# Frequency Domain Watermarking: An Overview

**Article** · January 2005

Source: DBLP

CITATIONS
12

READS
1,652

**3 authors:**

Khaled Mahmoud
Princess Sumaya University for Technology
**17** PUBLICATIONS **43** CITATIONS

SEE PROFILE

S. Datta
Loughborough University
**81** PUBLICATIONS **864** CITATIONS

SEE PROFILE

James Flint
Loughborough University
**116** PUBLICATIONS **431** CITATIONS

SEE PROFILE

# Frequency Domain Watermarking: An Overview

Khaled Mahmoud, Sekharjit Datta, and James Flint
Department of Electrical and Electronic Engineering, Loughborough University, UK

**Abstract:** *With rapid growth in computer network and information technology, a large number of copyrighted works now exist digitally as a computer files, and electronic publishing is becoming more popular. These improvements in computer technology increase the problems associated with copyright enforcement and thus future developments of networked multimedia systems are conditioned by the development of efficient methods to protect ownership rights against unauthorized copying and redistribution. Digital watermarking has recently emerged as a candidate to solve this difficult problem. In the first part of this paper we introduces an overview to digital watermarking: The general framework, its main applications, the most important properties, the main aspects used to classify watermarking, and we discuss the attacks that watermarking system may face. Finally we introduce human visual system and its interaction with watermarking as well as some open problems in digital watermarking. In the second part we introduces an overview of watermarking in frequency domain. The general properties for frequency domain as well as specific properties for each sub-domain are introduced. The sub-domains considered are discrete cosine domain, discrete wavelet domain and discrete Fourier domain. We also introduce some different watermarking techniques in each category.*

**Keywords:** *Watermarking, steganography, information hiding, frequency domain, human visual system.*

*Received August 9, 2003; accepted March 8, 2004*

## 1. Introduction

The mid-1990s saw the convergence of a number of different information protection technologies, whose theme was the hiding (as opposed to encryption) of information. Hiding can refer to either making the information imperceptible or keeping the existence of the information secret [9]. Important sub-disciplines of information hiding are steganography and watermarking. steganography and watermarking describe techniques that are used to imperceptibly convey information.

*Watermarking* is the practice of hiding a message (copyright notices or individual serial numbers) about an image, audio clip, video clip, or other work of media within that work itself [9] without degrading its quality in such a way that it is expected to be permanently embedded into the digital works and can be detected later. *Steganography*, on the other hand, is the study of the techniques used to hide one message inside another, without disclosing the existence of the hidden message or making it apparent to an observer that this message containing a hidden message [2]. From the previous definitions we distinguished them as follows [9, 19]:

1. The information hidden by a watermarking system is always associated with the digital object to be protected or its owner while steganographic systems just hide any information.
2. As the purpose of Steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists of detecting the existence of this communication. Watermarking, as opposed to Steganography, has the additional requirement of robustness against possible attacks; even if the existence of the hidden information is known it should be hard for attacker to destroy the embedded watermark. In other words, Steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal by a pirate.
3. Steganographic communications are usually point-to-point (between sender and receiver) while watermarking techniques are usually one-to-many.

The rest of this part is organized as follows. Section 2 gives the general framework of a digital watermarking system. Section 3 discusses several instances in which digital watermarking is already being used. Section 4 illustrates different aspects used in watermarking classification. Section 5 lists some important properties for watermarks. Section 6 describes how a digital watermarking system can be attacked. Section 7 introduces some related disciplines and subjects and finally, list some open problems in this field.

## 2. Watermarking Framework

All watermarking schemes share the same generic building blocks (Figure 1). These blocks and their functions are described below [33, 34]:

1. *Watermark embedding system (signature casting)*: The embedded data is the watermark that one wishes to embed. It is usually hidden in a message

referred to as a cover (work), producing the watermarked cover. The inputs to the embedding system are the watermark, the cover and an optional key. A key is used to control the embedding process so as to restrict detection and/or recovery of the embedded data to parties who know it. The watermarked cover may face some intentional and/or unintentional distortion that may affect the existence of the watermark. The resultant outputs called the "Possibly Distorted Watermarked Cover".

2. *Watermark detection system (extraction)*: The inputs to the detection system are the possibly distorted watermarked cover, the key and depending on the method the original cover or the original watermark. Its output is either the recovered watermark or some kind of confidence measure indicating how likely it is for a given watermark at the input to be present in the work under inspection (e. g., Correlation). Current watermarking schemes may be viewed as spread-spectrum communications systems [9], whose aim is to send the watermark between two parties with two sources of noise: Noise due to the original cover and noise due to processing.

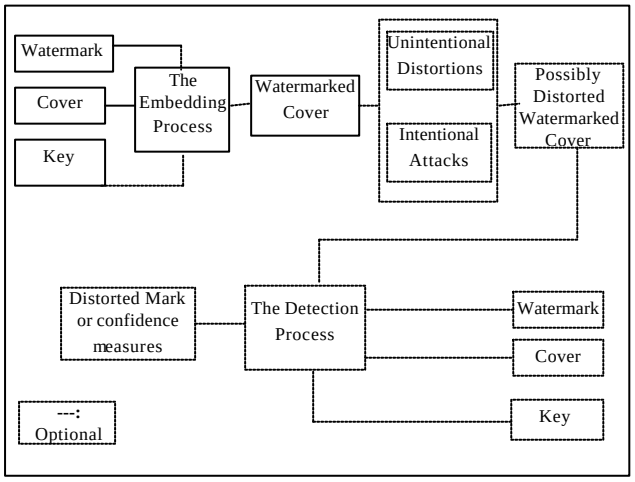



Figure 1. The general framework of a watermarking system.

## 3. Applications

In this section we discuss some of the scenarios where watermarking is being already used as well as other potential applications. The list given in [7, 9, 19, 34] is by no means complete and intends to give a perspective of the broad range of possibilities that digital watermarking opens.

- *Owner identification*: Embedding the identity of a work's copyright holder as a watermark in order to prevent other parties from claiming the copyright of the data.
- *Labeling*: The hidden message could also contain labels that allow, for example, annotation of images or audio. Of course, the annotation may also been included in a separate file, but with watermarking it becomes more difficult to destroy or lose this label, since it becomes closely tied to the object that it annotates. This is especially useful in medical applications since it prevents potentially dangerous errors.
- *Fingerprinting (transaction tracking)*: This is similar to the previous application and allows acquisition devices (such as video cameras, audio recorders, etc.) to insert information about the specific device (e. g., an ID number and date of creation). This is especially useful to identify people who obtain content legally but illegally redistribute it. This involves the embedding of a different watermark into each distributed copy.
- *Authentication*: Embedding signature information in a work that can be later checked to verify if it has not been tampered with.
- *Copy and playback control*: The message carried by the watermark may contain information regarding copy and display permissions. A secure module can be added in copy or playback equipment to automatically extract this permission information and block further processing if required. In order to be effective, this protection approach requires agreements between work providers and consumer electronics manufacturers to introduce compliant watermark detectors in their video players and recorders. This approach is being taken in Digital Videodisc (DVD).
- *Broadcast monitoring*: Identifying when and where works are broadcast by recognizing watermark embedded in the cover.
- *Additional information*: The embedded watermark could be an n-bit index to a database of URLs stored on a known location on the Internet. This index is used to fetch a corresponding URL from the database. Then the URL is used to display the related web pages.

## 4. Classification

Watermarking systems can be classified according to several aspects; some of them are listed below:

### 4.1. According to the Inputs and Outputs

*Private marking systems (informed detector)*: Require at least the original cover. This means that only the copyright holder can detect the watermark. In a private system we can identify where the distortions were, and invert them before applying the watermark detector (use the original cover to reverse the embedding process or use the original work as a hint to find where the watermark could be in the distorted watermarked cover). These kinds of systems may require also a copy of the embedded watermark for detection and just yield a 'YES' or 'NO' answer to the question: Does the distorted marked object contain this watermark?

