Chapter 1
Introduction

1.1 Motivation

Due to the rapid development of multimedia technologies and the popularity of the Internet, various multimedia data can be transmitted or displayed through the Internet quickly and conveniently. Digital videos, which are popular multimedia files transmitted on the Internet recently, can be acquired and tampered with easily through advanced information technologies. Therefore, it is necessary to develop effective methods for protecting copyrights of digital videos as well as authenticating digital videos.

For video copyright protection, one of several useful approaches is to utilize visible digital watermarking techniques. When using such techniques to certify the copyright of a video, a chief advantage is that the visible watermark can immediately claim the ownership of the video. But the video content will be partially occluded due to the visible watermark. In order to solve this problem, an *active visible watermarking* technique is developed in this study in which an active agent is designed to protect downloaded videos by visible watermarks, and in the mean time legal users can watch complete videos through the active agent which removes the watermark.

For video authentication, the main purpose of this study is to verify the integrity and fidelity of a video, especially surveillance videos. Because surveillance videos usually contain suspicious or criminal acts, malicious users might acquire the video in an illegal way and tamper with it for misrepresentation. A useful approach to video authentication is to embed invisible authentication signals into a video, resulting in a

protected video. If a protected video is tampered with, the hidden authentication signals will be destroyed. Then by checking the presence of the hidden authentication signals, we can verify the fidelity of the protected video. In addition, we may want to know how a protected video was tampered with; in other words, we want to check the integrity of the protected video. For the reasons mentioned above, we can understand that a good video authentication system should not only check whether a video has been tampered with or not but also display where and how the tampering was made. And it is tried in this study to design such a video authentication system.

Furthermore, with the rapid rise of crime rates nowadays, environment surveillance systems become more and more essential for security monitoring in public places. Generally speaking, most frames in surveillance videos taken by stationary cameras are still images with the same backgrounds. But what we really care about is those infrequent frames in the surveillance video, which contain motions or specific events. Hence, an effective searching method is desired for the convenience of finding out such frames. One useful approach for searches in surveillance videos is to embed information related to motions or specific events into corresponding frames by a data association technique.

In this study, we will develop appropriate techniques for accomplishing the different purposes mentioned above.

1.2 General Review of Related Works

In this study, some new methods for information hiding applications are developed by embedding a variety of information within videos. Chae et al. [16] proposed a method to hide data into the DCT coefficients of a host video, in which the method is adaptive to the local texture content of the host video frame blocks. The

reason why the data are hidden in the texture region is that the human visual system (HSV) is more sensitive to the change in low frequency regions than in high frequency ones. Besides, there are also many approaches to hiding data into a video.

A detailed review of active agent, visible watermarking, video authentication, and video data hiding techniques developed in recent years will be made in Chapter 2. In addition, because the proposed information hiding and watermarking techniques are applied to MPEG-4 videos, we will also make a review of the MPEG-4 standard in Chapter 2.

1.3 Overview of Proposed Methods

1.3.1 Terminologies

The definitions of some related terminologies used in this study are described as follows.

1. *Watermarked video*: a watermarked video is a video in which a visible watermark has been embedded.
2. *Recovered video*: a recovered video is a video made by removing the embedded visible watermark from a watermarked video.
3. *Protected video*: a protected video is a video in which authentication signals have been embedded.
4. *Video authentication*: video authentication is a process for verifying the integrity and fidelity of a suspicious surveillance video.
5. *Captured image*: a captured image is an image which is taken by a web camera.
6. *Stego-video*: a stego-video is a video in which some digital information is embedded.

1.3.2 Brief Descriptions of Proposed Methods

1.3.2.1 An Active Copyright Protection Method for MPEG-4 Videos

A method using a removable visible watermarking technique and limited video play counts is proposed for copyright protection of downloaded videos in this study, which uses an active agent to check available play counts and recover a watermarked video. By performing a variable length decoding on a given video, the quantized discrete cosine transform (DCT) coefficients of all the 8×8 luminance blocks of each frame of the video are obtained. Each luminance block is utilized to embed one pixel of a visible watermark image by utilizing the specific alternating current (AC) coefficient. After completing the embedding process, a variable length coding is performed to regenerate a watermarked video.

Once the downloaded video is played, the corresponding play counts will be decremented by one. If the play count of the video is not zero, the active agent will remove the visible watermark embedded in the video; otherwise, a visible watermark will appear immediately to state the prohibition of further display of the video.

1.3.2.2 A Method for Authentication of Surveillance Videos

A method using data hiding techniques for authenticating surveillance video sequences and contents is proposed in this study. First, variable length decoding is performed on a surveillance video, and motion-vector information of the P frames in each group of pictures (GOP) is analyzed to generate authentication signals. For each I frame, all the 8×8 luminance blocks in the frame are used to embed authentication signals; moreover, authentication signals also include temporal information of the video. After completing the embedding process, a variable length coding process is

performed to regenerate a protected video. In addition, a voting technique is utilized to extract authentication signals precisely.

1.3.2.3 A Method for Searching Motions in Surveillance Videos

A method using image watermarking techniques for searching motions in surveillance videos is proposed in this study. First, we apply a motion detection technique to judge whether an image captured from a video camera contains motions or not. If so, a human detection algorithm is performed on the image to obtain the type of motion. Then an MPEG-4 encoder is employed to compress the image, and embed in the mean time the type of motion into the quantized DCT coefficients of the I frame detected to contain motions. Finally, a variable length coding process is performed to generate a stego-video. By extracting the types of motion through an MPEG-4 decoding process, we can easily find out where motions exist and what types they are in the surveillance video.

1.3.2.4 A Method for Searching Targeted Persons in Recorded Videos

A method using data association techniques for searching targeted persons by hiding special information in recorded videos is proposed in this study. Moreover, we integrate a smart card technique into the MPEG-4 encoder for reading personal identification data, which are utilized as special information and hidden into the recorded video. First, each image captured from a surveillance camera is put into a real-time encoding process. And personal identification data are embedded into the quantized DCT coefficients of the I frame when someone triggers the smart card device. A variable length coding process is performed finally to generate a

stego-video. By extracting the personal identification data through an MPEG decoding process, we can clearly judge whether the targeted person in the surveillance video is suspicious or not.

1.4 Contributions

Several contributions are made in this study, as described in the following.

1. An active watermarking method is proposed for protecting the copyright of a downloaded MPEG-4 video by limiting the play counts of the video.
2. A video authentication system is proposed for verifying the fidelity and the integrity of recorded surveillance videos as well as for recognizing tampering types and attacked image areas.
3. A method is proposed for search and classification of motions in surveillance videos by image watermarking techniques.
4. A method is proposed for search of targeted persons in recorded videos by hiding and retrieving special information.

1.5 Thesis Organization

In the remainder of this thesis, a review of related works about active agent, visible watermarking, and video authentication techniques and the MPEG-4 standard is given in Chapter 2. In Chapter 3, the proposed method for actively protecting the copyright of MPEG-4 videos is described. In Chapter 4, the proposed video authentication system for surveillance videos is described. In Chapter 5, the proposed method for searching motions in surveillance videos is described. In Chapter 6, the proposed method for searching targeted persons in recorded videos is described. Finally, conclusions and some suggestions for future works are given in Chapter 7.