Embedding and Extracting Technique for Implementing Image Watermarking Based on DCT (Discrete Cosine Transform)

Irfan *, Nazori Agani**

* Engineering Faculty, UHAMKA University, Jakarta, Indonesia

** Department of Electrical Engineering and Computer Science Postgraduate, Budi Luhur University, Jakarta, Indonesia

Keywords:
watermarking, DCT, image, embedding, extracting, algorithm

ABSTRACT
The protection of ownership and prevention of unauthorized tampering with multimedia data (audio, video, image and text) have become important concerns. Image authentication verifies the originality of an image by detecting malicious manipulation. Digital watermarking is the process that embeds data called watermark into multimedia object such that watermark can be detected or extracted later only with appropriate decoding mechanism. We proposed invisible watermarking using DCT (Discrete Cosine Transform) and explain its algorithm (embedding and extracting image). The ultimate goal to the watermark is retrieve the right owner information from the received data in a correct way. Digital watermarking technology plays important role in content protection issues. Attacks and obstacles are also had to be faced by this technology. The main obstacle is that there is no standard available for watermarking techniques. Without any specific standard, it is difficult to determine how robust a watermarking technique should be.

Corresponding Author:
Irfan
Engineering Faculty, UHAMKA University, Jakarta, Indonesia
Jl. Limau II, Kebayoran Baru, Jakarta 12130
Email: irfan03092008@gmail.com

1. INTRODUCTION
In the era of digital Data is now experiencing very rapid growth. Many of the digital data is exchanged for various purposes. Start from interest in a positive and a negative interest. One of them is the doubling of illegally as piracy of CD, digital image ownership conflicts and so on. This resulted in the digital data into one of the limelight due to the ease of this data to be duplicated without fear or worry about any quality loss [2]. So much effort or methods developed to protect digital data from a doubling of effort over. Watermarking is present as an alternative to protecting digital data from people who are not responsible. But watermarking in fact also very often have a variety of attacks. This attack can be a natural attack i.e. processing the image in general like the rotation, translation, and cropping as well as attacks that are not really natural aims to remove the watermark.

Actually abuse problem possession document digital in the plane of multimedia is not just about doubling and distribution course, but also on labels possession. Current product multimedia not only can be distributed in offline, but could do too online via internet. And most of multimedia products circulating in internet does not mention the owner, information so that the product multimedia it can be claimed by anyone as a his right.

The information that is inserted into the image is called a watermark, and the watermark can be considered as digital prints (digital signature) the legitimate owners of the digital image. In other words, a watermark is inserted into a label document ownership digital the landlord. Inserting data with techniques of Watermarking is done in such a way that the information inserted does not damage the digital data that is protected. Inserted Data is hidden and its existence is not realized by the human senses.

Literature review, Watermarking has been around for 700 years ago. In the late 13th century, paper mills in Fabriano, Italy, making paper with watermarks or water marks by pressing print drawing or writing
on the new paper in half so. When the paper is dried it is making a paper berwatermark. This paper is commonly used by artists or poets to write in their paper. Paper that has been labelled the water at once made the identification that the artwork on it are their property [1]. Juan r. Hernández, et al [8] use the application domain watermarking using DCT (Discrete Cosine Transform) on the images to analyze the performance of the detector, Jafilun [9] using digital watermarking application on spatial domain method using LSB (Least Significant Bit), a watermark in the form of text and images with the cover image of stylized images. Used for application protection and ownership of copyright. Joseph Perwej, et al [10], technique watermarking used is edge detection use gabor filter, and encrypt message used technique lsb (least significant bits), force watermarking the calculated use pnsr (peak signal to noise ratio) and normalized cross correlation (nc) to count its similarity level. Mei Jiansheng, et al [11] using watermarking using DWT on medical image produces a good resilience in doing image processing on digital watermarking. Rinaldi Munir [12] using correlation-based method in DCT domain for watermarking of colored image produced on a robust watermarks against some attacks on non-malicious attack like JPEG compression, histogram equalization, gamma correction, cropping, resizing, noising, sharpening. Rahmatri Mardiko [13] use of image watermarking based on SVD evaluate (Singular Value Decomposition), dither and quantization detection side showed that the scheme of watermarking robust against JPEG compression, rotation, zoom/diminution, and PSNR. The removal of reliable in-line or column is deletion and cropping up to a certain level.

