# A Survey of Digital Image Watermarking Techniques

Vidyasagar M. Potdar, Song Han, Elizabeth Chang

School of Information Systems, Curtin University of Technology, Perth, Western Australia
e-mail: Vidyasagar.Potdar, Song.Han, Elizabeth.Chang@cbs.curtin.edu.au

*Abstract* — **Watermarking, which belong to the information hiding field, has seen a lot of research interest recently. There is a lot of work begin conducted in different branches in this field. Steganography is used for secret communication, whereas watermarking is used for content protection, copyright management, content authentication and tamper detection. In this paper we present a detailed survey of existing and newly proposed steganographic and watermarking techniques. We classify the techniques based on different domains in which data is embedded. Here we limit the survey to images only.**

*Index Terms*— **Watermarking, Watermark Detection, Spatial Domain, Image Transforms, DWT, DCT, DFT.**

## I. INTRODUCTION

Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Copyrighted material can be easily exchanged over peer-to-peer networks, and this has caused major concerns to those content providers who produce these digital contents. In order to protect the interest of the content providers, these digital contents can be watermarked. In this paper we provide a survey of the latest techniques that are employed to watermark images. Image watermarking techniques can be applied to digital videos as well. However, in this paper we limit our self to the image domain. The paper is organized in the following sections. In Section II we describe digital watermarking process. In Section III we identify the main requirements of image watermarking. In Section IV we discuss the main application of watermarking. In Section V we provide a detailed survey of image watermarking techniques. We conclude this paper in section VI where we give some guidelines on developing robust watermarking algorithms.

## II. DIGITAL WATERMARKING TECHNIQUE

The process of *embedding* a *watermark* in a *multimedia object*[1] is termed as watermarking. Watermark can be considered as a kind of a signature that reveals the owner of the multimedia object. Content providers want to embed watermarks in their multimedia objects (digital content) for several reasons like copyright protection, content authentication, tamper detection etc. A watermarking algorithm embeds a *visible* or *invisible watermark* in a given multimedia object. The embedding process is guided by use of a *secret key* which decided the locations within the multimedia object (image) where the watermark would be embedded. Once the watermark is embedded it can experience several *attacks* because the multimedia object can be digitally processed. The attacks can be unintentional (in case of images, low pass filtering or gamma correction or compression) or intentional (like cropping). Hence the watermark has to be very robust against all these possible attacks. When the owner wants to check the watermarks in the possibly attacked and distorted multimedia object, s/he relies on the secret key that was used to embed the watermark. Using the secret key, the embedded watermark sequence can be extracted. This extracted watermark may or may not resemble the original watermark because the object might have been attacked. Hence to validate the existence of watermark, either the original object is used to compare and find out the watermark signal (*non-blind watermarking*) or a correlation measure is used to detect the strength of the watermark signal from the extracted watermark (*blind watermarking*). In the correlation based detection the original watermark sequence is compared with the extracted watermark sequence and a statistical correlation test is used to determine the existence of the watermark.

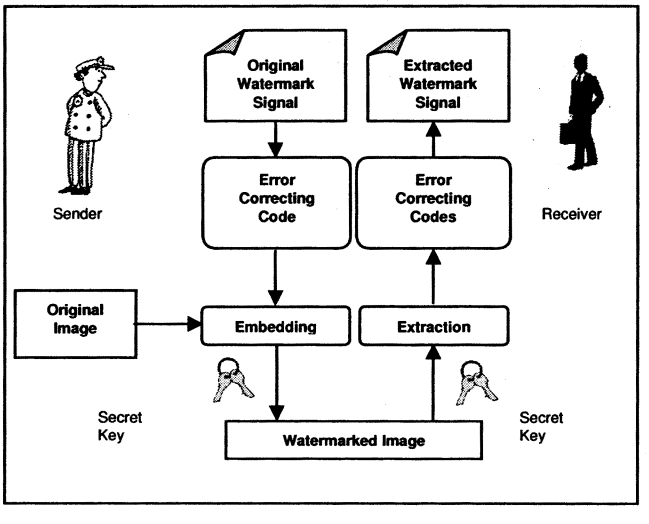


**Fig.1 Watermarking Technique**

## III. REQUIREMENTS OF DIGITAL WATERMARKING

There are three main requirements of digital

[1] Multimedia object refers to images, video and audio clips or any digital content that can be used for the purpose of information hiding.

watermarking. They are *transparency*, *robustness*, and *capacity*.

### A. Transparency or Fidelity

The digital watermark should not affect the quality of the original image after it is watermarked. Cox et al. (2002) define transparency or fidelity as "perceptual similarity between the original and the watermarked versions of the cover work". Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

### B. Robustness

Cox et al. (2002) defines robustness as the "ability to detect the watermark after common signal processing operations". Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks. Stirmark[2] classifies attacks into four basic categories, attacks that try to remove watermarks totally, attacks that try to remove the synchronization between the embedder and the detector, cryptographic attacks and protocol attacks.

