Chapter 6
Searches of Targeted Persons in Recorded Videos by Hiding of Special Information

6.1 Introduction

In the recent years, surveillance systems are widely integrated into some commercial security systems, such like Automatic Teller Machines (ATMs), entrance guard systems, etc. In these systems, special information must be given as input in order to obtain permission for legal actions. For example, when you want to draw money from an ATM, you must insert your ATM card and enter the corresponding password to activate your card. In this scenario, the special information mentioned above includes both your correct password and the data stored in your ATM card. In other words, this kind of information can also be treated as a kind of personal identification data.

In this chapter, we propose a method which hides personal identification data into surveillance videos via a *data association* technique in order to search targeted persons in the videos. Furthermore, this method can verify whether the hidden personal identification data match to the targeted person in the video or not.

The remainder of this chapter is organized as follows. In Section 6.1.1, some related problem definitions are given. In Section 6.1.2, the basic idea of the proposed scheme and the system configuration are presented. In Section 6.2, a review of smart card techniques is stated, and the propose method for real-time embedding of personal identification data into videos is described in Section 6.3. In Section 6.4, experimental results are shown to prove the feasibility of the proposed method. Finally, some discussions and a summary will be made in the last section of this chapter.

6.1.1 Problem Definition

In the proposed method, we utilize an MOICA (Ministry of The Interior Certificate Authority) IC card with a USB card reader to simulate a simple ATM or entrance guard system. The reason why we use the MOICA card will be explained in Section 6.2 in detail. Therefore, the first problem is how to communicate with the smart card and read personal identification data through the card reader. The second is how to embed personal identification data into the quantized DCT-domain of I frames of videos for a subsequent searching process.

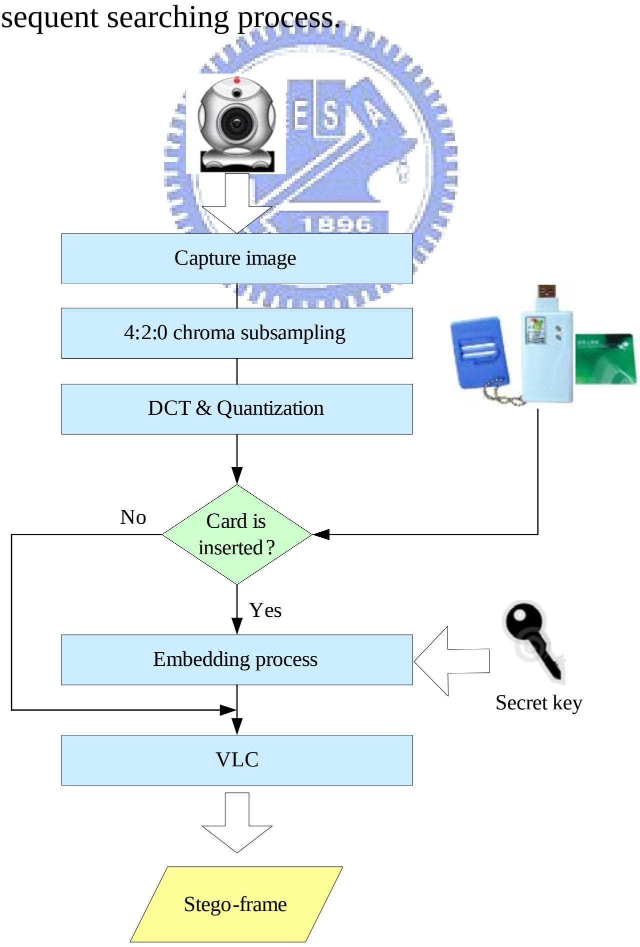


Figure 6.1 Illustration of the proposed system configuration.

6.1.2 Proposed Idea and System Configuration

Taking the ATM system for example, we can enter an account number into the proposed system for searching persons who have used an ATM card in front of a specific ATM. If the searched person in the surveillance video is not the owner of this ATM card, we can reasonably suspect that he/she committed a crime at that time. In addition, we can further give the search result as evidence to the police for arresting the suspected person.

In the proposed method, the system will read the card number of the MOICA when the IC card is inserted into the card reader. Simultaneously, the event occurring time will be combined with the card number as the personal identification data to be embedded into the I frames of the video by an image watermarking technique. An illustration of the system configuration is shown in Figure 6.1.

