การประยุกต์ใช้เทคโนโลยีไวรัสในกลไกการป้องกันข้อมูลเสีย

นายกุลภัทร ธีรอังคณานนท์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์และสารสนเทศ ภาควิชาคณิตศาสตร์
คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2553

APPLYING VIRUS TECHNOLOGY IN AUDIO PROTECTION MECHANISM

Mr. Kullapat Theera-angkananon

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Science Program in Computer Science and Information

Department of Mathematics

Faculty of Science

Chulalongkorn University

Academic Year 2010

Thesis Title	APPLYING VIRUS TECHNOLOGY IN AUDIO PROTECTION MECHANISM
By	Mr. Kullapat Theera-angkananon
Field of Study	Computer Science and Information
Thesis Advisor	Assistant Professor Pattarasinee Bhattarakosol, Ph.D.

Accepted by the Faculty of Science, Chulalongkorn University in Partial Fulfillment of the Requirements for the Master's Degree

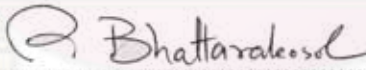
..... Dean of the Faculty of Science

(Professor Supot Hannongbua, Dr.rer.nat.)

THESIS COMMITTEE

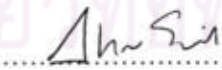
..... Chairman

(Assistant Professor Nagul Cooharojananone, Ph.D.)



..... Thesis Advisor

(Assistant Professor Pattarasinee Bhattarakosol, Ph.D.)



..... External Examiner

(Assistant Professor Ohm Sornil, Ph.D.)

กุลภัทร ธีรอังคณานนท์: การประยุกต์ใช้เทคโนโลยีไวรัสในกลไกการป้องกันข้อมูลเสียง. (APPLYING VIRUS TECHNOLOGY IN AUDIO PROTECTION MECHANISM) อ. ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ.ดร. ภัทรสินี ภัทรโกศล, 63 หน้า.

อินเทอร์เน็ตเป็นเครือข่ายการติดต่อสื่อสารขนาดใหญ่ที่มีการเชื่อมโยงกันทั่วโลก จึงทำให้ผู้ใช้งานทั่วไปนั้นสามารถเข้าถึงข้อมูลดิจิทัลต่างๆ เช่น ไฟล์เพลง MP3 ได้โดยง่ายจึงเป็นช่องทางที่ทำให้ผู้ไม่ประสงค์ดีลักลอบขโมยข้อมูลหรือละเมิดลิขสิทธิ์ข้อมูลดิจิทัลก่อให้เกิดปัญหาการละเมิดทรัพย์สินทางปัญญาของข้อมูลดิจิทัล วิธีการป้องกันลิขสิทธิ์ข้อมูลดิจิทัลหลากหลายวิธีได้ถูกนำเสนอขึ้นมาเพื่อป้องกันการละเมิดเหล่านี้ แต่เป็นที่น่าเสียดายที่มันกลายเป็นสิ่งชักจูงให้ผู้ไม่ประสงค์ดีทำลายกลไกการป้องกันต่างๆ ดังนั้นโครงงานนี้จึงได้นำเสนอเทคนิคการป้องกันข้อมูล BENPro สำหรับป้องกันไฟล์เสียง เช่น ไฟล์สกุล MP3 จากการทำสำเนา หรือแจกจ่ายโดยผู้ที่ไม่มีสิทธิ์ จุดประสงค์หลักของโครงงานนี้ก็คือกลไกการป้องกันข้อมูลนั้นไม่สามารถถูกตรวจพบได้โดยผู้ไม่หวังดีและผู้ใช้งานทั่วๆไป ผลจากการทดลองชี้ให้เห็นว่าผู้ใช้งานส่วนใหญ่เชื่อว่าปัญหาที่เกิดขึ้นจากการใช้งานโดนผิดวิธีนั้น เกิดจากกลไกในการเชื่อมต่อและรับส่งข้อมูล มากกว่าที่จะเป็นกลไกทางการป้องกันข้อมูล ดังนั้นการป้องกันการละเมิดลิขสิทธิ์ข้อมูลจึงได้ถูกดูแลรักษาไว้ตามที่ต้องการ

ภาควิชา คณิตศาสตร์..... ลายมือชื่อนิสิต.....
สาขาวิชา วิทยาการคอมพิวเตอร์และสารสนเทศ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก.....
ปีการศึกษา 2553.....

5273602423 : MAJOR COMPUTER SCIENCE AND INFORMATION

KEYWORDS : DIGITAL RIGHT MANAGEMENT / LABORATORY TESTING / ISO 9241-11 STANDARD / HUMAN-COMPUTER INTERACTION

KULLAPAT THEERA-ANGKANANON : APPLYING VIRUS TECHNOLOGY IN AUDIO PROTECTION MECHANISM. ADVISOR : ASST. PROF. PATTARASINEE BHATTARAKOSOL, Ph.D., 63 pp.

Internet is a global system of interconnected computer networks that helps users reach to all digital data, such as multimedia files. So, this leads to plagiarization, violation of copyrights and data over the Internet. Thus, the digital intellectual property becomes a big issue of the Internet sharing system. Various techniques have been proposed to protect these violations; unfortunately, they became the hackers' stimuli in breaking the protection mechanisms. Therefore, this thesis proposes a protection mechanism, Byte Encoding Protection (BENPro), for preventing an audio file, such as mp3 format from copying and distributing by illegal distributors. The aim of this thesis is that the protection mechanism cannot be recognized from hackers and users. The result of this experiment indicates that most users believe that the defects occur from the transfer mechanism rather than the protection mechanism. Thus, the protection of IP is maintained as expected.

Department : Mathematics Student's Signature .....

Field of Study : Computer Science and Information Advisor's Signature .....

Academic Year : 2010

Acknowledgements

I would like to acknowledge my thesis advisors, Assistant Professor Dr. Pattarasinee Bhattarakosol for helpful guidance and encouragement. She has suggested the solutions to many experimental problems and helped finish this thesis in time. Moreover, I would like to thank the staffs of the Advanced Virtual and Intelligent Computing (AVIC) Research Center for all their great support.

Finally I would like to thank my father, mother and friends for everything they suggested and supported me.

CONTENTS

PAGE

Abstract (Thai)……..…. iv

Abstract (English)……... v

Acknowledgements…… vi

Contents…… vii

List of Tables…… x

List of Figures…….. xi

CHAPTER

I. INTRODUCTION…….……..…… 1

1.1 Introduction……..…….. 1

1.2 Problem Description…….. 1

1.3 The Objective of Research…….. 2

1.4 The Scope of Study…….. 3

1.5 Expected Outcomes…… 3

1.6 The Benefits of Research…… 3

II. RELATED WORKS…..……... 5

2.1 Related Works…… 5

2.2 Principal of virus …….. 7

2.2.1 Spreading of computer virus..…….. 7

2.2.2 How virus infected system?..…… 8

2.2.3 How does virus working?..…… 8

2.3 MP3 format …….. 10

2.3.1 MP3 Structure..…….. 13

III. EXPERIMENTAL DESIGN AND METHODOLOGY…..…….. 14

3.1 Audio Preparation System (APS)…….…… 16

CHAPTER PAGE

3.1.1 Encoding Module……. 16
3.1.2 Embedding Module……..…. 17
3.2 Digital Media Access Controller…..……..……..…… 18
3.2.1 Extraction Module.……..…..……..……. 18
3.2.2 Decoding and Integrating Module ……..……..……..…. 19
3.2.3 How to Play the file……..……..…..…. 19
3.3 Steps for create protected audio files……..……..…… 24
3.3.1 Mechanism to create an encoded audio file…..……..……. 24
3.3.2 Mechanisms to create an embedded audio file ……..…..…. 26

IV. EVALUATIONS AND EXPERIMENTAL RESULTS ……..…….. 27
4.1 Evaluation Method ……..……..…… 27
4.2 Sample groups and testing condition …..……..……..…… 27
4.3 Software Evaluation ……..……..…… 27
4.4 Testing Hypothesis of Protection Mechanism ……..…… 29
4.4.1 Test of re-download the audio when it cannot be opened ..…. 29
4.4.2 Test of remove and quit using DMAC when it cannot open the audio file ……. 30
4.4.3 Test of find the crack or tools to fix the program when it cannot open the audio file ..…… 31
4.4.4 Test of realize the DMAC was protected when it cannot open the audio file from other sources …… 32
4.4.5 Test of realizes the downloaded audio file was encoded when it cannot be opened ……. 33
4.4.6 Test of realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened ……. 34
4.4.7 Test of thinking this data protection will reduce the hackers' motivation …….. 35

CHAPTER PAGE

4.4.8 Test of thinking the defect is an effect from the transfer mechanism rather than the protection mechanism ..…….. 36
4.4.9 Test of using DMAC and BENPro system was easy.....…… 37
4.4.10 Test of the quality of the played audio is the same as the original file.....…… 38
4.4.11 Test of General Aspects ..…… 39

V. CONCLUSIONS AND DISCUSSIONS……..... 42
5.1 Discussions ……..……..…… 42
5.2 Conclusions ……..……..…… 43

REFERENCES……..……..…….…..... 44
APPENDICES……..……..…….…..... 46
Appendix A The questionnaire satisfaction of applying virus technology on BENPro system……..…… 47
Appendix B Installation of BENPro protection system……... 48
Appendix C BENPro program manual guide……..…… 54
VITAE……..……..……..…….…..... 64

List of Tables

Table Page

4.1 Experimental results..... 39

List of Figures

Figure		Page
2.1	Virus appended to a program	8
2.2	Virus surrounding a program	9
2.3	Virus integrated to a program	9
2.4	MP3 Header Format	12
3.1	BENPro Protecting system architecture for audio files	15
3.2	Encoding technique	16
3.3	Embedding mechanism	17
3.4	Use case diagram of the BENPro system	20
3.5	Class diagram of the BENPro system	22
3.6	Sequence diagram of the BENPro system	22
3.7	Activity diagram of the BENPro system	23
3.8	Audio Preparation System.....	24
3.9	Encoding algorithm	25
3.10	Embedding algorithm.....	26
4.1	Digital Media Access Controller Program	29

CHAPTER I

INTRODUCTION

1.1 Introduction

Currently, there are tremendous Internet services available for the Internet users. However, these services are visible in various forms for users, such as web applications, ftp sites, or social networks. One common service is the entertainment media that users can access through the Internet channels. In addition, these entertainment media are protected by the Intellectual Property (IP) law and the media providers must not abandon this law. Many protection systems and mechanisms are implemented, but the most common solution is the use of the member system for the online media players. Unfortunately, the member system can be counted as the primary protection of the IP over the online distribution since the illegal usage occurs after the legal download finished.

Since the downloaded files cause problem of the IP intrusion, some encryption mechanisms are implemented and embedded into the media files before the download starts, such as digital signature, fingerprinting, and watermarking. The benefit of these protection methods is that the copied of all illegal files cannot be accessed by any illegal users. Unfortunately, these mechanisms are motivation for implementing the cracking mechanisms. Thus, it is like an endless chain rule of the IP protection.

1.2 Problem Description

Presently, the infringement of musical file types, especially .mp3 and .mp4, is widely occurred over the Internet, and it cannot be easily prevented. Hence, there are many researches and development of new techniques and methods to protect these file types. One of the existing methods is to manage and restrict the access right to a file for each user by implementing the member system. Unfortunately, the

protection cannot cover when members download files according to their right; then, distribute it without permission.

Although various techniques and methods have been proposed and installed in the real world, users of these multimedia files are able to detect. Thus, the protection mechanism becomes a stimulus for users who are also hackers because of the challenge in breaking the prevention mechanism. As a consequence, the implementing of these mechanisms should be blinded from these users as much as possible.

Based on the contents mentioned previously, the problems that are considered in this research are listed as follow.

1. Most of the available protection mechanisms cannot cover the illegal copied of the files.
2. Most of the available protection mechanisms can be detected by hackers.
3. Most of the protection mechanisms create motivation in breaking the encryption or protection techniques.

Referring to the problems above, this research presents a mechanism to protect the downloaded file from any faithless distributors under the objective of eliminating hackers' motivation. The proposed mechanism will not be obviously shown the blocking of the IP protection, but it can guarantee that users will not be able to use and distribute without authorization from the company.

1.3 The Objective of Research

In this thesis, the main point is to improve the protection mechanism that can prevent the unlawful usages of unauthorized users by applying a simple virus technology. Another objective is to indicate that if the protection mechanism was not detected by users, the motivation to break the encoding audio files will not exist.

1.4 The Scope of Study

As the fact that there are different digital media formats over the cyber world, such as .mp3, .mp4, and .wma, the research will focus only the audio file according to the size and popularity of use. In addition, in this research, the prototype system will be performed on only one type of the audio file format which is .mp3 although there are various types of audio files available over the digital world. The reason of choosing this format is because it is the most common usage and can be played by all media player software. However, the implemented mechanism is expected to be able to apply to other types of media.

After the implementation, the evaluation of the proposed solution is performed. The samples for this test are randomly selected from unknown population with and without computer technical background. The reason of choosing these two groups is based on the assumption that the motivation in hacking the protection mechanism may be different. Moreover, there are various age-ranges existed in each group, with the same distribution. However, all samples are Thai citizen.

There is no comparison of performance between available protection mechanism and the proposed mechanism because the protection mechanism of all commercial software cannot be found.

1.5 Expected Outcomes

The expected outcomes for this study are the protection mechanism preventing an audio file, such as .mp3 format from copying and distributing by illegal distributors. Additionally, the protection mechanism must not be recognized from any hackers and users.

1.6 The Benefits of Research

The benefits of this research will be as follows:

1) The new protection mechanism can prevent the unlawful usages of unauthorized users by applying a simple virus technology.

2) The motivation to break the encoding audio file will be decrease because the protection mechanism was not detected by users.

3) The intellectual property (IP) of the media is protected.

This thesis proposes a virus-based encoding technique, or byte encoding protection mechanism for preventing an audio file from copying and distributing by illegal distributors. Thus, Chapter II provides related works, and details of related theory, such as format of the .mp3. Chapter III will describe the architecture and the features of the proposed solution while the experimental results are elaborated in Chapter IV. Chapter V is the discussion, including conclusion and future works.

CHAPTER II

RELATED WORKS

2.1 Related Works

Digital right management, or DRM, is known as a set of technologies used by publishers to protect all digital media from an unauthorized access in order to maintain intellectual property that are distributed over the Internet or the digital world. Currently, the IP protection is a serious issue for any business companies who provide services in all kinds of digital media. The digital protection is the main concern of every business multimedia distributors since it is difficult to control after storing into a storage, such as hard disk, or CDs, or distributed over the Internet [1]. Thus, DRM is an important subject of all digital media servers.