### C. Capacity or Data Payload

Cox et al. (2002) define capacity or data payload as "the number of bits a watermark encodes within a unit of time or work". This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark should be able to carry enough information to represent the uniqueness of the image. Different application has different payload requirements [1].

## IV. Watermarking Applications

Before beginning the discussion on watermarking algorithms we discuss the applications. The main applications of digital watermarking are discussed here.

### A. Copyright Protection

Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.

### B. Content Archiving

Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a very fragile technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems.

### C. Meta-data Insertion

Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records.

### D. Broadcast Monitoring

Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. This has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

### E. Tamper Detection

Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.

### F. Digital Fingerprinting

Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital content. Hence a single digital object can have different fingerprints because they belong to different users

## V. Watermarks and Watermark Detection

Basically there are three main types of watermarks that can be embedded within an image.

### A. Pseudo-Random Gaussian Sequence

A Gaussian sequence watermark is a sequence of numbers comprising 1 and -1 and which has equal number of 1's and -1's is termed as a watermark. It is termed as a watermark with zero mean and one variation. Such watermarks are used for objective detection using a correlation measure.

### B. Binary Image or Grey Scale Image Watermarks

Some watermarking algorithms embed meaningful data in form of a logo image instead of a pseudo-random gaussian sequence. Such watermarks are termed as binary image watermarks or grey scale watermarks. Such watermarks are used for subjective detection.

[2] Stirmark is a benchmark to test robustness of watermarking algorithms. http://www.petitcolas.net/fabien/watermarking/stirmark

Based on the type of watermark embedded, an appropriate decoder has to be designed to detect the presence of watermark.

If it's a pseudo random gaussian sequence hypothesis, testing is done to detect the presence of watermark. Suppose $W$ is the original watermark bit sequence and $W'$ is the extracted watermark bit sequence, then we can calculate *bit error rate* (BER) to detect the presence of watermark. If the BER is zero it indicates the presence of watermark; however, if it is one, it indicates absence of watermark. BER is calculated as follows. Suppose D is the retrieved signal and N is the number of bits in watermark then:

$$D = \begin{Bmatrix} 1 \ if \ W_i \neq W_i' \\ 0 \ if \ W_i = W_i' \end{Bmatrix} \qquad BER(W,W') = \frac{\sum D}{N}$$

*Normalized Correlation Coefficient* can also be used to detect the presence of watermark.

$$NC(W,W') = \frac{\sum W\,W'}{\sqrt{\sum W_i^2}\,\sqrt{\sum W_i'^2}}$$

## VI. Image Watermarking Survey

Within the field of watermarking, image watermarking has attracted a lot of attention in the research community for two reasons. Firstly, because of its ready availability, and secondly because it carriers enough redundant information that could be used to embed watermarks.

Images can be represented in spatial domain and transform domain. The transform domain image is represented in terms of its frequencies; however, in spatial domain it is represented by pixels. In simple terms transform domain means the image is segmented into multiple frequency bands. To transfer an image to its frequency representation we can use several reversible transform like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), or Discrete Fourier Transform (DFT). Each of these transforms has its own characteristics and represents the image in different ways.

Watermarks can be embedded within images by modifying these values, i.e. the pixel values or the transform domain coefficients. Simple watermarks could be embedded in the spatial domain of images by modifying the pixel values or the least significant bit (LSB) values; however, more robust watermarks could be embedded in the transform domain of images by modifying the transform domain coefficients. Since robust watermarking has many applications we would limit this survey towards robust watermarking algorithms.

In this paper we would discuss robust watermarking algorithm within the DCT, DWT and DFT domain. We begin our discussion with DCT based robust watermarking algorithms.

## VII. DCT Domain Watermarking

DCT based watermarking techniques are more robust compared to simple spatial domain watermarking 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.

DCT domain watermarking can be classified into *Global* DCT watermarking and *Block based* DCT watermarking. One of the first algorithms presented by Cox et al. (1997) used global DCT approach to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS). Embedding in the perceptually significant portion of the image has its own advantages because most compression schemes remove the perceptually insignificant portion of the image. In spatial domain it represents the LSB however in the frequency domain it represents the high frequency components [3]. The main steps of any block based DCT algorithm are shown in Fig.2.

