Analysis of image watermarking with a discrete wavelet transform for digital data security

MA Muslim\textsuperscript{1,2}, Y Dasril\textsuperscript{2}, M Khusniati\textsuperscript{1}, S Subhan\textsuperscript{1}

\textsuperscript{1}Department of Computer Science, Faculty of Mathematics and Natural Science, Universitas Negeri Semarang, Indonesia
\textsuperscript{2}Postgraduate Student, Faculty of Technology Management, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia.

\textsuperscript{*}Corresponding author: a212muslim@mail.unnes.ac.id

Abstract. One of the ways to secure digital data is image watermarking. The method for image watermarking is used with discrete wavelet transform (DWT). The problem in this article is how the performance of DWT for image watermarking. The stages of the research method are: (1) Collecting the dataset that will be used as the trial host (2) Processing data with watermarking techniques, (3) Inserting data using DWT (4) checking the quality of each method, (6) analyzing the results each method. This research has revealed the stages of data security on image watermarking with DWT and the results show that the images provided with watermarking are well secured.

1. Introduction
Image processing is popularly used in many fields, such as biology [1], medical field [2], physics [3-4], and manufacturing [5], also astronomy [6], defense, and law enforcement fields [7]. One part of this image processing is image watermarking. Image watermarking is used to secure digital data, especially digital works piracy [8-9]. This piracy is very detrimental to its owner.

Image watermarking is a technique for inserting information into digital data media in the form of images. Images are vulnerable to attacks in the form of data manipulation and replication. Image watermarking can be used to secure, protect copyright, and authenticate multimedia content [8].

An effective watermarking algorithm has invisible and robust characteristics [8]. Invisible means that the difference between the original image and the watermark image cannot be distinguished by the human eye, while solid means that an unauthorized individual or group cannot remove the watermark. Digital watermarking techniques can be classified into two; namely, spatial domain and domain transform [10-11]. In the spatial domain, the watermark is embedded in pixels. One method in the spatial domain is the least significant bit (LSB). Whereas in the transform domain, the watermark is embedded by changing the frequency component. The transform domain method has good resistance for general image processing such as compression, noise, filtering, cutting, rotation and others [12].

Image transformation can be defined as a change in the shape of an image. This form change can be in the form of geometric changes such as rotation (rotation), shift (translation), scaling, etc. It can also change the image space (domain) to another domain, such as the Fourier transform, which changes an image from a spatial domain to a frequency domain.
The wavelet transformation was introduced in the 1980s by Morlet and Grossman. This wavelet transformation represents data or mathematical functions to handle resolution problems. This transformation has two types, namely Continuous Wavelet Transform (CWT) and Discrete Wavelet Transform (DWT) [13]. The foundation of DWT started in 1976, where a technique for decomposing discrete-time signals was invented. In CWT, the signal is analyzed using a basic set of functions that are interconnected with simple scaling and transitions. Meanwhile, in DWT, a digital signal time scale of digital signals using digital filtering techniques. This process is by passing the signal to be analyzed on filters with different frequencies and scales [14].

A signal must be passed in two DWT filters, namely a high pass filter and a low pass filter, so that the frequency of the signal can be analyzed. Signal analysis is carried out on the high pass filter results and low pass filter where the high pass filter is used to analyze high frequencies, and the low pass filter is used to analyze low frequencies. This sharing of the signal is referred to as decomposition. Technically, an image with two dimensions (rows and columns) can be decomposed, as shown in Figure 1. With I is the image, H (ω) is the high pass filter, and G (ω) is the low pass filter.

![Figure 1. Image Decomposition](image)

The decomposition of the image produces information on different frequency ranges, namely LL (low-low frequency), LH (low-high frequency), HL (high-low frequency), and HH (high-high frequency), as shown in Figure 2. Frequency ranges LL is the range of scaling estimates, while the frequency ranges of LH, HL, and HH are the frequency ranges of detailed information [15].

2. Methods
This study discusses the implementation of image watermarking in digital images using Discrete Wavelet Transform (DWT). There are two images used in this study. The first image is called the host image or the original image in BMP format with grayscale color. Simultaneously, the second image is called a watermark image or message image, or secret image in BMP format with grayscale color. In this research, the message image will be inserted into the original image (host image), after this referred to as a watermarked image. The program used for the coding process in making application programs is the Matlab programming language.

In general, the process carried out is as follows: the user inputs two images, namely the host image and the watermark. Then inserts it using the Discrete Wavelet Transform (DWT) process, where the watermark image will be inserted into the host image to produce a watermarked image. The image with the watermark is then calculated using the PSNR process for the quality of the image. The watermarked image is read again and then entered into the image attack process in the watermark extract. Suppose the user does not carry out an image attack. In that case, the watermarked image enters the Daubechies process, where the watermark image in the watermarked image will be extracted to produce the extracted image. The user carries out an image attack, so the watermarked image will experience an image attack in the form of cropping or rotation, which will be carried out in the cropping or rotation process to produce a watermark cropping or rotation image. Image quality with watermark cropping or rotation will be calculated through the PSNR value.
The DWT insertion process begins by reading the host image to be inserted with the watermark. Then the watermark image is converted into a series of matrices. Meanwhile, watermark insertion is carried out in the following steps:

a) After the host image is decomposed in 1 (one) DWT level, the watermark is inserted into the LL frequency because the LL frequency is an approximation signal.

b) Find the largest coefficient f LL of the LL frequency range.

c) Inserting watermark into the LL frequency range.

d) Perform inverse discrete wavelet transform (IDWT) to form a watermarked image.

