CHAPTER 2
Introduction

With the growth of the Internet and the immediate availability of computing resources to everyone, "digitized property" can be reproduced and instantaneously distributed without quality loss at basically no cost. Until now, intellectual property (IP) and value has always been bound to some physical container that could not be easily duplicated, thereby guaranteeing that the creator benefits from his work.

Nowadays, traditional copyright law is inappropriate for the "digital age" and suggest to overcome the restrictions and problems by associating value not to digital content itself but mainly to service and personal 'experience' built around to it. Since personal experience can hardly be duplicated over the Internet, there is no extensive regulations.

Clearly, there are businesses like the music or photography industry that can not adopt this paradigm since they trade basic content and therefore have to stick with traditional copyright enforcement to guarantee income. As audio, video and other works become available in digital form, it may be that the ease with which perfect copies can be made will lead to large-scale unauthorized copying which will undermine the music, film, book and software publishing industries.

One technical way to make law enforcement and copyright protection for digital media possible and practical is digital watermarking which is aimed to automatically detect and possibly also prosecute copyright infringement. There has therefore been significant recent research into "watermarking" (hiding copyright messages) and "fingerprinting" (hiding serial numbers or a set of characteristics that tend to distinguish and object from other similar objects); the idea is that the latter can be used to detect copyright violators and the former to prosecute them.
Table 2.1: Number of publications in the watermarking field during the past years.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pub</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>13</td>
<td>29</td>
<td>64</td>
<td>103</td>
<td>200+</td>
<td>150+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Year</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pub</td>
<td>170+</td>
<td>200+</td>
<td>220+</td>
<td>250+</td>
<td>270+</td>
<td>290+</td>
<td>310+</td>
<td>330+</td>
</tr>
</tbody>
</table>

Watermarking is a relatively young research field. In spite of the very active research (see table 2.1) and the heavy industrial demand, successful real-world applications have not been developed yet. Petitcolas [24] has shown that commercial image watermarking applications available today can be easily attacked.

The music industry is about to set a new standard for compressed audio files in order to replace the ubiquitous but unprotected MPEG audio streams. Likely, audio watermarking will become the key technology in that effort. Similarly, DVD technology depends on video watermarking for copy protection and copy management.

2.1 Copyright Protection

The goal of watermarking for copyright protection [10, 13, 18] is to embed a “mark” into the image data that can identify the copyright holder of the work. Together with owner identification, one might also want to embed a mark (or fingerprint) identifying the buyer of a work for circulation tracking. The mark can be a registered number (like the UPC found on compact disk media), a text message or graphical logo, or some unique pattern (similar to a DNA fingerprint). The term watermark stems from the ancient art of marking paper with a logo for the same purpose.
Digital watermarks can either be perceptible or imperceptible. Visible image watermarks, often the logo of the copyright holder, can be easily applied to the image but are hard to remove. Many applications require the watermark to be invisible, however. This work focuses on invisible watermarks in digital images only.

The embedded, invisible watermark has to be robust against common image processing operations like image compression (e.g. JPEG), image filtering (edge enhancement, contract enhancement, ...), and geometrical transformations (e.g. cropping, scaling, ...). Therefore, the watermark can not be stored in the file format, but has to be embedded into the image data itself. In order to establish a proof of ownership in a trial, a watermarking scheme also has to be secure against intentional malicious attacks.

Figure 2.1: Intellectual property transfer between the creator and the customers of a work. (a) The photography is distributed traditionally and therefore hard to duplicate or manipulate. The clients pay for the work of the IP creator. (b) The work is distributed in electronic, digitized form. Making copies is cheap and easy, there seems to be no reason for a third party to pay.
royalties to the creator of the work. (c) The creator has difficulties to track copies of his digitized work and claim ownership in a legal trial. (d) A watermark

can be used to convince the IP customers to pay the royalties without limiting usage of the work. In addition, a watermark may provide extra information and guarantee data integrity.