Various techniques have been proposed to manage different kinds of digital media. The practical method has been proposed in the year 2004 by Louma and Vahtera [2], this paper stated that multiple agreements and the negotiations among actors must be concluded and signed before performing any protection and management processes. However, these agreements are ideal in the real world since users may break the agreement without intention.

According to Jonker and Linnartz [3], there are two fundamental concepts to secure these digital resources from unauthorized access. The first method is to encrypt content of these resources a certified mechanism and the private key concept. The other alternative method is to store these contents behind a specific device, such as firewall, including access keys. Although encryption methods and implementing of protection are applied when storing multimedia contents into media, these protections exclude the situation that the media is the Internet channel.

The research of [4] proposed a broadcast encryption method which enables media or broadcast-based distribution possible for any low-cost devices. Therefore, the media can be protected and using distributed over the Internet easily to any consumers. Moreover, this concept is applied to the consumer products, such as DVD-audio players and DVD recorders. The similar objective is applied to the research

of [5] who proposed the “family domain” concepts. Additionally, in the year 2004, the “Authorized Domain” technique is proposed by [6].

Moreover, the integration between the digital right management and fingerprinting system had been proposed by [7] in the year 2006. This technique embedded a fingerprinting code generated from a fingerprinting server into the audio content, this fingerprint code will be verified when a client requests the file. In addition, in the year 2009, [15] proposed a framework to analyze collusion attacks on fingerprinting systems and improve a new technique called Anti-Collusion Dither (ACD) which random dither signal to the compressed host before embedding so as to make the effective host signal appear more continuous.

Several models [10], [11], [12], have been proposed which have used different technologies like watermarking, fingerprinting [11], cryptography etc. There are several of techniques which have been proposed for copyright protection of digital content. One general but efficient method is the use of a watermark technology. The digital watermark is a signal embedded in the multimedia content. This technology aims to protect the digital media contents. It gives the contents available freely for download as a preview. Thus, when this technique is applied to the multimedia files, it has to be modified as proposed by [8][9]. In [8], the proposed technique is embedded the removable watermark into the audio files that causes the audio files to be in the lower quality. Based on the similar objective, [9] proposed an unconventionally invertible perceptible watermarking method based on DCT (Discrete cosine transform) coefficients. This mechanism can be used to protect the audio content by two methods. The first method, “perceptible watermark”, aims to reduce the audio quality by adding an audible removable watermark as a part of the audio signal. The second method, “imperceptible watermark”, is the use of a secret key for digital right management control. Furthermore, the technique of [13] guarantees that the received data is the original copy for their receivers.

Since DRM is a significant factor related to the business operations, so [14] proposed a scheme that can convert one DRM’s content to other DRM’s content. They provide the conversion process which is separated into two steps. The first step is mutual authentication to determine whether it is a legal DRM, to verify the target user,

and to check the license to find permission. The second step is the conversion from the source DRM content to the target DRM content. The conversion means that the specific DRM content is converted into neutral DRM content format. This content format provides the secure structure to protect the DRM data which offers beneficial for providers and users; providers can extend their service area without opening their secret and users can freely enjoy using audio content without considering that DRM system is used on their audio player.

Although various methods have been mentioned above, integration of DRM and fingerprinting in [7], removable watermarking in [8], and etc., most of them are complicated and might not be practical. Moreover, the significant issue of these researches is the noticeable of protection methods that users might recognize, especially audio files. This recognition is a motivation for some users who love challenging in breaking the protection mechanism. Therefore, the destruction of the protection rules begins. According to this motivation, this research proposes a mechanism that most users are hardly realized as the protection mechanism. Therefore, the IP protection is maintained.

2.2 Principal of virus

A computer virus is a program that was created which has ability to spread from one computer system to another computer system. Spreading of computer virus will be embedded with a computer program or hiding in the memory, which can be the main memory or the cache memory.

2.2.1 Spreading of computer virus

Virus can infect to a computer via a diskette or a flash drive, when the infected device is used. Then, virus will transfer to the computer. Another way to infect is spreading itself through the computer network; the virus uses the transferred packets such as E-mail or downloaded files from un-trustable sources.

2.2.2 How virus infected system?

By far one of the most common way, a computer becomes infected is the user accepts all operations without reading the prompt or understand what it is asking.

Some common example:

1. While browsing the Internet, an Internet advertisement or window appears that says “your computer is infected” or that “a unique plug-in is required”. Without fully understanding what it is getting and click accept the prompt.
2. When installing or updating a program, users is prompted (often checkboxes already checked) to install an additional program that the users may not want and that program was designed to monitor their usage of the program.
3. Downloading any other software from the Internet can also contain viruses and other malware. When downloading any software (programs, utilities, games, updates, demos, etc.), make sure users are downloading the software from a reliable source and while installing it, users are reading all prompts about what the program is putting on your computer.

2.2.3 How does virus working?

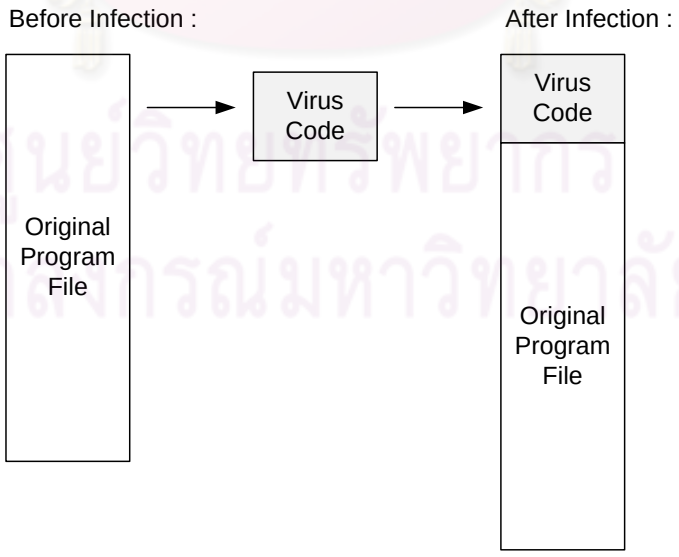


Fig.2.1 Virus appended to a program

- **Append virus**: This way virus will attach with a target program. When the target program was executed, the virus will be executed before the target program after that the target program will working properly, as showing in Fig. 2.1.

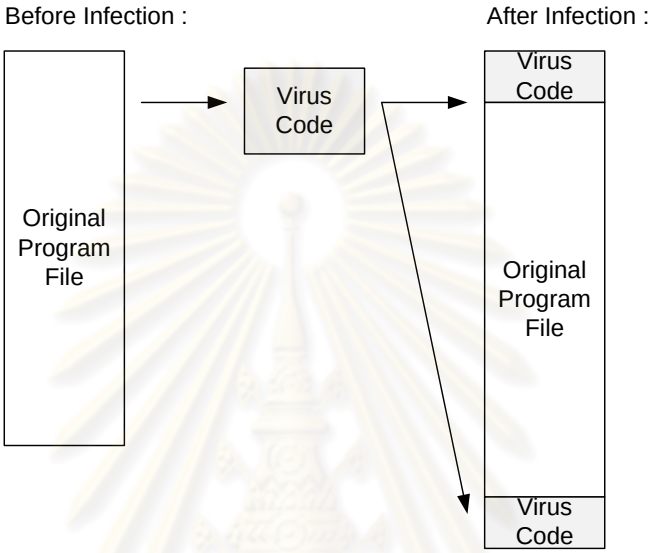


Fig.2.2 Virus surrounding a program

- **Virus that surrounds a program**: In this way virus will embedded to the first and the last positions of the target program to control the processes before the target program started and after it finished, as see in Fig. 2.2.

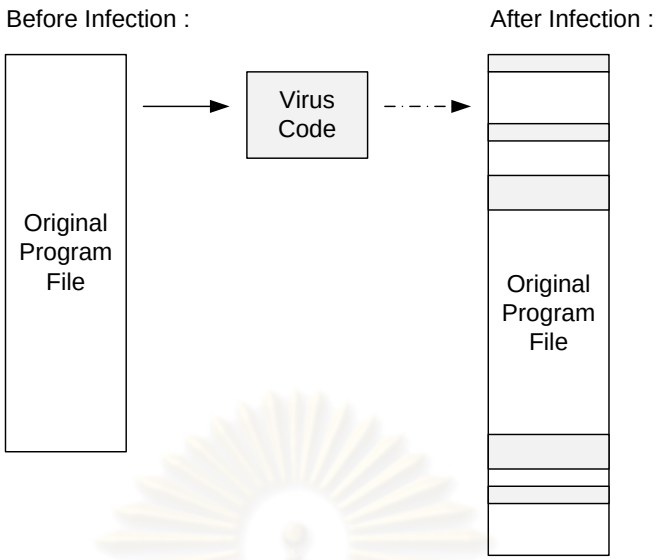


Fig.2.3 Virus integrated to a program

- **Integrated virus and replacement**: the virus program will be embedded and replaced to the some part of a target program as see in Fig. 2.3.

2.3 MP3 format

MPEG-1 or MPEG-2 Audio Layer III, more commonly referred to as .mp3, is a patented digital audio encoding format using a form of lossy data compression. It is a common audio format for consumer audio storage, as well as a de facto standard of digital audio compression for the transfer and playback of music on digital audio players.

.mp3 is an audio-specific format that was designed by the Moving Picture Experts Group as part of its MPEG-1 standard and later extended in MPEG-2 standard. The first MPEG subgroup – *Audio* group was formed by several teams of engineers at Fraunhofer IIS, University of Hannover, AT&T-Bell Labs,Thomson-Brandt, CCETT, and others. MPEG-1 Audio (MPEG-1 Part 3), which included MPEG-1 Audio Layer I, II and III was approved as a committee draft of ISO/IEC standard in 1991, finalized in 1992 and published in 1993 (ISO/IEC 11172-3:1993). Backwards compatible MPEG-2 Audio (MPEG-2 Part 3) with additional bit rates and sample rates was published in 1995 (ISO/IEC 13818-3:1995).

The use in .mp3 is a lossy compression algorithm is designed to greatly reduce the amount of data required to represent the audio recording and still sound like a faithful reproduction of the original uncompressed audio for most listeners. An .mp3 file that is created using the setting of 128 kbit/sec will result in a file that is about 11 times smaller than the CD file created from the original audio source. An .mp3 file can also be constructed at higher or lower bit rates, with higher or lower resulting quality.

The compression works by reducing accuracy of certain parts of sound that are considered to be beyond the auditory resolution ability of most people. This method is commonly referred to as perceptual coding. It uses psychoacoustic models to discard or reduce precision of components less audible to human hearing, and then records the remaining information in an efficient manner.

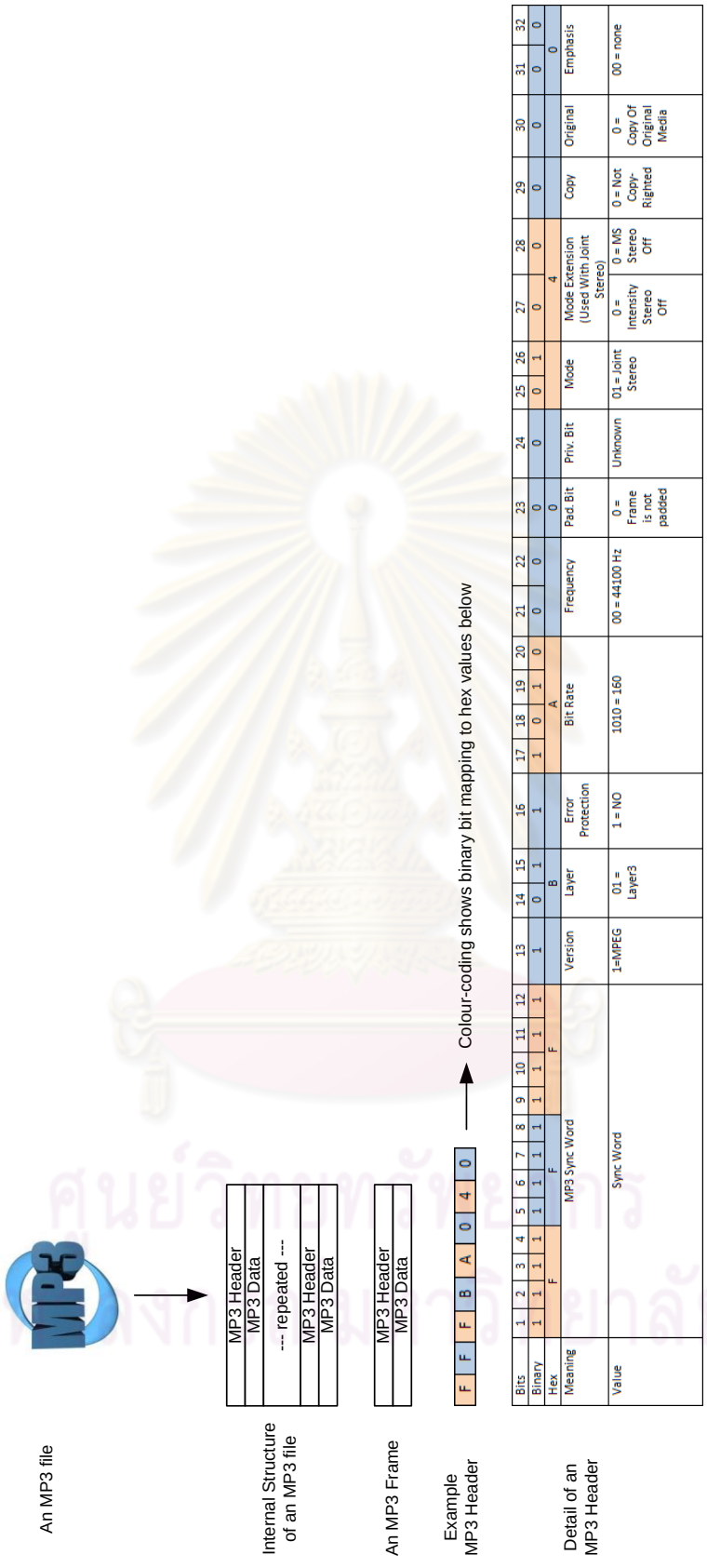


Fig.2.4 MP3 Header Format

2.3.1 MP3 Structure

An .mp3 file is constructed from multiple .mp3 frames, which can be classified as a header and a data block. This sequence of frames is called an elementary stream. Frames are not independent items ("byte reservoir") and, therefore, cannot be extracted on arbitrary frame boundaries. The .mp3 data blocks contain the (compressed) audio information in terms of frequencies and amplitudes. Fig.2.4 shows that the .mp3 Header consists of a sync word, which is used to identify the beginning of a valid frame. This is followed by a bit indicating that this is the MPEG standard and two bits that indicate that layer 3 is used; hence MPEG-1 Audio Layer 3 or .mp3. After this, the values will be differ, depending on the .mp3 file. ISO/IEC 11172-3 defines the ranges of values for each section of the header along with the specification of the header. Currently, most .mp3 files contain ID3 metadata, which precedes or follows the .mp3 frames; as noted in the Fig. 2.4.

