ความปลอดภัยในระบบจัดการลิขสิทธิ์สื่อดิจิตอล

Digital Rights Management Security

คุณนิธิ ชาญเวชช์

วศะ โชคสุวัฒนสกุล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2550

ปริญญานิพนธ์ปีการศึกษา 2550

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ความปลอดภัยในระบบจัดการลิขสิทธิ์สื่อดิจิตอล

Digital Rights Management Security

ผู้จัดทำ

1. นายคุณนิธิ ชาญเวชช์ รหัสนักศึกษา 47010079
2. นายวศะ โชคสุวัฒนสกุล รหัสนักศึกษา 47010675

อาจารย์ที่ปรึกษา

(อาจารย์อัครเดช วัชระภูพงษ์)

อาจารย์ที่ปรึกษา

(ผศ.ธนา หงษ์สุวรรณ)

อาจารย์ที่ปรึกษา

(อาจารย์ธนัญชัย ตรีภาค)

ความปลอดภัยในระบบจัดการลิขสิทธิ์สื่อดิจิตอล

นายคุณนิธิ	ชาญเวชช์	47010079
นายวศะ	โชคสุวัฒนสกุล	47010675
อาจารย์อัครเดช	วัชระภูพงษ์	อาจารย์ที่ปรึกษา
ผศ.ธนา	หงษ์สุวรรณ	อาจารย์ที่ปรึกษา
อาจารย์ธนัญชัย	ตรีภาค	อาจารย์ที่ปรึกษา

ปีการศึกษา 2550

บทคัดย่อ

โครงงานนี้เป็นโครงงานที่มุ่งเน้นศึกษาระบบจัดการลิขสิทธิ์สื่อดิจิตอล เพื่อหาจุดอ่อนและปัญหาของระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่มีใช้ในปัจจุบัน แล้วนำมาแก้ไขเพื่อสร้างเป็นต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่เหมาะสมกับยุคสมัยปัจจุบัน

โดยการพัฒนาระบบจัดการลิขสิทธิ์บนสื่อดิจิตอลโดยเฉพาะสื่อดิจิตอลประเภทเพลงและภาพยนตร์นี้ เนื่องจากสื่อดิจิตอล โดยเฉพาะเพลงและภาพยนตร์ ได้เข้ามาทดแทนสื่อแบบดั้งเดิมแล้ว ส่งผลให้เกิดการละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญาผ่านสื่อดิจิตอลอย่างกว้างขวาง เพราะสื่อดิจิตอลเป็นสื่อที่สามารถคัดลอกได้ง่าย และเนื่องจากปัจจุบันระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่มีใช้อยู่ได้รับผลตอบรับในทางลบทำให้ผู้ใช้งานทั่วไป มีความต้องการที่จะเลิกใช้ ถึงแม้จะเป็นระบบที่ดีก็ตาม ดังนั้นต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่พัฒนาขึ้นนี้เพื่อใช้จัดการลิขสิทธิ์บนสื่อดิจิตอลโดยที่ยังคงความสามารถในการใช้งานทั่วไปของไฟล์ดิจิตอลไว้ โดยยึดถือหลักการที่ว่าผู้บริโภคที่เป็นผู้ซื้อสื่อดิจิตอลจะสามารถใช้งานได้คุณภาพสูง แต่ผู้ที่ละเมิดจะสามารถใช้งานได้คุณภาพต่ำ

Digital Rights Management Security

Mr. Khunnithi Chanvech	47010340
Mr. Wasa Choksuwattanasakul	47010675
Mr. Akkradach Watcharapupong	Advisor
Asst.Prof. Thanna Hongsuwan	Advisor
Mr. Thananchai Treepak	Advisor
Academic Year 2007	

ABSTRACT

This project focuses on study in digital rights management system on digital media. To find the weakness and problems of digital rights management system in the market for make solutions to solve them and develop new prototype of digital rights management system that based on security issue and be appropriate at this time

To develop digital rights management system based on digital media, digital audio and video, due to the fact that it replaces the old school media lead to widely intellectual property violated because digital file format is easy to copy and modify. In the last few years digitals rights management system most receives negative feedback. The new prototype of digital rights management system will use concept "You pay you gain otherwise you lose", which mean if you are authenticated user you will receive high quality but if you don't you will receive low quality.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ได้รับคำแนะนำและคำปรึกษาเกี่ยวกับการวิจัยและการค้นคว้าจาก อาจารย์อัครเดช วัชระภูพงษ์ อาจารย์ผู้ควบคุมปริญญานิพนธ์ และผศ.ธนา หงส์สุวรรณและอาจารย์ ธนัญชัย ตรีภาค ผู้ควบคุมปริญญานิพนธ์ร่วม ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากอาจารย์ทั้งสามท่านเป็นอย่างสูง

ขอบคุณห้องวิจัย ISAG ภาควิชาคอมพิวเตอร์ที่ได้สนับสนุนในส่วนของอุปกรณ์ เครื่องมือ ตลอดจนหนังสือต่างๆที่มีเอื้อประโยชน์แก่การวิจัยในครั้งนี้ด้วย

