DIGITAL IMAGE WATERMARKING TECHNIQUES: A SURVEY

Vaishali¹, Priyanka²

¹Associate professor
Department of Electronics and Communication Engineering
Deenbandhu chhotu Ram University Of Science And Technology, Murthal, Sonipat, India

Abstract: Image Watermarking has become very popular due to wide use of internet and multimedia applications. Watermarking has many applications such as copyright protection, content authentication, data integrity etc. In image watermarking, additional information is added to the host image in the form of logo/audio/video or text. This provides more security to the image preventing it from tampering or fraud. In this paper, various watermarking techniques have been discussed. Classification, features, comparison and applications of various watermarking techniques have also been presented.

Keywords- Image watermarking, robustness, DCT, DWT, MSE, PSNR, BER

I. INTRODUCTION

The term “Digital Watermark” was coined by Andrew Tirkel and Charles Osborne in December 1992. Tirkel et. al.[15] demonstrated the first successful embedding and extraction of stegnographic spread spectrum watermark 1993[1]. Digital watermarking is an effective method of hiding digital data in digital media such as image, audio, video etc for preventing illegal duplication of data and to ensure copyright protection and security. In earlier days manufacturers used watermarking on their products to ensure authenticity. Nowadays, watermarks are more commonly used in currencies, papers and postage stamps in order to prevent fraud and forgery.

Watermarking is basically a four step procedure:
(i) Generation: - In the watermark generation step a logo is generated in the form of audio/video/text such that any distortion in the host image can be easily detected.
(ii) Embedding: - Embedding step embeds the generated watermark into the host image using suitable watermark technique.
(iii) Distribution/attacks: - Distribution can be seen as the transmission of the watermarked image over the media and any attempt to distort the transmitted image is called attack on the image.
(iv) Extraction: - Extraction is the reverse process of embedding process. It is done to extract the embedded watermark at the receiver side. Any change in the properties of watermark implies that the image has been subjected to one or other type of attack.

Basic watermarking procedure is shown in Fig. 1.

![Fig. 1.Basic watermarking procedure](image-url)
II. DESIRABLE FEATURES OF WATERMARK

Following are the desirable features for a watermark:

**Imperceptibility:** The viewer should not be able to notice the watermark. It creates suspicion in case of visible distortions. Also watermark should not degrade the quality of the content.

**Robustness:** This is the most important requirement of any watermarking technique. A digital watermark is called robust if it resists a designated class of attacks. It will remain intact after common editing processing, lossy compression etc and hence is a desirable feature for copyright information of digital work. Cox et. al. (2002) defines robustness as the “ability to detect watermark after common signal processing operation”[3]. Robust watermarking is used mainly for copyright protection.

**Verifiability:** Watermark should be able to provide full and reliable evidence for the ownership of copyright protected information products.

**Capacity:** Image watermarking capacity is the measure of amount of information that can be hidden within a digital image. Generally, it should be as high as possible. Different applications have different capacity requirements

III. APPLICATIONS OF DIGITAL IMAGE WATERMARKING [4]

**Broadcast Monitoring:** It is used to confirm the content which is to be transmitted over a media. Television news often contains watermarked video from international agencies.

**Authentication:** The purpose of authentication application is to detect any modification in the image content. Fragile watermark can be used for image authentication. A watermark is called Fragile if it can’t be detected even after the slightest modification. Example of this application is satellite imagery or medical imagery.

**Copyright protection:** Watermarking can be used to protect the redistribution of copyrighted material over the untrusted network like internet. Prevention of illegal copying of songs, images etc. is one of the practical application of watermarking under this category.

**Digital Fingerprinting:** Digital fingerprinting is a technology which enables content owners exercise greater control on their copyrighted content. Fingerprints are unique to the owner of the digital content.

**Medical Applications:** Names of the patients can be printed on the X-ray reports and MRI scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If the report of two patients get mixed up this could lead to a disaster.

IV. WATERMARKING ATTACKS [5]

There are various possible malicious intentional or unintentional attacks that a watermarked object is subjected to. The robustness of watermarking system is highly vulnerable to various attacks due to the presence of wide range of image processing softwares. These attacks prevent the watermark from performing its intended purpose. A brief introduction to various types of watermarking attacks is as under:

**Removal Attack:** Removal attacks intend to remove the watermark data from the watermarked object. Such attacks exploit the fact that the watermark is usually an additive noise signal present in the host signal.
Interference attack: Under this category, additional noise is added to the watermarked object which interferes with the properties of the existing watermark. Lossy compression, quantization, collusion, denoising, averaging, and noise storm are some examples of this category of attacks.