CHAPTER III

EXPERIMENTAL DESIGN AND METHODOLOGY

In this research, the member system of audio files downloading is applied as a fundamental protection mechanism for the digital right management over the Internet. However, in order to fortify the Intellectual Properties (IP) of the digital media over the Internet, the mechanism called Byte Encoding Protection (BENPro) is proposed after the media has been downloaded from a provider. This proposed system of the digital media provider consists of two subsystems. The first subsystem is responsible for digital media encoding, while the second subsystem is the digital media access controller. Fig.3.1 shows the BENPro system architecture of the protecting technique.

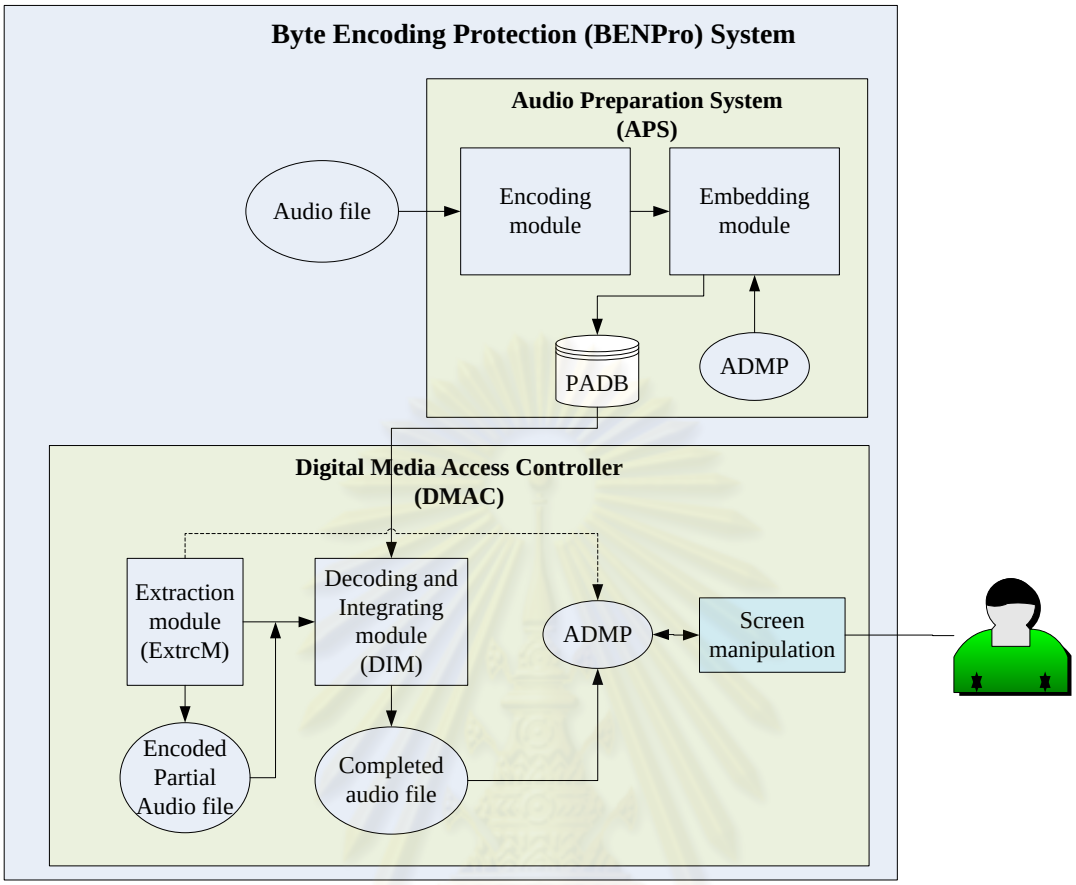


Fig.3.1 The BENPro Protecting system architecture for audio files

According to Fig. 3.1, the audio providers must start their services by passing all audio files to the Audio Preparation System (APS) before broadcasting through the Internet. In this system, the audio files will be encoded and embedded with an executable file. Therefore, this process is the first step of the protection mechanism because users will obtain the encoding file when requested the access.

Since the BENPro mechanism is relied on the member system, all members must install the Digital Media Access Controller (DMAC) as if it is the media player of the BENPro system. The system is responsible for decoding and playing the requested audio file downloaded from the Internet. Moreover, this system will delete the necessary information that the DMAC uses to play the audio after the play is terminated. Therefore, the functions of the DMAC are the second protection step for all

audio providers. Details of all these systems, the APS and the DMAC, are described as follow.

3.1 Audio Preparation System (APS)

The APS is responsible for creating all protected audio files. It consists of two methods inside this system: the encoding, and the embedding algorithm. This APS is the important part in preparing the original files before they are retrieved and accessed over the Internet. Although users can obtain the digital files by authorized download but they cannot distributed the full version of audio files to an unauthorized person because the proposed algorithms have extracted some part of the audio files and stored it in the Partial Audio Database (PADB). Details of all these processes are described in the next section.

3.1.1 Encoding Module

It is necessary that before all digital media are distributed over the Internet, the providers must encode these files using some available techniques. One interesting encoding technique is the swapping bytes among contents of the file.

Every multimedia file will contain fields to inform the file format for media players. Thus, changing the file content by switching among bytes, as shown in Fig.3.2, will change the values of these meaning fields. This is the first step of the data protection process for audio files. When these encoded audio files are executed by various media players, such as windows media player, winamp, and aimp player, most of these media players present the low quality of sound, including the annoying signal, or cannot be recognized, by any media players.

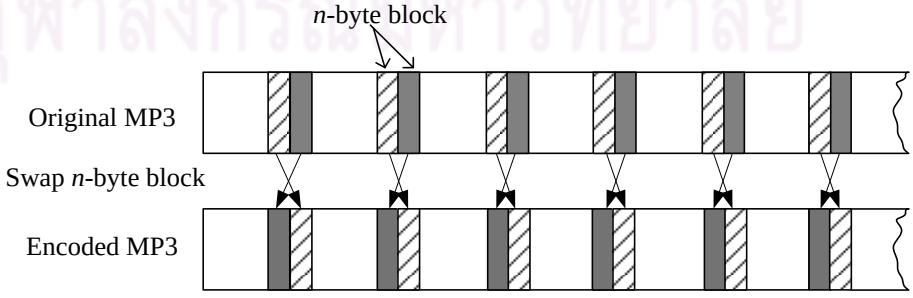


Fig. 3.2 Encoding technique

Although the contents are changed, it cannot guarantee that hackers are not able to swap them back to normal. So, the second module, embedding module, in the APS is applied.

3.1.2 Embedding Module

This module is implemented to serve the objective that the downloaded files must not be able to run by an unauthorized person under an authorized download. The concept of this module is based on a security protection mechanism, byte stuffing of the transferred packet over a network. Nevertheless, the set of stuffing bytes in this research is an executable file, named as the ADditional Music Player (ADMP). This ADMP will be partitioned in *n*-block bytes as same as the swapping bytes, see Fig. 3.3.

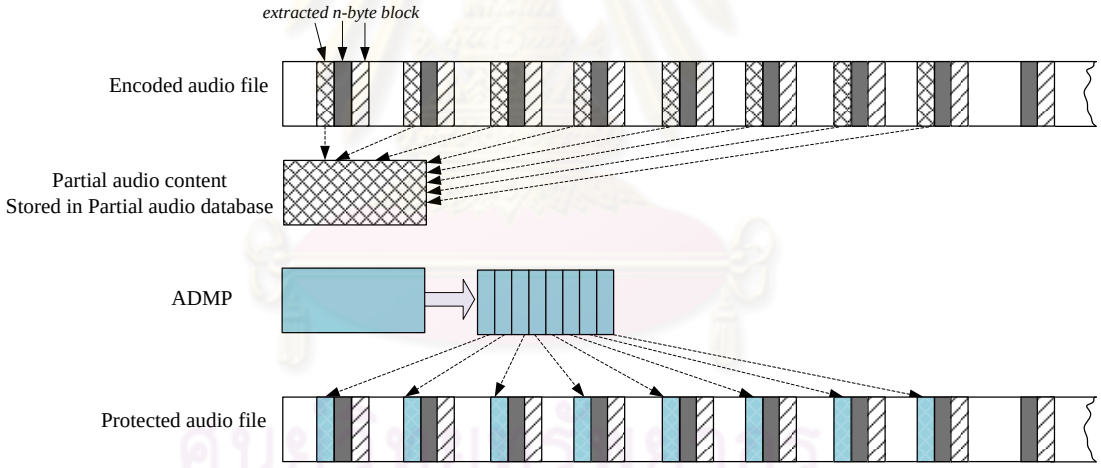


Fig. 3.3 Embedding mechanism

The mechanism of this module is that the audio file will be segmented into small pieces, as shown in Fig. 3.3. However, the total amount of segments will be equal to the size of the ADMP executable file which will be embedded into the same locations of all segmented contents. After finishing the segmentation, these segments will be stored in the Partial Audio DataBase (PADB). These parts of the audio files will

be called by the ADMP whenever users request for accessing the file under a control of the second system, the DMAC.

3.2 Digital Media Access Controller (DMAC)

The second part of the BENPro is the most important part after the audio file was encoded by the APS. The execution of this system starts when users select an audio content with permission through the DMAC interface. Then, the downloading mechanism will start, the encoding audio will be sent to the user system, called as a client. This encoding audio will be extracted to obtain the ADMP as a back-end process by the DMAC system. Then, the ADMP will perform its task by playing the audio files as requested while the network connection must be available. Additionally, all clients can control the play through the DMAC interface, as shown in Fig. 4.1 and details are described in Chapter 4.

According to the functions of the DMAC mentioned above, this system must be installed in the user's computer after the membership is assigned and it consists of 2 important modules. The first part is the Extraction Module (ExtrcM) where the ADMP will be reassembled and temporary saved in the user's hard disk. The second part is the Decoding and Integrating Module (DIM); this module will reorganize the encoded audio file to be similar to the original one. Moreover, it is responsible for integrating the remaining part of the requested audio file to the decoded content. Thus, the final outcome from the process of the DIM is the original audio file that is ready to be played. Details of these modules are described as follows.

3.2.1 Extraction Module (ExtrcM)

This module is an executable file that will be run when users call for a play. The DMAC will start this ExtrcM after the download of the selected audio finished and the encoded audio is stored in a temporary space. The ExtrcM will extract the ADMP out from the content of the audio file, remaining only the pure encoded content; these output files will be stored in the temporary space in the user's hard disk. The ADMP will play the selected audio file as a background process without user's interference.

3.2.2 Decoding and Integrating Module (DIM)

This module is an executable file which is hidden in the client's computer after installed the DMAC media player. It is used for reorganizing the audio file content, including reassembling the partial audio file from the server. In the process of reorganization, all swapped contents from the encoding process will be restored back to their original locations. However, this decoded file cannot be accessed by any media players until it will be integrated with the remaining part from the server site.

Within this module while the content is decoding, the remaining contents from the server site of the audio provider will be put back to their original locations. Thus, after finishing the process of the DIM, the audio file is ready to play.

3.2.3 How to Play the File?

After finishing the DIM module, the ADMP will run under the control of users via the user interface. The user interface sub-module is the interface that interacts with users when users want to control the play, such as play, pause, and stop the audio files. Whenever the user requests a play through the interface module, the request will be sent to the ADMP to run the audio file obtained from the DIM process. Nevertheless, this audio file will be erased when the user exits the playing mode or closes the program. Fig. 3.4 illustrates the use case of the system. Furthermore, the class diagram of the whole system presents in Fig 3.5.

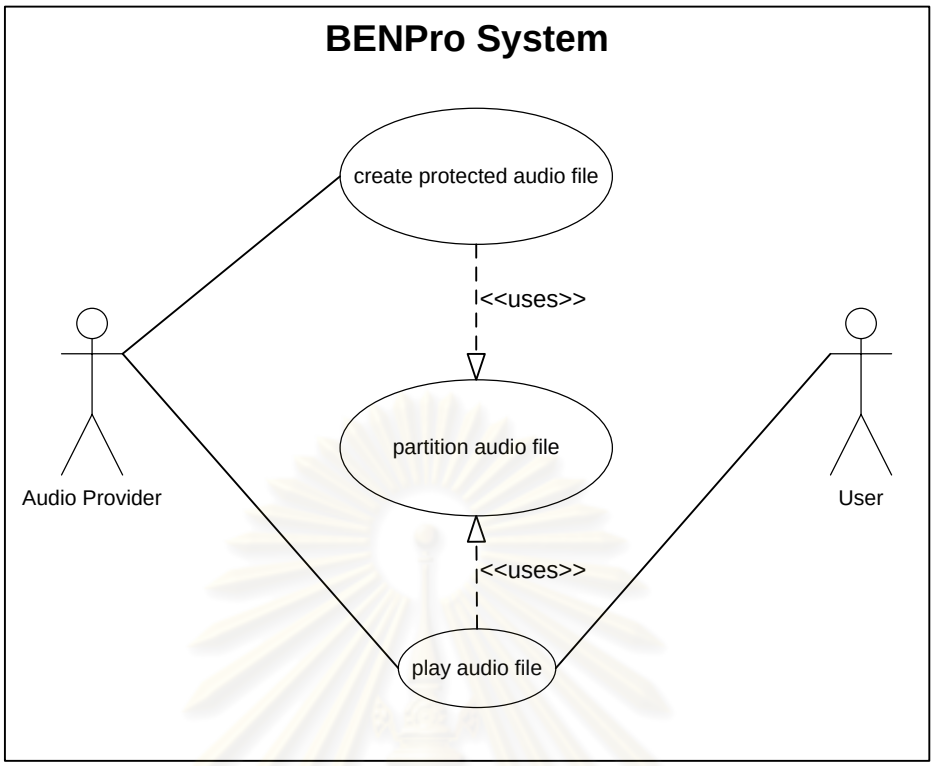


Fig. 3.4 Use case diagram of the BENPro system

Use case diagram: Template

- Use case name: BENPro System
- Participant actors:
  - Audio provider
  - User
- Entry condition:
  - User plays an audio file using BENPro System.
- Flow of events
  - An audio provider creates the protected audio files using encoding module.
  - The process of create protected audio file calls the partition-audio-file process that will segment the audio file into small pieces and store it in database then embedded the ADMP into the same locations of all segmented contents.
  - The audio provider grants permission for retrieving the protected audio file.

- A user plays the protected audio file using the DMAC.
- The process of the play-audio-file extracts the ADMP player out from the protected audio content; then, the process of the partition-audio-file will be called to retrieve the partial audio contents and merge them back to the audio file.
- The ADMP will be executed via the back-end process to start the playing audio file.
- The user presses the stop button to stop playing audio file.

