Transform Based Digital Image Watermarking Techniques for Image Authentication

Mrugesh Prajapati

1M.Tech (EC Deptt.), Truba Institute Of Engineering And Information Technology, Bhopal, India

Abstract—In the past few years many new techniques and concepts based on data hiding have been introduced for image authentication and copyright protection. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. Digital watermarking is a popular technique that is used for copyright protection and authentication. Digital watermarking is hiding the information inside a digital media. This paper attempts to first introduce general idea behind digital watermarking as well as some of its basic characteristics followed by describing some applications of watermarking techniques. In spatial domain, Least-Significant Bit (LSB), Patchwork algorithm and Texture mapping coding method and in the transform domain, Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) has been discussed. In this paper it can be proposed frequency domain watermarking using DCT and watermark is embedded in the Mid Frequency Band of DCT.

Keywords—watermarking, authentication, copyright protection, (LSB), Discrete Cosine Transform, Discrete Wavelet Transform.

I. INTRODUCTION

With the increase in the availability of digital data such as multimedia services on the Internet, there is a pressing need to manage and protect the illegal duplication of data. The problem of protecting multimedia information becomes more and more important. Of the many approaches possible to protect visual data, digital watermarking is probably the one that has received most interest. Digital watermarking is the process of embedding information into a digital signal. The signal may be audio, pictures or video, for example. The kind of watermark consist the author and the user’s information, which could be the text, owner’s logo, serial number or any other control information [1,6,7]. If the signal is copied, then the information is also carried in the copy.

There are four factors that are used to determine the quality of watermarking. They are robustness, imperceptibility, capacity, and blindness [4-7]. Robustness means that the watermark should be difficult to remove or destroy.

It is a measure of immunity of the watermark against the different attacks like additive noise, scanning JPEG compression, filtering, scaling, rotation, and cropping. Imperceptibility means the quality of original host image should not be changed or destroyed by the presence of watermark. Capacity includes techniques that make it possible embed majority of information. Blind watermarking means that the extraction of watermark from watermarked image without the original image because the sometimes the original image is not available. An efficient watermarking algorithm is one which finds a good balance in all the above mentioned characteristics. [11,13]

II. LITERATURE REVIEW

There have been many watermarking techniques proposed for the digital images. The watermarking techniques can be broadly classified into two categories: spatial domain techniques (LSB, Patchwork algorithm, Texture mapping coding method) [12] and Transform domain techniques (DFT, DCT, DWT). [1,7,9,10,12]

Cox et. al [10] uses the DCT domain for the watermark embedding for the first time. As JPEG standard also uses DCT for image compression it is always a good idea to explore image watermarking in DCT domain.

B. Ram [1] described a digital image watermarking techniques based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT), where the method operates in the frequency domain embedding a pseudo random sequence of a real numbers in a selected set of DCT coefficients and watermark added to this selected DCT coefficients.

R. Shukla et. al [2] described a method that can recovered the watermarked image by the use of LSB modification and DCT techniques. This technique can be analyze by using various distortion matrices to verify their robustness.

In [3], P.Khatkale et.al discussed the basic principle and different spatial and frequency domain algorithms. Furthermore they also discussed application area, different attacks on watermarked images and proposed algorithm used a block based DCT.
D. Singh et al. in [4], described the comparative studies of spatial and frequency domain watermarking scheme. It can be concluded that frequency domain techniques embeds more bits and more robust than spatial domain techniques. From the result of this paper, it can be conclude that DCT method introduce a low noise.

R. Chaturvedi et al. in [5] proposed algorithm of image watermarking techniques based on DCT using Mid Band Coefficients for robustness. They have been used DCT Mid band coefficient for different image format and analyze PSNR value for different image format.

F. Namazi et al. in [6] described Block based Adaptive Image Watermarking techniques based on DCT and human visual characteristics. In order to achieve more robustness and transparency watermark has been embedded in to middle frequency component of the image.

V. Santhi et al. in [7] proposed a robust non blind watermarking algorithm based on DC-coefficients for the color image.

M. Choubiaa et al. in [8] proposed algorithm of digital image watermarking based on DCT using permuting the image. In this algorithm, First permuted the original image using pseudo random sequence and apply DCT to permuted image and then embed the watermark. It can achieve better balance between robustness and invisibility.

