A non-blind robust and impercept watermarking using discrete cosine transform and discrete wavelet transform

Eko Hari Rachmawanto¹, Heru Agus Santoso*²
Universitas Dian Nuswantoro, Indonesia ¹,²

Article Info
Keywords:
Non-Blind Watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Attacks, Peak Signal to Noise Ratio

Article history:
Received: October 20, 2020
Accepted: January 5, 2021
Published: February 28, 2021

Cite:

*Corresponding author.
Heru Agus Santoso
E-mail address: heru.agus.santoso@dsn.dinus.ac.id

Abstract
Non-blind watermarking is a form of watermarking with a watermark image validation process that requires a host image. The use of the transform domain is more robust and imperceptible. The transform domain method is resistant to various forms of digital image attacks. In this study, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) were selected as watermark insertion algorithms. DCT is faster and more resistant to attacks, especially in image compression attacks, but has lower imperceptibility than DWT. DWT is also known to be resistant to noise attacks, filtering, blurring, cropping, and has high imperceptibility depending on the sub-band selection but is not resistant to image compression attacks. Based on each algorithm's advantages and disadvantages, there is an opportunity to combine it to analyze and compare the insertion results with DCT and DWT itself. To test the results of imperceptibility, we used the Peak Signal to Noise Ratio (PSNR), while to test the robustness, we used Cross-Correlation (CC) and Bit Error Ratio (BER). Without attacks, the PSNR on the proposed method can reach 71 dB. The CC value without attack can reach a perfect value of 1 and BER = 0. The highest attack test result is CC = 1 on the filtering attack. From the various tests we have conducted, it has been proven that the DCT-DWT is more imperceptible and robust than previous studies.

1. Introduction
The ease with which people, especially young people, access the internet is used for various things such as social media, playing music, playing films, and exchanging photos. Digital information exchange can easily disseminate information without giving the source. For irresponsible individuals [1], digital data can be misused by modifying it and spreading it back such as digital image. Such actions need to be prevented, one of which is by labeling watermarks in an invisible form.

Digital watermarking means entering information into digital material in a way that people find difficult to detect [2] but can easily be detected by computer algorithms [3]. A digital watermark is a transparent and invisible information fed into a digital data source component using a specific computer algorithm. When a watermark is included in a test image with a key known to an algorithm, it is known as the digital watermark embedding process, and when the watermark is taken from a watermarked image using the original image and the key is known as the digital watermark extraction process [4]. There are various algorithms for digital watermarking. A watermarking scheme's success depends mostly on the choice of the watermark structure and the embedding strategy. The quality of digital watermarking [5] can be measured by two different parameters: imperceptibility and robustness. Imperceptibility is measured by the PSNR (Peak Signal to Noise Ratio) of the host image, and the embedded image is in dB. A higher PSNR is desirable because it hides the tagged image efficiently, whereas robustness is measured by comparing the original watermark image and the extracted watermark image [6].

Invisible watermark insertion has two domains, namely spatial domain and transforms domain. Watermarking can also be categorized as blind watermarking (a watermark image validation process that does not require a host image) and non-blind watermarking (a watermark image validation process that requires a host image) [7]. In the spatial domain, the watermark image can be inserted into the host image pixels directly, and it can be done easily and quickly; if the transform domain, the host image will be converted into a frequency before inserting the watermark image [8]. The transform domain method is resistant to various kinds of image attacks, such as the compression process [9]; therefore, this research will use the transform domain method. According to [10][6] DCT is faster and more resistant to attacks, especially in image compression attacks. DWT [11] is also known to be resistant to noise attacks, filtering, blurring, cropping, and produces higher imperceptibility [12] than DCT [13]. Haar Wavelet method is competitive and efficient using numerical solution of evolution equations, while [14] Haar Wavelet has advantages in hardware area and consumption decrease and mainly speed increases.
In a study conducted [10] using the HWT-DCT (Haar Wavelet Transform) on a 512x512 grayscale image and a 32x32 binary image watermark. The experiment results on eight attacks resulted in the Correlation Coefficient (CC) value, which did not produce a perfect value for the Gaussian noise attack, which only reached 0.6. In contrast, the image without attack resulted in CC = 1, and the highest PSNR was 45 dB [7]. Also carried out the merger of DCT and DWT was in 2015 [7]. In this study, DWT has applied first then DCT. By inserting the last 10 pixels in the DCT block, the PSNR value is obtained without attaching with a value of more than 50 dB; while in an attack, there are still many PSNRs of less than 30 dB [15], proposed DCT and SVD. This research got PSNR highest PSNR in 49.50 dB. On the other hand, the CC value of several attacks is excellent and close to 1. Based on several studies reviewed above, there is an opportunity to combine DCT-DWT or DWT-DCT by changing the watermark insertion location in the DWT sub-band variations pixel location the DCT and several different watermark sizes. In this paper, we have written the results of various experiments carried out to overview and information about which combination is the most optimal.

