國立交通大學

資訊科學系

碩士論文

主動式資訊隱藏與應用之研究

A Study on Active Information Hiding and Applications

研究生：羅楠焜

指導教授：蔡文祥 教授

中華民國九十三年六月

主動式資訊隱藏與應用之研究
A Study on Active Information Hiding and Applications

研究生：羅楠焜　　Student：Nan-Kun Lo

指導教授：蔡文祥　　Advisor：Wen-Hsiang Tsai

國立交通大學
資訊科學研究所
碩士論文

A Thesis
Submitted to Institute of Computer and Information Science
College of Electrical Engineering and Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master
in

Computer and Information Science

June 2004

Hsinchu, Taiwan, Republic of China

中華民國九十三年六月

主動式資訊隱藏與應用之研究

研究生：羅楠焜　　　　指導教授：蔡文祥 博士

國立交通大學資訊科學研究所

摘要

隨著電腦科技的進步與網際網路的蓬勃發展，越來越多的資料利用網路傳輸，本論文利用資訊隱藏和數位浮水印技術在個人電腦與手機的操作平台上作秘密通訊、驗證與版權保護之研究與應用。在秘密通訊方面，我們將秘密訊息分別隱藏在MPEG視訊檔案與遮蔽影像中，再透過網頁與手機上之無線網路系統安全地將其傳送。在版權保護方面，我們在MPEG視訊檔案中隱藏一種不同於以往的版權資訊，當MPEG視訊檔案在網頁上被下載時，會主動地將可視的版權資訊表現出來。對於MPEG視訊檔案與利用手機所拍攝的影像內容是否遭到竄改，我們也提出了兩個方法可以在網頁上讓MPEG視訊檔案主動地自我驗證以及在手機上對影像做驗證。相關的實驗結果證明了所提方法的可行性。

A Study on Active Information Hiding and Applications

Student: Nan-Kun Lo Advisor: Dr. Wen-Hsiang Tsai

Institute of Computer and Information Science
National Chiao Tung University

Abstract

With the advance of computer technologies and the popularity of the Internet, more and more data can be transmitted speedily and conveniently on public networks. In this study, several methods for three data hiding applications, namely, covert communication, authentication, and copyright protection, on two application platforms, namely, personal computers and cellular phones, are proposed. In order to transmit large-volume secret messages on the web page more securely, an active covert communication method for MPEG videos is proposed. Because contents of web pages are getting richer, authors need to protect their ownership of MPEG videos on web pages. Two active watermarking methods for copyright protection of this purpose are proposed. Due to the prevalence of hacker activities, receivers cannot be sure that MPEG videos received from the public network are genuine, so an active authentication method is also proposed to verify the integrity and the fidelity of them. Furthermore, with the prevalence of using cellular phones, mobile computing technologies of cellular phones are getting more powerful. They can be used to take images and transmit them through wireless networks provided by telecommunication companies. In order to transmit secret messages via cellular phones, two covert communication methods using cover images are proposed. Moreover, for the purpose of using cellular phones to transmit captured images and ensuring the validity of them, an authentication method based on data hiding techniques is also proposed. Good experimental results show the feasibility of the proposed methods.

ACKNOWLEDGEMENTS

The author is in hearty appreciation of the continuous guidance, discussions, support, and encouragement received from his advisor, Dr. Wen-Hsiang Tsai, not only in the development of this thesis, but also in every aspect of his personal growth.

Thanks are due to Mr. Chih-Hsuan Tzeng, Mr. Chang-Chou Lin, Mr. Chih-Jen Wu, Mr. Tsung-Yuan Liu, Mr. Cheng-Jyun Lai, Mr. Yen-Chung Chiu, Miss Yen-Lin Chen, Mr. Wei-Liang Lin, Mr. Yi-Chieh Chen and Mr. Kuei-Li Huang for their valuable discussions, suggestions, and encouragement. Appreciation is also given to the colleagues of the Computer Vision Laboratory in the Department of Computer and Information Science at National Chiao Tung University for their suggestions and help during his thesis study.

Finally, the author also extends his profound thanks to his family for their lasting love, care, and encouragement. He dedicates this dissertation to his parents.

CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

1.1 Motivation

With the advance of computer technologies and the popularity of the Internet, more and more data can be transmitted speedily and conveniently on the public network. Hence, videos become suitable *cover media* for carrying large-volume secret messages from one site to another. Data hiding techniques can be used to hide secret messages in videos as *stego-videos* for covert communication on the public network more securely.

Because of the development of computer networks, contents of web pages are getting richer. There are not only still images and texts on web pages but also a lot of videos for presenting fantastic effects. Nowadays, authors need to protect their ownership of videos on web pages because some illicit users may download these videos for misrepresentation. In order to deal with this problem, it is desired to design a digital watermarking technique to generate *watermarked videos* for copyright protection.On the other hand, due to the prevalence of hacker activities, receivers cannot be sure that videos received from the public network are genuine. It is desired to design a data hiding technique to hide authentication signals in videos and generate *protected videos*. In this way, after receivers obtain suspicious videos from others, authentication signals can be extracted and utilized to verify the fidelity and the integrity of the videos.

Furthermore, with the prevalence of using cellular phones, mobile computing technologies of cellular phones are getting more powerful. They can be used to take pictures and transmit data through wireless networks provided by telecommunication companies. When transmitting secret messages via cellular phones, it is desired to design a data hiding technique to hide secret messages in cover images. Moreover, using cellular phones to transmit *captured images* is very often and simple. In order to ensure the validity of received images, it is also desired to design a data hiding technique to hide authentication signals in them. In this way, after receivers get suspicious images from others, authentication signals can be extracted and used to verify the fidelity and the integrity of the images. The computing power of cellular phones and the data hiding capacity of captured images are limited in general. The designed data hiding technique must take these problems into consideration.

In this study, it is desired to develop appropriate techniques for the above-mentioned goals.

1.2 Review of Related Studies

1.2.1 Active Information Hiding Techniques

Active information hiding techniques has been proposed by Yu et al. in 2001 [15]. In fact, active information hiding is a subset of the research area of information hiding which so far focuses mostly on *passive* information hiding. Active information hiding means essentially to hide imperceptibly an *active agent*, such as an applet or an executable file, in a cover media which can be any type of multimedia, such as audio, image, or video, unlike embedding watermarks or secret messages by passive information hiding in which no active agent is involved.

Because active agents are executable files, there should yield no error bit in the extraction process or it will cause the extracted active agent to be unexecutable. Since active agents might also be applets, they can perform tasks, such as sending feedback information to the server site, showing the ownership of cover media, scrambling the cover media when authenticity checks fail, etc. With the use of active agents, more applications can be implemented by information hiding techniques.

Since the data hiding capacity of cover media is fixed and the sizes of executable files are usually large, it will be difficult to hide large-volume secret messages if both of the active and the passive data stream have to be hidden in the cover media. Another method should be found out to solve this problem.

An application of active watermarking methods was proposed by Chang and Tsai [17] for copyright protection of images. When illicit users want to download images without any authorization, the active agent will be extracted and a visible watermark on the image to claim the ownership will be produced.

1.2.2 Passive Information Hiding Techniques

1.2.2.1 Information Hiding Techniques for Images

In recent years, many methods for hiding data in cover images have been proposed. All of them can be categorized into two kinds: frequency-domain methods and spatial-domain ones. In spatial-domain methods, the simplest way to hide data in cover images is to replace the least significant bit (LSB) of every image pixel directly. The LSB information hiding technique was proposed by Adelson [12] in 1990. This method is fast and easy, and a lot of data can be hidden imperceptibly in cover images.

In order to increase the data hiding capacity, more than one least significant bit may be modified for hiding data, but the image quality will be degraded. Recently, many methods based on the LSB technique [11, 13, 14] utilizing more than one least significant bit to embed data have been proposed.

1.2.2.2 Information Hiding Techniques for MPEG Videos

Nowadays, many methods of video data hiding have been proposed for hiding data in cover videos. In this way, secret messages can be carried covertly from one site to another. Chae and Manjunath [1] proposed one method to hide data in the DCT coefficients of a cover video, in which the hiding method is adaptive to the local texture content of the cover video frame blocks. The reason why the data are hidden in texture regions is that the human visual system is more sensitive to the change in low frequency regions than in high frequency ones. There are also many approaches to hiding data in a video.

Video authentication techniques are proposed to ensure that received videos have not been tampered with. Recently, many methods have been proposed for authenticating videos. They can be categorized into three types: digital signature techniques [5], digital watermarking techniques [3, 4], and random signal techniques [10]. Methods of using digital signatures for video authentication are to use the public/private key infrastructure to ensure trustworthiness and an additional signature must be saved and transmitted separately from protected videos. Yin and Yu [4] has proposed a semi-fragile watermarking technique to authenticate videos. Fragile watermarks are often utilized for multimedia authentication because any modification can destroy contents of hidden watermarks. Therefore, they can provide a very high detection probability. Chen and Tsai [10] have proposed an authentication method of hiding random signals in videos. In this method, all authentication signals, called random signals, generated by a key are hidden in videos and there is no signature has to be saved.

A number of visible watermarking techniques [6-9] of videos for copyright protection have been proposed in recent years. Meng et al. [8] has proposed one method to hide visible watermarks in MPEG videos. In this method, the visibility of the watermark is adjusted dynamically, depending on the local content features derived in the DCT domain. Mohanty et al. [6] has proposed a DCT-domain visible watermarking technique for images. In this method, hiding visible watermarks in DCT coefficients is based on a mathematical model developed by utilizing the texture sensitivity of the human visual system. The modification of the DC value will cause the image block look different.

1.2.3 Brief Descriptions of MPEG Standard

The MPEG video consists of many groups of pictures (GOP) and a GOP is comprised of various types of frames, including intra-coded frames (I), predictive-coded frames (P), and bi-directionally predictive-coded frames (B). Each frame can be divided into several slices and every slice comprises a lot of macroblocks. An illustration of the MPEG structure is shown in Figure 1.1.

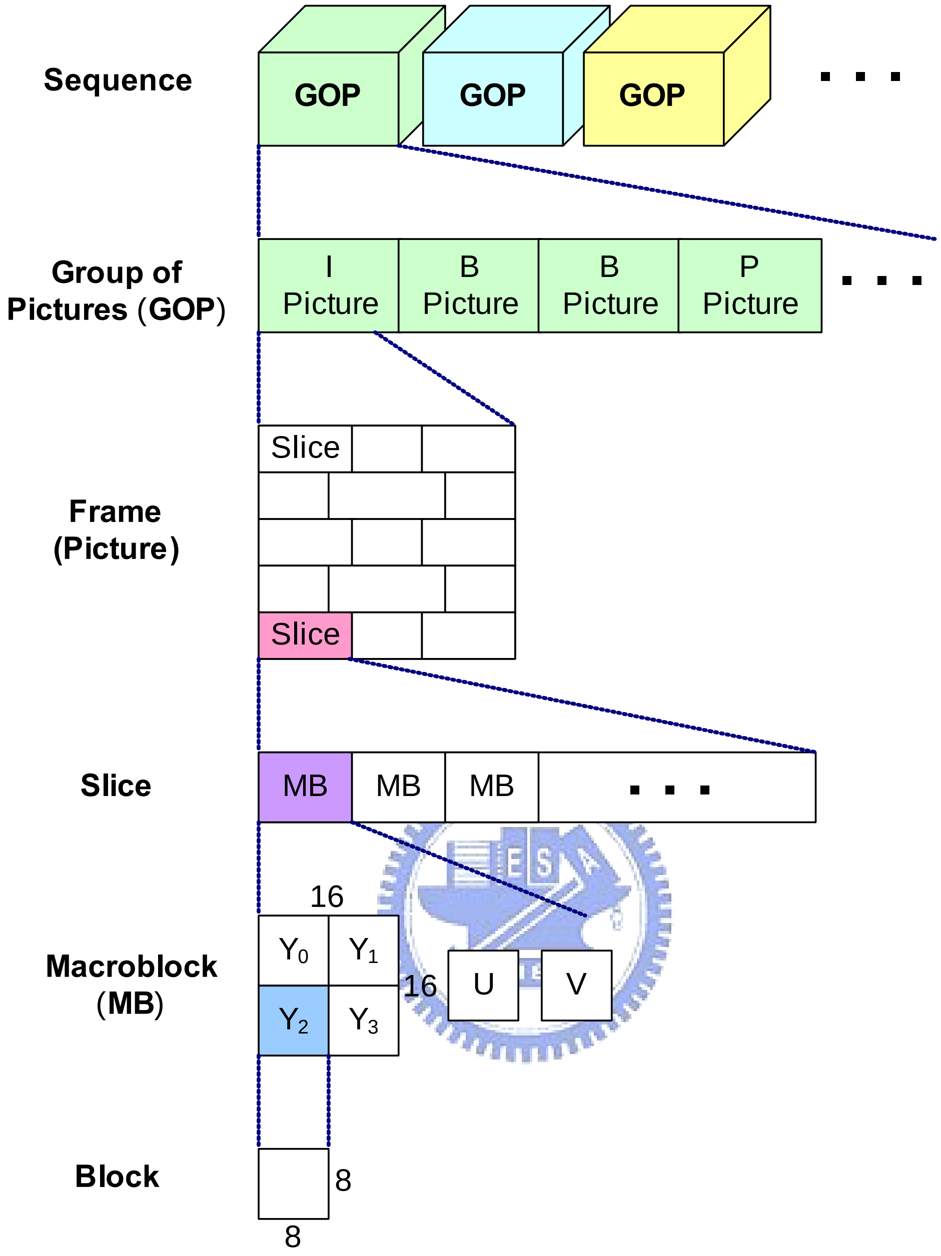


Figure 1. 1 An illustration of the MPEG structure.

The MPEG video compression method not only uses the discrete cosine transform (DCT) to reduce the spatial redundancy but also the motion-compensation algorithm to reduce the temporal redundancy among frames in a GOP. In the MPEG standard, a macroblock (MB) is adopted as a motion-compensation unit and each type of frames has different types of macroblocks. An illustration of the relationships between frames and macroblocks is shown in Figure 1.2.

	Intra-coded MB	Forward-coded MB	Backward-coded MB	Bidirectionally-interpolated MB
I	●			
P	●	●		
B	●	●	●	●

Figure 1. 2 An illustration of the relationships between frames and macroblocks.

After reducing the spatial and the temporal redundancy, all frames are processed with variable-length coding (VLC) to generate the MPEG bitstream, called the MPEG video. With the use of variable-length decoding (VLD), the frequency domain data of each frame can be acquired.

1.3 Overview of Proposed Methods

1.3.1 Definitions of Terms

The definitions of related terms used in this study are described in this section in the following.

1. *Cover media*: Cover media, such as an image, a text-type document, an HTML document, or a video, is a file in which a message may be embedded.
2. *Stego-video*: A stego-video is a video in which a message has been embedded.
3. *Public video*: A public video is a video which is published by an author and can be downloaded by any user arbitrarily.
4. *Protected video*: A protected video is a video in which authentication signals

have been embedded.

5. *Watermarked video*: A watermarked video is a video in which visible or invisible watermarks have been embedded.
6. *Captured image*: A captured image is an image which is taken by a camera built in a cellular phone.
7. *Protected image*: A protected image is an image in which authentication signals have been embedded.

1.3.2 Brief Descriptions of Proposed Methods

1.3.2.1 Proposed Active Covert Communication Method for MPEG Videos

A steganographic method is proposed in this study for covert communication, which exploits the use of MPEG videos exhibited on public web pages to hide secret messages and transmits them to the receiver site via video downloading. First, MPEG videos are processed with variable-length decoding and the frequency-domain data of each frame are obtained. Then, secret messages can be embedded in MPEG videos with the use of every luminance block and motion vectors of macroblocks in each frame. After the embedding process is complete, these frames will be processed with variable length coding to generate stego-videos.

When a user wants to acquire the message from others, without installing a data extraction program, the user can browse a public web page and download stego-videos with secret messages.

1.3.2.2 Proposed Active Authentication Method for

MPEG Videos

A data hiding method for authentication is proposed in this study, which uses active agents to verify suspicious MPEG videos on web pages. Original videos are first processed with variable length decoding and the frequency-domain data of each frame can be obtained. Then, the index of the GOP of the video and the number of inter-coded frames in the GOP are embedded in the frames. After the embedding process is completed, these frames are processed with variable length coding to regenerate protected videos.

When a user wants to get the message from a protected MPEG video on a web page, without installing a video authentication program, the user may require the proposed system to verify the fidelity and the integrity of the suspicious videos and generate an authentication report.

1.3.2.3 Proposed Active Copyright Protection Method for MPEG videos

Two methods using digital watermarking techniques are proposed for copyright protection in this study, which use active agents to transform embedded watermarks in MPEG videos. Original videos are first processed with variable length decoding and the frequency domain data of each frame are obtained. The input watermark is embedded in MPEG videos with the use of the DC value of each luminance block of the macroblocks in each frame. After the embedding process is completed, these frames are processed with variable length coding to regenerate a watermarked video.

When an illicit user wants to download the watermarked video which is put on a public web page, the proposed system will transform the invisible watermark to a visible one and claim immediately the ownership of the MPEG video. Another reverse application situation is that multimedia providers may put a video with a removable visible watermark on a public web page for people to preview. An authorized user with an authentic key can access the proposed system and clear the visible watermark on the video displayed on the public web page. On the contrary, an unauthorized user can just see the watermarked video.

1.3.2.4 Proposed Active and Passive Covert Communication Method for Cover Images on Cellular Phones

Two steganographic methods are proposed in this study for covert communication, which utilize cover images to embed secret messages and transmit them to the receiver site via the wireless network provided by telecommunication companies.

The first proposed method is one useful for active covert communication, in which secret messages are embedded in cover images using a 2-LSB data hiding technique and cover images are encapsulated with a JAVA program before being put on public web pages. Then, users can browse the public web page and download cover images with secret messages. In the other proposed method which is useful for passive covert communication, large-volume secret messages are first divided into several segments according to the data hiding capacity of each cover image and embedded in them using a 2-LSB data hiding technique. After the embedding process is completed, users just have to key in the receiver’s cellular phone number to the proposed system and the cover images will be transmitted to the receiver site via the wireless network. Both of these two methods have the capability of verifying the fidelity of the secret messages.

1.3.2.5 Proposed Authentication Method for Captured Images on Cellular Phones

A data hiding method for authentication is proposed in this study, which can generate authentication signals to produce protected images. First, a captured image is divided into several 4×4 blocks and an input user key together with certain related information of the current block are used to generate a random integer as an authentication signal. With the use of a 2-LSB data hiding technique, an integer with the length of 32 bits can be embedded completely in a 4×4 block. After the embedding process is completed, the resulting protected images can be transmitted to a receiver site and the receiver can utilize the proposed system to verify the fidelity and the integrity of the received images.

1.4 Contributions

Several contributions are made in this study, as described as follows.

1. A steganographic method with a secret authentication capability is proposed to hide large-volume secret messages in MPEG videos and transmit the secret messages via public web pages.
2. An authentication method is proposed to verify the fidelity of on-line MPEG videos actively without the need of installing authentication programs.
3. Two methods utilizing digital watermarking techniques are proposed to protect the copyright and the ownership of public MPEG videos.

4. Two covert communication methods with a secret authentication capability implemented on the platforms of cellular phones are proposed to hide secret messages in captured images and transmit secret messages via wireless networks provided by telecommunication companies.
5. An authentication method implemented on the platforms of cellular phones is proposed to verify the fidelity of captured images.

1.5 Thesis Organization

In the remainder of this thesis, an analysis of possible designs of active agents for active information hiding is described in Chapter 2. In Chapter 3, the proposed method for active covert communication for MPEG videos on web pages is described. In Chapter 4, the proposed method for active authentication for MPEG videos on web pages is described. In Chapter 5, the proposed methods for active copyright protection are described. In Chapter 6, the proposed methods both for active and for passive covert communications are described. In Chapter 7, the proposed method for authentication of captured images is described. Finally, conclusions and some suggestions for future works appear in Chapter 8.

Chapter 2

Design of Active Agents

2.1 Introduction

To design an effective active agent involves several factors like the access method, the cover media type, the extraction program type, and the platform type. The access method means how to access active agents from public networks. The cover media type means the kind of media used to hide secret data. The extraction program type means the language adopted in writing the program used to extract active agents. The platform type means where to execute active agents. These four factors about active information hiding are elaborated in Figure 2.1.

Access	Information Hiding	Extraction Program	Platform
From web pages	Video	ActiveX program	PC
From downloaded files on FTP sites	Image	JAVA program	Cellular phone
From attached files in E-mails	Audio	Executable program	Mobile device
	Text		

Figure 2. 1 Factors involved in active information hiding.

In Section 2.1, a detailed definition of the active agent and some application environments will be introduced. In Section 2.2, three different ways about how to access and trigger the active agent will be presented. In Section 2.3, various methods of hiding active agents in different platforms will be proposed. In Section 2.4, a summary and some discussions will be given.

2.1.1 Definition of Active Agent

Generally speaking, an active agent is an *active* data stream in the sense that it is executable to perform specific tasks actively by itself, such as an executable program or an applet. The original meaning of the active agent is its role to make the cover media look *alive*. Each action done by the active agent will let users feel that the cover media did the work by itself. Hidden active agents inject controllability and personality into the media so that the media can control the use of itself to protect itself from misuse or to provide a certain function to proper users of it.

Yu, et al. [15] designed one function, such as copyright protection of the host media, for the active agent. Another meaning of the active agent proposed in this study is to accomplish a certain function without installing an information extraction program on the local computer in advance. Here is an example. When employees working outside want to receive secret messages from superiors, they can use computers in a Cybercafé, for example, to access the Internet and browse a public web page. And on the web page, they can see cover movies and extract secret messages hidden behind the movies without installing a program in advance.

In this study, different kinds of platforms, including cellular phones supporting JAVA programming languages, are utilized to create various types of applications using active agents. They will be introduced in this chapter.

2.1.2 Application Environments

With the advance of computer and information technologies, more and more electronic devices, such as personal digital assistants (PDA), cellular phones, and notebooks (NB), have the mobile computing ability. A lot of complicated computations can be executed on them and wireless connections, such as Wireless Local Area Network (WLAN), General Packet Radio Service (GPRS), Short Messaging System (SMS), Bluetooth, or Infrared Rays technologies, can be used to transmit data to others.

Nowadays, both personal digital assistants and cellular phones are getting more powerful and there is almost no difference between them. The functions which personal digital assistants can do are also being implemented on cellular phones, and vice versa. A very important property which could not be implemented on these devices in the past is that programs written in JAVA or C^{++} programming languages can be executed now.

In the experimental environment of mobile devices in this study, NOKIA 6600 cellular phones built with the Symbian operating system supporting JAVA programming languages is adopted because this cellular phone supports Mobile Media API (MMAPI) which can be utilized to use the camera built in the cellular phone to take pictures as well as Wireless Messaging API (WMA) which can be utilized to send short messages through a telecommunications company.

The proposed system which is designed by JAVA programming languages can also be executed on personal digital assistants. The reason why we choose JAVA programming languages to be our programming tool is that it can be implemented in various kinds of operating systems as long as these operating systems support these.

2.2 Methods for Active Agent Access

We all know that a program cannot be executed by itself. It needs users to trigger directly or invoke indirectly. Since the active agent is a kind of executable programs embedded in the cover media, it still needs another program, called an *extraction program*, to trigger. In this study, three different access ways, namely, from web pages, from FTP sites, and from E-mails, are proposed to access the active agent.

2.2.1 From Web Pages

The first way proposed in this study to access the active agent is from web pages. With the use of ActiveX programs, called extraction programs, active agents can be extracted and executed. After users browse the web page, an ActiveX program can be downloaded into the local computer automatically. When users click the triggering button on the web page, the ActiveX program will extract an active agent hidden in the cover media.

2.2.2 From FTP Sites

The second way to access the active agent proposed in this study is from FTP sites. An executable file, called an extraction program, is used to extract an active agent hidden in the cover media. The cover media will be packaged in an extraction program and transmitted to the receiver site via FTP programs. After receivers acquire this extraction program from a downloaded file and click a triggering button on it, it will extract and execute an active agent.

2.2.3 From E-Mails

The third way proposed in this study to access the active agent is from E-Mails.

An executable file, called an extraction program, is used to extract an active agent hidden in the cover media. The cover media is also included in an extraction program and transmitted to the receiver site via e-mail programs. After receivers acquire this extraction program from an attached file in an electronic mail and click a triggering button on it, it will extract and execute an active agent.

2.3 Methods for Active Agent Hiding

Because the size of the active agent is often very large and the data hiding capacity of the cover media is usually limited, the proposed methods should take this problem into consideration. There are four ways for hiding active agents.

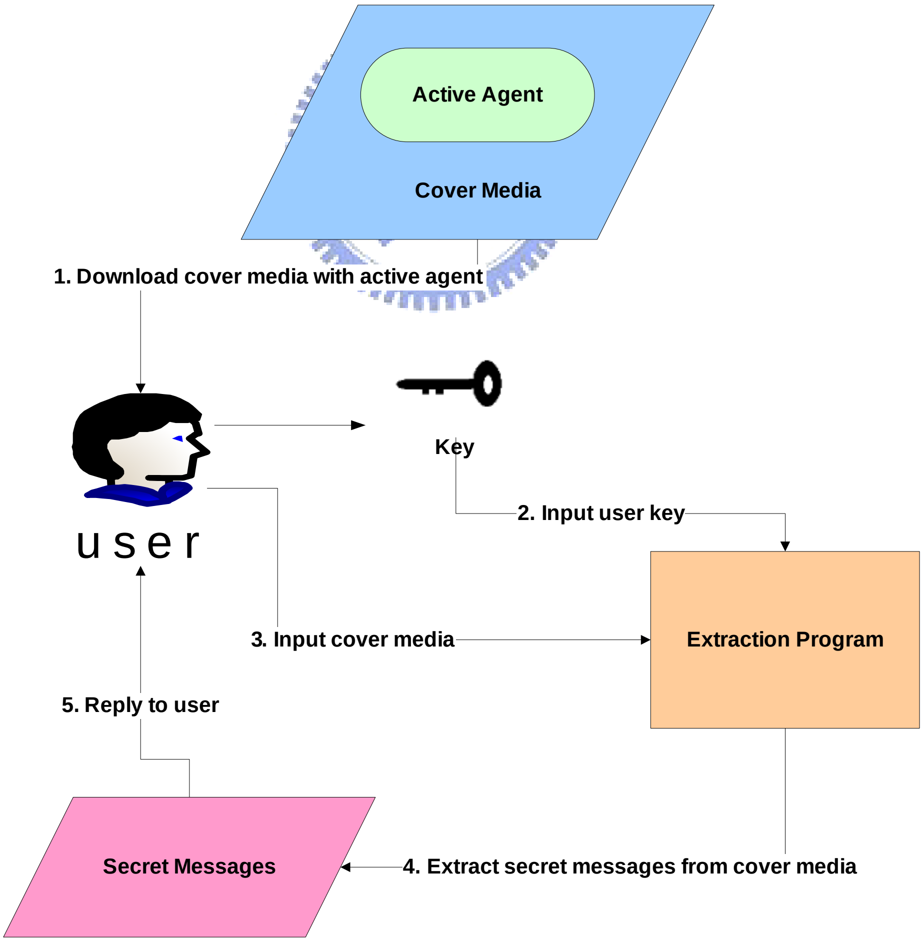


Figure 2. 2 An illustration of hiding active agents in cover media.

2.3.1 Hiding Agents in Cover Media

The original way proposed by Yu, et al. [15] to hide the active agent is to embed it in the cover media. It is also the most intuitive method because the active agent can be totally hidden in the cover media without involving other media. However, the use of this method will cost a lot of the data hiding capacity. An illustration of the situation about how to hide the active agent in the cover media is shown in Figure 2.2. In this method, an additive extraction program is necessary for extracting and executing active agents.

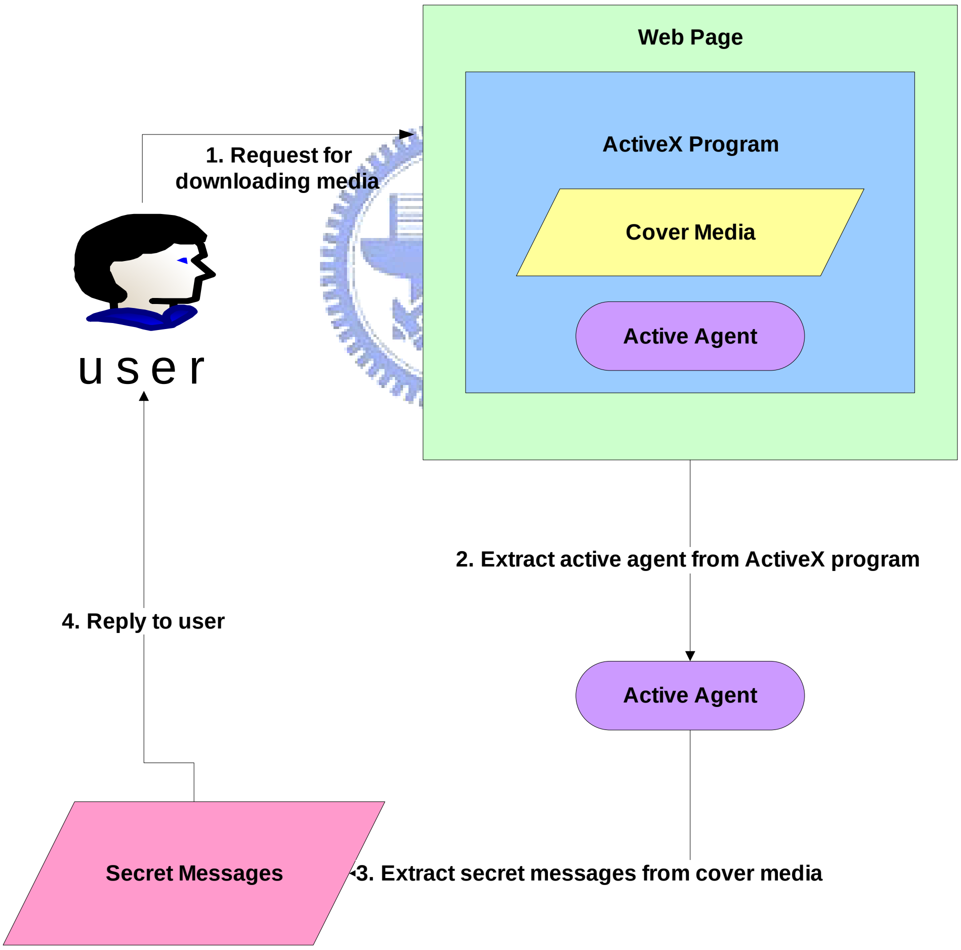

Web Page
ActiveX Program
Cover Media
Active Agent
1. Request for downloading media
user
2. Extract active agent from ActiveX program
Active Agent
4. Reply to user
Secret Messages
3. Extract secret messages from cover media

Figure 2. 3 An illustration of hiding active agents in ActiveX programs.

2.3.2 Hiding Agents in ActiveX Programs

Another way proposed by Chang and Tsai [17] to hide the active agent is to embed it in an ActiveX program. In this method, the ActiveX program on a web page is utilized to hide the active agent. The active agent can be downloaded to the local computer when a user browses the web page. An illustration of the process about embedding and extracting the active agent by this method is shown in Figure 2.3.

2.3.3 Proposed Method for Hiding Agents in ActiveX Programs and Cover Media

For the sake of the convenience of program design and solving the problem of the limited data hiding capacity of the cover media, a method to hide active agents by utilizing ActiveX programs and cover media on web pages is proposed in this study. The active agent is separated into two parts in this method. One is the *main agent* which includes a core part of the active agent and a multi-function program, and the other part is the *goal agent* which gives commands to the main agent.

In the proposed method, the main agent is hidden behind the ActiveX program and the goal agent embedded in the cover media. Because the size of the goal agent is much smaller than that of the main agent, an amount of the data hiding capacity of the cover media can be saved. Since all program functions are designed in the main agent, this main agent can be reused to do different works by different goal agents without redesigning a new active agent. The proposed method is shown in Figure 2.4.

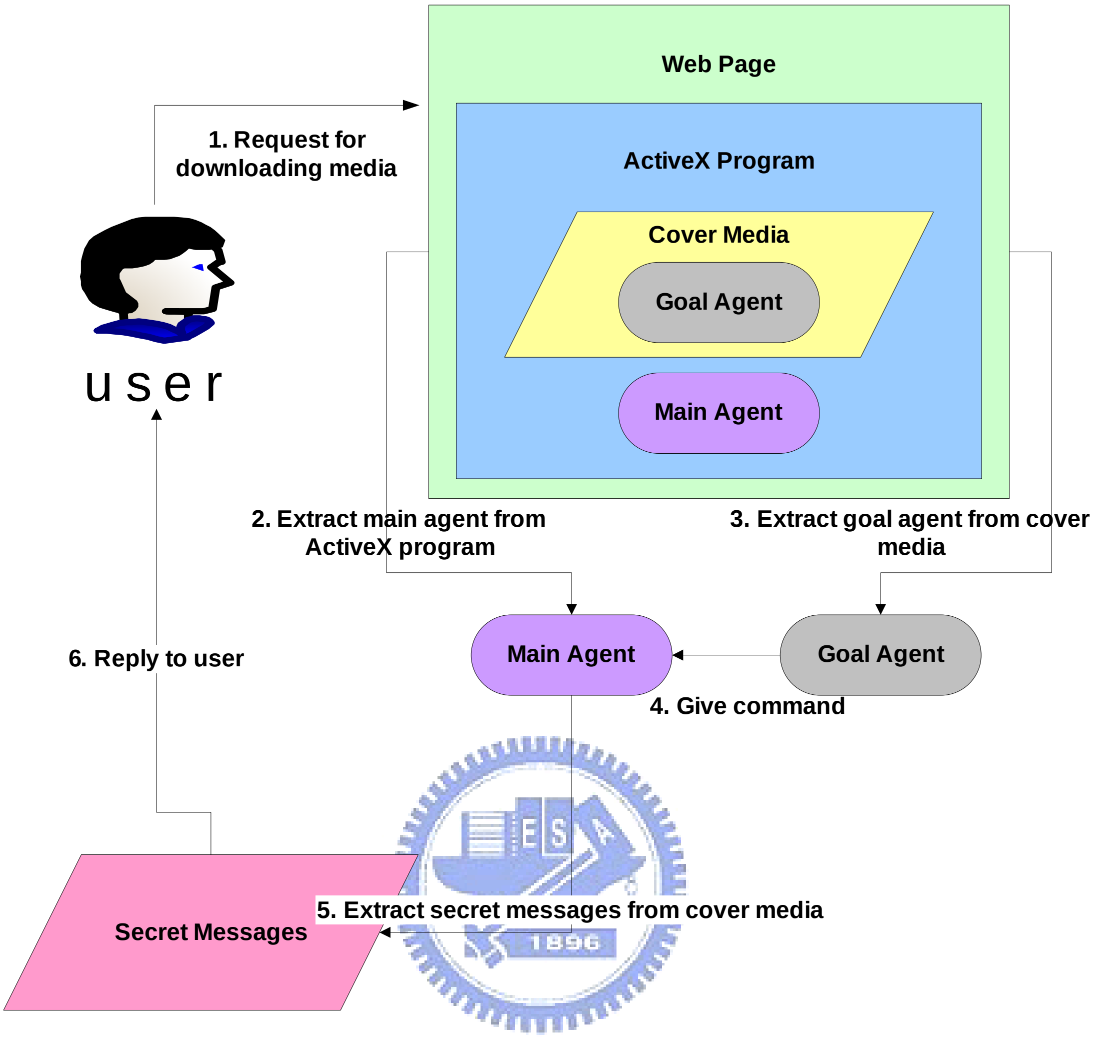

Web Page
ActiveX Program
Cover Media
Goal Agent
Main Agent
1. Request for downloading media
user
2. Extract main agent from ActiveX program
3. Extract goal agent from cover media
Main Agent
Goal Agent
4. Give command
6. Reply to user
Secret Messages
5. Extract secret messages from cover media

Figure 2. 4 An illustration of hiding active agents in active programs and cover media.

2.3.4 Proposed Method for Hiding Agents in JAVA Programs

On the platform of a cellular phone, an active agent can be hidden in a JAVA program like hiding it in an ActiveX program on the platform of a personal computer. The cover media will be packaged with the active agent and compiled into Java Archive (JAR) format which can then be downloaded by users. After completely downloading a JAR file, a user can utilize the active agent to do its predefined task. A flowchart of the proposed method is shown in Figure 2.5.

