Comparative study about Digital Image Watermarking Using DCT and robustness testing of technique

1) Priyanka Dashrathsinh Puvar,
Asst Professor,Computer Engineering Dept,ADIT, New V V Nagar. Priyanka.puvar@gmail.com

2) Amar D. Puvar,
Student of Master of Computer science and Engineering, Parul Institute of Engineering & Technology, Vadodara. Amarpuwar77@gmail.com

Abstract— In the today's world of rapidly growing internet services (Commercial and educational), security always comes in picture even at low level. Same way in the field of Information Technology and Computer Science and Engineering, security is always the first requirement. If we take an example of audio, video, images in which sometimes it is required to prove our ownership, to secure our data or information some means of security is always required. So, this paper illustrates ideas for making our own images to be secured from unauthorized persons, which can also be applied to videos and audios in terms. The process of making changes into images to secure it is called "IMAGE WATERMARKING". There are various ways to watermark images. The concept, considered in this paper is to hide image (watermark) behind cover image (which needs to be owned) and this concept is explained using DCT [Discrete Cosine Transform].In which both, cover image and watermark image, are converted in DCT forms. Then watermark image is embedded into cover image. Finally, IDCT [Inverse Discrete Cosine Transform] is applied on DCT formed watermarked cover image to get watermarked image in which watermark is invisible. To check the effect we can try to extract watermark from watermarked image and we can notice similarities between original watermark and extracted one. Then to check robustness of this watermarking technique we can apply some attacks on watermarked image and then we can extract watermark from it to check similarities between original watermark and extracted one using PSNR[Pick Signal to Noise Ratio]values.

Keywords:

Security, Watermarking, DCT, IDCT, Watermark, PSNR, Host image.

INTRODUCTION

An aim of Digital image Watermarking is to add some information into original image to provide security. Concept is to embed information into the cover signal in order to convey the hidden data or to prove ownership of cover image.

The development of effective digital image copyright protection methods have recently become an urgent and necessary requirement in the multimedia industry due to the ever-increasing unauthorized manipulation and reproduction of original digital objects.

New technology of digital watermarking has been advocated by many specialists as the best method to such multimedia copyright protection problem. It is expected that digital watermarking will have a wide-span of practical applications such as digital cameras, medical imaging, image databases, and video-on-demand systems, among many others. In order to be effective, digital image watermarking technique should be imperceptible and robust to common image manipulations like compression, filtering, rotation, scaling cropping, and collusion attacks among many other digital signal processing operations. Current digital image watermarking techniques can be grouped into two major classes: spatial-domain and frequency-domain watermarking techniques. From last 50 years researchers have found various methods for various types of images. And that process is in continuation. Meaning is, no method is perfect for all types of images. As per different types of images there are different methods for watermarking. One way to secure our images is to hide one image behind another one (cover image). To hide watermark, low frequency or middle band frequency areas of cover image are used. Here, Watermark and watermarking terms are defined in section 1.1. As in this paper we consider DCT [Discrete Cosine Transform] for watermarking, cover image and watermark image are

converted into DCT form. Section 1.2 of this paper explains DCT in brief. Section 1.3 of this paper covers actual process of watermarking using some steps. After we complete watermarking process, we can extract watermark from watermarked image then we can compare original watermark and extracted one to see effect on watermark [1]. Further to check robustness of watermarking technique, attack [like Scaling] is required to apply on watermarked image and then watermark is extracted from watermarked image for comparing it with original one with the help of PSNR value.

1.1 Watermark and Watermarking

Although there are different meanings for the word 'watermark' according to different authors, it is mostly agreed that the watermark is one, which is imperceptibly added to the cover-signal in order to convey the hidden data. Unlike printed

Watermarks, which are intended to be somewhat visible, digital watermarks, are designed to be completely invisible. Digital watermarking is the process of adding some information into original digital signals. This information can be in the form of either image or text.

Digital watermarking is very effective method for copyright protections. A digital image watermarking system is also same as some secured communication system. Here also there are three elements. Watermark embedded, a communication channel, and a watermark detector [2].

1.2 DCT as a step of watermarking

DCT the Discrete Cosine Transform is a technique for converting a signal into elementary frequency components. In DCT, the baseband of the discrete decomposed image has the most energy of the host image, so it has crucial effect on the image quality. The conventional algorithms don't utilize the characteristics of the DC coefficients which will participate in the watermark embedding. To reduce the drawbacks of the conventional algorithms, the proposed algorithm uses the DC coefficients in the watermark embedding step unlike the conventional algorithms [2]. It represents an image as a sum of sinusoids of varying magnitudes and frequencies. With an input image x, the DCT coefficients for the transformed output image y, are computed according to Eq. 1 shown bellow. In the equation, x is the input image having N x M pixels, x(m, n) is the intensity of the pixel in row m and column n of the image, and y(u, v) is the DCT coefficient in row u and column v of the DCT matrix.

The block-based DCT transform algorithm segments image into non-overlapping blocks and applies DCT to each block. This results in three frequency sub-bands: low frequency sub-bad, mid frequency sub-band and high frequency sub-band. DCT-based watermarking is based on two facts. The first fact is most of the signal energy lies at low-frequencies sub-band, which contains the most important visual parts of the image. The second fact is that high frequency components of the image are usually removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle frequency sub-band. Due to that the visibility of the image will not be affected and the watermark will not be removed by compression.