2. Research Method

2.1 Discrete Cosine Transform (DCT)

As an orthogonal transform, in DCT, two frequency layers can be used for watermark insertion, namely AC and DC Coefficient [16] according to Figure 1. Based on Nilima, the process complexity of DCT is lower than DWT [17]. DCT is resistant to digital image compression, especially JPEG 2000 [18].

According to [19], DCT is used to transform the block intensity value of 8x8 pixels sequentially from images to 64 DCT coefficients into its basic frequency, changed the coefficients, and then transformed back with IDCT (Inverse Discrete Cosine Transform). According to [20] the advantages of DCT even though the image is compressed with JPG compression will not raise suspicion because this method occurs in the frequency domain in the image, not in the spatial domain, so changes will not be visible in the image. While the DCT method’s weakness is not strong against an object change because of the straightforward deletion of data locations and data creation that have been done using the DCT method [12]. According to [21][22] DCT (Discrete Cosine Transform) is an N x N matrix. The DCT (Discrete Cosine Transform) equation for an N x N block matrix can be written as Equation 1.

\[
S(u, v) = \frac{2}{\sqrt{nm}} C(u)C(v) \sum_{y=0}^{m-1} \sum_{x=0}^{n-1} S(x, y) \cos \left( \frac{(2x+1)\pi u}{2n} \right) \cos \left( \frac{(2y+1)\pi v}{2m} \right)
\]

(1)

With \( u = 0, ..., n - 1 \), \( v = 0, ..., m - 1 \). Where \( S(u, v) \) is the data in the frequency domain, \( S(x, y) \) is the data in the space domain. The DCT (Discrete Cosine Transform) inverse formula is as Equation 2.

\[
S(u, v) = \frac{2}{\sqrt{nm}} C(u)C(v) \sum_{y=0}^{m-1} \sum_{x=0}^{n-1} S(u, v) C(u)C(v) \cos \left( \frac{(2x+1)\pi u}{2n} \right) \cos \left( \frac{(2y+1)\pi v}{2m} \right)
\]

(2)

With \( x = 0, ..., n - 1 \), \( y = 0, ..., m - 1 \). \( S(u, v) \) = data in the frequency domain, \( S(x, y) \) is the spatial domain data. To get the high frequency and low frequency, add the u and v values. So if \( u + v \) is higher, it means that \( S(u, v) \) states that the higher frequency component. The input and output of the DCT function is also a matrix with the size of NxN. P(x, y) is the pixel value at the (x, y) coordinate; the index starts at 0.
2.2 Discrete Wavelet Transform (DWT)

DWT is also known as part of the orthogonal transform with advantages in image decomposition [23], fast computation [24], and high imperceptible when applied to the LL sub-band [18][25]. In DWT, there are four sub-bands, namely LL, LH, HL, and HH, according to Figure 2. Each sub-band can be deepened through level decomposition.

![Figure 2. 2L-LL Sub band of DWT][26]

Based on Figure 2, LL is low frequency, LH and HL are medium frequency, HH is high frequency.

