Chapter 1
Introduction

1.1 Motivation

With the rapid growth of digital processing techniques, many kinds of digital multimedia, such as digital image, text, audio, and video, are developed in today's digital world. Digital multimedia can be preserved permanently and spread quickly via the Internet, so people can search digital media fast and find what they want on the Internet easily. This facilitates the propagation of knowledge, but on the other hand, results possibly in unauthorized uses of digital media and loss of intellectual property rights. Therefore, how to protect the copyright of digital media has become an urgent issue. In our study, we will focus on dealing with digital images.

Many researches have been proposed to solve the above-mentioned problems. The most general way is to use digital watermarking techniques for verifying the copyright of images. Such techniques can be classified into two types: visible watermarking and invisible watermarking. By embedding a watermark signal, which can be extracted later, into an image, the copyright of the image can be protected. Many researches have made efforts in invisible watermarking [1]-[8], while researches on visible watermarking are fewer [9]-[10]. A reason accounting for this might be that a visible watermark appearing on an image diminishes the commercial value of the image. Nevertheless, a considerable advantage of embedding a visible watermark in a given image is that it conveys an immediate claim of the ownership of the image and also prevents or at least discourages unauthorized uses of the

copyrighted image.

When using watermarking techniques to protect the copyright of images, the owner needs to preserve both original images and corresponding watermarked ones, called *cover image*s and *stego-images*, respectively, in this study. This demands double storage space to keep cover images and their stego-versions and brings in waste of storage space. Therefore, developing a *lossless recovery* method for removing the embedded watermark is quite worthy. By such a kind of method, the owner only needs to preserve stego-images without saving original images, which are exactly the results of lossless recovery processes using stego-images as input.

In addition, the processes of invisible watermark and visible watermark embedding usually result in image distortions. Even though the distortions are usually tiny, in some applications, such as medical and military, such distortions are unacceptable due to the high precision requirement in these applications. Then, using lossless watermarking techniques to protect copyright will be the best choice.

Finally, the results of the copyright verification might be disputed sometimes. That is, illegal users might disclaim the infringement of the copyright of images. This highlights the necessary for a *central image authentication center* for arbitration of the dispute. A central image authentication center can function as a trusted third party to convince illegal users of the results of the copyright verification. In this study, we propose an innovative method for online image authentication which can be carried out in the central authentication center.

1.2 Review of Related Works

1.2.1 Lossless Invisible Watermarking

Many different invisible watermarking techniques for copyright protection have been proposed in recent years, but most of the techniques are lossy, that is, not revertible, and few are lossless. A lossless invisible watermarking technique for circular interpretation of bijective transformations was proposed in Vleeschouwer *et al.* [4]. And in Thodi *et al.* [4], a reversible watermarking algorithm based on prediction-error expansion and histogram shifting was proposed. This method can embed a larger payload than the existing schemes of relying on compression to create space for embedding, like Tian [6], Goljan *et al.* [7] and Celik *et al.* [8]. Zou *et al.* [5] presented a semi-fragile lossless digital watermarking scheme based on the integer wavelet transform (IWT), which embeds data into some IWT coefficients. The exact cover media can be losslessly recovered if the stego-image has not been altered.

1.2.2 Removable Visible Watermarking

Some visible watermarking techniques for copyright protection have been proposed in the last few years. None of the visible watermarking techniques focus on the property of “lossless.” In Hu *et al.* [9], a removable visible watermark system was implemented using the discrete wavelet transform. The original image can be legally recovered with good visual quality, but not exactly. In the system proposed in this study, the original image can be losslessly recovered without any distortion.

1.3 Overview of Proposed Methods

1.3.1 Terminologies

The definitions of several terms used later are given first as follows.

1. Cover image: a cover image is an image into which a watermark signal is embedded.
2. Stego-image: a stego-image is an image that is produced by embedding a watermark signal into a cover image.
3. Recovered image: a recovered image is an image that is produced by removing an embedded visible watermark from a stego-image.
4. Embedding process: an embedding process is a process to embed data into an image.
5. Extraction process: an extraction process is a process to extract watermark from an image.
6. Lossless recovery process: a lossless recovery process is a process to remove the embedded visible watermark from a stego-image and obtain exactly the cover image.
7. Central image authentication center: a central image authentication center functions as a trusted third party issuing certificates indicating the authentication results of copyrighted images.
8. Local image authentication center: a local image authentication center is an organization which has registered their images at the central authentication center and has the capability to conduct initial image authentication works using programs provided by the central image authentication center.
9. Certificate digest: a certificate digest is a 160-bit hash value produced by

the Secure Hash Algorithm-1 (SHA-1) with an input certificate.

1.3.2 Brief Descriptions of Proposed Methods

A diagram illustrating the proposed system of authentication centers is shown in Figure 1.1. A brief description of the proposed methods involved in the system is given here, and descriptions of more detailed structures and processes of the proposed system will be given in the following chapters.

A hierarchical image authentication system, which includes a single *central image authentication center* and multiple *local image authentication center*s, is implemented in our study. The central image authentication center is a third party, and the local image authentication centers can be some kinds of organizations, such as museums, galleries, and so on. After a digital museum, for example, registers their digital archives at the central image authentication center, it takes on the role of a local image authentication center with four main functions, as described in the following.

The local image authentication centers can search suspected images in webpages and in public FTP severs, and then check these suspected images for possibility of copyright infringement. We have proposed a *progressive* image matching technique for checking suspected images. If the suspected image is really a copyright-infringed one, the local image authentication center sends the uniform resource locator (URL) of the suspected image to the central image authentication center. And the central image authentication center will reconfirm the infringement of the copyrighted image, and issue a certificate with adequate security protection to keep a record of the infringement. The local image authentication center can then file a lawsuit with the certificate as a proof of the infringement when he/she requires.

