcomes this problem to a great extent.

$$SSIM = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{3}$$

Where  $\alpha$ ,  $\sigma$ ,  $\sigma_{xy}$  are mean, variance, and covariance of the images, and  $c_1$   $c_2$  are the stabilizing constants. The SSIM has a value between 0-1 and similar images have SSIM near to 1.

### 3. RESULTS AND DISCUSSION

This section explains the test result of the watermarking system after attacking by Gaussian, salt & pepper, and blurring noise. Figure 8(a) is the host image (Lena), and Figure 8(b) is the watermark image, while Figure 8(c) is the watermarked image.

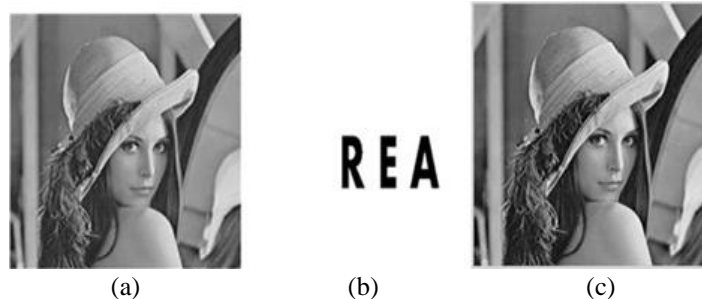


Figure 8. The images using in simulation for (a) the host image, (b) the watermark image, and (c) the watermarked image

The performance evaluation of the method is applied by measuring robustness and imperceptibility, i.e. the MSE, PSNR, and SSIM values. The following are the measurements results of image quality with some attacks using  $\alpha=0.01$ . Table 1 shows the effect of some attacks on the perceptual invisibility and robustness of the watermarked image. Furthermore, Table 2 shows the performance of the image quality using  $\alpha=0.03$ . The parameter  $\alpha$  influences the performance values in PSNR, MSE, and SSIM which is the greater of  $\alpha$  value, the better the performance value will be obtained. Comparing with the other experiment [25], the proposed method has a different result in PSNR value, which is shown in Table 3.

Table 1. Measurement of image quality with attacks with  $\alpha=0.01$

	Watermark image	Gaussian attack	Salt&pepper attack	Blurring attack	Compression attack
$\alpha=0.01$					
	PSNR (dB)	33.3 dB	37 dB	35.5 dB	40 dB
	MSE	0.41	0.13	0.35	0.06
	SSIM	0.66	0.89	0.75	0.92

Table 2. Measurement of image quality with attacks with  $\alpha=0.03$

	Watermark image	Gaussian attack	Salt&pepper attack	Blurring attack	Compression attack
$\alpha=0.03$					
	PSNR (dB)	35.2 dB	45.6 dB	36.1 dB	37.2 dB
	MSE	0.35	0.01	0.21	0.03
	SSIM	0.72	0.95	0.83	0.94

Table 3. The PSNR comparison between the proposed method and the difference method [25]

	Gaussian	Salt & pepper
Proposed	35.2 dB	45 dB
Singh	7.5688 dB	10.8871 dB

#### 4. CONCLUSION

The experimental results proved that the proposed method produced good imperceptibility with SSIM near to 1 and high robustness with PSNR value above 30 dB towards these attacks which are the  $\alpha=0.03$  obtained the best result. The salt & pepper attacker has the highest value in robustness and imperceptibility because this attacker does not spread to the whole watermarked image pixels. The future work will be performed by some optimization algorithms such as a particle swarm and an ant colony algorithms to achieve the best embedded watermarked image point location which yielding more robust and imperceptible performances.

#### ACKNOWLEDGEMENTS

This work was financially supported by the Ministry of Research, Technology & Higher Education of Republic Indonesia under research grant number 164 /E4.1/AK.04.PT/2021, through the PUP T 2021 scheme.




#### REFERENCES

- [1] F. Y. Shih, *Digital Watermarking And Steganography: Fundamentals And Techniques*, 2nd Ed., Taylor & Francis, Crc Press, 2017.
- [2] A. U. Rahman, K. Sultan, D. Musleh, N. Aldhafferi and A. Alqahtani, "Robust And Fragile Medical Image Watermarking: A Joint Venture Of Coding And Chaos Theories," *Journal of Healthcare Engineering*, vol. 2018, no. 8137436, pp. 1-11, 2018, doi: 10.1155/2018/8137436.




