A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques

Dhruv Arya

Abstract— Due to improvement in imaging technology and the ease with which digital content can be reproduced and manipulated there is a strong need for a digital copyright mechanism to be put in place. There is a need for authentication of the content as well as the owner. It has become easier for malicious parties to make scalable copies of copyrighted content with any compensation to the content owner. Digital Watermarking is being seen as a potential solution to this problem. Till date many different watermarking schemes have been proposed. This paper presents a comprehensive survey of the current techniques that have been developed and their effectiveness.

Index Terms— Image Retrieval, Transforms, Watermarking

1 INTRODUCTION

The field of digital watermarking is rather new; indeed, at this point many of its terms are not well defined. We define *watermarking* to be a process that embeds data, called *a watermark* into a multimedia object to help protect the owner's rights to that object.

A digitally watermarked image is obtained by invisibly hiding asignature information into the host image. The signature is recovered using an appropriate decoding process. The challenge is to ensure that the watermarked image is perceptually indistinguishable from the original and that the signature be recoverable even when the watermarked image has been compressed or transformed by standard image processing operations.

This paper describes a various digital watermark algorithms studying their strengths and weaknesses. Considering texture, luminance, corner and the edge information in the image to generate a mask that makes the addition of the watermark less perceptible to the human eye. The operation of embedding and extraction of the watermark is done in both the spatial and the frequency domain thereby providing us information about the robustness against common attacks including image compression and filtering. We use pseudo random sequences in embed the watermark. Weighted Peak Signal to Noise Ratio is used to evaluate the perceptual change between the original and the watermarked image.

2 FOUNDATION OF DIGITAL WATERMARKING

It should be noted that he reason why digital watermarking is possible is that human vision system (HVS) is not perfect. Digital watermark utilizes the limitation of HVS to make itself invisible, thus avoiding to degrade original digital products, as well being hard to get identified or destroyed.

3 REQUIREMENTS FOR DIGITAL WATERMARKING

In order to be an effective watermarking system it should possess the following characterstics –
Unobtrusive, an ideal watermark is perceptually invisible
Robust, the watermark should be resistant to distortion introduced during either normal use (unintentional attack), or a deliberate attempt to disable or remove the watermark present (intentional, or malicious attack). Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing and contrast enhancement.
Secure and High Capacity, retrieval of the watermark should unambiguously identify the owner. Furthermore, the accuracy of owner identification should degrade gracefully in the face of attack.

4 CLASSIFICATION OF WATERMARKING TECHNIQUES

4.1 By Domain of Watermarking

Spatial-domain watermarking technologies change the intensity of original image or gray levels of its pixels. This kind of watermarking is simple and with low computing complexity, because no frequency transform is needed. However, there must be tradeoffs between invisibility and robustness, and it is hard to resist common image processing and noise. Frequency-domain watermarking embeds the watermark into the transformed image. It is complicated but has the merits which the former approach lacks.

4.2 By Ability of watermark to resist attack

Fragile watermarks are ready to be destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image completeness. Robust watermarks are robust under most image processing methods and can be extracted from heavily attacked watermarked image. Thus it is preferred in copyright protection.

5 Process of Watermarking

The process of watermarking in the simplest form involves two steps – Watermark Embedding and Watermark Extraction.

Consider the function f() that denotes the embedding function and I, the original image. W, denotes the watermark to embed and I', denotes the watermarked image.

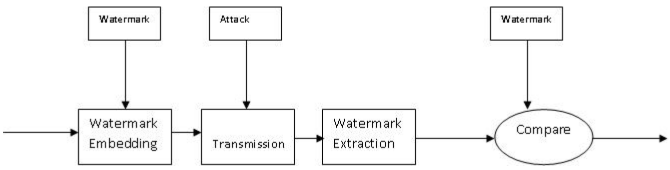

Fig. 1. Process of Watermarking

I' = f(I,W)

Common approach is as follows:
Select a group of coefficients from the original image

J = j1, j2… jn

Corresponding watermark sequence is

X = x1, x2… xn

Embed X into J according to certain model to obtain the adjusted sequence

J' = J + X = j'1, j'2…j'n.

