A Review on Digital Image Watermarking Techniques

Nirav Patel1 Yogesh Jadav2
1,2M. Tech. ECE Department
1Bhabha Engineering Research Institute Bhopal,
2A. D. Patel Institute of Technology New V. V. Nagar, India
1nirav.kadi@gmail.com 2jadavyogesh 123@yahoo.co.in

Abstract—Digital watermarking is a technique to protect the content of digital media like Image, Audio, Video or text using insertion of digital mark. Lot of research is going on in this field to develop secure and more robust digital watermarking algorithms. In this paper we survey recently existing and newly proposed Digital Image watermarking techniques. We classify the Digital Image watermarking techniques according to domain in which the watermark is embedded. Here, we limit to survey Image watermarking techniques only.

Keywords- DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), image watermarking, spatial domain, HVS.

I. INTRODUCTION

In the current trends of the world, most of the people like to use internet as a primary source to transfer information from one end to another end across the world. However security of the information is main issue while transferring the information data over the internet. There are many ways to hack the information and it is possible to copy the data and distribute this data over the internet by unauthorized person. So to withstand against such attacks and for security purpose Digital Watermarking come into the picture.

Multimedia file can be an image, video, audio or text. A watermark can be perceived as an attribute of the carrier (cover). It may contain information such as copyright, license, tracking and authorship etc [1]. Nowadays, Digital watermarking has many applications like owner identification, broadcast monitoring, copy control, data authentication etc. The digital watermarks can be a visible watermarks or Invisible watermarks. The visible watermarks are used to mark a digital image in a clearly detectable way so it can avoid unauthorized use of digital image. While the invisible watermarks are used to authenticate the content, to detect and to prevent unauthorized copy of the data [3],[5]. The Digital Watermarking can be divided into Blind and Non-Blind digital watermarking techniques. In Blind digital watermarking algorithms, the original image is not required to extract the watermark from watermarked image. While in the Non-Blind Digital Watermarking algorithms, the original image is required to compare and extract the watermark [4].

The generalized Process of watermarking is shown in Fig. 1. In watermarking the digital data is hiding in the Cover Image using spatial or transform domain algorithm. This paper is organized as follow. In section II Characteristics of Digital watermarking is discussed. Section III represents applications of watermarking. Section IV represents types of digital watermarking techniques. Section V represents the survey of digital image watermarking. Attacks on Digital Image watermarking are discussed in section VI. Section VII represents conclusion and future work.

II. CHARACTERISTICS OF DIGITAL WATERMARKING

The characteristics of digital watermarking can be classified as following [4], [5], and [6]:

A. Imperceptibility
The embedded watermark in the digital image should be imperceptible to the human eye as well as it should not create any visible mark or defects in the watermarked image.

B. Robustness
The digital watermarking should be such that it can support different levels of robustness against different types of attacks. The attacks on images are mainly two types. One of them is unintentional attacks which are come under the result of common signal processes like digital to analog conversion, analog to digital conversion, filtering, zooming or shrinking, rotation and quantization of the data. Second one is those which are done intentionally to destroy or detect the watermark.
C. Inseparability
Once the digital watermark is embedded in the image it should not possible to separate the original watermark without appropriate algorithm.

D. Security
After the embedding of watermark in the image using digital watermark technique, the watermarking algorithm should strong enough that it can prevent the unauthorized users to detect or modifying the watermark.

E. Transparency or Fidelity
The watermark should be such that it cannot affect the quality of the original image. The fidelity of the original image should not be change.

III. APPLICATIONS OF DIGITAL WATERMARKING
There are many applications of digital watermarking. The main applications are discussed as following [9],[4],[5]:

A. Fingerprints
Digital watermarks are used to specify authorized users of the content. It hides the information about the users who can use this content. It can used to identify users who can legally copy and distribute the content. The digital watermarking technique used to tracking is called fingerprinting.

B. Ownership Assertion
Digital watermarking can be used for owner identification and authentication. Using digital watermarking we can inset the owner of the content. So it is used to establish the ownership of the data.

C. Content labeling
Using digital watermarking we can embed the extra bits through which we can further insert information about the content such as graphic image with time and place information.

D. Usage control
Digital watermarking can be used to embed the information about how many times the given data can be copy. It can be added to limit the number of copies created and after every copying of data the watermark is modified. So after some number of copy created, it cannot create any more copies.