2. RESEARCH METHOD

Watermarking is one form of Steganography, which is the study of how to hide data in another data. Watermarking (watermark) is a bit different with the watermark on banknotes. Watermark on banknotes are still visible to the senses (in particular paper position), but the Watermarking on digital media will not be perceived by human presence without digital processing machine tools such as computers [3]. Watermarking is utilizing the deficiencies of the system senses such as eyes and ears. The existence of these deficiencies, the method of Watermarking can be applied to a variety of digital data. So it is a way of Watermarking to hide or to plant a certain data/information into any other digital data, but not known its presence by the human senses. The process of inserting watermarks into images is called encoding. Encoding can be accompanied with key lock entry. The key required to watermark can only be extracted by a legitimate party. The key is also intended to prevent watermark removed by the party not entitled to [5].

![Figure 1. The process of watermark on digital image][9]

Visible watermarking, This type of Watermark can be seen by the human senses. Visible watermarks are extremely robust due to its existence can be seen and recognized easily and use visible watermarks on digital imagery is difficult to remove. A Watermark is inserted can be solid or semi transparent, some characteristics are shared by a visible watermark is as follows [6]:

![Figure 2. Process decodes watermark on digital image][9]
must can be seen clearly either on color image and image monochrome
• a watermark used not reduced quality detail of the original image considerably
• a watermark must be hard to be omitted (robustness).

Invisible watermarking, this type of Watermark is not visible and difficult to detect his presence by human senses, but can be extracted by using the method of computation. The purpose of this is to watermark invisible in use in the purposes of the verification process of ownership of an image file, usually when the information is in the image on the extract required a password that is used to process the information extraction and password this is called with the watermark key.

This figure shows invisible watermarking.

DCT (Discrete Cosine Transform), Digital image Watermarking against can be applied to different domains. There are carried out directly on the digital data type or first made the transformation into other domains. One of the transformation is used the Discrete Cosine Transform (DCT) which converts digital data into frequency domain. Method in DCT transformation techniques do in is to break the digital image into small blocks of a fixed size and then converted from the spatial domain into the frequency domain. DCT techniques are reconstructed the matrix image into 3 areas of frequency of Low Frequency (LF), Medium Frequency (MF) and High Frequency (HF). Human senses which sense vision of the human eye is only able to see the picture at the level of the low frequency or low frequency (LF). The Discrete Cosine Transform (DCT) method of transformation is used as a basis in the compression Joint Photographic Experts Group (JPEG). Part of DCT has the highest energy called DC, located on the top left of the image. The following is the formulation used in the DCT method.

\[
DCT = C(p,q) = \alpha_p \alpha_q \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} I(m,n) \cos \frac{\pi(2m+1)p}{2N} \cos \frac{\pi(2n+1)q}{2N}
\]

While the formula used for the inverse of a return value generated by the DCT image is defined by using the following formula:

\[
IDCT = I(m,n) = \sum_{p=0}^{N-1} \sum_{q=0}^{N-1} \alpha_p \alpha_q C(p,q) \cos \frac{\pi(2m+1)p}{2N} \cos \frac{\pi(2n+1)q}{2N}
\]