2.3 Proposed Method

The main idea that we implemented was to combine DCT and DWT. The image will be processed first at the AC coefficient and then continued to DWT on the LL subband. Several studies use a combination of the DWT and DCT techniques. Operating DCT or DWT first will certainly produce embedding images and different robustness results, as did in research using DWT-DCT [7]. Using the same image, according to research conducted using HWT-DCT [9] and Heidari using DWT-SVD [15], it is proven to produce different impercept values and robustness. This paper proposed a combination method to increase imperceptibility and robustness value better than [7][9][15].

![Figure 3. Proposed Method: a) Embedding, b) Extracting][27]
Figure 3 about embedding process has been spelled out here:

1. The host image is transformed to DCT according to the coding $\text{imgdct} = \text{dct2(Citra\_host)}$.
2. The host image that has been DCT done is then decomposed using the DWT level 1 method into LL, LH, HL, and HH. Image LL yang akan dilakukan penyisipan image watermark pada DWT level 2 (LL2).
3. Then the watermark is inserted into the LL2 sub-band according to the Equation 3.
   \[
   X_w \begin{cases} 
   \sigma, & \text{if } W = 1 \\ 
   -\sigma, & \text{if } W = 0 
   \end{cases}
   \tag{3}
   \]
   where $\sigma$ is the standard deviation of the host image and the alpha value we use is 0.2. Insertion on matlab using
   \[\text{img}(1:x,1:y) = \text{img}(1:x,1:y) + \text{alpha} \times \text{double(w\_gray)};\]
4. Produced watermarked LL2 sub-band.
5. Proses inversi DWT dilakukan pada image Newhost_LL2.
   \[\text{watermarkedg} = \text{idwt2(newhost\_LL2,o\_LH2,o\_HL2,o\_HH2,'haar');}\]
6. The DCT inversion process is carried out on the watermarked image. The watermarked image is obtained.
   \[\text{watermarkedg} = \text{idct2(watermarkedg);}\]

Extraction process due to getting the message image in Figure 3 b) had been spelled here:

1. The watermarked image is transformed by the DCT method through \[\text{watermarkedgdct}=\text{dct2(watermarked);}\]
2. The watermarkedgdct image is decomposed using the DWT level 1 LL, LH, HL, and HH methods, and then it is continued at DWT level 2 to become LL2, LH2, HL2, and HH2.
3. Take the LL2 sub-band for watermark extraction.
4. Perform watermark extraction on the LL sub-band with the help of the LL2 sub-band host image with the coding
   \[\text{eWatermarkedg}=(\text{eimg}(1:x,1:y)-\text{o\_LL}(1:x,1:y))./\text{alpha};\]

3. Results and Discussion

For all experiments, we used 20 grayscale cover images measuring 512x512 pixels with the file types * .bmp, * .bmp, and * .jpg to analyze the difference in results between the file extensions. The embedded message image is a grayscale image measuring 32x32 pixels and 64x64 pixels. The cover image and message can be seen in Figure 4 and Figure 5, respectively. The cover image is taken from http://www.imageprocessingplace.com/root_files_V3/image_databases.htm, [10][15][7].
We have done watermarking by implementing the AC coefficient on DCT then continued with the selection of the LL subband on the DWT at the second level (2L-DWT). The results of the embedding and extraction are as shown in Figure 6.

![A Comparison PSNR between 32, 64, 128 pixels message image](Image)