ขอกราบขอบพระคุณ คณาอาจารย์ รวมถึงผู้ช่วยสอนทุกท่านในภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังทุกท่านที่ประสิทธิ์ประสาทวิชาความรู้และประสบการณ์ดีๆให้แก่ข้าพเจ้ามาตลอดระยะเวลา 4 ปีที่ทำการศึกษา

ขอขอบคุณเพื่อนๆ พี่ๆ และน้องๆ ในภาควิชาวิศวกรรมคอมพิวเตอร์ที่คอยให้กำลังใจ และคำแนะนำ รวมถึงประสบการณ์ต่างๆที่ได้ทำร่วมกันตลอดมา

สุดท้ายนี้ข้าพเจ้าขอขอบพระคุณบิดา มารดาและครอบครัวของข้าพเจ้าที่เป็นกำลังใจและเป็นแรงผลักดันให้ข้าพเจ้าสามารถทำปริญญานิพนธ์นี้ด้วย

อย่างไรก็ตามข้าพเจ้าหวังเป็นอย่างยิ่งว่ารายงานของข้าพเจ้าจะเป็นประโยชน์ต่อทุกท่านและเป็นคำแนะนำแก่นักศึกษารุ่นต่อไปในอนาคตข้างหน้า

นายคุณนิธิ ชาญเวชช์

นายวศะ โชคสุวัฒนสกุล

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

รูปที่ **หน้า**

สารบัญภาพ(ต่อ)

รูปที่ **หน้า**

บทที่1
บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

โครงงานนี้เป็นโครงงานที่มุ่งเน้นศึกษาระบบจัดการลิขสิทธิ์สื่อดิจิตอล โดยเฉพาะเพลงและภาพยนตร์ในปัจจุบัน เพื่อหาจุดอ่อน และปัญหาของระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่มีใช้ในปัจจุบัน แล้วนำมาแก้ไขสร้างเป็นต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่เหมาะสมกับยุคสมัยปัจจุบัน

ปัจจุบันถือได้ว่าสื่อดิจิตอล โดยเฉพาะเพลงและภาพยนตร์ ได้เข้ามาทดแทนสื่อแบบดั้งเดิมแล้ว ส่งผลให้เกิดการละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญาผ่านสื่อดิจิตอลอย่างกว้างขวาง เนื่องจากสื่อดิจิตอลเป็นสื่อที่สามารถคัดลอกได้ง่าย ทำให้บริษัทและองค์กรชั้นนำอย่าง RIAA, Microsoft และ Apple ต่างพยายามพัฒนาและนำเสนอแนวทางการป้องกันการละเมิดดังกล่าว ซึ่งเรียกแนวทางเทคโนโลยีนั้นว่า Digital Rights Management

ทั้งนี้เนื่องมาจาก ความสะดวกในการใช้งานและความแพร่หลายของตัวโปรแกรมเล่นสื่อดิจิตอล ความรวดเร็วในการติดต่อสื่อสาร ไม่มีข้อจำกัดในเรื่องวัสดุในการบรรจุสื่อดิจิตอล เช่น ซีดี ดีวีดี เป็นต้น และโปรแกรมสมัยนี้สามารถทำให้เล่นสื่อดิจิตอลที่มีระบบจัดการลิขสิทธิ์สื่อดิจิตอลได้โดยง่าย ทำให้ผู้คนทั่วไปสนใจใช้โปรแกรมประเภทนี้ในการละเมิดลิขสิทธิ์สื่อดิจิตอลมากขึ้น ฝ่ายผู้บริโภค ที่ได้รับผลกระทบจากการบังคับ ด้วยโปรแกรมหรือชุดคำสั่งที่แฝงมากับสื่อดิจิตอลที่ซื้อมา โดยไม่มีการแจ้งเตือน หรือจากกฎข้อบังคับต่างๆ ของฝ่ายผู้ผลิตเองก็ตาม เช่น การบังคับให้เล่นกับเครื่องเล่นสื่อดิจิตอลทั่วไป เท่านั้นไม่สามารถเล่นในคอมพิวเตอร์ได้ หรือ การจำกัดการทำซ้ำ เป็นต้น เหมือนเป็นการละเมิดสิทธิ์ของผู้บริโภคทางหนึ่ง โครงการนี้จึงมุ่งพัฒนาโปรแกรมเพื่อนำมาใช้ผลิดสื่อดิจิตอลที่มีระบบจัดการลิขสิทธิ์สื่อดิจิตอล เพื่อให้เกิดการยอมรับ

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อศึกษาโครงสร้างและระบบการทำงานของระบบจัดการลิขสิทธิ์สื่อดิจิตอล (Digital Rights Management system)

1.2.2 เพื่อพัฒนาต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลให้มีเหมาะสมกับผู้ผลิตและผู้บริโภคในปัจจุบันยิ่งขึ้น

1.2.3 เพื่อสร้างโปรแกรมที่สามารถเข้าและถอดรหัสลับสื่อดิจิตอล เพื่อทำให้ผู้ใช้มั่นใจได้ว่า สื่อดิจิตอลที่มีการจัดการด้วยระบบจัดการลิขสิทธิ์สื่อดิจิตอลนี้ จะปลอดภัยต่อการลักลอบอ่าน / ทำซ้ำ / แก้ไข ข้อมูล

