

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

Irfan *, Nazori Agani**

* Engineering Fakultas, 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.

Copyright © 2013 Information Systems International Conference.
All rights reserved.

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. Hern ndez, 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 psnr (peak signal to noise ratio) and normalized cross correlation (nc) to count its similirity 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].

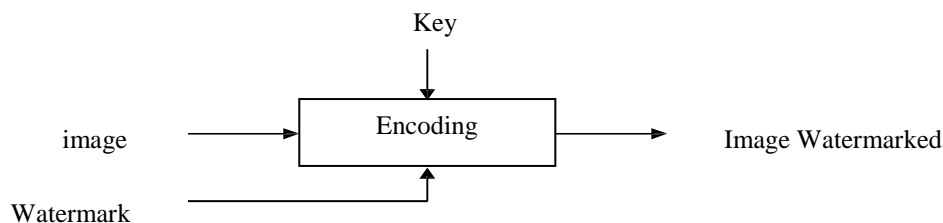


Figure 1. The process of watermark on digital image[9].

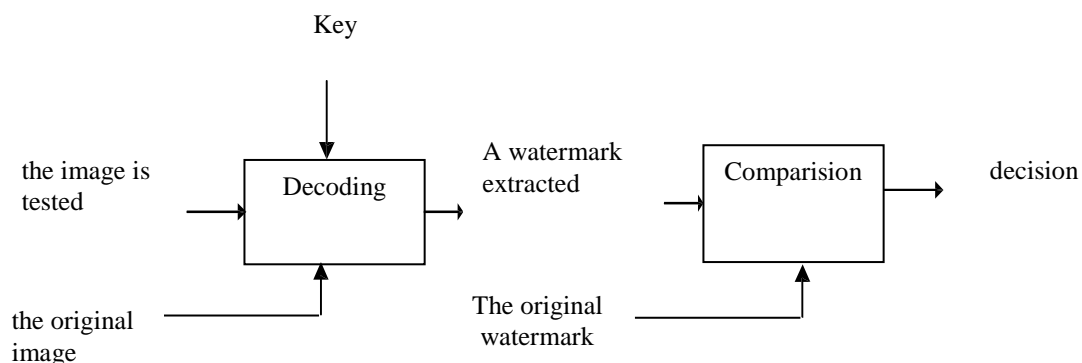


Figure 2. Process decodes watermark on digital image[9].

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]:

3. Select DCT coeficien on middle frequency (FM) through the taking dct coeficien, from coefficient L+1 to coefficient L+N. e.g all coefficient DCT which selected is store in latic V.
4. Insert watermark W into latic 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.

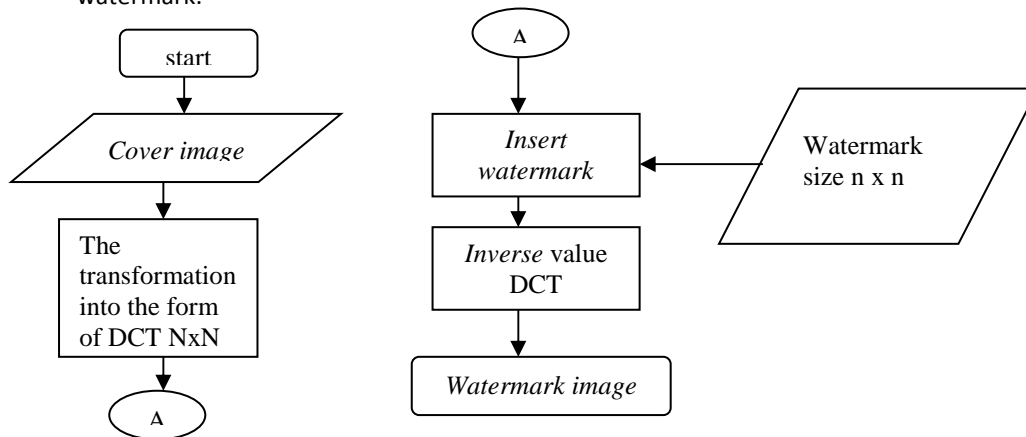


Figure 4. insert watermark to image

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

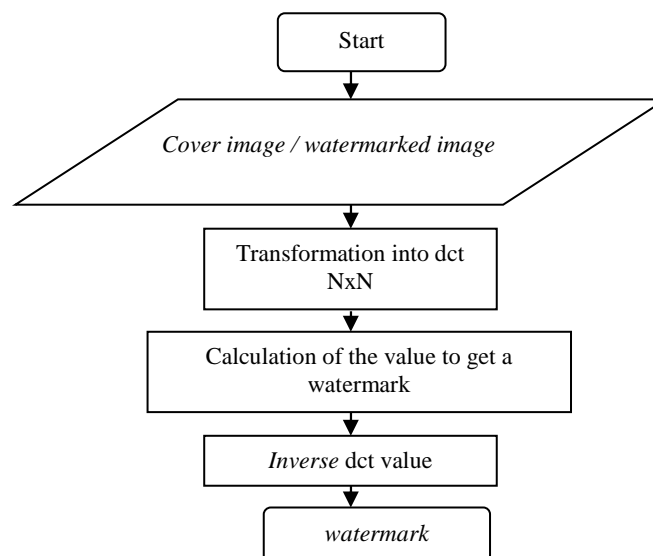


Figure 5. decode watermark

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 1. property of various image