- Exit conditions
  - User presses Stop button.

Use case diagram: Scenarios

- Scenario Name: BENPro
- Participating actor instances:
  - Ball: The audio provider
  - Nitch: User
- Flow of events
  - Ball put the original audio file into BENPro system to created protected audio file using encoding and embedding module.
  - Nitch retrieve the protected audio file from Ball.
  - Nitch start playing the protected audio file with DMAC.
  - The DMAC extracted the ADMP out from protected the audio file.
  - Nitch tries to use others features of the DMAC, such as pause and stop function.
  - Nitch exits the DMAC program.

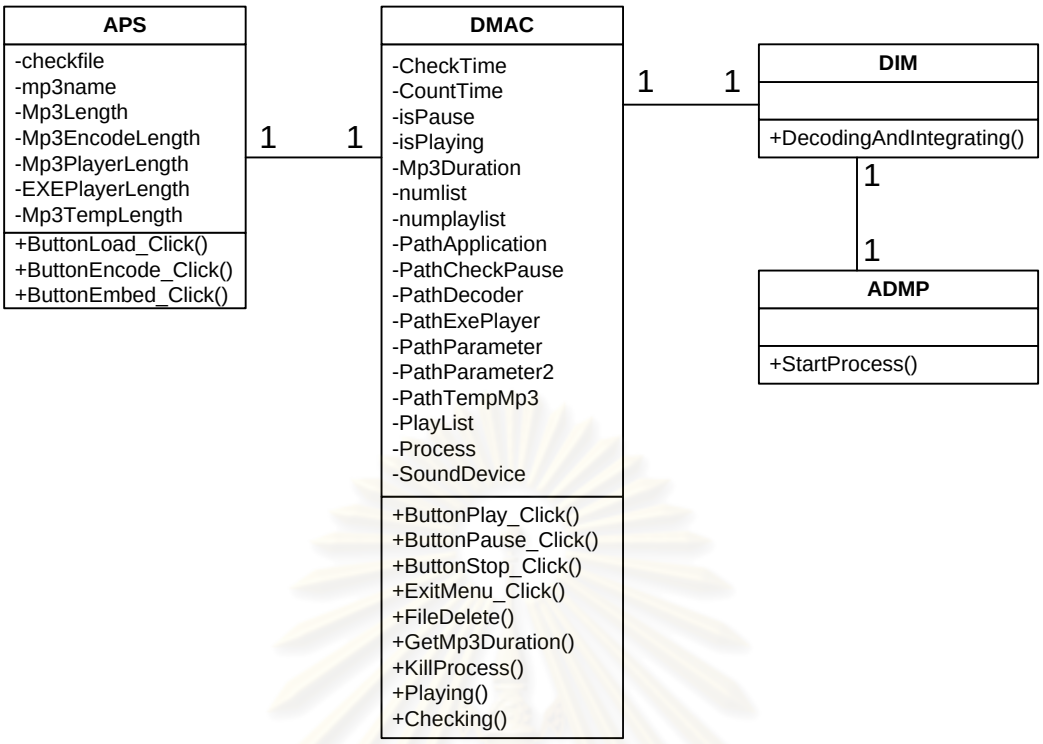


Fig. 3.5 Class diagram of the BENPro system

In the Fig. 3.6, it will demonstrate the sequence diagram of the playing process.

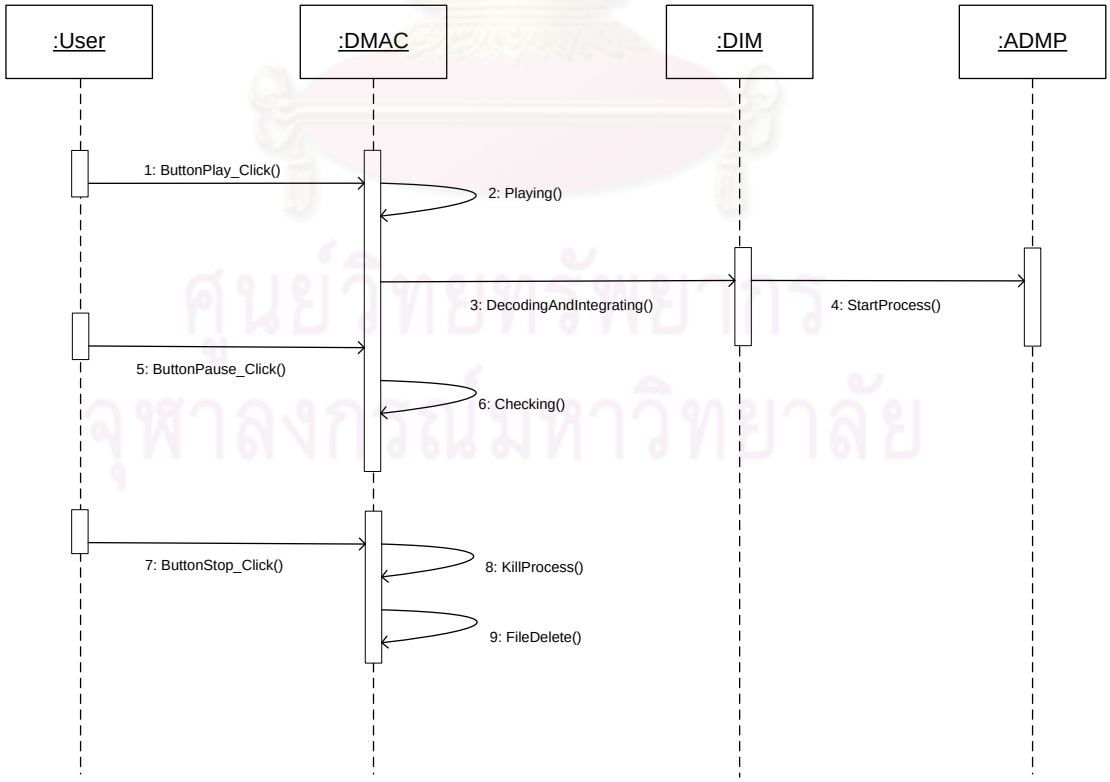


Fig. 3.6 Sequence diagram of the BENPro system

From Fig. 3.6, the process of the play, pause, and stop process can be describes as follow.

(1) Users press a play button on the DMAC interface.

(2) The DMAC starts the playing function and commands to manipulate the play will be sent to the DIM module.

(3) A protected audio file will be decoded and integrated with partial audio content and the ADMP will be extracted from the protected audio file.

(4) The ADMP will execute the play command.

(5) Users press a pause button on the DMAC interface.

(6) The DMAC will update the configuration file and send the pause command to the ADMP.

(7) Users press a stop button on the DMAC interface.

(8) The DMAC will kill the ADMP's process.

(9) All files in the temporary storage will be deleted.

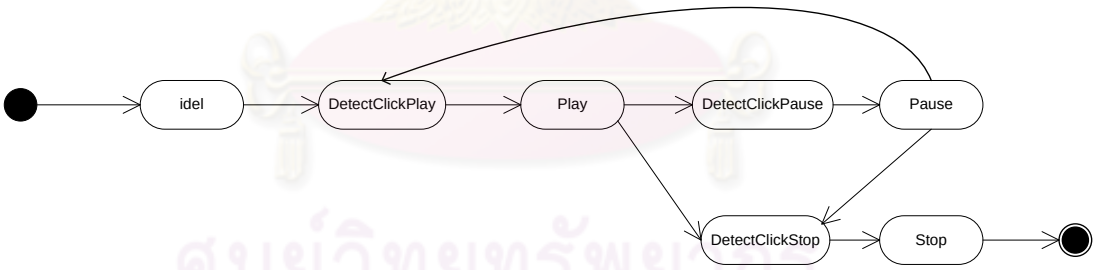


Fig. 3.7 Activity diagram of the BENPro system

According to the activity diagram, Fig. 3.7, the first step is that user press a command button on the DMAC interface. Once an icon is pressed, the DMAC calls the playing function and commands to manipulate the play are sent to DIM module. Then, a protected audio file is decoded and integrated with the partial audio content. Moreover, the ADMP is extracted from the protected audio file. After finishing the decoding and integrating, the ADMP executes the command as requested. When users

press a pause button on the DMAC interface, the DMAC will update the configuration file which is stored in the user computer and send the pause command to the ADMP. On the other hand, if users press a stop button on the DMAC interface, the DMAC will kill the ADMP's process and all files in the temporary storage such as the ADMP, the configuration files, the completed audio file, and the partial audio file will be eliminated from the user hard disk.

3.3 Steps for create protected audio files

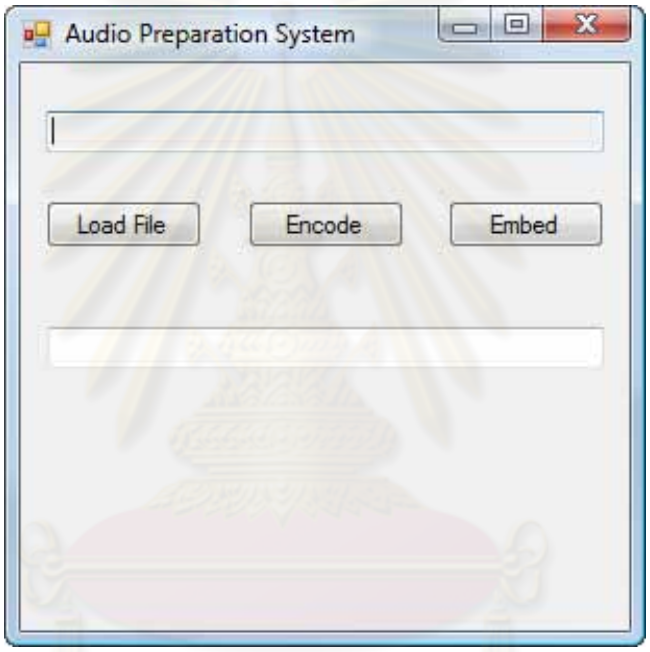


Fig. 3.8 Audio Preparation System

In the Audio preparation system (APS), there are two significant parts: the part of encoding, and the part of embedding ADMP into the audio files. Fig. 3.8 shows the interface of the APS program. Mechanisms to perform these tasks are described in the following sub-sections.

3.3.1 Mechanism to create an encoded audio file

The objective of this mechanism is to transform an original audio file to be a new audio file that cannot be run smoothly with another media player. This mechanism is based on the encoding algorithm as elaborated below in Fig. 3.9.

```
While Mp3Input.Length <> Mp3Input.Position
    If Mp3Input.Length - Mp3Input.Position >= 2048 Then
        'Write the Original data 2048 bytes to Mp3Output
    Else
        'define LastByte of data by (Mp3Input.Length - Mp3Input.Position)
        'Write the LastByte a into Mp3Output
    End If

    If Mp3Input.Length - Mp3Input.Position >= 256 Then
        'Read 128 bytes from Mp3Input and keep it in bufferA
        'Read the next 128 bytes from Mp3Input and keep it in bufferB
        'Write data from bufferB and bufferA into Mp3Output respectively
    Else
        'define LastByte of data by (Mp3Input.Length - Mp3Input.Position)
        If LastByte > 128 Then
            'Read 128 bytes from Mp3Input and keep it in bufferA
            'define LastByte of data by (Mp3Input.Length - Mp3Input.Position)
            'Read LastByte from Mp3Input and keep it in bufferB
            'Write data from bufferB and bufferA into Mp3Output respectively
        Else
            'Write the LastByte a into Mp3Output
        End If
    End If
End While
```

Fig. 3.9 Encoding algorithm

In the first part of the encoding algorithm in Fig. 3.9, it will read the original audio file for 2048 bytes and write it into the audio output file. For the second part, it will read the original file for 256 bytes, keeping in two buffers (bufferA, bufferB), and separating equally for 128 bytes. After that bytes are swapping in pairs and wrote into the output file. However, the algorithm needs to recheck the condition before swapping the bytes to ensure that the remaining bytes are over 2048 bytes for the original data, or over 256 bytes for swapping. In the first part, if the remaining bytes are less than 2048 bytes, these are the last bytes of original data. On the other hand, they are the last swapping.

When it comes to the last swapping bytes, the algorithm needs to check the remaining bytes whether it is more than 128 bytes by keeping the remaining in the variable name LastByte. If it is larger than 128 bytes, the program will read the original audio file for another 128 bytes and keep it in the bufferA then swap it with the rest of the original file and forming a new audio file. If the last byte is less than 128 bytes, read the original audio file and write into the output file.

Finally a new encoded audio file is obtained. Additionally, this file will not be run smoothly with other music players.

3.3.2 Mechanisms to create an embedded audio file

Embedding ADMP file and extracting some part of audio file from encoded audio file, we have steps as follow:-

```
While Mp3EncodeLength <> Mp3EncodeInput.Position
    If Mp3EncodeLength - Mp3EncodeInput.Position >= 1920 Then
        'Write the Original data 1920 bytes to Mp3Embed
    Else
        'define LastByte of data by (Mp3EncodeLength - Mp3EncodeInput.Position)
        'Write the LastByte into Mp3Embed
    End If

    If EXEPlayerLength - EXEPlayer.Position >= 128 Then
        'Read 128 bytes from Mp3EncodeInput and Write it into TempMp3
        'Read 128 bytes from EXEPlayer and Write it into Mp3Embed
        'Read 256 bytes from Mp3EncodeInput and Write it into Mp3Embed
    Else
        'define lastEXEPlayerByte and lastMp3TempByte of data by (EXEPlayerLength - EXEPlayer.Position)
        'Read lastMp3TempByte from Mp3EncodeInput and Write it into TempMp3
        'Read lastEXEPlayerByte from EXEPlayer and Write it into Mp3Embed
        'define AmountLastByte of data by (Mp3EncodeLength - Mp3EncodeInput.Position)
        'Write the AmountLastByte into Mp3Embed
    End If
End While
```

Fig. 3.10 Embedding algorithm

In the first part of the embedded algorithm as shown in Fig. 3.10, the program will read the encoded audio file for 1920 bytes and write it into audio output file. For the second part, it will read the encoded audio file for 128 bytes and write it into temporary file, called the partial audio content. Then, it will read 128 bytes of the ADMP file and storing into the buffer and read the encoded audio file 256 bytes then keep in another buffer. After that the program will retrieve value from buffers and write it into the new audio output file, called protected audio file using the ADMP 128 bytes, and the encoded audio file 256 bytes swapping each other until the last bytes of ADMP are not more than 128 bytes.

After the remaining bytes of the ADMP are not greater than 128 bytes, it will read the encoded audio file according to the last byte of the ADMP which storing in the buffer and write it into a temporary file. Finally, it will write the last byte of the ADMP to output file then read the encoded audio file of the remaining bytes and set up a new protected audio file.