Steps in DCT Block Based Watermarking Algorithm
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 (e.g. HVS)*
4) *Apply coefficient selection criteria (e.g. highest)*
5) *Embed watermark by modifying the selected coefficients.*
6) *Apply inverse DCT transform on each block*

**Fig.2 Block based DCT Watermarking**

Most algorithms discussed in this section are classified based on step 3 and 4 i.e. the main difference between most algorithms is that they differ either in the block selection criteria or coefficient selection criteria. Based on the perceptual modeling strategy incorporated by the watermarking algorithms they could be classified as algorithms with:

### A. *No Perceptual Modeling*

Such algorithms do not incorporate any perceptual modeling strategy while embedding a watermark.

| Name of the Author | Year | Embedding Type | Watermark type | Transform Domain | Embedding Location |
|---|---|---|---|---|---|
| Noore [33] | 2003 | Additive | Binary Image | Modified DCT | Not Specified |
| Fotopoulos and Skodras [34] | 2000 | Additive | Not Specified | Subband DCT | Not Specified |

**Fig.3 List of Block based DCT Algorithms without any Perceptual Modeling**

### B. *Implicit Perceptual Modeling*

Such algorithms incorporate the transform domain properties for perceptual modeling. The coefficient selection criterion is as follows:

1) Select those transform coefficients which have large perceptual capacity, because they allow stronger watermarks to be embedded and result in least perceptual distortion [39]. DC component satisfy this criteria and hence can be used.
2) Select only those coefficients which are least changed by common image processing attacks like low-pass filtering, noise addition etc [39]. Low frequency AC components (or high magnitude coefficients) as well as high magnitude DC components satisfy the above criteria and can be selected.
3) High frequency components are affected by common image processing operations hence they are not a good choice for watermarking.

These are some of the selection criterion adopted by the algorithms listed in Fig.4.

| Name of the Author | Year | Embedding Type | Watermark type | Watermark Detection | Embedding Location |
|---|---|---|---|---|---|
| Choi and Aizawa [35] | 2002 | Additive | Gaussian Vector | Correlation | Luminance Domain |
| Suhail and Obaidat [36] | 2003 | Additive | Gaussian Vector | Correlation | Not Specified |
| Golikeri and Nasiopoulos [37] | 2004 | Additive | Gaussian Vector | Correlation | Luminance Domain |

**Fig.4 List of Block based DCT Algorithms using Implicit Perceptual Modeling**

### C. *Explicit Perceptual Modeling*

Such algorithms incorporate the HVS properties for perceptual modeling. HVS models allow us to raise or lower the strength of the watermark because it takes into account the local image properties like contrast, brightness, variance etc.

| Name | Embedding Type | Perceptual Modeling Strategy | Watermark Type | Watermark Detection | Embedding Location |
|---|---|---|---|---|---|
| Tao [15] | Additive | Regional Classifier | Not Specified | Correlation | Luminance Domain |
| Hsu [38] | Additive | Frequency Classifier | Gaussian Vector | Correlation | Mid Frequency |
| Huang et al. [39] | Additive | Luminance Texture Masking | Gaussian Vector | Correlation | DC Component |
| Wong et al. [40] | Additive | Bandpass Filtering | Gaussian Vector | Correlation | DC Component |

**Fig.5 List of Block based DCT Algorithms using Explicit Perceptual Modeling**

Hence only those coefficients are selected and modified which satisfy the HVS criterion. Some of these algorithms which adopt the HVS are listed in Fig.5.

## VIII. DWT Domain Watermarking

In the last few years wavelet transform has been widely studied in signal processing in general and image compression in particular. In some applications wavelet based watermarking schemes outperforms DCT based approaches. One such scheme is proposed here [4]. Hence it makes it an important topic for research.

### A. *Characteristics of DWT*

1) The wavelet transform decomposes the image into three spatial directions, i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely [41].
2) Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution.
3) Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL) [42].
4) The larger the magnitude of the wavelet coefficient the more significant it is.
5) Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved.
6) High resolution subbands helps to easily locate edge and textures patterns in an image.

### B. *Advantages of DWT over DCT*

1) Wavelet transform understands the HVS more closely than the DCT.
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.
3) Visual artifacts introduced by wavelet coded images are less evident compared to DCT because wavelet transform doesn't decompose the image into blocks for processing. At high compression ratios blocking artifacts are noticeable in DCT; however, in wavelet coded images it is much clearer.
4) DFT and DCT are full frame transform, and hence any change in the transform coefficients affects the entire image except if DCT is implemented using a block based approach. However DWT has spatial frequency locality, which means if signal is embedded it will affect the image locally [43]. Hence a wavelet transform provides both frequency and spatial description for an image.

### C. *Disadvantages of DWT over DCT*

1) Computational complexity of DWT is more compared to DCT [44]. As Feig (1990) pointed out it only takes 54 multiplications to compute DCT for a block of 8x8, unlike wavelet calculation depends upon the length of the filter used, which is at least 1 multiplication per coefficient [45].

### D. *DWT watermarking*

DWT based watermarking schemes follow the same guidelines as DCT based schemes, i.e. the underlying concept is the same; however, the process to transform the image into its transform domain varies and hence the resulting coefficients are different. Wavelet transforms use wavelet filters to transform the image. There are many available filters, although the most commonly used filters for watermarking are Haar Wavelet Filter, Daubechies Orthogonal Filters and Daubechies Bi-Orthogonal Filters. Each of these filters de-

composes the image into several frequencies. Single level decomposition gives four frequency representations of the images. These four representations are called the LL, LH, HL, HH subbands as shown in Fig.6.