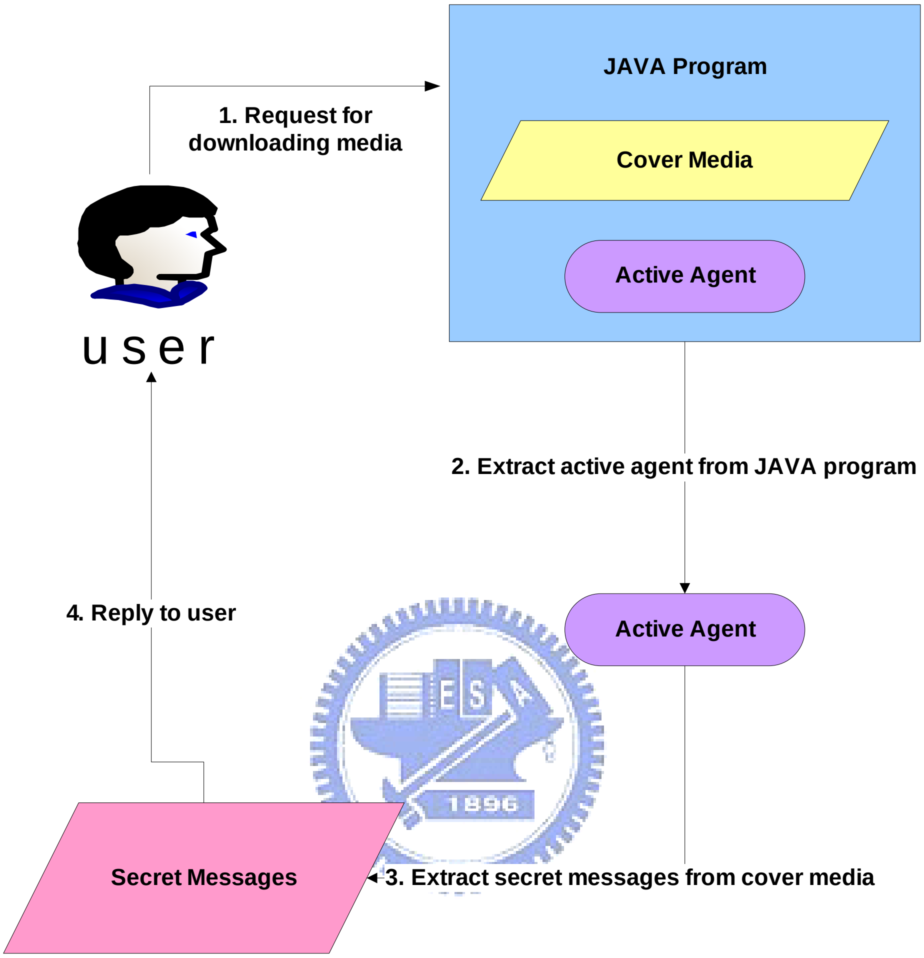

JAVA Program
Cover Media
Active Agent
1. Request for downloading media
user
2. Extract active agent from JAVA program
Active Agent
4. Reply to user
Secret Messages
3. Extract secret messages from cover media

Figure 2. 5 An illustration of hiding active agents in JAVA programs.

2.4 Summary and Discussions

In this chapter, several ways about how to access active agents and some methods for hiding active agents are proposed. On different kinds of platforms, different kinds of media are used to hide active agents for saving the data hiding capacity of the cover media.

In the following chapters of this thesis, two execution platforms, including a personal computer and a cellular phone, and two extraction programs containing an ActiveX program and a JAVA program are adopted. The way to access an active agent investigated in this thesis study is from public web pages and the types of the cover media are images and videos.

Chapter 3

Active Covert Communication by MPEG Videos with Secret Authentication Capability

3.1 Introduction

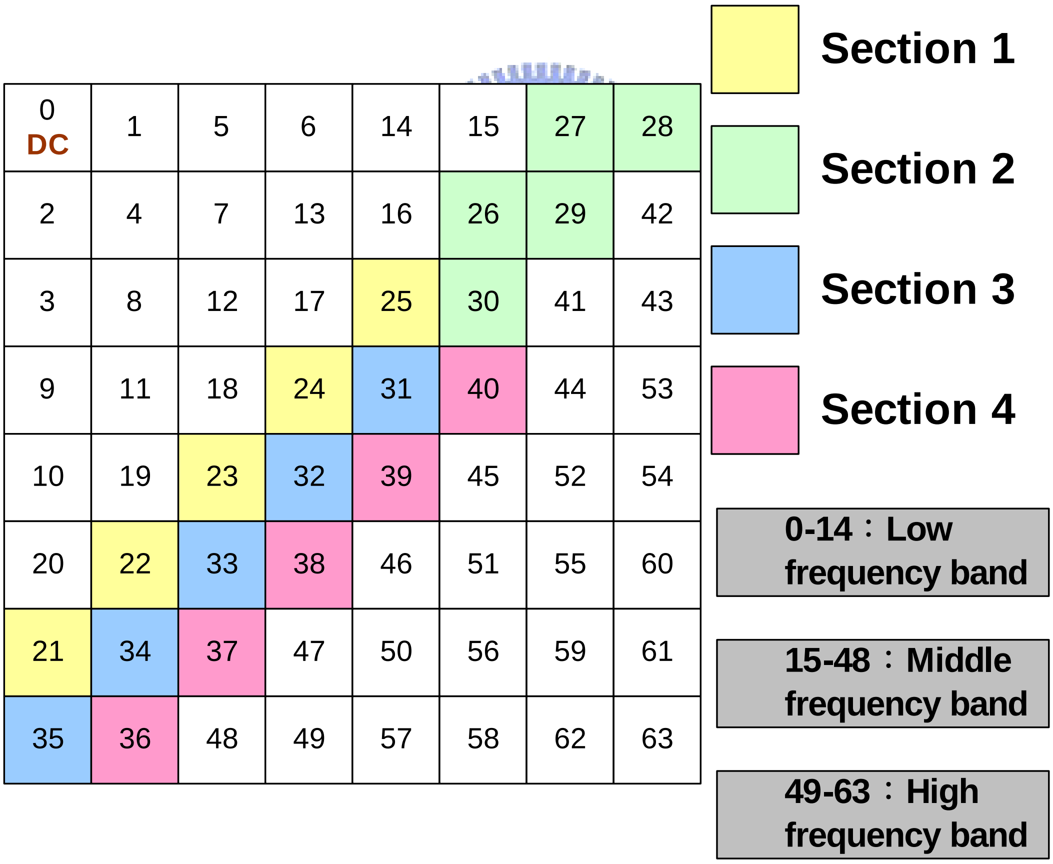
Due to the popularity of computer networks, more and more data is transmitted through the public Internet and many security problems arise when secret messages are transmitted. An illicit user can employ various network tools to intercept these secret messages very easily for misuses. Thus, in this study, a video data hiding method with the secret authentication capability for active covert communication is proposed.

In Section 3.2, some reviews of the data hiding method for MPEG videos are made. In Section 3.3, an authentication method for verifying secret messages is proposed, which calculates authentication signals of secret messages and embeds these signals into the messages. In Section 3.4, an active covert communication method for MPEG videos is proposed and two related processes are presented. In Section 3.5, experimental results are shown to prove the proposed methods, and finally in Section 3.6, some discussions and a summary are given .

3.2 Review of A Secret Data Hiding

Method for MPEG Videos

In the MPEG standard, all macroblocks in I frames are intra-coded ones without referencing to others. The compression technique used in I frames is similar to the one of the JPEG standard, so the DCT-based data hiding technique may be applied. There are three kinds of frequency bands, namely, low-frequency bands, middle-frequency ones, and high-frequency ones, in an 8×8 DCT block. In order to maintain a trade-off between imperceptivity and data hiding capacity, the middle-frequency band in Figure 3.1 is chosen to embed secret data in this study.



0 DC	1	5	6	14	15	27	28
2	4	7	13	16	26	29	42
3	8	12	17	25	30	41	43
9	11	18	24	31	40	44	53
10	19	23	32	39	45	52	54
20	22	33	38	46	51	55	60
21	34	37	47	50	56	59	61
35	36	48	49	57	58	62	63

Figure 3. 1 An illustration of an 8×8 DCT block.

P and B frames are inter-coded frames different from I ones and are encoded by motion compensation prediction to reduce the temporal redundancy between frames. In P frames, there are many forward-coded macroblocks and some intra-coded macroblocks. In B frames, there are many backward-coded macroblocks, forward-coded macroblocks and some intra-coded macroblocks. Because many motion vectors are used in inter-coded macroblocks to reduce the temporal redundancy, they may be utilized to hide secret data efficiently.

The same encoding type of macroblocks in different kinds of frames facilitates the use of the same method to hide data in them. In Section 3.2.1, a data hiding method based on the use of DCT coefficients in intra-coded macroblocks is introduced. In Section 3.2.2, a method of hiding secret data in forward-coded macroblocks is presented. Then in Section 3.2.3, a method of hiding secret data in backward-coded macroblocks is reviewed.

3.2.1 Process for Hiding Secret Data in I Frames

After MPEG video are processed with variable-length decoding, the quantized DCT coefficients of each 8x8 block of the input I frame can be obtained. An algorithm of the process is described as follows.

***Algorithm* 1:** Hiding secret data in intra-coded macroblocks.

***Input*:** secret data *S*, and a macroblock *M*.

***Output*:** a macroblock *M'* in which the secret data are embedded.

***Steps*:**

1. Get an 8x8 luminance block *L* from *M* which has four 8x8 luminance blocks and find the coefficient C_i whose magnitude is the maximum in each pre-defined section as shown in Figure 3.1.
2. Acquire a bit *b* of *S* sequentially and hide it into every C_i. The hiding rules *R* are illustrated in the following.

    I. *If* $C_i \geq 0$:

i. *if* $b = 1$ *and* C_i *is even, then set* $C_i = C_i + 1$;

ii. *if* $b = 0$ *and* C_i *is odd, then set* $C_i = C_i + 1$;

iii. *otherwise, leave* C_i *unchanged.*

II. *If* $C_i < 0$:

i. *if* $b = 1$ *and* C_i *is even, then set* $C_i = C_i - 1$;

ii. *if* $b = 0$ *and* C_i *is odd, then set* $C_i = C_i - 1$;

iii. *otherwise, leave* C_i *unchanged.*

An illustration of the hiding process for I frames is presented as a flowchart in Figure 3.2 as follows.

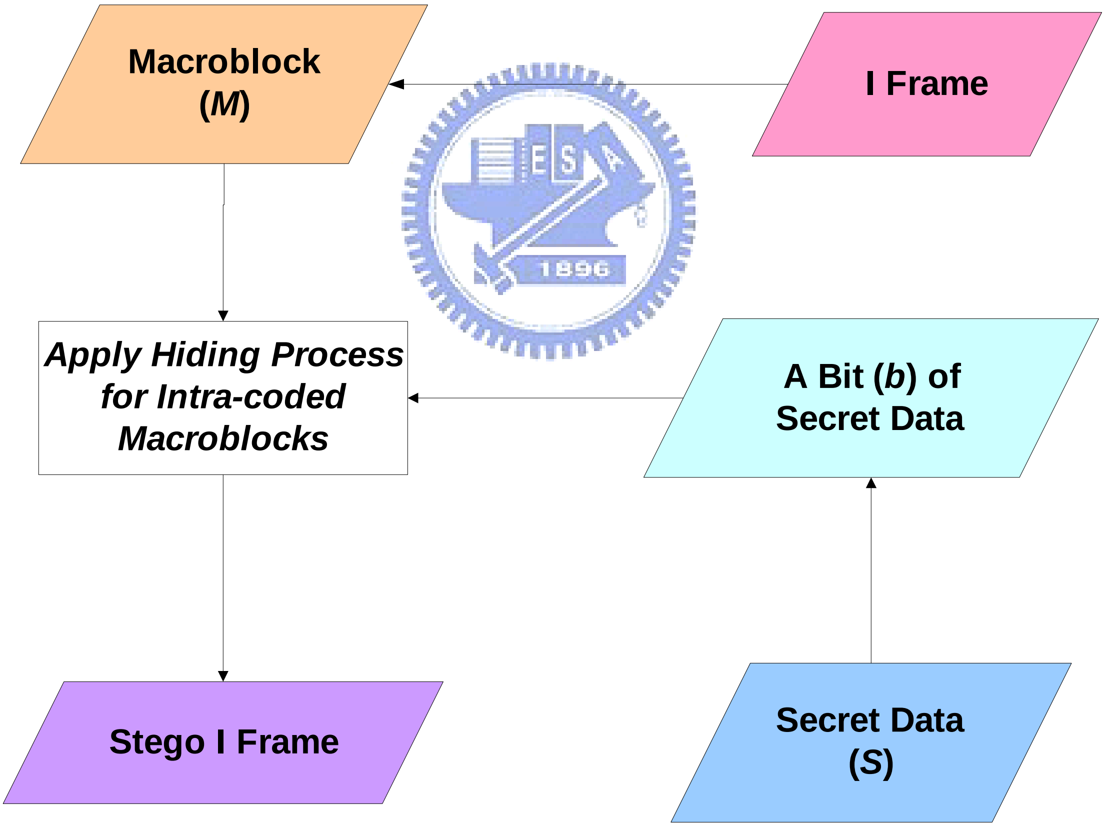

Macroblock
(*M*)
I Frame
Apply Hiding Process for Intra-coded Macroblocks
A Bit (*b*) of Secret Data
Stego I Frame
Secret Data
(*S*)

Figure 3. 2 A flowchart of the process of hiding secret data in I frames.

3.2.2 Process for Hiding Secret Data in P Frames

There are two encoding types of macroblocks, namely, intra-coded ones and forward-coded ones, in P frames. Because the data hiding method of intra-coded macroblocks is similar to the one used in I frames, in this section, a data hiding method of forward-coded macroblocks is introduced. A detailed algorithm is presented in the following.

***Algorithm* 2:** Hiding secret data in forward-coded macroblocks.

***Input*:** secret data *S*, and macroblock *M*.

***Output*:** a macroblock *M'* in which the secret data are embedded.

***Steps*:**

1. Acquire a horizontal component *H* and a vertical one *V* from a motion vector of the input forward-coded macroblock and use a threshold *T* to decide if the current macroblock is proper to hide secret data. The decision rule is described as follows:

   $$|H| > T \text{ or } |V| > T.$$

   The magnitude of *T* is just a tradeoff between the video quality and the data hiding capacity. The larger *T* is, the less distortion the video has to bear and the less data can be hidden into the video.

2. Use following embedding rules *R* to embed a bit *b* of *S* into the selected motion vector if the above condition is true.

   I. *If* $|H| \geq |V|$ *and* $H \geq 0$:

      i. *if* $b = 1$ *and H is even, then set* $H = H + 1$;

      ii. *if* $b = 0$ *and H is odd, then set* $H = H + 1$;

      iii. *otherwise, leave H unchanged.*

   II. *If* $|H| \geq |V|$ *and* $H < 0$:

      i. *if* $b = 1$ *and H is even, then set* $H = H - 1$;

      ii. *if* $b = 0$ *and H is odd, then set* $H = H - 1$;

      iii. *otherwise, leave H unchanged.*

III. *If* $|H| < |V|$ *and* $V \geq 0$:

i. *if* $b = 1$ *and* V *is even, then set* $V = V + 1$;

ii. *if* $b = 0$ *and* V *is odd, then set* $V = V + 1$;

iii. *otherwise, leave* V *unchanged.*

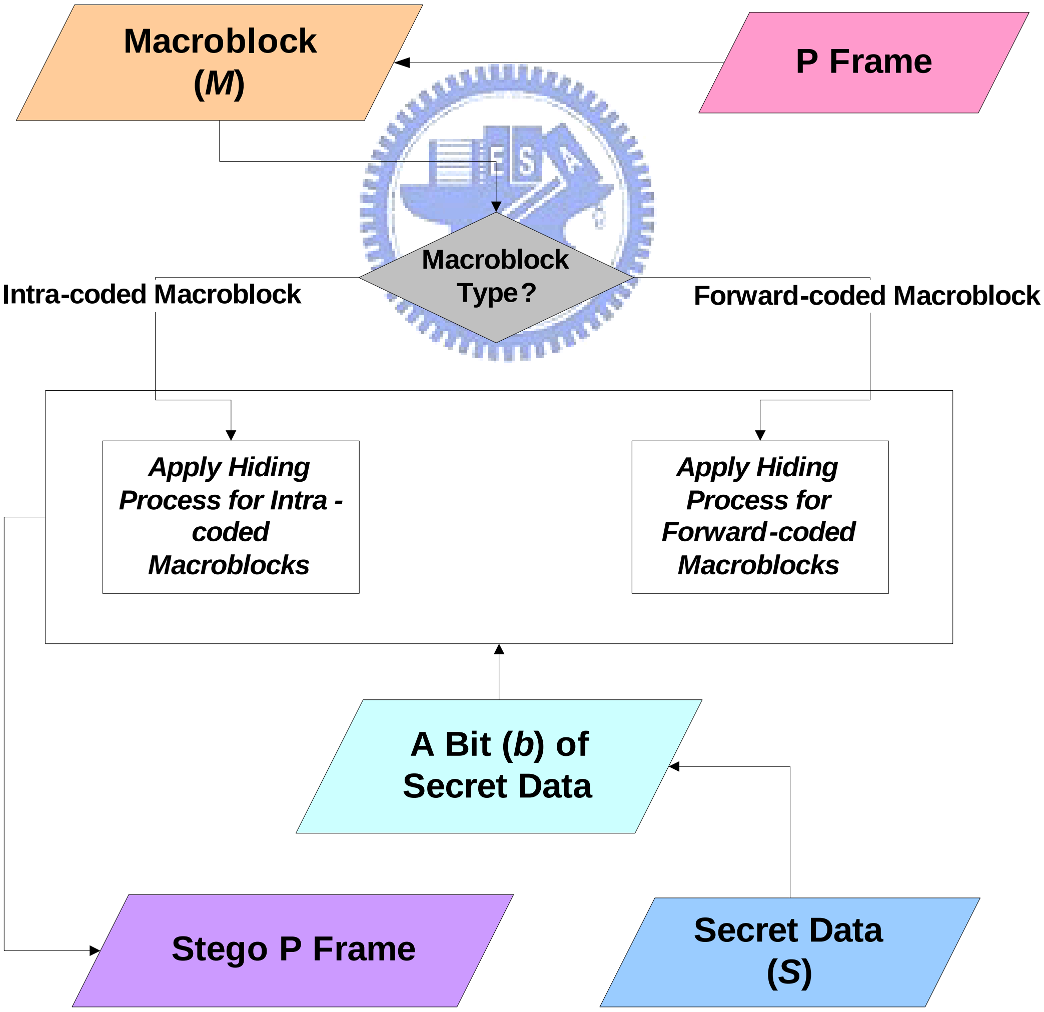
IV. *If* $|H| < |V|$ *and* $V < 0$:

i. *if* $b = 1$ *and* V *is even, then set* $V = V - 1$;

ii. *if* $b = 0$ *and* V *is odd, then set* $V = V - 1$;

iii. *otherwise, leave* V *unchanged.*

An illustration of the hiding process for P frames is presented as a flowchart in Figure 3.3 as follows.



Macroblock (*M*)
P Frame
Macroblock Type?
Intra-coded Macroblock
Forward-coded Macroblock
Apply Hiding Process for Intra-coded Macroblocks
Apply Hiding Process for Forward-coded Macroblocks
A Bit (*b*) of Secret Data
Stego P Frame
Secret Data (*S*)

Figure 3. 3 A flowchart of the process of hiding secret data into P frames.

3.2.3 Process for Hiding Secret Data in B Frames

There are three encoding types of macroblocks, namely, intra-coded ones, forward-coded ones and backward-coded ones, in B frames. Both data hiding methods for intra-coded macroblocks and for forward-coded macroblocks in B frames are similar to those in P frames. In this section, a data hiding method for backward-coded macroblocks is introduced. A corresponding algorithm is described in the following.

***Algorithm* 3:** Hiding secret data in backward-coded macroblocks.

***Input*:** secret data *S*, and macroblock *M*.

***Output*:** a macroblock *M'* in which the secret data are embedded.

***Steps*:**

1. Acquire a horizontal component *H* and a vertical one *V* from a motion vector of the input backward-coded macroblock and use a threshold *T* to decide if the current macroblock is proper to hide secret data by the following rule:

$$|\,H\,| > T \text{ or } |\,V\,| > T.$$

2. Use following embedding rules *R* to embed a bit *b* of *S* into the selected motion vector if the above condition is true.

   I. *If* $|\,H\,| \geq |\,V\,|$ *and* $H \geq 0$:

      i. *if* $b = 1$ *and H is even, then set* $H = H + 1$;

      ii. *if* $b = 0$ *and H is odd, then set* $H = H + 1$;

      iii. *otherwise, leave H unchanged.*

   II. *If* $|\,H\,| \geq |\,V\,|$ *and* $H < 0$:

      i. *if* $b = 1$ *and H is even, then set* $H = H - 1$;

      ii. *if* $b = 0$ *and H is odd, then set* $H = H - 1$;

      iii. *otherwise, leave H unchanged.*

   III. *If* $|\,H\,| < |\,V\,|$ *and* $V \geq 0$:

i. *if* $b = 1$ *and* V *is even, then set* $V = V + 1$;

ii. *if* $b = 0$ *and* V *is odd, then set* $V = V + 1$;

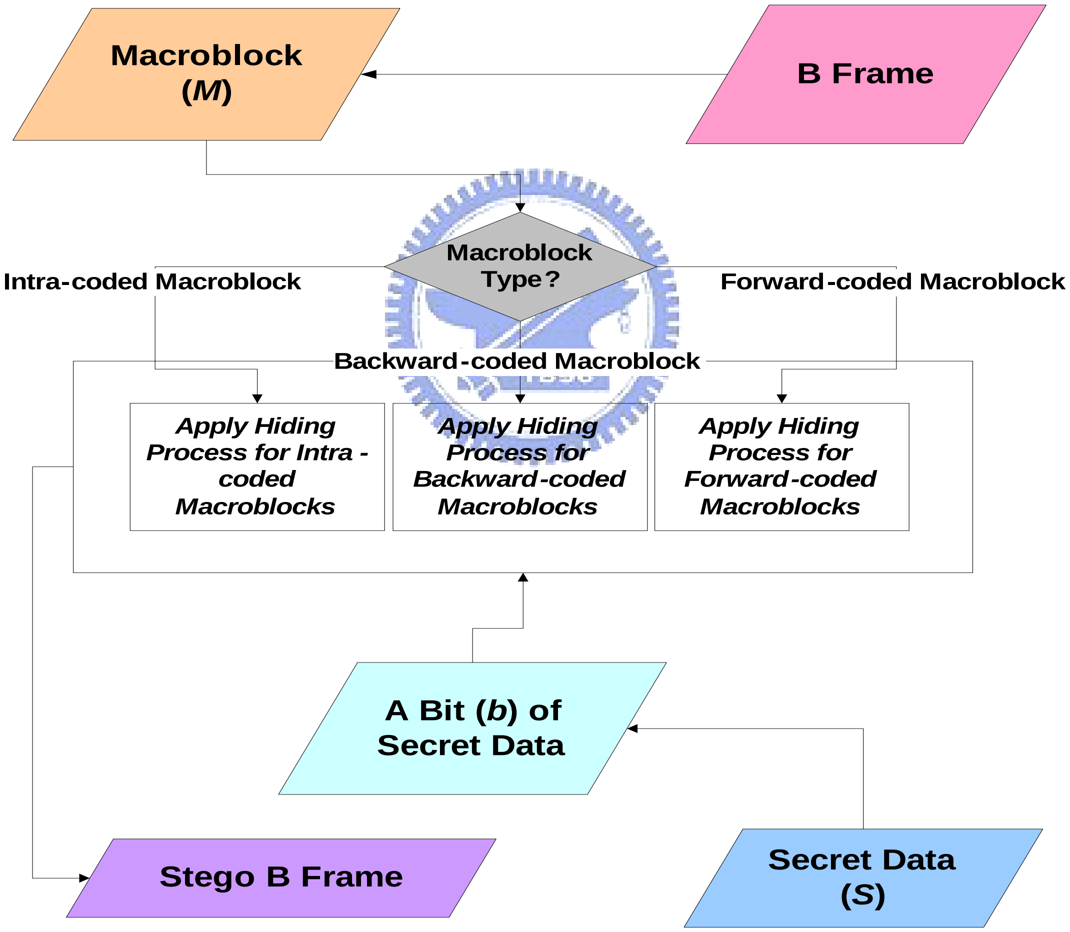
iii. *otherwise, leave* V *unchanged.*

IV. *If* $|H| < |V|$ *and* $V < 0$:

i. *if* $b = 1$ *and* V *is even, then set* $V = V - 1$;

ii. *if* $b = 0$ *and* V *is odd, then set* $V = V - 1$;

iii. *otherwise, leave* V *unchanged.*



Macroblock (*M*)
B Frame
Macroblock Type?
Intra-coded Macroblock
Forward-coded Macroblock
Backward-coded Macroblock
Apply Hiding Process for Intra-coded Macroblocks
Apply Hiding Process for Backward-coded Macroblocks
Apply Hiding Process for Forward-coded Macroblocks
A Bit (*b*) of Secret Data
Stego B Frame
Secret Data (*S*)

Figure 3. 4 A flowchart of the process of hiding secret data in B frames.

Just like what we mentioned before, the magnitude of *T* used in Step 1 above is just a tradeoff between the video quality and the data hiding capacity. The larger *T* is, the less distortion the video has to bear and the less data can be hidden into the video. An illustration of the hiding process for B frames is presented as a flowchart in Figure 3.4 as follows.

3.3 Authentication Method for Secret Messages

Under the process of transmitting the cover media with the secret messages on public networks, malicious users might use various methods to intercept the cover media and try to extract the secret messages hidden in it or modify the secret messages to cheat the receiver who needs the secret messages. If this receiver is an employee who works for a company, fake secret messages can lead him/her to make wrong decisions and cause a great loss to the company. In order to avoid situations like this to happen, a method for calculating authentication signals of the secret messages and embedding them in the secret messages is proposed. With the use of the authentication signals, the fidelity of the secret messages can be ensured by our method proposed in this study, as described in the following sections.

3.3.1 Calculation of Authentication Signals of Secret Messages

Let *M* be certain given secret messages with the size of *l*, and *A* be authentication signals to be embedded in *M*. The size of *A* is the same as one integer of 4 bytes. A detailed algorithm of the calculation of *A* for *M* is described in the following.

***Algorithm* 4:** Calculation of authentication signals for secret messages.

***Input*:** secret messages *M* with the size of *l* bytes.

***Output*:** authentication signals *A*.

***Steps*:**

1. Transform *M* into a byte form $(b_1\ b_2\ \ldots\ b_l)_{256}$ with each b_i ($i = 1, 2, \ldots, l$) being one byte of *M*.
2. Calculate the sum of b_i ($i = 1, 2, \ldots, l$) to generate *A* which is described as the following equation:

$$A = (b_1 + b_2 + \ldots + b_l) \bmod 2^{32}$$

3.3.2 Process for Embedding Authentication Signals

After calculating authentication signals for secret messages, these signals will be embedded in the secret messages and new messages are generated. A corresponding detailed algorithm is shown in the following.

***Algorithm* 5:** Embedding process for authentication signals.

***Input*:** secret messages *M* with the size of *m* bytes, authentication signals *A* with the size of 4 bytes, and a user key *K* for generating a non-repeating random number sequence.

***Output*:** temporary messages *T* for the concatenation of *M* and *A*, and new secret messages *M'*.

***Steps*:**

1. Transform both *M* and *A* into a byte form and concatenate them into temporary messages *T* as follows:

$$M = (a_1\ a_2\ \ldots\ a_m)_{256},\ A = (b_1\ b_2\ b_3\ b_4)_{256}$$

$$T = M + A = (a_1\ a_2\ \ldots\ a_m\ b_1\ b_2\ b_3\ b_4)_{256}$$

2. Use *K* to generate a non-repeating random number sequence to randomize *T* and produce the desired new secret messages *M'*.

3.3.3 Process for Extracting Authentication Signals

After generating the new messages as authentication signals, they will be embedded in the cover media and transmitted to the receiver site. On the receiver site, the secret messages can be extracted and authenticated. The extraction algorithm is an inverse process of the embedding one and is described in the following.

***Algorithm* 6:** Extraction process for authentication signals.

***Input*:** secret messages *M'* with the size of *m* bytes extracted by Algorithm described later, and a user key *K* for generating a non-repeating random number sequence.

Output*:** authentication signals *A* with the size of 4 bytes extracted by Algorithm described later, and recovered secret messages *M* with the size of (m - 4) bytes, and temporary messages *T*, and authentication signals *A'* recalculated by ***Algorithm 4 described before.

***Steps*:**

1. Use *K* to generate a non-repeating random number sequence to de-randomize *M'* and produce temporaray messages *T*.
2. Transform *T* into the byte form and decompose *T* to get *M* and *A* by the following way:

$$T = (\mathrm{a}_1\ \mathrm{a}_2 \ldots \mathrm{a}_m\ \mathrm{b}_1\ \mathrm{b}_2\ \mathrm{b}_3\ \mathrm{b}_4)_{256};$$

$$M = (\mathrm{a}_1\ \mathrm{a}_2 \ldots \mathrm{a}_m)_{256};$$

$$A = (\mathrm{b}_1\ \mathrm{b}_2\ \mathrm{b}_3\ \mathrm{b}_4)_{256}.$$

3. Recalculate authentication signals *A'* using *M* as follows:

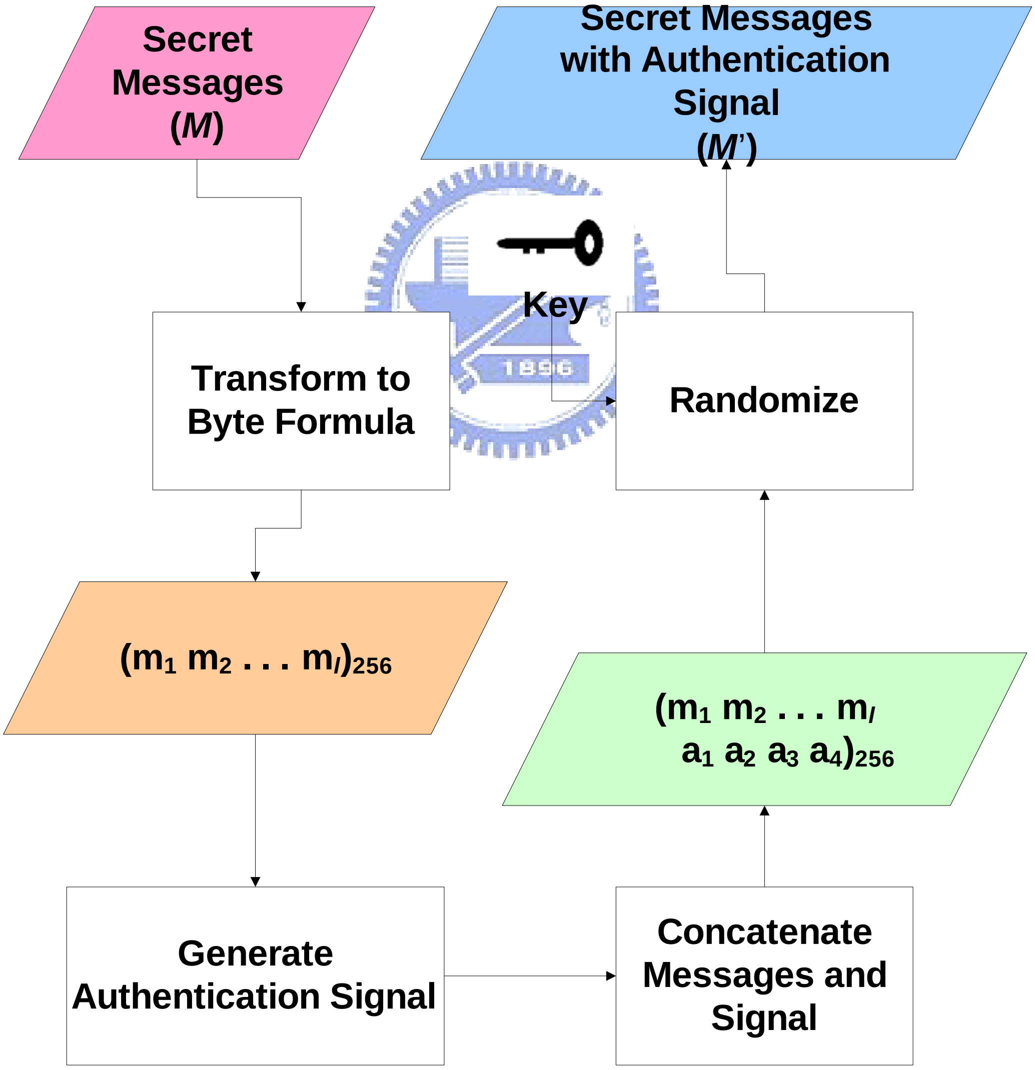
$$A' = (\mathrm{a}_1 + \mathrm{a}_2 + \ldots + \mathrm{a}_m) \bmod 2^{32}.$$

4. Compare *A* and *A'* to make the decision as follows:

$$\begin{cases} if\ \ A = A',\ then\ keep\ M; \\ otherwise,\ discard\ M. \end{cases}$$

If *A* does not equal *A'*, regard the original secret messages to have been tampered with or the cover media to have been modified, discard the extracted secret messages, and inform the sender of the errors.

Note that if the user key provided by the receiver is wrong, *A* will not equal to *A'*, either. An illustration of the authentication method for secret messages is shown in Figure 3.5.



Secret Messages (*M*)
Secret Messages with Authentication Signal (*M'*)
Key
Transform to Byte Formula
Randomize
(m₁ m₂ . . . mₗ)₂₅₆
(m₁ m₂ . . . mₗ a₁ a₂ a₃ a₄)₂₅₆
Generate Authentication Signal
Concatenate Messages and Signal

Figure 3. 5 An illustration of the authentication method for secret messages.

3.4 Proposed Active Covert Communication Method for MPEG Videos

The pre-defined environment of active covert communication is built on a web page with an ActiveX program. An ActiveX program in which an active agent has been embedded includes an active video player and a MPEG video clip. Here is an application example. When an employee works outside and has to receive messages from a superior, the employee can browse a public web page and get secret messages hidden in an MPEG video without the need of installing data extraction programs.

In this example, the task of the active agent is to extract secret messages. Before beginning the extraction process, the receiver has to provide an authentic user key. If this user key is wrong, the receiver will get nothing after seeing the video on the web page.

3.4.1 Process for Embedding Secret Messages

The embedding process is executed on the platform of a sender-site computer. An illustration of the entire process is shown in Figure 3.6.

First, authentication signals are generated by the input secret messages. Then, these secret messages are concatenated with authentication signals and randomized by a user key. After generating randomized secret messages, they are hidden in an MPEG video.

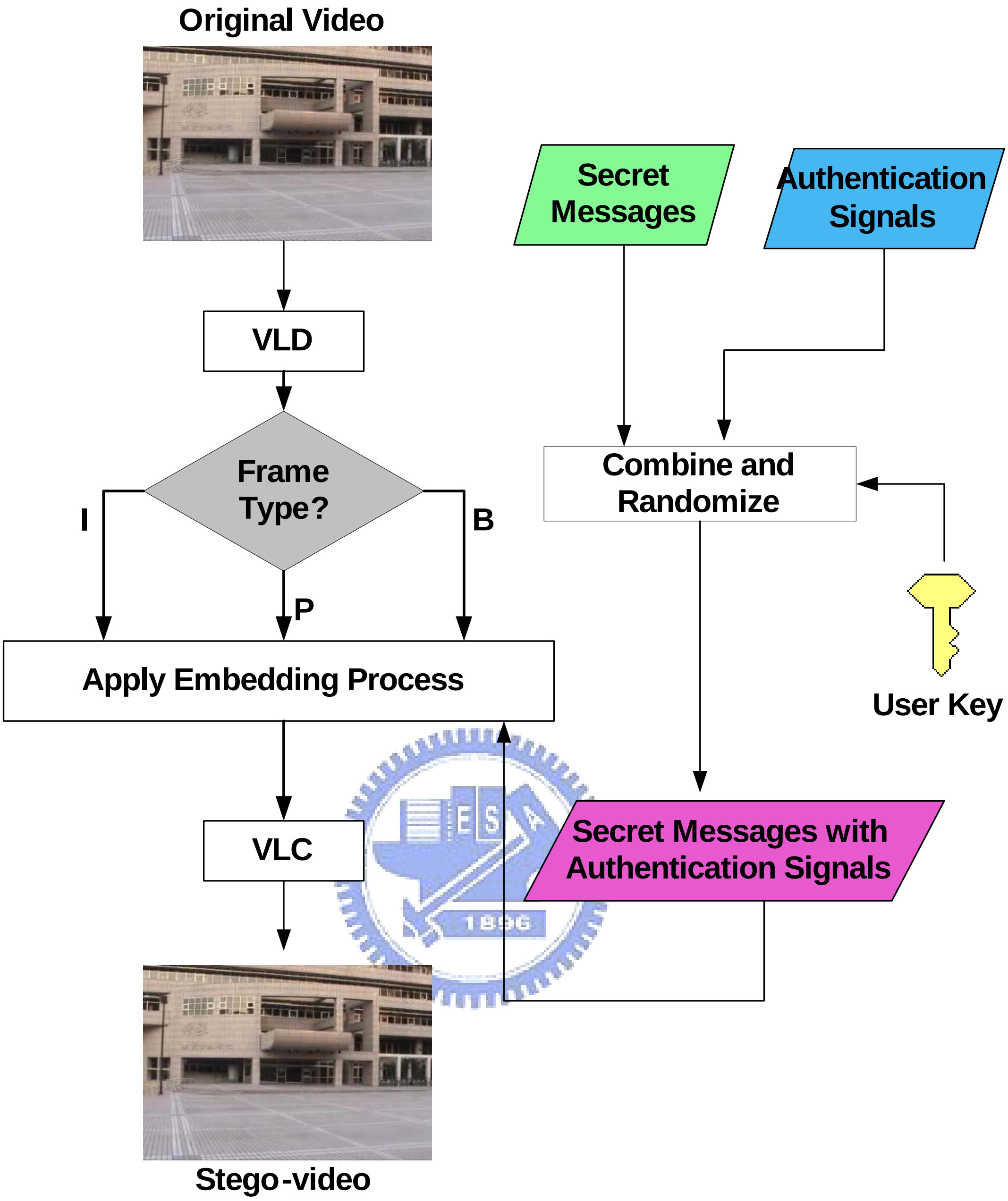
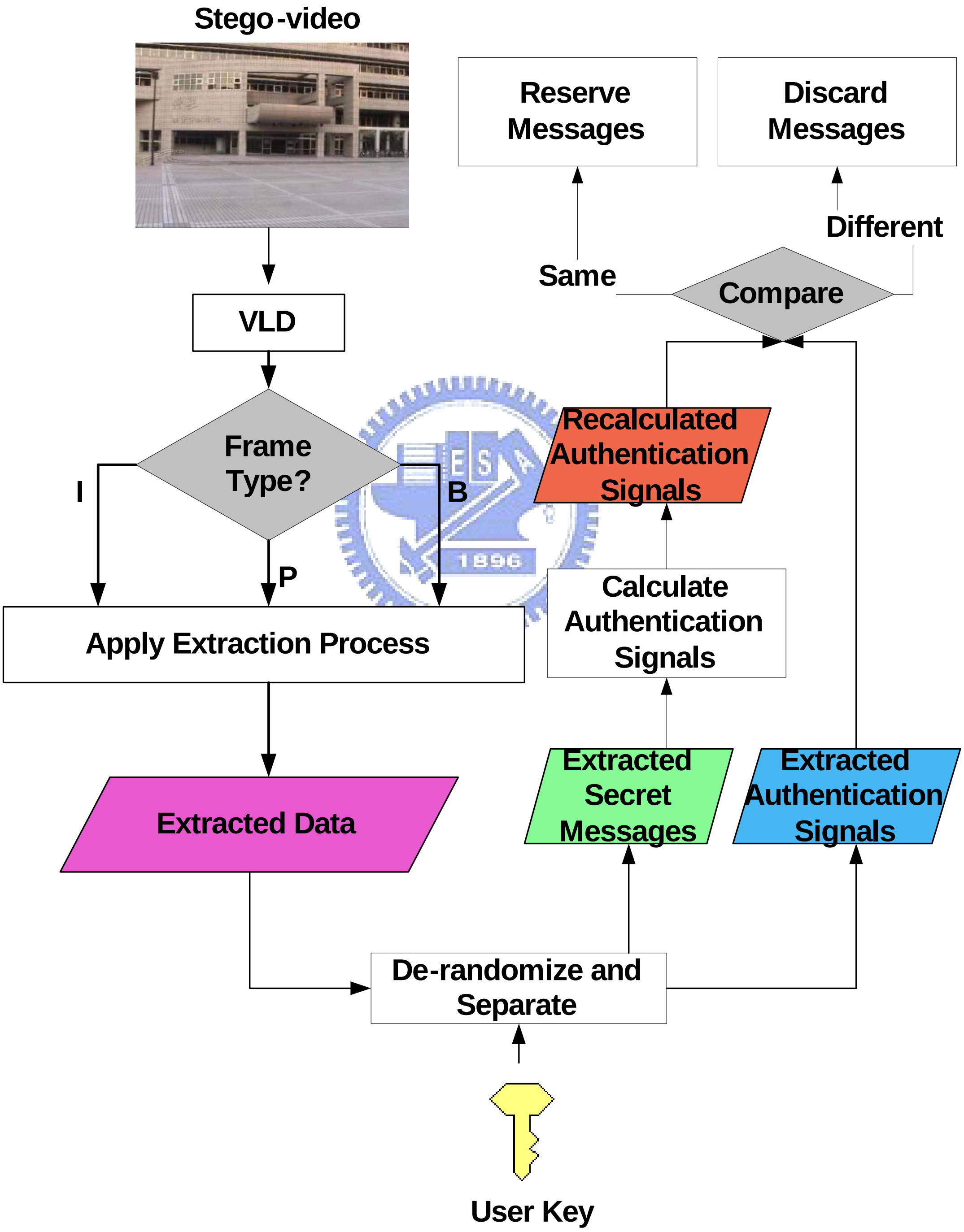


Figure 3. 6 A flowchart of the process of embedding secret messages in an MPEG video.