Geometric attack: All manipulations that affect the geometry of the image such as flipping, rotation, cropping, etc. should be detectable. A cropping attack from the right-hand side and the bottom of the image is an example of this attack.

Forgery attack: The forgery attacks that result in object insertion and deletion, scene background changes are all tantamount to substitution.

Security Attack: In particular, if the watermarking algorithm is known, an attacker can further try to perform modifications to render the watermark invalid or to estimate and modify the watermark. In this case, we talk about an attack on security. A secure watermarking algorithm prevents the embedded information from being destroyed, detected or forged.

Active Attacks: Here, the hacker tries deliberately to remove the watermark or simply make it undetectable. This is a big issue in copyright protection, fingerprinting or copy control etc.

Passive Attacks: In this case, the attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not. Cox et al (2002) suggest that, protection against passive attacks is of the utmost importance in covert communications where the simple knowledge of the presence of watermark is often more than sufficient.

V. WATERMARKING TECHNIQUES
According to the domain, digital watermarking techniques can be classified as:

i. Spatial domain watermarking

ii. Frequency domain watermarking

Table 1. shows a comparative analysis of spatial domain and frequency domain watermarking techniques.

<table>
<thead>
<tr>
<th>FACTORS</th>
<th>SPATIAL DOMAIN</th>
<th>FREQUENCY DOMAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computation cost</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Robustness</td>
<td>Fragile</td>
<td>More Robust</td>
</tr>
<tr>
<td>Perceptual quality</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Computational complexity</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Computational time</td>
<td>Less</td>
<td>More</td>
</tr>
<tr>
<td>Capacity</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Computational power</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Example of application</td>
<td>Mainly authentication</td>
<td>Copyright protection</td>
</tr>
</tbody>
</table>

Table 1 Comparison between spatial domain and frequency domain watermarking [5]

5.1 SPATIAL DOMAIN WATERMARKING
In spatial domain watermarking techniques, main focus is on modifying the pixels of one or two randomly selected subsets of image. It directly loads the raw data into the image pixels. Least Significant Bit (LSB), Spread Spectrum Modulation (SSM) modulation based techniques are some of the algorithms of spatial domain watermarking.
Least Significant Bit Method (LSB): In this method first subset of image is obtained. Encoder first selects the subsets of images and then selects the number of bits to be replaced. It replaces LSB of the host image with the MSB of watermark image. Since human eyes can’t detect changes in LSB of image pixels easily, embedding is done in LSB. In this method size of host and watermark image must be same [2].

Spread Spectrum Modulation (SSM) Method: SSM techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time. In this method a small pseudonoise signal is modulated by the watermark. The information is then embedded by linearly combining the host image with the modulated pseudonoise signal [5]. This method enhances the security of the watermarked image.

5.2 FREQUENCY DOMAIN WATERMARKING
Frequency domain watermarking technique applies the different transformations on an image like DCT, DWT, DFT and embed the watermark information into the coefficients by altering the coefficient value.

Discrete Cosine Transform (DCT) Method: DCT based watermarking techniques are more robust compared to spatial domain watermarking techniques. Such algorithm are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. at the same time they are weak against geometric attacks like rotation, scaling, cropping etc. Steps in DCT block based algorithm [6]

1. Segment the image into non-overlapping Blocks of 8x8.
2. Apply forward DCT to each of these blocks.
3. Apply some block selection criteria like Human Visual System (HVS).
4. Apply coefficient selection criteria (e.g. Highest).
5. Embed the watermark by modifying the Selected coefficients.
6. Apply IDCT on each block.

Discrete Wavelet Transform (DWT) Method:
In past few years, studies have shown that in some applications wavelet based watermarking schemes outperform DCT based approaches. This technique decomposes the given image into set of basic wavelets. DWT is a suitable technique to identify the area in the image that contains secret image. DWT decomposes given image into low and high frequency components and finds high frequency components and embeds an image into high frequency components.Wavelet transform decomposed the image into 3 spatial directions i.e. horizontal, vertical and diagonal. Magnitude of DWT coefficient is larger in lowest bands (LL) and is smaller for other bands (HH, LH, HL)[2][7].

