CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Cryptography and steganography are used as methods to add secrecy to communications. The following sections explain the basic concepts of cryptography, steganography and watermarking. It also lists some of the most common applications of watermarking in today’s world. Finally the objectives of this thesis are mentioned.

Digital watermarking includes number of techniques that are used to imperceptibly convey information by embedding it into the original data. There has always been a problem in establishing the identity of the owner of an object. In case of a dispute, identity was established by either printing the name or logo on the objects. But in the modern era where things have been patented or copyrighted, more modern techniques to establish the identity and leave it untampered have come into picture.

Unlike printed watermarks, digital watermarking is a technique where bits of information are embedded in such a way that they are completely invisible. The problem with the traditional way of printing logos or names is that they may be easily tampered or duplicated. In digital watermarking, the actual bits are scattered in the image so that they cannot be identified by unauthorized persons and show resilience against attempts to remove the hidden data (Kundur et al 2001).
1.2 CRYPTOGRAPHY

Cryptography, a word with Greek origins, means “secret writing”. It can be defined as the science of transforming messages to make them secure and immune to attacks. It allows two people, commonly known as Alice and Bob, to communicate with each other securely. This means that an eavesdropper known as Eve will not be able to listen their communication.

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext. A decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm. This process is shown in Figure 1.1.

![Cryptography for secure communication](image)

Figure 1.1 Cryptography for secure communication

1.3 STEGANOGRAPHY

While cryptography is about protecting the content of the messages, steganography is about concealing their very existence (Yang et al 2007). Steganography comes from a Greek word that means covert writing. It embeds secret data into digital media such as images, texts, audio and video. Examples can be thought as messages exchanged by spies in covert communication. Steganography is the art and science of writing hidden
messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message as shown in Figure 1.2.

Let us consider that Alice, who wants to share a secret message $m$ with Bob, selects randomly a cover object $C$. The message to be shared is then embedded into $C$, by using key $K$ (called stego-key), and the cover object $C$ is transformed to stego object $S$. This stego object can be transmitted to Bob without raising any suspicion. This should be done in such a way that a third party knowing only the apparently harmless message $S$ cannot detect the existence of the secret. The cover object could be any data such as image files, written text or digital sound. In a perfect system, a normal cover object should not be distinguishable from the stego object, neither by a human nor by a computer looking for statistical patterns.

![Diagram of a steganographic system](image)

**Figure 1.2 A steganographic system**

Alice transmits the stego object $S$ to Bob over an insecure channel. Bob can reconstruct the message $m$ by using the same key $K$ as used by Alice during embedding the message in the cover object. The extraction process does not need any knowledge of the cover object.
Any third person watching the communication should not be able to decide whether the sender is sending covers with messages embedded into them. In other words, a person with a number of cover objects should not be able to tell which cover object has the message embedded in it, and the security of invisible communication lies in the inability to distinguish cover objects from the stego objects.

However, all the cover objects cannot be used to hide the data for covert communication, since the hidden data should not be visible to anyone, not involved in the communication. The cover object needs to have sufficient redundant data, which can be replaced by secret information.

1.4 WATERMARKING

Watermarking is a process in which a signal is hidden or embedded into another signal, usually an image, text, audio, or video (Cox et al 1999). Images are the major component of multimedia content. Examples of images are digital arts, illustrative diagrams, cultural heritage paintings in digitized form and digital photographs. Advances in computing hardware, software, and networks have created threats to copyright protection and content integrity. For instance, images can be copied, modified, and distributed easily. Digital watermarking is a potentially good tool to enable copyright protection. Encryption can offer confidentiality and integrity in content protection, and the decrypted content can be further protected using digital watermarks.

The watermarking process embeds a watermark into the image without significantly degrading its visual quality. Then the watermarked image can be made public or sent to the end user. Later, the detected watermark can be used for the purposes of copyright protection and content authentication.
The working principle of the watermarking techniques is similar to the steganography methods. A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a key which could be either a public or a secret key. The key is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark. The embedding and extraction processes of watermarking are shown in Figures 1.3 and 1.4.

![Figure 1.3 Digital Watermarking – Embedding](image)

![Figure 1.4 Digital Watermarking – Extraction](image)

For the embedding process the inputs are the watermark, cover object and the key. The watermark can be text, numbers or an image. The output is the watermarked object.

The inputs during the extraction process are the watermarked data and the key. The output is the recovered watermark. The watermarking technique is referred to as “blind”, if the original image is not needed for extraction; it is “non-blind”, if the original image is used in extraction (Wang and Lin 2004).
1.5 PROPERTIES OF DIGITAL IMAGE WATERMARKING

The following section explains the important properties of digital image watermarking.