3. Results and Discussion

In this study, the original images used were true color (RGB) and grayscale images. In selecting true color (RGB) images, both the original image and the watermark image must be changed to a grayscale image because the domain used in the MATLAB programming language is the grayscale domain. The original image used has various sizes, both RGB and grayscale images. At the same time, the inserted watermark image is an RGB image with dimensions of 100 x 100.

The images used in this study are as shown in table 1. The image consists of images of Bike, Babon, and Airfield. This image is then watermarked with a cherry image.

| Name | Image |
|------|-------|
| Airfield | ![Airfield Image](image1.png) |
| Babon | ![Babon Image](image2.png) |
| Bike | ![Bike Image](image3.png) |
| Cherry | ![Cherry Image](image4.png) |

In this watermarking analysis process, an application is made to provide watermarking of existing images. This application uses the Matlab programming language, as shown in Figure 2.

![Figure 2. Watermarking Analysis Application](image5.png)
This application applies the steps of the image watermarking embedding process and the watermark image extraction process that has been given a watermark. The image embedding step is shown in Figure 3. Figure 4 shows the steps for the image extraction process.

Figure 3. Image Embedding step With DWT Algorithm

```
DWT Algorithm

Original Image

Watermark Image

Embedding process

Watermarked
```

Figure 4. Watermark Image Extraction Process

```
DWT Algorithm

Test Image

Original Image

Extraction process

Extracted Watermark
```

In this study, the embedding of the cherry image was carried out in this watermarking image. Furthermore, the results of this administration are extracted again. Look at the result of inserting the bike image with the following cherry image. This process is shown in figure 5.

Figure 5. The process of giving a watermark with DWT Algorithm
To evaluate imperceptibly, we use the Mean Squared Error (MSE) and Peak-Signal-to-Noise Ratio (PSNR), which is defined as follow:

\[
MSE = \left( \frac{1}{MN} \right) \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{ij} - \bar{X}_{ij})^2
\]

\[
PSNR = 10 \cdot \log_{10}\frac{I^2}{MSE} \text{ dB}
\]

The PSNR measures the similarity between two images, while the MSE measures the difference between these two images.

**Table 2. PSNR and MSE of DWT Algorithm**

| Image   | MSE     | PSNR    |
|---------|---------|---------|
| Bike    | 7.9674e-09 | 186.5979 |
| Airfield| 7.9674e-09 | 184.5581 |
| Baboon  | 7.9674e-09 | 183.5576 |

Table 2 shows that the PSNR and MSE values are stable. This large PSNR value and small MSE also indicate that the image watermarking process produces almost no different images between images before being inserted with the watermark and after being inserted. These results indicate that DWT algorithm is reliable. It is appropriate that watermarks are reliable if there is no known key in digital data [16]. The results of this process indicate that the watermarking process with the DWT algorithm is running well.

### 4. Conclusion

This article has provided an analysis of image watermarking using the DWT algorithm. In this article, we have shown the results of the large PSNR and the small MSE. This shows that the DWT algorithm is reliable. The algorithm is running well so that it can be used for digital data security.

### Acknowledgments

The authors would like to express their gratitude and appreciation to the Universiti Tun Hussein Onn Malaysia (UTHM) through the research grant TIER 1 (H777).

### References

[1] Ruszczycki B, Bernas T, 2018 *Bioinformatics* **34** 845
[2] Noor SSM, Michael K, Marshall S, Ren J, 2017 *Sensors* **17** 2644.
[3] Li H, Kingston A, Myers G, Recur B, Sheppard A 2015 *IEEE Trans. Nucl. Sci.* **62** 2075
[4] Bianco V, Memmolo P, Paturzo M and Ferraro P 2016 *Opt. Lett.* 41, 5226–5229
[5] Torabi M, Mousavi SGM, Younesian D 2018 *IEEE Trans. Ind. Electron.* **65** 8239
[6] Kremer J, Stensbo-Smidt K, Gieseke F, Pedersen KS, Igel C 2017 *IEEE Intell. Syst.* **32** 16
[7] Peng C, Gao X, Wang N, Li J 2017 *Syst. Video Technol.* **27** 288
[8] Liu S, Pan Z & Song H 2017 *IET Image Processing* **11**(10) 815
[9] Muzakir A & Habibi M 2017 *Sci. J. Inform.* **4**(1) 20
[10] Moosazadeh M & Ekbatanifard G 2017 *Opt. - Int. J. Light Electron Opt.* **140** 975
[11] Setiadi DRIM, Sutojo T, Rachmawanto EH & Sari CA 2017 2017 5th International Conference on Cyber and IT Service Management (CITSM). doi:10.1109/citsm.2017.8089229
[12] Wang FH, Pan JS, Jain LC 2009 *Studies in Computational Intelligence* (Springer: Berlin, Heidelberg)
[13] Aloitaib RA & Elrefaei LA 2018 *Applied Computing and Informatics* **15**(2) 191
[14] Choudhary R & Parmar G 2016 2016 2nd International Conference on Communication Control
and Intelligent Systems (CCIS). doi:10.1109/ccintels.2016.7878213

[15] Makbol NM, Khoo BE, Rassem TH & Loukhaoukha, K 2017 Inf. Sci. 417 381

[16] Tao H, Chongmin L, Mohamad Zain J & Abdalla AN 2014 J. Appl. Res. Technol. 12 (1) 122