	Properties		Measurement Technique		
	Dimension	Size	Mean	Standar Deviation	Median
Image 1.jpg	870 X 579	68.9 KB	92.3333	22.2988	100.5
Image 2.jpg	870 X 579	11.1 KB	92.4	22.1611	100.5
Image 3.bmp	128 X 128	48 KB	91.5714	23.0174	99.5
Image 4.bmp	128 X 128	48 KB	93.6875	22.8763	99.5
Image 5.png	814 X 880	490 KB	92	23.2213	99
Image 6.png	1118X1105	361 KB	92.0714	23.08	99
Image 7.tif	278 X 181	159 KB	91.8571	23.2209	99
Image 8.tif	234 X 216	159 KB	91.9286	23.08	99

And image watermark (logo) that used to insert is as follows:

Table 2.The property of the logo image watermark

	Properties		Measurement Technique		
	Dimension	Size	Mean	Standar Deviation	Median
logo1.jpg	225 X 225	6.65 KB	93.0625	23.5130	103
logo2.jpg	148 X 144	4.23 KB	93.1250	23.3891	103
Logo3.bmp	225 X 225	148 KB	92.2667	24.2678	105.5000
Logo4.bmp	225 X 225	148 KB	92.3333	24.1414	105.5000
Logo5.png	225 X 225	75.1 KB	95.2000	23.6347	82
Logo6.png	225 X 225	21.5 KB	95.2667	23.4961	82
Logo7.tif	225 X 225	161 KB	92.8000	24.6060	104
Logo8.tif	225 X 225	159 KB	92.8667	24.4799	104

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

```
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;
```

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

Table 3.The property of the image watermarked results

	Properties		Measurement Technique		
	Dimension	Size	Mean	Standar Deviation	Median
Image 1'.jpg	872X 576	103KB	96.1765	22.774	103
Image 2'.jpg	256 X 192	15.2KB	96.2353	22.6454	103
Image 3'.bmp	128 X 128	48 KB	95.625	23.551	97.5
Image 4'.bmp	128 X 128	48 KB	95.6875	23.42	97.5
Image 5'.png	816 X 880	1.72 MB	96.375	23.7539	103
Image 6'.png	1120X1104	2.73 MB	96.4375	23.6219	103
Image 7'.tif	280 X 184	152 KB	80.125	20.2151	83
Image 8'.tif	232 X 216	145 KB	80.1875	20.1137	83

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

Table 4. MSE and PSNR testing results on the image watermarked

	Testing	
	MSE	PSNR
Image 1'.jpg	3.8432	42.28387
Image 2'.jpg	3.8353	42.29281
Image 3'.bmp	4.05	42.05239
Image 4'.bmp	2.00	45.1205
Image 5'.png	4.375	41.72102
Image 6'.png	4.3661	41.72987
Image 7'.tif	11.7321	37.43705
Image 8'.tif	11.7411	37.43372
Image 1'.jpg	11.75	37.43042

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

- [1] Alfatwa, Dean fathony, "Watermarking pada citra digital menggunakan discrete wavelet transform". Institut Teknologi Bandung, 2009
- [2] Aris S., Eko A.S. "Watermarking Pada Beberapa Keluarga wavelet", Jurnal Matematika dan Ilmu Komputer Jurusan Matematika FMIPA UNDIP Semarang, **7**: 18 – 25, 2004
- [3] Supangkat, Suhono H., "Watermarking Sebagai Teknik Penyembunyian Label Kepemilikan dokumen digital Pada Citra Digital", Jurnal Teknik Elektro, Vol. 6, No. 3, 2000
- [4] Munir, Rinaldi., "Pengolahan Citra Digital Dengan Pendekatan Algoritmik", Informatika, Bandung, 2004.
- [5] Fatta, Hanif AL., "Watermarking: Penyandian Format Data Multimedia", Jurnal Ilmiah Dasi, Vol. 4, No. 4, Amikom, Yogyakarta, 2003
- [6] Saraju P. Mohanty, K.R. Ramakrishnan, Mohan S Kankanhalli, "A DCT Domain Visible Watermarking Technique for Images", ICME 2000.
- [7] Dr. Vipula Singh, Digital Watermarking – A Tutorial, "Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)", January Edition, 2011.
- [8] Juan R. Hernández, Martín Amado, and Fernando Pérez-González, "DCT-Domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", IEEE transactions on image processing, vol. 9, no. 1, January 2000.
- [9] Jafilun, "Digital Watermarking Pada Domain Spasial Menggunakan Teknik Least Significant Bit", Seminar Nasional Sistem Dan Informatika 2006; Bali, November 17, 2006.
- [10] Perwej. Y, Parwej. F, Perwej. A, "An Adaptive Watermarking Technique for the copyright of digital images and Digital Image Protection", the international journal of multimedia & its applications (IJMA) vol.4, no.2, April 2012.
- [11] Jiansheng Mei, Sukang Li dan Xiaomei Tan, "A Digital Watermarking Algorithm Based On DCT and DWT", Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), Nanchang, P. R. China, May 22-24, 2009, pp. 104-107
- [12] Munir. Rinaldi, "Image Watermarking untuk Citra Berwarna dengan Metode Berbasis Korelasi dalam Ranah DCT", Jurnal petir vol. 3 no. 1 Januari 2010
- [13] Mardiko, Rahmatri dan Basaruddin, T. "Evaluasi Skema Watermarking citra berbasis singular value decomposition, kuantisasi dither, dan deteksi sisi", Jurnal makara, sains, vol.14, no.2, November 2010 : 168-172.
- [14] Fabien AP Petitcolas, Ross J Anderson, Markus G Kuhn. "Attacks on copyright marking systems. Second Workshop on Information Hiding", Portland, USA, April 1998
- [15] YiCheng, MingSheng Zhang, "Auto-adaptive image watermark algorithm of DCT", Shanghai: Computer Engineering and Applications, 2005.

BIBLIOGRAPHY OF AUTHORS

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