3.4.2 Process for Extracting Secret Messages

The extraction process is an inverse process of the embedding one. The process is executed on the platform of a receiver-site computer. An illustration of how to extract secret messages is shown in Figure 3.7.

After extracting data from an MPEG video, the data needs to be de-randomized by a user key to obtain secret messages and authentication signals. Then, the extracted secret messages have to be verified, so the extracted authentication signals will be compared to the recalculated ones. If there is no difference between these two signals, the extracted secret messages are kept, otherwise discarded.



Stego-video
Reserve Messages
Discard Messages
Different
Same
Compare
VLD
Frame Type?
I
B
P
Recalculated Authentication Signals
Calculate Authentication Signals
Apply Extraction Process
Extracted Data
Extracted Secret Messages
Extracted Authentication Signals
De-randomize and Separate
User Key

Figure 3. 7 A flowchart of the process of extracting secret messages into an MPEG video.

A flowchart of the process of the active covert communication method is illustrated in Figure 3.8. In the server-site process, secret messages with authentication signals are embedded in a MPEG video put on a public web page. While a user requests for downloading secret messages, the proposed system can extract and execute active agents. Then, the active agents can extract secret messages from the MPEG video and authenticate them for the authentic user.

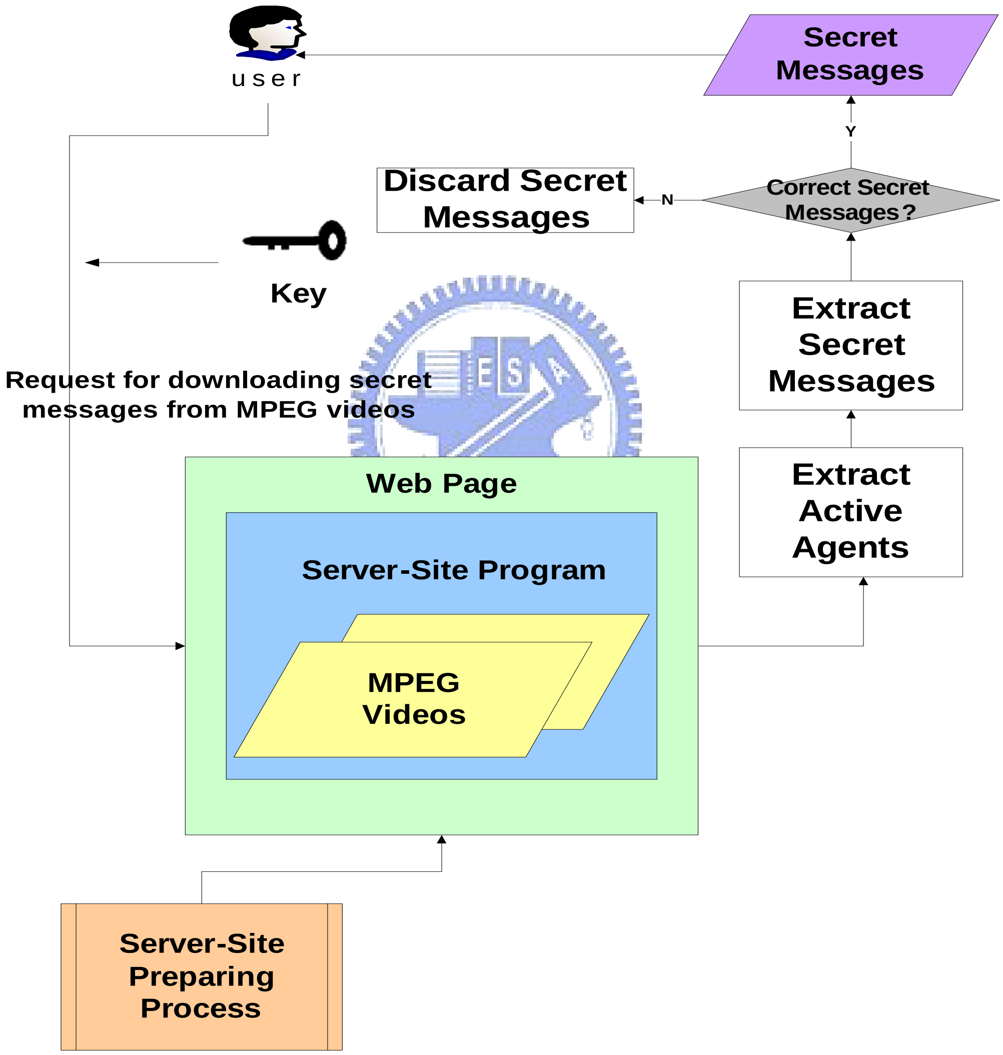
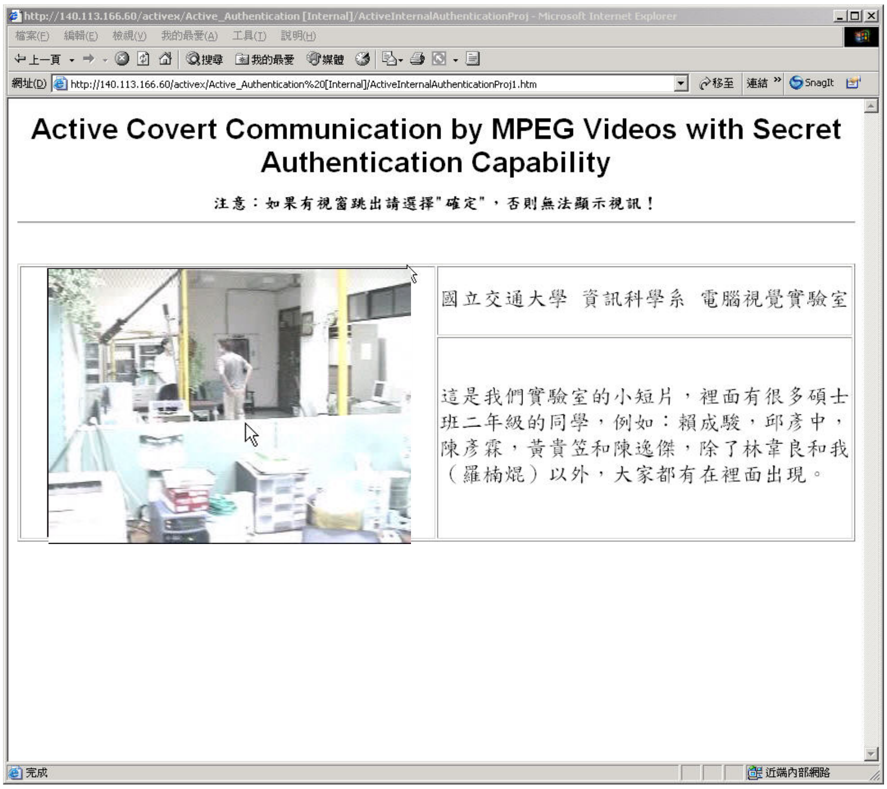


Figure 3. 8 A flowchart of the process of the active covert communication method.

3.5 Experimental Results

In our experiments, a stego-video with secret messages is put on a public web page for people to preview. When a user browses this web page, the stego-video with a description is displayed on the screen shown in Figure 3.9(a). After pressing the replay button on the pop-up menu in Figure 3.9(b) four times, a dialog in which the user key can be keyed in will be shown for the user. If the input key is authentic, secret messages which are hidden in the stego-video can be extracted into the local computer in Figure 3.9(e). On the contrary, an illegal user can just get nothing.



http://140.113.166.60/activex/Active_Authentication [Internal]/ActiveInternalAuthenticationProj - Microsoft Internet Explorer

http://140.113.166.60/activex/Active_Authentication%20[Internal]/ActiveInternalAuthenticationProj1.htm

Active Covert Communication by MPEG Videos with Secret Authentication Capability

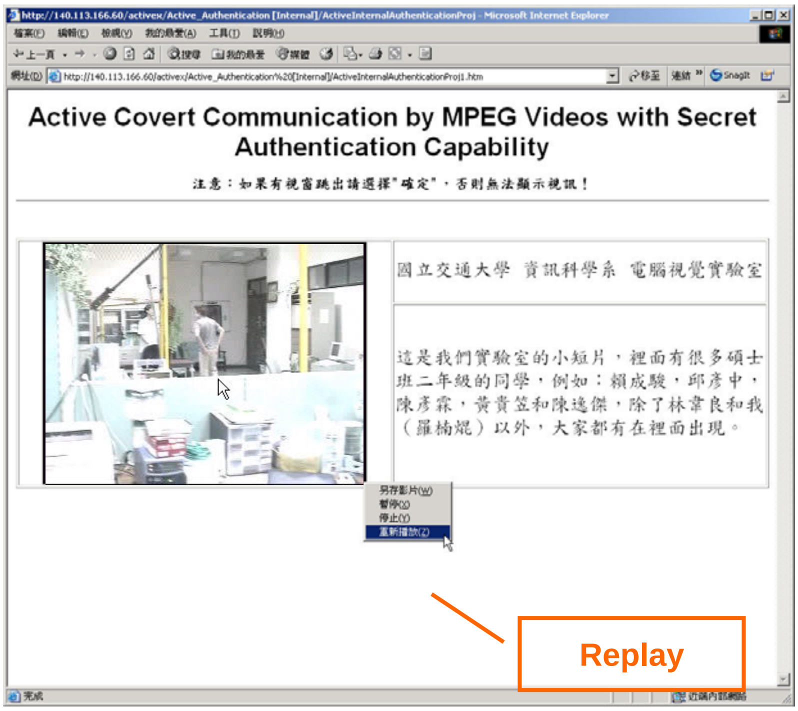
注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

國立交通大學　資訊科學系　電腦視覺實驗室

這是我們實驗室的小短片，裡面有很多碩士班二年級的同學，例如：賴成駿，邱彥中，陳彥霖，黃貴笠和陳逸傑，除了林韋良和我（羅楠焜）以外，大家都有在裡面出現。

(a)

Figure 3.9 The process of the proposed active covert communication method. (a) An initial web page with a stego-video displayed on the browser. (b) A replay button on a pop-up menu. (c) A dialog in which a user key can be inputted. (d) A dialog which can select the saving location of extracted secret messages. (e) The extracted secret messages on the desktop. (f) The content of the extracted secret messages. (continued)



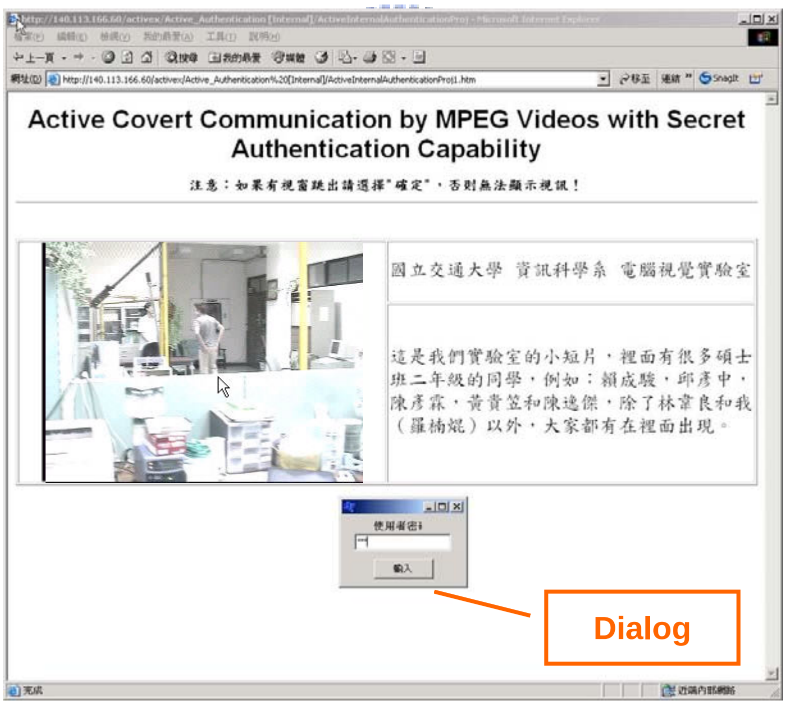
Active Covert Communication by MPEG Videos with Secret Authentication Capability

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

國立交通大學 資訊科學系 電腦視覺實驗室

這是我們實驗室的小短片，裡面有很多碩士班二年級的同學，例如：賴成駿，邱彥中，陳彥霖，黃貴笠和陳逸傑，除了林韋良和我（羅楠焜）以外，大家都有在裡面出現。

(b)



Active Covert Communication by MPEG Videos with Secret Authentication Capability

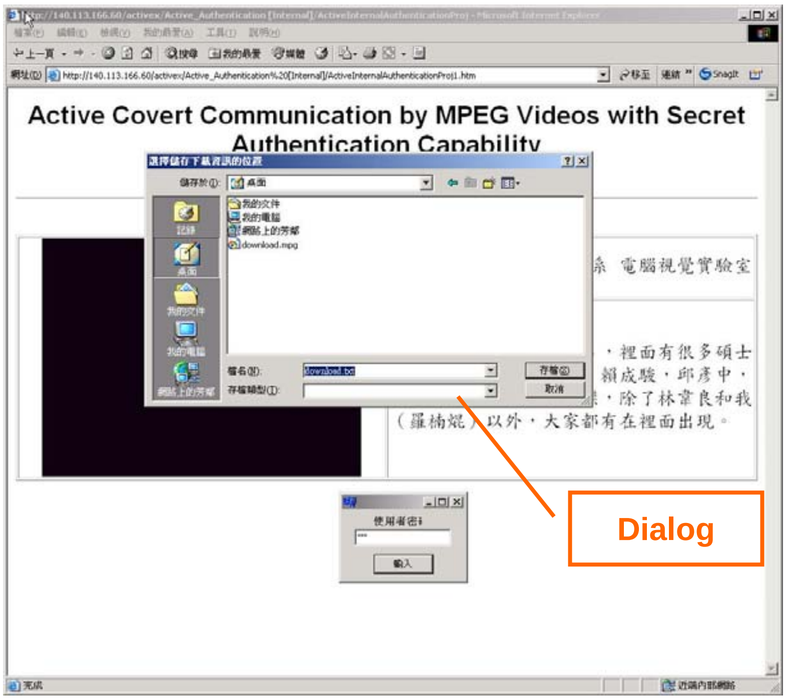
注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

國立交通大學 資訊科學系 電腦視覺實驗室

這是我們實驗室的小短片，裡面有很多碩士班二年級的同學，例如：賴成駿，邱彥中，陳彥霖，黃貴笠和陳逸傑，除了林韋良和我（羅楠焜）以外，大家都有在裡面出現。

(c)

Figure 3.9 The process of the proposed active covert communication method. (a) An initial web page with a stego-video displayed on the browser. (b) A replay button on a pop-up menu. (c) A dialog in which a user key can be inputted. (d) A dialog which can select the saving location of extracted secret messages. (e) The extracted secret messages on the desktop. (f) The content of the extracted secret messages. (continued)

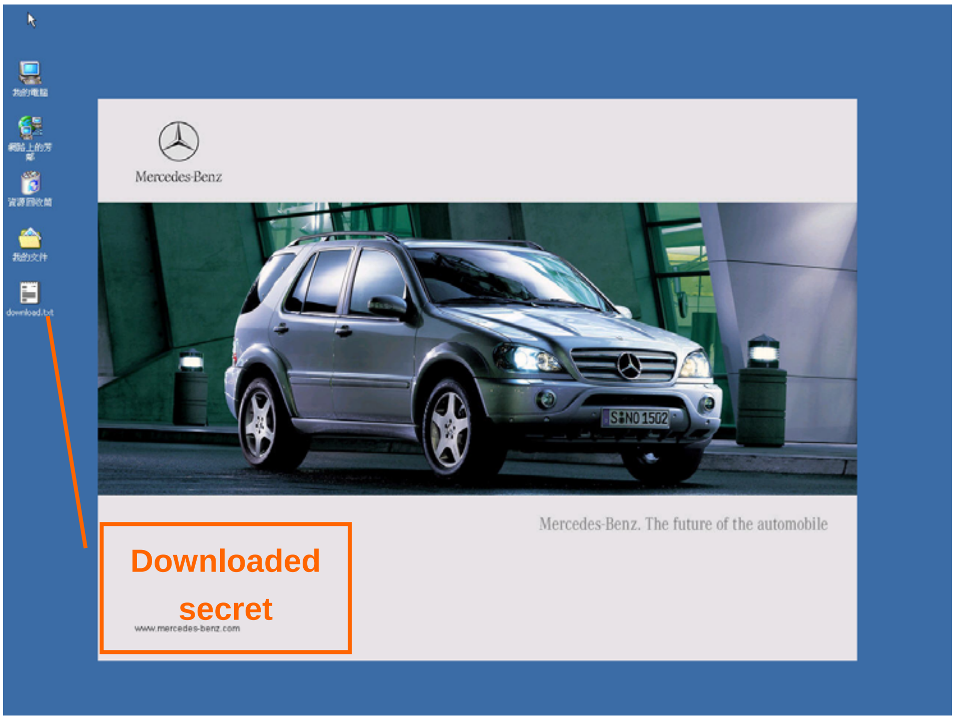


Active Covert Communication by MPEG Videos with Secret Authentication Capability

糸 電腦視覺實驗室

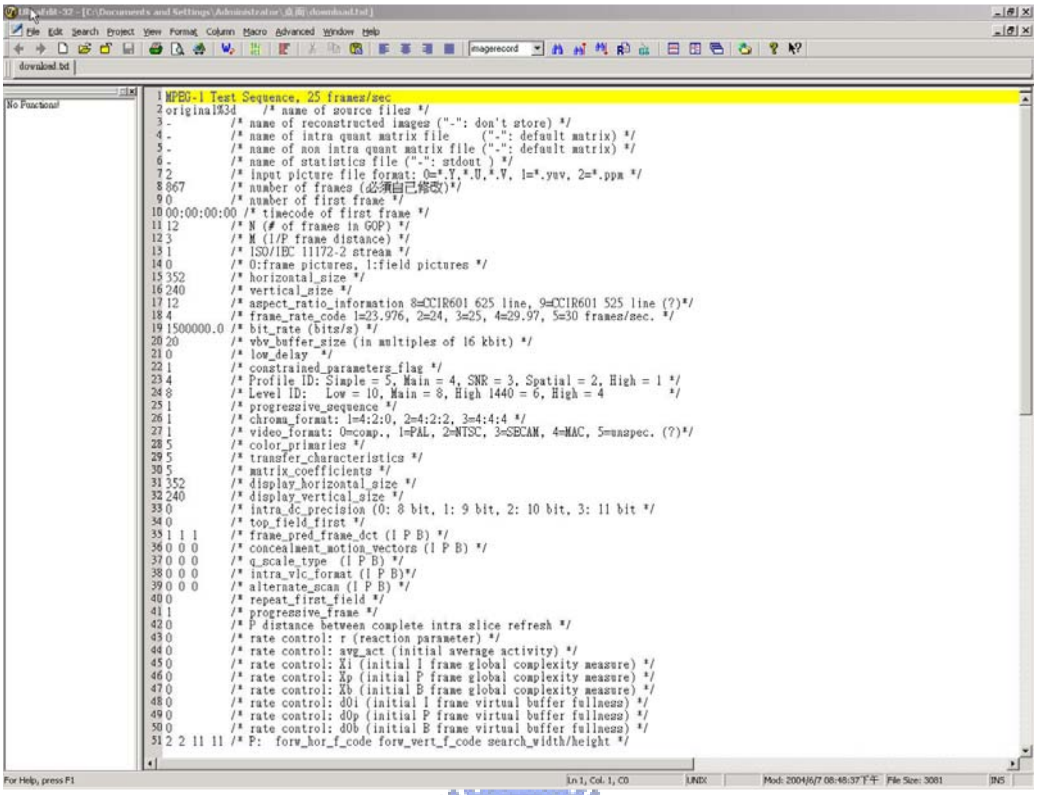
，裡面有很多碩士
縝成駿，邱彥中，
，除了林韋良和我
（羅楠焜）以外，大家都有在裡面出現。

(d)



(e)

Figure 3.9 The process of the proposed active covert communication method. (a) An initial web page with a stego-video displayed on the browser. (b) A replay button on a pop-up menu. (c) A dialog in which a user key can be inputted. (d) A dialog which can select the saving location of extracted secret messages. (e) The extracted secret messages on the desktop. (f) The content of the extracted secret messages. (continued)


File Edit Search Project View Format Column Macro Advanced Window Help
imagerecord
download.txt
No Functions!
For Help, press F1
Ln 1, Col. 1, C0
UNIX
Mod: 2004/6/7 08:46:37下午
File Size: 3081
INS

```
MPEG-1 Test Sequence, 25 frames/sec
original%3d    /* name of source files */
-           /* name of reconstructed images ("-": don't store) */
-           /* name of intra quant matrix file     ("-": default matrix) */
-           /* name of non intra quant matrix file ("-": default matrix) */
-           /* name of statistics file ("-": stdout ) */
2           /* input picture file format: 0=*.Y,*.U,*.V, 1=*.yuv, 2=*.ppm */
867         /* number of frames (必須自己修改)*/
0           /* number of first frame */
00:00:00:00 /* timecode of first frame */
12          /* N (# of frames in GOP) */
3           /* M (I/P frame distance) */
1           /* ISO/IEC 11172-2 stream */
0           /* 0:frame pictures, 1:field pictures */
352         /* horizontal_size */
240         /* vertical_size */
12          /* aspect_ratio_information 8=CCIR601 625 line, 9=CCIR601 525 line (?)*/
4           /* frame_rate_code 1=23.976, 2=24, 3=25, 4=29.97, 5=30 frames/sec. */
1500000.0 /* bit_rate (bits/s) */
20          /* vbv_buffer_size (in multiples of 16 kbit) */
0           /* low_delay  */
1           /* constrained_parameters_flag */
4           /* Profile ID: Simple = 5, Main = 4, SNR = 3, Spatial = 2, High = 1 */
8           /* Level ID:   Low = 10, Main = 8, High 1440 = 6, High = 4          */
1           /* progressive_sequence */
1           /* chroma_format: 1=4:2:0, 2=4:2:2, 3=4:4:4 */
1           /* video_format: 0=comp., 1=PAL, 2=NTSC, 3=SECAM, 4=MAC, 5=unspec. (?)*/
5           /* color_primaries */
5           /* transfer_characteristics */
5           /* matrix_coefficients */
352         /* display_horizontal_size */
240         /* display_vertical_size */
0           /* intra_dc_precision (0: 8 bit, 1: 9 bit, 2: 10 bit, 3: 11 bit */
0           /* top_field_first */
1 1 1       /* frame_pred_frame_dct (I P B) */
0 0 0       /* concealment_motion_vectors (I P B) */
0 0 0       /* q_scale_type  (I P B) */
0 0 0       /* intra_vlc_format (I P B)*/
0 0 0       /* alternate_scan (I P B) */
0           /* repeat_first_field */
1           /* progressive_frame */
0           /* P distance between complete intra slice refresh */
0           /* rate control: r (reaction parameter) */
0           /* rate control: avg_act (initial average activity) */
0           /* rate control: Xi (initial I frame global complexity measure) */
0           /* rate control: Xp (initial P frame global complexity measure) */
0           /* rate control: Xb (initial B frame global complexity measure) */
0           /* rate control: d0i (initial I frame virtual buffer fullness) */
0           /* rate control: d0p (initial P frame virtual buffer fullness) */
0           /* rate control: d0b (initial B frame virtual buffer fullness) */
2 2 11 11 /* P:  forw_hor_f_code forw_vert_f_code search_width/height */
```

(f)

Figure 3.9 The process of the proposed active covert communication method. (a) An initial web page with a stego-video displayed on the browser. (b) A replay button on a pop-up menu. (c) A dialog in which a user key can be inputted. (d) A dialog which can select the saving location of extracted secret messages. (e) The extracted secret messages on the desktop. (f) The content of the extracted secret messages. (continued)

3.6 Summary and Discussions

In this chapter, an active covert communication method that can be carried out on a web page with an ActiveX program has been proposed. In this method, the security of the communication becomes better with the use of a user key to randomize secret messages and authentication signals. Authentication signals of secret messages not only help us detect transmission errors over the public network but also find out any illicit tampering of the cover media or secret messages.

If the given user key is wrong, the extracted secret messages and the extracted authentication signals will also be incorrect. That is, the recalculated authentication signals of the extracted secret messages will not be the same as the extracted ones. In this situation, the extracted secret messages will be discarded and malicious users can just get nothing.

Chapter 4

Active Authentication of MPEG Videos

4.1 Introduction

With the advance of computer networks, the data transmission rate on networks is getting higher. More and more videos are transmitted on public networks. Since these MPEG videos are exposed on the Internet, illicit users might want to intercept and modify them for deceiving the receiver. Thus, the verification of the fidelity of suspicious MPEG videos is necessary. The scheme proposed in this study is executed on a web page and can authenticate on-line MPEG videos to generate verification reports.

In Section 4.2, a review of an authentication method for I, P and B frames of MPEG videos is introduced. Then in Section 4.3, the proposed active authentication method for MPEG videos on web pages and flowcharts of the processes are described. Finally, experimental results and some discussions are given.

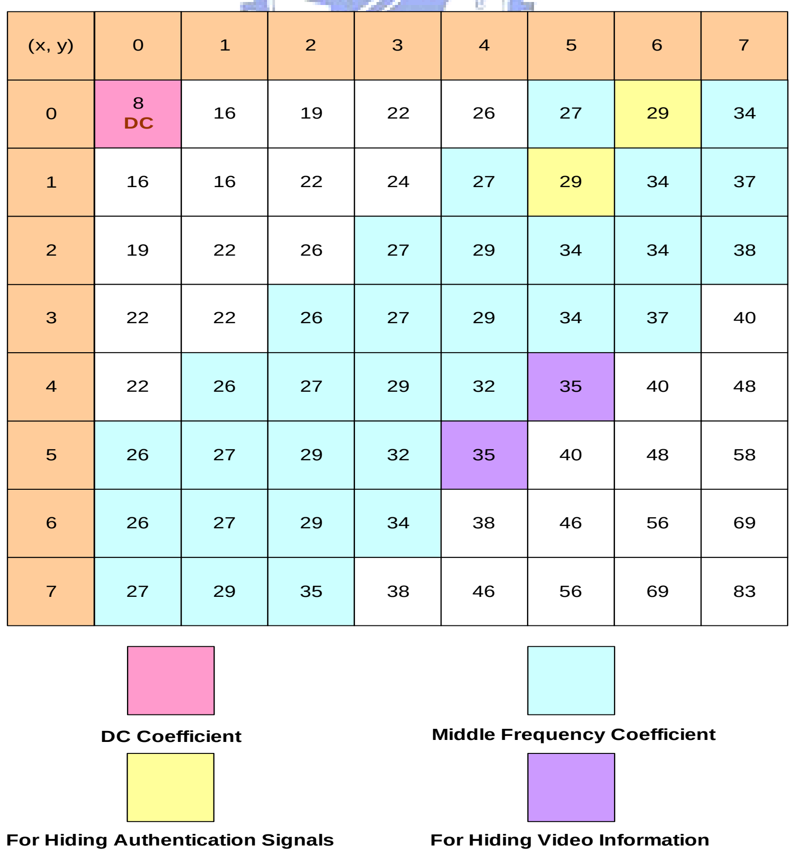
4.2 Review of An Authentication Method for MPEG Videos

In this section, two authentication signal hiding methods for different frames of

MPEG videos are reviewed. In Section 4.2.1, a process for hiding authentication signals in I frames is introduced and a process for P and B frames is described in Section 4.2.2.

4.2.1 Process for Hiding Authentication Signals in I Frames

In the reviewed method, two different DCT coefficients with the same quantization step size in the luminance block of intra-coded frames are chosen as a pair to hide an authentication signal. There need two pairs of DCT coefficients for hiding authentication signals. One pair is for hiding random number authentication signals, and the other is for hiding video information, including the number of P and B frames in a GOP and the index of a GOP.



(x, y)	0	1	2	3	4	5	6	7
0	8 DC	16	19	22	26	27	29	34
1	16	16	22	24	27	29	34	37
2	19	22	26	27	29	34	34	38
3	22	22	26	27	29	34	37	40
4	22	26	27	29	32	35	40	48
5	26	27	29	32	35	40	48	58
6	26	27	29	34	38	46	56	69
7	27	29	35	38	46	56	69	83

DC Coefficient
Middle Frequency Coefficient
For Hiding Authentication Signals
For Hiding Video Information

Figure 4. 1 An illustration of a DCT quantization table.

The method for hiding a pair of two coefficients is to adjust their relative values according to the hidden data. Because of the quantization step size of the selected frequency-domain coefficients are the same, hidden authentication signals may have the capability against image recompression. In order to reduce the probability of erroneous extraction of hidden bits, the number of inter-coded frames and the index are duplicated as many times as possible before the embedding process. A detailed algorithm is described as follows.

***Algorithm* 1:** Hiding authentication signals in intra-coded macroblocks.

***Input*:** an index of i-th GOP G_i, the number of inter-coded frames in (i-1)-th GOP N_i, a user key K, and a macroblock M.

***Output*:** a protected macroblock M'.

***Steps*:**

1. Transform G_i and N_i into a binary form $(g_1\ g_2\ \ldots\ g_p)_2$ and $(n_1\ n_2\ \ldots\ n_q)_2$ and duplicate them into as many copies as possible.
2. Combine each position of a luminance block and K to generate a random number authentication signal A.
3. Use one pair of DCT coefficients C_1 at (5, 1) and C_2 at (6, 0) in the block coefficient matrix to hide an authentication signal S according the following rules.

    I. *If* $C_1 - C_2 \leq T_1$:

    - i. *if* S *is odd, then set* $C_1 > C_2$ *and* $|C_1 - C_2| = T_1$;
    - ii. *if* S *is even, then set* $C_1 < C_2$ *and* $|C_1 - C_2| = T_1$.

    II. *If* $C_1 - C_2 > T_1$:

    - i. *if* S *is odd, then set* $C_1 = (C_1 + C_2)/2 + T_1/2$ *and* $C_2 = (C_1 + C_2)/2 - T_1/2$;
    - ii. *if* S *is even, then set* $C_1 = (C_1 + C_2)/2 - T_1/2$ *and* $C_2 = (C_1 + C_2)/2 + T_1/2$.

4. Use another pair of DCT coefficients C_3 at (4, 5) and C_4 at (5, 4) to hide a bit b of G_i and N_i according to the following formulas.

   I. *If* $C_3 – C_4 \leq T_1$:

      i. *if* b *is odd, then set* $C_3 > C_4$ *and* $|C_3 – C_4| = T_1$;

      ii. *if* b *is even, then set* $C_3 < C_4$ *and* $|C_3 – C_4| = T_1$.

   II. *If* $C_1 – C_2 > T_1$:

      i. *if* b *is odd, then set* $C_3 = (C_3 + C_4)/2 + T_1/2$ *and* $C_4 = (C_3 + C_4)/2 – T_1/2$;

      ii. *if* b *is even, then set* $C_3 = (C_3 + C_4)/2 – T_1/2$ *and* $C_4 = (C_3 + C_4)/2 + T_1/2$.

Notice that T_1 is a threshold value of a tradeoff between the quality of MPEG videos and robustness. The lower T_1 is, the higher quality of MPEG videos is retained and less robustness can be kept. An illustration of the process is shown in Figure 4.2.

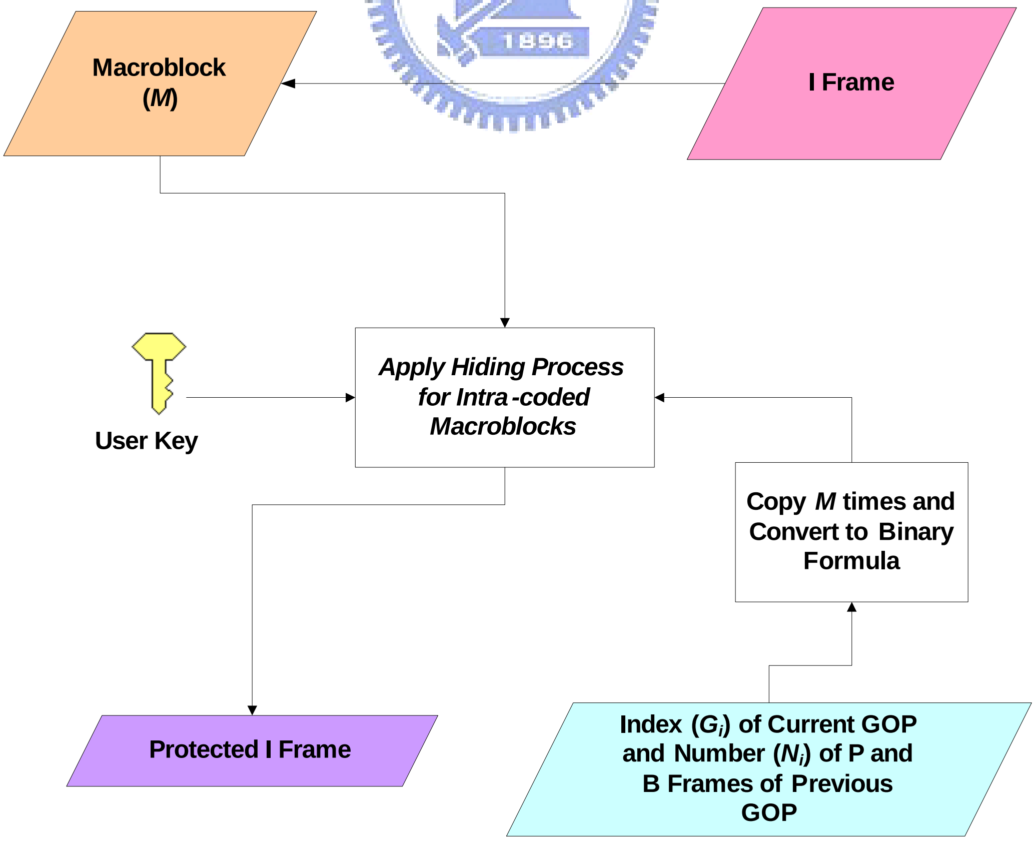

Macroblock
(*M*)
I Frame
User Key
Apply Hiding Process for Intra-coded Macroblocks
Copy *M* times and Convert to Binary Formula
Protected I Frame
Index (G_i) of Current GOP and Number (N_i) of P and B Frames of Previous GOP

Figure 4. 2 An illustration of the process for hiding authentication signals in I frames.