DWT multiresolution technique decomposes given image into four subbands:
LL (High Scale Low Frequency Component)
LH (Vertical High Scale High Frequency Component)
HL (Horizontal Low Scale High Frequency Component)
HH (Diagonal Low Scale High Frequency Component)

In two dimensional applications, for each level of decomposition, the DWT is first performed in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. For each successive level of decomposition, the LL subband of the previous level is used as the input. To perform second level
decomposition, the DWT is applied to LL1 band which decomposes the LL1 band into the four sub-bands LL2, LH2, HL2, and HH2. To perform third level decomposition, the DWT is applied to LL2 band which decompose this band into the four sub-bands – LL3, LH3, HL3, HH3. This results in 10 sub-bands per component. LH1, HL1, and HH1 contain the highest frequency bands present in the image tile, while LL3 contains the lowest frequency band [8]. Two level resolution is shown in Fig.2

![Image](image-url)

*Fig.2. 2-level DWT Resolution [9]*

It embeds watermark into LH and HL bands. This method doesn’t provide strong robustness against different types of geometric and image processing attacks but is robust to low-pass and median filtering.

**Discrete Frequency Transform (DFT) Method [6]:**
DFT domain offers robustness against geometric attacks like rotation, scaling, translation etc. DFT of a real image is generally complex valued, which results in phase and magnitude representation of an image. The strongest components of the DFT are the central components which contains low frequency.

In DFT method watermark is embed into the host image by changing the coefficients of DFT thus obtained.

Coefficients to be modified are selected as below-

i. modification to low frequency coefficients can cause visible artifacts in spatial domain. Hence low frequency components should be avoided.

   - high frequency coefficient aren’t suitable because they are removed during JPEG compression.

   - best location to embed the watermark is the mid frequency.
Table 2. summarize the advantages and disadvantages of image watermarking techniques discussed above.

<table>
<thead>
<tr>
<th>ALGORITHM</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
</table>
| LSB       | (i) Easy to implement and understand  
(ii) Low degradation of image quality  
(iii) High perceptual transparency | (i) poor robustness  
(ii) Vulnerable to noise  
(iii) Vulnerable to cropping, scaling |
| DCT       | (i) Visibility of image will not get affected  
(ii) Watermark will not be removed by any kind of attack  
(iii) robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. | (i) Block wise DCT destroys invariance properties of the system  
(ii)Some of the higher frequency components gets suppressed during quantization  
(iii) they are weak against geometric attacks like rotation, scaling, cropping etc. |
| DWT       | (i) it has higher compression ratios  
(ii) Better identification of which data is relevant to human perception  
(iii), this approach shows robustness to low-pass and median filtering. | (i) The use of larger DWT basis functions or wavelet filters produces blurring and ringing noise near edge regions in images or video frames  
(ii) Longer compression time.  
(iii) high cost of computing |
| DFT       | (i) DFT is rotation, scaling and translation (RST) invariant  
(ii) it can be used to recover from geometric distortions | (i) Complex implementation  
(ii) watermark property affects the overall quality of an image differently |

Table. 2. Advantages and Disadvantages of various watermarking techniques

VI. PERFORMANCE EVALUATION METRIC
In order to evaluate the performance of the watermarked images, there are some quality measures such as SNR, PSNR, MSE, and BER.

The **Mean square error (MSE)** is defined as average squared difference between a reference image and a distorted image. It is calculated by the formula given below

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

X and Y are height and width respectively of the image. The c (i, j) is the pixel value of the cover image and e (i, j) is the pixel value of the embed image.

**Signal to Noise ratio (SNR)** measures the sensitivity of the imaging. It measures the signal strength relative to the background noise. It is calculated by the formula given below

$$\text{SNR}_{\text{db}} = 10 \log_{10} \left( \frac{P_{\text{signal}}}{P_{\text{noise}}} \right)$$
The Peak signal to noise ratio (PSNR) is used to determine the degradation in the embedded image with respect to the host image. It is calculated by the formula as

$$PSNR = 10\log_{10}(L \ast L/MSE)$$

L is the peak signal value of the cover image which is equal to 255 for 8 bit images.

The Bit error ratio (BER) is the ratio that describes how many bits received in error over the number of the total bits received. It is calculated by comparing bit values of embed and cover image.

$$BER = P/(H \ast W)$$

H and W are height and width of the watermarked image. P is the counter initialized to zero and it increments by one if there is any bit difference between cover and embed image[10].

VII. CONCLUSION

In this paper a comprehensive survey of various aspects of Digital image watermarking, its applications and its techniques have been presented. Also a comparative analysis of various watermarking techniques is presented with their advantages and disadvantages which will help the new researchers in related areas.

REFERENCES

9. https://www.google.co.in/search?q=dwt+watermarking&biw=1366&bih=599&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjfyYChkebKAhWV1H4KHT43DosAQ_AUIBygB#imgrc=O8kuM_U8X62-aM%

@IJRTER-2016, All Rights Reserved