CHAPTER IV

EVALUATIONS AND EXPERIMENTAL RESULTS

4.1 Evaluation Method

In order to evaluate the proposed mechanism, there are two testes have to be performed. The first testing step is to test the implemented software in which the proposed protection technique was implemented. The second testing step is the statistical test where the experimental results gathering from various samples are computed and compared with statistical values to confirm the assumption of protection technique. Details of these evaluations are as follows.

4.2 Sample groups and testing condition

Since the objective of this research is to implement a protection technique that users cannot be recognized, the testing indicators are the quality of sound evaluated by a sample group, and the number of users in the samples who has curiosity in the IP protection mechanism. The sample group, 120 persons, consists of various academic backgrounds: computer technicians and non-technicians. Moreover, there are 20 audio files in the test.

4.3 Software Evaluation

After finishing the implementation, the system was tested by the developer. The test uses a simple software testing technique; with this test, there are 20 audio files that have been tested. The results of the 20 audio plays indicate that when the encoded audio file is accessed by the DMAC, the quality of the voice is the same as the original file. Unlikely to the play with the general audio players, the presentation quality is low and unsmooth. Fig. 4.1 shows the interface of the DMAC program.

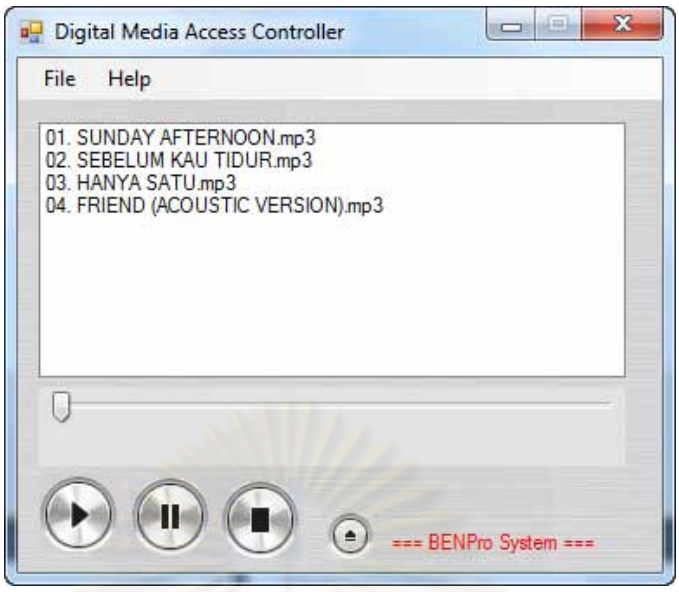


Fig. 4.1 Digital Media Access Controller Program

4.4 Testing Hypothesis of Protection Mechanism

Since the proposed mechanism was implemented completely in the software mentioned above, 120 samples are randomly selected by volunteers to test the proposed protection technique. The hypothesis to test the protection mechanism can be listed as follows.

4.4.1 Test of re-download the audio when it cannot be opened

H_{01Ed}: People who have different backgrounds will have the same decision about re-downloading the audio file when it cannot be opened.

H_{11Ed}: People who have different backgrounds will have different decisions about re-downloading the audio file when it cannot be opened.

Since some rows in the contingency table contains number of data less than 5, the test of this hypothesis is based on the Likelihood Ratio with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about re-downloading the audio file when it cannot be opened, according to the Likelihood Ratio = 3.067, df = 2, p-value = 0.216 > α=0.05. The raw data confirms that most users, both technical and non-technical, will re-download the audio file (technical = 81%, non-technical = 86%).

H_{01Ag}: People who have different age ranges will have the same decision about re-downloading the audio file when it cannot be opened.

H_{11Ag}: People who have different age ranges will have different decisions about re-downloading the audio file when it cannot be opened.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the same decision about re-downloading the audio file when it cannot be opened, according to the Chi-Square = 0.589, df = 2, p-value = 0.745 > α=0.05. The raw data confirms that most users, both youth and working age ranges, will re-download the audio file (age (16-25) = 83.33%, age (26-35) = 84%).

4.4.2 Test of remove and quit using DMAC when it cannot open the audio file

H_{02Ed}: People who have different backgrounds will have the same decision about remove and quit using the DMAC when it cannot open the audio file.

H_{12Ed}: People who have different backgrounds will have different decisions about remove and quit using the DMAC when it cannot open the audio file.

Since some rows in the contingency table contains number of data less than 5, then the test of this hypothesis is based on the Likelihood Ratio with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about re-downloading the audio file when it cannot be opened, according to the Likelihood Ratio = 5.023, df = 2, p-value = 0.081 > α=0.05. The raw data confirms that most users, both technical and non-technical, will not remove and quit using the DMAC when it cannot open the audio file (technical = 51.6%, non-technical = 55.67%).

H_{02Ag}: People who have different age ranges will have the same decision about remove and quit using DMAC when it cannot open the audio file.

H_{12Ag}: People who have different age ranges will have different decisions about remove and quit using DMAC when it cannot open the audio file.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the same decision about remove and quit using the DMAC when it cannot open the audio file, according to the Chi-Square = 3.402, df = 2, p-value = 0.183 > α=0.05. The raw data confirms that most users, both youth and working age ranges, will not remove and quit using the DMAC when it cannot open the audio file (age (16-25) =57.33 %, age (26-35) = 50%).

4.4.3 Test of find the crack or tools to fix the program when it cannot open the audio file

H_{03Ed}: People who have different backgrounds will have the same decision about find the crack or tools to fix the program when it cannot open the audio file.

H_{13Ed}: People who have different backgrounds will have different decisions about find the crack or tools to fix the program when it cannot open the audio file.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about find the crack or tools to fix the program when it cannot open the audio file, according to Chi-Square = 2.450, df = 2, p-value = 0.294 > α=0.05. The raw data confirms that most users, both technical and non-technical, will not find the crack or tools to fix the program when it cannot open the audio file (technical = 52.67%, non-technical = 46%).

H_{03Ag}: People who have different age ranges will have the same decision about find the crack or tools to fix the program when it cannot open the audio file

H_{13Ag}: People who have different age ranges will have different decisions about find the crack or tools to fix the program when it cannot open the audio file.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the different decision about find the crack or tools to fix the program when it cannot open the audio file, according to the Chi-Square = 14.886, df = 2, p-value = 0.001 < α=0.05. The raw data indicated that a number of users in ages 26-35 will find the crack or tools to fix the program when it cannot open the audio file (age (26-35) = 48.33%) more than the users in ages 16-25 and most users in this range will not find the crack or tools to fix the program when it cannot open the audio file (age (16-25) = 50.67%).

4.4.4 Test of realize the DMAC was protected when it cannot open the audio file from other sources

H_{04Ed}: People who have different backgrounds will have the same decision about realize the DMAC was protected when it cannot open the audio file from other sources.

H_{14Ed}: People who have different backgrounds will have different decisions about realize the DMAC was protected when it cannot open the audio file from other sources.

Since some rows in the contingency table contains number of data less than 5, then the test of this hypothesis is based on the Likelihood Ratio with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the different decision about realize the DMAC was protected when it cannot open the audio file from other sources, according to the Likelihood Ratio = 6.668, df = 2, p-value = 0.036 < α=0.05. The raw data indicated that a few users in computer technician will not realize the DMAC was protected when it cannot open the audio file from other sources (technical = 61%) but most of users in non-technician will realize the DMAC was protected when it cannot open the audio file from other sources (non-technical = 52.67%).

H_{04Ag}: People who have different age ranges will have the same decision about realize the DMAC was protected when it cannot open the audio file from other sources.

H_{14Ag}: People who have different age ranges will have different decisions about realize the DMAC was protected when it cannot open the audio file from other sources.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the same decision about realize the DMAC was protected when it cannot open the audio file from other sources, according to the Chi-Square = 2.405, df = 2, p-value = 0.300 > α=0.05. The raw data confirms that most users, both youth and working age ranges, will not realize the DMAC was protected when it cannot open the audio file from other sources (age (16-25) = 54%, age (26-35) = 60%).

4.4.5 Test of realizes the downloaded audio file was encoded when it cannot be opened.

H_{05Ed}: People who have different backgrounds will have the same decision about realizes the downloaded audio file was encoded when it cannot be opened.

H_{15Ed}: People who have different backgrounds will have different decisions about realizes the downloaded audio file was encoded when it cannot be opened.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about realizes the downloaded audio file was encoded when it cannot be opened, according to Chi-Square = 1.644, df = 2, p-value = 0.439 > α=0.05. The raw data confirms that most users, both technical and non-technical, will not realizes the downloaded audio file was encoded when it cannot be opened (technical = 57.67%, non-technical = 52.67%).

H_{05Ag}: People who have different age ranges will have the same decision about realize the downloaded audio file was encoded when it cannot be opened.

H_{15Ag}: People who have different age ranges will have different decisions about realize the downloaded audio file was encoded when it cannot be opened.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the same decision about realizes the downloaded audio file was encoded when it cannot be opened, according to the Chi-Square = 2.060, df = 2, p-value = 0.357 > α=0.05. The raw data confirms that most users, both youth and working age ranges, will not realizes the downloaded audio file was encoded when it cannot be opened (age (16-25) = 57.33%, age (26-35) = 53.33%).

4.4.6 Test of realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened.

H_{06Ed}: People who have different backgrounds will have the same decision about realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened.

H_{16Ed}: People who have different backgrounds will have different decisions about realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened, according to Chi-Square = 1.340, df = 2, p-value = 0.512 > α=0.05. The raw data confirms that most users, both technical and non-technical, will not realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened (technical = 51%, non-technical = 55%).

H_{06Ag}: People who have different age ranges will have the same decision about realize the downloaded audio file was encoded if copied to others computer and it cannot be opened.

H_{16Ag}: People who have different age ranges will have different decisions about realize the downloaded audio file was encoded if copied to others computer and it cannot be opened.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the different decision about realizes the downloaded audio file was encoded if copied to others computer and it cannot be opened, according to the Chi-Square = 15.178, df = 2, p-value = 0.001 < α=0.05. The raw data indicated that a number of users in ages 16-25 will realize the downloaded audio file was encoded if copied to others computer and it cannot be opened more than the users in ages 26-35 (age (16-25) = 56.67%) and most users in this range will not realize the downloaded audio file was encoded if copied to others computer and it cannot be opened (age (26-35) = 49.33%).

4.4.7 Test of thinking this data protection will reduce the hackers' motivation.

H_{07Ed}: People who have different backgrounds will have the same decision about this data protection will reduce the hackers' motivation.

H_{17Ed}: People who have different backgrounds will have different decisions about this data protection will reduce the hackers' motivation.

Since some rows in the contingency table contains number of data less than 5, then the test of this hypothesis is based on the Likelihood Ratio with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the different decision about this data protection will reduce the hackers' motivation, according to the Likelihood Ratio = 13.804, df = 2, p-value = 0.001 < α=0.05. The raw data indicated that a few users in computer technician think this data protection will reduce the hackers' motivation (technical = 80%) but most of users in non-technician think this data protection will reduce the hackers' motivation (non-technical = 91.67%).

H_{07Ag}: People who have different age ranges will have the same decision about this data protection will reduce the hackers' motivation.

H_{17Ag}: People who have different age ranges will have different decisions about this data protection will reduce the hackers' motivation.

Since some rows in the contingency table contains number of data less than 5, then the test of this hypothesis is based on the Likelihood Ratio with 95% confident level (α=0.05). The result from the SPSS shows that people who have age ranges will have the same decision about this data protection will reduce the hackers' motivation, according to the Likelihood Ratio = 3.043, df = 2, p-value = 0.218 > α=0.05. The raw data confirms that most users, both youth and working age ranges, though that this data protection will reduce the hackers' motivation (age (16-25) = 84%, age (26-35) = 87.67%).

4.4.8 Test of thinking the defect is an effect from the transfer mechanism rather than the protection mechanism.

H_{08Ed}: People who have different backgrounds will have the same decision about the defect is an effect from the transfer mechanism rather than the protection mechanism.

H_{18Ed}: People who have different backgrounds will have different decisions about the defect is an effect from the transfer mechanism rather than the protection mechanism.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about the defect is an effect from the transfer mechanism rather than the protection mechanism, according to Chi-Square = 2.353, df = 2, p-value = 0.308 > α=0.05. The raw data confirms that most users, both technical and non-technical, though that the defect is an effect from the transfer mechanism rather than the protection mechanism (technical = 74%, non-technical = 79%).

H_{08Ag}: People who have different age ranges will have the same decision about the defect is an effect from the transfer mechanism rather than the protection mechanism.

H_{18Ag}: People who have different age ranges will have different decisions about the defect is an effect from the transfer mechanism rather than the protection mechanism.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the different decision about the defect is an effect from the transfer mechanism rather than the protection mechanism, according to the Chi-Square = 18.129, df = 2, p-value = 0.000 < α=0.05. The raw data indicated that a number of users in ages 16-25 will realize the defect is an effect from the transfer mechanism (age (16-25) = 85%) rather than the protection mechanism more than the users in ages 26-35 and most users in this range will not realize the defect is an effect from the transfer mechanism rather than the protection mechanism (age (26-35) = 67.67%).

4.4.9 Test of using the DMAC and the BENPro system was easy.

H_{09Ed}: People who have different backgrounds will have the same decision about using the DMAC and the BENPro system was easy.

H_{19Ed}: People who have different backgrounds will have different decisions about using the DMAC and the BENPro system was easy.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different backgrounds will have the same decision about using the DMAC and the BENPro system was easy, according to Chi-Square = 2.870 df = 2, p-value = 0.238 > α=0.05. The raw data confirms that most users, both technical and non-technical, though that using the DMAC and the BENPro system was easy (technical = 67.33%, non-technical = 65.67%).

H_{09Ag}: People who have different age ranges will have the same decision about using the DMAC and the BENPro system was easy.

H_{19Ag}: People who have different age ranges will have different decisions about using the DMAC and the BENPro system was easy.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result from the SPSS shows that people who have different age ranges will have the same decision about using the DMAC and the BENPro system was easy, according to the Chi-Square = 2.046, df = 2, p-value = 0.359 > α=0.05. The raw data confirms that most users, both youth and working age ranges, though that using the DMAC and the BENPro system was easy (age (16-25) = 67.67%, age (26-35) = 65%).

4.4.10 Test of the quality of the played audio is the same as the original file.

H_{09Ed}: People who have different backgrounds will have the same decision about the quality of the played audio is the same as the original file.

H_{19Ed}: People who have different backgrounds will have different decisions about the quality of the played audio is the same as the original file.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result shows that people who have different backgrounds will have the same decision about the quality of the played audio is the same as the original file, all of users in both technical and non-technical give the same scores, which is rating 3. The raw data confirms that most users, both technical and non-technical, though that the quality of the played audio is the same as the original file (technical = 100%, non-technical = 100%).