6.2 Review of Smart Card Techniques

In Section 6.2.1, a brief introduction to smart cards is presented, and the process for reading personal identification data from smart cards is described in Section 6.2.2.

6.2.1 A Brief Introduction to Smart Cards

As implied by the name, a smart card which belongs to the ICC (Integrated Circuit Card) includes an intelligent microchip embedded on a pocket-sized plastic card. The built-in microprocessor and memory of the smart card are used for security and performing complicated operations, such as financial transactions. In other words, they can be treated as a small operation system. In contrast to the traditional magnetic stripe technology, the smart card can store more information and process sensitive data on the card without network transmission. Besides, the smart card is recently applied to several applications, such like banking, person identification, permission of transportation, telecommunication, and healthcare transactions.

According to the transmission interface, smart cards can be roughly categorized into three types: contact card, contactless card, and combination card. A contact card, used in this study, means that it needs to contact an interface device when transferring data; on the contrary, a contactless card transfers data by infrared or electromagnetic waves without contacting any device. And a combination card is composed of two interfaces mentioned above.

In order to communicate with a contact smart card or develop a contact smart card application, a card reader is required. With a card reader, a host computer can communicate with the microprocessor through a transmission protocol defined by the ISO 7816 Smart Card Standard for data reading or writing. The detailed process for reading data from the smart card is stated in the next section.

6.2.2 Reading Personal Identification Data from Smart Cards

In order to read personal identification data from the smart card, the card reader has to be introduced first. A smart card reader, which conforms to the PC/SC (Personal computer/Smart card) standard, is adopted as the communication bridge between the PC and the smart card in the proposed application. PC/SC is a standard framework which is developed by many companies for smart card access on Windows platforms, and a main advantage of PC/SC is that the application does not have to be aware of the details about the smart card reader when communicating with the smart card. In addition, the application can work with any card reader conforming to the PC/SC standard.

Generally speaking, the personal identification data, like the card number, are usually store in an EF(elementary file) of the smart card. A hierarchical structure of the file system in the smart card is defined by the ISO 7816-4 standard. The standard defines three types of files, DF(dedicated file), MF(master file), and EF(elementary file). The DF, which is a kind of directory file, can possess EFs or other DFs. The MF, which is the root of the file system, is also regarded as a DF but unique. The EF is a file for data storage and cannot include other files. The structure of the file system defined in smart cards is illustrated in Figure 6.2.

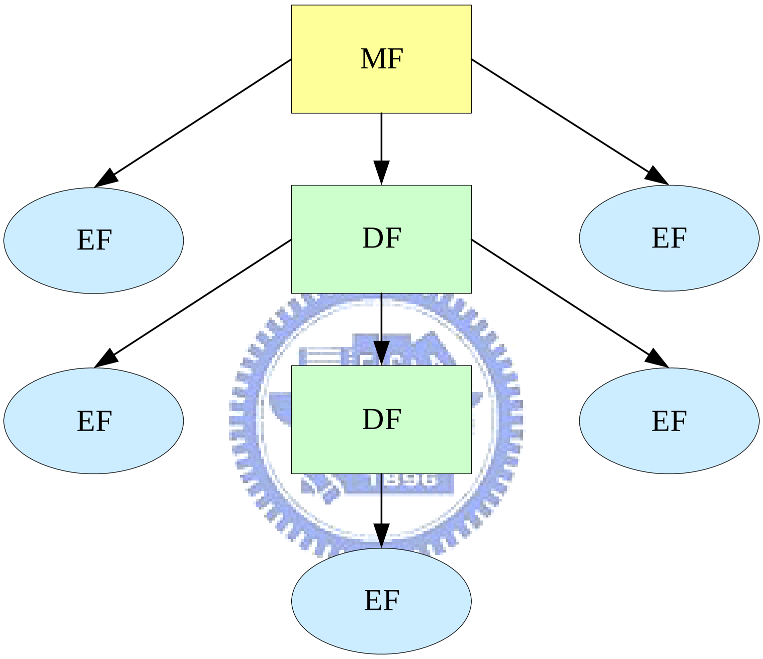


Figure 6.2 Illustration of hierarchical structure of the file system in the smart card.