In this section we discuss wavelet based watermarking algorithms. We classify these algorithms based on their decoder requirements as Blind Detection or Non-blind Detection. As mentioned earlier blind detection doesn't require the original image for detecting the watermarks; however, non-blind detection requires the original image.

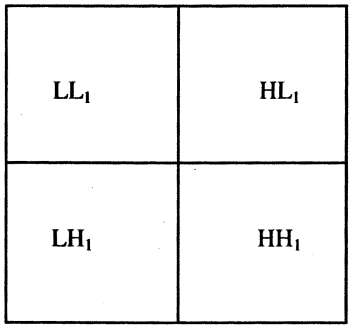


**Fig.6 Single level Decomposition using DWT**

### *E. DWT based Blind Watermark Detection*

Lu et al. (1999) present a novel watermarking technique called as "Cocktail Watermarking". This technique embeds dual watermarks which compliment each other. This scheme is resistant to several attacks, and no matter what type of attack is applied, one of the watermarks can be detected. Furthermore, they enhance this technique for image authentication and protection by using the wavelet based just noticeable distortion (JND) values. Hence this technique achieves copyright protection as well as content authentication simultaneously [6].

Zhu et al. (1999) present a multi-resolution watermarking technique for watermarking video and images. The watermark is embedded in all the high pass bands in a nested manner at multiple resolutions. This technique doesn't consider the HVS aspect; however, Kaewkamnerd and Rao [8, 9] improve this technique by adding the HVS factor in account.

Voyatzis and Pitas (1999), who presented the "toral automorphism" concept, provide a technique to embed binary logo as a watermark, which can be detected using visual models as well as by statistical means. So in case the image is degraded too much and the logo is not visible, it can be detected statistically using correlation. Watermark embedding is based on a chaotic (mixing) system. Original image is not required for watermark detection. However, the watermark is embedded in spatial domain by modifying the pixel or luminance values. A similar approach is presented for the wavelet domain [11], where the authors propose a watermarking algorithm based on chaotic encryption.

Zhao et al. (2004) presents a dual domain watermarking technique for image authentication and image compression. They use the DCT domain for watermark generation and DWT domain for watermark insertion. A soft authentication watermark is used for tamper detection and authentication while a chrominance watermark is added to enhance compression. They use the orthogonality of DCT-DWT domain for watermarking [12].

### *F. DWT based Non-Blind Watermark Detection*

This technique requires the original image for detecting the watermark. Most of the techniques found in literature use a smaller image as a watermark and hence cannot use correlation based detectors for detecting the watermark; as a result they rely on the original image for informed detection. The size of the watermark image (normally a logo) normally is smaller compared to the host image.

Xia et al. (1997) present a wavelet based non-blind watermarking technique for still images where watermarks are added to all bands except the approximation band. A multi-resolution based approach with binary watermarks is presented here [Hsu and Wu 1998]. Here both the watermark logo as well as the host image is decomposed into sub bands and later embedded. Watermark is subjectively detected by visual inspection; however, an objective detection is employed by using normalized correlation.

Lu et al. (2001) present another robust watermarking technique based on image fusion. They embed a grayscale and binary watermark which is modulated using the "toral automorphism" described in [10]. Watermark is embedded additively. The novelty of this technique lies in the use of secret image instead of host image for watermark extraction and use of image dependent and image independent permutations to de-correlate the watermark logos [31]. Raval and Rege (2003) present a multiple watermarking technique. The authors argue that if the watermark is embedded in the low frequency components it is robust against low pass filtering, lossy compression and geometric distortions. On the other hand, if the watermark is embedded in high frequency components, it is robust against contrast and brightness adjustment, gamma correction, histogram equalization and cropping and vice-versa. Thus to achieve overall robustness against a large number of attacks the authors propose to embed multiple watermarks in low frequency and high frequency bands of DWT [16].

Kundur and Hatzinakos (1997) present image fusion watermarking technique. They use salient features of the image to embed the watermark. They use a saliency measure to identify the watermark strength and later embed the watermark additively. Normalized correlation is used to evaluate the robustness of the extracted watermark. Later the authors propose another technique termed as FuseMark [18], which includes minimum variance fusion for watermark extraction. Here they propose to use a watermark image whose size is a factor of the host by 2xy.