1.2.4 เพื่อสร้างโปรแกรมที่สามารถใช้เล่นสื่อดิจิตอลเพื่อใช้ในการทดสอบการเล่นสื่อดิจิตอลที่มีการจัดการด้วยระบบจัดการลิขสิทธิ์สื่อดิจิตอลนี้

1.3 ขอบเขตของโครงงาน

1.3.1 ได้ต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล ที่ใช้แนวคิดที่ว่า ถ้าผู้ใช้เป็นเจ้าของจริงจะสามารถใช้แล้วได้รับคุณภาพสูง แต่ถ้าไม่ใช่จะคุณภาพต่ำ ตามการตกลง

1.3.2 ได้โปรแกรมเล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์

1.3.3 ได้โปรแกรมผลิตสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์

1.4 ขั้นตอนการดำเนินการ

1.4.1 ศึกษาหาข้อมูลและโครงสร้างของ ระบบจัดการลิขสิทธิ์สื่อดิจิตอล (Digital Rights Management system) ในปัจจุบัน

1.4.2 ศึกษาปัจจัยที่เป็นผลดีและ ผลเสียของการใช้งานระบบจัดการลิขสิทธิ์สื่อดิจิตอล (Digital Rights Management system) ในปัจจุบัน

1.4.3 ออกแบบต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล

1.4.4 ศึกษาการวิธีการเขียนโปรแกรมติดต่อไฟล์สื่อดิจิตอลประเภทต่างๆ

1.4.5 ศึกษาการ โครงสร้างและการเขียนโปรแกรมเล่นสื่อดิจิตอล

1.4.6 ศึกษาการโครงสร้างและการขียนโปรแกรมเพื่อการเข้าและถอดรหัสลับ

1.4.7 ศึกษาอัลกอลิทึ่มที่จะนำมาใช้ในส่วน การซ้อนลายน้ำดิจิตอล (Digital Watermarking) โดยในที่นี้ ใช้การ การซ่อน Text ในการทำ MP3 Encoder

1.4.8 ศึกษาและเขียนโปรแกรมในส่วนของอินเตอร์เฟสและการติดตั้ง

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 สามารถรู้และเข้าใจการทำงานของระบบจัดการลิขสิทธิ์สื่อดิจิตอล (Digital Rights Management system) ในปัจจุบันเพื่อนำมาปรับให้เหมาะสมกับยุคสมัย

1.5.2 ผู้ใช้สามารถใช้งานสื่อดิจิตอลที่ มีการจัดการด้วยระบบจัดการลิขสิทธิ์สื่อดิจิตอล (Digital Rights Management system) ได้อย่างพอใจ และไม่รู้สึกโดนบังคับจนเกินไป

1.5.3 สามารถตรวจสอบได้ว่า สื่อดิจิตอลที่มีลิขสิทธิ์ เป็นของใคร และอาจใช้เป็นหลักฐานทางกฎหมายได้

1.5.4 ช่วยลดการต่อต้านระบบจัดการลิขสิทธิ์สื่อดิจิตอล (Digital Rights Management system) ในปัจจุบัน ซึ่งผลิตออกมาใช้ในเชิงบังคับ และผูกขาด ทำให้เกิดผลกระทบต่อการใช้งานต่อผู้บริโภค ซึ่งอาจเป็นผลให้ความพยายามละเมิดลิขสิทธิ์สื่อดิจิตอลจากการถูกบังคับลดลง

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 5 บทด้วยกัน ดังต่อไปนี้

บทที่ 1 กล่าวถึงความเป็นมาและความสำคัญของปัญหา ความมุ่งหมายและวัตถุประสงค์ ขอบเขตของการศึกษา ขั้นตอนของการศึกษา ประโยชน์ที่คาดว่าจะได้รับ และ ส่วนประกอบของปริญญานิพนธ์

บทที่ 2 กล่าวถึงทฤษฎีและหลักการที่ใช้ในการพัฒนาโดยประกอบไปด้วยทฤษฎีพื้นฐานเกี่ยวกับระบบจัดการลิขสิทธิ์สื่อดิจิตอล, ทฤษฎีรูปแบบของไฟล์สื่อดิจิตอล, ทฤษฎีการการเข้าและถอดรหัสข้อมูล, ทฤษฎีการการซ้อนลายน้ำดิจิตอล และทฤษฎีเกี่ยวกับ CSS และ DeCSS

บทที่ 3 กล่าวถึงการออกแบบและการพัฒนา โดยวาง โครงสร้างของต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล และการออกแบบต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล,การออกแบบและการพัฒนาซอฟต์แวร์สร้างสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ (ISAGDRM)และซอฟต์แวร์เล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ (ISAG Player) โดยจะกล่าวถึงขั้นตอนการทำงานของซอฟต์แวร์และขั้นตอนการทำงานของระบบจัดการลิขสิทธิ์ ISAGDRMS