**Figure 6. Impercept Value DCT-DWT by PSNR against Several Types of Message Image without Attack**

Based on Figure 6, the watermarking process using binary as message image produces the highest PSNR value. The binary image is considered lighter and faster in processing because it only operates bits 0 and 1; this also makes PSNR higher than if we used grayscale message image. The use of smaller images also results in a higher PSNR value, as in the comparison between using 32x32 pixels and 128x128 pixels. Larger message images are heavier and involve more pixel changes. In this experiment, we use a message image with six variations to prove that the message image size affects PSNR. In Figure 6, the PSNR acquisition of jpg images is relatively higher than that of BMP images. This is because the use of DCT, which can compress the jpg image, is better than the bmp image. In the absence of digital image attacks, the highest PSNR in our proposed method is 79.61 dB for the babbon.jpg image, carried out by a 32x32 binary pixel image watermark. At the same time, the lowest PSNR is 68.71 dB on the earth.bmp image with a watermark in the form of a 128x128 grayscale image. Our proposed method proved to be imperceptible, where all the PSNRs produced were still higher than 40 dB. According to [4][27][28], the lowest PSNR to be able to meet imperceptibility is 40 dB. The standard for calculating the PSNR that we do is as in research conducted by their research.

<table>
<thead>
<tr>
<th>Name of the image</th>
<th>32x32 pixels grayscale</th>
<th>32x32 pixels binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.bmp</td>
<td>51.4532</td>
<td>73.69</td>
</tr>
<tr>
<td>Pirate.bmp</td>
<td>51.4534</td>
<td>68.71</td>
</tr>
<tr>
<td>Bee.bmp</td>
<td>-</td>
<td>73.33</td>
</tr>
</tbody>
</table>

Based on Table 1, compared with the previous method [7] using 32x32 pixels message image and 512x512 pixels cover image proposed with 1LL-DWT and 8X8 block DCT yielded the highest PSNR in 51.45 dB [10] using a 32x32 pixel message image and 512x512 pixel image grayscale proposed with DWT in Haar filter called IWT and DCT yielded the highest PSNR in 45.01 dB. Another proposed in DCT-SVD by [15] in 32x32 pixels binary and 512x512 pixels grayscale image yielded the highest PSNR in 49.50 dB. Based on the comparison with the methods they have done, it is proven that our algorithm is more imperceptible, which means that the watermarked image does not look different from the original image. Using grayscale as a message image, our proposed method yielded the lowest PSNR in 68.71 dB in Pirate.bmp and the highest PSNR in Lena.bmp in 73.69 dB. Using binary as message image, PSNR [15] left very far behind ours. The use of DWT in LL2 makes PSNR more imperceptible than LL1.

\[
MSE = \frac{1}{m \times n} \sum_{i=1}^{n} \sum_{j=1}^{m} (f_{ij}^o - f_{ij})^2
\]

(4)

\[
PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right)
\]

(5)

Where, $f^i$ is the cover image, and $f^o$ is watermarked image as shown in Equation 4 and Equation 5. To prove the robustness of the DCT-DWT, we have calculated the CC and BER values using Equation 6 and Equation 7. Robustness is used to determine the results of image extraction, whether the extraction process is not well studied, resulting in an image that cannot be extracted back into the original message image. The perfect CC value is one while the perfect BER value is 0 [29]. If the CC and BER values have been met, then the extraction process has fulfilled the imperceptibility aspect. In this experiment, the proposed method DCT-DWT succeeded in producing perfect CC and BER values in both jpg and bmp images in binary and grayscale messages.

$$cc = \frac{\sum_m \sum_n (w_{mn} - \bar{w})(w'_{mn} - \bar{w'})}{\sqrt{(\sum_m \sum_n (w_{mn} - \bar{w})(\sum_m \sum_n r_{mn} - \bar{r}')}}}$$  (6)

$$BER = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} W(i,j) \oplus W'(i,j)}{m \cdot n}$$  (7)

Table 2. Robustness Value DCT-DWT by NCC and BER without Attack

<table>
<thead>
<tr>
<th>Image Name</th>
<th>NC binary</th>
<th>NC grayscale</th>
<th>BER binary</th>
<th>BER grayscale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32</td>
<td>64</td>
<td>128</td>
<td>32</td>
</tr>
<tr>
<td>a.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>b.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>d.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>e.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>f.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>g.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>h.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>j.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>k.jpg</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>l.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>m.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>n.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>o.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>p.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>q.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>r.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>s.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>t.bmp</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Based on Table 3, we had been investigated our proposed method with attacks condition. Here, we tested using compression, noise, filtering, and cropping. For compression we compared with [10] in JPEG compression with Q = 30. Our proposed method slightly higher than [10]. In Table 4, we tested using noise are salt and pepper in $p = 0.03$ and Gaussian noise in $V = 0.3$. For [15] result in all the noise attacks yielded better performance than [10], while our proposed method better than [15]. Best CC value is 1, and the worst is 0—Table 4 shows that our results highest than two previous research.