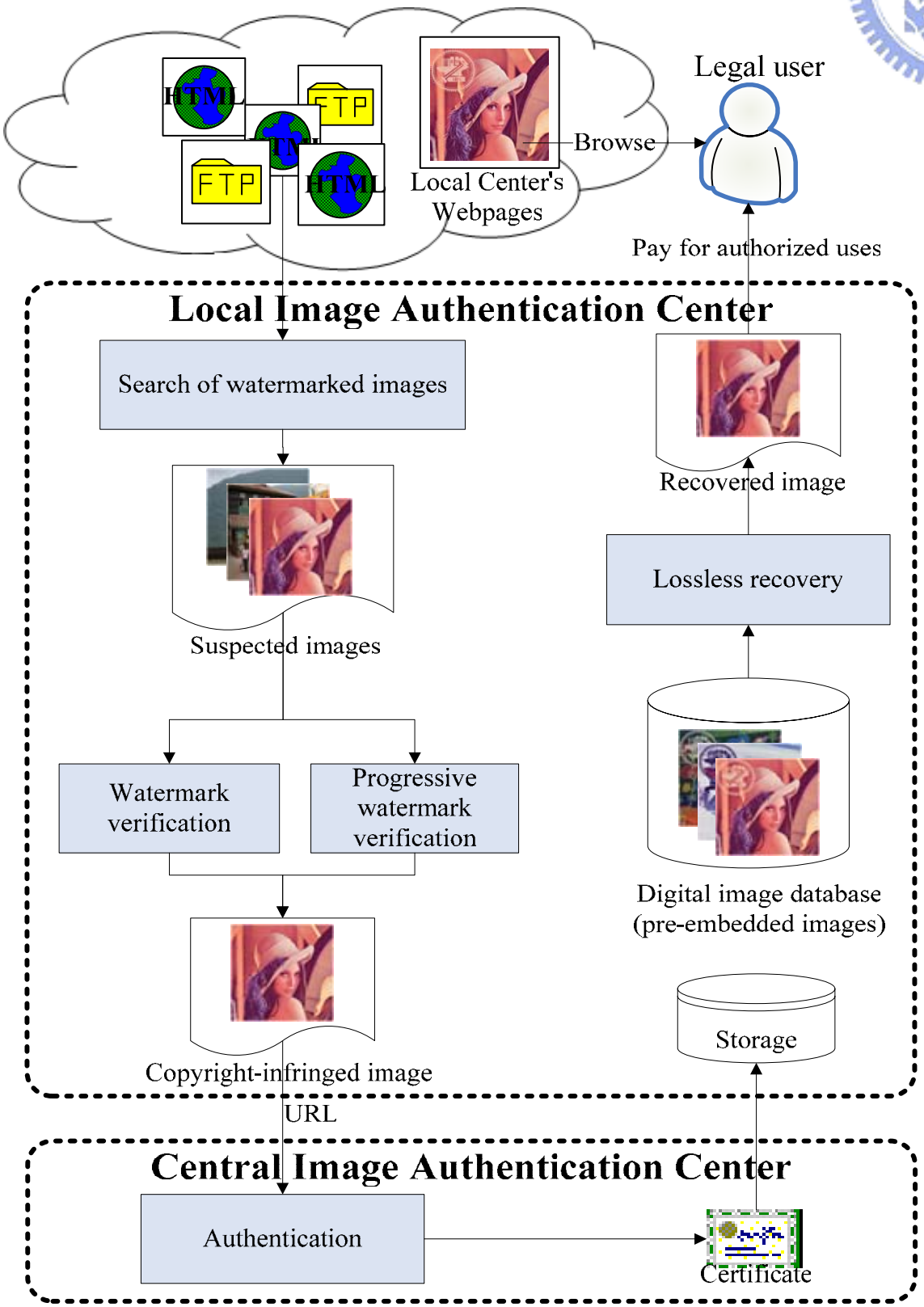

Figure 1.1 A diagram illustrating proposed system of authentication centers with multi-capabilities.

In addition, we propose a visible lossless watermarking technique for copyright protection. The local image authentication center can embed watermarks into their images in advance and preserve only the watermarked images in the database. The local image authentication center can post the watermarked images on their websites for browsing and even allow free downloads. However, the watermark-free original image can be obtained when a legal user pays and requests for authorized uses of the image.

1.4 Contributions

Some major contributions made in this study are listed as follows.

1. A hierarchical online image authentication mechanism is proposed.
2. An image authentication system with multi-capabilities is proposed.
3. A method for online search of suspected images is proposed.
4. A system for integration of visible watermarking techniques and invisible watermarking techniques is proposed.
5. A novel mechanism for image authentication with security protection of authentication certificates for copyright claiming is proposed.
6. An effective method for fast watermark verification is proposed.
7. A novel method for robust lossless visible watermarking is proposed.

1.5 Thesis Organization

The remainder of this thesis is organized as follows. In Chapter 2, a more detailed overview of the proposed hierarchical online authentication centers with multi-capabilities is described to introduce the following chapters. In Chapter 3, the proposed methods about online search and verification of watermarked images for copyright infringement detection are described. And then, the proposed process for online image authentication and a method for security protection of authentication certificates are described in Chapter 4. In Chapter 5, a method for fast watermark verification of compressed images is described. In Chapter 6, a method is proposed to embed visible watermarks into palette images and to remove embedded watermarks losslessly. Finally, conclusions and some suggestions for future works are included in Chapter 7.