Put j' back and take the place of J, then we get the watermarked image I'. Let e() denote the extraction function and I' the image to be examined. Extract the watermark from I'. If the correlation function C(W, W') satisfies

CWWT>= (T is the threshold value)

Then we consider there is a watermark W in I'.

Signal-to-noise ratio (SNR) is a common metric in signal processing industry. Suppose the original image is I(m,n) the output image is I'(m,n) then generally SNR is defined as:

$$SNR = 10\log_{10}[\sum_m \sum_n I(i,j)^2 / \sum_m \sum_n (I(i,j) - D(i,j))^2]$$

When SNR approaches infinity, the original image and output image are totally the same.

Another similar one is Peak SNR (PSNR). For images with 255 gray levels, the PSNR is defined as:

$$PSNR = 10\log_{10}[\sum_m \sum_n 255^2 / \sum_m \sum_n (I(i,j) - D(i,j))^2]$$

6 Watermarking Technologies

Compared to spatial-domain watermark, watermark in frequency and wavelet domain is more robust and compatible to popular image compression standards. Thus frequency and wavelet domain watermarking obtains much more attention. To embed a watermark, a frequency or wavelet transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT). Similarly in the wavelet domain we use the Discrete Wavelet Transform (DWT).

6.1 DCT Domain Watermarking Technique

The first efficient watermarking scheme was introduced by Koch et al. In their method, the image is first divided into square blocks of size 8x8 for DCT computation. A pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. Bors and Pitas developed a method that modifies DCT coefficients satisfying a block site selection constraint. After dividing the image into blocks of size 8x8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson. Cox developed the first frequency-domain watermarking scheme. After that a lot of watermarking algorithms in frequency domain have been proposed.

Most frequency-domain algorithms make use of the spread spectrum communication technique. By using a bandwidth larger than required to transmit the signal, we can keep the SNR at each frequency band small enough, even the total power transmitted is very large. When information on several bands is lost, the transmitted signal can still being recovered by the rest ones. The spread

ISSN 2229-5518

spectrum watermarking schemes are the use of spread spectrum communication in digital watermarking. Similar to that in communication, spread spectrum watermarking schemes embed watermarks in the whole host image. The watermark is distributed among the whole frequency band. To de-stroy the watermark, one has to add noise with sufficiently large amplitude, which will heavily degrade the quality of watermarked image and be considered as an unsuccessful attack.

One major reason why frequency domain wa-termarking schemes are attractive is their compatibility with existing image compression standards, in par-ticular, the JPEG standard. The compatibility ensures those schemes a good performance when the watermarked image is subject to lossy compression, which is one of the most common image processing methods today. In consequence, those schemes become particularly useful in practical applications on the Internet.

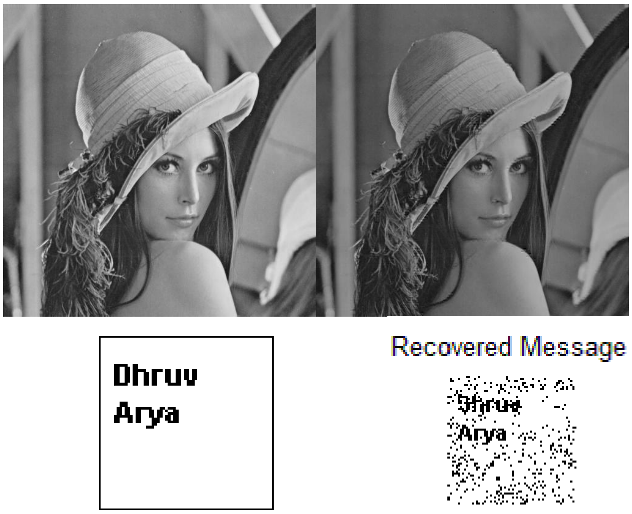

Fig.1 . DCT Domain Watermarking Technique using Mid Band Coefficient Exchange with PSNR = 2.53. Going from Top Left to Right A. Original Image B.Watermarked Image C. Watermark D. Extracted Watermark

