Digital Image Watermarking Based on Wavelet Techniques: A Review

Sanjeet Kumar
M. Tech. (CSE)
DCRUST, Murthal, India

Sanjeev Indora
Assistant Professor (CSE)
DCRUST, Murthal, India

ABSTRACT
Digital watermarking is a technique for embedding information in to cover media to prove ownership. It became very important in the number of application areas such as copyright protection, fingerprinting, broadcast monitoring, and medical application. During the last several years, various watermarking techniques have been proposed by different authors. Wavelet based watermarking is gaining more and more popularity because of its resemblance to the human visual system. In this paper, we aim to elaborate wavelet based watermarking techniques, to compare different wavelet used for wavelet based watermarking techniques, to compare different wavelet used for wavelet based watermarking and to provide in-depth review of existing work done on wavelet based watermarking techniques.

Keywords
Digital Image Watermarking, DWT, SVD, Imperceptibility, Robustness.

1. INTRODUCTION
In recent years, there has been tremendous growth in computer networks and use of multimedia technologies. It leads to the easier accessing, copying and malicious attacks of multimedia data ubiquitous [1]. Multimedia authentication and copyright protection became a problem that needs to be solved urgently. Digital watermarking has been proposed as a solution of content authentication and copyright protection [2]. Digital watermark is perceptible or imperceptible identification code that is embedded inside an image. Watermark acts as a digital signature, which uniquely identifies ownership of image [3]. Two important characteristics of watermarking algorithm are imperceptibility and the robustness. Imperceptibility refers as the difference between the watermarked image and the original image, where as robustness means the unauthorized individuals or groups can't eliminate the watermark from the embedded data [2]. The two popular approaches for watermarking are spatial domain methods and transform domain methods. In the spatial domain watermark is embedded directly to the pixel locations chosen based on the texture of the given image. While in transfer domain, the watermark is embedded into the transform coefficients using methods such as the DWT, the DCT and the DFT. Due to the multi-resolution characteristics and good robustness to common image processing such as compression, noise, filtering, cutting and rotation, etc, DWT has been used more frequently in digital image watermarking [4].

1.1 Applications of Digital Image Watermarking

1.1.1 Copyright protection
Copyright information can be inserted as a watermark, when a new work is produced. This watermark can provide evidence in case of dispute of ownership [5].

1.1.2 Broadcast monitoring
we can use watermark for broadcast monitoring by putting a watermark in each video clip or sound clip prior to broadcast. Automated monitoring stations, then receive broadcasts and look for these watermarks and identifying when each clip prior to broadcast [1].

1.1.3 Tamper detection
For tamper detection fragile watermarks are used. If the watermark is degraded or destroyed, it indicates the existence of tampering and hence digital content can't be trusted [5].

1.1.4 Content authentication
Content authentication is able to detect any change in the digital content. This can be achieved by using fragile or semi-fragile watermarks as a digital signature, which has low robustness to modification of an image [13].

1.1.5 Fingerprinting
Fingerprinting involves embedding a different watermark in each distributed digital data and allows the owner to locate and monitor pirated data that are illegally obtained. It is a process of associating unique information about each
distributed copy of digital content. It is easily implemented using watermarking because it’s invisible and inseparable from the content [6].

1.1.6 Medical applications
The medical reports play a significant role in the treatment offered to the patient.
If there is a mix up in the medical reports of two patients, this could lead to a disaster. To handle this problem patient’s name can be printed on the x-ray reports and MRI scan reports using techniques of visible watermarking [7].

2. DESIRED CHARACTERISTICS OF DIGITAL WATERMARKING
The desired characteristics of digital watermarking are as follows[8],[9],[10].

2.1 Imperceptibility
Imperceptibility is a measure that determines the similarity level between the original and watermarked image. Sometimes the perceptual similarity of the system can be sacrificed for better performance with respect to other characteristics like robustness or low cost.

For Watermark imperceptibility analysis Different literatures have reported different metrics. Following metrics provides quantitative measurements of imperceptibility. The notations used are listed below.

$X(i,j) :$ Original image $\text{Y}(i,j) :$ Watermarked image, and $\text{Si} :$ Size of image

2.1.1. Mean square error (MSE)
The mean square error between original image and watermarked image is computed by averaging the squared intensity of the original (input) image and the resultant (output) image pixels as in (1).

$$MSE = \frac{1}{\text{Si}} \sum_{i,j} (X(i,j) - Y(i,j))^2$$  

2.1.2. Peak signal to noise ratio (PSNR) :-
The PSNR is a mathematical measure of image quality, which is calculated between the original image and watermarked image. Larger the value of PSNR, the more similar is a watermarked image to the original image. PSNR is defined as in (2).

$$PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right)$$  

If the PSNR value is greater than 30db then perceptual quality is acceptable.