1.5.1 Imperceptibility

Imperceptibility means that the watermarked image should be perceptually equivalent to the original image (Su and Girod 2002). Watermarking should be done in a way such that it does not affect the quality of the image after watermarking. The changes in the image should not be noticeable to the naked eye.

1.5.2 Robustness

Robustness means that the watermarking scheme should preserve the watermark under various attacks. The attack could be anything like rotation, translation, cropping, scaling or passing the image through various types of filters. Sometimes noise may be introduced by the attacks.

There are several ways of classifying watermarking methods. One of the most widely adopted classifications is based on robustness. Under this classification, watermarking can be grouped into three types (Podilchuk and Delp 2001). They are robust, fragile and semi-fragile watermarking.

1.5.2.1 Robust Watermarking

Robust watermarking can resist both malicious and non-malicious distortions (Liu and Tan 2002). An unauthorized party should not be able to destroy the watermark without making the watermarked object as useless. Attempts to remove the watermark will result in severe degradation of its
visual quality. Watermark will be detectable or extractable after application of common signal processing operations to the watermarked object.

Application-wise, robust watermarking schemes are suitable for copyright protection because they can resist common signal processing operations.

1.5.2.2 Fragile Watermarking

In fragile watermarking (Yu et al 2008), watermark is embedded in such a way that any manipulation or modification of the watermarked image would alter or destroy the watermark. In this technique, watermark is easily destroyed by all image distortions. It can be used to detect tampering and authenticate an image because it is sensitive to changes.

1.5.2.3 Semi-fragile Watermarking

In semi-fragile watermarking (Maeno et al 2006), watermark can be destroyed by certain types of distortions while resisting other minor changes. Semi-fragile watermarks, try to differentiate between content-preserving (nonmalicious) processes, e.g., compression, and malicious manipulations, e.g., removal of objects from a scene. Watermarks in this class are designed to withstand content-preserving operations, while detecting any malicious manipulations (Celik et al 2002). Semi-fragile watermarking is usually applied in some special cases of authentication and tamper detection.

1.5.3 Security

There is always a possibility that the attacker knows the exact algorithm for detecting and rendering the watermark inactive. The only way to secure the watermark is the selection of a key used for watermarking. Now,
even if the attacker on the other side knows the exact algorithm, it should be practically impossible to find the exact key (Wang et al 2002).

1.6 APPLICATIONS OF WATERMARKING

The requirements of a digital watermarking system depend upon the specific type of application. A few most common applications involve the following (Ru and Gang 2006).

1.6.1 Copyright Protection

The author embeds a watermark, into the digital object without the loss of quality. Whenever the copyright of a digital object is in question, the watermark is extracted to identify the rightful owner. Obviously, the watermark has to be designed to survive the attacks that pirates could perform to remove it. Even if this application was one of the first to be faced, it is also one of the most challenging, since the opponents are supposed to be aware of the watermark existence and a wide range of attacks has to be considered. Robust watermarks can be used in copyright protection because they are persistently associated with the object.

1.6.2 Fingerprinting

It is a way to achieve copy deterrence by providing a mechanism to trace unauthorized copies of a protected work. In each copy of data that is distributed, the owner inserts a distinct watermark, called fingerprint, which unambiguously identifies the buyer. In this way, if an unauthorized copy of the protected work is found, the owner of the copyright can retrieve the identity of the buyer that illegitimately distributed the content.
1.6.3 Copy Control

It aims at preventing users from making copies of a protected content, when this is not allowed. The embedded watermark describes the rights of copying owned by the user and every recording device is supposed to be equipped with a watermark detector, so that the device can prohibit recording whenever the watermark that prevents copying is detected in the content.

1.6.4 Authentication

The availability of cheap and effective digital multimedia editing tools makes easy the modification of original contents without leaving any perceptible traces of tampering. In this way, a digital data can never be trusted to be authentic. In this application, the embedded watermark, which is modified together with the host signal, reveals when it has been tampered, even after small changes, so that modifications on the watermarked content can be detected (Kundur and Hatzinakos 1999). These schemes are said to use fragile watermarks, in contrast to robust watermarks which must remain unchanged by processing. As an example, they are used to guarantee the integrity of automatic video surveillance data.