4.2.2 Process for Hiding Authentication Signals in P and B Frames

Since P and B frames are inter-coded frames in MPEG videos, a lot of motion vectors are utilized for motion compensation prediction. These vectors should be utilized efficiently for hiding authentication signals for checking the fidelity of MPEG videos. Two proper non-overlapping adjacent macroblocks are selected to hide an authentication signal and the detailed algorithm is described in the following.

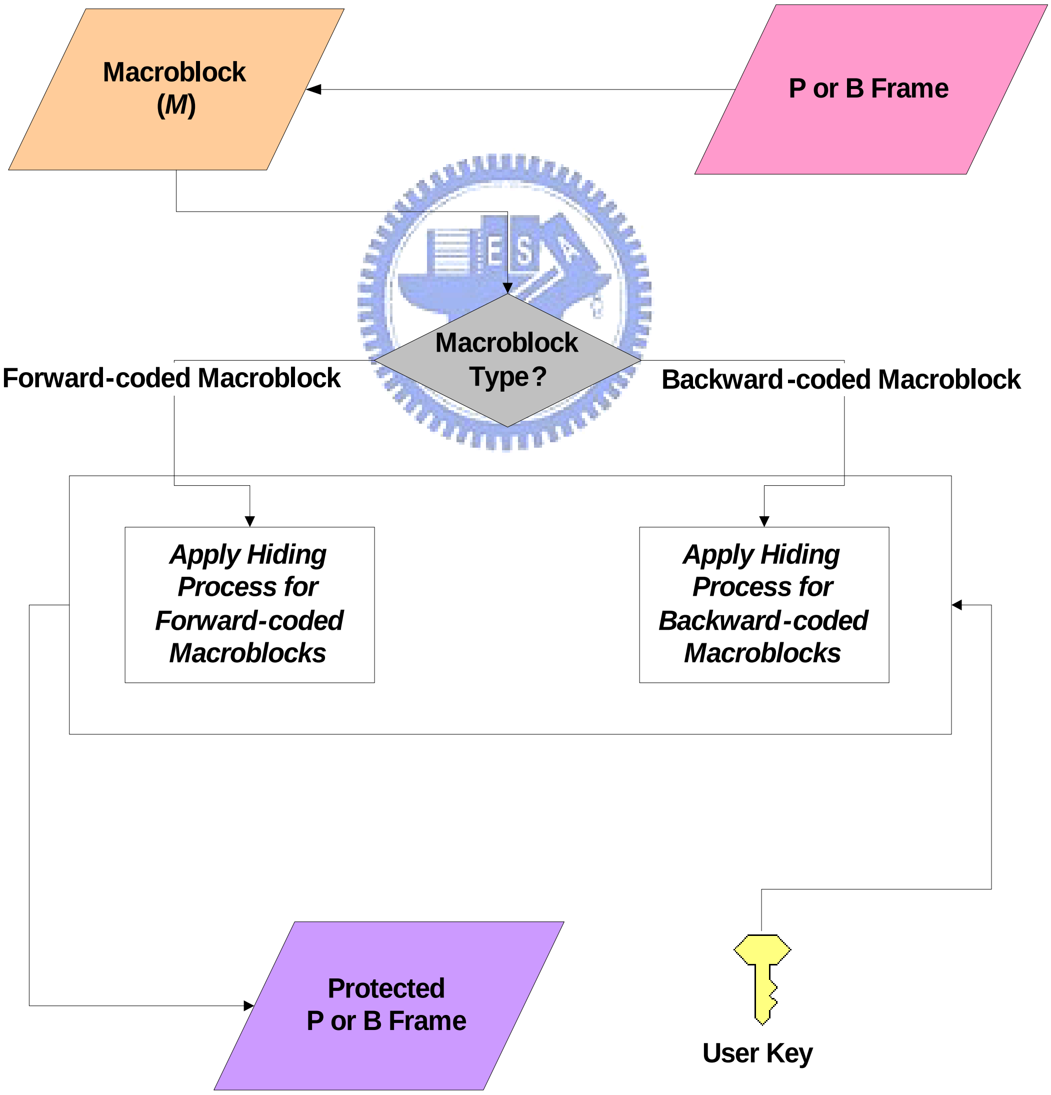

Macroblock
(*M*)
P or B Frame
Macroblock
Type?
Forward-coded Macroblock
Backward-coded Macroblock
Apply Hiding Process for Forward-coded Macroblocks
Apply Hiding Process for Backward-coded Macroblocks
Protected
P or B Frame
User Key

Figure 4. 3 A flowchart of the process of hiding authentication signals in P and B frames.

***Algorithm* 2:** Hiding authentication signals in inter-coded macroblocks.

***Input*:** a user key K, and a P or B frame F.

***Output*:** a protected macroblock M'.

Steps:

1. If F is a P frame, then go to step I; otherwise step II:

   I. Select horizontal motion vectors (H_i, H_j) and vertical ones (V_i, V_j) as two candidates of two non-overlapping adjacent macroblocks (MB$_i$, MB$_j$) in forward-coded macroblocks and use following rules to decide if they are proper or not.

      i. If $H_i > T_2$, $H_j > T_2$ and $|H_i - H_j| \leq 1$, then regard them as a proper pair for hiding an authentication signal and denoted them as (H_1, H_2); otherwise go to step ii.

      ii. If $V_i > T_2$, $V_j > T_2$ and $|V_i - V_j| \leq 1$, then regard them as a proper pair for hiding an authentication signal and denoted them as (V_1, V_2); otherwise go to step iii.

      iii. If both of above conditions are false, then the input macroblock is not proper for hiding authentication signals.

   II. Select horizontal vectors (H_i, H_j) and (H_i', H_j') for forward-coded macroblocks and backward-coded ones and vertical vectors (V_i, V_j) and (V_i', V_j') for forward-coded macroblocks and backward-coded ones. Then use identical rules described above to select a proper pair to hide an authentication signal. If (H_i, H_j) or (H_i', H_j') is selected, then denote it as (H_1, H_2). If (V_i, V_j) or (V_i', V_j') is selected, then denote them as (V_1, V_2).

2. Combine the position of the selected pair of macroblocks and K to generate a random number authentication signal A and use the following formulas to hide it.

   I. *If* the selected vector is (H_1, H_2):

i. *if A is odd, then set* $H_1 > H_2$ *and* $|H_1 - H_2| = 1$;

ii. *if A is even, then set* $H_1 < H_2$ *and* $|H_1 - H_2| = 1$.

II. *If* the selected vector is (V_1, V_2):

i. *if A is odd, then set* $V_1 > V_2$ *and* $|V_1 - V_2| = 1$;

ii. *if A is even, then set* $V_1 < V_2$ *and* $|V_1 - V_2| = 1$.

The threshold T_2 is a pre-defined value and an illustration of the process is shown in Figure 4.3.

4.3 Proposed Active Authentication Method for MPEG Videos

The platform for the proposed active authentication method for MPEG videos is a web page with an ActiveX program. This program includes an active video player, a clip of MPEG videos, and an active agent.

An example of the application is that if a superior wants to deliver messages, which cannot be completely explained by text files, to his employees who work outside, the superior can use a digital video recorder or a digital camera to record a period of video. The video, including work assignments from the superior, in which authentication signals can be hidden, are put on a web page. The employees just have to browse a web page and see these videos to check the assignments.

Because the video needs to be transmitted through the public network, illicit users may intercept the video and modify it for misrepresentation. In order to verify the fidelity of it, an active authentication method is proposed in this study and described in this Section. The employees can use the proposed system to authenticate the video without the need of installing authentication programs.

In Section 4.3.1, an embedding process to implement the proposed approach is introduced. Then, in Section 4.3.2, a process for extracting authentication signals is proposed and different types of attack are presented.

4.3.1 Process for Embedding Authentication Signals

First, MPEG videos with work assignments are processed with variable length decoding and the frequency-domain data of each frame can be obtained.

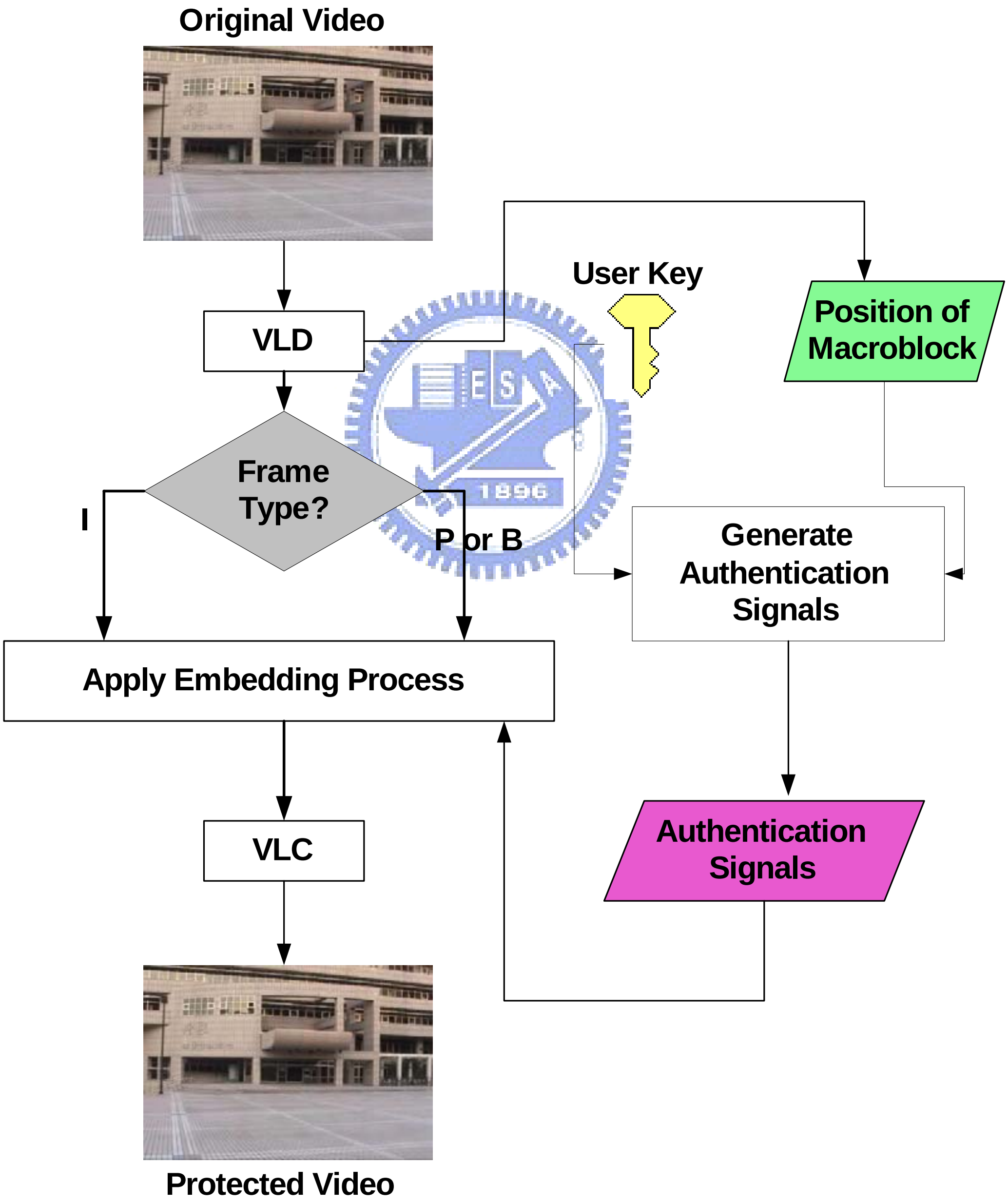


Figure 4. 4 A flowchart of the process of embedding authentication signals into MPEG videos.

After the decoding process is completed, an input user key together with certain related information of the macroblock in each frame is used to generate authentication signals. The signals are hidden in an MPEG video to produce a protected video. A flowchart of the entire process is shown in Figure 4.4.

4.3.2 Process for Extracting Authentication Signals

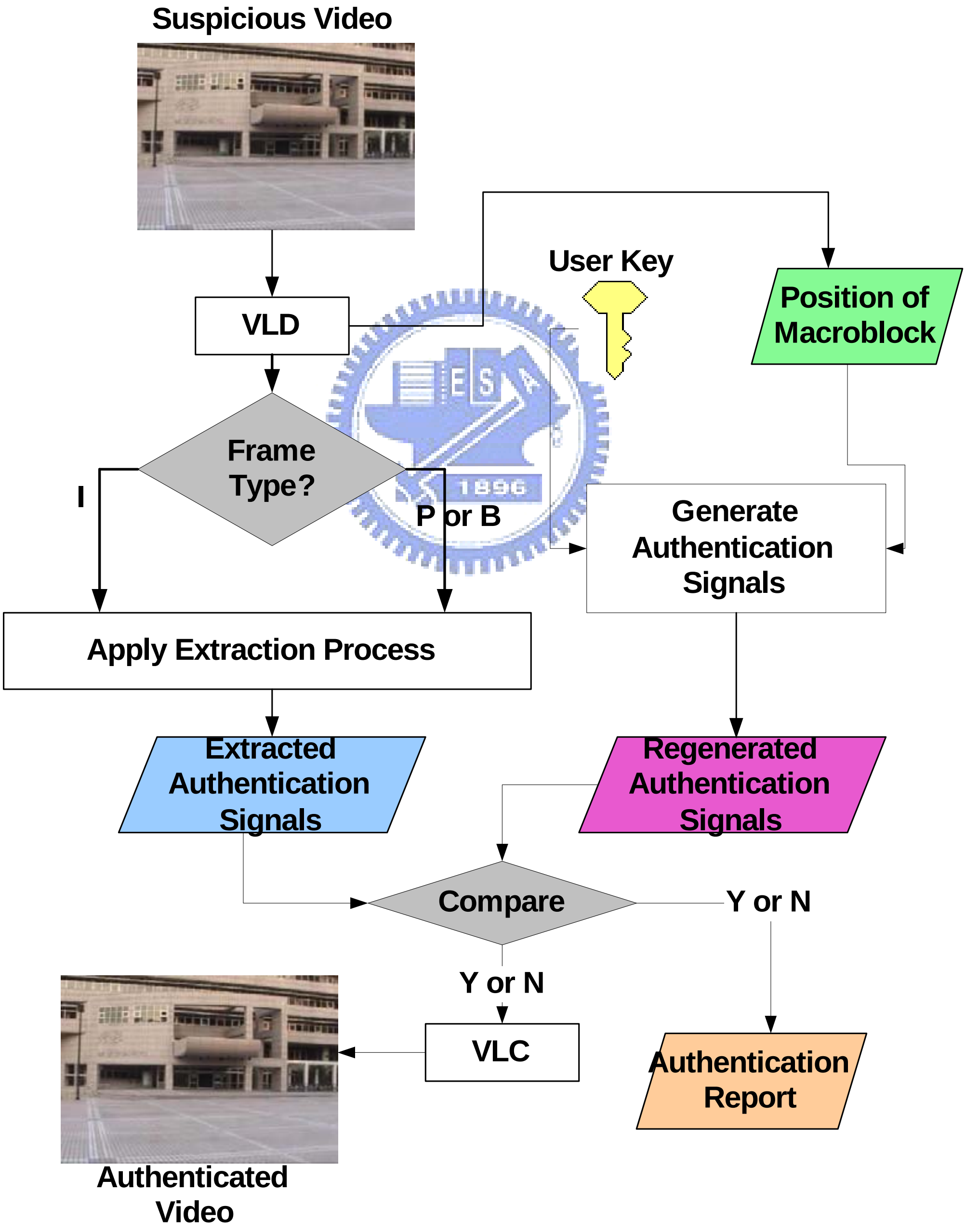


Figure 4. 5 A flowchart of the process of extracting authentication signals.

When the MPEG video is to be authenticated, a user also has to provide an authentic key to regenerate the authentication signals. After comparing the extracted authentication signals with the regenerated ones, the proposed system can decide if the video has been under attack. An extraction process is shown in Figure 4.5.

Different types of attacks presented in an authentication report are described in the following.

1. *Cropping*: This type of attack means that some frames are removed from the MPEG video. In this situation, the difference between two extracted successive indices does not equal one and each frame is authentic. If the difference of indices equals one and another difference between the extracted number of inter-coded frames and the counted number of inter-coded frames in successive GOPs does not equal zero, it is decided that the video has been under a cropping attack.
2. *Replacement*: This type of attack means that some frames are replaced by unauthentic frames in the MPEG video. In this situation, the difference of two extracted successive indices does not equal one and there are several unauthentic frames.
3. *Insertion*: This type of attack means that there are some redundant authentic frames in the MPEG video. In this kind of attack, the difference of two extracted successive indices equals one and there are some unauthentic frames.
4. *Spatial tampering*: This type of attack means that there are some unauthentic macroblocks in the frame.

After creating a protected MPEG video, it is put on a web page for users to see. When a user opens a web page, the proposed system can extract active agents to authenticate the video and generate an authentication report to show if the video is authentic.

When a suspicious video is detected, the user should request the superior to retransmit the correct one. An illustration of the active authentication method is shown in Figure 4.6.

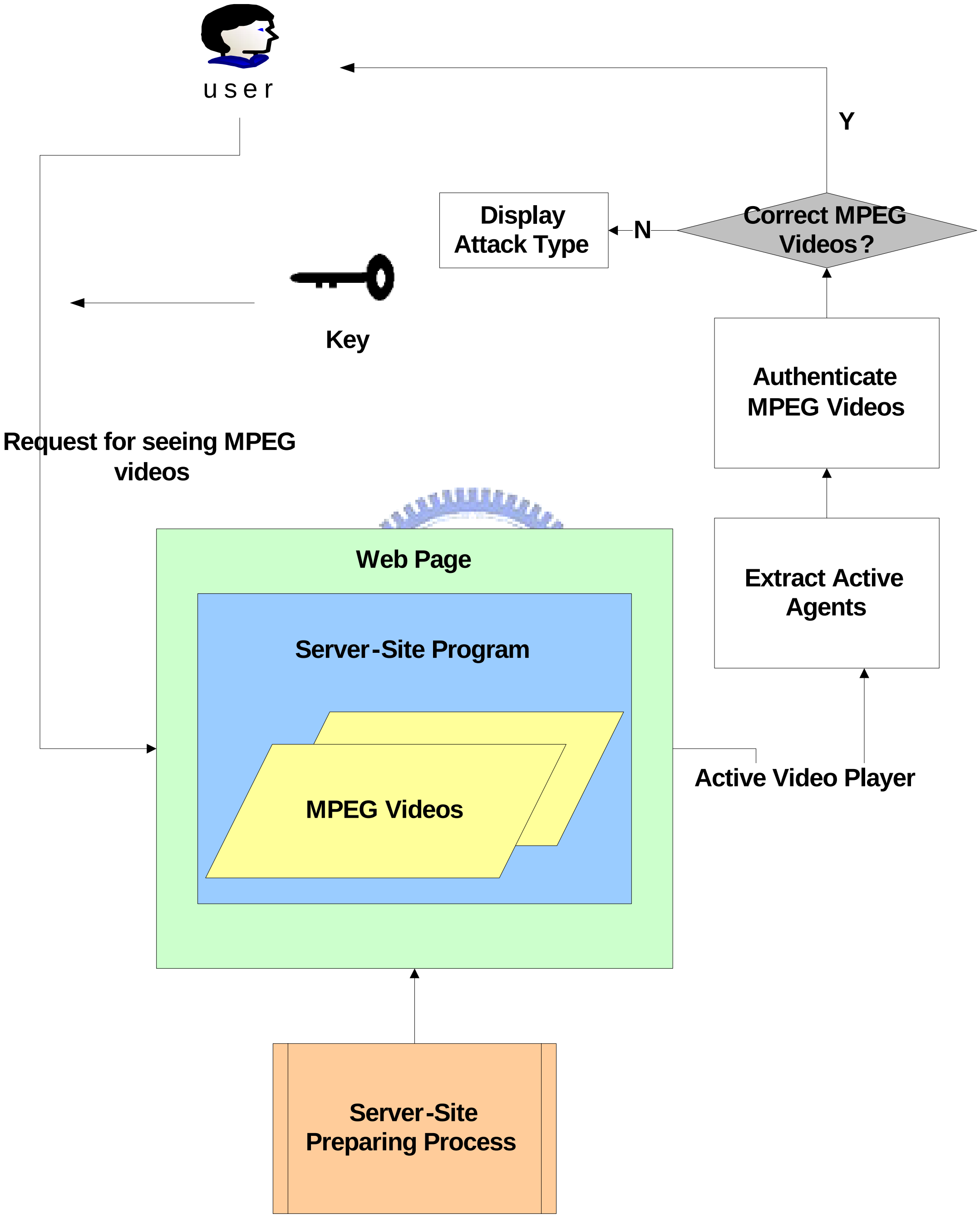
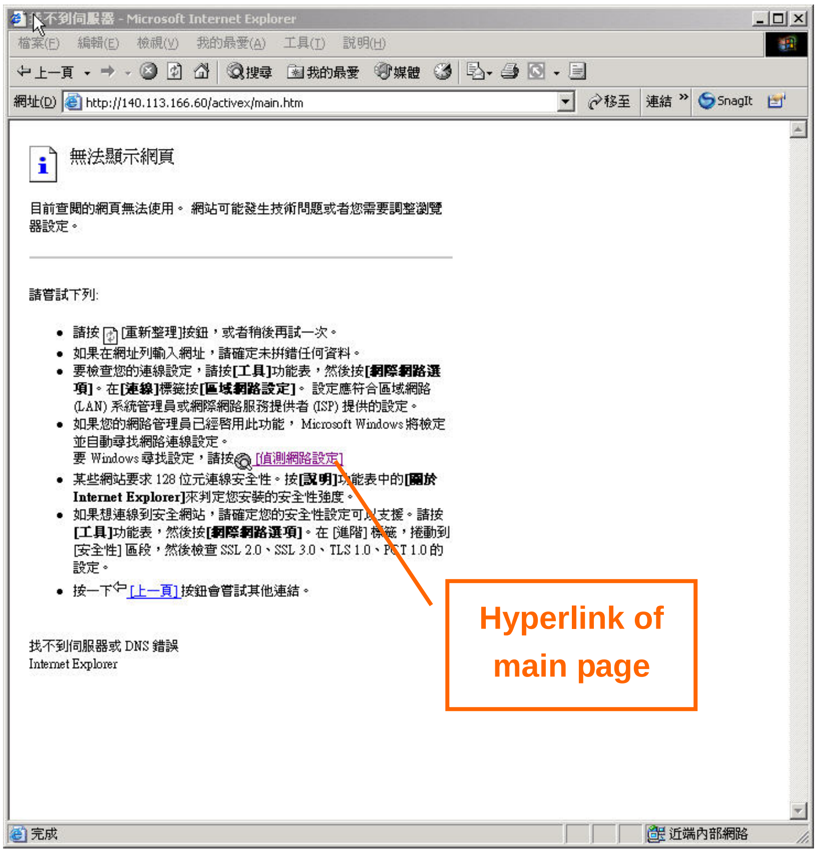


Figure 4. 6 A flowchart of the process of the active authentication method.

4.4 Experimental Results

In our experiments, a protected video with authentication signals is put on a web page for people to see. Before a user get into the main page in Figure 4.7(b), a web page in Figure 4.7(a) as a camouflage will be displayed first. Only those who know where the hyperlink of the main page is can browse the main page. In order to prevent imprudent users from accessing the proposed system, keying in a login password is necessary for authorized users. According to the input user key, the proposed system can extract active agents and authenticate videos which the user is seeing before generating an authentication report. A video list on the left side of the proposed system is displayed and different kinds of attacks are presented in Figure 4.7(c)-(f).


找不到伺服器 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 媒體
移至 連結 SnagIt
完成
近端內部網路

網址(D) http://140.113.166.60/activex/main.htm

無法顯示網頁

目前查閱的網頁無法使用。 網站可能發生技術問題或者您需要調整瀏覽器設定。

請嘗試下列:

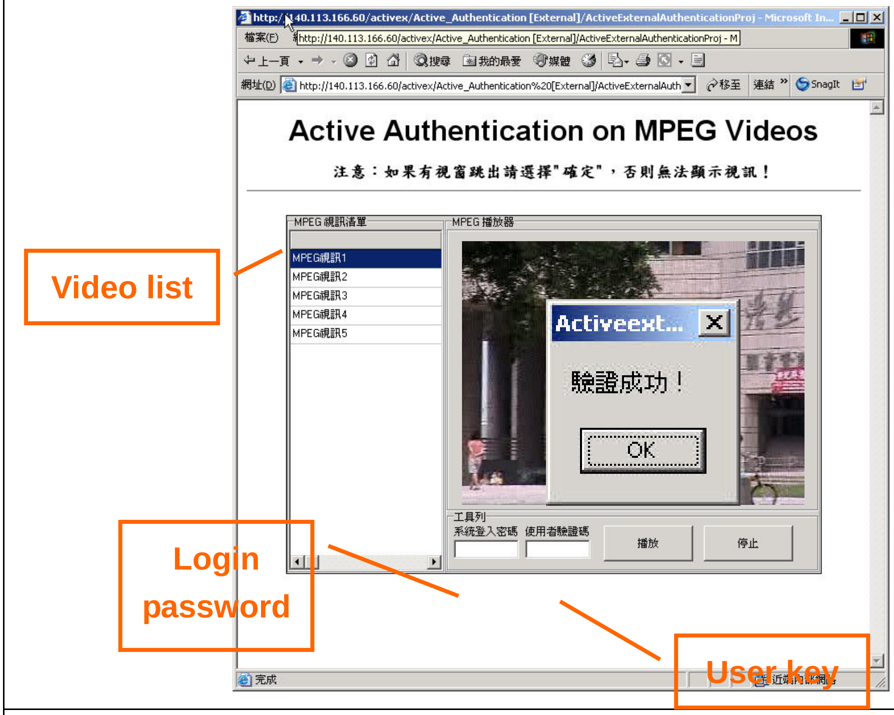
- 請按 [重新整理]按鈕，或者稍後再試一次。
- 如果在網址列輸入網址，請確定未拼錯任何資料。
- 要檢查您的連線設定，請按**[工具]**功能表，然後按**[網際網路選項]**。在**[連線]**標籤按**[區域網路設定]**。 設定應符合區域網路 (LAN) 系統管理員或網際網路服務提供者 (ISP) 提供的設定。
- 如果您的網路管理員已經啓用此功能， Microsoft Windows 將檢定並自動尋找網路連線設定。
  要 Windows 尋找設定，請按 [偵測網路設定]
- 某些網站要求 128 位元連線安全性。按**[說明]**功能表中的**[關於 Internet Explorer]**來判定您安裝的安全性強度。
- 如果想連線到安全網站，請確定您的安全性設定可以支援。請按**[工具]**功能表，然後按**[網際網路選項]**。在 [進階] 標籤，捲動到 [安全性] 區段，然後檢查 SSL 2.0、SSL 3.0、TLS 1.0、PCT 1.0 的設定。
- 按一下 [上一頁] 按鈕會嘗試其他連結。

找不到伺服器或 DNS 錯誤
Internet Explorer

Hyperlink of main page

(a)

Figure 4.7 An experimental result. (a) A web page as a camouflage. (b) MPEG video 1 which is authentic. (c) MPEG video 2 which has cropping attack. (d) MPEG video 3 which has insertion attack. (e) MPEG video 4 which has replacement attack. (f) MPEG video 4 which has spatial attack. (continued)



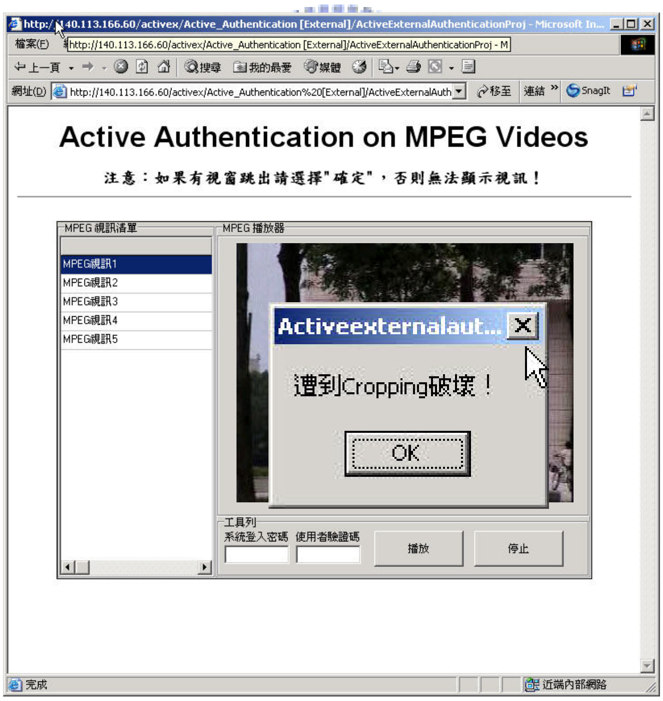
Active Authentication on MPEG Videos

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

驗證成功！

http://140.113.166.60/activex/Active_Authentication [External]/ActiveExternalAuthenticationProj - Microsoft In...
http://140.113.166.60/activex/Active_Authentication%20[External]/ActiveExternalAuth
Video list
Login password
User key
MPEG 視訊清單
MPEG視訊1
MPEG視訊2
MPEG視訊3
MPEG視訊4
MPEG視訊5
MPEG 播放器
Activeext...
OK
工具列
系統登入密碼
使用者驗證碼
播放
停止
完成

(b)



Active Authentication on MPEG Videos

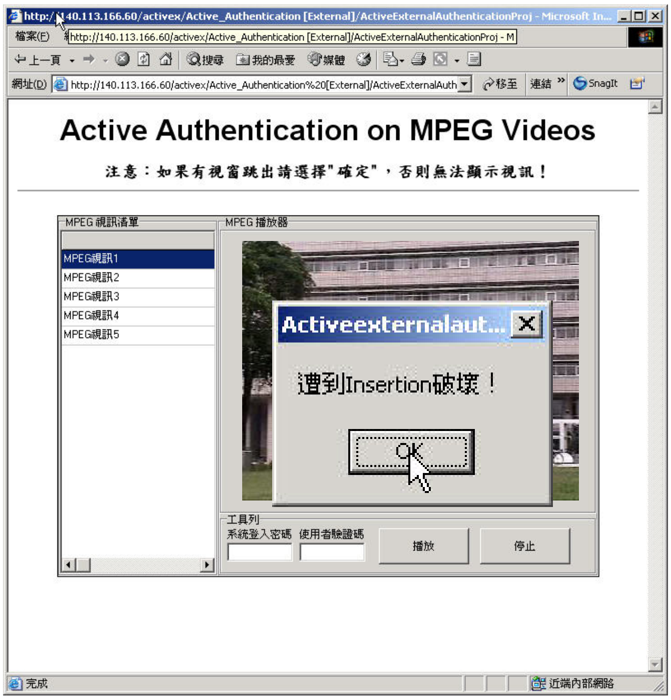
注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

遭到Cropping破壞！

http://140.113.166.60/activex/Active_Authentication [External]/ActiveExternalAuthenticationProj - Microsoft In...
http://140.113.166.60/activex/Active_Authentication%20[External]/ActiveExternalAuth
MPEG 視訊清單
MPEG視訊1
MPEG視訊2
MPEG視訊3
MPEG視訊4
MPEG視訊5
MPEG 播放器
Activeexternalaut...
OK
工具列
系統登入密碼
使用者驗證碼
播放
停止
完成
近端內部網路

(c)

Figure 4.7 An experimental result. (a) A web page as camouflage. (b) MPEG video 1 which is authentic. (c) MPEG video 2 which has cropping attack. (d) MPEG video 3 which has insertion attack. (e) MPEG video 4 which has replacement attack. (f) MPEG video 4 which has spatial attack. (continued)



http://140.113.166.60/activex/Active_Authentication [External]/ActiveExternalAuthenticationProj - Microsoft In...

Active Authentication on MPEG Videos

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

MPEG 視訊清單

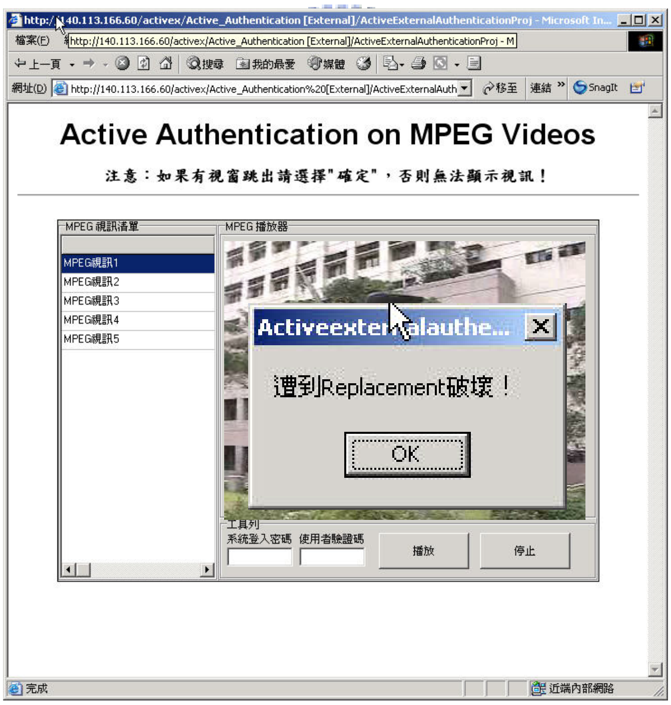
- MPEG視訊1
- MPEG視訊2
- MPEG視訊3
- MPEG視訊4
- MPEG視訊5

MPEG 播放器

Activeexternalaut...

遭到Insertion破壞！

(d)



http://140.113.166.60/activex/Active_Authentication [External]/ActiveExternalAuthenticationProj - Microsoft In...

Active Authentication on MPEG Videos

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

MPEG 視訊清單

- MPEG視訊1
- MPEG視訊2
- MPEG視訊3
- MPEG視訊4
- MPEG視訊5

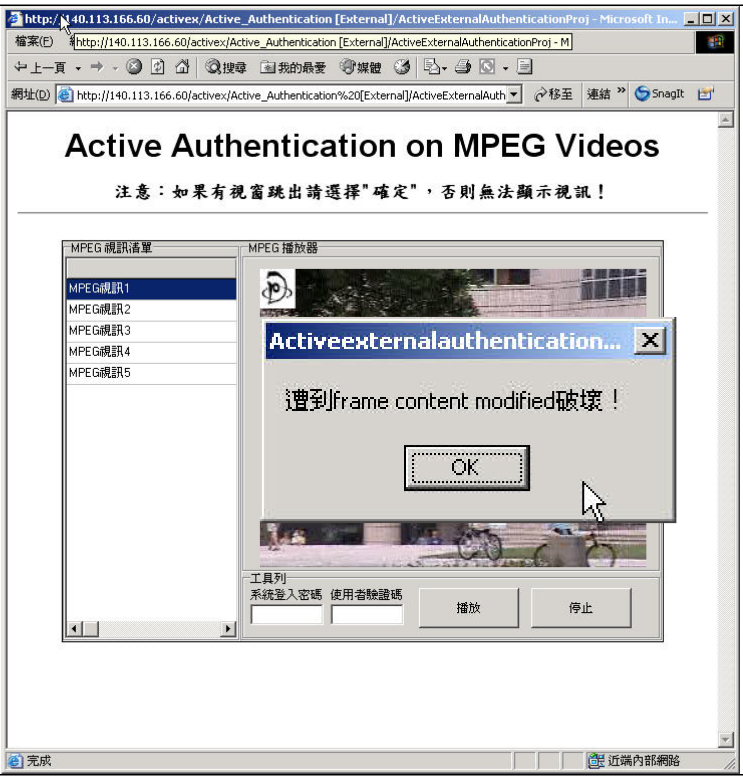
MPEG 播放器

Activeexternalauthe...

遭到Replacement破壞！

(e)

Figure 4.7 An experimental result. (a) A web page as camouflage. (b) MPEG video 1 which is authentic. (c) MPEG video 2 which has cropping attack. (d) MPEG video 3 which has insertion attack. (e) MPEG video 4 which has replacement attack. (f) MPEG video 4 which has spatial attack. (continued)



http://140.113.166.60/activex/Active_Authentication [External]/ActiveExternalAuthenticationProj - Microsoft In...

http://140.113.166.60/activex/Active_Authentication%20[External]/ActiveExternalAuth

Active Authentication on MPEG Videos

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

Activeexternalauthentication...

遭到frame content modified破壞！

(f)

Figure 4.7 (a) A web page as camouflage. (b) MPEG video 1 which is authentic. (c) MPEG video 2 which has cropping attack. (d) MPEG video 3 which has insertion attack. (e) MPEG video 4 which has replacement attack. (f) MPEG video 4 which has spatial attack. (continued)

4.5 Summary and Discussions

In this chapter, an active authentication method has been proposed and some experimental results presented. Both temporal and spatial tamperings can be detected by the proposed method through the use of a web page. With the use of a user key, the user may be sure about whether the extracted authentication signals are forged or not. If the provided user key is wrong, the user also gets a wrong authentication report.

In order to reduce the probability of the error verification of MPEG videos, the hidden authentication signals are duplicated as many times as possible and the generation of authentication signals utilizes a user key together with related information of frames.

Chapter 5

Active Copyright Protection of MPEG Videos

5.1 Introduction

In the current century of technology, data are digitized and transmitted on the public network. Although many people are glad to share their MPEG videos on the Internet, they still want to protect their ownership and copyright of the videos. In order to take this problem into consideration, an active watermarking technique for copyright protection of MPEG videos is proposed. In this study, both a visible watermarking technique and an invisible one are utilized for protecting the copyright of MPEG videos.