A. Aggarwal et al. in [9] discussed review of spatial domain watermarking for the digital images. In this paper, Block based watermarking scheme, LSB techniques and secured watermarking algorithm were discussed.

T. Tewari et al. in [10] proposed DCT based additive watermarking technique. In this paper, watermark is embedded in to mid frequency sub band of the DCT.

In [11] B. Gunjal et al. described the complete overview of the digital image watermarking techniques in spatial domain as well as frequency domain. This paper indicates result of LSB, DCT and DWT.

Jiang Xuehua in [12] discussed the basic principle, characteristics and algorithms of digital watermarking techniques and DCT algorithm is selected to do the application test.


A. Taherinia et al. in [14] proposed and implemented a DCT based blind watermarking scheme based on spread spectrum communication. In this algorithm watermark can extract even if watermarked image was compressed with quality factor of 1%. From the result, it can be conclude that it can robust with respect to Gaussian noise.

### III. Watermarking Process

A watermarking system is usually divided into two distinct steps, embedding, and detection. The general watermarking process is shown in figure 1.

In embedding, an algorithm accepts the original host image and the watermark to be embedded and produces a watermarked signal. The watermarked signal is then transmitted or stored, usually transmitted to another person. In watermark extraction, an algorithm accepts the signal to extract the watermark from it. If the signal was unmodified during transmission, then the watermark is still present and it can be extracted.

### IV. Application Area

Watermarking can be really useful in several areas of interest involving digital images. Some applications of invisible watermarks are listed here to; [2]

**Copyright Protection:** This is the most prominent application of watermarks. With lots of images being exchanged over insecure networks every day, copyright protection becomes a very important issue. Watermarking will prevent redistribution of copyrighted images.

**Authentication:** Sometimes the ownership of the contents has to be verified. This can be done by embedding a watermark and providing the owner with a private key which gives him an access to the message. ID cards, ATM cards, credit cards are all examples of documents which require authentication.

**Broadcast Monitoring:** As the name suggests broadcast monitoring is used to verify the programs broadcasted on TV or radio. It especially helps the advertising companies to see if their advertisements appeared for the right duration or not.
Content Labeling: Watermarks can be used to give more information about the cover object. This process is named content labeling.

Tamper Detection: Fragile watermarks can be used to detect tampering in an image. If the fragile watermark is degraded in any way then we can say that the image or document in question has been tampered.

Digital Fingerprinting: This is a process used to detect the owner of the content. Every fingerprint will be unique to the owner.

Content protection: In this process the content stamped with a visible watermark that is very difficult to remove so that it can be publicly and freely distributed.

V. CLASSIFICATION
Watermarking algorithms can be classified on several criteria as given below. [11]

1) According to domain of watermark insertion:
   a) Spatial Domain Techniques
   b) Frequency Domain Techniques.

2) According to Watermark detection and extraction:
   a) Blind Watermarking
   b) Non-blind Watermarking.

The non-blind watermarking requires that original image to exist for detection and extraction whereas blind techniques do not require original image.

3) According to ability of watermark to resist attack:
   a) Fragile Watermarking
   b) Semi-fragile Watermarking

4) According to Visibility:
   a) Visible Watermarks
   b) Invisible Watermarks

VI. WATERMARKING DOMAIN
There are mainly two direction of embedding the watermark in the original image namely the spatial domain and transform domain as shown in fig.3

In the spatial domain watermarking method, the watermark embedded using patchwork techniques, LSB, Statistical, texture mapping coding and block based technique. Spatial domain techniques works directly with pixel values. Generally the spatial domain techniques are easy to implement from a computational point of view [10], but more vulnerable in the common image attacks such as filtering and JPEG compression. [4,7,9] The frequency domain approaches are widely used for image watermarking. In these techniques, the image is being transformed via some common frequency transform and the watermarking is achieved by altering the transformed coefficients of the images. The transformed usually used are DFT, DWT, DCT [1-4] [7-8] [10-11] and HARR.

As per P. Khatkale et.al in [3] Table 1 shows a small comparison between the spatial and frequency domain techniques.