When the application tries to communicate with the smart card for acquiring information, they exchange some data packets named APDU (Application Protocol Data Unit). There are two types of APDUs: command APDU and response APDU. As implied by the name, the former is sent by the application to the card, and it may represent various commands according to the instruction byte INS. For instance, before we want to access a file, we have to send the command APDU with INS equal to A4 representing the “SELECT FILE” command defined in the ISO 7816-4 standard. The latter is sent by the card to the application with data requested in the command

APDU. The structure of both kinds of APDU is illustrated in Figure 6.3 and a detailed explanation of the other fields is described in the ISO 7816 standard. However, the formats of command APDUs defined by card manufacturers are different from card to card and usually are not open sources for application developments. In other words, we cannot access information in the card unless we request the card manufacturer for the card specification. And that is the reason why we use the MOICA card in this study instead of the ATM card.

	Header				Body		
Command APDU	CLA	INS	P1	P2	[Lc field]	[Data field]	[Le field]

	Body	Trailer	
Response APDU	[Data field]	SW1	SW2

Figure 6.3 Structure of command and response APDU.

With the knowledge of smart cards presented in this section, we can acquire the card number from the MOICA card by sending the corresponding command APDU according to the open specification of the MOCIA card.

6.3 Real-time Embedding of Personal Identification Data into Videos

In this section, we propose a method for embedding personal identification data into the I frame of the video during the real-time encoding process. An illustration of the embedding process is shown in Figure 6.4. In Section 6.3.1, the principle of the proposed method is given, and the proposed process for embedding personal identification data is described in Section 6.3.2.

6.3.1 Principle of Proposed Method

Basically, the proposed embedding method in this chapter is similar to the one proposed in Chapter 5. The embedding process is triggered by a card insertion event, and a 16-digit card number of the MOICA card will be read out and embedded into the quantized DCT-domain of the frame which is treated as an I frame by an MPEG-4 encoder. Moreover, we also put a timestamp into the personal identification data to indicate the time of card insertion.

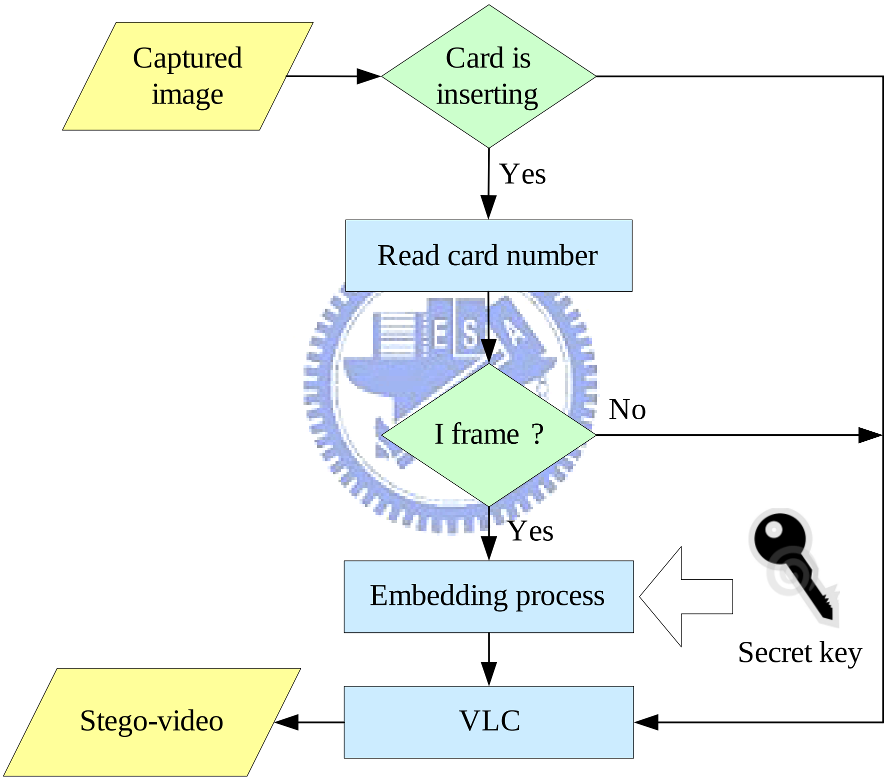


Figure 6.4 Illustration of the proposed embedding process of personal.