1.6.5 Error Recovery

Transmission of data in compressed formats, such as Joint Photographic Experts Group (JPEG) or Moving Picture Experts Group (MPEG), is vulnerable to transmission errors. A typical way to cope with these errors is channel coding at cost of introducing a controlled amount of redundancy. A similar approach can be performed through data hiding, which allows hiding into the content redundant information that can be possibly used
to recover from errors at the decoder side. As an example, the hidden redundant information can be simply a low quality version of the content.

1.6.6 Covert Communications

The ultimate goal of covert communications is to hide the very existence of the hidden message, so that the major requirement for this application is the undetectability of the presence of the message by a third person. The term steganology is used to refer to both steganography and steganalysis, which are respectively the practice of undetectably altering a content to embed a secret message and the practice of discovering the presence of steganographic channels.

1.6.7 Link Quality Estimation

A fragile watermark has been also used to provide a method for blind estimation of a quality of multimedia communication links at the receiver side. This quality assessment system is based on the evaluation of the mean squared-error between the received and the actual watermark signal, providing a quality measure of the effective status of the link without increasing the bit rate.

1.6.8 Broadcast Monitoring

A commercial advertisement may be watermarked by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring systems can then receive broadcasts and check for these watermarks, identifying when and where each clip appears. This proves very helpful for the advertisers as they actually pay for only the number of times the advertisement was actually relayed.
1.6.9 Medical Applications

Names of the patients can be printed on the X-ray reports and Magnetic Resonance Imaging (MRI) scans using techniques of visible watermarking. The medical reports play a very important role in the treatment offered to the patient. If there is a mix up in the reports of two patients this could lead to a disaster.

As a final comment, this brief overview cannot be clearly exhaustive and exact boundaries between applications are quite difficult to be drawn, since some of them can be overlapping.

1.7 MOTIVATION

Recent developments in computing hardware, software, and networks have created threats to copyright protection. For example, images can be copied, modified, and distributed easily. Digital watermarking is a potentially good tool in enabling copyright protection. Encryption can offer confidentiality and integrity in content protection, and the decrypted content can be further protected using digital watermarks. The watermarking process embeds copyright information into the image without significantly degrading its visual quality. Then the watermarked image can be made public or sent to the end user. Later, the detected watermark can be used for the purposes of copyright protection.

1.8 OUTLINE OF THE THESIS

The central idea of this thesis is to develop robust digital image watermarking algorithms using DWT for application to gray scale and color images. Chapter 2 surveys the basic and existing watermarking techniques. Some of the possible attacks are also discussed in Chapter 2. Chapter 3
focuses how to embed and recover watermark using one-level DWT in gray scale and color images. Chapter 4 focuses how to embed and recover watermark using two-level DWT in gray scale and color images. Chapter 5 deals with analysis of results obtained using DWT at level one and two for both gray scale and color images. Also the obtained results are compared with existing methods. Chapter 6 concludes the performance of the proposed methods.

The aims of this research are three-fold:

(i) To investigate the strength and limitations of current watermarking schemes.

(ii) To design and develop new schemes to overcome the limitations.

(iii) To evaluate new schemes using application scenarios of copyright protection.

To preserve the visual appearance of images, one has to focus on invisible watermarking. The experiments are performed using gray scale images and color images.

1.8.1 Objectives

The objectives of this research are:

- To design, implement and improve digital image watermarking system using DWT by proposing randomized methods of embedding and extracting the watermark for copyright protection.
• To analyze the performance of proposed methods in terms of watermark imperceptibility of the watermarked image using Peak Signal to Noise Ratio (PSNR) calculations and watermark robustness of the extracted watermark using Normalized Correlation (NC) value.

• To study the effects of various types of attacks on the proposed methods.

1.8.2 Problem Definition

To design and develop robust digital image watermarking schemes for the copyright protection of gray scale and color images. Specific further the motivation of the work also explains about the problem.

1.8.3 Significance

Robust digital image watermarking is mainly used for copyright protection. Copyright protection inserts copyright information (watermark) into the digital image without the loss of quality. Whenever the copyright of a digital image is in question, the watermark is extracted to identify the rightful owner.

1.8.4 Methodology

Frequency domain watermarking techniques using discrete transforms are commonly used in the implementation of digital image watermarking. Frequency domains such as Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and DWT are widely used in digital image watermarking. In this research digital image watermarking system is developed using DWT domain. The main advantage of the DWT is that it is
believed to give more accurate model of the human visual system (HVS) as compared to the DFT or DCT (Barni et al 2001).

1.8.5 Limitations

The developed method is applicable only for copyright protection of digital images. For audio and video watermarking the proposed approach needs development of separate algorithms.