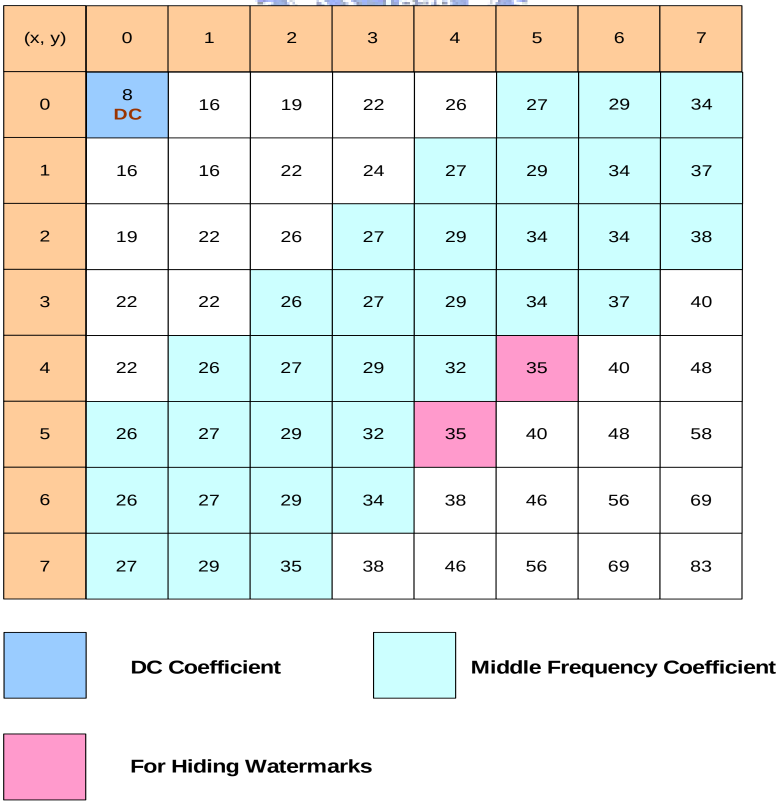
In Section 5.2, a review of a watermark hiding method for MPEG videos is made and this method is utilized in Sections 5.3 and Section 5.4. In Section 5.3, a method for transforming removable visible watermarks actively into invisible ones is proposed. In Section 5.4, a method for transforming invisible watermarks actively into visible ones is proposed. Finally, some experimental results and a summary are given.

5.2 Review of A Watermark Hiding Method for MPEG Videos

In this section, processes for hiding watermarks in I, and in P and B frames proposed in Chen and Tsai [10] are reviewed in Section 5.2.1 and Section 5.2.2, respectively. Watermarks are considered as binary images and each pixel in a watermark is referred to be white or black according to its binary value 0 or 1, respectively.

5.2.1 Process for Hiding Watermarks in I Frames

In the method proposed by Chen and Tsai [10], for each luminance block in macroblocks, its DC value is modified according to the grayscale value of an input pixel of a binary watermark. If the binary value is 1, it means that the current pixel is black and the DC value should be decreased; otherwise the DC value is kept unchanged. An illustration of the position of the DC value is shown in Figure 5.1 and a detailed algorithm is described in the following.



(x, y)	0	1	2	3	4	5	6	7
0	8 DC	16	19	22	26	27	29	34
1	16	16	22	24	27	29	34	37
2	19	22	26	27	29	34	34	38
3	22	22	26	27	29	34	37	40
4	22	26	27	29	32	35	40	48
5	26	27	29	32	35	40	48	58
6	26	27	29	34	38	46	56	69
7	27	29	35	38	46	56	69	83

🟦 DC Coefficient

🟩 Middle Frequency Coefficient

🟪 For Hiding Watermarks

Figure 5. 1 An illustration of the position of the DC value.

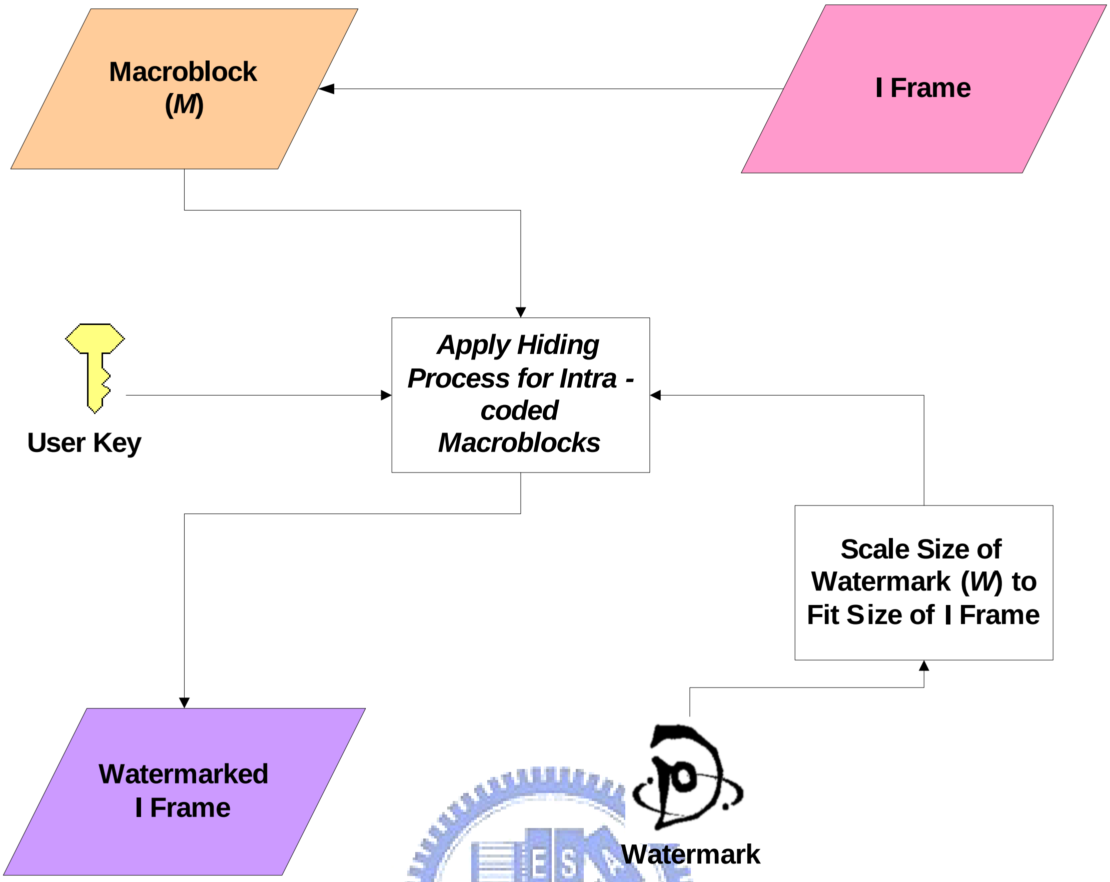

Macroblock
(M)
I Frame
Apply Hiding Process for Intra - coded Macroblocks
User Key
Scale Size of Watermark (W) to Fit Size of I Frame
Watermarked I Frame
Watermark

Figure 5. 2 A flowchart of the process for hiding watermarks in I frames.

***Algorithm* 1:** Hiding watermarks in intra-coded macroblocks.

***Input*:** a user key *K*, a watermark *W*, an I frame *F*, and a macroblock *M* .

***Output*:** a watermarked macroblock *M'*.

***Steps*:**

1. Modify the height and the width of *W* to make its shape similar to that of *F*.
2. Combine *K* and the position of the current luminance block to generate two binary signals $S = (s_1\ s_2)_2$ for black pixels and $S' = (s_1'\ s_2')_2$ for white pixels.
3. Select a pair of DCT coefficients (C_1, C_2) at positions (5, 4) and (4, 5) are shown in Figure 5.1 for recording the watermark.
4. Get the DC value *L* of an input luminance block and the corresponding pixel *P* of *W*, and perform the following steps to hide a pixel of *W*:

I. If $P = 1$, then set $L = L – T$ and use the LSB data hiding technique to replace the LSB of C_1 by s_1 and the LSB of C_2 by s_2, where T is a pre-selected threshold value.

II. If $P = 0$, then keep L unchanged and use the LSB data hiding technique to replace the LSB of C_1 by s_1’ and the LSB of C_2 by s_2’.

The threshold value T is pre-selected in such a way as to make the luminance of the current block darker. A flowchart of the process for hiding watermarks in I frames is shown in Figure 5.2.

5.2.2 Process for Hiding Watermarks in P and B Frames

P or B frames have two types of macroblocks, namely, intra-coded ones and inter-coded ones. The hiding process for intra-coded macroblocks is similar to the process for I frames, so only the process for inter-coded macroblocks is introduced in this section.

The *coded block pattern* (CBP) in the MPEG standard is used to record if the current block in a macroblock has been encoded in the MPEG bitstream or not. If the current bit of CBP is 1, it means that the corresponding block and the reference block have been encoded. On the contrary, if the bit is 0, the current block is not encoded in the MPEG bitstream. A detailed algorithm of the hiding process is described as follows.

***Algorithm* 2:** Hiding watermarks in inter-coded macroblocks.

***Input*:** a user key K, a watermark W, a P or B frame F, and a macroblock M.

***Output*:** a watermarked macroblock M’.

***Steps*:**

1. Obtain the current bit *b* of CBP of the corresponding luminance block. If *b* equals to 1, keep *b* unchanged. If *b* equals to 0 and the current frame is a B frame, set *b* set to be 1.
2. Modify the height and the width of *W* into a shape similar to that of *F*.
3. Combine *K* and the position of the current luminance block to generate two binary signals $S = (s_1\ s_2)_2$ for black pixels and $S' = (s_1'\ s_2')_2$ for white pixels.
4. Select a pair of DCT coefficients (C_1, C_2) at (5, 4) and (4, 5) are shown in Figure 5.1 for recording the watermark.

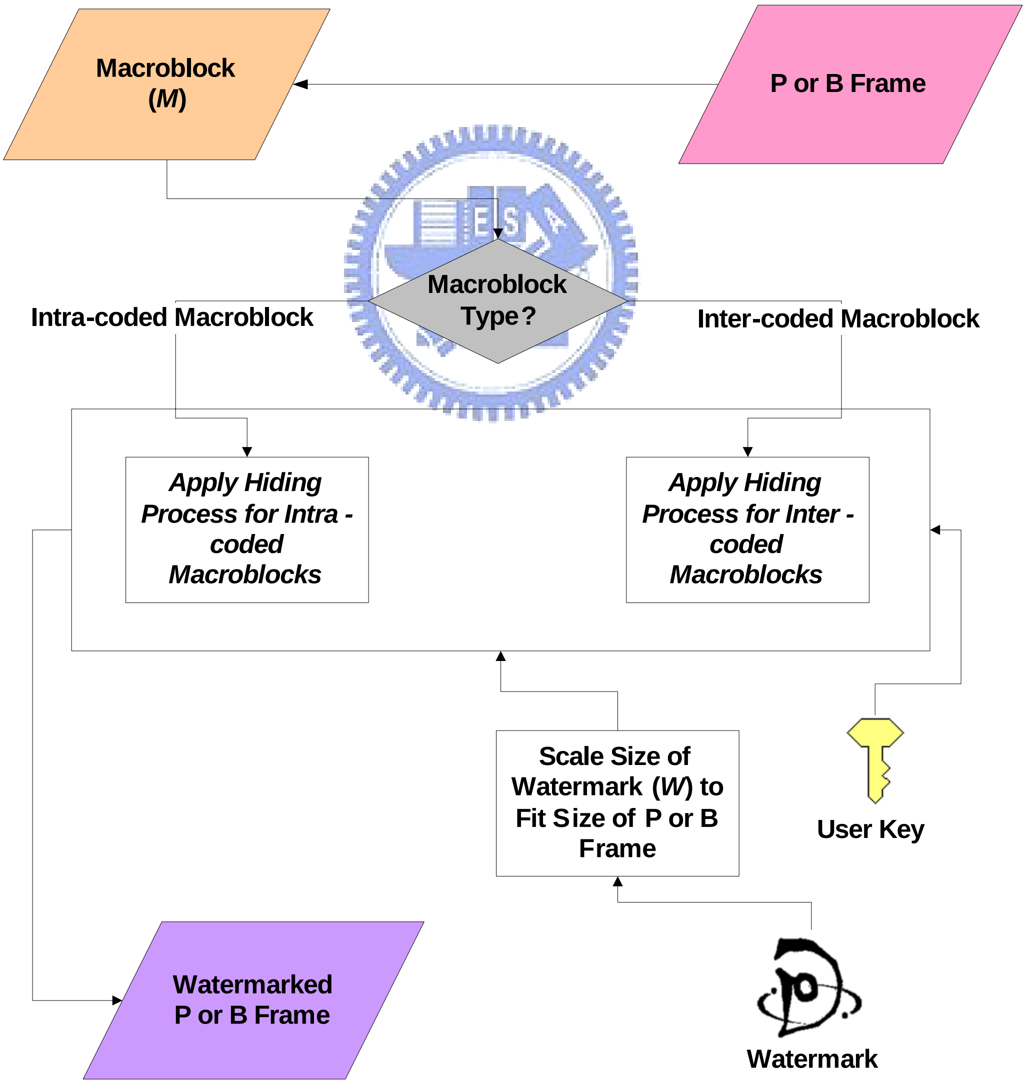

Macroblock
(*M*)
P or B Frame
Macroblock Type?
Intra-coded Macroblock
Inter-coded Macroblock
Apply Hiding Process for Intra - coded Macroblocks
Apply Hiding Process for Inter - coded Macroblocks
Scale Size of Watermark (*W*) to Fit Size of P or B Frame
User Key
Watermarked P or B Frame
Watermark

Figure 5. 3 A flowchart of the process for hiding watermarks in P and B frames.

5. Get the DC value L of an input luminance block and the corresponding pixel P of W, and perform the following steps to hide a pixel of W:

   I. If $P = 1$, then set $L = L - T$ and use the LSB data hiding technique to replace the LSB of C_1 by s_1 and the LSB of C_2 by s_2 where T is a pre-selected threshold value.

   II. If $P = 0$, then keep L unchanged and use the LSB data hiding technique to replace the LSB of C_1 by s_1' and the LSB of C_2 by s_2'.

The threshold value T is pre-selected in such a way as to make the luminance of the current block be darker. A flowchart of the process for hiding watermarks in P and B frames is displayed in Figure 5.3.

5.3 Proposed Method for Transforming Removable Visible Watermarks Actively to Invisible Ones

The platform for applying the proposed method is a personal computer. The environment for the method is a web page with an ActiveX program, including an active agent and an active video player.

Here is an application example. A multimedia provider puts MPEG videos with removable visible watermarks on the Internet for people to see. If a user wants to see a video *clearly* (i. e., without the annoying watermarks), an authentic key should be used. If the provided key is correct, the proposed system will extract the active agent and transform the visible watermarks into invisible ones. Then, clear videos will be displayed on the web page.

In Section 5.3.1, the proposed process for embedding removable visible watermarks is introduced. In Section 5.3.2, the proposed process for transforming removable visible watermarks into invisible ones is described.

5.3.1 Embedding Process for Removable Visible Watermarks

At the beginning of the proposed removable watermark embedding process, the video provider should input a user key and a watermark for each MPEG video to be publicized. After the video is processed with variable length decoding, the frequency-domain data of each of its frames can be obtained.

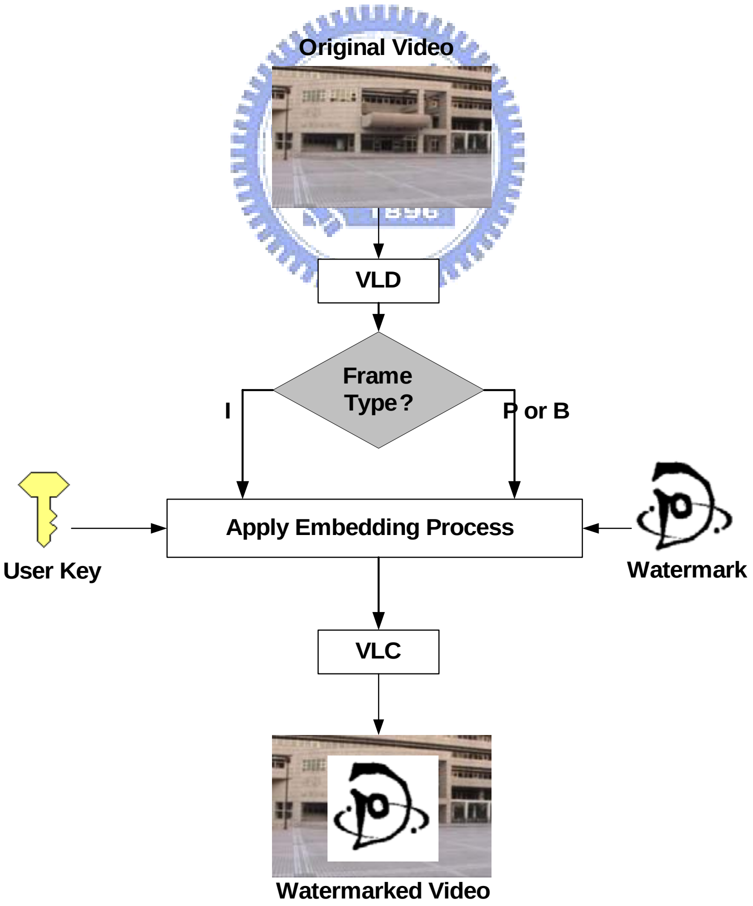


Figure 5. 4 A flowchart of the process for embedding removable visible watermarks.

With the use of the embedding process for intra-coded macroblocks and inter-coded ones, a watermark can be embedded in the video. A visible watermark can be displayed to claim the provider's ownership of the videos and also protects the copyright of them. An illustration of embedding removable visible watermarks is shown in Figure 5.4.

5.3.2 Transformation Process for Invisible Watermarks

At the beginning, a user can only see watermarked MPEG videos on a web page with an active video player.

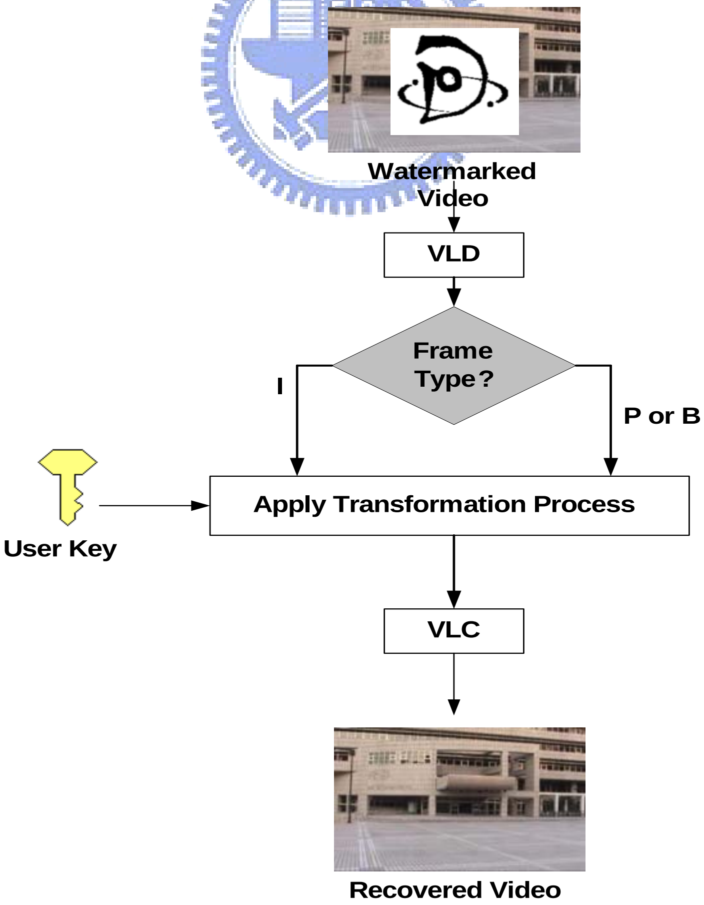


Figure 5. 5 A flowchart of the transforming process of invisible watermarks.

After an authentic key is provided, the proposed system uses this key together with related information of each block in frames to generate certain signals to decide if there is a watermark embedded in the current block. If the provided key is wrong, the regenerated signals will not equal to the extracted signals, so that removable visible watermarks cannot be removed. A flowchart of the transformation process of invisible watermarks is shown in Figure 5.5.

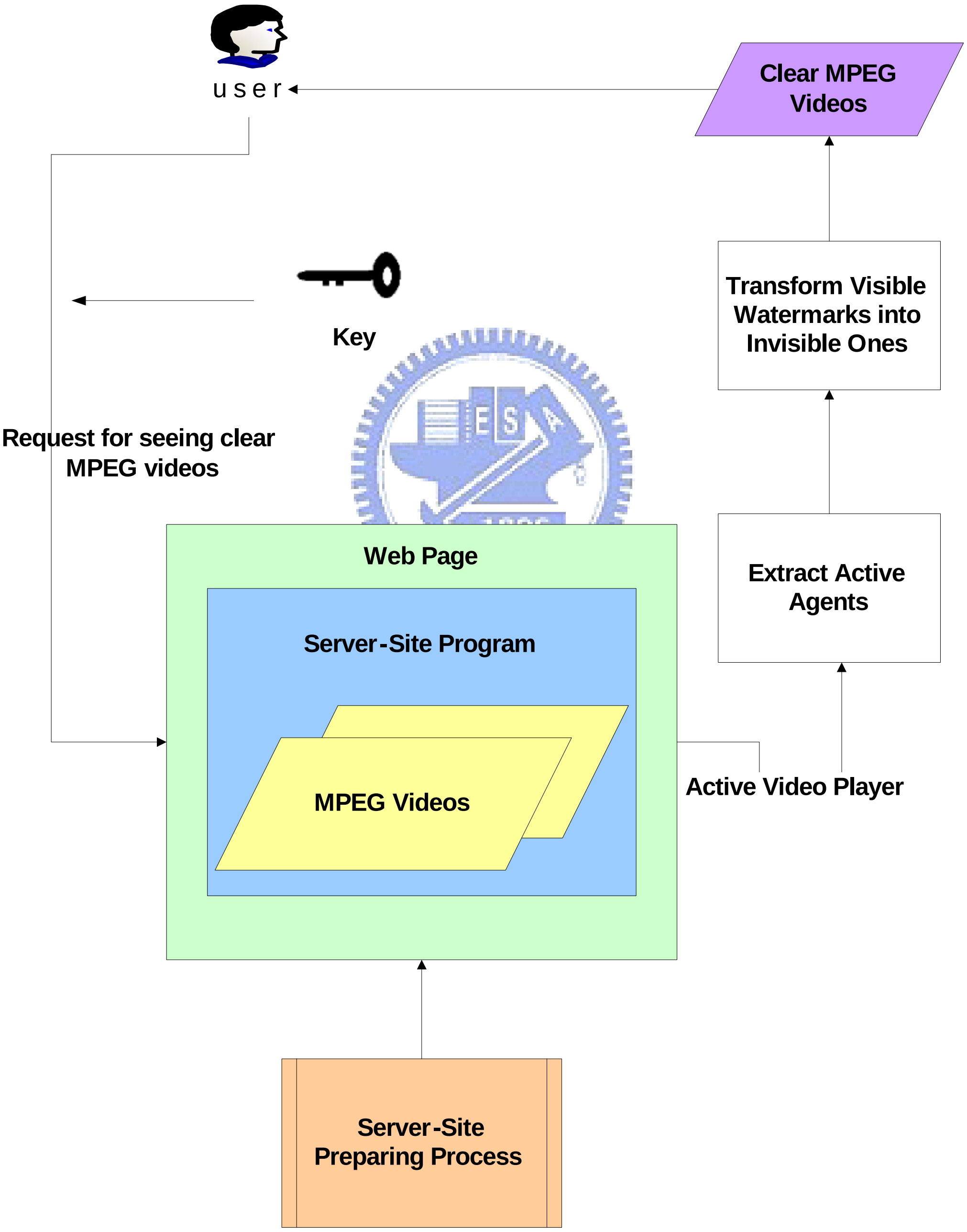

user
Clear MPEG Videos
Transform Visible Watermarks into Invisible Ones
Key
Request for seeing clear MPEG videos
Extract Active Agents
Web Page
Server-Site Program
MPEG Videos
Active Video Player
Server-Site Preparing Process

Figure 5. 6 An illustration of the proposed method for transforming removable visible watermarks actively into invisible ones.

After transforming removable visible watermarks into invisible ones, these invisible watermarks can still protect the copyright of the videos when authentic users modify them for misrepresentation. An illustration of the proposed method is shown in Figure 5.6.

5.4 Proposed Method for Transforming Invisible Watermarks Actively to Visible Ones

The method for hiding watermarks in MPEG videos in this section is similar to that described in Section 5.3, but the transformation process for visible watermarks makes visible watermarks not only have black appearances but also have random intensity values in grayscale. Here is an application example. A multimedia provider puts public videos on the Internet for people to see. But if someone wants to download the videos from a web page, the proposed system can extract the invisible watermarks from the videos, transform them into visible ones with random intensity values in grayscale, and affix them on the videos. This method can declare the copyright of these videos.

In Section 5.4.1, the proposed embedding process for invisible watermarks is introduced. And in Section 5.4.2, the proposed transformation process for visible watermarks is described.

5.4.1 Embedding Process for Invisible Watermarks

At the beginning of the proposed process for embedding invisible watermarks, the video provider should provide a watermark for publicizing the MPEG videos.

After these MPEG videos are processed with variable-length decoding, the frequency-domain data of each of the produces frames can be obtained. With the use of the previously-mentioned embedding process for intra-coded macroblocks and inter-coded ones, watermarks can be embedded in the MPEG videos. Invisible watermarks can protect the copyright of MPEG videos from illicit downloading and make authentic users see clear MPEG videos on a web page. An illustration of embedding removable visible watermarks is shown in Figure 5.7.

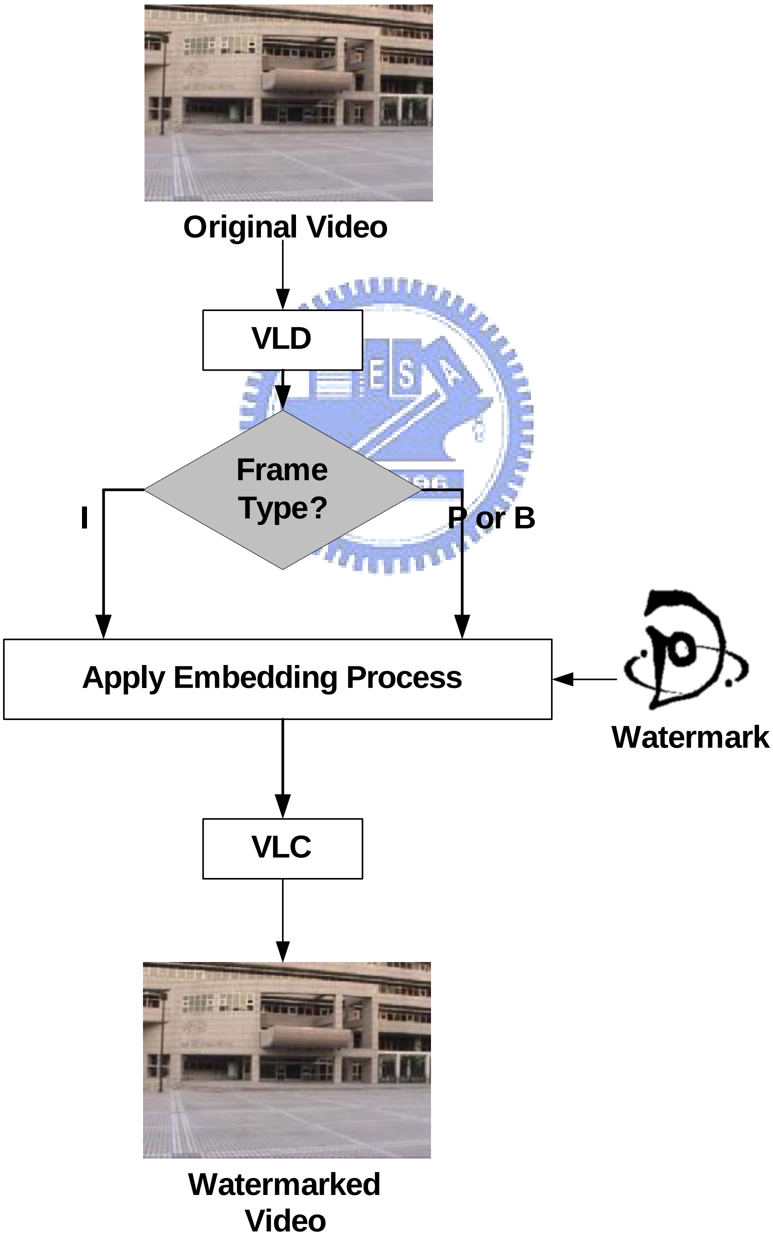


Figure 5. 7 A flowchart of the embedding process for invisible watermarks.

5.4.2 Transformation Process for Visible Watermarks

At the beginning of the proposed process for transforming invisible watermarks into visible ones, users can see clear MPEG videos on a public web page.

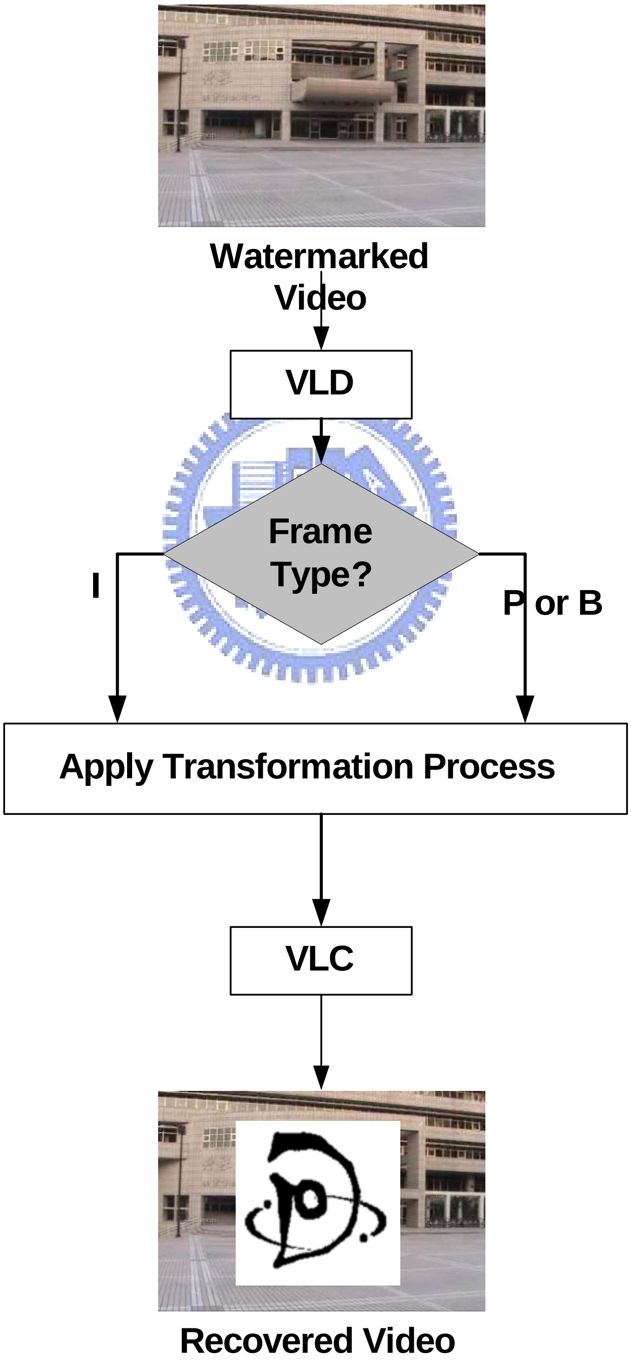


Figure 5. 8 A flowchart of the transformation process for visible watermarks.

Everyone can see these videos without paying anything, but if someone wants to download them, the proposed system will extract the hidden active agents and transform the embedded invisible watermarks into visible ones with random intensity values in grayscale. A flowchart of the current process is shown in Figure 5.8.

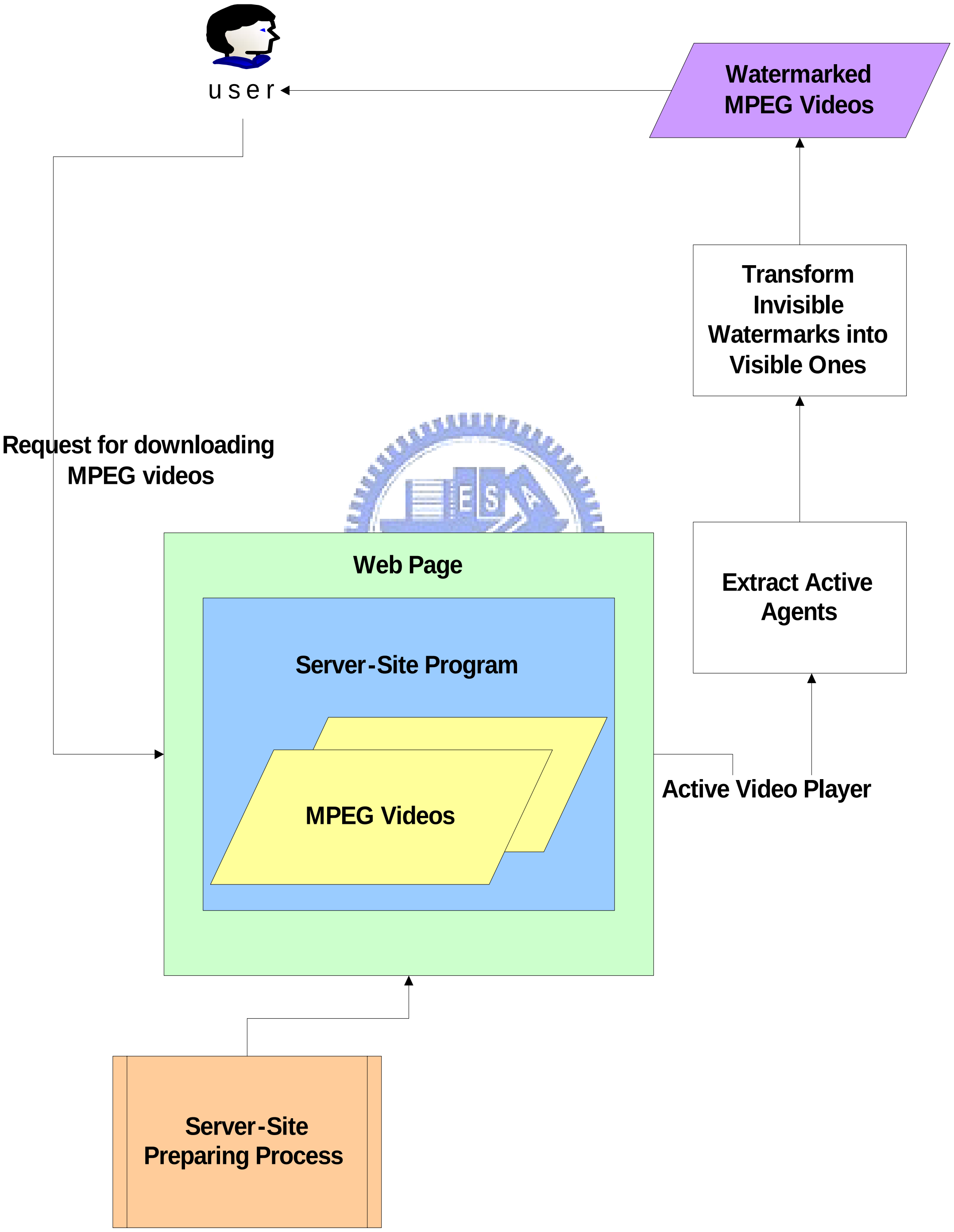

user
Watermarked MPEG Videos
Transform Invisible Watermarks into Visible Ones
Request for downloading MPEG videos
Extract Active Agents
Web Page
Server-Site Program
MPEG Videos
Active Video Player
Server-Site Preparing Process

Figure 5. 9 An illustration of the proposed method for transforming invisible watermarks actively into visible ones.

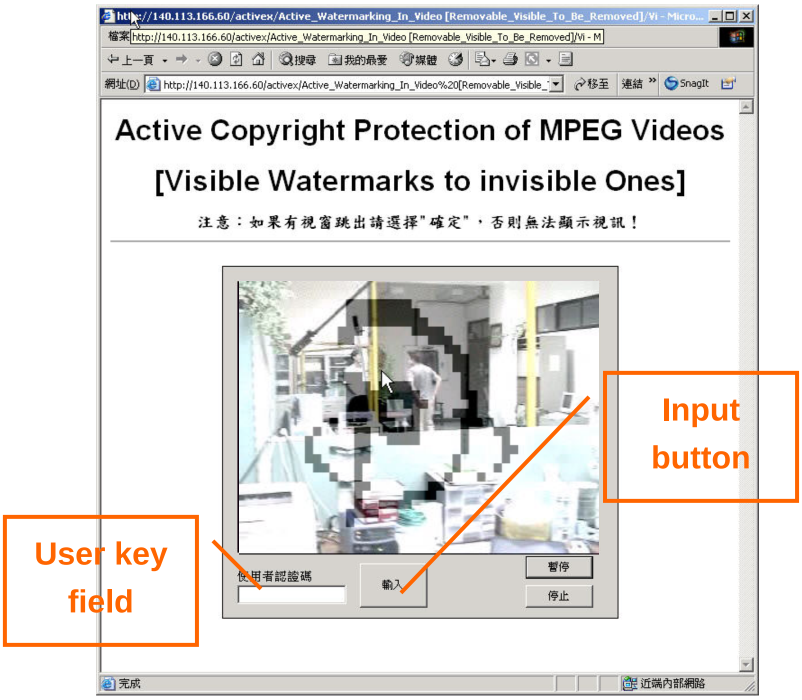
After transforming invisible watermarks into visible ones, visible watermarks can immediately show the ownership of the MPEG videos. Because these visible watermarks are with random intensity values in grayscale, they are not easy to remove. An illustration of the proposed method is shown in Figure 5.9.