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\alpha_u\alpha_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n) \cos\frac{(2m+1)u\prod}{2M}\cos\frac{(2n+1)v\prod}{2N} \quad (1)$$

where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{2}} & u = 0 \\ 1 & u = 1,2,\ldots, N-1 \end{cases}$$

$$\alpha_v = \begin{cases} \frac{1}{\sqrt{2}} & v = 0 \\ 1 & v = 1,2,\ldots, N-1 \end{cases}$$

Inverse DCT: The image is reconstructed by applying inverse DCT operation according to Eq. 2:

$$x(m,n) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\alpha_u\alpha_v y(u,v) \cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \quad (2)$$

1.3 Process of watermarking using DCT:

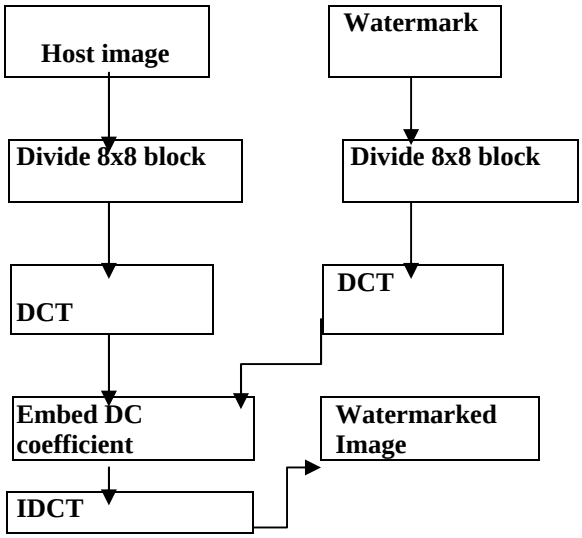

Figure 1: Block diagram of watermarking process

- Read the cover or host image [As in Fig: 1]
- Divide host image in 8x8 blocks [As in Fig: 1]
- Convert image into DCT form[As in Fig: 1]
- Read the watermark image [As in Fig: 1]
- Divide into 8x8 blocks [As in Fig: 1]
- Convert watermark into DCT form[As in Fig: 1]
- Add watermark in the mid-frequency band of cover image [As in Fig: 1]
- Apply Inverse DCT on watermarked image[As in Fig: 1]

Cover image is main image which is used to embbed watermark into it. Cover image should be larger inough to accomadate watermark into it.

Discrete cosine transform expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. In short, through DCT, the spatial domain data can be transformed into frequency domain data and the frequency domain data can be transformed back to the spatial domain data by applying Inverse DCT(IDCT).

We can show this process of watermarking by using one example of simple image of house as shown in Fig. 2

Figure 2: House image with names of objects shown in the form of watermarks [4]

Here in the uper image we can not see names of objects as they are embedded in image as watermarks. So actual watermarked image is as shown in lower part of image but watermarks are hidden so it looks loke uper part of image such that anauthorised people can not identify it.

1.4 Robustness testing

There are many methods available for watermarking. Depending on application requirements and based on its characteristics method is selected. One of its most considerable characteristics is robustness. In our case of DCT based image watermarking to check robustness we can apply various attacks like scaling, translating, rotation etc. Here we consider scaling to check robustness by taking an example of Lena as shown in fig 3 and fig 4.

Figure 3: Original Image of Lena

Figure 4: scaled image of Lena by factor of 0.5

The invariant centroid of the original image is shown in Fig 3 marked as cross on the band of hat. We can observe that after attack also it is on the similar point. If we look at first sight we can see both are same but if we observe more closely, it has slightly different gray levels between original and scaled image [5].

Now to check robustness we can rescale image and then we can compare original with rescaled one by using PSNR equation. In this way we can decide weather proposed scheme is robust or no.

1.5 Conclusion:

As we have come to know that watermarking is a way to provide security by hiding information as well as a way to prove identity and to make documents confidential, this scheme would be highly useful in real world applications.

Over here we have seen watermarking using DCT. This technique becomes easy for all users to understand and to watermark their own information. Even it is robust over attacks so this can be said simple, easy and robust way of watermarking. In addition we can also apply other attacks like rotation, translation and reflection and we can see the effect of each.

1.6 REFERENCES

[1] "Data compression" by David Salomon, 3rd Edition Springer Publication
[2] "Robust Image Watermarking Method Using Discrete Cosine Decomposition and just Noticeable Distortion, The 23rd International Technical Conference On Circuits/system" computers and communications (ITC-cscc 2008).
[3] Automatic Detection of the Presence of Stego-signals and Watermarks in Images Department of Computer and Information science, Polytechnic University, Brooklyn, NY, USA
[4] Interactive Image using illustration Watermarks: Techniques, Studies and Applications, Henry sonnet, Guericke University, Germany.
[5] Robust digital image watermarking method against geo-
[6] Metrical attacks, Received 17 April 2002; received in revised form 19 February 2003; accepted 28 February 2003