บทที่ 4 กล่าวถึงการทดลอง และ ผลการทดลอง การเขียนโปรแกรม ติดต่อสื่อดิจิตอลประเภทต่างๆ การสร้างระบบจัดการลิขสิทธิ์บนสื่อดิจิตอล และผลทดทองการเปรียบเทียบคุณภาพของสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ กับไฟล์สื่อดิจิตอลทั่วไป และเปรียบเทียบการใช้งานด้วยซอฟต์แวร์เล่นสื่อดิจิตอลทั่วไปกับซอฟต์แวร์ของโครงการ

บทที่ 5 เป็นบทวิจารณ์และสรุปซึ่งกล่าวถึงบทสรุปของโครงงาน ปัญหาและอุปสรรคและแนวทางการแก้ไข แนวทางในการพัฒนาต่อไปในอนาคต 3

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 ทฤษฎีพื้นฐานที่เกี่ยวข้องกับโครงงาน

2.1.1 ระบบจัดการลิขสิทธิ์สื่อดิจิตอล

ระบบจัดการลิขสิทธิ์สื่อดิจิตอล (DRMs หรือDigital Rights Management system) คือ ระบบการจัดการสิทธิ์ของผู้ใช้ข้อมูลที่อยู่ในรูปแบบดิจิตอล เป็นข้อกำหนดที่ว่าด้วยการเข้าถึงข้อมูลภายในสื่อ คือ ผู้ผลิตจะกำหนดว่า ผู้ที่ซื้อสามารถทำอะไรกับสินค้าที่ซื้อไปได้บ้าง ผู้ที่ซื้อสื่อเหล่านั้นจะสามารถเล่นได้ที่ไหนและอย่างไร ซึ่งก็รวมถึงการอนุญาตให้มีการทำซ้ำหรือการทำสำเนาด้วย หรืออีกนัยหนึ่งคือผู้ที่ซื้อเพลงหรือภาพยนตร์ ที่มี DRM ติดมาด้วยนั้นจะไม่สามารถเป็นเจ้าของได้อย่างแท้จริง แต่จะเป็นเพียงผู้ที่มีสิทธิ์ในการเล่นสื่อเท่านั้น นอกจากนั้น DRM

ในปัจจุบันได้มีการติดตั้ง DRM ลงไปไว้กับอุปกรณ์ต่าง ๆ มากมาย เช่น เครื่องเล่นดีวีดี เครื่อง iPod หรือแม้กระทั่งเครื่องพีซีที่ใช้ระบบปฏิบัติการวินโดว์สก็มีการนำ DRM มาใช้แล้ว

2.1.2 องค์ประกอบของระบบจัดการลิขสิทธิ์สื่อดิจิตอล

- Encryption กระบวนการการเข้ารหัส
- Access control (conditional access) เงื่อนไขการใช้งาน หรือการเข้าถึงข้อมูล
- Copy control or copy prevention การป้องกันการคัดลอก หรือทำซ้ำข้อมูล
- Identification and tracing การพิสูจน์ตัวตนเพื่อการใช้งาน หรือการตรวจสอบข้อมูล

2.1.3 ผลกระทบต่อระบบจัดการลิขสิทธิ์สื่อดิจิตอล

สิ่งที่ต้อง คำนึงในการนำ DRM มาใช้ว่าจะมีผลกระทบต่อการเข้าถึง หรือการใช้งานสื่อดิจิตอลอย่างไร โดยสามารถแบ่งวัดผลกระทบได้ 4 ปัจจัย คือ

- Transparency

การมีอยู่ของ DRM คือ ผู้ใช้สื่อดิจิตอลรู้ว่าสื่อดิจิตอลที่ให้งานอยู่มี การจัดการด้วย DRMs หรือไม่ หรือ ผู้ใช้ได้รับข้อมูล หรือข้อตกลงการใช้งาน หรือผลกระทบอย่างไรบ้าง

- Effect on Use

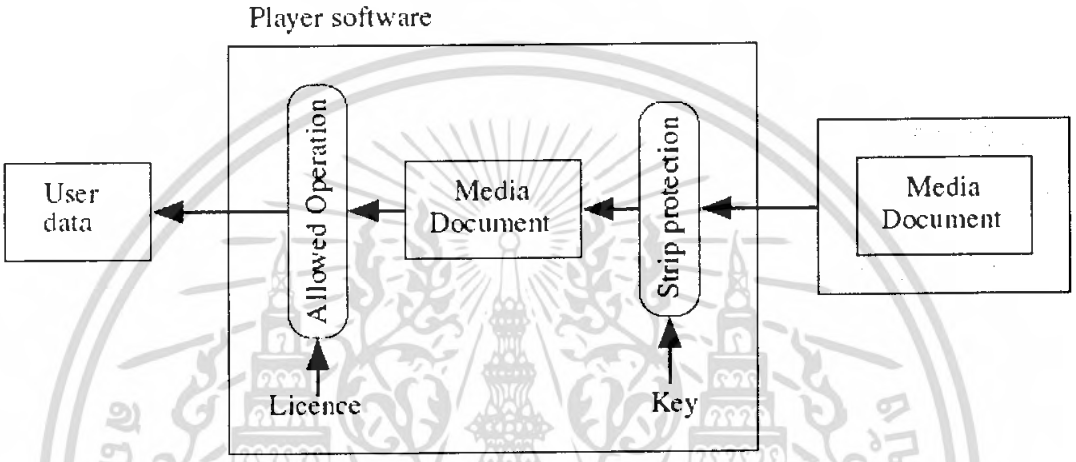
เงื่อนไขในการใช้งาน การเข้าถึงข้อมูล มีผลกระทบต่อการใช้งานมากน้อยเพียงใด ทำให้การใช้งานยุ่งยากมากขึ้นหรือไม่ ทั้งในด้านของการใช้ซอฟต์แวร์ หรือ เครื่องมือในการใช้งานสื่อก็ตาม