Private systems usually feature increased robustness (greater strength to the embedded bits) not only

towards noise-like distortions, but also distortions in the data geometry since it allows the detection and inversion of geometrical distortion [7]. Unfortunately, for these techniques to be applied, the possibility to access the original image must be granted. This mean that the set-up of a watermarking system becomes more complicated, and on the other side the owners of the original images are compelled to insecurely share their works with anyone who wants to check the existence of the watermark.

*Semi-private marking system*: This system uses the original watermark only and checks whether it exists in the cover or not.

*Public marking system (blind marking)*: Remains the most challenging problem since it requires neither the secret original nor the embedded watermark[1]. Blind watermarking techniques are less robust and are therefore more suitable for applications requiring lower security than copyright application, such as authorized copying distribution in electronic commerce.

### 4.2. According to the Workspace Used

Another classification criterion distinguishes schemes into spatial domain techniques and transform-domain techniques depending on whether the watermark is encoded by directly modifying pixels (such as simply flipping low-order bits of selected pixels) or by altering some frequency coefficients obtained by transforming the image into the frequency domain. Spatial domain techniques are simple to implement and often require a lower computational cost, although they can be less robust against tampering than methods which place the watermark in the transform domain. Watermarking schemes that operate in a transform space are increasingly common, as this can aid robustness against several attacks and distortions (transform domain method hide messages in significant area of the cover image which makes them more robust to attacks). However, while they are more robust to various kind of signal processing, they remain imperceptible to the human sensory system. Most schemes operate directly on the components of some transform of the cover like discrete cosine transform, discrete wavelet transforms and discrete Fourier transforms.

### 4.3. According to the Visibility

Copyright marks do not always need to be hidden, as some systems use visible digital watermarks [33], but most of the literature has focussed on invisible or (transparent) digital watermarks which have wider applications. Modern visible watermarks may be visual patterns (e. g., a company logo or copyright sign) overlaid on digital images.

### 4.4. According to the Watermark Robustness

*Fragile marks* are watermarks that have very limited robustness and they are destroyed as soon as the object is modified too much. They are applied to detect modifications of the watermarked data, rather than conveying unerasable information [8]. Cryptographic techniques have already made their way in authentication. However, there are two significant benefits that arise from using watermarking: First, the signature becomes embedded in the message. Second, it is possible to create 'soft authentication' algorithms that offer a multi-valued measure that accounts for different unintentional transformations that the data may have suffered instead of the classical yes/ no answer given by cryptography-based authentication.

*Robust marks* have the property that it is infeasible to remove them or make them useless without destroying the object at the same time. This usually means that the mark should be embedded in the most robust significant components of the object [7].

### 4.5. According to the Watermark Natural

Watermarks ranges from pseudo-random sequence to small image logo that can be easily recovered and authenticated.

## 5. Properties

Watermark system can be characterized by a number of defining properties [7, 9, 33]. The relative importance of each property is dependent on the requirements of the application and the role that the watermark will play, some important properties are listed below:

1. *Fidelity (watermark imperceptibility)*: Perceptual similarity between the original and the watermarked versions must be very high (i. e., the difference between the original image and the embedded watermarked work should be invisible). It has been argued that the watermark should not be noticeable to the viewer instead of being imperceptible [7]. Furthermore, if a signal is truly imperceptible, then perceptually base lossy compression algorithms should, in principle, remove such a signal. Current compression algorithms probably still leave room for an imperceptible signal to be inserted. This may not be true of next generation compression algorithms. Thus to survive the next generation of lossy compression algorithm, it is probably be necessary for a watermark to be noticeable to a trained observer.
2. *Statistically invisible*: The watermark must be statistically invisible to thwart unauthorized removal

[1] In many applications -such as Transaction tracking- access to the original data is not possible. In other applications, it may be impracticable to use the original data because of the large amount of data that would have to be processed.

(i. e., a statistical analysis should not produce any advantage from the attacking point of view). The noise–like watermark is statistically invisible and has good auto-correlation properties.

3. *Readily extracted*: If decoder must run in real-time, then it is necessary for the decoding process to be significantly simpler than the encoding [7]. In some applications this requirement is reversed depending on the purpose of watermarking.
4. *Data payload*: Refer to the amount of information that can be carried in a watermarked cover. This raises the capacity issues in digital watermarking. The length of the watermark serves as a measure of the capacity. A longer watermark signal means that more coefficients need to be modified; hence the watermarked images 'look noisier'. The more information one wants to embed, the lower the watermark robustness.
5. *Embedding effectiveness*: The probability that the embedder will successfully embed a watermark in a randomly selected work. This property related to real-time embedding system (which must be high).
6. *False positive rate*: The frequency with which we should expect watermark to be detected in un-watermarked object (which must be low).
7. *Robustness (security)*: The watermark should be resilient to standard manipulations of unintentional as well as intentional nature. Some authors [9] distinguish between resistance to intentional and unintentional attacks. They use "security" when dealing with the ability of the watermark to resist hostile attacks while use the "robustness" when dealing with the ability of the watermark to survive normal processing of content such as spatial filtering, lossy compression, printing and scanning, geometric distortions (such as rotation, translation, and scaling). Note that robustness actually comprises two separate issues 1) whether or not the watermark is still present in the data after distortion and 2) whether the watermark detector can detect it. For example, watermarks inserted by many algorithms remain in the data after geometric distortion but the corresponding detection algorithm can only detect the watermark if the distortion is first removed otherwise the detector can't detect the watermark [7]. Note that, any increase in robustness comes at the expense of increased watermark visibility. Also the presence of the original cover increases the robustness. For example: The use of the original image permits some pre-processing to be carried out before the watermark checking such as: Rotation angles, translation and scale factors can be estimated, and missing parts of the image can be replaced by corresponding parts of the original one. It would be possible to do exhaustive search on different rotation angles and scaling factors until a watermark found, but this is prohibitively complex.

## 6. Distortions and Attacks

In practice, a watermarked cover may be altered either intentionally or unintentionally, so the watermarking system should still be able to detect and extract the watermark. The distortions are limited to those that do not produce excessive degradations, since otherwise the transformed object would be unusable. Several authors have classified attacks based on several aspects. One famous classification has been carried out by Craver *et al.* [10, 11].

### 6.1. Craver Classification for Attacks

Craver defines four general classes of attacks, organized by the way in which the attacks try to defeat the watermarking technology. These classes are illustrated below, as well as examples for each class are also presented. Some of them may be intentional or unintentional, depending on the application.

#### 6.1.1. Robustness Attacks (Unauthorized Removal):

This kind of attacks aim to diminish or remove the presence of a digital watermark from its associated content, while preserving the content so that it is not useless after the attack is over. Examples of robustness attacks:

- *Additive noise*: This may happen (unintentionally) in certain applications such as D/ A (printing) and A/ D (scanning) converters or from transmission errors. It could happen intentionally by an attacker who is trying to destroy the watermark (or make it undetectable) by adding noise to the watermarked cover.
- *Filtering*: Linear filtering such as low-pass filtering or non-linear filtering such as median filtering.
- *Collusion attack*: In some watermarking schemes, if an image has been watermarked many times under different secret keys, it is possible to collect many such copies and "average" them into a composite image that closely resembles the original image and does not contain any useful watermarking data [27].
- *Inversion attack (elimination attack)*: An attacker may try to estimate the watermark and then remove the watermark by subtracting the estimate or reverse the insertion process to perfectly remove the watermark. This means that an attacked object can't be considered to contain a watermark at all (even using more sophisticated detector). Note that with different watermarked objects it would be possible to improve the estimate of the watermark by simple averaging.
- *Lossy compression*: This is generally an unintentional attack, which appears very often in multimedia applications. Practically all the audio, video and images that are currently being distributed

via Internet have been compressed. Lossy image compression algorithms are designed to disregard redundant perceptually-insignificant information in the coding process. While watermarking try to add invisible information to the image. An optimal image coder would therefore simply remove any embedded watermark information. However, even state-of-the-art image coding such as JPEG 2000 do not achieve optimal coding performance and therefore there is a "distortion gap" that can be exploited for watermarking. Actually one can observe that the use of a particular transform gives good results against compression algorithms based on the same transform. For instance, DCT-domain image watermarking is more robust to JPEG compression than spatial-domain watermarking.