Tao and Eskicioglu (2004) present an optimal wavelet based watermarking technique. They embed binary logo watermark in all the four bands. But they embed the watermarks with variable scaling factor in different bands. The scaling factor is high for the LL sub band but for the other three bands its lower. The quality of the extracted watermark is determined by Similarity Ratio measurement for objective calculation [19].

| Name | Filter Used | Level | Embedding Type | Water mark type | Watermark Embedded |
|---|---|---|---|---|---|
| **DWT Based Non-Blind Watermarking Algorithms** | | | | | |
| Ganic and Eskicioglu 2005 | Haar | 1 | Additive | Grey Scale Image | High and Low pass bands |
| Tao and Eskicioglu 2004 | Haar | 2 | Additive | Binary Image | All Bands |
| Kundur and Hatzinakos 2004 | Daubechies 10 pt wavelet | 3 | Additive | Gray Scale Image | High ass bands |
| Raval and Rege 2003 | Not Specified | 2 | Additive | Binary Image | 2nd Level LL and HH bands |
| Kang et al.2003 | Daubechies 9/7 biorthogonal | 3 | Additive BCH (61, 8), 2D Interleaving | Gaussian Vector | Low pass LL |
| Hsieh and Wu 2001 | Not Specified | 3 | Additive | Gaussian Vector | High and Low pass bands |
| Niu et al. 2000 | Not Specified | 3 | Additive | Grey Scale Image | Not Specified |
| Hsu and Wu 1998 | Daubechies tap-6 | Multi | Neighboring Relationship | Binary Logo | Not Specified |
| Chae and Manjunath 1998 | Haar | 1 | Additive | Gray Scale Image | Not Specified |
| Xia et al. 1998 | Haar | Multi | Additive | Gaussian Vector | High pass bands |
| Xia at al. 1997 | Haar | 2 | Additive | Gaussian Vector | High pass bands |
| Kundur and Hatzinakos 1997 | Not Spec. | 4 | Additive | Binary Image | Low Pass Bands |
| **DWT Based Blind Watermarking Algorithms** | | | | | |
| Xiao et al. 2002 | Not Spec. | Not Spec. | Additive | Gaussian Vector | Mid Freq Component |
| Kaewkamnerd 2001 | Quadrature Mirror | Multi | Additive | Gaussian Vector | High pass bands |
| Kaewkamnerd 2000 | Quadrature Mirror | 4 | Additive | Gaussian Vector | High pass bands |
| Lu et al. 1999 | Not Spec. | Not Spec. | Additive | Binary and Grey scale Image | Visually Significant Coef. |
| Zhu et al. 1999 | Not Spec. | Multiple | Additive | Gaussian Vector | High pass bands |
| Kundur and Hatzinakos 1998 | Daubechies 10 pt wavelet | Not Spec. | Additive | Binary Watermark {-1,1} | High pass bands |

**Fig.7 List of DWT based Blind and Non-Blind Watermarking Algorithms**

Ganic and Eskicioglu (2005) inspired by Raval and Rege (2003) propose a multiple watermarking technique based on DWT and Singular Value Decomposition (SVD). They argue that the watermark embedded by Raval and Rege (2003) scheme is visible in some parts of the image especially in the low frequency areas, which reduces the commercial value of the image. Hence they generalize their technique by using all the four sub bands and embedding the watermark in SVD domain. The core technique is to decompose an image into four sub bands and then applying SVD to each band. The watermark is actually embedded by modifying the singular values from SVD [20]. Fig. 6 gives complete technical details of the parameters used in these algorithms.

## IX. DFT Domain Watermarking

DFT domain has been explored by researches because it offers robustness against geometric attacks like rotation, scaling, cropping, translation etc. In this section we discuss some watermarking algorithms based on the DFT domain.

### *A. Characteristics of DFT*

1) DFT of a real image is generally complex valued, which results in the phase and magnitude representation of an image.
2) DFT shows translation invariance. Spatial shifts in the image affects the phase representation of the image but not the magnitude representation [21], or circular shifts in the spatial domain don't affect the magnitude of the Fourier transform.
3) DFT is also resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, which are normalized coordinates, there is no need of any synchronization [21].
4) The strongest components of the DFT are the central components which contain the low frequencies.
5) Scaling of image results in amplification of extracted signal and can be detected by correlation coefficient. Translation of image has no result on extracted signal.
6) Rotation of image results in cyclic shifts of extracted signal and can be detected by exhaustive search [21]
7) Scaling in the spatial domain causes inverse scaling in the frequency domain. Rotation in the spatial domain causes the same rotation in the frequency domain [22].

### *B. Coefficient Selection Criteria*

1) Modification to the low frequency coefficients can cause visible artifacts in the spatial domain [21, 22]. Hence, low frequency coefficients should be avoided
2) High frequency coefficients are not suitable because they are removed during JPEG compression [21, 22].
3) The best location to embed the watermark is the mid frequency [21, 22].

### *C. Advantages of DFT over DWT and DCT*

1) DFT is rotation, scaling and translation (RST) invariant. Hence it can be used to recover from geometric distortions, whereas the spatial domain, DCT and the DWT are not RST invariant and hence it is difficult to overcome from geometric distortions.

Literature shows two different kinds of DFT based watermark embedding techniques. One in which watermark is directly embedded or template based embedding. We discuss each of these techniques in detail in this section.

