DIGITAL IMAGE WATERMARKING TECHNIQUES: A DETAILED REVIEW

Jyoti Kumari¹, Ankit²,

¹M. Tech Scholar, Department of Electronics and Communication, CBS Group of Institutions, Jhajjar
(Maharshi Dayanand University, Rohtak)
Haryana, India

²Assistant Professor, Department of Electronics and Communication, CBS Group of Institutions, Jhajjar
(Maharshi Dayanand University, Rohtak)
Haryana, India

Abstract
Digital Watermarking, a concept of data hiding has been subjected to lot of research and studies in past few years. A lot of work has been done in this field since its emergence. Image watermarking techniques have wide range of application in present world some of them are content protection, audience measurement, copyright management, content authentication and tamper detection. In this paper we present a detailed survey of DCT based watermarking. We classify the techniques based on different domains in which data is embedded. Here we limit the survey to images only.
Keywords: Watermarking, Watermark Detection, Spatial Domain, Image Transforms, DWT, DCT, DFT

1. Introduction
Digital Watermarking is a newly developed and an efficient technique to hide information used to encrypt text, images, audio, video etc. As the digital contents can be disseminated easily over internet, this has caused serious copyright violation issues.[1] Hence it matters of concern for the digital content providers. These contents could be encrypted using digital image watermarking technique. In this paper we detail about DCT watermarking used to watermark the image. Digital videos could also be encrypted using digital watermarking techniques. However, this paper is restricted to image watermarking domain sonly [2]. In this paper we have discussed about prerequisites of digital image watermarking, some major applications of watermarking. Further we have discussed DCT based digital watermarking, advantages and disadvantages of DCT based image watermarking as compared to other methods. We have also discussed about future scope of this technology [3].

Digital watermarking is a newly developed technique widely used in which a multimedia information is encrypted using watermark which can be extracted to make certainty about multimedia information [4]. This can be further classified as visible and invisible watermarks. For example, visible watermarking is the logo visible super-imposed on the corner of television channel in a television picture [5]. In other way, invisible watermark is hidden in the object, which can be detected by an authorized person. Such watermarks are used for suit the author authentication and detecting unauthorized copying. Protection of copyright has emerged as serious issue due to easy sharing of contents on internet. Digital watermarking technology protects the interests of content owners by encrypting different multimedia information using watermarking [6].

2. Prerequisites of Digital Watermarking
Fidelity

It should be ensured that watermark should not affect the image after encryption of digital watermark into it [7]. According to Cox et al. (2002) transparency or fidelity could be defined as “perceptual similarity between the original and the watermarked versions of the cover work” [8]. After watermarking the visible distortion of image should be avoided to retain commercial value of watermarked image [9].
Robustness

According to Cox et al. (2002) robustness could be defined as the "ability to detect the watermark after common signal processing operations" [10]. Digital watermark i.e., encryption could be removed easily to get original image by performing simple operations like contrast or brightness enhancement, gamma correction etc. over it [11]. Hence watermark should be safe against such things [12]. The attacks over digital watermark can be enlisted under four categories, attacks that try to erase watermarks completely, attacks that intend to erase the synchronization among the embedder and the detector, cryptographic attacks and protocol attacks [13].

Data Payload

According to Cox et al. (2002) capacity or data payload could be defined as "the number of bits a watermark encodes within a unit of time or work" [14]. This characteristic is about amount of data to be encrypted so that image could be retained successfully [15]. Watermark must carry enough information so that uniqueness of image is retained. Payload information varies depending upon the different applications of digital watermarking [16].

3. Applications of watermarking

Some of the major applications of Digital image watermarking are are explained below:

Copyright Protection

Watermarking is used to secure the distribution of copyrighted material of content owners over widely used insecure networks like internet [17]. Networks should use watermarking encryption to sort out or retain digital copyrighted contents [18].

Content Archiving

Watermarking could be used to indexing or serialise the image and other multimedia files in order to archive them [19]. It can also be used for classification and organization of digital contents. Usually, digital contents are recognized by their file names; however, this is a very fragile technique as file names can be changed easily [20]. Hence encrypting the object identifier inside the object, itself diminishes the probability of tampering and hence this way easily used for archiving [21].

Broadcast Monitoring

Broadcast monitoring is the technique used ensure whether the contents intended to be broadcasted over TV or radio are broadcasted or not. Digital Watermarking has emerged as powerful technique to perform this [22]. It is used widely by the commercial advertisers to ensure that their advertisement was run properly at right time and right duration of time by the broadcasters [23].

Meta-data Insertion

Meta data is the term defined for data which describes any other data. Contents could be labeled inside the image and could be search engines [24]. Lyrics or other useful things could be inserted inside the audio songs [25]. Cover story or headline of the news could be inserted inside the image by journalists. Records of the patient could be embedded within the X-ray or MRI reports [26].

4. DCT Based Watermarking

The Discrete Cosine Transform (DCT) is a technique based on spatial domain and digital image watermarking in order to transform the data. Evolved from discrete fourier transform discrete cosine transform represents data in terms of frequency space in place of an amplitude space [27]. The spatial domain technique can be changed into the frequency domain, and the frequency domain technique can be transformed back again to the spatial domain by using inverse discrete cosine transform. The discrete cosine transform (DCT) is a technique for converting a signal into effortless frequency components. The image is represented as a sum of sinusoids of varying magnitudes and frequencies [28]. DCT only has orthogonal transformation of a real number. This is far better than discrete Fourier transform, in which we have to compute the image as part of a complex number. A DCT transformation matrix has a symmetrical coefficient matrix with the same summation between every auxiliary diagonal, which is parallel to a diagonal. DCT is provided by extracted items with cosine in discrete Fourier
transform. It has major advantages such as high-compression ratio, high-computational complexity, and lower error rate, as compared to others [29].

5. Pros and Cons of DCT based Watermarking

Pros
a) Semantically useful watermark pattern.
b) Better perceptual invisibility.
c) Robustness at acceptable level.
d) Different user-customized objectives.
e) Reasonable complexity/execution time.
f) Swift and Suitable for robustness against JPEG compression.

Cons
a) Block wise DCT hampers the properties of invariance of the system.
b) Certain higher frequency components tend to be suppressed during the quantization step.

6. Conclusion
From the above discussion it can be concluded conveniently that digital image watermarking is very useful technique in present times for various purposes such as protection of intellectual property rights of digital content owners in the age of unsafe networks like internet. It is also used for meta-data insertion, broadcast monitoring and many more purposes. It can be also concluded that Discrete Cosine transformation is one of the best compatible ways to embed a watermark inside an image as compared to other technologies such as Discrete Fourier Transformation used for this purpose [30].

7. Further Scope
There is huge potential of future work in this newly developed technique, this technique is still applicable for images only but it technique can also developed for audio, videos because it is known to us that audio could also represented as frequency distribution also video is collection of different image frames hence watermark could be easily embedded inside them to serve the same purpose as in case of image watermarking.

References