#### 6.1.2. A Presentation Attack (Masking Attack):

This attack does not attempt to remove the watermark, but instead alters the content so that the watermark can no longer be detected or extracted easily. This means that the attacked work can still be considered to contain the watermark, but the watermark is undetectable by existing detector (such as detector sensitive to image rotation). Examples of presentation attack:

- *Chopping attack (mosaic attack)*: In which an image is chopped into distinct sub-images, which are embedded one after another in a web page. Common web browsers render sub images together as a single image, so the result is identical to the original image. But the chopping process distributes the original image's watermark into many pieces, and the watermark cannot be recovered unless the original image is reconstructed first.
- *Rotation and spatial scaling*: Detection and extraction fail when rotation or scaling is performed on the watermarked image because the embedded watermark and the locally generated version do not share the same spatial pattern anymore. This kind of attacks can be unintentional happening in scanning-printing process (copies from printing, scanning maybe rotated, scaled, cropped or translated in comparison with the initial image).
- *Cropping*: This is a very common attack since in many cases the attacker is interested in a small portion of the watermarked object, such as parts of a certain picture or frames of a video sequence. With this in mind, in order to survive this kind of attack, the watermark needs to be spread over the dimensions where this attack takes place.

#### 6.1.3. An Interpretation Attack

This kind of attacks seeks to forge invalid or multiple interpretations from watermark evidence [10] whereby an attacker can devise a situation, which prevents assertion of ownership. As an example:

- *Multiple watermarking*: An attacker may watermark an already watermarked object (creating uncertainty about which watermark was inserted first) and later make claims of ownership. The easiest solution is to timestamp the hidden information by a certification authority.
- *Unauthorized embedding (forgery)*: Embed illegitimate watermark into works that should not contain them. Or use watermark inversion to remove the original watermark before inserting a new watermark.

#### 6.1.4. A Legal Attack

In a legal attack, the attacker uses a legal precedent, the identity or reputation of the object owner, or some other non-technical information to establish doubt in court whether a watermark actually constitutes the proof that its owner claims.

### 6.2. Cox Classification for Attacks

Cox *et al.* [9] classify the attacks into two main categories: Active and passive attack:

1. Active attack (i. e., Change the Cover) such as: Unauthorized removal (robustness attack) and Unauthorized Embedding (forgery).
2. Passive attack (i. e., Doesn't Change the Cover) such as: Unauthorized detection, this can be in three levels according to severe:
    1. The adversary detects and deciphers an embedded message.
    2. The adversary detects the watermark and distinguishes one mark from another, but can't decipher what the marks mean.
    3. The adversary detects the watermark but without distinguish and decipher.

*Note:* There are situations in which the watermark has no hostile enemies and need not to be secure (when watermark is used to provide enhanced functionality).

## 7. Related Disciplines and Subjects

In this section we will look for other techniques that can be used for information hiding and why watermarking is more powerful than them. In this section also, we will introduce the importance of Human Visual System (HVS) to watermarking.

### 7.1. Watermarking Against other Techniques

Watermarking is distinguished from other techniques such as: Placing the mark in the Media header, encoding it in a visible bar, or speaking it loud as an introduction to an audio clip in three ways:

- Watermark is imperceptible.
- Watermark is inseparable from work (Once the digital images are printed on paper, all data in the header is left behind, also, this data may not survive a change in the image format).
- Watermark undergoes same transformations as the work and this can help in authentication and detection the kind of alteration that the image has undergone.

### 7.2. Problems with Cryptography as a Solution

Cryptography is defined as the study of secret writing, i. e., concealing the contents of a secret message by transforming the original message into a form that cannot be easily interpreted by an observer. Thus, the mere discovery of encrypted data suggests that something illicit, or at least secret, is occurring. Cryptographic techniques can hide a message from plain view during communication, and can also provide auxiliary information that effectively proves the messages. However traditional cryptosystems suffer from one important drawback, which renders them useless for the purpose of enforcing copyright law [11]: They do not permanently associate cryptographic information with work. Thus, cryptography alone cannot make any guarantees about the redistribution or alteration of content after it has initially passed through the Cryptosystem (i. e., Cryptography can't help the seller monitor how a legitimate customer handles the content after decryption). Watermarking can fulfil this need; it places information within the content where it is never removed during normal usage. Also Steganography has a distinct advantage over cryptography; it allows principals to communicate secret information to each other without even alerting an attacker to the presence of the secrets.

### 7.3. HVS and Image Watermarking

It is today widely accepted that robust/ high fidelity watermarking techniques should largely exploit the characteristic of the HVS and Human Auditory System (HAS) for more effectively hiding watermarks. Perceptual masking techniques exploits the perceptual masking properties of the human auditory system and of the human vision system [32]. In this section we will concentrate on HVS and image watermarking.

- *HVS and fidelity*: A good watermarking schema has to adapt to the particular image being watermarked in order to exploit specific HVS characteristics and hence amplifying the watermark where the alterations are least likely to be noticed. Local image characteristics that can help determine the visibility of a watermark are listed below:
  1. *Fine against high texture area*: It is usually true that the human eyes are not sensitive to the small changes in texture but is very sensitive to the small changes in the smooth areas of an image. So it should be possible to incorporate more information into those parts of the image that contain more textures than smooth area. Related methods accomplish this by calculating a value of local contrast, and mapping increasing contrast values to increasing watermark magnitudes [13].
  2. *Edges*: Edge information of an image is the most important factor for perception of the image. This can present a problem though, as directional edges separating two distinct objects in an image may be identified as a high contrast areas. This results in the application of a higher strength watermark signal around the connected edges, which causes an objectionable watermark ringing on connected edges. Methods have also been proposed which identify areas of true high contrast texture while protecting connected directional edges [13, 18] (region that contains a sudden transition in luminance).
  3. *Brightness sensitivity*: When the mean value of the square of the noise is the same as the background, the noise tends to be most visible against mid-gray background. The mid-gray regions have lower noise-capacity as compared to the other regions [18].
- *HVS and robustness*: The key to making the watermark robust and to prevent the watermark from being easily attacked is to embed the watermark in the perceptually significant regions of the image. These regions do not change much after several signal processing or compression operations. Moreover, if these regions lose their fidelity significantly, the reconstructed image could be perceptually different from the original one (i. e., visual fidelity is only preserved if the perceptually significant regions remain intact). Also, lossy image compression algorithms are designed to disregard redundant information. Information bits placed within textured areas of the image are therefore more vulnerable to attack. The question, therefore, is how much extra watermark information we can add to the perceptually significant regions without any impact on the visual fidelity? There is a compromise to be reached between hiding a large number of information bits where they can least be seen, but where they can be attacked by image compression algorithm, or placing a fewer bits on less textured but safer portions of the image.
- *Measure of capacity*: Every pixel value of an image can be altered only to a certain limit without making perceptible difference to the image quality. This limit can be called as the "*Just Noticeable Distortion*" or *JND* level [13, 17, 18]. For instance, smooth areas are assigned relatively low JND as compared to strongly textured regions (i. e., strongly textured region has a very high capacity for noise).