- Collateral Impact

ผลกระทบด้านอื่นๆ ที่มีต่อผู้ใช้งาน มีมากน้อยเพียงใด เช่น การละเมิดสิทธิ์ผู้บริโภค ละเมิดความเป็นส่วนตัว เป็นต้น

- Purpose and Consumer Benefit

จุดประสงค์การนำ DRMs มาใช้ต้องชัดเจน ว่าทำเพื่อการพัฒนาระบบธุรกิจรูปแบบใหม่ หรือต้องการเพียงแค่จะบังคับผู้บริโภคในด้านต่างๆเท่านั้น



รูปที่ 2.1 แสดงการทำงานของระบบจัดการลิขสิทธิ์สื่อดิจิตอล บนโปรแกรมเล่นสื่อดิจิตอล

2.1.4 ประโยชน์ของระบบจัดการลิขสิทธิ์สื่อดิจิตอล

2.1.4.1 การป้องกันการละเมิดลิขสิทธิ์ด้วยการเข้ารหัสลับด้วยโครงสร้างกุญแจพื้นฐานสาธารณะนั้น สามารถช่วยป้องกันไม่ให้โปรแกรมโดยทั่วไป สามารถลักลอบอ่าน / ทำซ้ำ / แก้ไข สื่อดิจิตอลที่มีลิขสิทธิ์ได้ โดยผู้ที่จะสามารถมีสิทธิ์ใช้สื่อลิขสิทธิ์ได้นั้น มีเพียงผู้ซื้อที่ถูกต้องเท่านั้น และสามารถตรวจสอบได้ว่าสื่อดิจิตอลนั้นเป็นสื่อดิจิตอลที่มีลิขสิทธิ์ ได้

2.1.4.2 ได้ระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่ เหมาะสมและยอมรับได้จากทั้งทางผู้ผลิตและผู้บริโภค คือยังคงต้องรักษาและป้องกันการละเมิดลิขสิทธิ์ และต้องไปเป็นการละเมิดหรือบังคับสิทธิ์ของผู้บริโภคจนเกินไป

2.1.4.3 ได้นำระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่ดี ได้รับการตอบรับที่ไม่ดีกลับมาพัฒนาให้ดีและน่าใช้ยิ่งขึ้น ที่ไม่ใช่การบังคับใช้เหมือนระบบที่มีในปัจจุบัน แต่เป็นควบคุมด้านต่างๆของไฟล์ดิจิตอล เช่นการลดทอนคุณภาพ และเพิ่มบางอย่างให้ตรวจสอบได้ว่าสื่อดิจิตอลนั้นๆมีลิขสิทธิ์ หรือไม่

2.1.5 จุดอ่อนของระบบจัดการลิขสิทธิ์สื่อดิจิตอล

จากการศึกษาจะเห็นได้ว่า จุดอ่อนที่สำคัญของ ระบบ DRM ในปัจจุบัน ก็คือการ ที่ต้องการบังคับหรือควบคุมผู้ใช้ในการเข้าถึงข้อมูลสื่อดิจิตอล แต่ในขณะเดียวกันก็ยังต้องทำให้ผู้ใช้เข้าถึงได้โดยผ่านกรรมวิธี ต่างๆ ซึ่งเป็นความพยายามดังกล่าวทำให้ระบบ DRM มีช่องโหว่ เช่น ทำการเข้ารหัสข้อมูลไม่ให้สามารถเล่นได้ แต่เมื่อผ่าน player ของระบบเองก็การถอดรหัส ออกทำให้เล่นได้ ถ้ามีความพยายามที่ต้องการจะดักจับข้อมูลส่วนนี้ ก็สามารถทำได้

2.1.6 ปัญหาของระบบจัดการลิขสิทธิ์สื่อดิจิตอล

จากการศึกษาระบบจัดการลิขสิทธิ์สื่อดิจิตอลในปัจจุบัน

<u>ปัญหาในมุมมองของผู้บริโภค</u>

2.1.6.1 มีความไม่พอใจมาก จำกัดสิทธิ์ของผู้ใช้ เช่น แม้จะซื้อมา แต่จะมีความรู้สึกไม่ได้เป็นเจ้าของ 100%

2.1.6.2 ระบบจัดการลิขสิทธิ์สื่อดิจิตอลบางตัวที่ติดมา บังคับผู้บริโภค เช่น เล่นได้กับ player ในเครือ หรือเล่นในคอมพิวเตอร์ไม่ได้ มีการแบ่งโซน หรือเล่นได้กับบางเครื่องเล่นเท่านั้น