### *D. Direct Embedding*

There are few algorithms that modify these DFT magnitude and phase coefficients to embed watermarks. Ruanaidh et al. (1996) proposed a DFT watermarking technique in which watermark is embedded by modifying the phase information within the DFT. It has been shown that phase based watermarking is robust against image contrast operation [23]. Later Ruanaidh and Pun (1998) showed how Fourier Mellin transform can be used for digital watermarking. Fourier Mellin transform is similar to applying Fourier Transform to log-polar coordinate system for an image. This scheme is robust against RST attacks [24].

De Rosa et al. (1999) propose a scheme to insert watermark by directly modifying the mid frequency bands of the DFT magnitude component [25]. Ramkumar et al. (1999) also present a data hiding scheme based on DFT, where they modify the magnitude component of the DFT coefficients. Their simulations suggest that magnitude DFT survives practical compression, and this can be attributed to the fact that most practical compression schemes try to maximize the PSNR. Hence using magnitude DFT is a way to exploit the hole in most practical compression schemes. The proposed technique is shown to be resistant to JPEG and SPIHT compression [26].

Lin et al. (2001) present a RST resilient watermarking algorithm. The watermark is embedded in the magnitude coefficients of the Fourier transform re-sampled by log-polar mapping. The technique is however not robust against cropping and shows weak robustness against JPEG compression (QF 70) [27].

Solachidis and Pitas (2001) present a novel watermarking technique. They embed a circularly symmetric watermark in the magnitude of the DFT domain [22]. Since the watermark is circular in shape with its centre at image centre it is robust against geometric rotation attacks. The watermark is centered around the mid frequency region of the DFT magnitude. Neighborhood pixel variance masking is employed to reduce any visible artifacts. The technique is computationally not expensive to recover from rotation. Robustness against cropping, scaling, JPEG compression, filtering, noise addition and histogram equalization is demonstrated.

A semi-blind watermarking technique has been proposed by Ganic and Eskicioglu (2004). They embed circular watermarks with one in the lower frequency while the other is in the higher frequency. Their work is inspired by [16]. They follow the same argument as that endorsed by embedding watermarks in the low frequency component, which is robust against one set of attacks, while embedding in the high frequency components is robust to another set of attacks.

### *E. Template based Embedding*

Pereira and Pun (2000) propose robust watermarking algorithm resistant to affine transformations. They introduce the concept of Template. A template is a structure which is embedded in the DFT domain to estimate the transformation factor. Once the image undergoes a transformation this template is searched to resynchronize the image, and then use the detector to extract the embedded spread spectrum watermark [21].

## X. FFT AND DHT DOMAIN WATERMARKING

Pereira et al. (1999) present a watermarking algorithm based on FFT that is robust against compression and RST attacks. It is a template based embedding algorithm similar to the one discussed in the previous section. Apart from the template, an informative watermark is embedded to prove ownership. In case the image undergoes a geometric distortion the template is reversed back to its original location and then the watermark is extracted. They employ the concept of log-polar maps and log-log maps to recover the hidden template. This technique is shown to be robust against cropping, print and scan attack; however, it is very difficult to implement [28].

DHT based watermarking techniques rely on the Discrete Hadamard Transform. Falkowski and Lim (2000) propose a watermarking technique based on multi-resolution transform and complex Hadamard transform [30]. Initially the multi-resolution Hadamard transform is applied to the image to decompose it into various frequency bands like low-low, low-high and high-high. The lowest frequency band is then divided into 8x8 blocks and 2D complex Hadamard transform is applied. Watermark is embedded in this domain by altering the phase component of the most significant image component. The watermark is embedded in the phase component because phase modulation is more robust to noise than amplitude modulation. The proposed scheme is shown to be robust against several attacks like JPEG compression (10% quality factor), image scaling at 56.25%, dithering, cropping and successive watermarking. It's a non-blind watermarking algorithm.

Another watermarking technique proposed by Gilani and Skodras (2001), embeds the watermark by modifying the high frequency Hadamard coefficients. An image undergoes double frequency transform initially by Haar Wavelet Transform and later by Hadamard Transform. This gives rise to the multi-resolution Hadamard Frequency domain. The Hadamard transform concentrates most of the energy in the upper left corner, and hence it is selected to embed watermark information. The authors argue that high frequency bands of Hadamard transform are robust against noise and hence can resist JPEG compression attacks at a low quality factor [29].

## XI. CONCLUSION

In this paper we surveyed the current literature on digital image watermarking. We classified watermarking algorithms based on the transform domain in which the watermark is embedded. Due to the space limitation we couldn't cover enough technical details but we have tried to be as clearer as possible.

## XII. REFERENCES


[1] Cox, IJ, Miller, ML & Bloom, JA 2002, Digital Watermarking, Morgan Kaufmann Publisher, San Francisco, CA, USA.