- *Watermark shaping*: There is an advantage to shaping the watermark spectrum based on the cover to match currently known human visual system. Inserting a watermark that is a function of the cover leads to a non-linear embedding procedure. Such a procedure has the advantage that when the image energy in a particular area is small, the watermark energy is also reduced, thereby avoiding artifacts, and when the image energy is large, the watermark energy is increased, thereby improving the robustness of the procedure. Conversely, if simple linear addition to the watermark and image occurs then the energy of the watermark must be very low in order to avoid the worst case scenarios in which the image energy in a particular place is very low and artifacts are created because the watermark energy was too strong relative to the image [7].
- *HVS and spread spectrum techniques*: Spread-spectrum techniques spread a narrow band signal (watermark) over a much wider band (cover) such that the signal-to-noise ratio in any single band is very low. However, with precise knowledge of the spreading function, the receiver is able to extract the transmitted signal, summing up the signals in each of the bands such that the detector signal-to-noise ratio is strong. Spread spectrum techniques are useful because they have a low probability of interception by an attacker [32]. Also, instead of embedding watermark in the high frequency (no robustness) or embedding the watermark in the low frequency (visible impacts). Spread spectrum can reconcile these conflicting points by allowing a low-energy signal to be embedded in each one of the frequency bands.

## 8. Open Problems

Even though watermarking is a fast growing field there are still a lot of problems facing it such as [1]:

- Optimisation between robustness and visibility limiting the capacity.
- Detection speed is crucial especially in a real time application.
- Reading the watermark after geometric distortion is a challenging problem.
- Printing process, paper and ink may degrade the watermark. Moreover the printed images do not maintain their quality over time. They are subject to aging, soiling, crumbling, tearing, and deterioration. Designing a watermark scheme to compensate for these kinds of unintentional attacks is another challenge.
- Different input devices (scanner and cameras) introduce different types of distortions. Accounting for this difference in detection is also a major challenge.

## 9. Transform Domain General Features

In this part we will explore the main features of the frequency domain that make it more appropriate for watermarking. In subsequent sections, we will introduce three sub-domains and discuss the properties of each and introduce techniques that hide watermarks in these sub-domains.

Watermarking schemes that operate in a transform space are increasingly common, as these schemes posses a number of desirable features such as:

- By transforming spatial data into another domain, statistical independence between pixels as well as high-energy compaction can be obtained.
- The watermark is irregular distributed over the entire spatial image upon inverse transform, which makes it more difficult for enemies to decode and read the mark.
- One can mark according to the perceptual significance of different transform domain components, which means that one can adaptively place a watermark where they are least noticeable, such as within the textured area.
- Transform domain methods can hide messages in significant area of the cover which makes them more robust against several attacks and distortion. However, while they are more robust to various kind of signal processing, they remain imperceptible to the human sensory system.
- Cropping may be a serious threat to any spatially based watermark but is less likely to affect a frequency-based scheme. Since watermarks applied to the frequency domain will be dispersed over the entirely of the spatial image upon inverse transformation so we can retrieve part of the watermark.
- Lossy compression is an operation that usually eliminates perceptually unimportant components of a signal. Most processing of this sort takes place in the frequency domain. In fact, matching the transform with compression transform may result in better performance of the data-hiding schema (i. e., DCT for JPEG, Wavelet for JPEG-2000).
- Characteristic of HVS can be fully exploited in the frequency domain.

## 10. HVS and Frequency Domain

It is usually true that human eyes are not sensitive to small changes in edges and texture but they are very sensitive to small changes in the smooth areas of an image. In flat featureless portions of the image the important information concerned with the flat parts concentrate on the lowest frequency components, while, in a highly textured image, energy is concentrated in the high frequency components. Thereby, the human eyes are more sensitive to lower

frequency noise, rather than high frequency noise. From the previous points:

- The watermark should be embedded into the higher frequency components to achieve better perceptual invisibility, however, high frequencies might be discarded after most of attacks such as lossy compression, shrinking or scanning.
- In order to prevent the watermark from being easily attacked, it is often necessary to embed the watermark in the lower frequency coefficients. The attacker can't change these coefficients, otherwise the image maybe damaged. However, the human eyes are more sensitive to lower frequency noise.
- From the previous contradiction, to invisibly embed the watermark, which can survive most of the attacks, a reasonable trade-off is to imbed the watermark into the middle frequency range of the image [15].

## 11. Frequency Domain Transforms

In watermarking in the transform domain, the original host data is transformed, and the transformed coefficients are perturbed by a small amount in one of several possible ways in order to represent the watermark. Coefficient selection is based on perceptual significance or energy significance. When the watermarked image is compressed or modified by any image processing operations, noise is added to the already perturbed coefficients. The private retrieval operation subtracts the received coefficients from the original ones to obtain the noise perturbation. The watermark is then estimated from the noisy data as best as possible. The most difficult problem associated with blind watermark detection in the frequency domain is to identify the coefficients used for watermarking. Embedding can be done by adding a pseudo-random noise, quantization (threshold) or image (logo) fusion. Most algorithms consider HVS to minimize perceptibility. The aim is to place more information bits where they are most robust to attack and are least noticeable. Most schemes operate directly on the components of some transform of the cover like Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), and Discrete Fourier Transforms (DFT). In this section we will introduce each domain, illustrates its main features and introduce some techniques that used this domain in watermarking.

### 11.1. Discrete Cosine Transform

The DCT transform has a number of advantages in respect of watermarking:

- The DCT has the primary advantage that it is a sequence of real numbers, provided that the input sequence is real.
- The two-dimensional DCT is the heart of the most popular lossy digital image compression system used today: The JPEG system.
- The sensitivity of HVS to the DCT basis images has been extensively studied resulting in a default JPEG quantization table.

Zhao *et al.* [41] approach the problem by segmenting the image into 8x8 blocks. Block DCT transformation and quantization steps are applied on each block. A bit of information can be encoded in a block using the relation between three quantized DCT coefficients ($c_1$, $c_2$, and $c_3$) from this block. The three coefficients must correspond to middle frequencies. One block encodes a "1", if $c_1 > c_3 + d$ and $c_2 > c_3 + d$. On the other hand, a "0" is encoded, if $c_1 + d < c_3$ and $c_2 + d < c_3$. The parameter $d$ accounts for the minimum distance between two coefficients. The higher $d$ is the more robust the method will be against the image processing techniques. If the relations between the coefficients don't correspond to the encoded bit, a change must be made to the coefficients so that they can represent the encoded bit. If the modification required to code one bit of information are too large, then the block is not used and marked invalid block. Afterwards the blocks are de-quantized and the inverse DCT is applied. In the decoding step, comparing the three coefficients of every block in the quantized DCT domain can restore the label.

Cox *et al.* [8] present an image watermarking method in which the mark (a sequence of real numbers $\{w_i\}$ having a normal distribution with zero mean and a unity variance) is embedded in the $n$ (excluding the DC term) most perceptually significant frequency components $V = \{v_i\}$ of an image's DCT to provide greater robustness to JPEG compression. The watermark is inserted using the formula: $v'_i = v_i + a\, v_i\, w_i$. This modulation law is designed to take into account the frequency masking characteristics of the human visual system. This non-linear insertion procedure adapts the watermark to the energy present in each coefficient. The advantage of this is that when $v_i$ is small, the watermark energy is also small, thereby avoiding artifacts; and when $v_i$ is large, the watermark energy is increased for robustness. The parameter $\alpha$ represents a compromise between robustness and image fidelity. The presence of the watermark is verified by extracting the main components of original image, and those with same index from a watermarked image and inverting the embedding formula to give a possibly modified watermark $W'$. The watermark is said to be present if the correlation between $W$ and $W'$ is greater than a given threshold.

