Chapter 1

Introduction

The rapid advance of data compressions leads to massive multimedia data transmission including 2-D/3-D images, videos, audios and speech over the wide-spreading wired and wireless networks in the recent years. Moreover, a variety of low-cost digital devices and storage media promotes wide distribution of multimedia data. The increasing popular and user-friendly multimedia manipulation tools enable nonprofessionals to practice complicated operations on digital data. Consequently, the demand for copyright protection and content integrity techniques arise since the content owners are urgent to protect their work from illegal copying and editing.

The secure communication and access of digital data can be restricted via the technology of cryptography. The data content is concealed from unauthorized persons; nevertheless, the decrypted data content at the user end is exposed to possible infringement. Digital watermarking is one of the techniques that help reducing this from happening. Digital watermarking places hidden messages such as ownership information permanently in the host data while it is not detected by human perceptions so that the commercial value of the host data is retained. People may access or modify the data content for normal use and still the embedded important message can be detected.

The requirements regarding watermarking designs may vary with applications (e.g., copyright control, transaction tracking and content authentication) and host data types (e.g.,

image, video and audio). A watermark can be designed to be either robust or fragile for different purposes. Till now, it is still very difficult for a single watermarking scheme to meet all requirements due to the conflicts among different requirements.

In this thesis, both the analyses and designs of robust digital image watermarking techniques are studied. In this chapter, Section 1.1 describes the definition of digital watermarking. The contributions of this thesis are outlined in Section 1.2. Finally, the thesis organization is given in Section 1.3.

1.1 What is Digital Watermarking

Before discussing digital watermarking schemes, we first give a commonly accepted definition of watermarking and discuss the differences between *steganography* and *watermarking* because they are different though related subjects [1]. The term "steganography" comes from Greek words *stegano* meaning "covered" and *graphia* meaning "writing". This term emphasizes that the communication is in a secret sense and thus the message existence is concealed. Watermarking, the art of inserting "content related message" (watermark) into the host data, is one of the information hiding techniques which either make the inserted information imperceptible (watermark) or keep the data distinct from a specified group (non-watermark).

In general, the watermarking design issues consist of robustness, imperceptibility, data payload, false alarm/false rejection, blind detection and security. One essential requirement of a watermarking system is robustness. A steganographic system, on the other hand, focuses on security and capacity issues [2]. In this thesis, the term *watermarking* is used since our work primarily aims at the robustness issue.

1.2 Problem Statements

Our work is divided into two parts. For the first target, we are interested in the watermark payload and error detection probability under the combined criteria of robustness and visual fidelity. Previous researches have tried to estimate the theoretical watermark capacity bound (e.g., [3]), to improve the watermark robustness, or to decrease the detection error probability, but few of them identify the exact locations of the transform coefficients of a given picture for watermark embedding under given constraints. Intuitively, one may think that using more coefficients would be more beneficial for detection robustness and reliability. However, the tradeoffs among conflict requirements much complicate this problem. Moreover, different types and amount of attacks produce different patterns and magnitude of damages on the watermarks.

The first work employs a non-blind detector to explore performance-limit. Since we adopt the non-blind detection structure, there is no synchronization problem due to attacks. Our second work further tackles the problem of blind detector with geometric distortion. In the delivery of multimedia data, either the intentional or unintentional attacks may be applied to the watermarked data. A success attack should keep the perceptual quality of the attacked data while render the watermark undetected. Attacks can roughly be classified into two sets: geometric distortions and noise-like signal processing. Geometric distortions can induce synchronization errors between the extracted watermark and the original watermark, even though the watermark may still exist in the attacked image. Designing a geometric distortion invariant watermark is a difficult and complicated task.

1.3 Contributions

In this thesis, we tackle several important problems in watermarking as described in Section 1.2. The main contributions of this thesis are as follows.

1. A procedure is proposed for identifying the effective (watermarking) coefficients for a given natural image. This set of coefficients ensures both high detection reliability and watermark robustness, and in the meanwhile, the watermark is kept transparent. Since the achievable rate (data payload) in the case of blind detection is upper-bounded by that of non-blind detection [3], the non-blind detection structure is employed and the attack source is assumed to be known for exploring the best achievable performance under the above assumptions. To a certain extent, we are exploring the "performance limit" of DCT-domain watermarking for a given specific attack. In general, this method can be extended to other watermarking schemes with multiple attacks.

2. A set of coefficient selection rules is presented for efficiently determining the effective DCT watermarking coefficients for natural images. The JPEG compression is taken as an example of the attacks. These rules are simple in computation and they are derived from the theoretically optimized data set with the aid of parametric classifiers. They improve the watermark robustness (correct decoding) and, in the mean time, they decrease the error detection probability (correct detection).

3. A robust digital image watermarking scheme that resists both geometric distortion and signal processing attacks is proposed. This scheme combines image feature extraction and image normalization techniques. We adopt a feature extraction method called Mexican Hat wavelet scale interaction. The extracted feature points can survive a variety of attacks and can be used as reference points for both watermark embedding and detection. The normalized image of an image (object) is nearly invariant with respect to rotations. As a result, the watermark detection task can be much simplified when it is applied to the normalized image. The algorithm is less sensitive to the local variation since we apply image normalization to non-overlapped image disks centered at the feature points.

1.4 Thesis Organization

This thesis is structured as follows. In Chapter 2, a general watermarking system framework and the basic requirements for designing a robust watermarking scheme are described. Several possible attacks and watermarking applications are also stated. Chapter 3 reviews the previous works related to our proposed schemes. In Chapter 4, the first contribution of our dissertation is presented. It is an effective coefficient selection procedure for DCT-domain perceptual watermarking. A simplified fast scheme derived from the iterative procedure is further proposed in Chapter 5. We then develop a geometric invariant robust image watermarking scheme in Chapter 6. Finally, Chapter 7 concludes this thesis.