2.1.1 Image Authentication and Data Integrity

Another application of watermarking is image authentication and "tamper detection". Digital photographs are being used more and more often as court evidence nowadays. Here, watermarking is used to detect significant modification of the image. Digital images are susceptible to seamless modifications from sophisticated image processing applications. Watermarks can be used here as a means to verify the genuineness of an image. Verification watermarks are required to be fragile, so that any modification to the image will destroy (or detectable alter) the mark. Unlike cryptographic message digests which can only validate identical copies, watermarking for image authentication should tolerate some well-defined image distortion (e.g. file format conversion, re-sampling, re-compression or progressive transmission).

2.1.2 Data Hiding and Image Labeling

Data hiding tries to invisibly embed the maximum amount of data into a host signal (e.g. an image). This allows communication using often enciphered messages without attracting the attention of a third party. Typically, robustness requirements are low for data hiding purposes, instead invisibility and capacity are of prime importance.

Image labeling is an application where information about the image content is encoded as a watermark and inserted into the image to assist image retrieval from a database or provide extra information to the viewer.
Figure 2.2: Data integrity: hard to judge from a digital photography with the naked eye, is (a) or (b) a trustworthy photography
2.2 Application Aspects and Requirements

Different watermarking application have different requirements. Some application scenarios are described by Cox and other authors, as follows.

For image data authentication, the embedded watermark has to be invisible to a human observer and it should be altered (or broken) by virtually any intentional modification of the image. Furthermore, it should be difficult to insert a false watermark and the watermarking scheme should be able to indicate regions where alterations in the image have taken place. Several image copyright protection application scenarios are possible. First, the owner of an image can embed an invisible, robust and quickly extractable watermark to identify unauthorized copies.

Finally, the copyright holder (the seller of an image) might also want to know which customer leaked an unauthorized copy of the data. Here, fingerprinting and circulation tracking techniques come into play to identify not only the seller but also the buyer of an image, (by using image tagging technique) To this aim, some additional requirements are necessary.

2.2.1 Definition and aim

Watermarking is a technique for labeling digital pictures by securely hiding secret information into images. A novel technique for embedding watermarks into a host image on the frequency domain is proposed.

The main aim of digital watermarking is to discourage unauthorized copying or attest the origin of the images and protect the ownership of images for copyright protection.
2.2.2 Content of watermark

Watermarks, which are semantic meaningful pattern (such as binary image or binary data) that can be directly recognized by naked eyes, are important for oriental culture. That means the watermark is generated as a binary pattern (binary image) \( W \rightarrow \{0,1\} \). So, we choose a specific binary data as our watermark content.

2.2.3 Types of watermarking systems

There are three types of watermarking systems, and their difference is in the combination of input and output:

1. Private watermarking (non-blind watermarking): It requires at least the original image \( I' \times I \times K \times \{0,1\} \).

2. Semi-private watermarking (semi-blind watermarking): This system does not use the original image for detection of watermark \( I' \times K \times \{0,1\} \).

3. Public watermarking (blind watermarking): It requires neither the original image \( I \) nor the embedded watermark \( W \) \( I' \times K \rightarrow \{0,1\} \). It remains the most challenging problem in the current research. Out of three systems we choose Private watermarking (non-blind watermarking) as a project work.

2.2.4 Types of watermarking schemes

In general, the watermarking schemes can be classified into two categories

1. Spatial domain approach
2. Frequency domain approach

Early work in the spatial domain approach consisted of modifying the least significant bits (LSB) of images to embed the data. The hidden data was restricted to modifying the two least significant bits. This approach is not well suitable for watermarking system because watermark may be eliminated by common picture cropping operation. So it is believed that the
frequency domain approach has more advantage over spatial domain approach.

2.3 Choice of workspace

The hiding operation is most often carried in a transform domain, such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Mellin- Fourier Transform, Wavelet Transform, etc. Most of still images are compressed as JPEG to communicate through Internet currently. Thus, operate in DCT domain are often robust to JPEG compression. Additionally, embedding operator in the compression domain will minimize the computation time. Therefore, we choose 8 x 8 DCT as workspace.