<table>
<thead>
<tr>
<th></th>
<th>Spatial Domain</th>
<th>Frequency domain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computational cost</strong></td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>Robustness</strong></td>
<td>Fragile</td>
<td>More Robust</td>
</tr>
<tr>
<td><strong>Perceptual Quality</strong></td>
<td>High Control</td>
<td>Low Control</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>High (depends on the size of image)</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Example of Application</strong></td>
<td>Mainly Authentication</td>
<td>Copy rights</td>
</tr>
</tbody>
</table>
Another, well known spatial domain based scheme is patchwork-based technique given by Bender et al. [7]. Depending on the statistics, the algorithm uses the statistical characteristics of pixels to embed the information into the brightness values of pixel. It is mainly used for the security of printing bills.

Texture mapping coding method

In this method, a region of random texture pattern found in the image is copied to an area of the image with similar texture. Autocorrelation is then used to recover each texture region. The most significant problem with this scheme is that it is only appropriate for images that possess large areas of random texture. [13].

VII. FREQUENCY DOMAIN WATERMARKING

In Frequency Domain Watermarking, the watermark information is embedded in the transform domain. So this technique is also known as Transform Domain Watermarking. As discussed early, transformed domain watermarking schemes are more robust as compared to simple spatial domain watermarking schemes because information can be spread out to entire image. However, they are difficult to implement and are computationally more expensive. The most commonly used transforms are DCT, DFT, DWT and DHT. Each of these transforms has its own characteristics and represents the image in different ways. In this paper we will discuss watermarking in frequency domain such as DFT, DCT, and DWT.

Discrete wavelet Transform:

The basic idea in the DWT for a one dimensional signal is the following. A signal is split into two parts, usually high frequencies and low frequencies. This splitting is called decomposition. [7,11]

![Flow of DWT Process](image)

A step of wavelet transform decomposes an image into four parts: HH, HL, LH and LL in Figure. LL is low frequency coefficient, LH is high frequency coefficient horizontally, HL is high frequency coefficient vertically, and HH is high frequency coefficient diagonally. Watermark should be embedded in low frequency coefficients.

Furthermore, DWT image and video coding, such as embedded zero-tree wavelet (EZW) coding, are included in the upcoming image and video compression standards, such as JPEG2000. Thus DWT decomposition can be exploited to make a real-time watermark application. [11]

Discrete Cosine Transform

Discrete cosine transform (DCT) is a most popular transform domain technique [4] because of several reasons. One of the reasons is that most of the compression techniques developed in the DCT domain (JPEG, MPEG, MPEG1, and MPEG2) & therefore image processing is more familiar with it. DCT is a frequency linear transformation domain approach in digital signal process technology. DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. However, they are difficult to implement and are computationally more expensive. At the same time they are weak against geometric attacks like rotation, scaling, cropping etc.
Table II

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| **DFT**   | 1. DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions  
2. Cost of computing may be higher | 1. Complex implementation  
2. Cost of computing may be higher  
3. Noise near edges of images or video frames. |
| **DWT**   | 1. Allows good localization both in time and spatial frequency domain  
2. Higher compression ratio which is relevant to human perception | 1. Cost of computing may be higher.  
2. Longer compression time.  
3. Noise near edges of images or video frames. |
| **DCT**   | 1. The watermark is embedded into the coefficients of the middle frequency, so the visibility of image will not be affected and the watermark will not be removed by any kind of attack. | 1. Block wise DCT destroys the invariance properties of the system.  
2. Certain higher frequency components tend to be suppressed during the quantization step. |

**PERFORMANCE PARAMETER:**

The quality of watermarked image is studied with two metrics, peak signal to noise ratio (PSNR) and Similarity Factor (SM).

Peak Signal to Noise Ratio is calculated by the following formula

\[ PSNR = \log \left( \frac{2^n - 1}{\text{MSE}} \right) \]  

(2)

Where \( n \) is the number of bits used for image representation and MSE refers to the Mean Square Error between original and watermarked image of \( N \times N \) and is calculated with the formula.

\[ \text{MSE} = \frac{1}{N \times N} \sum_{x=1}^{N} \sum_{y=1}^{N} [I(x, y) - \tilde{I}(x, y)]^2 \]  

(3)

Where

\( I(x, y) \) : The pixel value of original image

\( \tilde{I}(x, y) \) : The pixel value of watermarked image

\( N \) : size of an image

Similarity Factor is measure of the similarity of pixel intensities between the original image and the watermarked image. This helps us to calculate the changes in the perceptual quality of the image more precisely. The similarity factor has value [0,1] calculated using following equation . If SM = 1 then the embedded watermark and the extracted watermark are same. Generally value of SM>.75 is accepted as reasonable watermark extraction.

\[ SF = \frac{\sum \sum I(x, y) \times \tilde{I}(x, y)}{\sum \sum I(x, y)^2} \]  

(4)

Where \( I(x, y) \) is the original image and \( \tilde{I}(x, y) \) is the watermarked image.