[2] I.J Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia" in *IEEE Transactions on Image Processing*, vol. 6, no. 12, Dec.1997, pp:1673 -1687

[3] Guan-Ming Su, "An Overview of Transparent and Robust Digital Image Watermarking". Available online at www.watermarkingworld.org/WMMLArchive/0504/pdf00000.pdf

[4] Kundur. D., Hatzinakos, D., "Digital Watermarking using Multiresolution Wavelet Decomposition", Proc. *IEEE Int. Conf. On Acoustics, Speech and Signal Processing*, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.

[5] Lu, C-S., Liao, H-Y., M., Huang, S-K., Sze, C-J., "Cocktail Watermarking on Images", 3rd International Workshop on Information Hiding, Dresden, Germany, Sep 29-Oct. 1, 1999

[6] Lu, C-S., Liao, H-Y., M., Huang, S-K., Sze, C-J., "Combined Watermarking for Images Authentication and Protection", in *1st IEEE International Conference on Multimedia and Expo,* vol. 3, 30 July-2 Aug. 2000 pp. 1415 - 1418

[7] Zhu, W., Xiong, Z., and Zhang, Y.-Q., "Multiresolution Watermarking for Images and Video", in *IEEE Trans. on circuit and System for Video Technology*, vol. 9, no. 4, pp. 545-550, June, 1999.

[8] Kaewkamnerd, N., Rao, K.R., "Multiresolution based image adaptive watermarking scheme", in *EUSIPCO*, Tampere, Finland, Sept. 2000. Available online www.ee.uta.edu/dip/paper/EUSIPCO_water.pdf Accessed on June 1, 2005

[9] Kaewkamnerd, N., Rao, K.R., "Wavelet based image adaptive watermarking scheme" in *IEE Electronics Letters*, vol.36, pp.312-313, 17 Feb.2000

[10] Voyatzis, G., Pitas, I., "Digital Image Watermarking using Mixing Systems", in *Computer Graphics, Elsevier*, vol. 22, no. 4,pp. 405-416, August 1998

[11] Xiao, W., Ji, Z., Zhang, J., Wu, W., "A watermarking algorithm based on chaotic encryption", in *Proceedings of IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering TENCON*, vol. 1, pp. 545-548, 28-31 Oct. 2002

[12] Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", in *IEEE Transactions on Image Processing*, vol. 13, no. 3, pp. 430-448, March 2004.

[13] Xie, L., Boncelet, G., Acre, G.R., "Wavelet transform based watermarking for digital images", in *Optics Express*, vol. 3, no. 12, Dec 1998

[14] Hsu, C.-T., Wu, J.-L., "Multiresolution Watermarking for Digital Images", *in IEEE Transactions on Circuits and Systems – II: Analog and Digital Signal Processing*, vol. 45, no. 8, pp. 1097-1101, August 1998

[15] Tao, B., Dickinson, B., "Adaptive Watermarking in DCT Domain", in *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP '97*, 1997, Vol.4, pp.1985-2988.

[16] Raval, M.S., Rege, P.P., "Discrete wavelet transform based multiple watermarking scheme", Conference on Convergent Technologies for Asia-Pacific Region, TENCON 2003, vol. 3, pp. 935 – 938, 15-17 Oct. 2003

[17] Kundur. D., Hatzinakos, D., "Digital Watermarking using Multiresolution Wavelet Decomposition", in *Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing*, Seattle, Washington, vol. 5, pp. 2969-2972, May 1998.

[18] Kundur. D., Hatzinakos, D., "Towards Robust Logo Watermarking using Multiresolution Image Fusion," *IEEE Transactions on Multimedia,* vol. 6, no. 1, pp. 185-198, February 2004

[19] Tao, P & Eskicioglu, AM 2004, 'A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain', in Symposium on Internet Multimedia Management Systems V, Philadelphia, PA.

[20] Ganic, E., Eskicioglu, A. M., "Robust digital watermarking: Robust DWT-SVD domain image watermarking: embedding data in all frequencies", *Proceedings of the 2004 multimedia and security workshop on Multimedia and Security*, September 2004, pp. 166 – 174.

[21] Pereira, S., Pun, T., "Robust Template Matching for Affine Resistant Image Watermarks," *in IEEE Transactions on Image Processing*, vol. 9, no. 6, pp. 1123-1129, June 2000

[22] Solachidis, V & Pitas, I 2001, 'Circularly Symmetric Watermark Embedding in 2-D DFT Domain', in *IEEE Transactions on Image Processing*, vol. 10, no. 11, pp. 1741-1753.

[23] Ruanaidh, J. J. K. O., Dowling, W. J., Borland, F. M. "Phase watermarking of digital images," in *Proc. IEEE Int. Conf. Image Processing*, pp. 239–242, Sept. 16–19, 1996.

[24] Ruanaidh, J. J. K. O., Pun, T., "Rotation, scale and translation invariant spread spectrum digital image watermarking," *Signal Process*, vol. 66, no. 3, pp. 303–317, 1998.

[25] De Rosa, A., Barni, M., Bartolini, F., Cappellini, V., Piva, A. "Optimum Decoding of Non-additive Full Frame DFT Watermarks", in *Procedings of the 3rd Workshop of Information Hiding*, 1999, pp. 159-171.