<table>
<thead>
<tr>
<th>Terms used in this work</th>
<th>Synonymous terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watermark embedding</td>
<td>casting, engraving, etching</td>
</tr>
<tr>
<td>Watermark extraction</td>
<td>recovery, detection</td>
</tr>
<tr>
<td>Host image</td>
<td>cover image</td>
</tr>
<tr>
<td>Signature</td>
<td>embedding message, water mark</td>
</tr>
<tr>
<td></td>
<td>stego image</td>
</tr>
<tr>
<td>Blind watermark</td>
<td>oblivious, public watermark</td>
</tr>
<tr>
<td>Non-blind watermarking</td>
<td>non-oblivious, private watermark</td>
</tr>
<tr>
<td></td>
<td>watermarking</td>
</tr>
</tbody>
</table>

Table 2.2: Watermarking terminology.

2.4 Terminology

The watermarking and data hiding problem has been examined by various research communities (such as image processing, communication and information theory, cryptography,....) each from a slightly different point of view. No standard terminology has been coined yet, although most of the approaches so far seem to share a common core model.
2.5 Human Visual System

The retina of our eye splits a visual signal into different components and each component excites the visual cortex via separate channels [2, 5]. Each component has the following characteristics:

- The spatial location in the image.
- The frequency of the image and
- The orientation of the signal (horizontal, vertical, diagonal).

Based on the knowledge of the structure of the human eye and human visual system (HVS), a hypothetical Cortex transform has been devised that models the known properties. When two signals have similar component characteristics, they excite the same channel in the cortex but are subject to the masking effect. Masking occurs when the detection threshold is increased because of the presence of another stronger signal with similar characteristics. The following effects of the HVS are described in more detail in the next section.

**Contrast masking:** The detectability of one signal in the presence of another signal.

**Frequency sensitivity:** The human eye's sensitivity to sine wave gratings at various Frequencies.

**Luminance sensitivity:** The detectability threshold of noise on a constant background.

**Just-noticeable-difference (JND) [1, 23] threshold:** The threshold beyond which any changes to the respective coefficient will most likely be invisible.

A visual model in the frequency domain can therefore be implemented as follows

---

*Department of Computer Science & Technology, S.K. University, Anantapur"*
1. Apply directional band pass filters [11] to the host image to obtain the amount of energy the image possesses in each spatial-frequency component.

(a) Compute the masking threshold based on the local energy.
(b) Scale the watermark energy in each component (assuming the watermark can be decomposed in the same way) so that it is just below this masking threshold.

In order to design optimal digital watermarking methods it is important to take the human visual system (HVS) into account. To understand effects such as masking and contrast sensitivity, a proper model of the visual information processing and representation in the brain is required. By exploiting these phenomena, the performance of watermarking schemes can be greatly improved.

2.5.1 Contrast sensitivity

Contrast sensitivity (also called intensity sensitivity) describes or predicts the visibility of noise. Assuming that the eye is adapted to the luminance of the uniform background I₀, the goal is to determine the minimal difference in luminance I between the central spot and the surrounding area for the human eye to resolve two stimuli. See figure 2.3 This minimal difference is often called just noticeable difference (JND).
Fig. 2.3. Test setup to determine the contrast sensitivity and just noticeable difference $\Delta I$ of the human visual system for varying background luminance intensities, $I$.

Figure 2.4: The contrast sensitivity function resulting from the test setup presented in figure 2.3. For a large part of the luminance range, the contrast is constant at about 1 to 3% of the luminance. This fraction is called the Weber–Fechner fraction. For low and high luminance values the sensitivity decreases rapidly.
2.5.2 Spatial frequency sensitivity

Also the spatial frequency (the "shape") has significant influence on the sensitivity of the HVS. The human eye is more sensitive to low-frequency noise. In contrast, high-frequency noise is less visible. The frequency response of the HVS is non-uniform which results in various phenomena, e.g. over-sensitivity in high-contrast areas and especially at edges. One phenomenon called the Mach band effect is illustrated in figure 2.4. The image shows a horizontally varying luminance, where the luminance changes in equal steps. Although each step has a uniform luminance, we perceive the intensity inside a step not as uniform, i.e. brighter on the left and darker on the right side of the edge between two steps.
2.5.3 Masking

Visual masking is a perceptual phenomenon where artifacts are locally masked (hidden) by the image. The image acts as a background signal that reduces the visibility of the artifacts due to image manipulation. Given an image distorted with additive noise, we can observe that the noise is much more visible in flat areas than in areas with high activity, such as textured areas.