Barni *et al.* [3] propose a watermarking algorithm similar to Cox's method. However, instead of using the $n$ largest DCT coefficients as Cox does, the set is produced by arranging the DCT coefficients in a zigzag order and a subset in the mid-frequency range is selected. The lowest coefficients are then skipped to

preserve perceptual invisibility. The watermark is then embedded in this set of coefficients in the same way as Cox. In order to enhance the invisibility of the watermark, the spatial masking characteristics of the HVS are also exploited to adapt the watermark to the image being signed: The original image ($I$) and the watermarked image ($I'$) are added pixel by pixel according to a local weighting factor $b_{i,j}$, thus getting a new watermarked image($I''$): $I''_{i,j} = I_{i,j}(1-b_{i,j}) + b_{i,j} I'_{i,j}$, in a region characterized by low–noise sensitivity, where the embedding of watermarking data is easier (e. g., highly textured regions) $b_{i,j} \sim 1$, i. e., the watermark is not dimensioned, whereas in regions more sensitive to change, in which the insertion of the watermark is more disturbing (e. g., uniform regions) $b_{i,j} \sim 0$, i. e., the watermark is embedded only to a minor extent. In the extraction phase, they first extract the subset of modified coefficients from the full frame DCT of the watermarked image. The correlation between the marked (possibly corrupted coefficients) and the mark itself is taken as a measure of the mark presence.

O' Ruanaidh *et al.* [30] present a private watermarking technique for images using bi-directional coding in DCT domain. In bi-directional coding, the image is divided up into blocks. The DCT is computed for each block. The mean of each block is incremented to encode a '1' or decremented to encode a '0'. This may be accomplished by using simple thresholding techniques. JPEG quantization table (visual masking) is used to weight the DCT coefficients in each block. The most significant components are then selected by comparing the square of the component magnitude to the total energy in the block. In the decoding step, the mean of each block in the original un-watermarked image is compared with the mean of the corresponding blocks in the tested copy to decode the stored bit.

Swanson *et al.* [38] embed the watermark by computing the DCT for each block in the cover. A perceptual mask is computed for each block. The resulting perceptual mask is then scaled and multiplied by the DCT of the pseudo-noise watermark. The schema uses a different m-sequence for each block. The watermark is then added to the corresponding block. The watermark can be detected by correlating the modified watermark with the original watermark and comparing the result to a threshold.

Chae *et al.* [6] used a public technique to embed a signature (watermark) into images. The signature DCT coefficients are quantized according to the signature quantization matrix. The resulting quantized coefficients are encoded using lattice-codes. The choice of signature quantization matrix affects the quantity and the quality of the embedded data. The codes are inserted into the middle frequency DCT coefficients of the host image. This insertion is adaptive to the local texture content of the host image blocks and is controlled by the block texture factor. The texture factor is computed using wavelet transform. The selected host coefficients are then replaced by the signature codes and combined with the original unaltered DCT coefficient to form a fused block of DCT coefficient. The fused coefficients are then inverse-transformed to give an embedded image.

Bors *et al.* [5] propose watermark algorithm based on imposing constraints in the DCT domain. The block sites for embedding the watermark are selected based on a Gaussian network classifier, then DCT constraints are embedded in the selected blocks. Two distinct algorithms are considered here. The first algorithm embeds a linear constraint on selected DCT frequency coefficients (i. e., $Y = FQ$, where $F$ is the vector of the modified DCT coefficient, and $Q$ is the weighting vector provided by the watermark). In the second approach circular regions are defined around certain DCT coefficients. For a selected block site, they evaluate the Euclidean distance between its DCT coefficient vectors and that of the watermark. The chosen DCT coefficients are changed to the value of the closest watermark parameter vector. After modifying the DCT values, the image is reconstructed based on the inverse DCT transform. In the detection stage they first check for the DCT constraints and afterwards for the respective block location. A given site is considered as being signed when the probability of detecting the DCT coefficients constraint and the probability of detecting the location constraint is maximized. The original image is not required for watermark detection and simulations have showed this method is resistant to JPEG compression and filtering.

Kankanhalli *et al.* [18] propose a way of analysing the noise sensitivity of every pixel based on the local region content (texture, edges and luminance). If the distortion caused by the watermarking algorithm is at or below the thresholds the degradation in the original image quality is imperceptible. The analysis is based on the DCT coefficients. The energy in the DCT coefficients can be used as a measure of roughness, and the count of large-magnitude fluctuations in a high-energy block can then used to decide if the block has an edge or is highly textured. The paper, also analyses the contribution of luminance to noise sensitivity. This luminance analysis is done at the pixel level in the spatial domain. The authors use the previous mask to embed an invisible watermark in the spatial domain.

Tao B. *et al.* [39] has an approach that is similar to that of [18]. Here, the block as a whole is given a sensitivity label that shapes the watermark based on texture and edges analysis. The embedding is then done in the DCT transform domain.

## 11.2. Discrete Wavelet Transform

DWT is identical to a hierarchical sub-band system, where the sub-bands are logarithmically spaced in

frequency and represent octave-band decomposition. DWT can be implemented using digital filters and down-samplers [12]. The original image is split into four quadrant bands after decomposition. The four quadrants contain approximation sub-band (LL), horizontal detail sub-band (LH), vertical detail sub-band (HL) and a diagonal detail sub-band (HH). This process can be repeatedly applied on the approximation sub-band to generate the next coarser scale of wavelet coefficients. The process continues until some final scale is reached. The Wavelets transform has a number of advantages [26, 40] over other transform that can be exploited for watermarking:

- It is well known that wavelet coding has been exploited in new compression standard such as JPEG2000 and MPEG4 due to the excellence performance in compression.
- The wavelet transform requires a lower computational cost *O (n)* than the Fourier or the Cosine transform *O (nlog (n))*, where *n* is the length of the signal.
- Wavelet process data at different scales or resolutions, highlighting both large and small features. This makes watermarking adaptive as it depends on the local image characteristic at each resolution level.
- The wavelet functions provide good space-frequency localization and thus they are suited for analysing images where most of the informative content is represented by components localized in space such as edges and borders.
- With DWT, the edges and texture are usually exploited very well in high frequency sub-band (HH, HL, and LH). Therefore, adding watermark on these large coefficients is difficult for the human eyes to perceive.
- Wavelet functions have advantages over traditional Fourier methods in analysing signals containing many discontinuities or sharp changes.
- The wavelet transform is flexible enough to adapt to a given set of images or particular type of application. The decomposition filters (such as Haar, Daubechies-4, 6 or bi-orthogonal filters) and the decomposition structure (wavelet packet, complex wavelet transform) can be chosen to reflect the characteristics of the image.
- Research into human perception [22] indicates that the retina of the eye splits an image into several frequency channels each spanning a bandwidth of approximately one octave. The signals in these channels are processed independently. Similarly, in a multi-resolution decomposition, the image is separated into bands of equal bandwidth on a logarithmic scale. It is therefore expected that use of this discrete wavelet transform will allow the independent processing of the resulting components without significant perceptible interaction between them, and hence makes the process of imperceptible marking more effective. For this reason the wavelet decomposition is commonly used for the fusion of images.

There are many attempts to use wavelet transform in watermarking. Some of them are presented here:

Xia *et al.* [40] propose a private watermarking system. The method utilizes large DWT coefficients of all sub-bands excluding the approximation image to equally embed a random Gaussian distributed watermark sequence in the whole image. The decoding process is based on hierarchical correlation of coefficients at different sub-bands. First, they apply one level DWT on watermarked image and then on the original image. The difference (corrupted watermark) of the DWT coefficients in *HH* band of the watermarked and the original image is then calculated. Then, the cross-correlation between the corrupted watermark and the part of the original watermark that was added in *HH* band is determined. If there is a peak in the cross correlation, the watermark is considered detected, otherwise they consider the other bands at the same level (i. e., HH and LH, then HH, LH, and HL). In case the watermark still cannot be detected, they compute a new level of the DWT and try to detect the watermark again. This process is performed until the watermark is detected or the last level of the DWT has been reached.

