SURVEY OF DIGITAL WATERMARKING USING DCT

Usha Pal
Department of EC
JSSATEN College NOIDA, MTU
NOIDA, U.P. (INDIA)
Pal.usha@yahoo.co.in

Dinesh Chandra
Hod of EC Department
JSSATEN College NOIDA, MTU
NOIDA, U.P. (INDIA)
dineshchandra@jssaten.ac.in

Abstract

Digital Watermarking is not a new name in the technology world but there are many new issues arise related with watermark. This paper surveys recent advances in watermarking techniques in digital images. The aim of digital watermarking is hidden information added into content of multimedia. In this paper, DCT technique is used and when size of image is increase then also increases PSNR without decreasing power of embedded factor[1] (alpha factor) in same format.

Keywords**:** Discrete Cosine Transform (DCT), Peak Signal to Noise Ratio (PSNR).

1. INTRODUCTION

Digital Watermarking represents an effective method for authentication and ownership right protections.It involves embedding watermark data into original information .Watermark information cannot be stored in file header because anyone with a computer and a digital editing workstation would be able to convert the information to another format and remove the watermark. Thus the watermark always embedded to multimedia signals. There are a lot of processes performed by unauthorized persons who aim to damage or corrupt the embedded information. These processes are called Attacks.

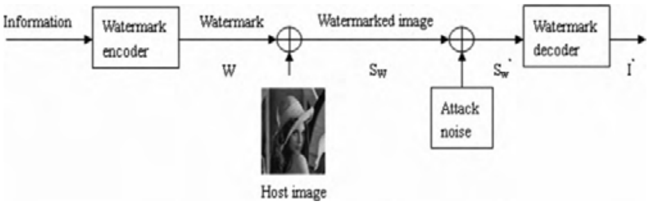

Fig.1. Watermark Model

Watermark is a design of watermark signal W to be added into a host image. The watermark signal, apart from depending upon watermark image Sw, may also depend upon key K and the host image I into which it is embedded [5].

$$W = f0(I, K, Sw)$$

2. ATTACKS

Different types of attacks are:

2.1. *Removal Attacks*

Removal attacks attempt to analyze or estimate the watermark, separate it out and discard only the watermark. Examples are lossy compression, averaging, denoising, collusion attack.

2.2. *Detection –disabling Attacks*

Detection-disabling attempt to break correlation and to make detection of watermark impossible. They make some geometric distortion like zooming, shift in spatial or temporal direction, rotation, cropping, removal or insertion.

2.3. *Simple Attacks*

Simple attacks attempt to damage the embedded watermark by modifications of whole image without any effort to identify and isolate the watermark. Examples are frequency based compression, addition of noise, cropping, correction.

2.4. *Cryptographic Attacks*

Cryptographic attacks are cracking the security methods in watermarking schemes and finding a way to remove the embedded watermark information. These attacks are also called brute force attacks which aim at finding secret information through an exhaustive search.

3. WATERMARK TECHNIQUES

Watermark techniques are mainly classified into spatial or frequency domain. Spatial domain watermarking is performed by modifying value of pixel color samples of frame whereas frequency domain watermarking are applied to coefficients obtained as the result of frequency transform of either a whole frame or single block- shaped region of frame. Discrete Fourier Transform and Discrete Wavelet Transform belong among whole-frame frequency transform. The representative of the block frequency transform is Discrete Cosine Transform.

3.1. Discrete Cosine Transform

Discrete cosine transform is basically obtained from real part (it carries the cosine term) of the discrete fourier transform. It transforms the time domain or space domain of real input into its elementary frequency components. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into middle frequency bands of an image. The middle frequencies are chosen such that they have minimized they avoid the most visual important parts of image (low frequencies) without over exposing themselves to removal through compression and noise attack (high frequencies)[5].

The important properties of watermark are robustness and imperceptibility in transform domain.