A widely accepted point now is the frequency-domain watermark should be embedded into the mid-band of the transformed host image. Watermarks in high frequency band tend to have less influence on the quality of original image, while watermarks in low band will achieve a better robustness (since a large portion of high frequency components may be quantized to zero under JPEG compression, as shown in figure 4). And the mid-bind scheme is right a tradeoff between the imperceptibility and robustness..

6.2 Wavelet Domain Watermarking Technique

The JPEG2000 standard had adopted a new technique, the wavelet transform. Although this standard has not been widely used yet, any new watermarking algorithm that intends to endure in the future should get along with it. The difference between different wavelet domain methods depends on the way the watermark is weighted. The reason for this is to reduce the presence of visual artifacts.

The DWT (Discrete Wavelet Transform) separates an image into four components, a lower resolution approximation image (LL) a horizontal (HL), a vertical (LH) and a diagonal (HH) detail component. The process can then be repeated to computes multiple “scale” wavelet decompositions.

One of the many advantages of the wavelet transform is that that it is believed to more accurately model aspects of the HVS (Human Visual System) as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH,HL,HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality. One of the most straightforward techniques is to use a similar embedding technique to that used in the DCT, the embedding of a CDMA sequence in the detail bands according to the equation

$$I_{W_{u,v}} = W_i + \alpha |W_i| x_i, u, v \in HL, LH$$
$$I_{W_{u,v}} = W_i, u, v \in LL, HH$$

Fig. 2. Wavelet Domain Watermarking Technique – Going from Top Left to Right A. Original Image B. Watermarked Image C. Extracted Watermark D. Watermark

ISSN 2229-5518

Where *Wi* denotes the coefficient of the transformed image, *xi* the bit of the watermark to be embedded, and a scaling factor. To detect the watermark we generate the same pseudo-random sequence used in CDMA generation and determine its correlation with the two transformed detail bands. If the correlation exceeds some threshold T, the watermark is detected. This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. During detection, if the correlation exceeds T for a particular sequence a "1" is recovered; otherwise a zero. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered (as shown in the results in Fig 2). Also as the embedding uses the values of the transformed value in embedded, the embedding process should be rather adaptive; storing the majority of the watermark in the larger coefficients.

7 Conclusion

In this paper, I have introduced some basic concepts in digital watermarking, including its foundation, properties, requirements as well as the comparison between digital watermark techniques.Schemes in frequency domain and wavelet domain are introduced with analysis of pros and cons, in terms of imperceptibility, robustness, implementation complexity etc., for each domain.

The last part of this paper presents some experimental results, taking the typical frequency-domain and wavelet domain algorithms. The watermark is embedded into the regions of low interest of host image to achieve a good tradeoff between the imperceptibility and robustness of the watermarking system. The results show that these algorithms have a satisfactory performance under image cropping and JPEG lossy compression.

Acknowledgment

I would like to thank Prof. Akash Tayal of Indira Gandhi Institute of Technology, New Delhi and Nivedita Yadav Research student at IIT Delhi for their guidance, support and motivation without which the paper could not have been completed

References

[1] J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673-1687, Dec. 1997

[2] A. Bors and I. Pitas, "Image watermarking using DCT domain constraints." in *Proc. IEEE. Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, pp. 231-234

[3] R.C. Gonzalez, R.E. Woods, "Digital Image Processing", Upper Saddle River, New Jersey, Prentice Hall, Inc., 2002

[4] Perez-Gonzalez, F.; Hernandez, J.R.;" A tutorial on digital watermarking" *Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on*. Oct. 1999 Page(s):286 – 292

[5] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom "Digital Watermarking" Morgan Kaufmann Publishers ISBN: 1-55860-714-5