- [3] S. Gong, C. Liu, Y. Ji, B. Zhong, Y. Li and H. Dong, "Advanced Image And Video Processing Using Matlab," Springer International Publishing Ag, Part Of Springer Nature, 2019.
- [4] D. Sundararajan, *Discrete Wavelet Transform: A Signal Processing Approach*, John Wiley & Son Singapore Pte.Ltd, 2015.
- [5] M. A. Abdullah, S. S. Olay and W. L. Woo, "Securing Iris Images With A Robust Watermarking Algorithm Based On Discrete Cosine Transform," *Proceedings Of The 10th International Conference On Computer Vision Theory And Applications*, Berlin, Germany, 2015, pp. 108-114, doi: 10.5220/0005305701080114.
- [6] R. Jain and M. Jain, "Digital Image Watermarking Using 3-Level DWT And FFT Via Image Compression," *International Journal Of Computer Applications*, vol. 124, no. 16, pp. 25-38, 2015.
- [7] L. Laur, P. Rasti, M. Agoyi and G. Anbarjaari, "A Robust Color Image Watermarking Scheme Using Entropy And QR Decomposition," *Radio Engineering*, vol. 24, no. 4, pp. 1025-1032, 2015, doi: 10.13164/re.2015.1025.
- [8] M. Mulya and Y. Utama, "Implementation Of Audio Watermarking Using Fast Fourier Transform For Audio Digital Copyright Protection," *Proceeding Of International Journal On Electrical Engineering, Computer Science And Informatics (EECSI)*, 2017.
- [9] M. Rajawat and D. S. Tomar, "A Secure Watermarking and Tampering Detection Technique on RGB Image Using 2 Level DWT," *Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 638-642, doi: 10.1109/CSNT.2015.245.
- [10] P. Viadya and C. Mouli, "Adaptive Digital Watermarking For Copyright Protection of Digital Images In Wavelet Domain," *Procedia Computer Science*, vol. 58, pp. 233-240, 2015, doi: 10.1016/j.procs.2015.08.063.
- [11] K. Kaur, "Fast Fourier Transform Based Hybrid Image Watermarking Using Arnold Scrambling," *Journal For Research In Applied Science & Engineering Technology (IJRASET)*, vol. 4, no. 2, pp. 204-2014, 2014.
- [12] S. B. Muldakar and N. Shenvi, "A Blind Digital Watermarking Algorithm Based On Dwt-Dct Transformation," *International Journal Of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering*, vol. 10, no. 2, pp. 212-216, 2016, doi: 10.17148/IJIREICE/NCAEE.2016.42.
- [13] I. A. Ansari, M. Pant and C. W. Ahn, "Robust And False Positive Free Watermarking In IWT Domain Using SVD And ABC," *Engineering Applications Of Artificial Intelligence*, vol. 49, pp. 114-125, 2016, doi: 10.1016/j.engappai.2015.12.004.
- [14] M. Haribabu, H. Bindu and V. K. Swamy, "A Secure & Invisible Image Watermarking Scheme Based On Wavelet Transform In His Color Space," *Procedia Computer Science*, vol. 93, pp. 462-468, 2016, doi: 10.1016/j.procs.2016.07.234.
- [15] M. Al Shaikh, L. Laouamer, L. Nana and A. Pascu, "A Novel CT Scan Images Watermarking Scheme In DWT Transform Coefficients," *International Journal Of Computer Science And Network Security (IJCSNS)*, vol. 16, no. 1, pp. 62-71.11, 2016.
- [16] S. Roy and A. K. Pal, "A Blind Dct Based Color Watermarking Algorithm For Embedding Multiple Watermarks," *International Journal Of Electronics And Communications*, vol. 72, pp. 149-161, 2017, doi: 10.1016/j.aeeu.2016.12.003.
- [17] M. Saqib and S. Naaz, "Spatial And Frequency Domain Digital Watermarking Techniqyes For Copyright Protection," *International Journal Of Engineering Science And Technology (IJEST)*, vol. 9, no. 6, Pp. 691-699, 2017.
- [18] S. A. Ali, M. J. Jawad and M. A. Naser, "Copyright Protection For Digital Image By Watermarking Technique," *Journal Of Information Processing Systems JIPS*, 2017, vol. 3, no. 3, pp. 599-617, doi: 10.3745/JIPS.03.0074.
- [19] S. A. Parah, J. A. Sheikh, U. I. Assad and G. M. Bhat, "Realization And Robustness Of A Blind Spatial Domain Watermarking Technique," *International Journal Of Electronics*, vol. 104, no. 4, pp. 659-672, 2016, doi: 10.1080/00207217.2016.1242162.
- [20] N. H. Barnouti, Z. S. Sabri and K. L. Hamed, "Digital Watermarking Based On Dwt(Discrete Wavelet Transform) And Dct (Discrete Cosine Transform)," *International Journal Of Engineering & Technology (IJET)*, vol. 7, no. 4, pp. 4825-4829, 2018, doi: 10.14419/ijet.v7i4.25085.
- [21] M. J. Aqel, A. Umar and M. Agoyi, "Performance Evaluation Of Transform Domain Algorithm In Watermarking Based On Different Levels Of Sub-Band Of Discrete Wavelet Transform," *Periodicals Of Engineering And Natural Science*, vol. 7, no. 2, pp. 546-554, 2019, doi: 10.21533/pen.v7i2.549.
- [22] G. N. Mohammed, A. A. Al Fahawi and A. T. Kamil, "Combined Dwt-Disb Based Image Watermarking Optimized For Decision Making Problems," *Periodicals Of Engineering And Natural Sciences*, vol. 7, no. 3, pp. 1009-1020, doi: 10.21533/pen.v7i3.633.
- [23] W. H. Jing, "A DCT Domain Image Watermarking Method based on Matlab," *International Journal Of Advanced Network Monitoring And Controls*, vol. 2, no. 2, pp. 38-45, 2017.
- [24] P. Sharma and S. Swami, "Digital Image Watermarking Using 3 Level Discrete Wavelet Transform," *Conference On Advances In Communication And Control System (CCAC2S)*, pp. 129-133, 2013.
- [25] P. Singh, A. Agarwal, and J. Gupta, "Image Watermark Attacks: Classification and Implementation," *The International Journal of Electronics & Communication Technology*, vol. 4, no. 2, pp. 95-100, 2013.