6.3.2 Proposed Embedding Process

In the proposed embedding process, we combine the card number with the time when the card is inserted to form a string *N* for representing the personal identification data. As mentioned in Chapter 3, we will randomly select one of the ten pairs of DCT coefficients defined according to the zig-zag scanning order for embedding one bit of the personal identification data by a secret key *K*. A flowchart of the embedding process is illustrated in Figure 6.5 and a corresponding detailed algorithm is described in the following.

***Algorithm* 6.1**: The process for embedding personal identification data.

Input: an I frame *F* in the quantized DCT-domain, the personal identification data *N*, and a secret key *K*.

Output: a stego I frame *F'*.

Steps:

1. Denote the binary form of *N* as $N_b = b_1b_2b_3\ldots b_L$, where *L* represents the length of N_b.
2. Combine the input secret key *K* and the position *P* of the corresponding 8×8 luminance block B_{ij} to form a seed for a random number generation.
3. Select one pair of DCT coefficients (C_1, C_2) from the ten pre-defined pairs according to the result of random number generation.
4. Embed each bit b_k of N_b by changing the relation between C_1 and C_2 according to the following rule:

   (1) When $b_k = 0$ and $k \neq L$:

$$\begin{cases} if\ C_1 < C_2, then\ swap\ C_1\ and\ C_2 \\ if\ C_1 = C_2, then\ set\ C_1 = C_2 + T_1 \end{cases} \tag{6.1}$$

   where T_1 is a pre-defined threshold.

   (2) When $b_k = 1$ and $k \neq L$:

$$\begin{cases} if\ C_1 > C_2, then\ swap\ C_1\ and\ C_2 \\ if\ C_1 = C_2, then\ set\ C_2 = C_1 + T_1 \end{cases} \tag{6.2}$$

   where T_1 is a pre-defined threshold.