Description of variables used in the formulation of the above is as follows:
• C = the image with the components of the original pixel values
• I = the image with the components of the inverse DCT calculation result
• 0 ≤ p ≤ M - 1
• 0 ≤ q ≤ N - 1

\[
\alpha_p = \begin{cases} 
\frac{1}{\sqrt{M}} & , p = 0 \\
\sqrt{\frac{2}{M}} & , 1 \leq p \leq M - 1
\end{cases}
\]

\[
\alpha_q = \begin{cases} 
\frac{1}{\sqrt{N}} & , q = 0 \\
\sqrt{\frac{2}{N}} & , 1 \leq q \leq N - 1
\end{cases}
\]

p, q = the position of pixels in the image
M = the number of rows of images
N = the number of columns of the image
Method of insertion of the ownership documents of digital data pat seen in Figure 4, Watermark embedding steps are as follows [4]:
1. Image I transformed by DCT
2. All DCT coefficient is arranged with zig-zag
3. Select DCT coefficient on middle frequency (FM) through the taking DCT coefficient, from coefficient \( L+1 \) to coefficient \( L+N \), e.g all coefficient DCT which selected is store in laric \( V \).

4. Insert watermark \( W \) into laric \( V \) with formula: \( v'(i) = v(i) + \alpha |v(i)|w(i) \)

5. Put into new DCT coefficient \( (v') \) on first position, so implements invers DCT to get image watermark.

![Diagram of watermark insertion](image1.png)

Figure 4. Insert watermark to image

While the method to extract the watermark from the watermark image can be seen from the following figures:

![Diagram of watermark extraction](image2.png)

Figure 5. Decode watermark

3. RESULTS AND ANALYSIS

This applied research a method selection sample randomly. Random in that it is a picture of what the author take with various dimensions and different image sizes, to get the property of image using matlab software are ; mean(‘image1.jpg’);std(‘image1.jpg’); and median(‘image1.jpg’);

<table>
<thead>
<tr>
<th>Table 1. Property of various image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
</tr>
<tr>
<td>Dimension</td>
</tr>
<tr>
<td>Image 1.jpg</td>
</tr>
<tr>
<td>Image 2.jpg</td>
</tr>
<tr>
<td>Image 3.bmp</td>
</tr>
<tr>
<td>Image 4.bmp</td>
</tr>
<tr>
<td>Image 5.png</td>
</tr>
<tr>
<td>Image 6.png</td>
</tr>
<tr>
<td>Image 7.tif</td>
</tr>
<tr>
<td>Image 8.tif</td>
</tr>
</tbody>
</table>
And image watermark (logo) that used to insert is as follows:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Measurement Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logo1.jpg</td>
<td>225 x 225, 6.65 KB, 93.0625, 23.5130, 103</td>
</tr>
<tr>
<td>Logo2.jpg</td>
<td>148 x 144, 4.23 KB, 93.1250, 23.3891, 103</td>
</tr>
<tr>
<td>Logo3.bmp</td>
<td>225 x 225, 148 KB, 92.2667, 24.2678, 105.5000</td>
</tr>
<tr>
<td>Logo4.bmp</td>
<td>225 x 225, 148 KB, 92.3333, 24.1414, 105.5000</td>
</tr>
<tr>
<td>Logo5.png</td>
<td>225 x 225, 75.1 KB, 95.2000, 23.6347, 82</td>
</tr>
<tr>
<td>Logo6.png</td>
<td>225 x 225, 21.5 KB, 95.2667, 23.4961, 82</td>
</tr>
<tr>
<td>Logo7.tif</td>
<td>225 x 225, 161 KB, 92.8000, 24.6060, 104</td>
</tr>
<tr>
<td>Logo8.tif</td>
<td>225 x 225, 159 KB, 92.8667, 24.4799, 104</td>
</tr>
</tbody>
</table>