5.5 Experimental Results

In our experiments, two applications for active copyright protection of MPEG videos are elaborated. One is a transformations of visible watermarks into invisible ones actively by an active agent, and another is an inverse process of the previous one.

In the first experiment, while a user browses a web page, the proposed system presented in Figure 5.10(a) shows a video with a visible watermark and an active video player. If the user wants to see a clear video displayed in Figure 5.10(b), an authentic key should be provided to the system. Otherwise, a degraded video still shows on the screen.

In the second experiment, an MTV video and a description are displayed on a public web page in Figure 5.11(a). While a user browses this web page, a clear video with an invisible watermark is presented. If the user calls a pop-up menu shown in Figure 5.11(b) and wants to download the video, the proposed system extracts an active agent and transform the invisible watermarks into visible ones actively. After the downloading process is completed as shown in Figure 5.11(d), the video with a visible watermarks shown on the local computer, as shown in Figure 5.11(e).



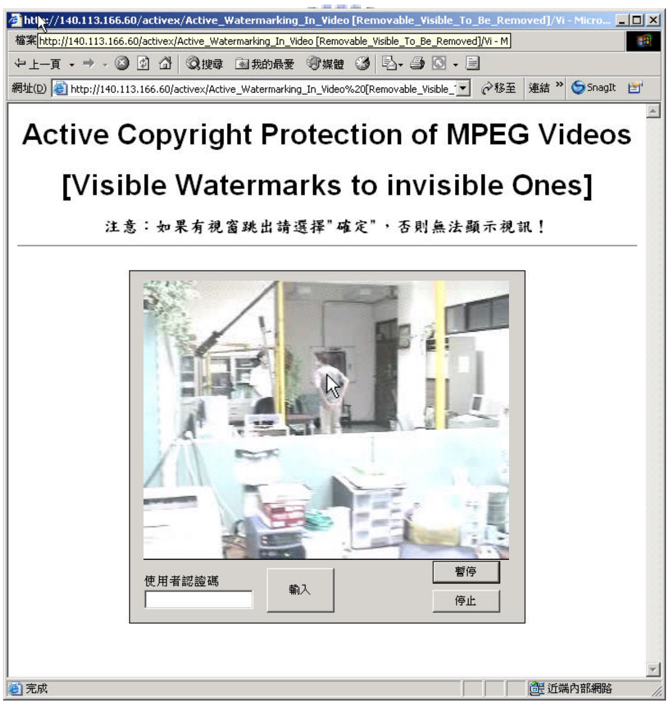
Active Copyright Protection of MPEG Videos

[Visible Watermarks to invisible Ones]

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

http://140.113.166.60/activex/Active_Watermarking_In_Video [Removable_Visible_To_Be_Removed]/Vi - Micro...
User key field
Input button
使用者認證碼
輸入
暫停
停止
完成
近端內部網路

(a)



Active Copyright Protection of MPEG Videos

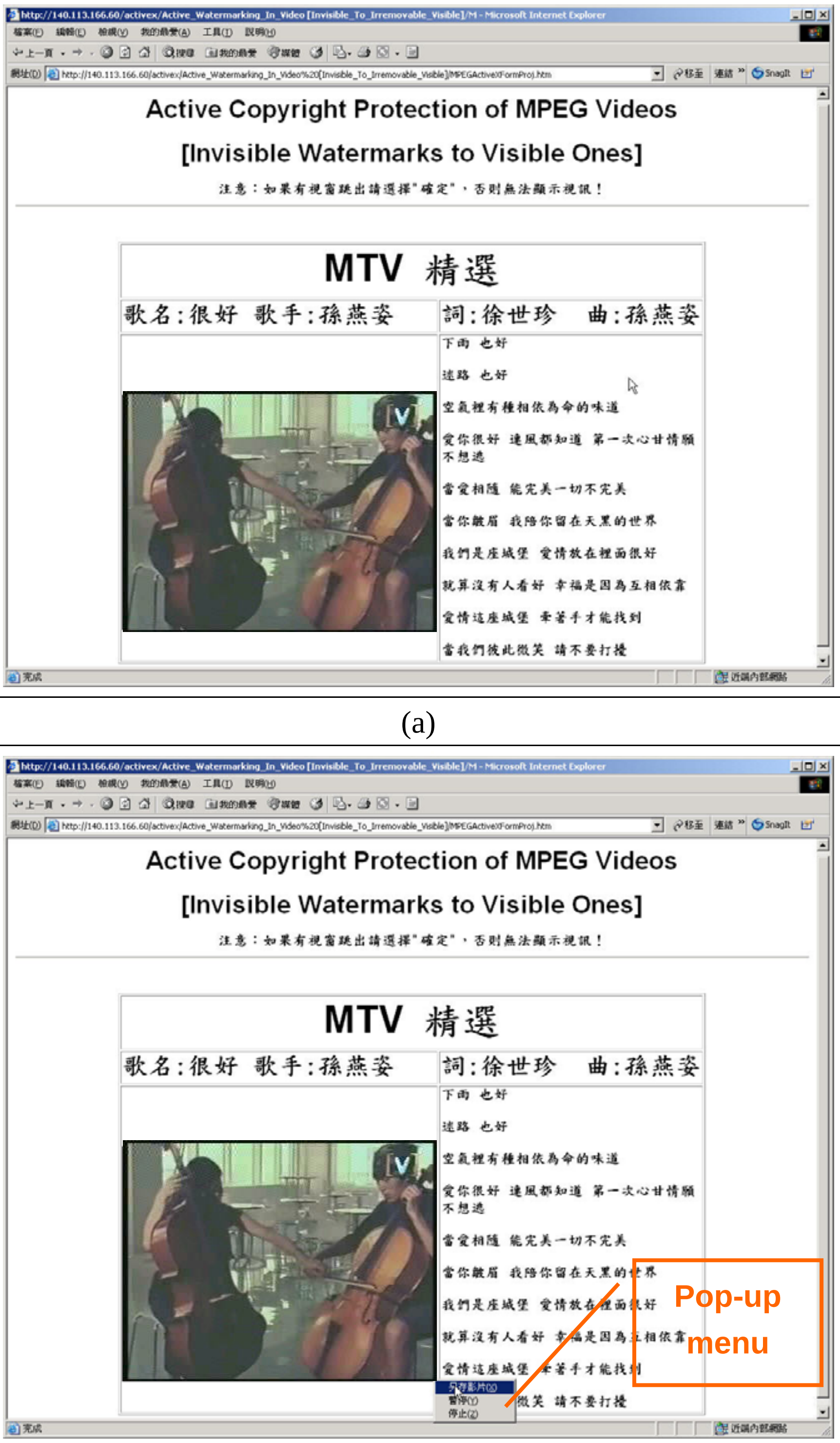
[Visible Watermarks to invisible Ones]

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

http://140.113.166.60/activex/Active_Watermarking_In_Video [Removable_Visible_To_Be_Removed]/Vi - Micro...
使用者認證碼
輸入
暫停
停止
完成
近端內部網路

(b)

Figure 5.10 (a) A video with a visible watermark. (b) A clear video with an invisible watermark after an authentic key is provided.



http://140.113.166.60/activex/Active_Watermarking_In_Video [Invisible_To_Irremovable_Visible]/M - Microsoft Internet Explorer

http://140.113.166.60/activex/Active_Watermarking_In_Video%20[Invisible_To_Irremovable_Visible]/MPEGActiveXFormProj.htm

Active Copyright Protection of MPEG Videos

[Invisible Watermarks to Visible Ones]

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

MTV 精選

歌名:很好 歌手:孫燕姿

詞:徐世珍 曲:孫燕姿

下雨 也好

迷路 也好

空氣裡有種相依為命的味道

愛你很好 連風都知道 第一次心甘情願不想逃

當愛相隨 能完美一切不完美

當你皺眉 我陪你留在天黑的世界

我們是座城堡 愛情放在裡面很好

就算沒有人看好 幸福是因為互相依靠

愛情這座城堡 牽著手才能找到

當我們彼此微笑 請不要打擾

(a)

http://140.113.166.60/activex/Active_Watermarking_In_Video [Invisible_To_Irremovable_Visible]/M - Microsoft Internet Explorer

http://140.113.166.60/activex/Active_Watermarking_In_Video%20[Invisible_To_Irremovable_Visible]/MPEGActiveXFormProj.htm

Active Copyright Protection of MPEG Videos

[Invisible Watermarks to Visible Ones]

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

MTV 精選

歌名:很好 歌手:孫燕姿

詞:徐世珍 曲:孫燕姿

下雨 也好

迷路 也好

空氣裡有種相依為命的味道

愛你很好 連風都知道 第一次心甘情願不想逃

當愛相隨 能完美一切不完美

當你皺眉 我陪你留在天黑的世界

我們是座城堡 愛情放在裡面很好

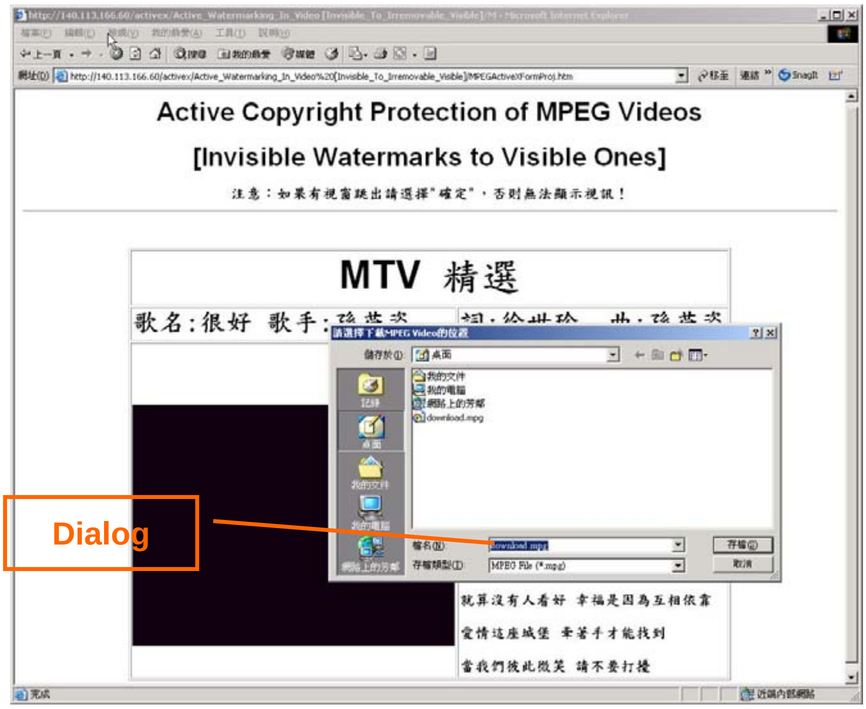
就算沒有人看好 幸福是因為互相依靠

愛情這座城堡 牽著手才能找到

當我們彼此微笑 請不要打擾

(b)

Figure 5.11 (a) A clear video with an invisible watermark. (b) A saving button on a pop-up menu. (c) A dialog which can select the saving location of the video. (d) The downloaded video on the desktop. (e) A video with a visible watermark in the local computer. (continued)



http://140.113.166.60/activex/Active_Watermarking_In_Video%20[Invisible_To_Irremovable_Visible]/MPEGActiveXFormProj.htm

Active Copyright Protection of MPEG Videos

[Invisible Watermarks to Visible Ones]

注意：如果有視窗跳出請選擇"確定"，否則無法顯示視訊！

MTV 精選

歌名：很好　歌手：孫燕姿　詞：徐世珍　曲：孫燕姿

請選擇下載MPEG Video的位置

儲存於(I)：桌面

我的文件
我的電腦
網路上的芳鄰
download.mpg

檔名(N)：download.mpg

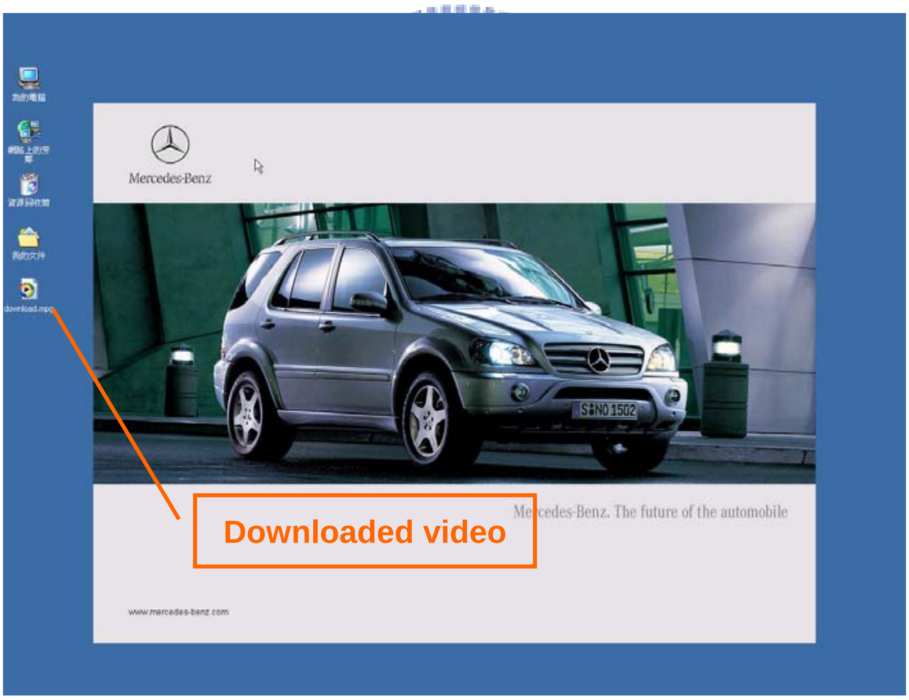
存檔類型(T)：MPEG File (*.mpg)

就算沒有人看好　幸福是因為互相依靠

愛情這座城堡　牽著手才能找到

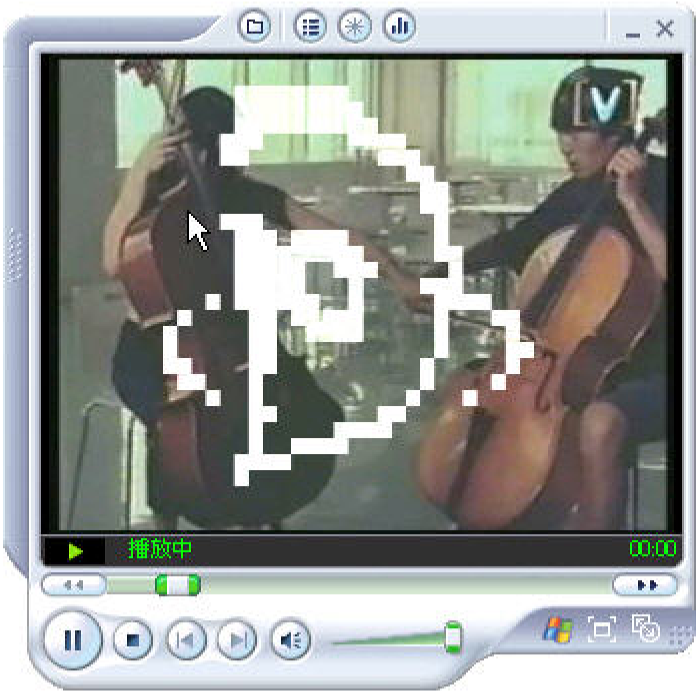
當我們彼此微笑　請不要打擾

(c)



(d)

Figure 5.11 (a) A clear video with an invisible watermark. (b) A saving button on a pop-up menu. (c) A dialog which can select the saving location of the video. (d) The downloaded video on the desktop. (e) A video with a visible watermark in the local computer. (continued)



(e)

Figure 5.11 (a) A clear video with an invisible watermark. (b) A saving button on a pop-up menu. (c) A dialog which can select the saving location of the video. (d) The downloaded video on the desktop. (e) A video with a visible watermark in the local computer. (continued)

5.6 Summary and Discussions

In this chapter, two methods for protecting the copyright of MPEG videos have been proposed and tested. Both of them can display the ownership of MPEG videos. In fact, the proposed method in Section 5.3 may be regarded as the inverse process of the proposed method in Section 5.4.

The application environment of the experiments for transforming invisible watermarks into visible ones is simulated as a real Internet Explorer program and illicit users does not easily notice anything different. After illegal downloading of the MPEG videos, users will get watermarked ones. Based on our experimental results, the proposed methods may be seen to be useful for real applications.

Chapter 6

Active and Passive Large-Volume Covert Communication by Cover Images with Secret Authentication Capability on Cellular Phones

6.1 Introduction

With the advance of mobile computing technologies, more and more electronic devices, such as personal digital assistants, cellular phones, and notebooks, support the ability of executing programming languages. Since these mobile devices can do so, various applications can be developed on them now.

Due to the popularity of using cellular phones and the progress of technology developments of them, the platform of a cellular phone may be adopted to perform data hiding applications now, as done in this study. And the applications can also be implemented on other electronic mobile devices which support JAVA programming languages.

In Section 6.2, an active covert communication method which carry out the method on the platform of a personal computer is proposed. In Section 6.2, a passive covert communication method which supports transmitting large-volume secret messages by multiple cover images is proposed. Finally, some experimental results and a summary are given.

6.2 Proposed Active Covert Communication Method for Cover Images on Cellular Phones

The original idea of the proposed application of active covert communication on cellular phones comes from that of the active covert communication method implemented on personal computers, in which it is desired to extract secret messages from cover media without the need of installing data hiding programs. The proposed method is that each cellular phone supporting JAVA programming languages can get secret messages from cover media on web pages.

In Sections 6.2.1 and 6.2.2, both the embedding process and the extraction process for secret messages hidden in cover media are introduced.

6.2.1 Process for Embedding Secret Messages

The secret message embedding process is implemented on the platform of a server-site personal computer. An illustration of the process is presented in Figure 6.1.

First, an authentication signal has to be generated by the secret messages and the user key. The method of calculating authentication signals is the same as that proposed in Chapter 3. After generating an authentication signal, it can be hidden behind the secret messages and the proposed system can utilize a user key to randomize it. Because the size of the display screen on the cellular phone is usually small, that of the cover image should be small enough so as to be displayed appropriately on the cellular phone screen. For the sake of the limited data hiding capacity of the cover image, a 2-LSB data hiding technique is adopted in this chapter. Every bit of randomized secret messages with an authentication signal is embedded in the cover image by modifying the two least significant bits of each pixel.

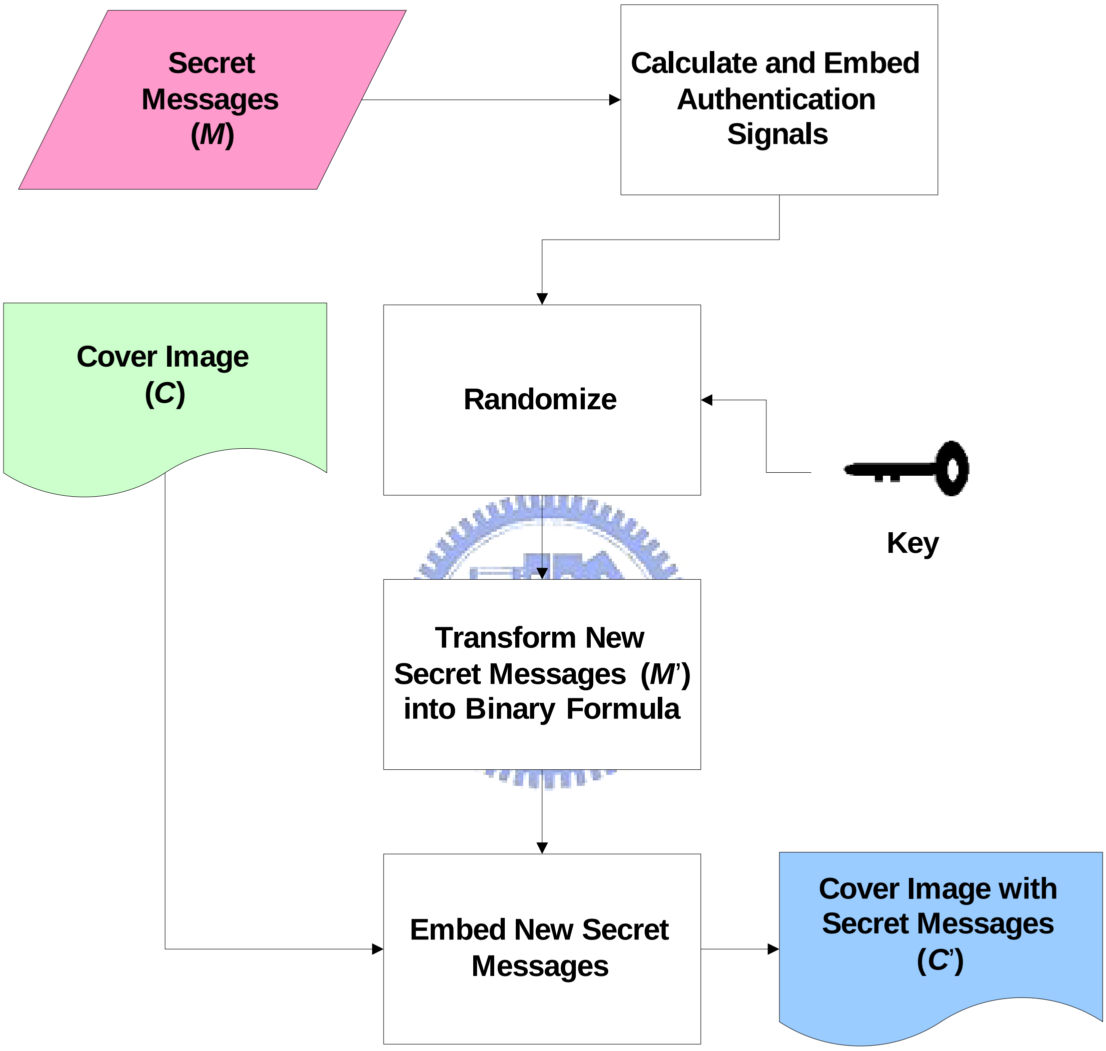
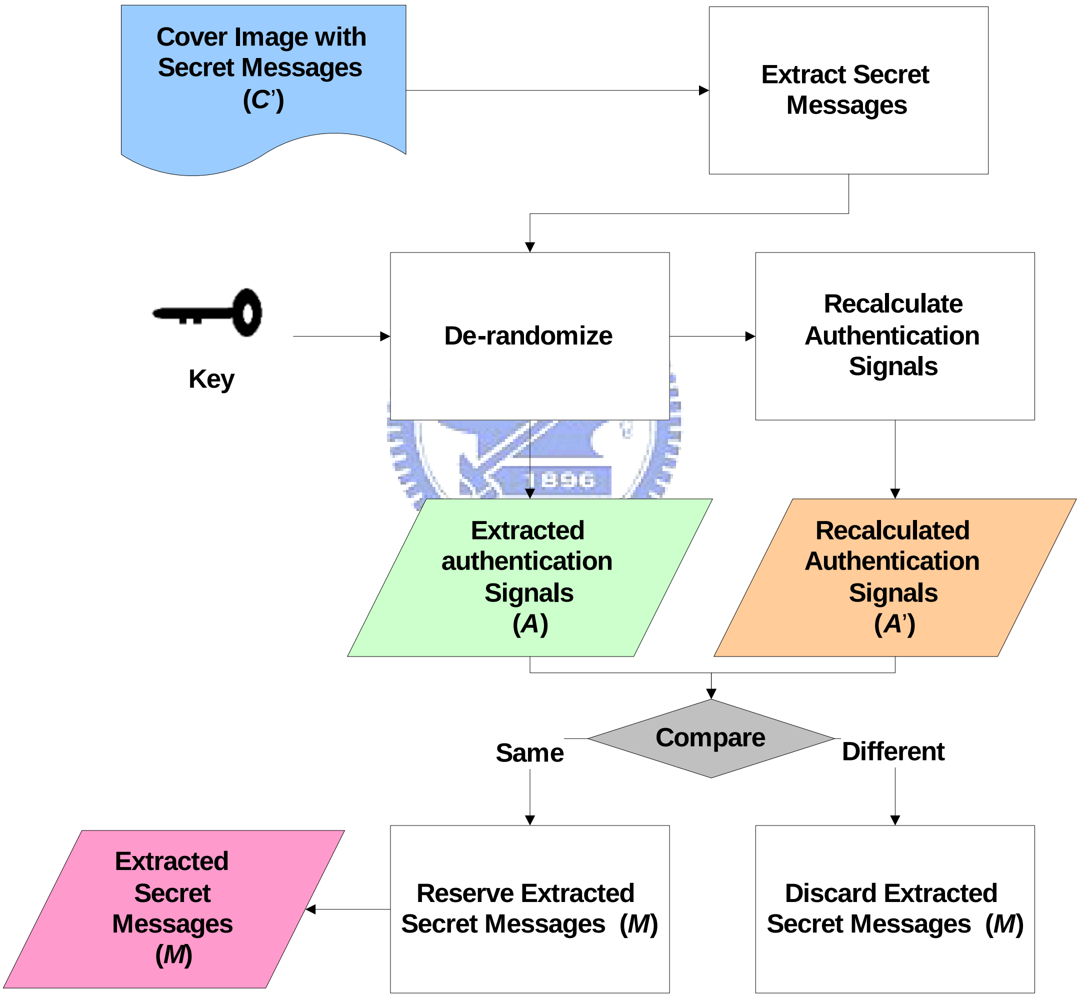

Secret Messages (*M*)
Calculate and Embed Authentication Signals
Cover Image (*C*)
Randomize
Key
Transform New Secret Messages (*M'*) into Binary Formula
Embed New Secret Messages
Cover Image with Secret Messages (*C'*)

Figure 6. 1 An illustration of the process for embedding secret messages.

6.2.2 Process for Extracting Secret Messages

The extraction process is implemented on the platform of a cellular phone. An illustration of the process is shown in Figure 6.2. It is the inverse process the embedding one. Secret messages with an authentication signal are extracted by a

2-LSB data hiding technique. After extracting all the hidden data, an input user key is used to de-randomize them and obtain an extracted authentication signal. Then, the extracted secret messages have to be used to regenerate an authentication signal. After comparing the extracted authentication signal and the regenerated one, if these two signals are the same, the extracted secret messages are considered as correct and kept; otherwise, they will be discarded.



Cover Image with Secret Messages (*C*')
Extract Secret Messages
Key
De-randomize
Recalculate Authentication Signals
Extracted authentication Signals (*A*)
Recalculated Authentication Signals (*A*')
Compare
Same
Different
Extracted Secret Messages (*M*)
Reserve Extracted Secret Messages (*M*)
Discard Extracted Secret Messages (*M*)

Figure 6. 2 An illustration of the process for extracting secret messages.

A flowchart of the proposed method is shown in Figure 6.3. After preparing a cover image with secret messages, they are put into a JAVA program on a web page for people to download. When a user downloads the JAVA program, the cover image is displayed on the screen of a cellular phone. If the user wants to extract the secret messages from the cover image, a button on the cellular phone has to be pressed and an authentic user key should be provided for correct extraction.

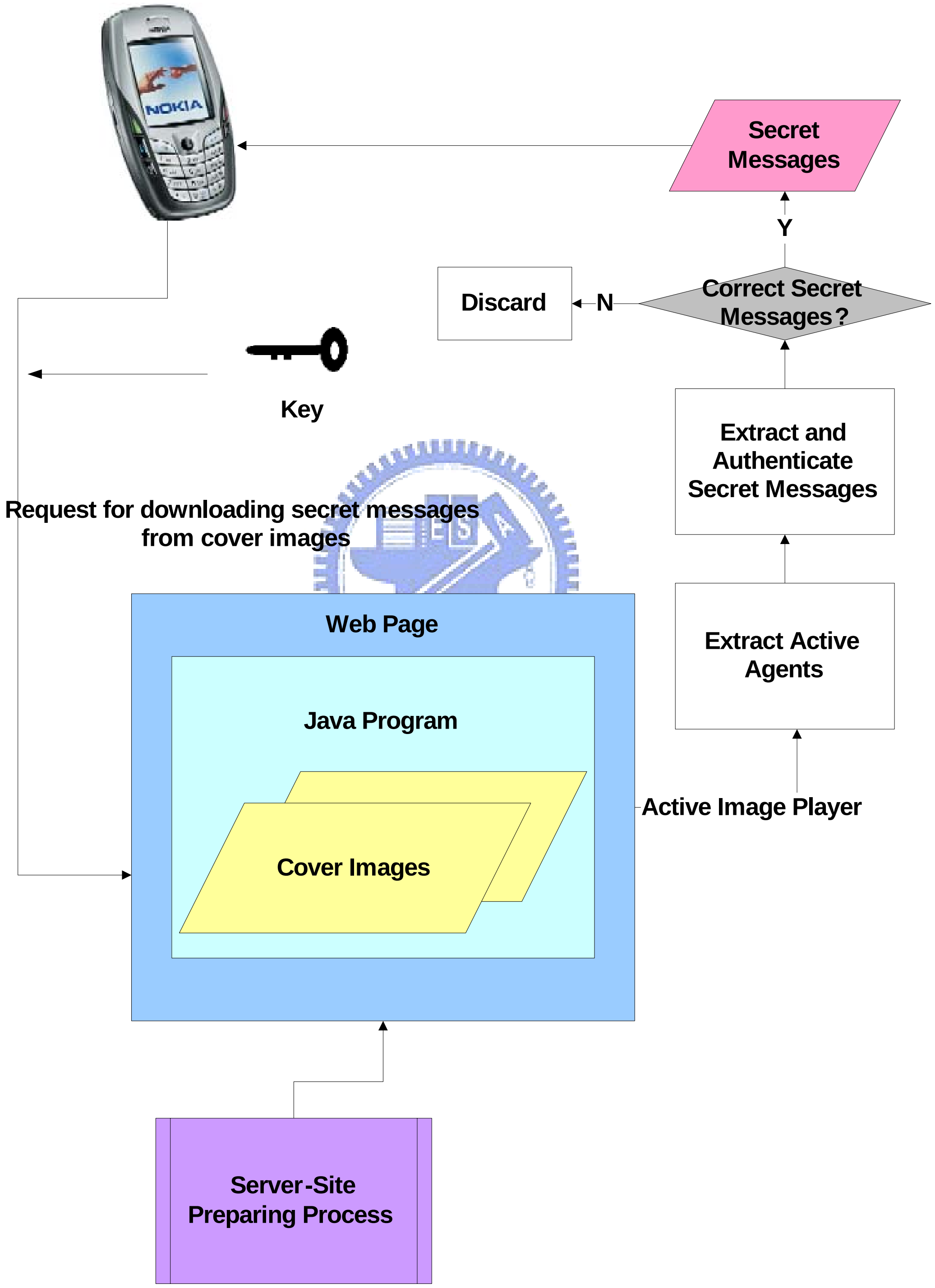

Secret Messages
Y
Discard
N
Correct Secret Messages?
Key
Extract and Authenticate Secret Messages
Request for downloading secret messages from cover images
Web Page
Extract Active Agents
Java Program
Active Image Player
Cover Images
Server-Site Preparing Process

Figure 6. 3 A flowchart of the proposed active covert communication method for cover images on cellular phones.

6.3 Proposed Passive Large-Volume Covert Communication Method for Cover Images on Cellular Phones

Using cellular phones to exchange secret messages is a kind of insecure behavior. No matter utilizing the voice conversation or sending short messages, both of these two methods let secret messages exposed under the public transmission environment. A passive covert-communication method for cover images on cellular phones is proposed to take this security problem into consideration. In order to transmit large-volume secret messages, both a dividing process and a combination one of the secret messages are proposed.

In Section 6.3.1, a method for dividing and combining large-volume secret messages is introduced. In Section 6.3.2 and Section 6.3.3, both an embedding process and an extraction process are presented.

6.3.1 Method for Dividing and Combining Large-Volume Secret Messages

Because the size of cover images is usually small, the corresponding data hiding capacity is usually not very large. To solve this problem, a method for dividing and combining large-volume secret messages is proposed.

An illustration of the dividing method is shown in Figure 6.4. According to the data hiding capacity of each cover image, secret messages are divided into several segments. Each segment has its own authentication signal and is randomized by an input user key.

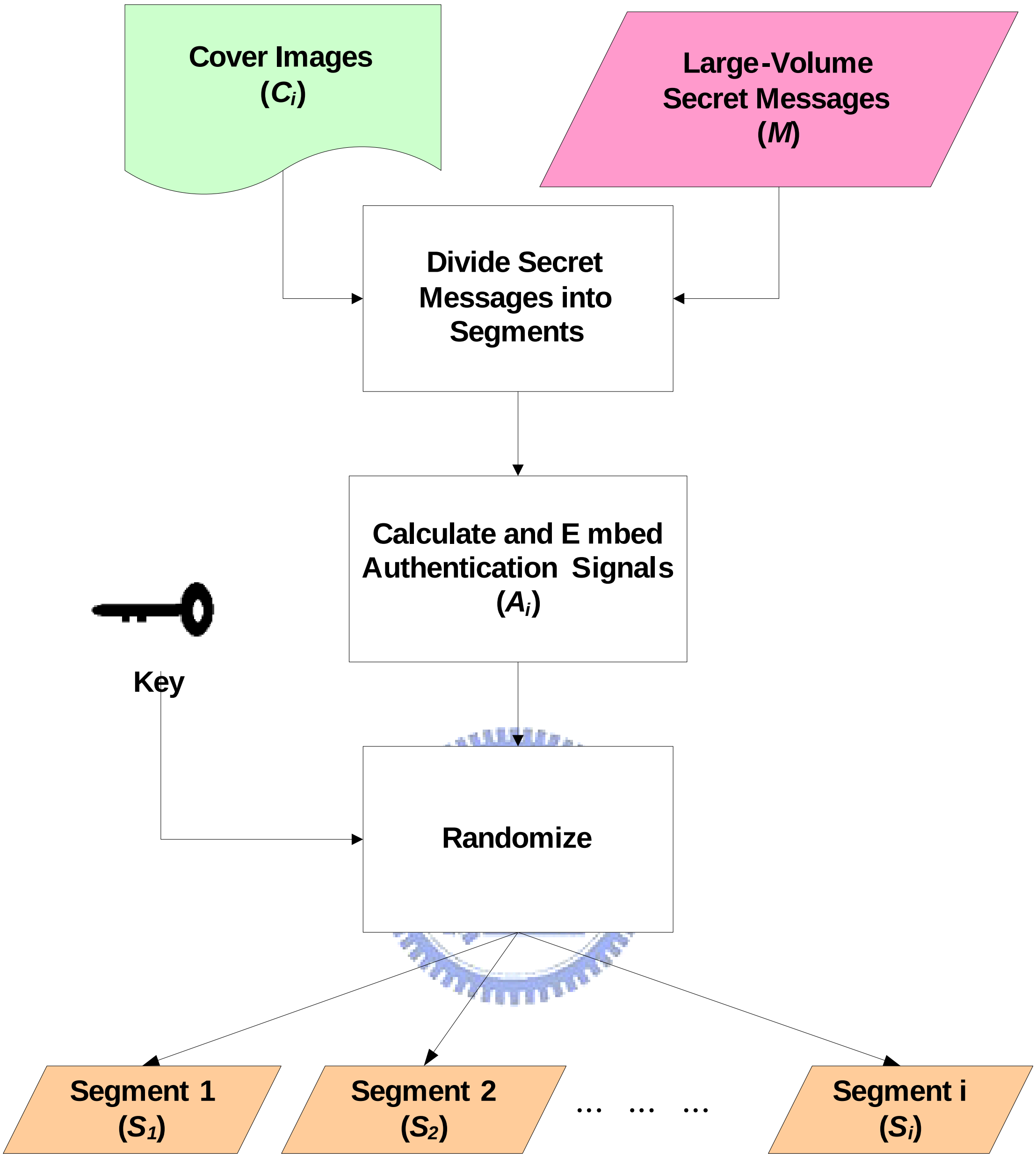


Figure 6. 4 An illustration of the process for dividing secret messages into segments.

An illustration of the combination method is shown in Figure 6.5. Each segment must be de-randomized by an input user key and then an authentication signal would be regenerated. After verifying the fidelity of the secret messages of each segment, the proposed system can combine them according to their original sequence. If there is any incorrect segment, the receiver should request for retransmissions of correct segments.