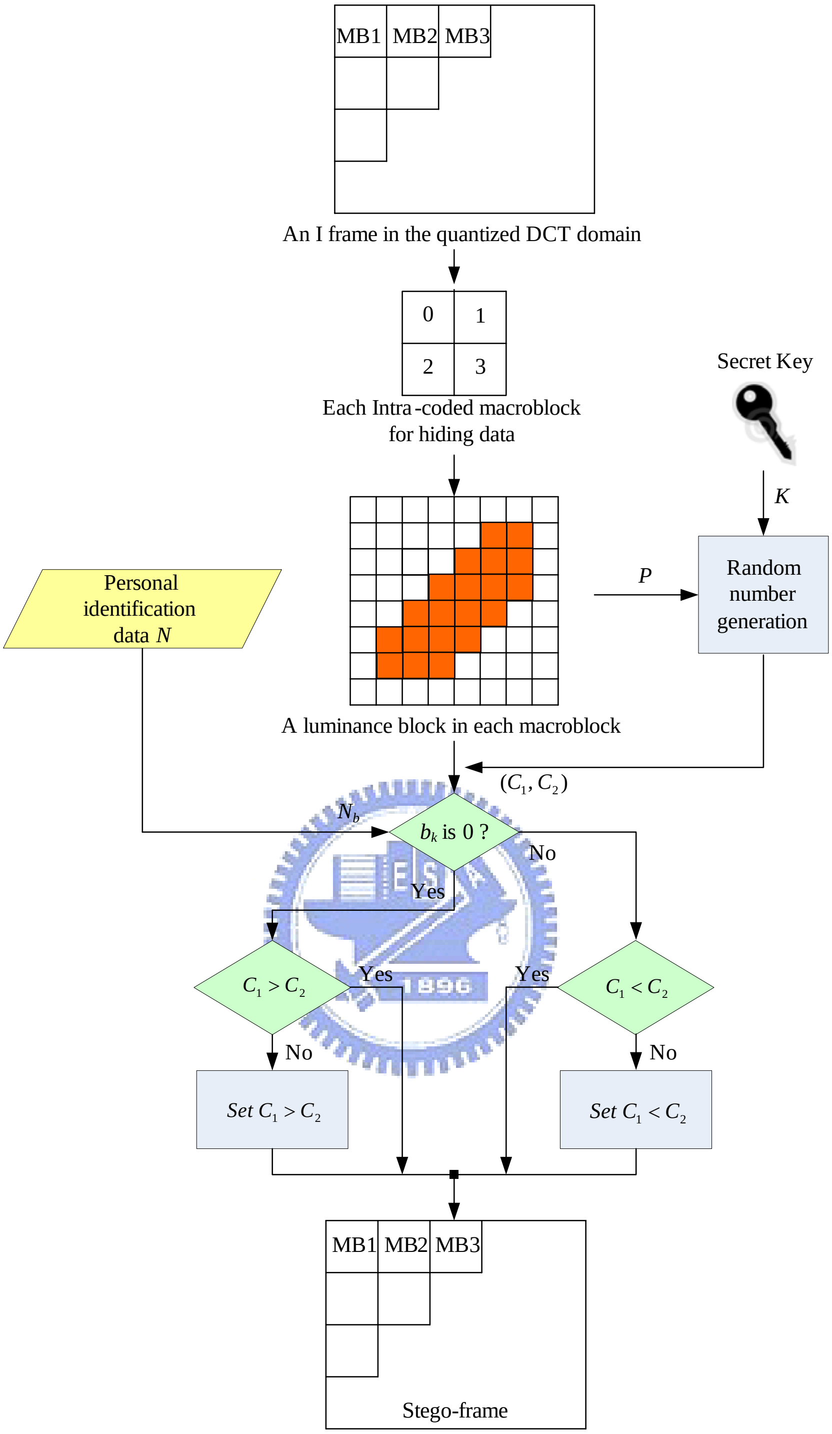


Figure 6.5 Flowchart of the proposed embedding process of personal identification data.

In order to search the targeted person in the resulting video, the extraction process, which is similar to the one mentioned in Chapter 5, is needed via partially decoding of the resulting video. The extracted personal identification data, including the MOICA card number and the occurring time, are utilized to verify whether the targeted person in the video is suspicious or not.

6.4 Experimental Results

In our experiment, each image captured by a video camera is encoded in real time by an MPEG-4 encoder to form an MPEG-4 compressed video with frame size 320×240. We simulate an ATM system which is equipped with a surveillance camera and a smart card reader as shown in Figure 6.6. Six frames of a resulting stego-video are shown in Figure 6.7. The proposed user interface used for searching targeted persons in the recorded video is shown in Figure 6.8 (a). We can enter a card number into the proposed system and check whether the person in the video is the corresponding card owner or not. The search result is shown in Figure 6.8 (b).