2.1.3. Image Fidelity (IF)
Image fidelity is a measure of transparency or imperceptibility of watermarked image. Image fidelity is defined as in (3).

$$IF = 1 - \frac{\sum_{i,j} (X(i,j) - Y(i,j))^2}{\sum_{i,j} (X(i,j))^2}$$  

2.2 Robustness
Watermarks should be robust against common image processing operations like compression, filtering, geometric distortion etc. Robustness is application dependent, it is not necessary that all applications requires robustness against all the operations. for example, the robustness is required only against the communication related manipulations in broadcast monitoring.

For Watermark robustness analysis following metrics are used in case of logo or binary sequenced watermarked as a quantitative measure. Readability and reliability of extracted watermark is indicated by these metrics. The notations used are listed below.

$W(i,j) :$ Original watermark  $W'(i,j) :$ Extracted watermark

2.2.1. Correlation coefficient (CRC)
To analyze compatibility of original watermark and extracted watermark this metric is used. The value range from 0 to 1. CRC is defined as in (4).

$$CRC = \frac{\sum_i \sum_j W(i,j) \text{W}'(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \sqrt{\sum_i \sum_j W'(i,j)^2}}$$  

2.2.2. Similarity measure (SIM)
A similarity measure is used for objective judgement of the extraction fidelity between extracted watermark and embedded watermark.

$$SIM(W,W') = \frac{\sum_i \sum_j W(i,j) \text{W}'(i,j)}{\sum_i \sum_j W(i,j)^2}$$  

2.2.3. Bit error rate (BER)
The probability of incorrectly decoded binary patterns is indicated by BER. BER is defined as in (6).

$$BER = \frac{DB}{NB}$$  

where,
$DB :$ No. of incorrectly decoded bits.
$NB :$ total no. of bits.

2.2.4. Accuracy Ratio :-
Similarity between the original watermark and extracted watermark is evaluated using accuracy
ratio. It is defined as ratio of number of correct bits between original watermark and extracted watermark and number of original watermark bits. AR is defined as in (7).

\[ AR = \frac{CB}{NB} \]  \hspace{1cm} (7)

CB : No. of correct bits. NB : Total no. of bits.

AR value closer to 1 indicates more similarity between extracted and original watermark.

2.3 Data embedding capacity

Data embedding capacity is the maximum amount of information that can be hidden without degrading image quality. How much data should be embedded as a watermark, so that it can be successfully detected during extraction is describe by data payload. For n bits watermark the system can encode any of \(2^n\) different messages. The fidelity of the system is affected when the watermark payload is increased.

2.4 Security

The secret key used for embedding and detection process in case security is a major concern. There are three types of keys used in watermark systems : private key, detection key and public key.

2.5 Computational complexity

Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. To ensure security and validity of watermark, more computational complexity is needed. Conversely, real time applications necessitate both speed and efficiency.

3. DISCRETE WAVELET TRANSFORM

The DWT decomposes input images into four components namely LL, HL, LH and HH as in fig. 1. Where the first letter corresponds to applying either a low pass frequency operation or high frequency operation to the rows and second letter refers to the filter applied to the column[11]. The lowest resolution level LL consists of the approximation part of the original image. The remaining consists of detail part and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies[12].

The image's energy is mainly focused on the low frequency. The other three level characterize the marginal information of the corresponding direction and have little energy[12]. DWT transform is based on small waves, called wavelets of varying frequency and limited duration. Wavelet transform provide both frequency and spatial description of an image [13].

3.1 Advantages of DWT

Merits of DWT transform are as follows.

1. HVS can be accurately model using wavelet transform than other transforms like DFT[14] or Discrete cosine transform (DCT)[15],[16].This allows higher energy watermarks in the regions where HVS is less sensitive.

2. Wavelet coded image is a multi-resolution description of image. Hence an image can be shown at different levels of resolution and can be sequentially processed from low resolution to high resolution. The advantage of such approach is that the features of an image that might go undetected at one resolution may be easy to spot at another.

3. Visual artefacts introduced by wavelet coded images are less evident compared to DCT because wavelet transform doesn't decompose image into blocks for processing.