E. Broadcast monitoring
The digital watermarking is used to broadcast monitoring. The watermark can be embedded in the commercial advertisement. As a watermark date, time, no of time the advertisement should be broadcasted such kind of information can be inserted.

IV. TYPES OF DIGITAL WATERMARKING
According to watermark embedded, there are two main types of digital watermarking which described as following [3], [5].

A. Spatial domain watermarking techniques
In the spatial domain image watermarking techniques, the watermark is embedded in the pixel domain using some algorithm. In this techniques the image is not transform to the another domain, but the actual pixel values are changed according to watermarking bit. Modification of bits can include the flipping of lower bits of the pixel values. The embedding process of the watermark in the cover image is based on the simple operation on the pixel values of the cover image according to the watermark bit.

B. Transform Domain Techniques
Transform domain methods are more widely used for watermarking as compared to spatial domain methods because its robustness against different attacks. In the transform domain methods, the original image is converted to frequency domain using discrete cosine transform (DCT), discrete Fourier transform or discrete wavelet transform (DWT). After converting the image in spectral coefficients using any one of the method mentioned above, the watermark is embedded in this domain by changing the coefficients of the transform domain. The reason for choosing frequency domain is that the characteristics of human visual system (HVS) are better understood using spectral coefficients. For example, HVS is more sensitive to low frequency coefficients while it is less sensitive to the high frequency coefficients [5].

V. SURVEY OF DIGITAL WATERMARKING
Digital watermarking can be used in many applications. So, the lot of research is going on to develop robust and fast watermarking algorithms. Basically, there are two main types of watermarking one is spatial domain and second one is transform domain watermarking. In this paper we would discuss different watermarking algorithms within the LSB, DCT and DWT domain. We begin our discussion with spatial domain watermarking algorithms.

A. Spatial domain algorithms:
The LSB method of embedding watermark into the cover image is the basic method of watermarking. The human visual system cannot perceive the changes make in the least significant bits because its weight is very small as compared to MSB’s. While the weight of the MSB’s are high enough so that one bit change in the upper 4 MSB’s can make visual change in the original image. So LSB’s mainly lower two LSB’s are used for watermark embedding. The basic algorithm to embed watermark in the cover image using LSB substitution is shown in Fig. 2. The LSB substitution algorithm is simple to implement. The summary of literature review is shown in table 1.

![Fig. 2: Simple LSB algorithm for watermarking](image)
A Review on Digital Image Watermarking Techniques
(IJSRD/Vol. 1/Issue 12/2014/0088)

Table 1 Summary of spatial domain methods

<table>
<thead>
<tr>
<th>Author</th>
<th>Year of publication</th>
<th>Embedding Algorithm</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Bamatraf et al. [7]</td>
<td>April 2011</td>
<td>Combination of LSB and inverse bit algorithm</td>
<td>54.5961</td>
</tr>
<tr>
<td>S. P. Maity and M. Kundu [8]</td>
<td>2002</td>
<td>Block based watermark bit substitution</td>
<td>42.40</td>
</tr>
</tbody>
</table>

Puneet Kr Sharma and Rajni [6] presents simple LSB based watermarking algorithm for Image watermarking. They embedded the binary watermark bits in different bit substitution from LSB to MSB. After they embed the bit in LSB the watermark is extracted without any distortion but as they embed the watermark in LSB to MSB the watermarked image start distorted. This method is simple to implement and robust to cropping or addition of noise, but it lacks basic robustness. The compression may defeat the watermark. The PSNR, using this algorithm is 55.878 db which good as compared to other spatial domain algorithms but security is less, Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd. Salleh [7] presents new algorithm based on combination of LSB and inverse bit. In this algorithm they used inverse of watermark and then they embedded it into LSB to MSB and also in the combination of LSB’s. Good in cropping and additive noise and it gives better results compared to 1-LSB algorithm, but it also lacks basic robustness against different attacks. By using this method the PSNR they obtain is 54.5961. Santi Prasad Maity and Malay Kumar Kundu [8] present a blind image watermarking scheme in spatial domain. In this technique recovery process needs only one secret image. To hide the data with less visual distortion, spatial mask of suitable size is used. This method is computationally efficient and robust against different attacks as compared to previous algorithms. In this method PSNR they obtain is 42.40 which is less than previous two methods. Harpuneet Kaur [9] proposed a new watermarking technique based on watermark nesting. This technique can embed more number of watermark bits as compared to previous techniques without affecting the imperceptibility of the watermark. To increase the capacity of watermark and security the concept of watermark in watermark is used. Means extra watermark is embedded into the main watermark and that nested watermark is embedded in to the cover image. This method is computationally complex but it provides more robustness and security as compared to previous algorithms discussed. In this method PSNR they get which is 17.3239 which is less than all methods but the security in this method is high as compared to other methods. Thanuja T C, P Nagaraju, Vinay J, Kavya N Bhushan and Naren S Vasanan [10] proposed a robust spatial domain watermarking for colour images. This algorithm is based on modulo operations to embed the watermark. In this method the embedding is carried out in blue plane of the Host Color image, since changes made to this layer is imperceptible to the human eye [10]. For embedding and extraction of watermark same degree of modulo operation is used along with majority logic. This algorithm is robust against various kinds of noise and geometric attacks. In this method they get 34.99 db PSNR.