Table 3. CC for 32x32 Pixels against JPEG Compression with Q=30

<table>
<thead>
<tr>
<th>Image Name</th>
<th>[10]</th>
<th>Our Proposed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena.bmp</td>
<td>0.9134</td>
<td>0.9220</td>
</tr>
<tr>
<td>Bee.bmp</td>
<td>0.9213</td>
<td>0.9320</td>
</tr>
</tbody>
</table>

© 2021 The Authors. Published by Universitas Muhammadiyah Malang
This is an open access article under the CC BY SA license. (https://creativecommons.org/licenses/by-sa/4.0/)
Filtering attacks such as unsharp filter and median filter in (5x5) kernel pixel has been implemented. Compared with [10] in Lena.bmp and Bee.bmp are reached lower CC than our proposed method, although CC values also obtain a value close to 1. We compared with the median filter attack [10][15]. Heidari had value = 1 in all his dataset, but our proposed method has one CC in 0.9986 while [15] got 1. This also happens with cropping attacks, that the herd is better than [10] but our proposed method is better than the two studies. Our CC obtained slightly adrift from the results [15].

<table>
<thead>
<tr>
<th>Table 4. CC for 32x32 Pixels Against Noise Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
</tr>
<tr>
<td>Lena.bmp</td>
</tr>
<tr>
<td>Pirate.bmp</td>
</tr>
<tr>
<td>Bee.bmp</td>
</tr>
<tr>
<td>Pepper.jpg</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5. CC for 32x32 Pixels Against Filtering and Cropping Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Name</td>
</tr>
<tr>
<td>Lena.bmp</td>
</tr>
<tr>
<td>Pirate.bmp</td>
</tr>
<tr>
<td>Bee.bmp</td>
</tr>
<tr>
<td>Pepper.jpg</td>
</tr>
</tbody>
</table>

Based on the presentation of several attacks that we have implemented and we have compared with research conducted by [10][15], there are several findings, namely the PSNR value that we produce is better than the two studies. This negates that our method is invisible. In the calculation of robustness, our research is superior to Susanto's proposed method, but there is one CC value belonging to Heidari that is better than ours, namely the median filter attack. On the other hand, all CC values other than the attack filter, especially in the Pirate.bmp image, are better than [15], so our method is still robust.

4. Conclusion

Blind watermarking is not a new method, but until now, it still exists to be used in this watermarking technique because it is easier to practice. In our research, we have presented the use of the DCT-DWT algorithm, where DCT is implemented on the AC coefficient while DWT is implemented in the 2LL sub band. This combination is carried out to achieve imperceptibility and robustness. We have implemented several message image sizes ranging from 32x32, 64x64, and 12x128 pixels engraving with binary and grayscale image types. From the PSNR, CC, and BER measurements, it has been proven that our proposed method is relatively better than the two studies we have chosen as a comparison. The PSNR value without attack reached 79 dB, BER = 0, CC = 1. Our PSNR values on all engraved message images were higher than 40 dB. For the PSNR value, we obtained was higher than the two studies we used for comparison. To prove robustness, we use several attacks, including compression, noise, filtering, and cropping. Our CC value is much higher than the research conducted [10] whereas, in the research conducted [15] is there only 1 CC value, which is higher than the value we obtained, namely the bmp image. For further research, we want to use message cyra measuring 256x256 pixels and 512xto investigate the PSNR value of the maximum size message and more dithe verse the use of attacks.

References


© 2021 The Authors. Published by Universitas Muhammadiyah Malang
This is an open access article under the CC BY SA license. (https://creativecommons.org/licenses/by-sa/4.0/)