2.1.6.3 ใช้งานยุ่งยาก เช่น สื่อที่เป็นการซื้อออนไลน์ หรือ ตัวโปรแกรม ต้องการการตรวจสอบผ่าน internet ว่าเป็นสื่อที่มลิขสิทธิ์

2.1.6.4 ระบบจัดการลิขสิทธิ์สื่อดิจิตอลบางตัวทำตัวเป็น malware ฝังตัวอยู่โดยไม่มีการบอกผู้บริโภค และออกมาบังคับเครื่องเล่น หรือ การใช้งานเป็นการละเมิดสิทธิ์ผู้บริโภค คล้ายเป็น Ester Egg program ที่ฝังมากับ software

2.1.6.5 บางครั้งถึงกับมีการ ล็อคเครื่องเล่น ไม่ให้เล่นได้อย่างอิสระ

<u>ปัญหาในมุมมองของผู้ผลิต</u>

2.1.6.6 ต้องการสร้างระบบจัดการลิขสิทธิ์สื่อดิจิตอลขึ้นมาเพื่อจะเป็นการป้องกันการละเมิดลิขสิทธิ์

2.1.6.7 รักษาผลประโยชน์ทางการตลาด

2.1.6.8 ต้องสร้างระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่มีความแข็งแกร่งเพิ่มขึ้นตลอดเวลา เพราะ มีความพยายาม ที่จะละเมิดอยู่ตลอด

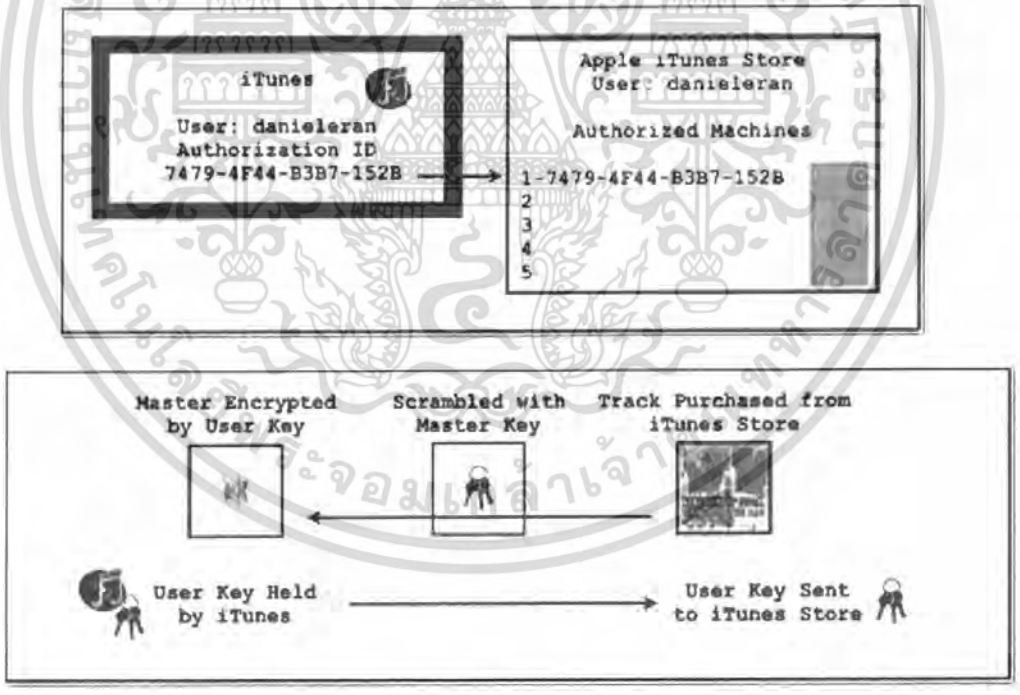
2.1.6.9 ต้องสร้างระบบการซื้อขายรูปแบบใหม่ๆ ตลอด เช่น ซื้อแบบ online เป็นการเลี่ยงการละเมิดลิขสิทธิ์ และลดต้นทุนด้านวัสดุ เช่น ซีดี ดีวีดี เป็นต้น

จะเห็นว่าเป็นปัญหาซึ่ง มีผลประโยชน์ ที่ขัดกันชัดเจน ทำให้ การพัฒนาระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่ดี หรือเหมาะสมเป็นไปได้ยาก หรือจะทำให้การละเมิดลิขสิทธิ์ หมดไปเป็นไปไม่ได้เลย และจากการศึกษาประวัติของระบบจัดการลิขสิทธิ์สื่อดิจิตอล จากอดีตจนถึงปัจจุบันจะเห็นได้ว่า เทคโนโลยีที่ใกล้ตาย ไม่ใช่เพราะระบบจัดการลิขสิทธิ์สื่อดิจิตอลเป็นเทคโนโลยีที่ไม่ดี แต่เป็นเพราะ การนำมาใช้ทำให้เกิดผลเสียมากกว่าผลดี ทำให้ไม่มีผู้ใดต้องการใช้ เห็นได้ จากเริ่มมีการปลดระบบจัดการลิขสิทธิ์สื่อดิจิตอลออกจากสื่อดิจิตอล ของค่ายสื่อดิจิตอลรายใหญ่ เช่น Apple เป็นต้น