4. DWT has spatial frequency locality. It means it will affect the image locally, if watermark is embedded.

3.2 Embedding watermark

The original image will be decomposed into n different levels for embedding watermark. In DWT coefficients the watermark is embedded. The assumption is that any changes in wavelet coefficients and embedded watermark are result of modification to image. Inverse DWT is taken to get watermarked image [13]. Embedding watermark is shown in fig. 2.

![Figure 2. Watermark Embedding using DWT](image)

3.3 Extraction and detection of watermark

Extraction of watermark from watermarked image may be blind or non-blind depending on requirement of original image for extraction. It
involves comparison of both the image or comparison with the threshold. The correlation between the extracted watermark and the embedded watermark signal is then calculated [13]. Detection process allows the owner to be identified and provides information to the intended recipient depending on threshold value. Watermark detection at lower resolution is computationally effective because at each successive resolution level smaller frequency bands are involved [13].

![Watermark Detection Diagram](image)

Figure 3. Extraction and Detection of Watermark.

### 3.4 Comparison of Different Wavelets

<table>
<thead>
<tr>
<th>Wavelets</th>
<th>Image</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haar</td>
<td>Peppers.jpg</td>
<td>0.9383</td>
<td>46.8272</td>
</tr>
<tr>
<td>Daubechies</td>
<td>Peppers.jpg</td>
<td>0.9835</td>
<td>46.6997</td>
</tr>
<tr>
<td>Cofiflets</td>
<td>Peppers.jpg</td>
<td>0.9727</td>
<td>46.6563</td>
</tr>
<tr>
<td>Symlets</td>
<td>Peppers.jpg</td>
<td>0.9901</td>
<td>47.6073</td>
</tr>
<tr>
<td>Discrete Mayer</td>
<td>Peppers.jpg</td>
<td>0.9911</td>
<td>47.5666</td>
</tr>
<tr>
<td>Biorhogonal</td>
<td>Peppers.jpg</td>
<td>0.9779</td>
<td>47.6290</td>
</tr>
<tr>
<td>Reverse Biorhogonal</td>
<td>Peppers.jpg</td>
<td>0.9927</td>
<td>47.5672</td>
</tr>
</tbody>
</table>

### 4. REVIEW OF WAVELET BASED IMAGE WATERMARKING

Review of image watermarking based on DWT is presented below.

Chunl in Song et al. [17] have proposed a novel watermarking technique using a combination of DWT and SVD techniques. They used different regions of the host image to embed watermark data. To facilitate this, the technique utilizes dual watermarking technologies and embeds part of watermark into selected regions in the host image. Li et al. [18] proposed a hybrid DWT-SVD domain watermarking technique considering human visual system (HVS) properties. After decomposing the host image into four sub-bands, they applied singular value decomposition to each sub-band and embedded singular values of the watermark into the sub-bands.

Hung-Hsu Tsai et al.[19] have proposed a novel blind watermarking technique for image copyright protection by using the DWT based on SVD and SVR, additionally the particle swarm optimization is further utilized to optimize the scheme where the watermark bit can be calculated using the watermarked coefficient and its corresponding estimate coefficient. Qi-yuan Sua and Hua-Qiang Yuan [20] have proposed an algorithm that is used in watermarking the digital audio using both DWT and DCT. This watermarking algorithm guarantees the reliability and origin source endorsement of the multimedia file without affecting its overall quality. The multi-resolution of DWT and the de-correlation capability and energy aggregation of DCT are used.

Chih-Chin Lai and Cheng-Chih Tsai [21] proposed a hybrid image-watermarking technique based on DWT and SVD, where the watermark data is embedded on the singular values of the host image’s DWT sub bands. Experimental results of the proposed method have shown both the significant enhancement in imperceptibility and the robustness under attacks.

Marzieh Amini et al. [22] have proposed a new halftone image watermarking based on DWT combined with SVD technique. Half toning is the process of presenting gray-scale images using just black and white i.e. binary levels. The cover image is an error diffusion halftone image, that decomposed into 2-level wavelet transform in the second level of wavelet transform, the sub band with the midst variance intensity is selected as a place for inserting the watermark. In extraction process, detector response is computed to get the original watermark; error diffusion based techniques achieve good visual quality and reasonable computational complexity. Shenchen ZHAO [23] has presented a new technique of image digital watermarking technique based on DWT. This technique uses a combination of pre-transformation in time domain with DWT. He exploits orthogonal matrix to multiply each matrix block of the host image, and then, embeds the watermark information into the DWT domain of the processed host image. Na Maet al.[24] have proposed DWT, Walsh and SV combination of digital watermarking algorithms. The energy in which Haar wavelet decomposition of the characteristics in the low frequency coefficients and by Walsh transformation, block and calculate the adaptive embedding strength, greatly improved watermark in the human visual transparency, then
using anti-geometric distortion of the SV decomposition. Experiments show that the algorithm is a crop, scale, translation, noise, (JPEG) compression, median filtering, image processing has good robustness, in rotation 45°of the extracted watermark image processing may be effective but the quality is not high.

