A Novel Approach on DWT Province for Colorant Watermarking

K. Suresh Kumar
Assistant Professor, Department of ECE,
Dadi Institute of Engineering & Technology,
Anakapalle, India

Abstract—This article aims at lightweight, visionless recognition of additive spread-spectrum watermarks in the DWT domain. We focus on two host signal clatter models and two types of postulate tests for watermark recognition. As a crucial point of our work we take a closer look at the computational necessities of watermark sensors. This involves the computation of the uncovering response, stricture estimate and porch selection. We show that by switching to estimated host signal parameter approximations or even stable parameter settings we attain an astonishing enlargement in runtime performance without surrendering recognition enactment. Our tentative results on a large number of images confirm the assumption that there is not necessarily a trade-off between calculation time and exposure concert.

Keywords- DWT, Images, Exposure, Watermarking, Spread spectrum, Threshold.

I. INTRODUCTION

A watermark is a pattern of bits inserted into a digital image, audio or video file that identifies the file's copyright information (author, rights, etc.). The name “watermark” is derived from the faintly visible marks imprinted on organisational stationery.

Unlike printed watermarks, which are intended to be somewhat visible (like the very light compass stamp watermarking this report), digital watermarks are designed to be completely invisible, or in the case of audio clips, inaudible. In addition, the bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated. And finally, a digital watermark must be robust enough to survive changes to the file its embedded in, such as being saved using a lossy compression algorithm eg: JPEG. Satisfying all these requirements is no easy feat, but there are a number of companies offering competing technologies. All of them work by making the watermark appear as noise - that is, random data that exists in most digital files anyway.

Digital Watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made whether legally or otherwise, regardless of attempts to damage/ remove it.

Digital watermarking is the process of embedding information into a digital signal which may be used to verify its authenticity or the identity of its owners, in the same manner as paper bearing a watermark for visible identification. In digital watermarking, the signal may be audio, pictures, or video. If the signal is copied, then the information also is carried in the copy. A signal may carry several different watermarks at the same time.

In visible digital watermarking, the information is visible in the picture or video. Typically, the information is text or a logo, which identifies the owner of the media. The image on the right has a visible watermark. When a television broadcaster adds its logo to the corner of transmitted video, this also is a visible watermark. In invisible digital watermarking, information is added as digital data to audio, picture, or video, but it cannot be perceived as such (although it may be possible to detect that some amount of information is hidden in the signal). The watermark may be intended for widespread use and thus, is made easy to retrieve or, it may be a form of steganography, where a party communicates a secret message embedded in the digital signal. In either case, as in visible watermarking, the objective is to attach ownership or other descriptive information to the signal in a way that is difficult to remove. It also is possible to use hidden embedded information as a means of covert communication between individuals.

One application of watermarking is in copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. In this use, a copy device retrieves the watermark from the signal before making a copy; the device makes a decision whether to copy or not, depending on the contents of the watermark. Another application is in source tracing. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

Annotation of digital photographs with descriptive information is another application of invisible watermarking.
While some file formats for digital media may contain additional information called metadata, digital watermarking is distinctive in that the data is carried right in the signal.

II. DIGITAL WATERMARKING LIFE-CYCLE PHASES

General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions.

![Digital Watermarking life cycle phases](Image)

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the host signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where pirates attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

III. WATERMARKING USING DCT/DWT

Compared to spatial-domain watermark, watermark in frequency domain is more robust and compatible to popular image compression standards. Thus frequency-domain watermarking obtains much more attention. To embed a watermark, a frequency 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) and others.

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 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 destroy 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.

Figure 2 and Figure 3 illustrate the watermark embedding and detection /extraction in frequency domain, respectively.
The new JPEG2000 standard has adopted a new technique, the wavelet transform. Though this standard has not been widely used yet, any new watermarking algorithm that intends to survive in the future should get along with it. Here come the watermarking schemes based on wavelet transform. 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 artefacts. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple “scale” wavelet decomposition, as in the 2 scale wavelet transform shown below in figure 4.

![Wavelet Transform Diagram](image)

**Figure 4.** Scale 2-Dimensional Discrete Wavelet Transform

GGD parameters estimation has been extensively covered in literature, we only provide a brief overview of the main results. Maximum Likelihood estimation is studied in the work of Varanasi et al. [7] including both, joint parameter estimation, and situations where one parameter is already known. Do and Vetterli provide a Newton–Raphson algorithm to find the root of the resulting transcendental equation in [8] which involves computation of the Digamma and Trigamma function. We refer to their algorithm for any computational discussion. The starting value for the Newton–Raphson iteration is usually obtained using the moment estimate of , presented by Birney et al. [5] and Mallat [1].

![GGD Parameter Estimation Diagram](image)

**Figure 5.** Illustration of Gaussian and Chi-square detection Response statistics

In this article, we have taken a closer look at four state-of-the-art detectors in the field of additive spread-spectrum watermarking in the DWT domain. We reviewed the a priori requirements and assumptions which are taken as a basis for the derivation of each detector. We then discussed parameter estimation issues in a maximum-likelihood framework as well as some approximate solutions. Our first experimental results showed that neither ML estimation nor the approximations lead to the optimal detection performance over a set of test images. More extensive experiments on a large number of images revealed that it is actually possible to find fixed parameter settings for each host-signal noise model which allow competitive or even better detection performance than the approaches using estimates. This is in accordance with the idea of lightweight detection since the parameter estimation process

![Probability of Miss Comparison](image)

**Figure 6.** Probability of miss comparison of the LRT-GG and Rao-GG detector.

IV. CONCLUSION

In this article, we have taken a closer look at four state-of-the-art detectors in the field of additive spread-spectrum watermarking in the DWT domain. We reviewed the a priori requirements and assumptions which are taken as a basis for the derivation of each detector. We then discussed parameter estimation issues in a maximum-likelihood framework as well as some approximate solutions. Our first experimental results showed that neither ML estimation nor the approximations lead to the optimal detection performance over a set of test images. More extensive experiments on a large number of images revealed that it is actually possible to find fixed parameter settings for each host-signal noise model which allow competitive or even better detection performance than the approaches using estimates. This is in accordance with the idea of lightweight detection since the parameter estimation process
poses a computational bottleneck. Regarding the computational effort to compute the detection statistics itself as well as detection thresholds, we favour the Rao-C detector due to a small number of arithmetic operations and one-time threshold determination.

REFERENCES