B. Discrete Cosine transform

Discrete cosine transform based watermarking is more robust as compared to spatial domain watermarking techniques, but it is more complex to implement and computationally more expensive. DCT based watermarking techniques are classified into global DCT based techniques and block DCT based techniques. In global DCT based watermarking techniques, DCT of cover Image is used. They convert the image globally to its frequency domain. In this domain the image is divided into smaller blocks and they do not use any secret/secret key. However, the PSNR in this method is lower compared to other methods. In the block based DCT watermarking the image is divided into non-overlapped blocks and then the DCT of each individual block is taken. After converting DCT of blocks the watermark is embedded in each block according to the coefficient selection criteria. The main steps in any block are based DCT watermarking is shown in Fig. 3. While embedding the watermark in frequency domain, the characteristics of human visual system (HVS) is very important. Embedding the watermark in the perceptually significant portion of the image is important because while compression it removes perceptually insignificant portion of the image. In frequency domain it is a high frequency values and in spatial domain it is least significant bits. The summery of literature review is shown in Table 2. Zhao Rui-mei et al. [11] Proposed a blind I mage watermarking scheme based on 8x8 block based DCT. In this method 2-bit image is embedded in an 8-bit gray image.

Step 1: Segment the image into non-overlapping blocks of 8x8
Step 2: Apply forward DCT to each of these blocks
Step 3: Apply some block selection criteria (e.g. HVS)
Step 4: Apply coefficient selection criteria (e.g. highest)
Step 5: Embed watermark by modifying the selected coefficients
Step 6: Apply inverse DCT transform on each block
Output: Watermarked Image

Fig. 3: Steps in DCT Block Based Watermarking Algorithm [4]

The 2-bit image watermark is pre-processed using Arnold scrambling to improve the robustness of the watermark. In the process of watermark embedding the image is divided into non-overlapped 8x8 blocks and then each block is transformed using DCT. The DCT coefficients are sorted by means of Zigzag pattern and an AC coefficient is selected in each block with calculation of average of each block. This method has better visibility and stronger robustness when it is attacked by JPEG compression, filtering, noise and
shearing [11]. The PSNR they get using this method is 35.1346.

<table>
<thead>
<tr>
<th>Author</th>
<th>Year of publication</th>
<th>Transform Domain</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>R. Juan et al. [12]</td>
<td>January 2000</td>
<td>Sub band DCT</td>
<td>29.34</td>
</tr>
<tr>
<td>M. Soleimani et al. [14]</td>
<td>June 2012</td>
<td>AC coefficient based Sub band DCT</td>
<td>64.5442</td>
</tr>
<tr>
<td>M. Barni et al. [15]</td>
<td>1998</td>
<td>Global DCT</td>
<td>-</td>
</tr>
<tr>
<td>Mr. N. S. Narawade et al. [16]</td>
<td>Aug 2012</td>
<td>Global DCT</td>
<td>24.1</td>
</tr>
<tr>
<td>Mrs. R. Chaturvedi et al. [17]</td>
<td>March 2012</td>
<td>Sub band DCT</td>
<td>42.09</td>
</tr>
</tbody>
</table>