So all the image calculate using DCT in matlab, code for DCT using matlab are:

```matlab
logo_size_height=double(src_size_height/8);
logo_size_width=double(src_size_width/8);
for x=1:logo_size_height
    for y=1:logo_size_width
        if ( src_size_height> (y+pointy) & src_size_width> (x+ pointx) )
            dct_logo(x,y,1)=dct_src((x+pointx),(y+pointy),1);
            dct_logo(x,y,2)=dct_src((x+pointx),(y+pointy),2);
            dct_logo(x,y,3)=dct_src((x+pointx),(y+pointy),3);
        else
            dct_logo(x,y,1)=0;
            dct_logo(x,y,2)=0;
            dct_logo(x,y,3)=0;
        end
    end
end
```

After watermarking, image has been image watermarked to be as follows:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Measurement Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1'.jpg</td>
<td>872X576, 103KB, 96.1765, 22.774, 103</td>
</tr>
<tr>
<td>Image 2'.jpg</td>
<td>256 X 192, 15.2KB, 96.2353, 23.6424, 103</td>
</tr>
<tr>
<td>Image 3'.bmp</td>
<td>128 X 128, 48 KB, 95.625, 23.551, 97.5</td>
</tr>
<tr>
<td>Image 4'.bmp</td>
<td>128 X 128, 48 KB, 95.6875, 23.42, 97.5</td>
</tr>
<tr>
<td>Image 5'.png</td>
<td>816 X 880, 1.72 MB, 96.375, 23.7539, 103</td>
</tr>
<tr>
<td>Image 6'.png</td>
<td>1120X1104, 2.73 MB, 96.4375, 23.6219, 103</td>
</tr>
<tr>
<td>Image 7'.tif</td>
<td>280 X 184, 152 KB, 80.125, 20.2151, 83</td>
</tr>
<tr>
<td>Image 8'.tif</td>
<td>232 X 216, 145 KB, 80.1875, 20.1137, 83</td>
</tr>
</tbody>
</table>

Than, the image quality testing through the calculation of the value of PSNR and MSE images are:

<table>
<thead>
<tr>
<th>Properties</th>
<th>Measurement Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image 1'.jpg</td>
<td>3.8432, 42.28387</td>
</tr>
<tr>
<td>Image 2'.jpg</td>
<td>3.8353, 42.29281</td>
</tr>
<tr>
<td>Image 3'.bmp</td>
<td>4.05, 42.05239</td>
</tr>
<tr>
<td>Image 4'.bmp</td>
<td>2.00, 45.1205</td>
</tr>
<tr>
<td>Image 5'.png</td>
<td>4.375, 41.72102</td>
</tr>
<tr>
<td>Image 6'.png</td>
<td>4.3661, 41.72987</td>
</tr>
<tr>
<td>Image 7'.tif</td>
<td>11.7321, 37.43705</td>
</tr>
<tr>
<td>Image 8'.tif</td>
<td>11.7411, 37.43372</td>
</tr>
<tr>
<td>Image 1'.jpg</td>
<td>11.75, 37.43042</td>
</tr>
</tbody>
</table>

4. CONCLUSION

The watermark technique created is expected to add a watermark into digital image document well without reducing image quality significantly or decreased quality of the image is still within a reasonable tolerance value. The use of the technique in the application of DCT watermark is expected to produce a robust watermark image so resistant to various image file manipulation attacks such as image filters, enhanced sharpness color (color enhancing sharp), image file compression (image compression).

ACKNOWLEDGEMENTS

Application of watermarking method technique using DCT to be applied to a various of digital document format, image, audio and video. The use of this method to be developed with a various of other methods so that the retrieved results watermarking is better again.
REFERENCES


BIBLIOGRAPHY OF AUTHORS

In 2004, Irfan have graduated a Bachelor degree from the information technology Faculty of science and technology Islam state University Jakarta, currently works as lecturer. Also student in master of computer science at Budi Luhur University, jakarta. His Research interests are Image Processing, Computer Vision and Computational techniques.

Nazori Agani receive the PhD degree in Electrical Engineering from University Technology Malaysia in 2007. Now, he stayed in Universitas Budi Luhur University as a lecturer, head of magister of Computer Science. His Research interest are Image Processing, Computer Vision and Computational techniques.