H_{09Ag}: People who have different age ranges will have the same decision about the quality of the played audio is the same as the original file.

H_{19Ag}: People who have different age ranges will have different decisions about the quality of the played audio is the same as the original file.

The test of this hypothesis is based on the Pearson Chi-Square with 95% confident level (α=0.05). The result shows that people who have different age ranges will have the same decision about the quality of the played audio is the same as the original file, all of users in both youth and working age ranges give the same scores,

which is rating 3. The raw data confirms that most users, both youth and working age ranges, though the quality of the played audio is the same as the original file (age (16-25) = 100%, age (26-35) = 100%).

4.4.11 Testing of General Aspects

Table 4.1: Experimental results

Experimental Results												
Specialist	Age		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Non-technical	16-25	Mean	2.63	1.73	1.43	1.53	1.70	1.77	2.73	2.63	2.03	3.00
		Std. Deviation	0.556	0.640	0.626	0.571	0.750	0.728	0.450	0.615	0.765	0.000
	26-35	Mean	2.53	1.37	1.33	1.63	1.47	1.53	2.77	2.10	1.90	3.00
		Std. Deviation	0.681	0.490	0.711	0.615	0.730	0.776	0.430	0.607	0.607	0.000
	Total	Mean	2.58	1.55	1.38	1.58	1.58	1.65	2.75	2.37	1.97	3.00
		Std. Deviation	0.619	0.594	0.666	0.591	0.743	0.755	0.437	0.663	0.688	0.000
Technical	16-25	Mean	2.37	1.70	1.60	1.70	1.73	1.63	2.30	2.47	2.03	3.00
		Std. Deviation	0.850	0.750	0.724	0.702	0.740	0.669	0.535	0.681	0.809	0.000
	26-35	Mean	2.50	1.63	1.57	1.97	1.73	1.43	2.50	1.97	2.00	3.00
		Std. Deviation	0.682	0.765	0.898	0.765	0.785	0.817	0.630	0.765	0.788	0.000
	Total	Mean	2.43	1.67	1.58	1.83	1.73	1.53	2.40	2.22	2.02	3.00
		Std. Deviation	0.767	0.752	0.809	0.740	0.756	0.747	0.588	0.761	0.792	0.000

Where: Q1: You designed to re-download the audio files if you are unable to open it.

Q2: You designed to remove and quit using DMAC if you are unable to open the audio files.

Q3: You find the crack or tools to fix the program when you cannot open the audio files.

Q4: You realized the DMAC was protected if you are unable to open a downloaded file from other sources.

Q5: You realized that a downloaded audio file was encoded if you are unable to open it via another media player.

Q6: You realized a downloaded audio file was encoded if you copied that file and were unable to open with others computer.

Q7: You think this data protection will reduce the hackers' motivation.

Q8: You think the defect is an effect from the transfer mechanism rather than the protection mechanism.

Q9: DMAC and this system are easy to use.

Q10: The quality of the played audio is the same as the original audio file.

The Table 4.1 above shows the experimental results that gathering from various samples, 60 samples from computer-technicians and 60 samples from non-technicians, and age between 16-25 and 26-35 years old for each group of the samples; using the DMAC and others audio players. In this testing, it has 10 questions for these samples to evaluate the scores, rating one, two, and three. From the question 1 (Q1), "You designed to re-download the audio files if you are unable to open it", the average scores from computer-technical and non-technical are 2.58 and 2.43, it shows that most of samples decided to re-download the encoded audio file when it cannot be opened. The average scores from both sample groups in Q2, "You designed to remove and quit using DMAC if you are unable to open the audio files", are 1.55 and 1.67, and in the Q3, "You find the crack or tools to fix the program when you cannot open the audio files", are 1.38 and 1.58, these results indicate that most of users did not decide to remove or find a crack to resolve the problem.

In addition, when run downloaded audio files from other sources with the DMAC and the results from Q4, "You realized the DMAC was protected if you are unable to open a downloaded file from other sources." from non-technician is 1.58 and from technician is 1.83 which means most samples in non-technician does not realize the DMAC was protected. Moreover, the testing is also performed in the situation that an encoded audio file was distributed to others users, the evaluation score in Q5 "You realized that a downloaded audio file was encoded if you are unable to open it via another media player." from both sample groups are 1.58 and 1.73 confirm. In the Q6 "You realized a downloaded audio file was encoded if you copied that file and were unable to open with others computer", the results are 1.65 and 1.53, these results from Q5 and Q6 indicate that most samples didn't realize the file was encoded or the audio player was protected by some security mechanism. Furthermore, both of the sample groups believe that the defect is an effect from the transfer mechanism rather than the protection mechanism.

Finally, in the Q10: "The quality of the played audio is the same as the original audio file", although the encoding algorithm is just swapping bytes along the audio content and it did not affect with the quality of the sound audio but the test needs to check by let the samples listen a protected audio file by the DMAC and an original

audio file plays with another music players. The result shows that all samples both in computer-technical and non-technical give the same scores, which is rating three. So, these results can confirm that the protected audio file and the original audio file represent the same quality to the users.

CHAPTER V

CONCLUSIONS AND DISCUSSIONS

5.1 Discussions

According to the high demand in digital media over the Internet, especially audio and video files, the DRM to protect IP becomes an important role in the digital businesses. Various researches are proposed and implemented to protect these media. One popular and acceptable method is the implementation of a member system where all agreements are signed among providers and clients based on the concept of [2]. Moreover, most protection methods have applied encryption techniques to protect the files from unauthorized accesses [3][4]. Another technique that is applied to the digital documents is the use of the watermark mechanism.

However, these methods mentioned above are complicated and cannot protect the digital files from hackers or illegal distributers after the files were downloaded legally. In addition, prohibition in accessing the files by the protection characteristics that is obviously seen or informed to clients is a good simulator to all hackers. Therefore, these interdiction mechanisms cannot complete the mission.

Considering the BENPro technique, the protection mechanism applies a simple shifting and stuffing bytes of the audio contents with an executable file. Additionally, some part of the audio file is extracted and stored in the database of the audio provider. So, although the audio files were unfaithfully distributed by some authorized users, these files cannot be played by any audio player as expected. Thus, the audio files are protected because some part of the audio in the PADB still needs the authority checking when users request the play.

The result of the test indicates that after downloading the files and running it by other audio players, most users hardly realize the shield mechanism. This is because all downloaded files that run by other audio players can play without satisfaction and correction. Thus, the evidence leads to indicate the defense mechanism of these digital files is unclear to hackers. Therefore, the motivation in illegally cracking the files is low comparing to other implementing methods.

5.2 Conclusions

Since the audio services are very popular over the Internet, the IP protection becomes a serious issue for all audio providers. Although many methods have been proposed and implemented, especially the encryption technique, these methods cannot protect the illegal usage from unauthorized users after legal downloaded was granted. Moreover, these protection mechanisms are obviously detected by users, especially hackers. Thus, they are strong stimuli with high challenge for hackers.

This thesis proposes the BENPro mechanism which is a simple protection method. Nevertheless, this mechanism can prevent the unlawful usages of unauthorized users by storing some part of the audio files at the PADB; this part of the audio will be retrieved and merged to the rest of the file at the client when the audio was accessed through the ADMP functions only. In addition, the partial audio file that is retrieved by users will be able to play unclearly and unsmooth by general audio players. Consequently, the hacking motivation will be decreased. Therefore, the objective of the IP media protection is satisfied and maintained.

References

1. M. Stini, M. Mauve, F. H.P. Fitzek, "Digital Ownership: From Content Consumers to Owners and Traders," IEEE Multimedia, vol. 13(4), pp. 1 – 6, October-December 2006.
2. E. Luoma, H. Vahtera, "Current and emerging requirements for digital rights management systems through examination of business networks," *Proceedings of the 37th Annual Hawaii International Conference on the System Sciences*. vol. 1, pp.1-10, February 2004.
3. W. Jonker, J.P. Linnartz, "Digital Right Management in Consumer Electronics Products," *IEEE Signal Processing Magazine*, pp. 82-91, March 2004.
4. J. Lotspiech, S. Nusser, F. Pestoni, "Anonymous Trust: Digital Rights Management Using Broadcase Encryption," *Proceedings of the IEEE*, vol. 92(6), pp. 898-909, June 2004.
5. T. S. Messerges, E. A. Dabbish, "Digital rights management in a 3G mobile phone and beyond." *Proceedings of the 3rd ACM workshop on Digital rights management*, pp. 27 – 38, October 2003.
6. B. C. Popescu, B. Crispo, A. S. Tanenbaum, F. L.A.J. Kamperman, "A DRM Security Architecture for Home Network," *Proceedings of the 4th ACM Workshop on Digital Rights Management*, pp.151-158, October 2004.
7. J.S. Lee, K.S. Yoon, "The System Integration of DRM and Fingerprinting," Proceedings of the 8th International Conference on Advanced Communication Technology, pp. 2180-2183, February, 2006.
8. M. Loytynoja, N. Cvejic, T. Seppanen, "Audio Protection with removable watermarking," Information, Proceedings of the 6th International Conference on Communications & Signal Processing, pp. 1-4, December 2007.
9. Dutta M.K., Gupta P., and Pathak V.K., "Perceptible Audio Watermarking for Digital Right Management Control," *Proceedings of the 7th International Conference on Information, Communications and* Signal Processing, pp. 1-5, December 2009.
10. Gordan L., "The Internet Marketplace and Digital Rights Management,"

Gaithersburg, 2001.

11. Q.Liu, R S Naini, N P Sheppard., “Digital Rights Management for Content distribution,” Proceedings the Australasian information security workshop, Vol. 21, pp. 49, 2003.
12. N. Wagner, “Fingerprinting,” Proceedings of the 1983 IEEE Symposium on Security and Privacy, pp. 12-22, April 1983.
13. Mandal, P.,Thakral, A., and Verma, S., “Watermark Based Digital Rights Management,” Proceedings of International Conference on Information Technology: Coding and Computing, pp. 74-78, 2005.
14. Y. Jeong, J. Kim, K. Yoon, “Audio DRM Conversion between Different DRM Content Formats,” Proceedings of the International Conference on Consumer Electronics, Digest of Technical Papers, pp. 1-2, Jan 2008.
15. Varna, A.L., Shan He, Swaminathan A., Min Wu, “Fingerprinting Compressed Multimedia Signals,” Information Forensics and Security, IEEE Transactions, pp. 330, September 2009.

APPENDICES

Appendix A

The questionnaire satisfaction of applying virus technology on BENPro system

Agreements

3 = Agree

2 = Neutral

1 = Disagree

1. General Data

   - Academic Background [] Computer technician [] Non-technician
   - Age [] 16 – 25 year old [] 26 – 35 year old [] Above 35 year old

2. Level of satisfaction : Make √ on the your satisfaction level according to above agreements

Question	Rating		
	3	2	1
1. You designed to re-download the audio files if you are unable to open it.			
2. You designed to remove and quit using DMAC if you are unable to open the audio files.			
3. You find the crack or tools to fix the program when you cannot open the audio files.			
4. You realize the DMAC was protected if you are unable to open a downloaded file from other sources.			
5. You realize that a downloaded audio file was encoded if you are unable to open it via another media player.			
6. You realize a downloaded audio file was encoded if you copied that file and were unable to open with others computer.			
7. You think this data protection will reduce the hackers' motivation.			
8. You think the defect is an effect from the transfer mechanism rather than the protection mechanism.			
9. DMAC and this system are easy to use.			
10. The quality of the played audio is the same as the original audio file.			

Appendix B

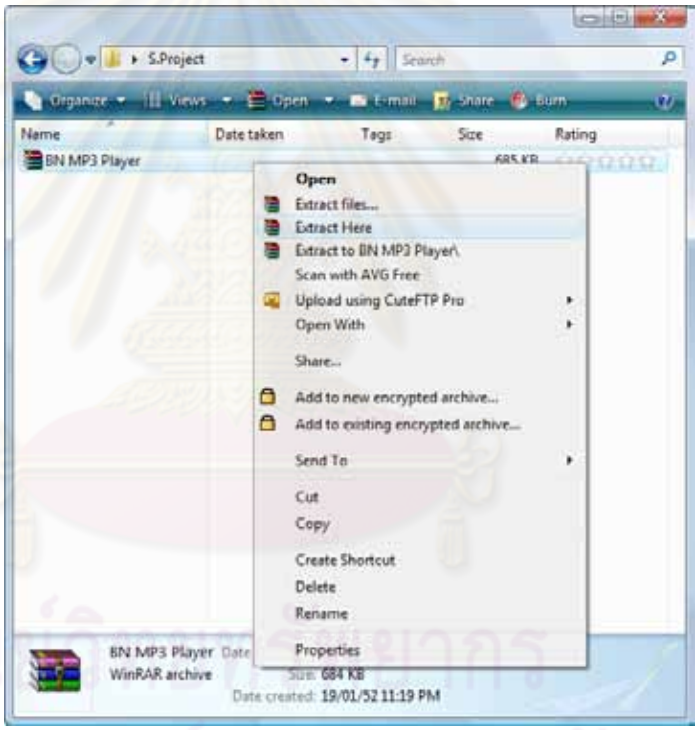
Installation of BENPro protection system.