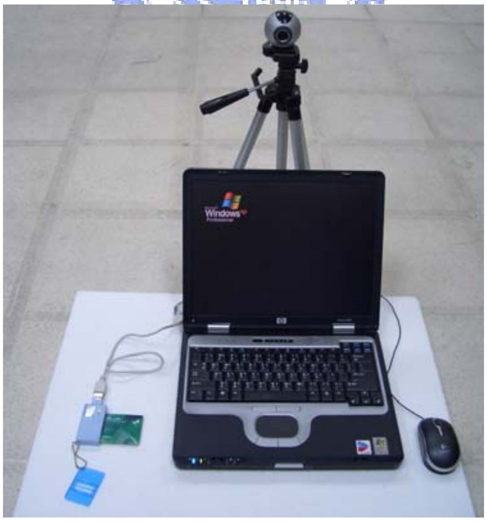
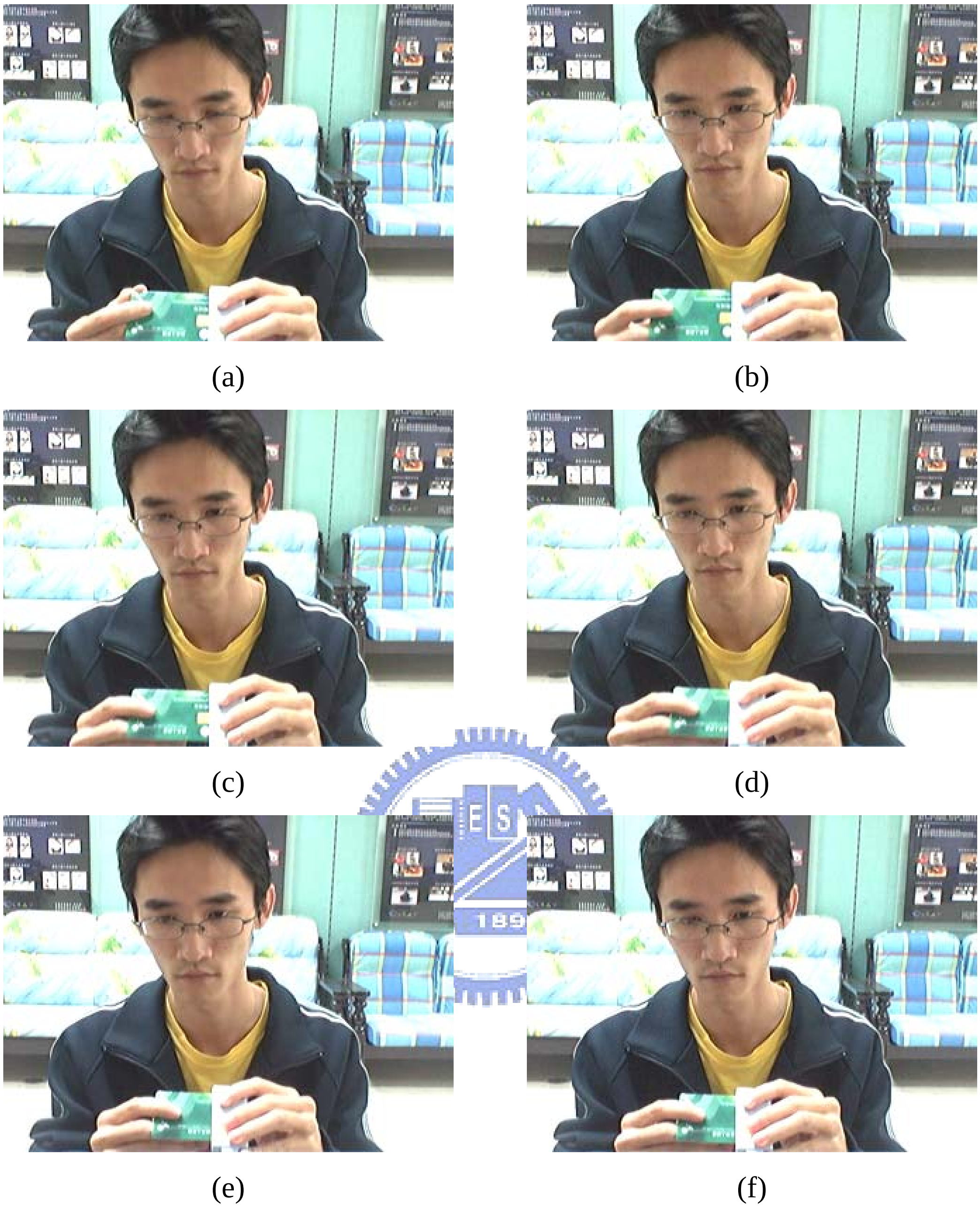


Figure 6.6 Equipments for simulating an ATM system with security surveillance capability.