Kundur *et al.* [22] embed a binary watermark into the detail wavelet coefficients of the host image with the use of a key. This binary randomly generated key is used to select the exact locations in the wavelet domain (ones location) in which to embed the watermark. First of all, they compute the $L^{th}$ level discrete wavelet decomposition of the host image to produce a sequence of $3L$ detail images. Then, for each level, the embedding modulation at any selected coefficients is done as follows:

- Order the horizontal, vertical and diagonal detail coefficients at this location (high, middle, and low).
- The range of values between high and low is divided into bins of width *(high-low) / (2Q-1)* where $Q$ is a user-defined variable. These bins represent 1 and –1 in periodic manner.
- To embed a watermark bit of value one, the middle coefficients is quantized to the nearest 1 bin. Alternatively, to embed a negative one, the middle coefficient is quantized to the nearest –1 bin.

Finally, apply the inverse wavelet transform to form the watermarked image.

In Kunder *et al.* [21] the host is transformed to the $L^{th}$ level discrete wavelet decomposition. Only the first level discrete wavelet decomposition of the watermark is performed. The watermark is a random binary two-dimensional array. It is required that the size of the watermark in relation to the host image be small. The

detail images of the host at each resolution level are segmented into a non-overlapping rectangle. Each rectangle has the same size as any bands of the watermark. A numerical measure of perceptual importance (salience) of each of these localized segments is computed. The watermark is embedded by a simple scaled addition of the watermark to the particular detail component. The scaling of the watermark is a function of the salience of the region. The greater the salience, the stronger the presence of the watermark. Finally the corresponding $L^{th}$ level inverse wavelet transform is performed. Salience is computed based on well-known model given by Dooly [23], which is based on contrast sensitivity. The original image is required in the extraction process. The extraction process is done by applying the inverse procedure at each resolution level to obtain the estimate of the watermark. The estimates for each resolution level are averaged to produce an overall estimate of the watermark.

Ohnishi [28] propose an algorithm similar to the Kunder [22] technique. The most significant difference between the two methods lies in the merging stage of the watermark. Here the author marks the host by forcing the modulo 2 difference between the largest and smallest wavelet coefficients for a particular position and resolution level to be one if $w(n) = 1$ and to be zero if $w(n) = -1$.

In Barni M. *et al.* [4] the authors present a public watermarking system. A binary pseudo-random sequence is weighted with a function, which takes into account the human visual system (orientation, brightness, and texture) and then added to the DWT coefficients of the three largest detail sub-bands of the image (i. e., first level). For watermark detection, the correlation between the watermark to be tested for presence and the marked coefficients is computed. The value of the correlation is compared to a threshold to decide if the watermark is present or not. Experimental results prove the imperceptibility of the watermark and the robustness against most common attacks. A model for estimating the sensitivity of the eye to noise - previously proposed for compression applications [24]- is used to adapt the watermark strength to the local content of the image.

Inoue *et al.* [16] propose two public digital watermarking schemes to embed a binary code. Both methods are built on a data structure called a zerotree, which is defined in the Embedded Zerotree Wavelet (EZW) algorithm of Shapiro [36]. Zerotree coding is based on the hypothesis that if a wavelet coefficient at a coarse scale is insignificant with respect to a given threshold $T$, then all wavelet coefficients of the same orientation in the same spatial location at a finer scale are likely to be insignificant with respect to $T$. The zerotree is used to classify wavelet coefficients as insignificant or significant as follows: Given an amplitude threshold $T$, if a wavelet coefficient $x$ and all of it descendants (i. e., coefficients corresponding to the same spatial locations but at finer scales of similar orientation) satisfy $|x| < T$ then they are called insignificant with respect to a given threshold $T$ or zerotree for the threshold $T$ (otherwise significant coefficients). In one method, the zerotrees are constructed for any coarsest sub-band (except LL sub-band) for a specific threshold. Each watermark binary digit is embedded by writing the same data in the location of all elements of the current zerotree. Data is redundantly embedded because insignificant coefficients are generally easy to change under the influence of common signal processing. In the second method, the watermark can be embedded by thresholding and modify significant coefficients at the coarser levels. However, it is well known that the modification of these components can lead to perceptual degradation of the signal. To avoid this they make the value of $T$ larger than the previous method. As a result, the regions in which the watermark is embedded are applied to detailed portions, that is edges or textures, in the coarsest scale component. Therefore, embedding the watermark into significant coefficients is difficult for human eyes to perceive. The watermark is detected by using the position of zerotree's root and the threshold value after the wavelet decomposition of the cover image. It is shown that the proposed method is robust against several common signal processes.

## 11.3. Discrete Fourier Transform

The DFT of a function provides a quantitative picture of the frequency content in terms of magnitude and phase. This is important in a wide range of physical problems and is fundamental to the processing and analysis of signals and images. It is very important to know the properties of DFT so that it can be exploited efficiently. Some of these properties are listed below:

- *Positive symmetric:* If $f(n, m)$ is real (which is the case of images), its Fourier transform is conjugate symmetric [12]; that is $F(p, q) = F^*(N - p, M - q)$. To ensure the inverse DFT is real, changing in the magnitude must preserve positive symmetry.
- *Negative symmetric:* The same thing can be said about the phase component ($F$), but here with negative symmetry:

$$F_{p,q} = F_{p,q} + d, \qquad F_{N-p,M-q} = F_{N-p,M-q} - d$$

- *Scaling:* Scaling in the spatial domain causes inverse scaling in the Fourier domain (i. e., as spatial scale expands, the frequency scale contracts and the amplitude increases vertically in such a way to keep the area constant):

$$\text{if } f(x_1,x_2) \xrightarrow{DFT} F(k_1,k_2) \text{ then } f(ax_1,ax_2) \xrightarrow{DFT} \frac{1}{a}F\left(\frac{k_1}{a},\frac{k_2}{a}\right)$$

- *Translation:* The translation property of Fourier transform is defined as follows:

$$\text{if } f(x_1,x_2) \xrightarrow{DFT} F(k_1,k_2) \text{ then}$$

$$f(x_1+a,x_2+b) \xrightarrow{DFT} F(k_1,k_2)\exp\left[-i(ak_1+bk_2)\right]$$

This indicates that the phase is altered only by a translation, i. e., the amplitude is insensitive to the spatial shift of an image. Note that both $f$ and $F$ are periodic function so it is implicitly assumed that the translation causes the image to be "Wrapped around" (circular translation) [28]. By translation, we mean zero padding of the image such as would occur if an image were placed on a scanner and scanned.

- *Rotation:* Rotating the image through an angle $q$ in the spatial domain causes the Fourier representation to be rotated through the same angle [28].

$$f(x_1\cos q - x_2\sin q, x_1\sin q + x_2\cos q) \xrightarrow{DFT} F(k_1\cos q - k_2\sin q, k_1\sin q + k_2\cos q)$$

- *Log-polar representation:* Most watermarking algorithms have problems in extracting the watermark after an affine geometric transformation on the watermarked object. Some methods try to inverse the effect of geometric distortion using the original image. An alternative way is to build a system that can detect the watermark even after a geometric distortion is applied, i. e., Rotation, Translation, and Scaling invariance (RST invariant). Most of these systems use the properties of log-polar representation of the spectrum. In log-polar mapping (which is defined as $x = e^r \cos ?, y = e^r \sin ?$) the rotation and scaling in the Cartesian coordinate system will result in a translation in the logarithmic coordinate system:

$$\text{if } f(x,y) \xrightarrow{\log\text{–}polar\text{–}mapping} f(m,q) \text{ then}$$

$$f(ax,ay) \xrightarrow{\log\text{–}polar\text{–}mapping} f(m+\log a,q) \text{ and}$$

$$f(x\cos(q+d)-y\sin(q+d), x\sin(q+d)+y\cos(q+d)) \xrightarrow{log\text{–}polar\text{–}mapping} f(m,q+d)$$

From the translation property of the Fourier transform as well as the properties of log-polar mapping we can create RST invariant domain by applying the Fourier transform to the log-polar version of the Fourier magnitude of an image, which is equivalent to computing the Fourier-Mellin transform.