2.1.7 ตัวอย่างการละเมิดลิขสิทธิ์สื่อดิจิตอล

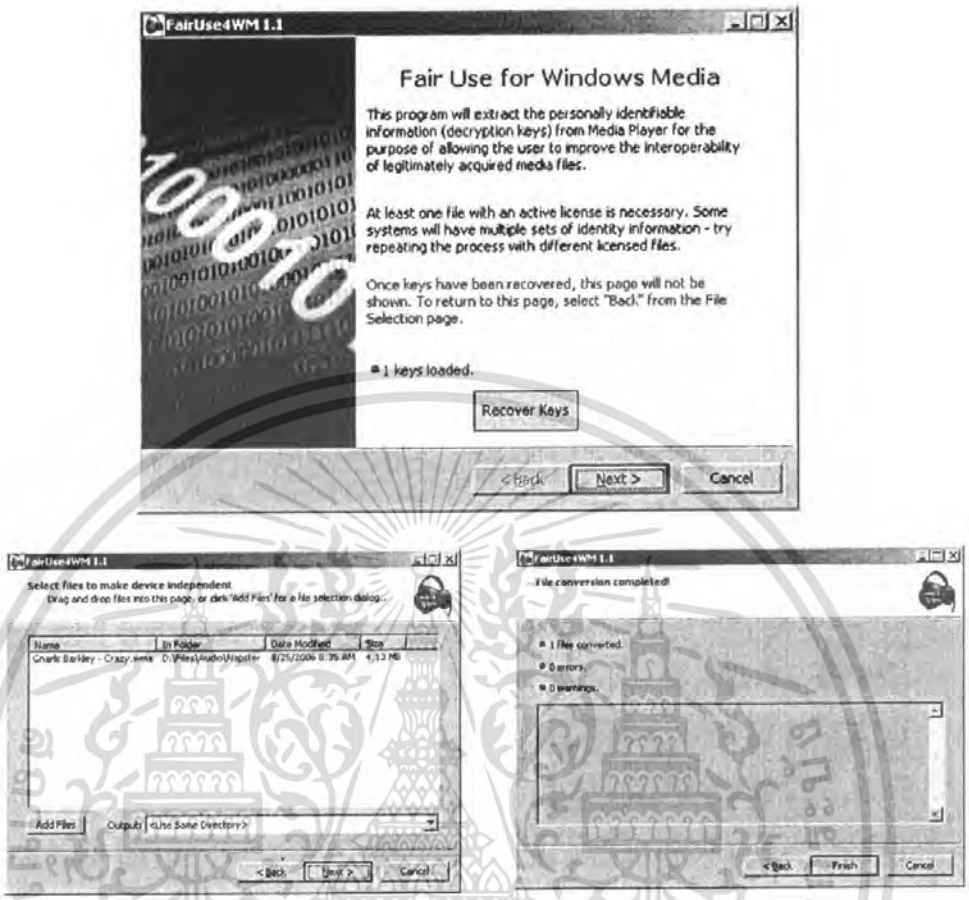
จากการศึกษาระบบการซื้อขายสื่อดิจิตอลของบริษัทต่างๆ เช่น

- Microsoft ----> PlayForSure
- Apple ----> FairPlay
- Open source ----> CSS on DVD



รูปที่ 2.2 แสดงการทำงานของระบบจัดการลิขสิทธิ์สื่อดิจิตอลของ Apple

- FairUse4WM เป็นโปรแกรมที่ใช้ในการ ปลด DRM ของ Microsoft



รูปที่ 2.3 แสดงการทำงานของโปรแกรม FairUse4WM

- ใช้โปรแกรม QTFairUse crack Fairplay โดยโปรแกรมจะเข้าไปดักข้อมูลหลังจากที่ iTune แกะ DRM เสร็จแล้ว
- โปรแกรม ในการ Rip CD เช่น iTunes , Windows Media Player
- การเขียนโปรแกรม อัดเสียงจากลำโพง โดยใช้ไมโครโฟน

2.2 ทฤษฎีรูปแบบของไฟล์สื่อดิจิตอล

2.2.1 นิยามและความหมาย

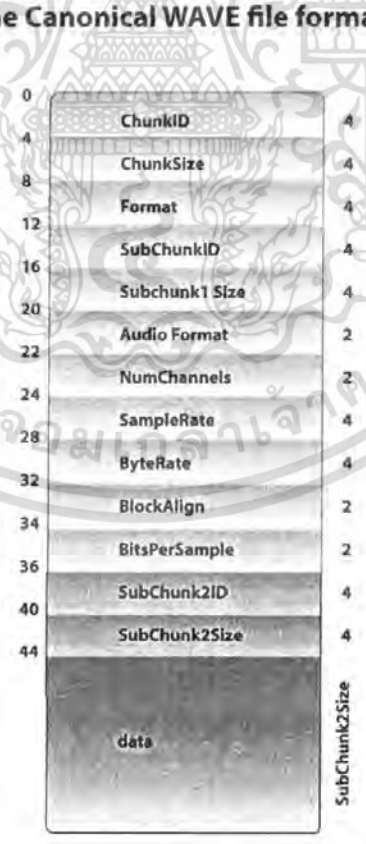
การจัดเก็บข้อมูลภาพ เสียง ข้อมูลต่างๆของสื่อ ไว้ในรูปของ Digital Format ไม่ว่าจะในรูปของเลขฐาน 2 หรือเลขฐาน 16 ก็ตาม ทำให้อยู่ในรูปแบบที่คอมพิวเตอร์ ใช้งานทำให้การเข้าถึงข้อมูล หรือการแก้ไขทำได้ง่ายและรวดเร็วขึ้น