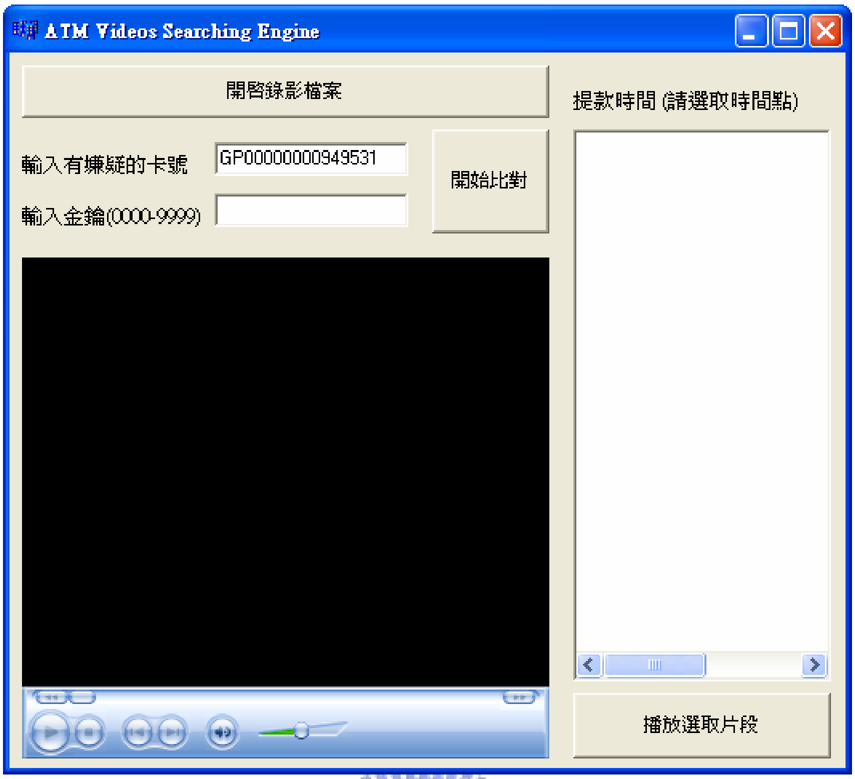


(a) (b)

(c) (d)

(e) (f)

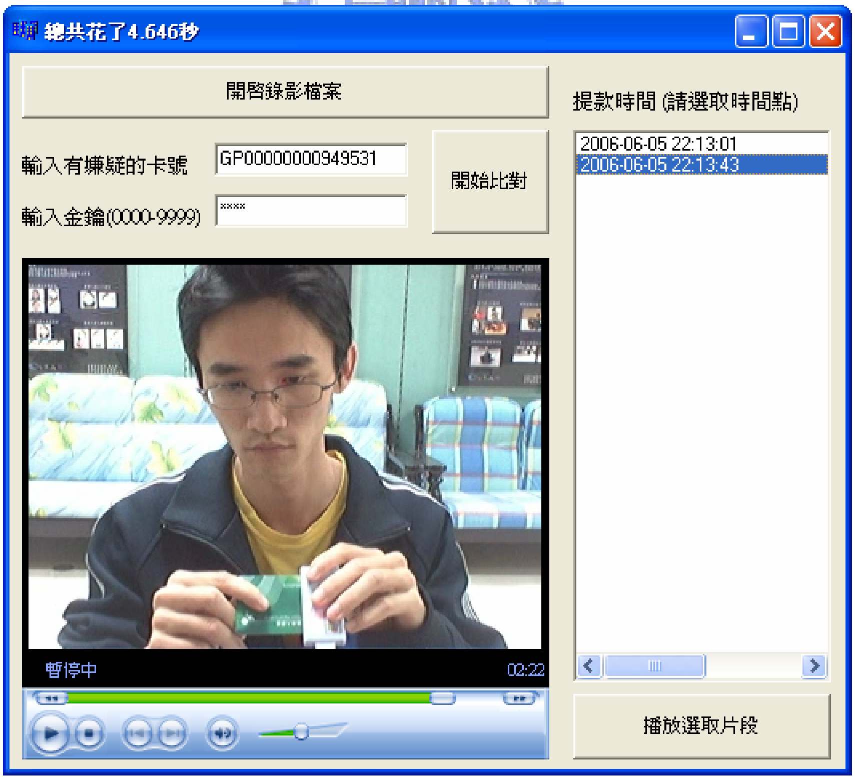
Figure 6.7 Six frames of the resulting stego-video. (a) The first frame (I frame). (b) The second frame (B frame). (c) The third frame (P frame). (d) The 4th frame (B frame). (e) The 5th frame (P frame). (f) The 6th frame (B frame).



輸入有嫌疑的卡號 GP00000000949531

輸入金鑰(0000-9999)

(a)



輸入有嫌疑的卡號 GP00000000949531

輸入金鑰(0000-9999) ****

2006-06-05 22:13:01
2006-06-05 22:13:43

(b)

Figure 6.8 The proposed (a) user interface and (b) searching result.

6.5 Discussions and Summary

In this chapter, a method for searching targeted persons in recorded videos by hiding personal identification data with an image watermarking technique has been proposed. The card number was read out from the MOICA card as personal identification data by utilizing the smart card technique and embedded into the quantized DCT coefficients in the real-time MPEG-4 encoding process. After the extraction process of the resulting video, we can enter the desired card number for searching the corresponding frames with insertion events of this card through a friendly user interface. Then we can easily check whether the card number matches the targeted person in each search result or not. This method can be applied to many systems which need input of identification information for further operations, like ATM or entrance guard systems, to verify targeted persons and find out suspects in the surveillance video.