Table 2 Summary of DCT domain methods

Juan R. Hernández, Martín Amado, and Fernando Pérez González [12] proposed a spread-spectrum based DCT domain watermarking technique for copyright protection of still images. This is the blind block based DCT watermarking technique. This method is blind watermarking technique. The original image’s DCT coefficients are selected to embed the watermark using generalized Gaussian model. For watermark extraction optimal ML detector is used. The PSNR they get using this method is 29.34. Chandra Mohan B and Srinivas Kumar S [13] proposed robust multiple image watermarking scheme using Multiple Descriptions and Quantization Index Modulation. In this technique the watermark embedding is done in two stages. In the first stage, the cover image is divided into odd and even images and then the watermark is embedded into the odd image using block based DCT. In the second stage the watermarked odd image and even image are combined to get watermarked image and then again the watermark is embedded in the watermarked image using block based DCT. By embedding the watermark in two stages provides robustness to both local and global attacks. The PSNR they get using this method is 39.37 which good as compared to other methods. Malihe Soleimani, Faezeh Sanaei Nezhad, Hadi Mahdipour, and Morteza Khadem [14] proposed a sub band DCT based image watermarking scheme. In this method each block is transformed using DCT and then the two AC components are selected to embed the watermark bit. This method is robust against JPEG compression or common channel noise. As compared other DCT domain methods the PSNR they get using this method is 64.5442. Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva [15] proposed a digital watermarking based on DCT. In this method a pseudo random sequence is used as a watermark. A pseudo random sequence of real numbers is embedded in selected set of DCT coefficients. The coefficients are selected by arranging L+M coefficients in Zigzag patterns. The proposed algorithm is robust against several signal processing attacks including JPEG compression, low pass and median filtering, histogram equalization and stretching, Gaussian noise and resizing. Mr. Navnath S. Narawade I and Dr. Rajendra D. Kanphade [16] proposed a DCT base reversible watermarking algorithm for military security application. The proposed watermarking method embeds the watermarking bits by modifying those DCT coefficients with high and medium frequency coefficients. This method is non-blind watermarking scheme developed to provide high security to the watermarked image. It provides strong robustness against geometric attacks. In this method they get very less PSNR (24.1 db) value as compared to other DCT methods.

Mrs. Rekha Chaturvedi, Mr. Abhay Sharma, Mr. Naveen Hemrajani, Mr. Dinesh Goyal [17] proposed blocked DCT based watermarking for colour images. This algorithm is based on average of middle-band coefficients of DCT domain. To make the algorithm robust against different attacks the random generator algorithm is used for embedding bit in coefficients. This method is robust for BMP image formats for different attacks. PSNR value they obtain is 42.09 which comparatively good as compared to other methods.

C. Discrete Wavelet transform: The wavelet based transform

The wavelet based transform follows same guidelines as the DCT, but the transforming method is different using filters so the coefficients in which the watermark is embedded are different. There are many filters available to transform the signal into wavelet based spectral coefficients. The filters used for this purpose can be a Haar Wavelet Filters, Daubechies Orthogonal Filters or Daubechies Bi-Orthogonal Filters [5]. Each filter decomposes the image into four frequency representations called LL, LH, HL and HH sub bands as shown in Fig 4.

In this section we discuss robust wavelet based watermarking algorithms. The summary of literature review is shown in Table 3.

Aree Ali Mohammed and Haval Mohammed Sidiqi [18] proposed a digital watermarking scheme based on multi wavelet transformation. The algorithm is developed to embed the watermark based on the bands selection criteria. The selection criteria are depends on the number of wavelet passes. In this algorithm they used three types of selection criteria to embed the watermark. This non-blind method get good correlation between the original watermark and extracted watermark for no. of pass = 3. The proposed
method is robust against JPEG compression, filtering, noises and geometric attacks but the disadvantage of this method is that it requires large no. of wavelet bands for watermark embedding. PSNR value by using this technique they obtain 38 db. Handapani Samiappan [19] proposed blind digital watermarking scheme based on Discrete Wavelet transformation. The algorithm is proposed to embed a binary watermark in the color image. The watermark is embedded in the sub band of the wavelet decomposition. To embed the watermark level 2 DWT is used. The watermark is embedded into the horizontal and diagonal coefficients of the DWT. This algorithm is robust against different attacks like JPEG compression, Gaussian filtering, median filtering, rotation and cropping. In this method the PSNR obtain by them are 38.6.