2.6 Terminology

The watermarking and data hiding problem has been examined by various research communities (such as image processing, communication and information theory, cryptography,...), each from a slightly different point of view. No standard terminology has been coined yet, although most of the approaches so far seem to share a common core model [180].

2.7 Relationship to Cryptography

Image cryptography is considered as an encoding technique for data transmission through communication channels under condition that a third party could not read and interpret the data [21]. However, transmitted data, especially in scrambled form, can attract attention and impel law-enforcing authorities to take a closer look [13]. Nevertheless, cryptography has become one of the main tool for privacy, access control, authentication, digital signatures and secure messaging.

Steganography implants the secret message in some form of cover data, typically digital images or video streams, concealed as ‘noise’. Without the correct key, it is virtually impossible to extract the hidden message or even detect its presence. This places an additional burden on the cryptanalyst who now has to examine unsuspicious-looking data for embedded steganographic messages [19].
Steganographic messages are usually encrypted in order to increase security, but also to conceal any statistical significant patterns.

The second relationship between cryptography and watermarking stems from the shared semantics of public – and private-key crypto-systems versus public and private-key watermarking systems. In private-key crypto-systems, the same key is used to encrypt and decrypt a message (symmetric cipher), while in public-key crypto-systems, the keys for encryption and decryption are different (asymmetric cipher).

2.7.1 Public-key Watermarking

In a public-key watermarking system, a digital object is marked with the private key but the presence of a watermark can be checked using a public key. Of course, computation of the corresponding private key is infeasible, despite the availability of the public key and the algorithm of the watermarking system. The public key only allows to read the watermark, it can not be used to remove or forge a watermark. Public-key watermarking generally assumes that the unmarked original host is not required in the detection or extraction process (blind recovery).

Traditional watermarking systems using symmetric, private keys almost always allow to remove or insert forged watermarks. Public-key schemes have to permit secure watermark verification by third persons. However, no public-key watermarking schemes is known to exist, since most current approaches can not withstand public detector device attacks as described by Kalker [15].
2.7.2 Asymmetric watermarking

Asymmetric watermarking techniques do not refer to the original image and employ different parameters than the ones used in the embedding process. The terms public–key watermarking and asymmetric watermarking are often used in the same context. If you take the terms literally you might differ between asymmetric watermarking, the keys enabling watermark detection differ from the keys needed for embedding the watermark, and public–key watermark, asymmetric watermarking might actually be a way of realizing a public–key watermarking system.

The public detector device attack described by Kalker and Linnartz which is based on the linearity of the detection process, does not work on asymmetric schemes.

2.7.3 Visual Cryptography

Visual cryptography is a type of a cryptographic scheme to conceal images without any cryptographic computations. It is a visual variant of the \( k \) out of \( n \) secret sharing problem. One would produce transparencies that contain parts of the secret. Any \( k \) of the \( n \) transparencies staked on a heap would reveal the secret, but less than \( k \) transparencies do not reveal any information. See figure 2.5 for an example for \( k=2 \).
Figure 2.6: Visual cryptography. The secret information (a) is split into two shares, (b) and (c). Only when combining the shares (d), the hidden information is revealed.
2.7.4 Conclusions

According to Kutter [18], the following conclusion can be drawn from our understanding of the HVS with regards to watermarking.

- High frequencies are less visible than low frequencies.
- Studies of the visual cortex showed a multi-resolution characteristic of our visual system. [5]
- In order to embed the watermark as strong as possible, we have to embed it just below the JND. This means, we have to visually adapt the watermark using contrast sensitivity and masking effects.
- The distribution of the blue cones is less dense than the distribution of the red and green cones in the human eye. Therefore, we suggest to put most watermark energy in the blue color component.