- *Phase and magnitude modulation:* The DFT is generally complex valued. This leads to a magnitude and phase representation for the image [29]. The human visual system is far more sensitive to phase distortion than the magnitude distortion and as a consequence the DFT magnitude can be altered significantly without affecting the perceived quality of the image. The phase modulation can possess superior noise immunity when compared to amplitude modulation. As a consequence if the watermark is introduced in phase components with high redundancy, the attacker would need to cause a serious damage to the quality of the image.

O' Ruanaidh *et al.* [29] investigate the use of DFT phase for the transformation of information. The condition that the image is a real data implies that the Fourier spectrum is symmetric, and because the human eye is more sensitive to phase distortion then the watermarking that changes the phase must preserve the negative symmetry. The most significant components are then selected by comparing the component magnitude squared to the total energy in the spectrum. To detect the watermark, the marked image is simply compared with the original image.

Solachidis *et al* [37] propose a watermarking method robust to rotation and scaling. The watermark consists of a 2-D circularly symmetric sequence taking values 1, -1. It has zero mean value. The region in which the watermark is embedded should be a ring covering the middle frequencies. The ring is separated in S sectors and in homocentric circles. Each sector is assigned the same value (1, -1). The watermark is added directly to the magnitude of the DFT domain. If the magnitude becomes negative, it is rounded to 0. The "conjugate symmetry" property for DFT must be preserved. The original is not required for detection. The detection is done by finding the correlation between the possibly watermarked coefficients and the original watermarks. Then comparing the correlation against a threshold.

Kim *et al.* [20] discuss the embedding of a binary image (seal image) into another image. The entire watermark is modulated by a binary pseudo-noise matrix ($P$). The pseudo noise serves for spreading the watermark evenly and is the secret key for retrieving the watermark. The watermark is embedded into the Fourier domain of the cover image by altering the magnitude components ($m_{ij} = m_{ij} + a * P_{ij} * w_{ij}$). The amplitude factor a, is a constant determining the signature strength. The retrieval process can be done without the knowledge of the original image. This process starts by approximating the magnitude of the Fourier coefficients of the original image. This can be done by finding the average of the magnitude coefficients around each point in the watermarked cover. The difference between the predicted and the actual value in the watermarked version is divided by the pseudo-noise that was used in the embedding process (can be regenerated using the key). Experimental results show that this schema gives a high robustness to the distortion such as blurring and lossy compression.

Chan *et al.* [29] have proposed a modification to the system in [20]. They embed a reduced version of the

watermark several times using the same method. This repetition can be used in the retrieval process to enhance the watermark.

Ó Ruanaidh *et al.* [28] have introduced the use of the Fourier-Mellin transform for watermarking to embed a watermark in RST invariant from a digital image. A Fourier transform is first applied which is then followed by a Fourier-Mellin transform. The invariant coefficients pre-selected for their robustness to image processing are marked using spread spectrum techniques. The inverse mapping is computed (An inverse log-polar mapping followed by an inverse FFT). Note that the inverse transformation uses the phase computed during the forward transformations. To extract the watermark, the watermarked image is transformed into the RST invariant domain which then decodes the watermark.

In Herrigel *et al.* [14] the embedding process starts by dividing the image into adjacent blocks. Then map each block into perceptually "flat" domain by replacing the intensity of each pixel with their logarithm. This step ensures that the intensity of the watermark is diminished in the darker regions of the image where it would otherwise be visible (Weber-Fechner law for HVS response to change of luminance). Fourier transform is then computed for each block. Finally, the watermark is modulated with magnitude components selected from the middle-frequency bands. To detect rotation and scaling, a template ($T$) is embedded into selected components in log polar space. To determine the rotation and scaling that the image suffered, calculate the normalized cross correlation between the log-polar components and the template pattern $T$ to find the point of best correlation. If the image has neither been rotated nor scaled, then this point is at the origin.

Lin *et al.* [25] proposed a watermarking algorithm that is robust to RST distortions. The watermark is embedded using the following steps: Find the discrete log-polar mapping for Fourier magnitude components of the input image (M rows, N Columns). Sum the logs of all values in each column (angle dimension) and add the result of summing column $j$ to the result of summing column $j + N/2$ storing the result in a vector ($v$). Mix the watermark with $v$ using a weighted average of $w$ and $v$ to produce vector $s$. Modify all the values in column $j$ of the log-polar Fourier transform so their logs sum to $s_j$ instead of $v_j$. Invert the log-polar re-sampling of the Fourier magnitude. Thus obtaining a modified Cartesian Fourier magnitude. The complex terms of the original Fourier transform would be scaled to have the new magnitudes found in the modified Fourier transform. The IFFT would be applied to obtain the watermarked image. The detection process is as follows: Apply the same signal-extraction process to the watermarked image to produce the extracted vector $v$. Compute the correlation coefficient between $v$ and input watermark vector $w$. if the correlation is grater than a threshold $T$, then the watermark is present, otherwise it is absent.

## 12. Summary

In this paper, we have given an overview of watermarking in general. We outlined a simple general framework that most of watermarking system relies on. We have listed some applications for watermarking and outlined some main aspects used to classify the watermarking system. We have then focused on the main properties for watermarking system and described several attacks that a watermark system may have to survive. We also have introduced some related subjects such as the human visual system. We have described the features and the strengths of frequency domain in watermarking that make embedding in frequency domain in many ways superiors to embedding in the spatial domain. We have outlined the main characteristics for three domains: DCT, DWT and DFT. We see that embedding in DCT domain is simple and straightforward, DWT can be used efficiently with HVS, and DFT is better used to deal with geometric distortion. We have also introduced some different watermarking techniques in each domain.

## References

[1] Alattar A., "Smart Images Using Digimarc's Watermarking Technology," *Digimarc Corporation in Proceedings of the 12th International Symposium on Electrnic Imaging (SPIE)*, vol. 3971, no. 25, 2000.

[2] Anderson R. J. and Petitcolas F., "On the Limits of Steganography," *IEEE Journal of Selected Areas in Communications*, vol. 16, pp. 474-481, May 1998.

[3] Barni M., Bartolini F., Cappellini V., and Piva A., "A DCT-Domain System for Robust Image Watermarking," *Signal Processing (EURASIP)*, vol. 66, no. 3, pp. 357-372, May 1998.

[4] Barni M., Bartolini F., Cappellini V., Lippi A., and Piva A., "A DWT-Based Technique for Spatio-Frequency Masking of Digital Signatures," in Wong and Delp (Eds.), San Jose, California, vol. 3657, pp. 31-39, 1999.

[5] Bors A. and Pitas I., "Image Watermarking Using Block Site Selection and D. C. T. Domain Constraints," *Optics Express*, vol. 3, no. 12, pp. 512-523, December 1998.

[6] Chae J. J. and Manjunath B. S., "A Technique for Image Data Hiding and Reconstruction without Host Image," in Wong and Delp (Eds), San Jose, California, vol. 3657, pp. 386-396, 1999.

[7] Cox I. J. and Miller M. L., "A Review of Watermarking and the Importance of Perceptual

Modeling," *SPIE, Human Vision & Electronic Imaging II*, vol. 3016, pp. 92-99, 1997.

[8] Cox I. J., Kilian J., Leighton T., and Shamoon T., "A Secure, Robust Watermark for Multimedia," *in Proceedings of the 1st International Workshop on Information Hiding*, pp. 183-206, 1996.

[9] Cox I. J., Miller M. L., and Bloom J. A., *Digital Watermarking*, Morgan Kaufmann Publishers, 2002.

[10] Craver S., Yeo B. L., and Yeung M., "Technical Trails and Legal Tribulations," *Communications of the ACM*, vol. 41, no. 7, pp. 44-54, July 1998.

[11] Ferril E. and Moyer M., "A Survey of Digital Watermarking," http://elizabeth.ferrill.com, 1999.

[12] Gonzalez R. C. and Woods R. E., *Digital Image Processing*, Reading, Prentice Hall, 2002.