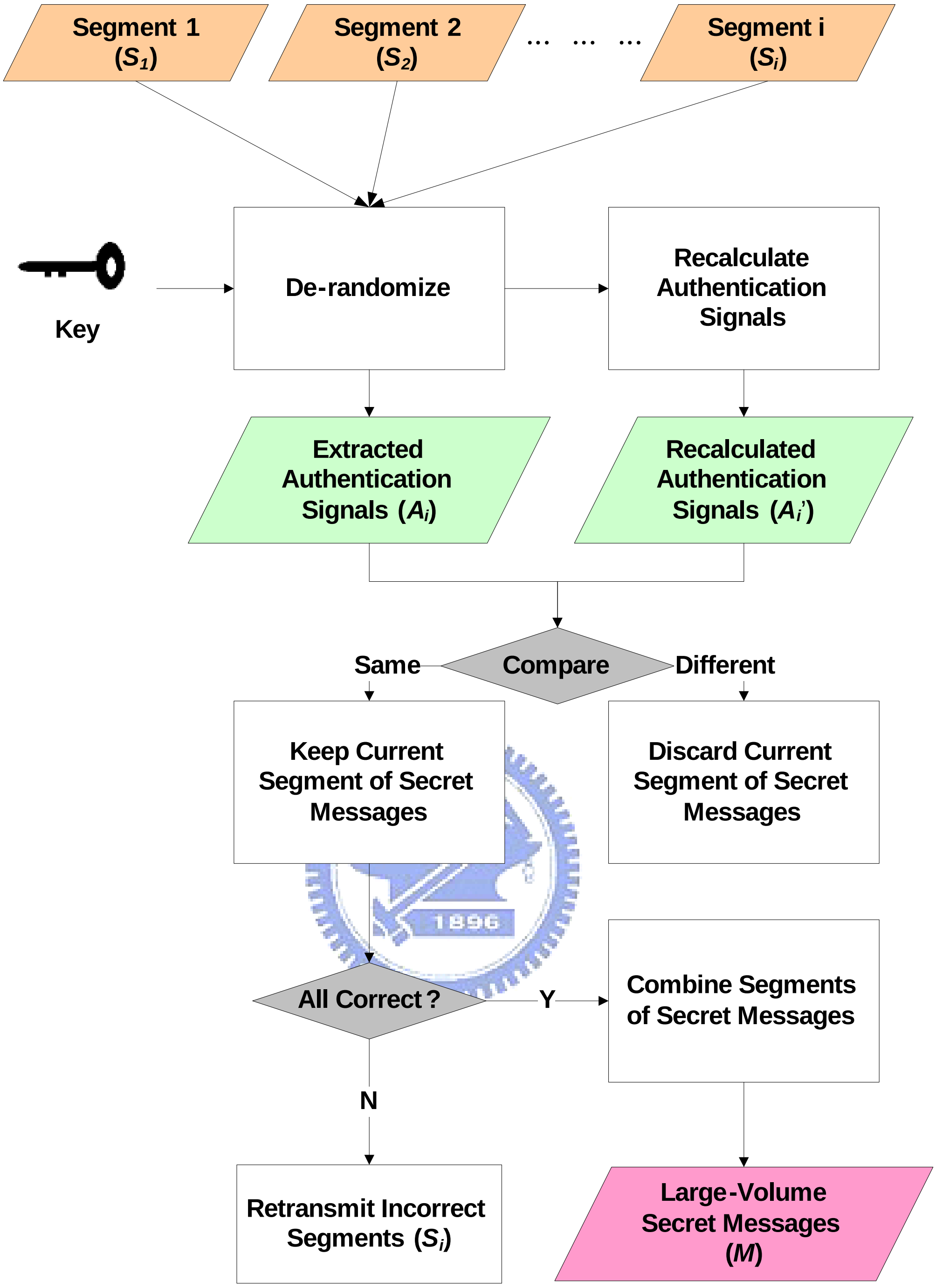

Segment 1 (S_1)
Segment 2 (S_2)
… … …
Segment i (S_i)
Key
De-randomize
Recalculate Authentication Signals
Extracted Authentication Signals (A_i)
Recalculated Authentication Signals (A_i')
Same
Compare
Different
Keep Current Segment of Secret Messages
Discard Current Segment of Secret Messages
All Correct ?
Y
Combine Segments of Secret Messages
N
Retransmit Incorrect Segments (S_i)
Large-Volume Secret Messages (M)

Figure 6. 5 An illustration of the process for combining segments of secret messages.

6.3.2 Process for Embedding Secret Messages in Multiple Cover Images

We all know that keying in large-volume messages on a cellular phone is not an easy job. With the use of wireless transmission devices of infrared rays or Bluetooth, a user can prepare all messages on a personal computer easily in advance and then use these wireless devices to transmit the messages into a cellular phone.

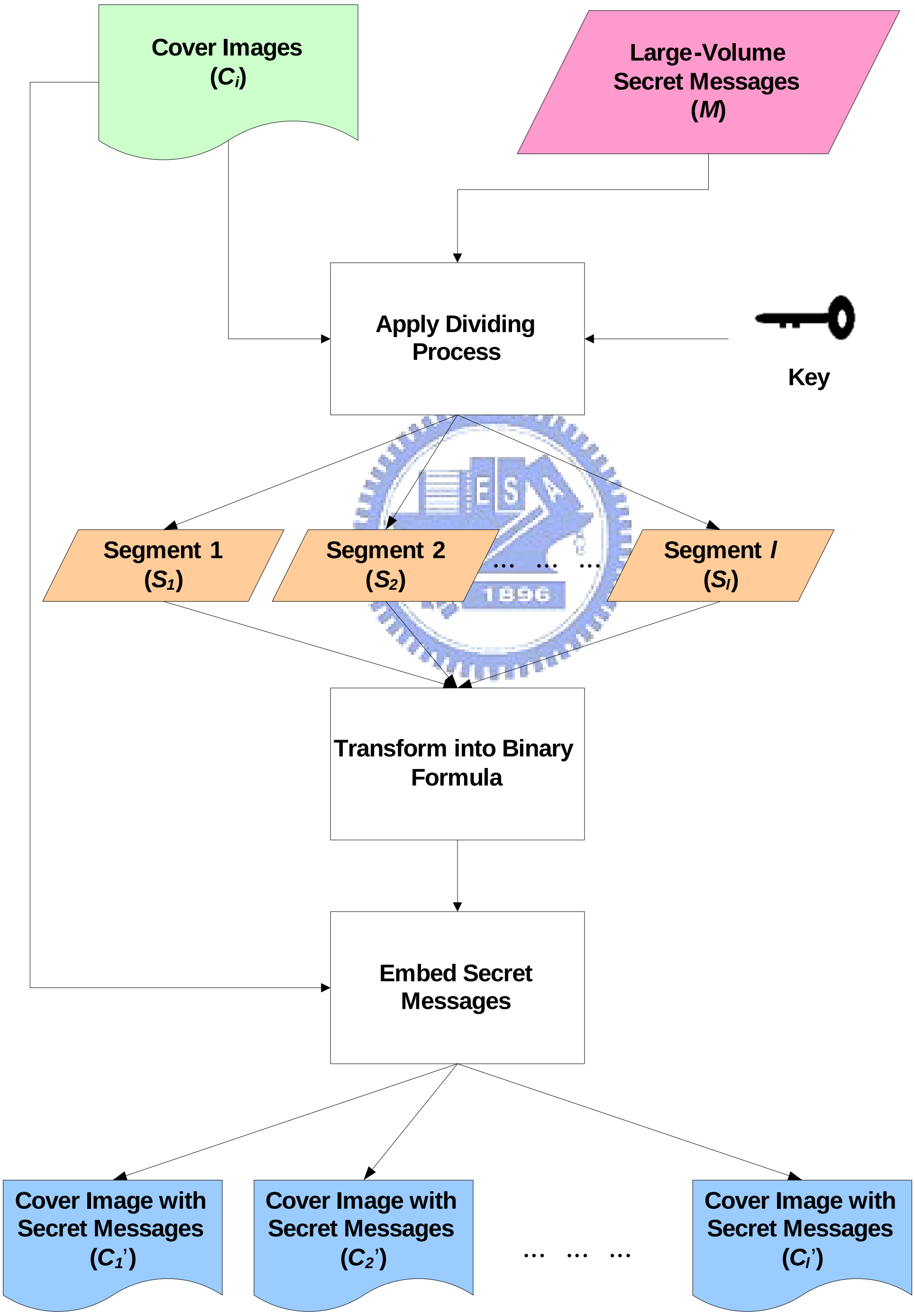


Figure 6. 6 An illustration of the process for embedding secret messages into multiple cover images.

After dividing large-volume secret messages into segments, the proposed system utilizes a 2-LSB data hiding technique to embed each segment in the corresponding cover image. An illustration of the process is shown in Figure 6.6.

6.3.3 Process for Extracting Secret Messages from Multiple Cover Images

An illustration of the process of extracting secret messages from multiple cover images is shown in Figure 6.7.

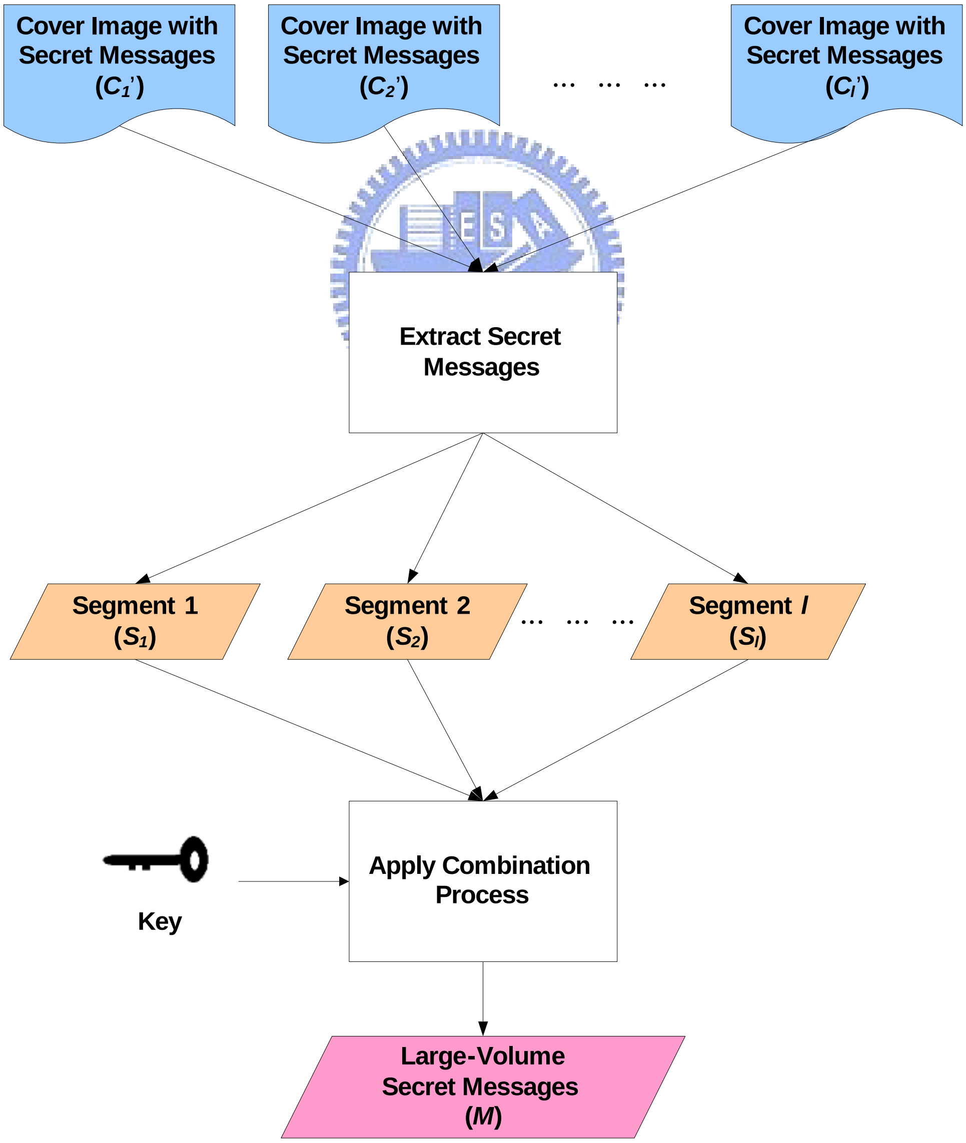

Cover Image with Secret Messages (C_1')
Cover Image with Secret Messages (C_2')
… … …
Cover Image with Secret Messages (C_l')
Extract Secret Messages
Segment 1 (S_1)
Segment 2 (S_2)
… … …
Segment l (S_l)
Key
Apply Combination Process
Large-Volume Secret Messages (M)

Figure 6. 7 An illustration of the process for extracting secret messages from multiple cover images.

On the receiver site, after collecting all the cover images from the sender site, the proposed system can use an input user key to authenticate each segment of the secret messages and do the combination manipulation.

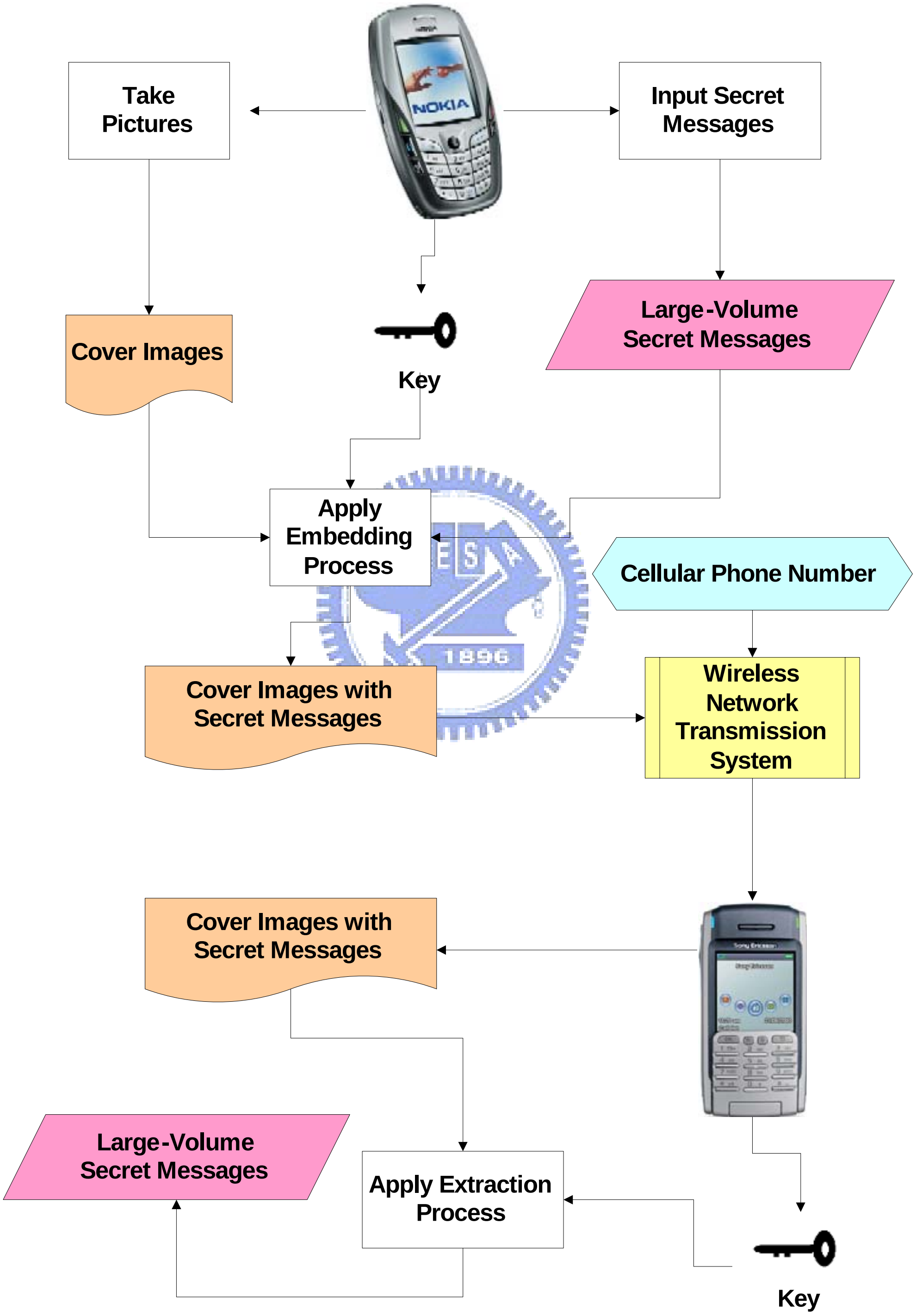
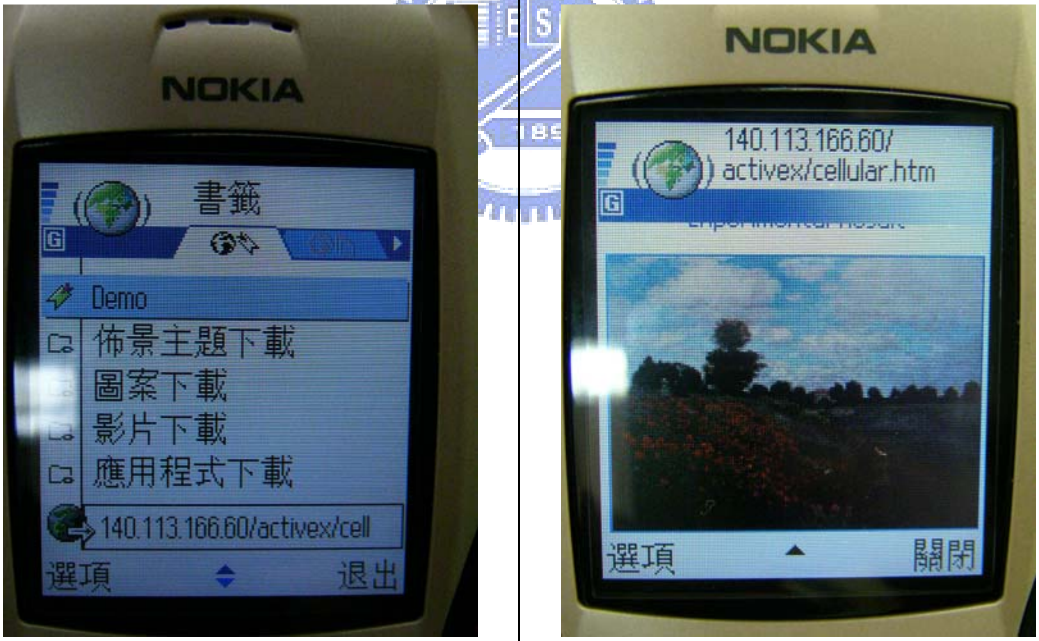

Take Pictures
Input Secret Messages
Cover Images
Key
Large-Volume Secret Messages
Apply Embedding Process
Cellular Phone Number
Cover Images with Secret Messages
Wireless Network Transmission System
Cover Images with Secret Messages
Large-Volume Secret Messages
Apply Extraction Process
Key

Figure 6. 8 A flowchart of the proposed passive large-volume covert communication method for cover images on cellular phones.

A flowchart of the proposed method is shown in Figure 6.8. The sender only needs to input the telephone number of the receiver's cellular phone and every cover image will be encapsulated as many short message packets and transmitted to the receiver through the wireless transmission of the short messaging system (SMS). At the receiver site, the proposed system can combine each packet to form a complete image and utilizes an input user key to extract and recover the hidden secret messages.

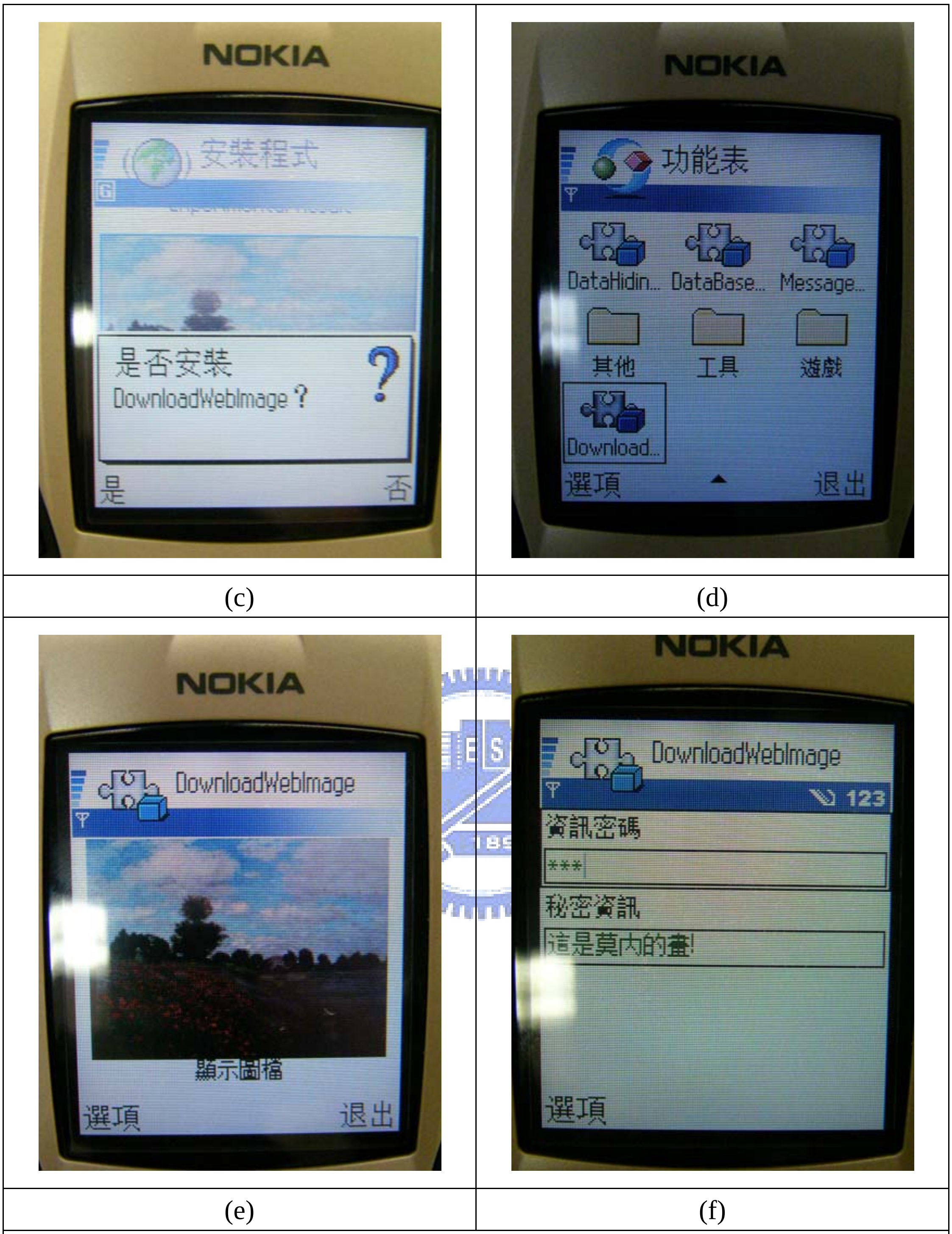
6.4 Experimental Results

In our experiments, two applications, namely, active and passive covert communication, via cover images are elaborated.



(a) (b)

Figure 6.9 An experimental result. (a) A browser in the cellular phone. (b) A public web page. (c) Downloading the JAVA program. (d) An icon of the program. (e) The execution screen of the program. (f) A success extraction with a user key 123. (g) A failed extraction with a user key 12. (continued)



(c)

(d)

(e)

資訊密碼

***

秘密資訊

這是莫內的畫!

(f)

Figure 6.9 An experimental result. (a) A browser in the cellular phone. (b) A public web page. (c) Downloading the JAVA program. (d) An icon of the program. (e) The execution screen of the program. (f) A success extraction with a user key 123. (g) A failed extraction with a user key 12. (continued)

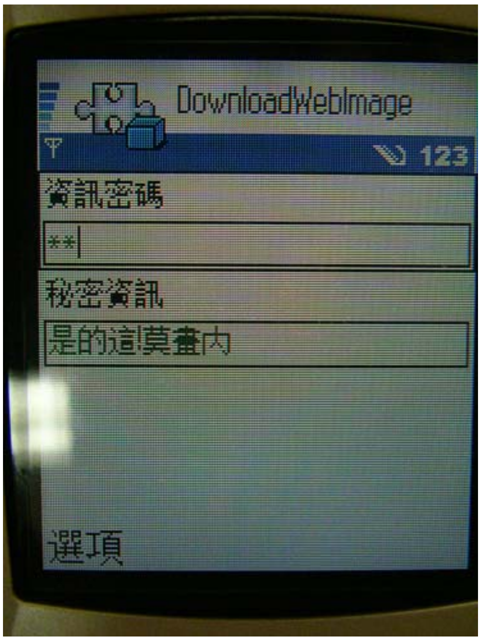
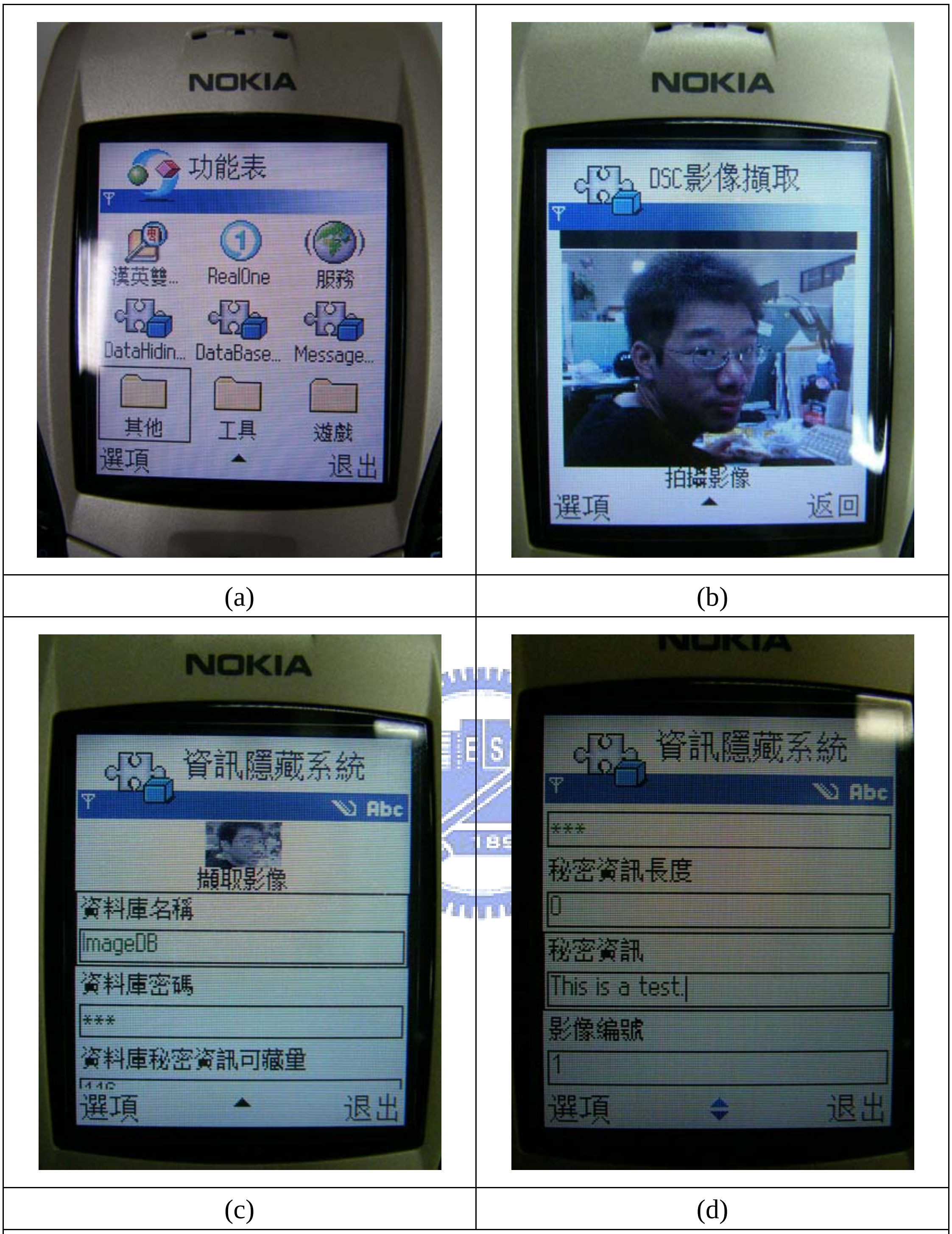
 DownloadWebImage 123 資訊密碼 ** 秘密資訊 是的這莫畫内 選項	
(g)	

Figure 6.9 An experimental result. (a) A browser in the cellular phone. (b) A public web page. (c) Downloading the JAVA program. (d) An icon of the program. (e) The execution screen of the program. (f) A success extraction with a user key 123. (g) A failed extraction with a user key 12. (continued)

In the first experiment, while a user utilizes a cellular phone to browse a web page, a website address must be inputted in a browser. Then, a cover image and some descriptions are displayed on the screen. The user can press the button on the cellular phone and download a JAVA program presented in Figure 6.9(c). After the installation is completed, an icon is shown on the main screen. If the user executes the downloaded program, the cover image can be displayed on the screen. While the selection button presented in Figure 6.9(e) is pressed, the user can input a user key to extract secret messages hidden in the cover image. If the provided key is wrong, the extraction process fails, as presented in Figure 6.9(g).



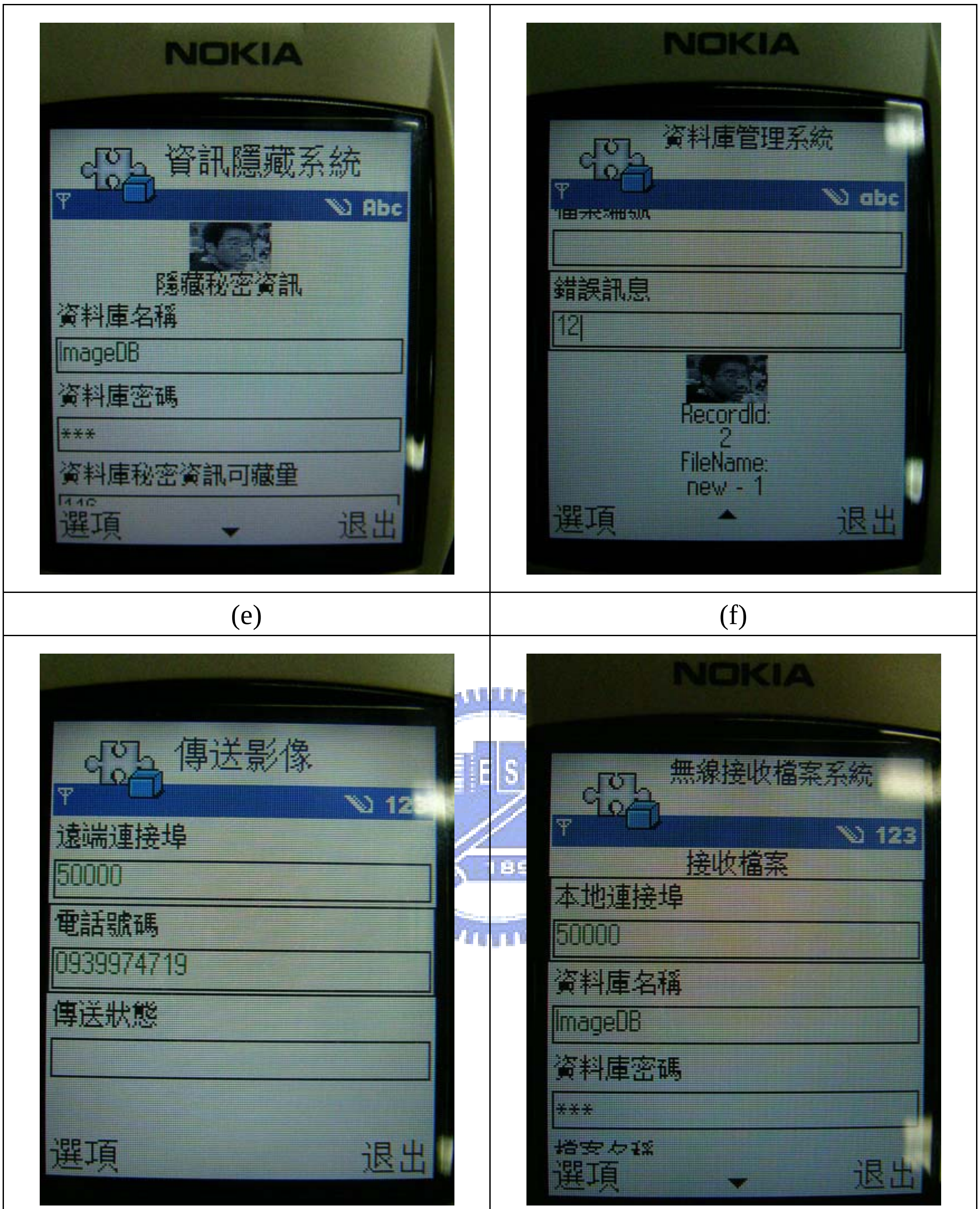
資料庫名稱
ImageDB
資料庫密碼
***
資料庫秘密資訊可藏量

***
秘密資訊長度
0
秘密資訊
This is a test.
影像編號
1

(a) (b)

(c) (d)

Figure 6.10 An experimental result. (a) Three icons of the proposed system. (b) Taking a picture. (c) A captured image. (d) Keying in secret messages. (e) The completed embedding process. (f) A cover image in the database. (g) The transmission system on the sender site. (h) The receiving system on the receiver site. (i) Loading of the received cover image. (j) The completed extraction process. (k) A success extraction with a user key 123. (l) A failed extraction with a user key 12. (continued)



資訊隱藏系統

Abc

隱藏秘密資訊

資料庫名稱

ImageDB

資料庫密碼

***

資料庫秘密資訊可藏量

選項 退出

(e)

資料庫管理系統

abc

錯誤訊息

12

RecordId:
2
FileName:
new - 1

選項 退出

(f)

傳送影像

遠端連接埠

50000

電話號碼

0939974719

傳送狀態

選項 退出

(g)

無線接收檔案系統

123

接收檔案

本地連接埠

50000

資料庫名稱

ImageDB

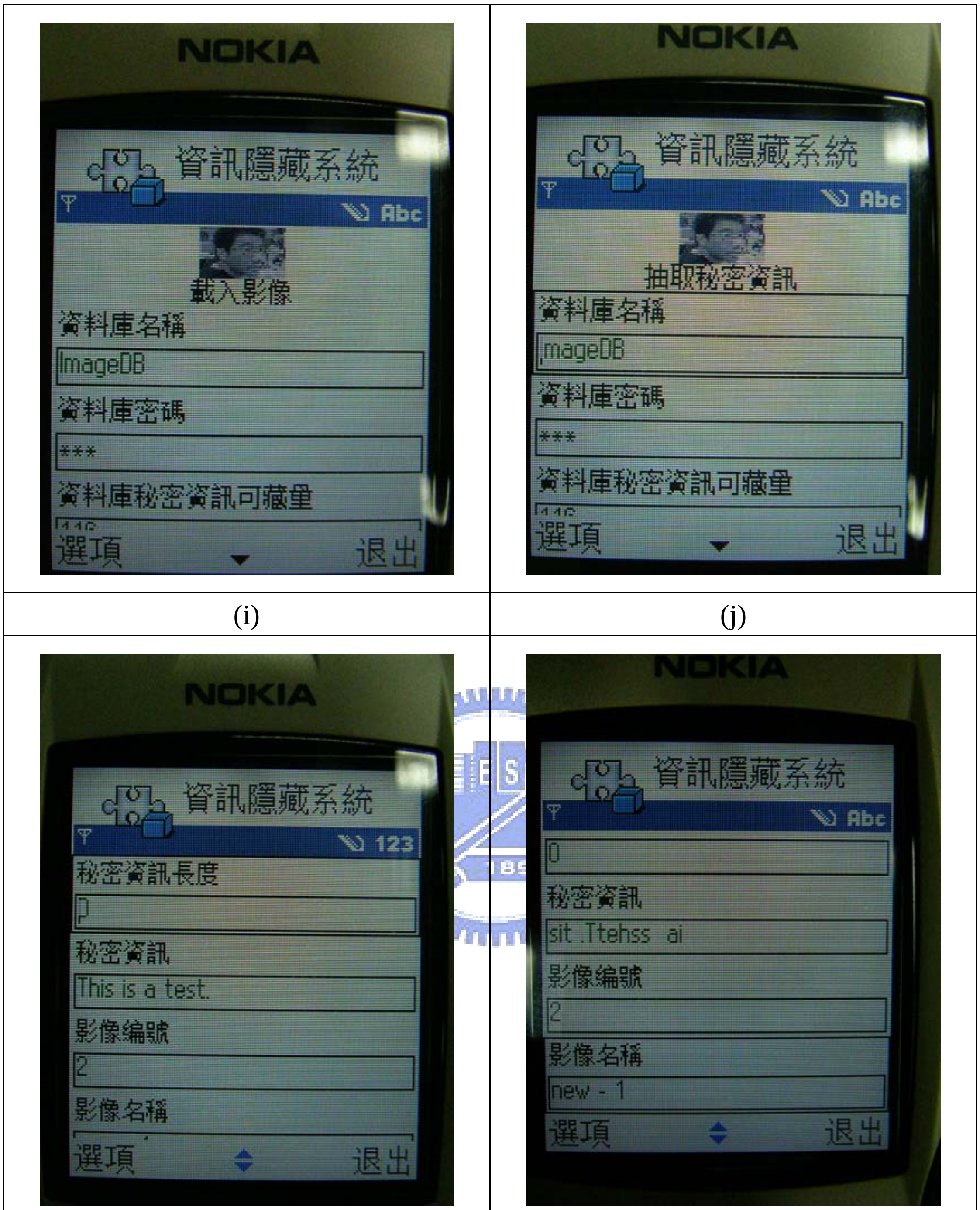
資料庫密碼

***

選項 退出

(h)

Figure 6.10 An experimental result. (a) Three icons of the proposed system. (b) Taking a picture. (c) A captured image. (d) Keying in secret messages. (e) The completed embedding process. (f) A cover image in the database. (g) The transmission system on the sender site. (h) The receiving system on the receiver site. (i) Loading of the received cover image. (j) The completed extraction process. (k) A success extraction with a user key 123. (l) A failed extraction with a user key 12. (continued)



資訊隱藏系統

Abc

載入影像

資料庫名稱

ImageDB

資料庫密碼

***

資料庫秘密資訊可藏量

116

選項 退出

(i)

資訊隱藏系統

Abc

抽取秘密資訊

資料庫名稱

mageDB

資料庫密碼

***

資料庫秘密資訊可藏量

116

選項 退出

(j)

資訊隱藏系統

123

秘密資訊長度

P

秘密資訊

This is a test.