## BIOGRAPHIES OF AUTHORS






**Lita Lidyawati**    was born in Yogyakarta (Indonesia), on March 9, 1977. She graduated from The Institut Teknologi Nasional (ITENAS) Bandung, Department of Electrical Engineering (Indonesia), in 2000. She received a Master's degree in electrical engineering from the Institut Teknologi Bandung (ITB) (Indonesia), in 2005. Her research interests concern: signals processing, visible light communications. She can be contacted at email: [lita@itenas.ac.id](mailto:lita@itenas.ac.id).






**Arsyad Ramadhan Darlis**    was born in Bandung (Indonesia), on May 1, 1987. He graduated from The Institut Teknologi Nasional (ITENAS) Bandung, Department of Electrical Engineering (Indonesia), in 2009. He received a Master's degree in electrical engineering from the Institut Teknologi Bandung (ITB) (Indonesia), in 2011. His research interests concern: visible light communications, digital signal processing, and Internet-of-Things. He can be contacted at email: arsyaddarlis@gmail.com.






**Lucia Jambola**    was born in Bandung (Indonesia), on July 3, 1977. She graduated from The Institut Teknologi Nasional (ITENAS) Bandung, Department of Electrical Engineering (Indonesia), in 2001. She received a Master's degree in electrical engineering from the Institut Teknologi Bandung (ITB) (Indonesia), in 2006. Her research interests concern: Optic communications. She can be contacted at email: shafihazidrahman@gmail.com.



**Lisa Kristiana**    was born in Semarang (Indonesia), on October, 25th, 1975. She graduated from Electrical Engineering at Universitas Katolik Soegijapranata Semarang (Indonesia), in 2001. She holds Master of Telecommunication System Engineering at Institut Teknologi Bandung (ITB) Indonesia and Ph.D in Informatics at University of Zurich, Switzerland in 2018. Her research interests are Mobile communications, Vehicular Ad-hoc Communication Network. She can be contacted at email: lisa@itenas.ac.id.



**Rea Ramada Jayandanu**    was born in Wonosobo (Indonesia), on January 24, 1996. He graduated from The Institut Teknologi Nasional (ITENAS) Bandung, Department of Electrical Engineering (Indonesia), in 2019. His research interests concern: digital signal processing. He can be contacted at email: reajramada13@gmail.com.