<table>
<thead>
<tr>
<th>Author and Year</th>
<th>Filter Used</th>
<th>Level</th>
<th>Wave- mark Embedded</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. A. Mohammed and H. M. Sidqi</td>
<td>9/7 Tap filter wavelet</td>
<td>3</td>
<td>Mid frequency bands</td>
<td>38</td>
</tr>
<tr>
<td>[18]</td>
<td>transfor m</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Samiappan and K. Ammasai</td>
<td>Not specified</td>
<td>2</td>
<td>All bands</td>
<td>38.6</td>
</tr>
<tr>
<td>[19]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Shaamala, S. M. Abdullah and A. A. Manaf [20]</td>
<td>2-level analysis filter bank</td>
<td>2</td>
<td>Not specified</td>
<td>-</td>
</tr>
<tr>
<td>Anuradha and R. P. Singh [21]</td>
<td>Haar wavelet</td>
<td>3</td>
<td>Low frequency bands</td>
<td>33.122</td>
</tr>
</tbody>
</table>

Table 3: Summary of DWT domain methods

Abduljabbar Shaamala, Shahidan M. Abdullah and Azizah A. Manaf [20] presents a comparison of a watermarking algorithm based on DCT and DWT. The proposed watermarking algorithm based on DCT is based on DC coefficients. The watermark bit is embedded in the DC coefficients of the image. To embed the watermark in the DWT domain two level of wavelet transformation they used. They studied the effect of the DCT and DWT on the robustness and the imperceptibility of the image. The DWT watermarking has good results with respect to DCT on the Imperceptibility and robustness of the watermarking. Anuradha, Rudresh Pratap Singh [21] proposed a robust watermarking algorithm based on DWT using 3rd level Haar wavelet. In this proposed method the gray-scale visual watermark is embedded in the low frequency coefficients of the Haar wavelet, since it provided better perceptibility of the watermark. The proposed algorithm has high fidelity and it robust to different attacks. The PSNR they obtain is 33.1224.

VI. ATTACKS ON DIGITAL WATERMARKING

The watermark attacks are classified as follows [9],[5]:

A. Simple attack:

These attacks are conceptually simple attacks which are done by manipulating whole watermarked image (Cover image plus watermark) without the intent to detect or destroy the watermark. ADC, DAC, filtering, compression, addition of noise, such kind of attacks come into this categories.

B. Geometric attack

Geometric attacks are intended to make difficult detection of watermark. It does not remove the watermark but it only makes the watermarked image such that the detector cannot extract the original watermark. Rotation, cropping, addition or deletions of row/column, zooming or shrinking are such type of attacks.

C. Ambiguity attacks

This type of attacks is intended to confuse the detector while detecting the watermark. In this type of attacks another more than one watermark are embedded into the watermarked image by another person to confuse the detector, which one is original. Such kinds of attacks are done by adding fake-watermarked image or fake watermark.

D. Forgery attacks

In this type of attacks, the hacker tries to insert its own valid watermark in place of original watermark. In such kinds of attacks hacker detects the original watermark and then it replaces this watermark by its own watermark.

VII. CONCLUSION AND FUTURE SCOPE

In this paper we have introduced some important concept of the watermarking including its characteristics, advantages, applications and different types of attacks on digital watermarking. After that common watermarking techniques are reviewed. Compared to spatial domain methods transform domain methods are more robust against different types of attacks. Transform domain methods are more secure as compared to spatial domain methods but the disadvantage of this method is that the watermarking bit capacity is less as compared to spatial domain methods. Due to space limitation we could not cover enough technical details about the different methods but we have tried to be as clear as possible. The future scope is that this watermarking technique can be further improved in terms of imperceptibility and also it will be possible to implement these techniques using DSP processor.

ACKNOWLEDGEMENT

I wish to express my deep gratitude to Mr. B. R. Patel, Assistant Professor, Electronics & Communication Engineering Department for providing his uncanny guidance and support throughout the preparation of this work. I am also thankful to Dr. V.K. Thakar, Head of Electronics & Communication Engineering Department, for the motivation and inspiration that triggered me to this work. I would also like to thank all the staff members and my co-
students who were always there at the need of the hour and provided with all the help and facilities, which I required for the completion of this work.

REFERENCES


All rights reserved by www.ijsrd.com 2890