Before install the BENPro system we need to prepare the system which can separate into 2 parts

- Microsoft .NET Framework
- Windows Installer

BENPro manual installation guide

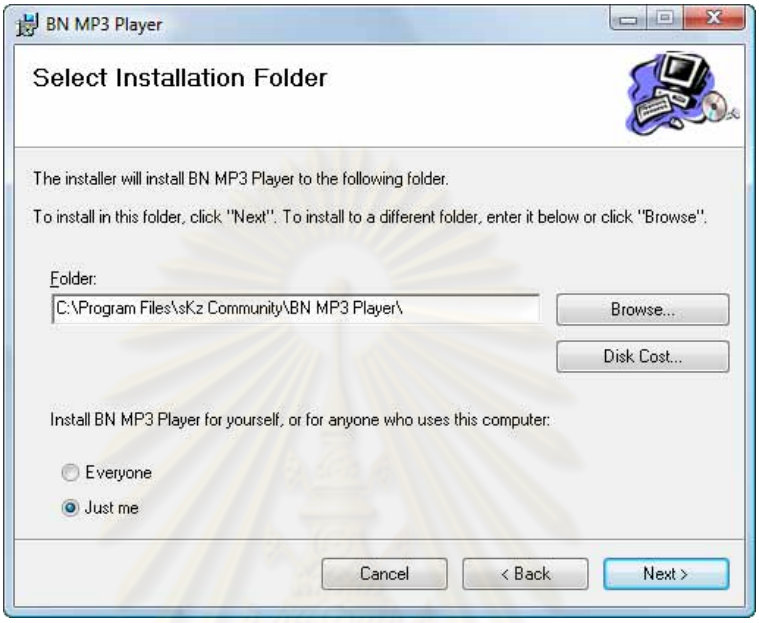
1. Extract BN MP3 Player

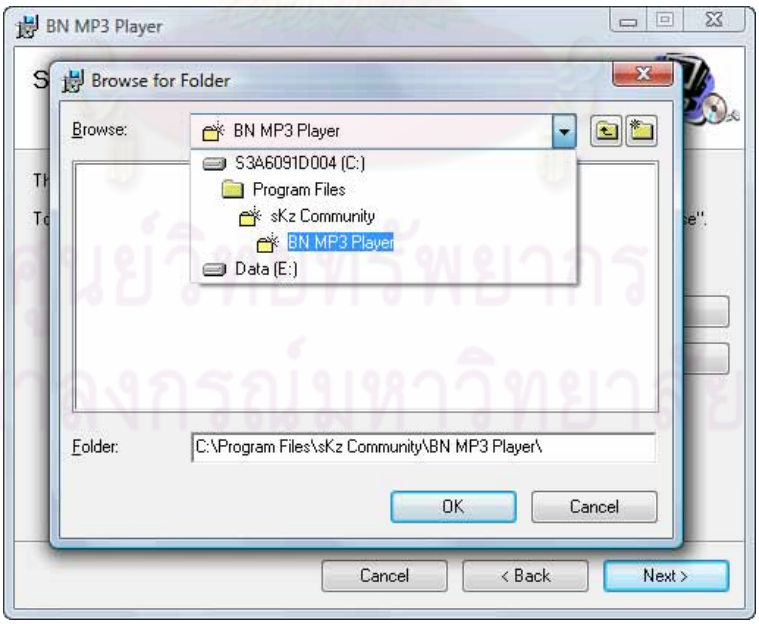


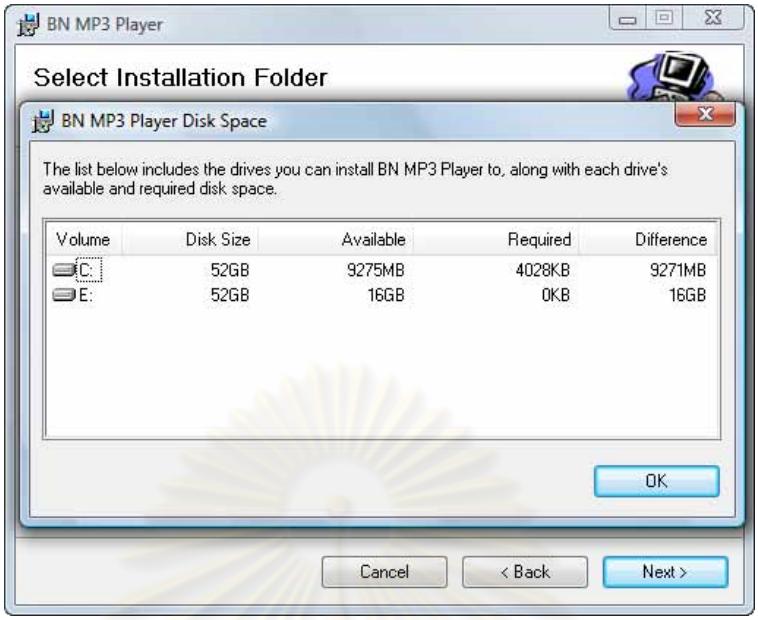
2. Open the BN MP3 Player folder and you'll see the setup file.

3. Double click on Setup.exe to start the installation process.

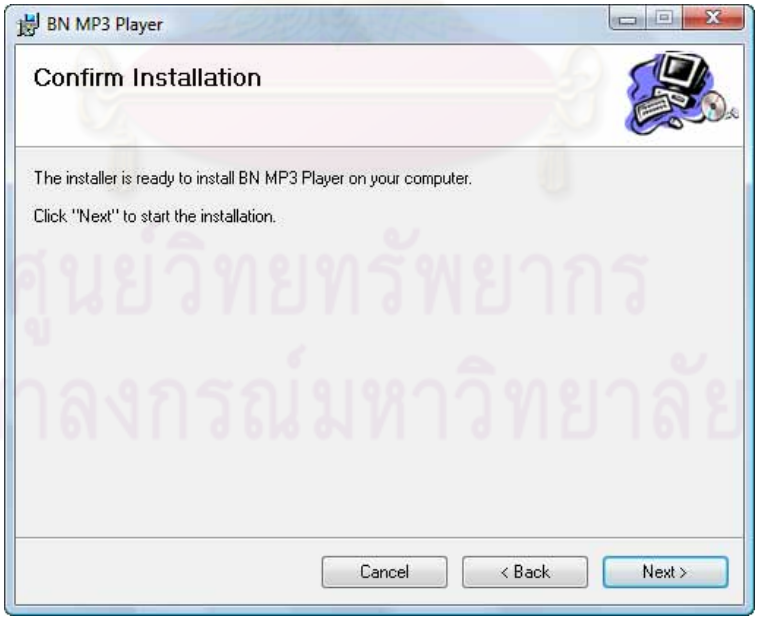
4. Click on Next button to choose where you want to install this product and you can changed the location of the installation. By the way you can check the disk cost for installation.



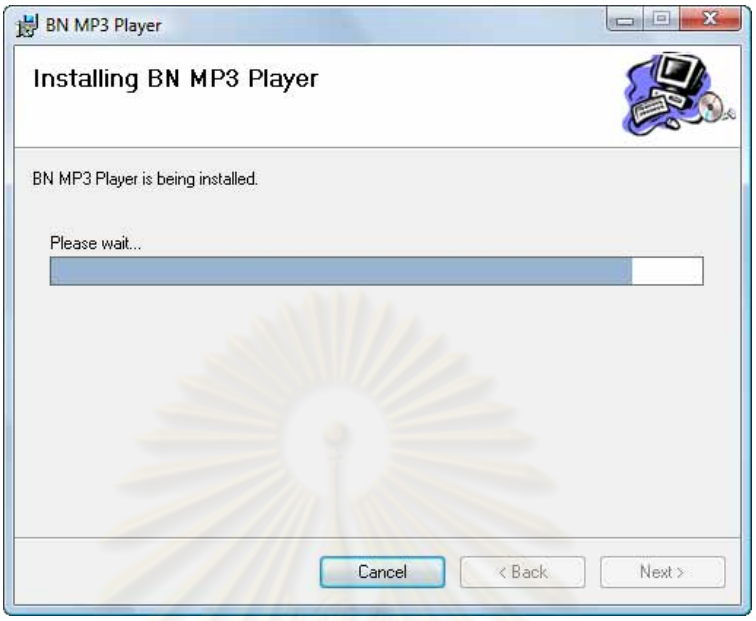




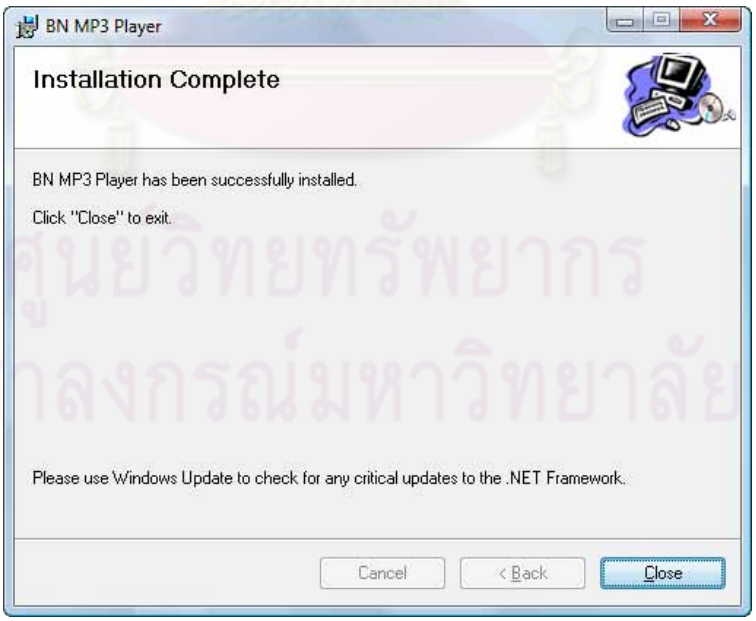
5. After finished choosing the location of the installation, click next to confirm the installation.



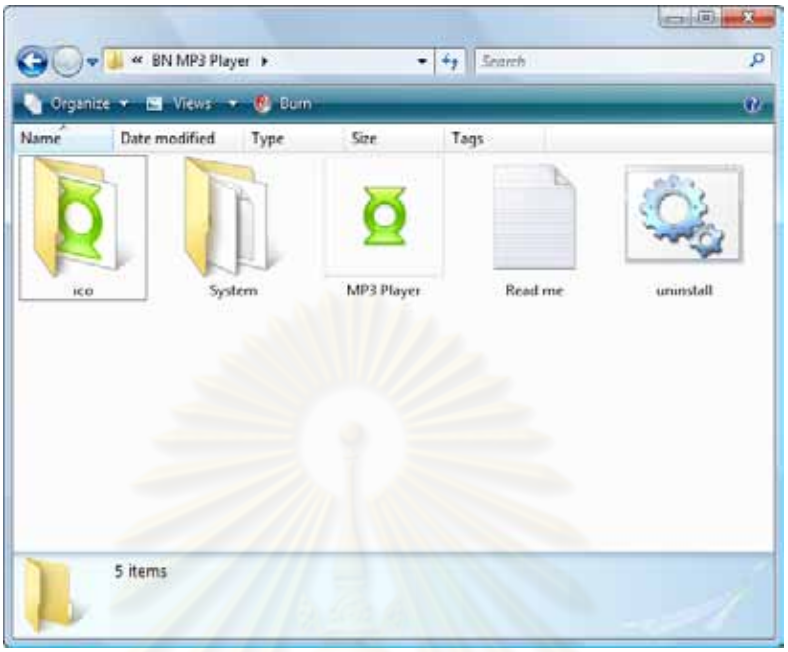
6. Click next to start the installation process.



7. After finished installation, click close button to exit the program.



8. When go to the installed folder you'll see these files.



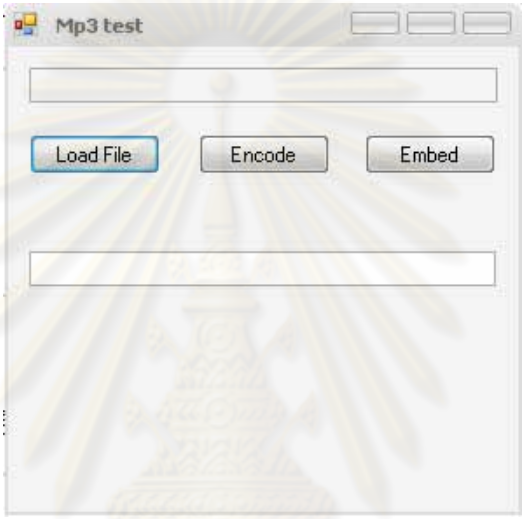
Appendix C

BENPro program manual guide.

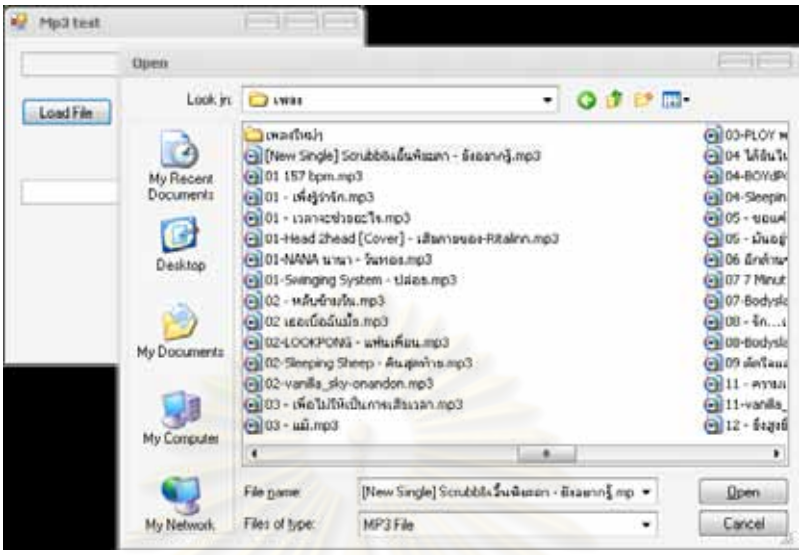
BENPro program manual is separate into 2 parts, first part is Audio preparation system and the second part is Digital media access controller.

1. Audio Preparation System

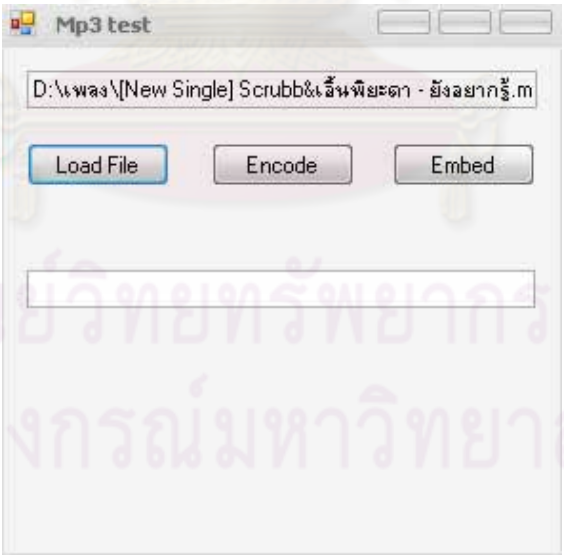
1. Double click aps.exe to open the APS program.



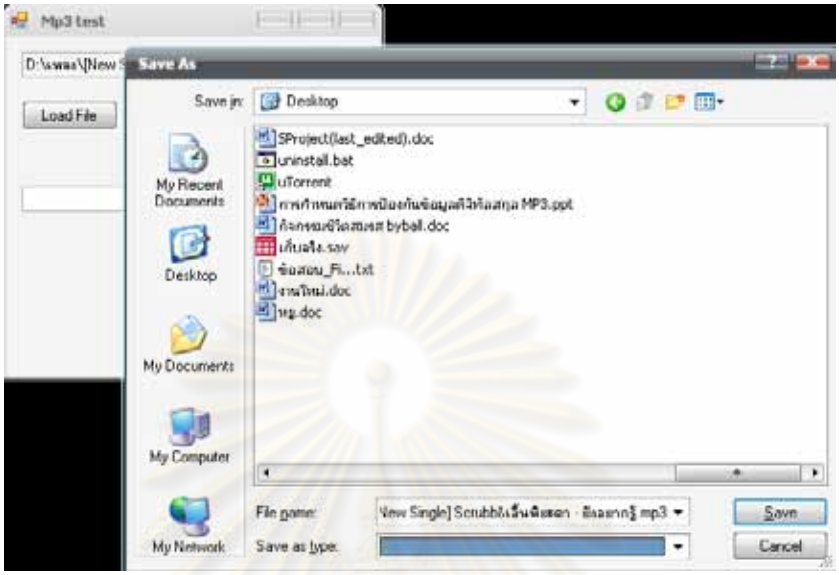
2. Click load file button and choose the audio file that you want to encode.