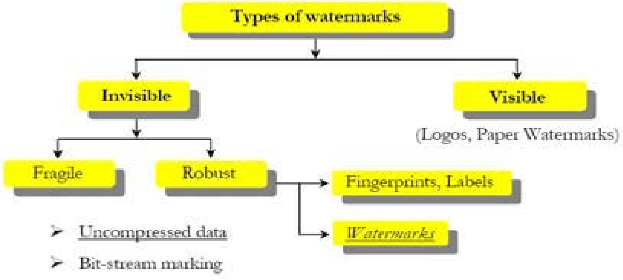

Fig.2. Types of Watermarking [6]

Additionally, classification can be based on robustness feature. Different techniques of this category are:

3.1.1. Robust Watermark

Robust watermarking aims to embed information into a file which cannot be easily destroyed. The watermarking algorithm is called robust if it can survive after common signal processing and lossy compression.

3.1.2. Fragile Watermark

Fragile watermarking involves embedding information into a file which is destroyed if the file is modified. This method is suitable for verification or authenticity of original content.

3.1.3. Semi-fragile Watermark

Semi-fragile watermark are robust to incidental modification such as jpeg compression, but fragile to other modification. It is sensitive to some degree of the change to a watermarked image.

4. Experimental Results

In experiments [8,9], firstly 256×256 and 537×358 standard test images are used, cameraman.tif, moon.tif. According to DCT technique, we can calculate PSNR [7], MSE at different values of alpha.

In Table1,

1) In Cameraman image(256×256),

   when

   Alpha = 0.01

   then

PSNR = 34.78

2) In Moon image(537×358),

when

Alpha = 0.01

then

PSNR = 40.54

We take different values of alpha examples, 0.01, 0.1, 0.2, 0.5, 1, and 2. So, we concluded that when increase the size of image at same value of alpha, PSNR value of large image is better than smaller image. So, PSNR value is increase means image quality increase without decreasing alpha factor [1].

Table 1. Cameraman and Moon Image with different values of alpha and PSNR

Cameraman Image (size=256×256)	**Moon Image (537×358)**
1) $\alpha = 0.01$, PSNR = 34.78	1) $\alpha = 0.01$, PSNR = 40.54
2) $\alpha = 0.1$, PSNR = 14.78	2) $\alpha = 0.1$, PSNR = 20.54
3) $\alpha = 0.2$, PSNR = 8.76	3) $\alpha = 0.2$, PSNR = 14.52
4) $\alpha = 0.5$, PSNR = 0.80	4) $\alpha = 0.5$, PSNR = 6.5
5) $\alpha = 1$, PSNR = –5.2	5) $\alpha = 1$, PSNR = 0.54
6) $\alpha = 2$, PSNR = –11.2	6) $\alpha = 2$, PSNR = –5.47

5. Conclusion

In Watermarking scheme, image is considered as a communication channel to transmit messages. Experimental results shown that image quality depends upon size of image and alpha factor. In this paper, we discuss the size of image and increases image quality without decreasing alpha factor (power of embedded factor).

6. References

[1] RIDZOŇ, R.; LEVICKÝ, D.: Usage of different color models in robust digital watermarking, 978-1-4244-3538-8/09/$25.00 ©2009 IEEE.

[2] RIDZOŇ, R.; LEVICKÝ, D.: Robust digital watermarking based on the log-polar mapping. In: *Radioengineering*. vol. 16, no. 4 (2007), p. 76-81.

[3] R.Gonzalez and R.Woods, “Digital Image Processing”, 1998.

[4] Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2Nd Ed. ISBN: 978-0123725851.

[5] Avani Bhatia, Mrs. Raj Kumari U.I.E.T, Panjab University: “Digital Watermarking Techniques”.

[6] Chunlin Song, Sud Sudirman, Madjid Merabti ,School of Computing and Mathematical Sciences Liverpool John Moores University,UK : “Recent Advances and Classification of Watermarking Techniques in Digital Images”, ISBN: 978-1-902560-22-9 © 2009PGNet.

[7] Wen Yuan Chen and Shih Yuan Huang ,Department of Electronic Engineering National Chin-Yi Institute of Technology: “Digital Watermarking Using DCT Transformation”.

[8] Www.advancesourcecode.com

[9] Www.codeforge.com/libs/highlight/stles/sunburst.css