**VIII. PROPOSED SCHEME**

The proposed algorithm uses the discrete cosine transform (DCT) using Mid Band Coefficient Exchange.

In the DCT, an image is segmented in non-overlapping 8x8 block and applies the DCT to each block. This will divide an image into three main region namely low frequencies sub-band (F\(_L\)), middle frequencies sub-band (F\(_M\)) and high frequencies sub-band (F\(_H\)) as shown in fig.4 which makes it easier to select the band in which the watermark is to be inserted. The literature survey indicates that middle frequency bands (F\(_M\)) are most widely chosen because of two facts. The first fact is that 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. Therefore the watermark is embedded by modifying the coefficients of the middle frequency sub band so that the visibility of the image will not be affected and the watermark will not be removed by compression.

Fig.4 Middle Band Frequencies in 8x8 DCT Block
The Two dimensional DCT of an M X N matrix is defined as follow:

\[ C(p, q) = \alpha_p \alpha_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} I(m, n) \cos \left( \frac{\pi}{2M} (m + 1)p \right) \cos \left( \frac{\pi}{2N} (n + 1)q \right) \]  

(5)

And the inverse DCT is given by

\[ I(m, n) = \frac{1}{\alpha_p \alpha_q} \sum_{p=-M/2}^{M/2-1} \sum_{q=-N/2}^{N/2-1} C(p, q) \cos \left( \frac{\pi}{2M} (m + 1)p \right) \cos \left( \frac{\pi}{2N} (n + 1)q \right) \]  

(6)

Where,

\[ \alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & p = 0 \\ \frac{1}{\sqrt{M}} & 1 \leq p \leq M - 1 \end{cases} \]

\[ \alpha_q = \begin{cases} \frac{1}{\sqrt{N}} & q = 0 \\ \frac{1}{\sqrt{N}} & 1 \leq q \leq N - 1 \end{cases} \]

IX. FLOW CHART AND ALGORITHM OF PROPOSED SCHEME

**Watermark Embedding Algorithm:**

Watermark embedding algorithm consists of following steps:

1. Read the cover image and watermark logo.
2. If the watermark logo is smaller than cover image then it is padded with ones (1’s).
3. Segment the cover image in to non overlapping blocks of 8*8.
4. Apply Forward DCT to these blocks.
5. Apply coefficient selection criteria (e.g. Highest, Mid, Lowest).
6. Embedded watermark information by modifying the selected coefficients using classical coefficient scheme.
7. Apply Inverse DCT transform on each block.

Most algorithms using DCT are classified based on step 5. The insertion of watermark information in mid band coefficient block gives the extra robustness to the watermark.

**Watermark extraction Algorithm:**

The watermark extraction algorithm consists of following steps:

1. Read the watermarked image and original watermark.
2. Segment the watermarked image into non-overlapping blocks of 8*8 and perform DCT on each blocks.
3. Selected DCT coefficients are compared for every block. If the pixel at \( M_1(u, v) \) is greater than the pixel at \( M_2(u, v) \), then hidden watermarked bit would be black i.e the DCT block will encode “0” otherwise the hidden watermarked bit would be a white i.e DCT block will encode a “1”. 
4. Reshaping the extracted message vector to 2D binary watermarked image.
5. Calculate the similarity ratio between the embedded and extracted watermark.
6. End
X. CONCLUSION

Digital Watermarking defines methods and technologies that hide information, for example a number or text, in digital media, such as images, copyright protection, tamper proofing, video or audio. In this paper we are briefly defining the concepts of watermarking, the properties of a watermarking system, embedding and extracting algorithm of watermarking as well as an application of watermarking discussed, and the DCT algorithm is selected to do the application test of digital image copyright protection.

REFERENCES