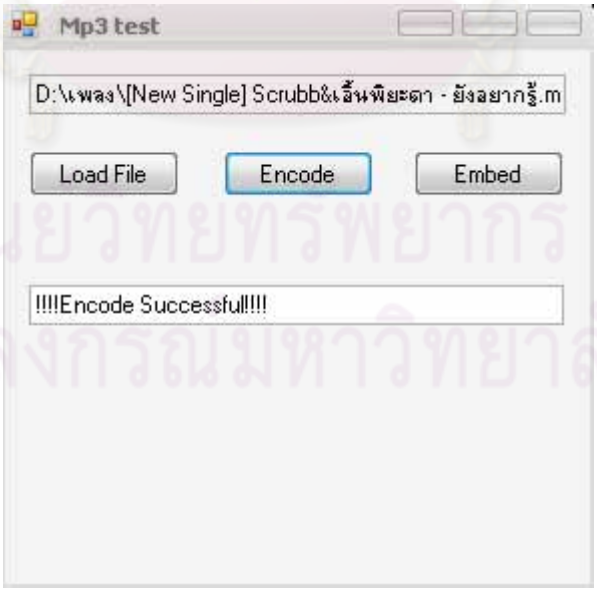
3. After choosing the audio file it will show the file name on the text box.



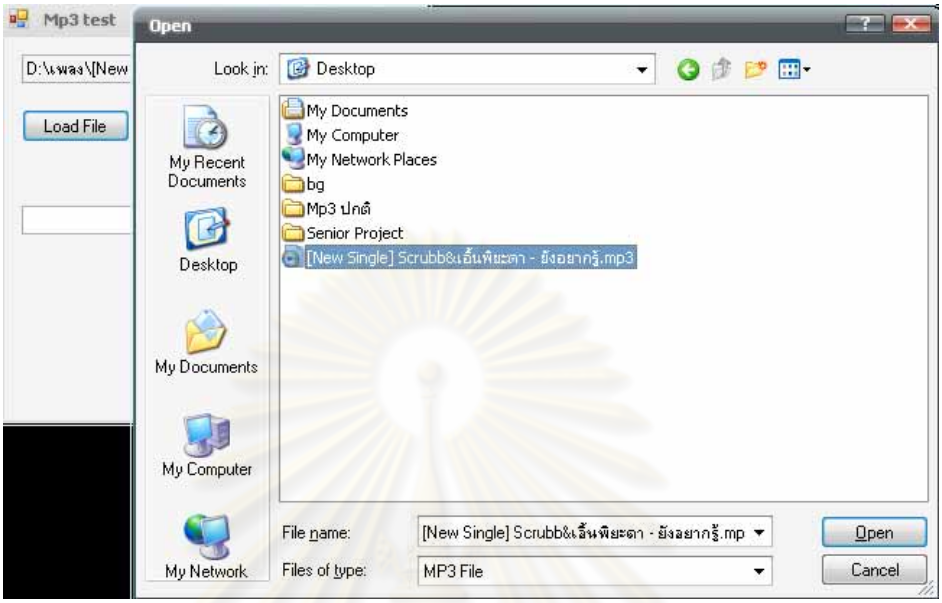
4. Click the encode button to encode the audio file then choose the location to save this file.

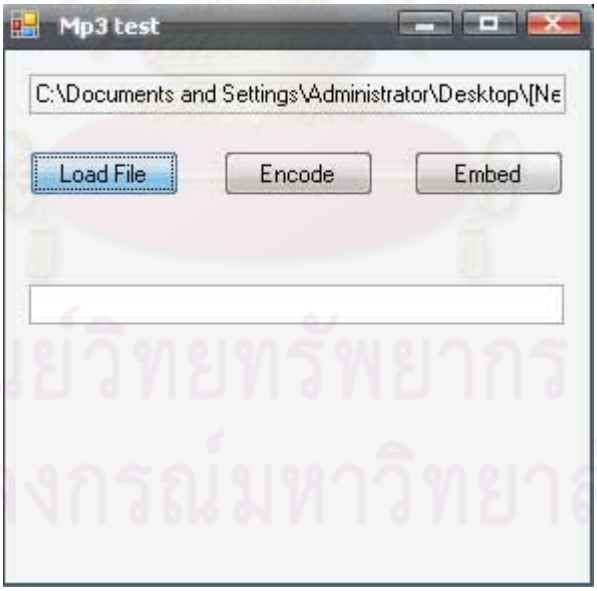


5. After finish encoding it will show the success text in the text box below.

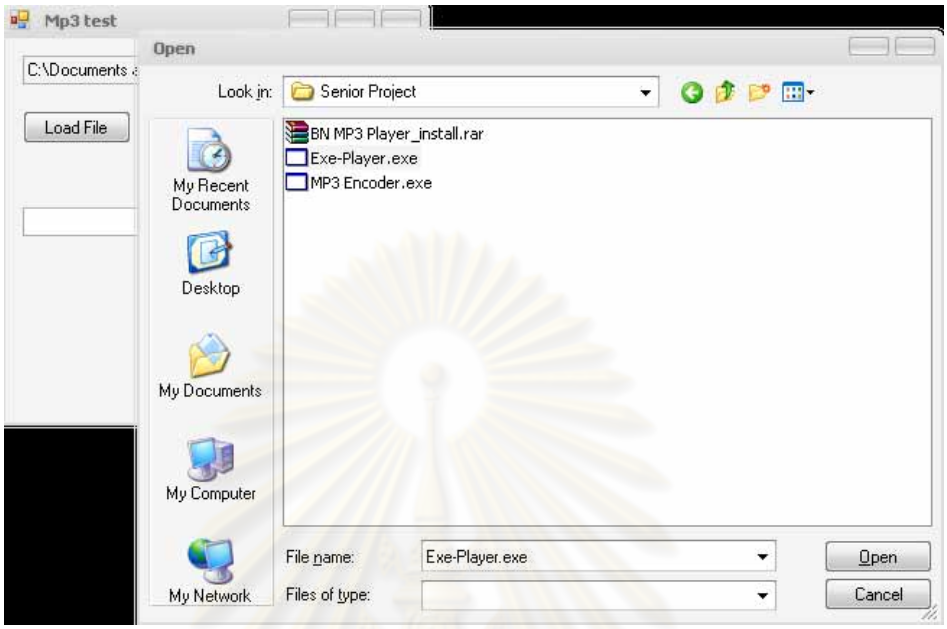


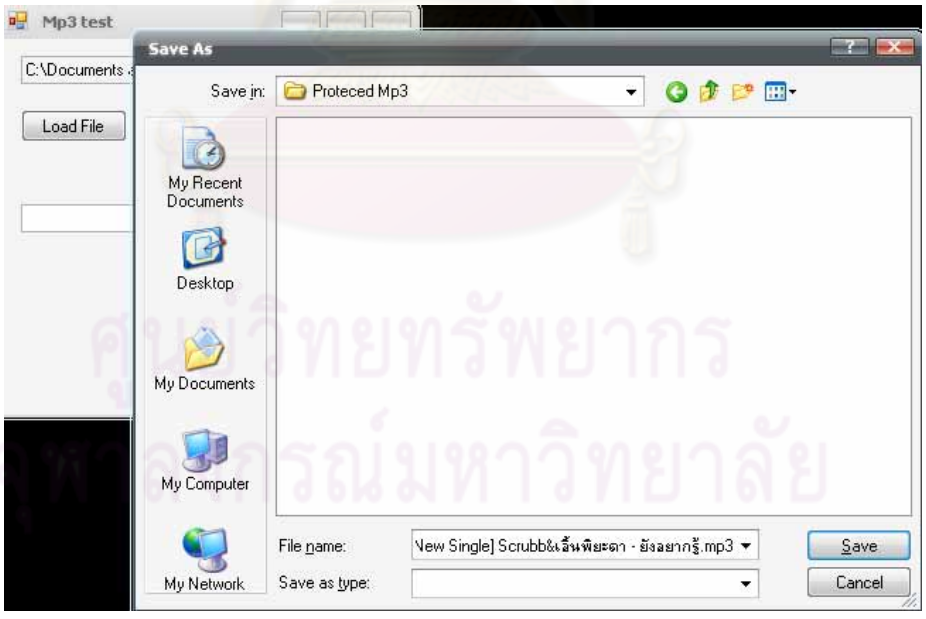
6. Click the load file button and choose the encoded audio file to embedded to ADMP into the encoded file.



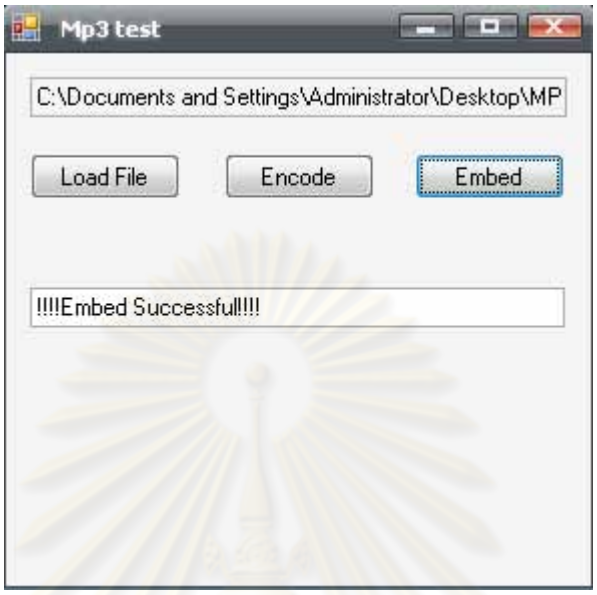


7. Click embed button and choose the ADMP file after that choose the location to save the protected audio file.



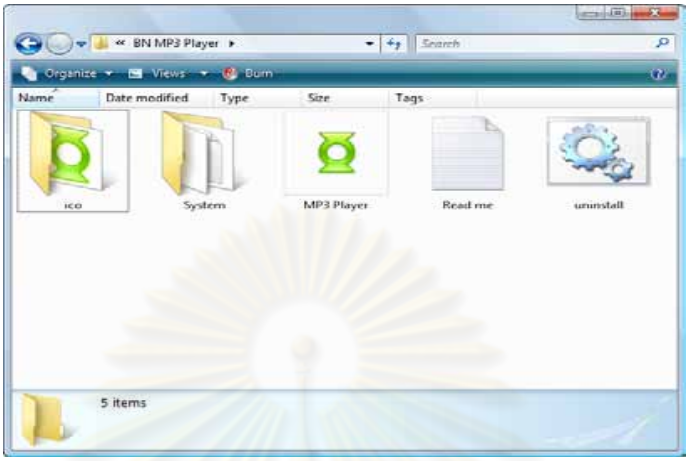


8. After finished embedding ADMP file it will show the success text in the text box below.



2. Digital Media Access Controller

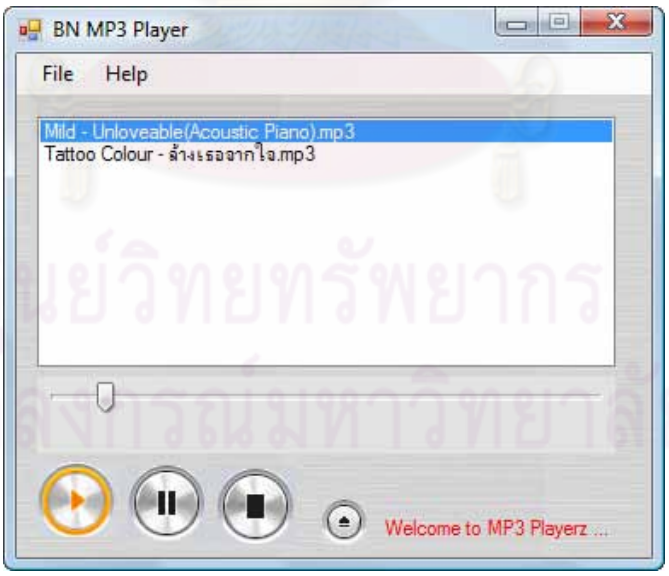
1. Open the folder that installed the BN MP3 Player.



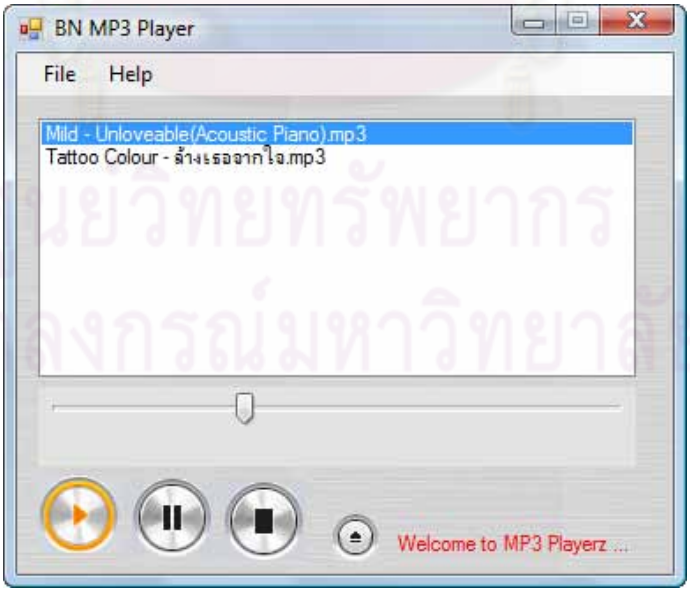
2. Double click on MP3 Player.exe to open the DMAC.

3. Click File -> Open File… and choose the protected audio file.

4. The audio file that we choose will be show in the DMAC playlist and you can double click on the name or press the play icon to start the playing process.



5. If you want to pause the audio file the you listening, you can press the pause button and you can press the play button if you want to continue playing.



6. If you want to stop playing the audio file, you can do it by press the stop button,

7. If you want to uninstall the program, you can do that by go to the folder that install the program and double click the uninstall.bat file to remove this program from your computer.

VITAE

Mister Kullapat Theera-angkanon was born on January 14th, 1987, in Bangkok, Thailand. He obtained his Bachelor's Degree in Computer Science from the Faculty of Science, Chulalongkorn University in 2008.

Research paper

1. "BENPro: A Blinding Protection method in Digital Right Management" presented at Seoul, Korea and published in IEEE-Computer Society.