[13] Hannigan B. T., Reed A., and Bradley B., "Digital Watermarking Using Improved Human Visual System Model," *in Proceedings of the SPIE*, Digimarc Corporation, vol. 4314, pp. 468-474, 2001.

[14] Herrigel A., O'Ruanaidh J., Petersen H., Pererira S., and Pun T., "Secure Copyright Protection Techniques for Digital Images," in Information Hiding, Aucsmith D. (Ed.), of Lecture Notes in Computer Science, Berlin, Springer-Verlag, vol. 1525, pp. 169-190, 1998.

[15] Hsu C. T. and Ling J., "Hidden Digital Watermarks in Images," *IEEE Transactions on Image Processing*, USA, vol. 8, no. 1, pp. 58-68, January 1999.

[16] Inoue H., Katsura T., Miyazaki A., and Yamamoto A., "A Digital Watermark Technique Based on the Wavelet Transform and its Robustness on Image Compression and Transformation," *IEICE Transactions on Fundamentals of Electronics*, vol. E82-A, no. 1, pp. 2-10, January 1999.

[17] Johnston J., Jayant N., and Safranek R., "Signal Compression Based on Models of Human Perception," *in Proceedings of the IEEE*, vol. 81, no. 10, pp.1385-1422, October 1993.

[18] Kankanhalli M. and Ramakrishnan R., "Content Based Watermarking of Images," *in Proceedings of the 6th ACM International Multimedia Conference*, Bristol, England, pp. 61-70, September 1998.

[19] Katzenbeisser S. and Petitcolas F., *Information Hiding Techniques for Steganography and Digital Watermarking*, Boston, Artech House, 2000.

[20] Kim W. G., Lee J. C., and Lee W. D., "An Image Watermarking Scheme with Hidden Signature," *IEEE Proceeding of the International Conference on Image Processing*, Japan, pp. 206-210, October 1999.

[21] Kundur D. and Hatzinakos D., "A Robust Digital Image Watermarking Method Using Wavelet-Based Fusion," *in Proceedings of the International Conference on Image Processing*, *IEEE*, California, USA, pp. 544-547, October 1997.

[22] Kundur D. and Hatzinakos D., "Digital Watermarking Using Multi-Resolution Wavelet Decomposition," *in Proceeding of the IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 6, pp. 2969-2972, 1998.

[23] Levine M. D., *Vision in Man and Machine*, McGraw-Hill, Toronto, 1985.

[24] Lewis A. S. and Knowles G., "Image Compression Using the 2-D Wavelet Transform," *IEEE Transactions Image Processing*, vol. 1, pp. 240-250, April 1992.

[25] Lin C. Y., Wu M., Bloom J. A., Cox I. J, Miller M. L., and Lui Y. M., "Rotation, Scale, and Translation Resilient Public Watermarking for Images," *in Security and Watermarking of Multimedia Contents II*, in Wong and Delp (Eds.), *in Proceedings of the SPIE*, vol. 3971, pp. 90-98, 2000.

[26] Lumini A. and Maio D., "A Wavelet-Based Image Watermarking Scheme," *in Proceedings of the IEEE International Conference on Information Technology: Coding and Computing*, pp. 122-127, March 2000.

[27] Mintzer F., Lotspiech J., and Morimoto N., "Safeguarding Digital Library Contents and Users," *D-Lib Magazine*, December 1997.

[28] Ó Ruanaidh J. J. K. and Pun T., "Rotation, Scale, and Translation Invariant Spread Spectrum Digital Image Watermarking," *Signal Processing (EURASIP)*, vol. 66, no. 3, pp. 303-317, May 1998.

[29] O' Ruanaidh J. J. K., Dowling W. J., and Boland F. M., "Phase Watermarking of Digital Images," *in Proceedings of the IEEE International Conference on Image Processing*, vol. 3, pp. 239-242, September 1996.

[30] O' Ruanaidh J. J. K., Dowling W. J., and Boland F. M., "Watermarking Digital Images for Copyright Protection," *IEE Proceedings on Vision, Signal and Image Processing*, vol. 143, no. 4, pp. 250-256, August 1996.

[31] Ohnishi J. and Matsui K., "Embedding a Seal into a Picture Under Orthogonal Wavelet Transform," *in Proceedings of the International Conference on Multimedia Computing and Systems*, pp. 514-521, June 1996.

[32] Petitcolas F., Anderson R., and Kuhn M., "Attacks on Copyright Marking Systems," *in Proceedings of the Information Hiding: 2nd International Workshop*, vol. 1525, pp. 218-238.

[33] Petitcolas F., Anderson R., and Kuhn M., "Information Hiding: A Survey," *IEEE*, vol. 87, no. 7, pp. 1062-1077, 1999.

[34] Pfitzmann B., "Information Hiding Terminology," *in Proceedings of the 1st International Workshop on Information Hiding*, pp. 347-350, 1996.

[35] Raymound H., Chan F., and Yeung K. M., "A Frequency Domain Watermarking Scheme," January 2001.

[36] Shoapiro J. M., "Embedded Image Coding Using Zerotrees of Wavelet Coefficients," *IEEE Transactions Signal Processing*, vol. 41, no. 12, pp. 3445-3462, 1993.

[37] Solachidis V. and Pitas I., "Circularly Symmetric Watermark Embedding in 2-D DFT Domain," *in Proceedings of the International Conference on Acoustics, Speech and Signal Processing*, *IEEE Signal Processing Society*, Phoenix, Arizona, USA, pp. 1653-1656, March 1999.

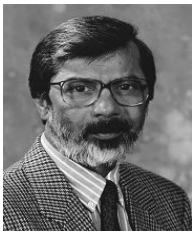
[38] Swanson M. D., Zhu B., and Tewfik A. H., "Transparent Robust Image Watermarking," *in Proceedings of the International Conference on Image Processing*, IEEE, vol. 3, pp. 211-214, 1996.

[39] Tao B. and Dickenson B., "Adaptive Watermarking in the DCT Domain," *in Proceedings of the International Conference on Acoustics and Signal Processing*, 1997.

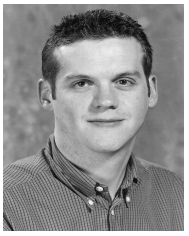
[40] Xia X. G., Boncelet C. G., and Arce G. R., "A Multi-Resolution Watermark for Digital Images," *in Proceedings of the IEEE International Conference on Image Processing*, vol. 1, pp. 548-551, October 1997.

[41] Zaho J. and Koch E., "Embedding Robust Labels into Images for Copyright Protection," *in Proceedings of the International Conference on Intellectual Property Rights for Information, Knowledge and New Techniques*, Munchen, Wien, Oldenbourg Verlag, pp. 242-251, 1995.

**Khaled Mahmoud** received his BSc and MSc degree in computer science from the University of Jordan. Currently, he is a lecturer in the Department of Computer Science at Zarqa Private University, Jordan, and working in his PhD thesis at Loughborough University, UK. His research is in print security and watermarking.



**Sekharjit Datta** received his BSc degree from the University of Calcutta and the MSc and PhD degrees from the University of London. He spent twenty years in industrial research relating to information technology and advanced signal processing, at the Research and Advanced Development Centre of International Computers Ltd, UK, where he worked as a senior research consultant. He became a member of academic staff at Loughborough University in 1987. His research activities have concentrated on various aspects of advanced signal processing. He has specific expertise in the areas of speech, image, bio-acoustic signal processing, and pattern recognition. He has authored/ co-authored over 130 publications in refereed journals and international conference proceedings.



**James Flint** is a lecturer in wireless systems engineering at Loughborough University, UK. He gained a PhD in electronic and electrical engineering for work on efficient electromagnetic modelling of vehicles and was subsequently employed in the Research Department of MIRA Ltd, UK as a project engineer. His current research is in the area of applied signal processing and includes the modelling of novel transducers and the design of high-integrity processors for automotive applications. He is a member of IEEE and IEE, UK, and is a chartered engineer.