Wang Hui-Qin and Zhao Min [25] proposed scheme for copyright protection and content authentication of digital color image based on SVD in DWT Domain. In this technique, the blue component of the original color image is decomposed with DWT, after that low-frequency coefficients are transformed by block-SVD and then and a binary watermark scrambled by logistic chaotic is embedded by quantizing the singular values of primitive image. Also the watermark extraction procedure was discussed without the original image.

Bo Chen and Hang Shen [26] developed a new robust fragile double image watermarking algorithm using a new bit substitution based on pseudo-random sequence and improved pixel-wise masking model. The method embeds robust and fragile watermark into the sensitive part and insensitive part of wavelet coefficients making both watermarks non-interfering. Peng Liu and Zhizhong Ding [27] proposed a blind image watermarking scheme based on wavelet tree quantization. Two largest coefficients are selected as significant coefficients and the difference between them is taken as significant difference. The significant difference with an average significant difference value and maximum difference coefficients are quantized for embedding watermark bit. [28] Jeril George et al. have proposed a novel technique for watermarking using discrete wavelet transformation and singular value decomposition. DWT ensures imperceptibility and SVD ensures robustness of the watermark against attacks. Arnold transform is used, to address the issue of watermark security. Watermark extraction is semi-blind, which avoids the need for host image for extraction.

[29] Xueyi Ye et al. proposed a robust Discrete Wavelet Transform (DWT) - Singular Value Decomposition (SVD) watermark technique based on multiple-level Discrete Cosine Transform (DCT), based on the advantage of DCT’s energy concentration. Firstly, Discrete wavelet transform is applied on carrier image and its low frequency sub-band is obtained. Secondly, the coefficient matrix of the low frequency sub-band is partitioned. Then each block is done multiple-level DCT. Thirdly, the appropriate DCT coefficients are selected in each block to form a new matrix based on the capacity of the embedded watermark data, and then the encrypted watermark data is embedded in the singular value matrix of the new matrix. Finally, the image containing watermark data is obtained by SVD synthesis, multiple-level inverse DCT and multiple-level inverse DWT.

[30] Md Saiful Islam and Ui Pil Chong propose a new digital watermarking algorithm with gray image based on discrete wavelet transform (DWT), 2-D discrete cosine transform (DCT) and singular value decomposition (SVD) for robust watermarking of digital images for copyright protection of digital media. One of the major advantages of the proposed method is the robustness of the technique on wide set of attacks. [31] Prasanna Shah et al. proposed a SVD-based digital watermarking technique for robust watermarking of digital images, to protect digital media copyright efficiently. The security of the proposed technique is increased by applying another wavelet function. One of the major advantages of the proposed method is the robustness of the technique on wide set of attacks. [32] Jagaseesh Bandi et al. proposed a robust Digital Image watermarking algorithm which is projected in DWT domain using back propagation neural networks and HVS Parameters like Luminous sensitivity and Texture sensitivity. Watermark is embedded and extracted using neural networks. The proposed method is more robust and provide protection against several attacks like: Resizing, Row-Column copying, Low pass filtering, Median filtering, JPEG Compression, Salt and Pepper Noise, Rotation, Cropping, Bit Plane Removal, Blurring, Row-Column blanking, Intensity Transformation, etc. [33] Rhman A. Md. and Rabbi F. M. M. proposed a SVD-DWT technique for deconstructing and reconstructing the image. The secret watermark data is embedded into the R band using a secret key after splitting the host image into three respective bands i.e. R, G and B. The extracting process is performed by dividing the watermarked image into all the colour channels and then further process is applied into R plane.

5. CONCLUSION

Due to rapid progress in watermarking research various researchers from various fields are focusing to develop robust watermarking schemes but none
of the techniques is robust to all possible attacks. This paper emphasizes wavelet based watermarking which is very popular today. It also reviews the applications and characteristics of digital watermarking. Wavelet based watermarking provides a good platform for two conflicting requirement of digital watermarking. First, the watermark needs to robust against intentional or unintentional attacks. Second, watermarked image needs to maintain good fidelity. This paper helps in providing the information about wavelet based watermarking to researchers.

7. REFERENCES