[26] Ramkumar, M., Akansu, A.N., Alatan, A.A., "A Robust Data Hiding Scheme For Digital Images Using DFT", in *IEEE ICIP*, vol 2, pp 211-215, October 99.

[27] Lin, C-Y, Wu, M, Bloom, JA, Cox, IJ, Miller, ML & Lui, YM 2001, 'Rotation, Scale and Translation Resilient Watermarking for Images', *IEEE Transactions on Image Processing*, vol. 10, no. 5, pp. 767-782.

[28] Pereira, S, ORuanaidh, JJK, Deguillaume, F, Csurka, G & Pun, T 1999, 'Template Based Recovery of Fourier-Based Watermarks using Log-polar and Log-log Maps', in *Proc. IEEE Int. Conf. Multimedia Computing and Systems, vol. 1, 1999, pp. 870--874.* Florence, Italy.

[29] Gilani, A.M., Skodras, A.N., "Watermarking by Multi-resolution Hadamard Transform," in *Proceedings Electronic Imaging & Visual Arts (EVA 2001)*, pp. 73-77, Florence, Italy, March 26-30, 2001.

[30] Falkowski, B.J., Lim, L.S., 'Image Watermarking Using Hadamard Transforms', in *IEE Electronics Letters*, United Kingdom, vol. 36, no. 3, pp. 211-213, February 2000.

[31] Lu, C. S., Huang, S.-K., Sze, C.-J., Liao, H.-Y., "A new watermarking technique for multimedia protection," in *Multimedia Image and Video Processing*, L. Guan, S.-Y. Kung, and J. Larsen, Eds. Boca Raton, FL: CRC, 2001, pp. 507--530.

[32] Ganic, E., Dexter, S.D., Eskicioglu, A.M., "Embedding Multiple Watermarks in the DFT Domain Using Low and High Frequency Bands" *IS&T/SPIE's 17th Annual Symposium on Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VII Conference*, San Jose, CA, January 17–20, 2005.

[33] Noore, A., "An improved digital watermarking technique for protecting JPEG images" in *IEEE International Conference on Consumer Electronics*, Morgantown, WV, USA, pp. 222- 223, 17-19 June 2003

[34] Fotopoulos, V., Skodras, A. N., "A Subband DCT Approach to Image Watermarking," in *Proceedings of X European Signal Processing Conference*, Tampere, Finland, September 4-8, 2000.

[35] Choi, Y., Aizawa, K., "Digital Watermarking Technique using Block Correlation of DCT Coefficients" in *Electronics and Communications*, Japan, Part 2, vol. 85, no. 9, 2002

[36] Suhail, M., A., Obaidat, M., s., "Digital Watermarking Based DCT and JPEG Model", in *IEEE Transactions on Instrumentation and Measurement*, Vol. 52, No. 5, Oct. 2003

[37] Golikeri, A., Nasiopoulos, P., "A Robust DCT Energy Based Watermarking Scheme for Images", Available Online www.ece.ubc.ca/~adarshg/DCT_Watermark.pdf Accessed on June 1, 2005

[38] Hsu, C-T., Wu, J-L., "Hidden Digital Watermarks in Images", in *IEEE Transactions on Image Processing*, vol. 8,nno. 1, pp. 56-68, 1999.

[39] Huang, J, Shi, YQ & Shi, Y 2000, 'Embedding Image Watermarks in DC Components', IEEE *Transactions on Circuits and System for Video Technology*, vol. 10, no. 6, pp. 974-979.

[40] Wong, P., H., W., Au, O., C., Wong, J., W., C., "Data Hiding and watermarking in JPEG Compressed Domain by DC Coefficient Modification", 2001. Available online www.ee.ust.hk/~eepeter/watermark/dchide.pdf Accessed on June 1, 2005.

[41] Voloshynovskiy, S, Deguillaume, F & Pun, T 2000, 'Content Adaptive Watermarking based on a Stochastic Multiresolution Image', in *Tenth European Signal Processing Conference (EUSIPCO'2000)*, Tampere, Finland, September 5-8 2000.

[42] Tao, P., Eskicioglu, A.M., "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain", in *Symposium on Internet Multimedia Management Systems*, Philadelphia, PA. October 25-28, 2004.

[43] Lee, C., Lee, H., "Geometric attack resistant watermarking in wavelet transform domain," in *Optics Express* vol. 13, no. 4, pp. 1307-1321 2005

[44] Zhu, W., Xiong, Z., and Zhang, Y.-Q., "Multiresolution Watermarking for Images and Video", in *IEEE Trans. on circuit and System for Video Technology*, vol. 9, no. 4, pp. 545-550, June, 1999.

[45] Feig, E., "A fast scaled DCT algorithm", in *Proc. SPIE Image Processing Algorithms and Techniques*, vol. 1224, pp. 2-13, Feb. 1990.