影像編號

2

影像名稱

選項 退出

(k)

資訊隱藏系統

Abc

0

秘密資訊

sit .Ttehss ai

影像編號

2

影像名稱

new - 1

選項 退出

(l)

Figure 6.10 An experimental result. (a) Three icons of the proposed system. (b) Taking a picture. (c) A captured image. (d) Keying in secret messages. (e) The completed embedding process. (f) A cover image in the database. (g) The transmission system on the sender site. (h) The receiving system on the receiver site. (i) Loading of the received cover image. (j) The completed extraction process. (k) A success extraction with a user key 123. (l) A failed extraction with a user key 12. (continued)

In the second experiment, when a user wants to deliver secret messages to others making use of the proposed system, a picture as a cover image can be taken by the camera built in the cellular phone, as presented in Figure 6.10(b). The user has to key in a user key and the secret messages, and the proposed system can embed them in the cover image. After the embedding process is completed, the user can utilize the wireless network transmission system presented in Figure 6.10(e) to transmit the cover image to others. On the receiver site, a corresponding receiving system should be executed to get the cover image. After the receiving process is completed, the receiver also has to key in an authentic user key to the proposed system to extract the secret messages, as presented in Figure 6.10(i).

6.5 Summary and Discussions

In this chapter, two types of data hiding applications, including active covert communication and passive covert communication, have been proposed and tested. A user can utilize the proposed system and a cellular phone to achieve the purpose of covert communication for data hiding applications.

There are some advantages of using cellular phones as the executing platform against personal computers, as illustrated in the following.

1. The size of a cellular phone is much smaller than a personal computer.
2. The acquisition of a cellular phone is much easier than a personal computer.
3. The ability of wireless connections of a cellular phone is much more convenient than personal computers.

But there are also some benefits of using personal computers as the executing platform against cellular phones illustrated as follows.

1. The computing power of a personal computer is much stronger than that of a

cellular phone.

2. The physical memory of a personal computer is much larger than a cellular phone.
3. The network transmission rate of a personal computer is much faster than a cellular phone.

In fact, the selection of the executing platform depends on applications which we want.

Chapter 7

Image Transmission with Authentication Capability on Cellular Phones

7.1 Introduction

Since the transmission of cover images on the platform of a cellular phone is exposed on the public wireless network environment, illicit users may intercept these images and edit them for deceiving receivers or misrepresentation. Thus, verifying the validity and the integrity of the transmitted images is necessary.

In Section 7.2, the proposed authentication method for captured images on cellular phones is introduced. This method describes how to generate authentication signals for images and two processes for embedding and extracting of them are also included here. Finally, some experimental results and discussions are given.

7.2 Proposed Authentication Method for Captured Images on Cellular Phones

Because most of modern cellular phones have built-in cameras, they have the ability of taking pictures. Combined with the wireless network transmission system, cellular phones can help users investigate confidential cases.

Here is an application example. When an employee is investigating classified cases and has to take important pictures for evidences, the employee can utilize a camera built on a cellular phone to accomplish this job. After collecting essential pictures, the employee can transmit them to superiors through the public wireless network environment. After the superiors receive these pictures, they do not know whether the received pictures are genuine or not and can use the proposed system to authenticate them.

In Section 7.2.1, an authentication signal generation method is proposed. After generating authentication signals, two processes for embedding and extracting them are needed, and they are described in Sections 7.2.2 and 7.2.3, respectively.

7.2.1 Method for Generating Authentication Signals

In order to verify the fidelity of captured images, a 4×4 block in an image is taken as an authentication unit. While a suspicious image is being authenticated, the proposed system can check an authentication signal hidden in each 4×4 block. An illustration of a 4×4 block is shown in Figure 7.1 and the corresponding detailed algorithm is described in the following.

***Algorithm* 1:** Generate an authentication signal for a 4×4 block.

***Input*:** a 4×4 block B, a user key K, and each pixel value of a 4×4 block P_i, $i = 1, 2, \ldots,$ 16.

***Output*:** an authentication signal S.

***Steps*:**

1. Use a binary mask $(1111\ 1100)_2$ and AND it with P_i to get P_i’.

2. Calculate the average pixel value of P_i' and denote it by M.
3. Utilize K and M to generate a random integer R with the length of 32 bits as an authentication signal S.

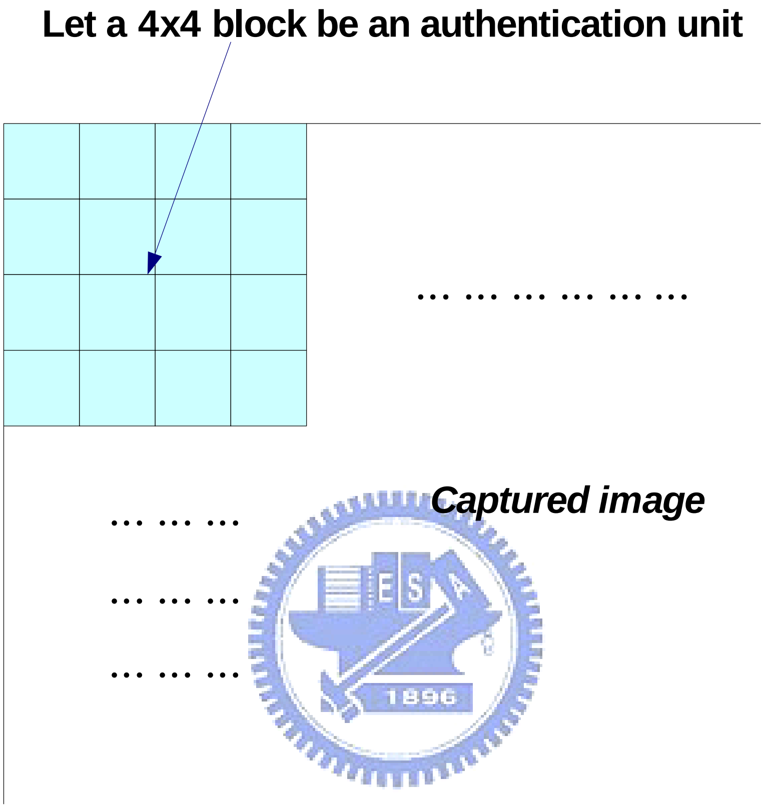


Figure 7. 1 An illustration of a 4×4 block on a captured image.

7.2.2 Process for Embedding Authentication Signals

After capturing images using a camera built on a cellular phone, a user should take these images and a user key as input to the proposed system. The system uses the method for generating authentication signals mentioned in Section 7.2.1 and a 2-LSB data hiding technique to hide an authentication signal into a 4×4 block. For each block, it has 16 pixels and the system can employ the two least significant bits of each pixel to embed a random integer with the length of 32 bits in the red, green, and blue channels, respectively. A flowchart of the process is shown in Figure 7.2.

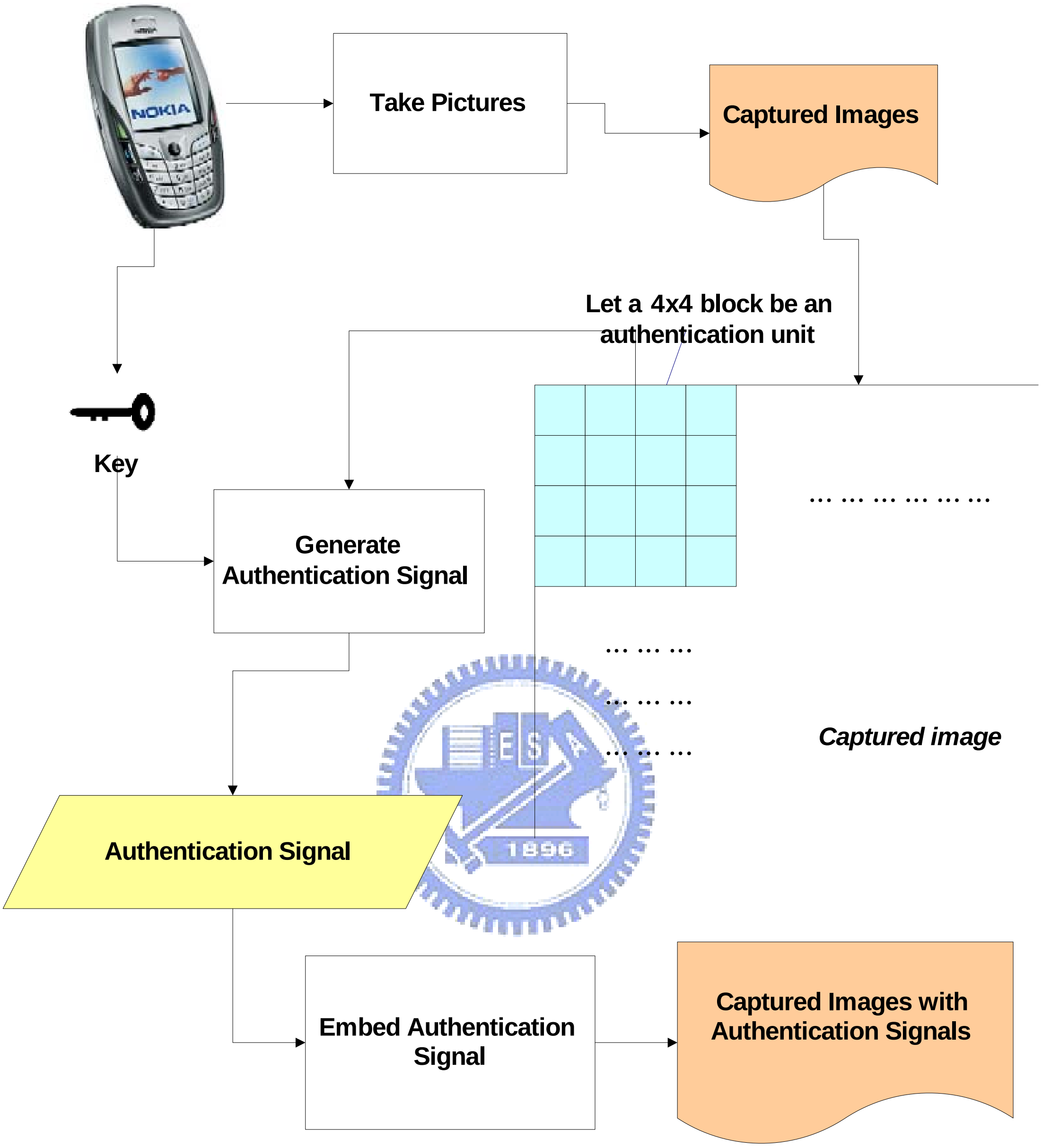

Take Pictures
Captured Images
Let a 4x4 block be an authentication unit
Key
Generate Authentication Signal
… … … … … …
… … …
… … …
… … …
Captured image
Authentication Signal
Embed Authentication Signal
Captured Images with Authentication Signals

Figure 7. 2 An illustration of the process for embedding authentication signals in a captured image.

7.2.3 Process for Extracting Authentication Signals

While the receiver gets a suspicious image, the system can utilize an input user key and the corresponding mean value of each block to regenerate an authentication signal. If an extracted authentication signal and a regenerated one is the same, the current block can be considered as authentic, otherwise, it is thought unauthentic. The extraction process is an inverse of the embedding one and both of them utilize the 2-LSB data hiding technique. A flowchart of the process is shown in Figure 7.3

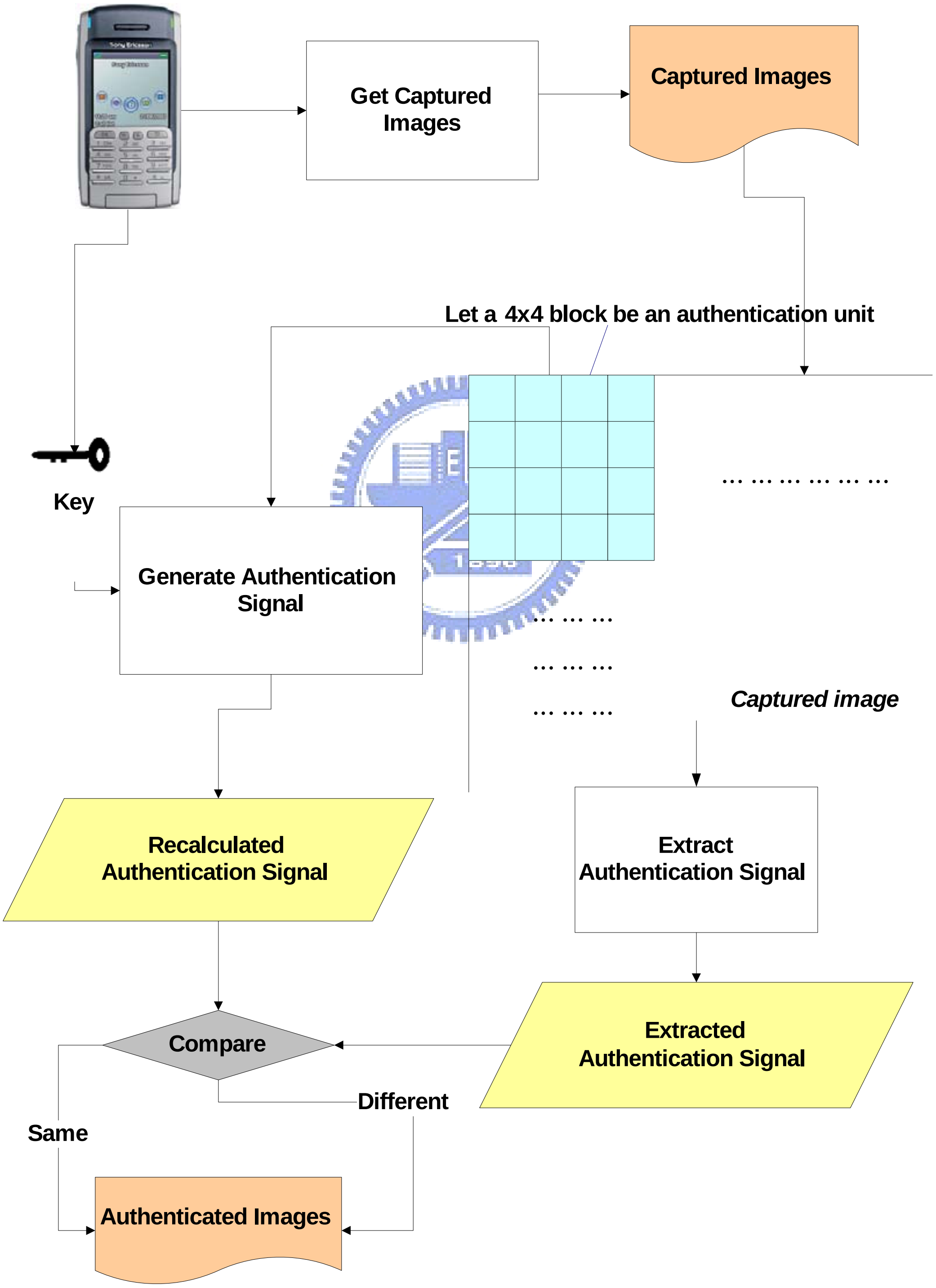

Get Captured Images
Captured Images
Let a 4x4 block be an authentication unit
… … … … … …
Key
Generate Authentication Signal
… … …
… … …
… … …
Captured image
Recalculated Authentication Signal
Extract Authentication Signal
Compare
Extracted Authentication Signal
Different
Same
Authenticated Images

Figure 7. 3 An illustration of the process for extracting authentication signals from a captured image.

An illustration of the proposed method is shown in Figure 7.4. Both the sender and the receiver should take the same user key as input for correct verification of suspicious captured images. At the sender site, the receiver's cellular phone number should be input to the proposed system and all data are transmitted to the receiver site through the public wireless network.

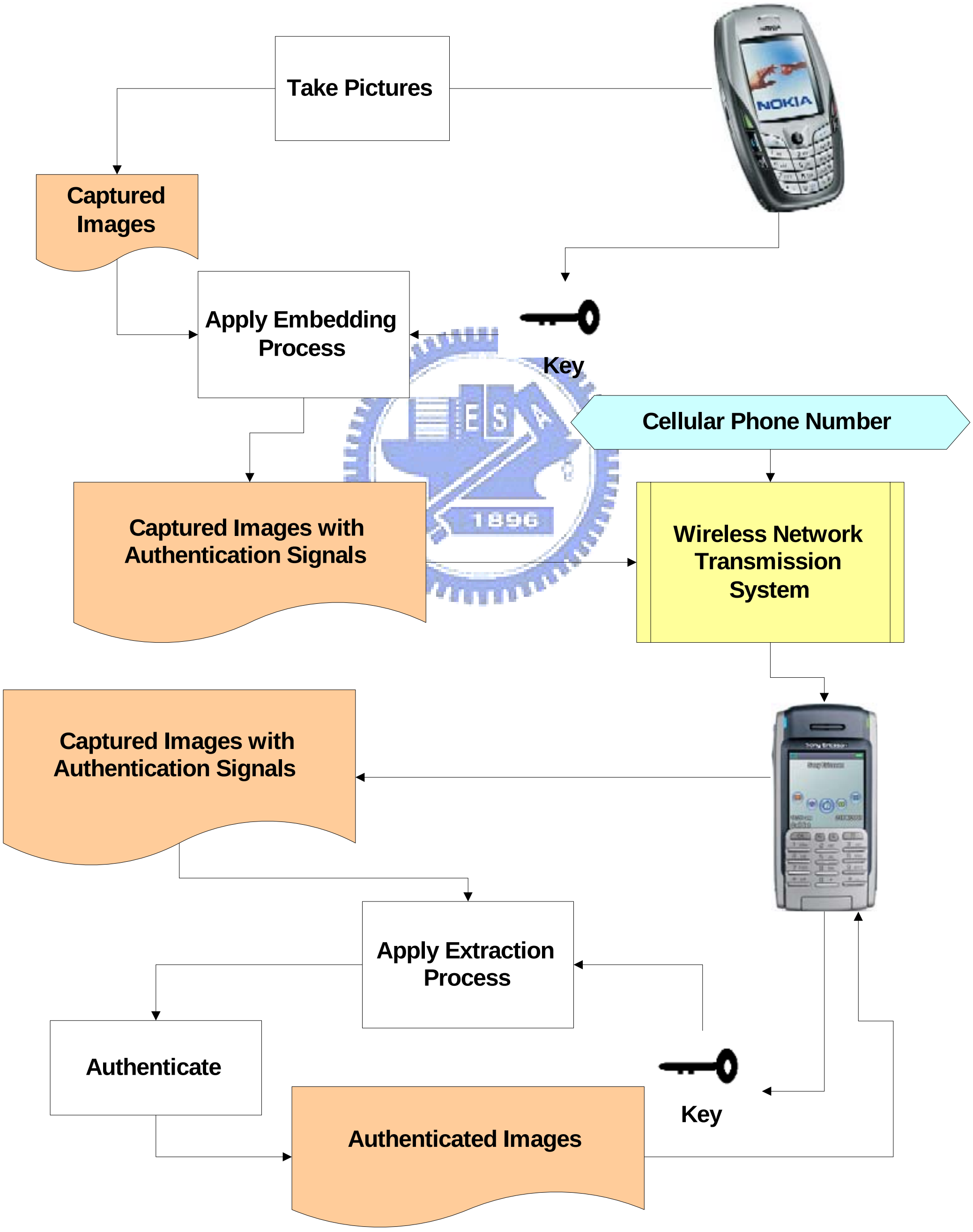
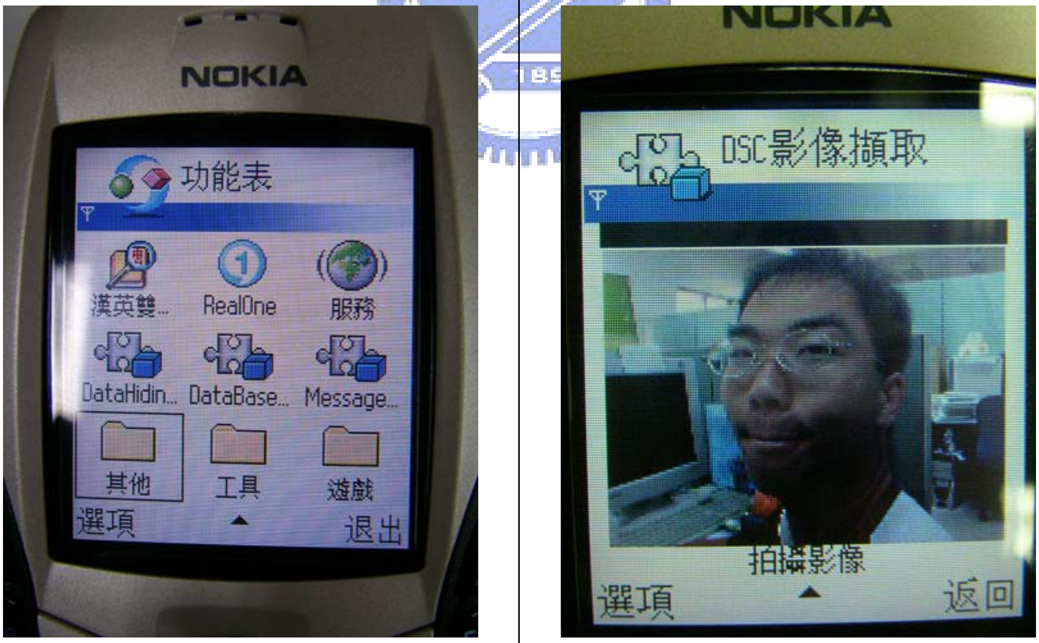


Figure 7. 4 An illustration of the proposed authentication method for captured images

on cellular phones.

7.3 Experimental Results

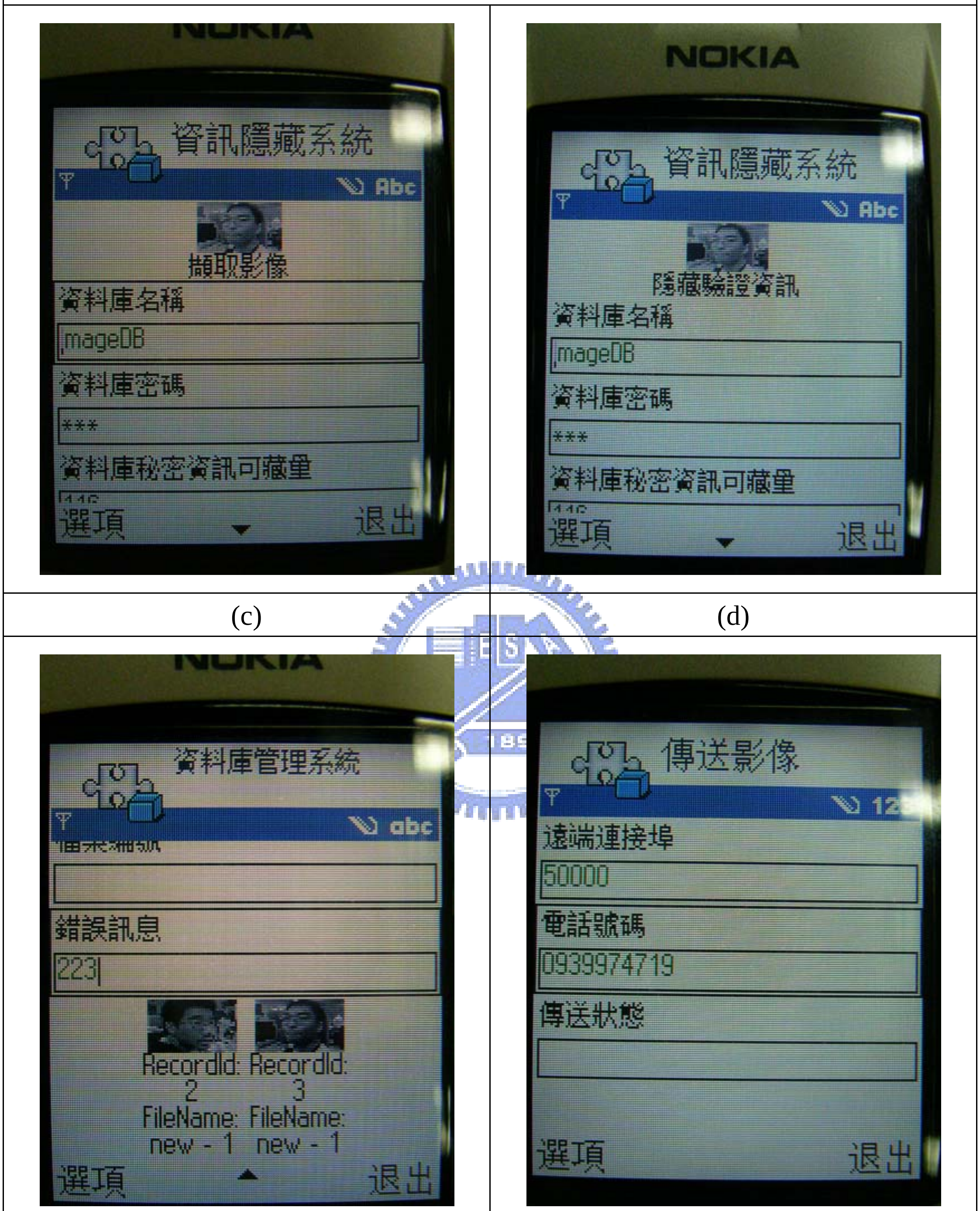
An example of our experiments is illustrated here, as shown in Figure 7.5. In our experiments, a protected captured image was transmitted on the platform of a cellular phone. While a user wants to take a picture, with the use of the proposed system, a captured image can be taken, as illustrated in Figure 7.5(b). After the process of embedding authentication signals in the captured image is completed, the user can transmit the image to others. On the receiver site, the receiver also has to key in a user key into the proposed system to verify the validity of the received image, as illustrated in Figure 7.5(i).



(a) (b)

Figure 7.5 An experimental result. (a) Three icons of the proposed system. (b) Taking a picture. (c) A captured image. (d) Embedding authentication signals. (e) A captured image in the database. (f) The transmission system on the sender site. (g) The receiving system on the receiver site.

(h) Loading of the received captured image. (i) A success authentication with a user key 123. (j) A failed authentication with a user key 12. (continued)



(c) (d)

(e) (f)

Figure 7.5 An experimental result. (a) Three icons of the proposed system. (b) Taking a picture. (c) A captured image. (d) Embedding authentication signals. (e) A captured image in the database. (f) The transmission system on the sender site. (g) The receiving system on the receiver site. (h) Loading of the received captured image. (i) A success authentication

with a user key 123. (j) A failed authentication with a user key 12. (continued)

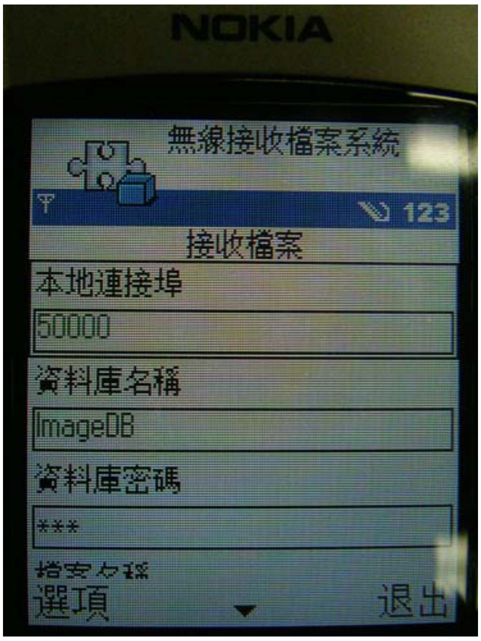
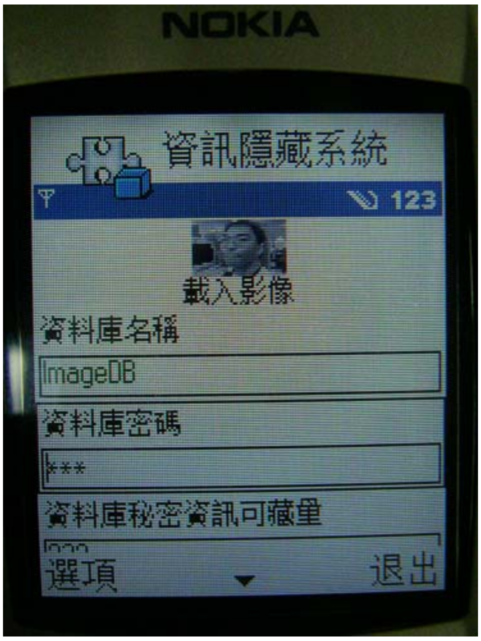
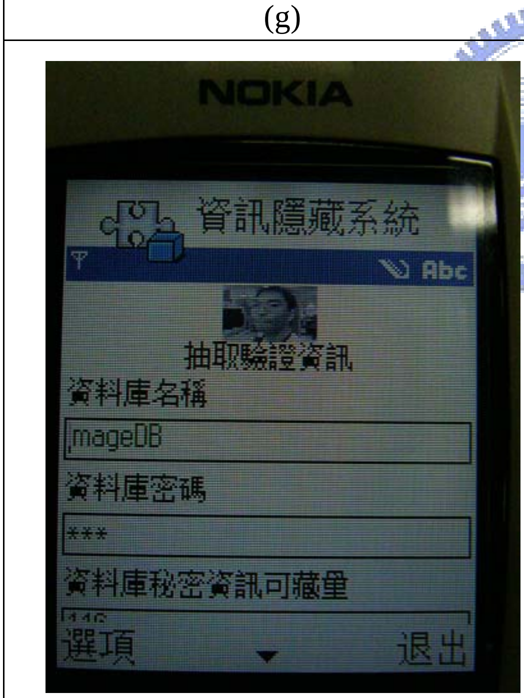
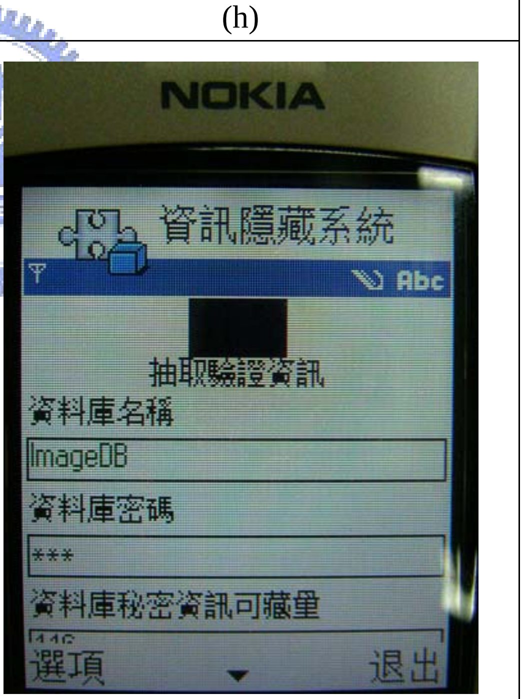
 無線接收檔案系統 123 接收檔案 本地連接埠 50000 資料庫名稱 ImageDB 資料庫密碼 *** 檔案名稱 選項 退出	 資訊隱藏系統 123 載入影像 資料庫名稱 ImageDB 資料庫密碼 *** 資料庫秘密資訊可藏量 選項 退出
(g)	(h)
 資訊隱藏系統 Abc 抽取驗證資訊 資料庫名稱 mageDB 資料庫密碼 *** 資料庫秘密資訊可藏量 選項 退出	 資訊隱藏系統 Abc 抽取驗證資訊 資料庫名稱 ImageDB 資料庫密碼 *** 資料庫秘密資訊可藏量 選項 退出
(i)	(j)

Figure 7.5 An experimental result. (a) Three icons of the proposed system. (b) Taking a picture. (c) A captured image. (d) Embedding authentication signals. (e) A captured image in the database. (f) The transmission system on the sender site. (g) The receiving system on the receiver site. (h) Loading of the received captured image. (i) A success authentication with a user key 123. (j) A failed authentication with a user key 12.

(continued)

7.4 Summary and Discussions

In this chapter, an authentication method for captured images on the platform of a cellular phone is proposed and experimented. If the authentication method only adopted a user key to generate random integers, illicit users could intercept transmitted images and modify them by copying the two least significant bits of each pixel of intercepted images to produce fake images for misrepresentation. The receiver cannot find out any difference between them.

With the use of a corresponding mean value of a 4×4 block and a user key, the security of the proposed method is improved and users can verify the fidelity of suspicious captured images without using authentication signatures.

Chapter 8

Conclusions and Suggestions for Future Works

8.1 Conclusions

In this study, we have proposed several data hiding methods for various application purposes, such as covert communication, authentication, and copyright protection. And some of them are implemented on the platform of a cellular phone in addition to on personal computers.

For covert communication, three methods for two different application platforms have been proposed. First, an active covert communication method implemented on a web page has designed to transmit large-volume secret messages using MPEG videos as cover media on the platform of a personal computer. Users can get secret messages from the public Internet more securely and more easily. Second, an active covert communication method which is also implemented on a web page has proposed to transmit secret messages using images as cover media on the platform of a cellular phone. Users can get secret messages from the public wireless network securely and easily. Finally, a method implemented on the platform of a cellular phone has been designed to transmit large-volume secret messages using multiple images as cover media. Users can get and transmit secret messages to each other via the proposed system. These three methods are also capable of verifying the fidelity of hidden secret messages.

For copyright protection, two active copyright protection methods using digital watermarking techniques have been proposed. Both of these two methods can be used to protect MPEG videos on a web page. One method transforms removable visible watermarks into invisible ones on the MPEG videos. Multimedia providers can use this method to check if a user, who wants to see videos, has an authentic key. Another method transforms invisible watermarks to visible ones on the MPEG videos. Multimedia providers can use this method to prevent illicit users from downloading and editing the videos for misrepresentation.

For authentication, two methods for two different application platforms have been proposed. First, an active authentication method implemented on a web page has been proposed to verify the integrity and the fidelity of MPEG videos on a web page. Users can obtain and authenticate the MPEG videos with work assignments pasted on a public web page without the need of installing authentication programs. Second, a method implemented on the platform of a cellular phone was proposed to authenticate images which are captured by a camera built in a cellular phone. Users can transmit captured images and utilize the proposed system to verify the fidelity of them.

8.2 Suggestions for Future Works

Several suggestions for future researches are enumerated as follows.

1. Active information hiding techniques, such as covert communication, copyright protection and authentication of MPEG videos, may be integrated in a new method.
2. Active information hiding applications may be developed on different media, such as text, audio, image, and video.
3. Active information hiding applications may be developed on more platforms like PDA's and other mobile devices.

4. Passive information hiding techniques on the platform of a cellular phone may be extended to deal with more types of multimedia and the latest technology can be utilized to transmit data in a faster way.

References

[1] J. J. Chae and B. S. Manjunath, "Data Hiding in Video," *Proceedings of IEEE International Conference of Image Processing*, Kobe, Japan, vol. 1, pp. 311-315, Dec 1999.

[2] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," *Proceedings of the IEEE*, vol. 87, issue: 7, pp. 1079-1107, Jul. 1999.

[3] B. G. Mobasseri et al., "Content Authentication and Tamper Detection in Digital Video," *Proceedings of IEEE International Conference on Image Processing*, Vancouver, BC, Canada, vol. 1, pp. 458-461, Sept. 2000.

[4] P. Yin and H. H. Yu, "A Semi-fragile Watermarking System for MPEG Video Authentication," *IEEE International Conference on Acoustics, Speech, and Signal Processing*, Orlando, Florida, USA, vol. 4, pp. 3461-3464, May 2002.

[5] M. Schneider and S. F. Chang, "A Robust Content Based Digital Signature for Image Authentication," *Proceedings of IEEE International Conference on Image Processing*, Lausanne, Switzerland, vol. 3, pp. 227-230, Sept. 1996..

[6] S. P. Mohanty et al., "A DCT Domain Visible Watermarking Technique for Images," *Proceedings of IEEE International Conference on Multimedia and Expo*, New York, NY, USA, vol. 2, pp. 1029-1032, Aug 2000.

[7] P. M. Chen, "A Visible Watermarking Mechanism using a Statistic Approach," *Proceedings of 5th International Conference on Signal Processing*, Beijing, China, vol. 2, pp. 910-913, Aug. 2000.

[8] J. Meng and S. F. Chang, "Embedding Visible Video Watermarks in the Compressed Domain," *Proceedings of IEEE International Conference on Image*

Processing, Chicago, IL, USA, vol. 1, pp. 474-477, Oct. 1998.

[9] Shan A. and Salari E., "Real-time Digital Video Watermarking," *Proceedings of IEEE International Conference on Consumer Electronics,* Los Angles, USA, pp. 12-13, June 2002.

[10] H. Y. Chen and W. H. Tsai, "Verification of MPEG Video Contents by Random Signal Hiding," *IPPR Conference on Computer Vision, Graphics, and Image Processing*, Kinmen, Taiwan, pp. 692-701, Aug. 16-18, 2003.

[11] D. C. Lou and J. L. Liu, "Steganographic Method for Secure Communications," *Computers and Security*, Vol. 21, Issue 5, pp. 449-460, October 1, 2002.

[12] E. H. Adelson, "Digital signal encoding and decoding apparatus," U.S. Patent 4939515, 1990.

[13] Y. K. Lee and L. H. Chen, "High capacity image steganographic model," Vision, Image and Signal Processing, IEE Proceedings-, Vol. 147, No. 3, pp. 288-294, June 2000.

[14] Dumitrescu S., Xiaolin Wu and Memon N., "On steganalysis of random LSB embedding in continuous-tone images," *Proceedings of International Conference on Image Processing*, New York, USA, Vol. 3, pp. 641-644, September 22-25, 2002.

[15] H. H. Yu, et al., "Smart Media: empower media with active data hiding," *Proceedings of 6th International Computer Science Conference on Active Media Technology*, Hong Kong, China, Vol. 2252, pp. 5-16, December 19-29, 2001.

[16] C. Y. Yin, "Copyright and Annotation Protection in Digital Museums by Using Data Hiding, Watermarking, and Image Authentication Techniques," *Master Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, June, 2001.

[17] Y. H. Chang, "New Methods and Applications of Data Hiding in Images,

Text-Type Documents, and Web Pages," *Master Thesis*, Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan, June, 2003.