ซึ่งความนิยมของคนทั่วไปในการเก็บสื่อบันเทิงต่างๆ ไว้ในรูปแบบของ Digital File เพิ่มสูงขึ้นเรื่อยๆ เพราะเป็นการจัดเก็บที่ง่าย รวดเร็ว ประหยัดเนื้อที่และสะดวกในการเรียกใช้

2.2.2 ประเภทและรูปแบบของไฟล์สื่อดิจิตอล

2.2.2.1 WAVE

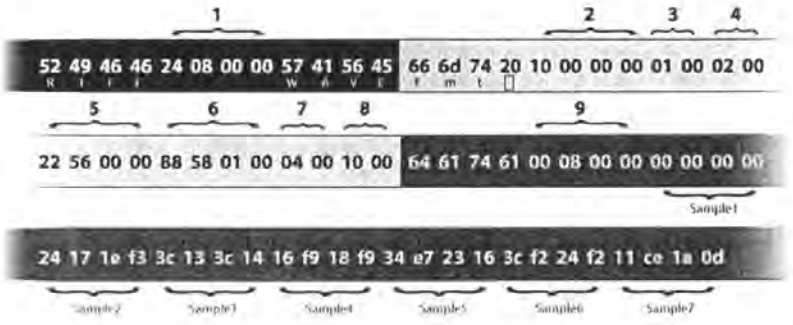
เป็นส่วนหนึ่งของ Microsoft RIFF สำหรับรองรับไฟล์ประเภท Multimedia โดยเริ่มต้นด้วยส่วนที่เรียกว่า Header และตามมาด้วยส่วนของข้อมูล โดย Wave จะประกอบไปด้วย 2 ส่วน คือ fmt ที่เก็บรายละเอียดของรูปแบบของข้อมูล และ data ที่เก็บข้อมูลจริงๆ โดยทั้งหมดนี้รวมเรียกว่า "Canonical form" โดย ณ ที่นี้จะใช้มาตราฐานของ Wave ที่สร้างขึ้นด้วย sox program



รูปที่ 2.4 แสดงรูปแบบการเรียงข้อมูลของไฟล์รูปแบบ wave

ตารางที่ 2.1 แสดงความหมายของข้อมูลที่เรียงกันในไฟล์ WAVE ส่วนหัวของแต่ละโครงสร้าง (Frame header)

ตำแหน่ง	ขนาด	ชื่อ	คำอธิบาย
0	4	ChunkID	เก็บตัวอักษร RIFF ในรูปแบบ ASCII
4	4	ChunkSize	คือขนาดของไฟล์ในหน่วย Byte ลบออกด้วย 8 สำหรับ 2 f2 fields รวมตัวเองด้วย
8	4	Format	เก็บตัวอักษร WAVE
12	4	Subchunk1ID	เก็บตัวอักษร fmt
16	4	Subchunk1Size	16 สำหรับ PCM เก็บค่าขนาดของ Subchunk ที่เหลือ
20	2	AudioFormat	PCM = 1 ค่าอื่นที่ไม่ใช่ 1 ใช้สำหรับรูปแบบการบีบอัด
22	2	NumChannels	Mono = 1 ,Stereo = 2,อื่นๆ
24	4	SampleRate	8000,44100, อื่นๆ
28	4	ByteRate	คือ SampleRate x NumChannels x BitsPerSample / 8
32	2	BlockAlign	คือ NumChannel x BitsPerSample / 8
34	2	BitsPerSample	8 bits คือ 8 ,16 bits คือ 16
36	4	SubChunk2ID	เก็บตัวอักษร data
40	4	SubChunk2Size	คือ NumSamples x NumChannels x BitsPerSample / 8
44	*	Data	ข้อมูลเสียงที่ใช้ในการฟัง



1. ChunkSize = 2084
2. Subchunk1Size = 16
3. AudioFormat = 1 (PCM)
4. NumChannels = 2
5. SampleRate = 22050
6. ByteRate = 88200
7. BlockAlign = 4
8. BitsPerSample = 16
9. Subchunk2Size = 2048

รูปที่ 2.5 แสดงตัวอย่างการเรียงข้อมูลของไฟล์รูปแบบ wave

2.2.2.2 MP3 (MPEG1 Audio Layer 3)

MPEG1 Audio Layer 3 (MP3) นั้นคือรูปแบบการเข้ารหัสของเสียง ซึ่งใช้วิธีการที่เรียกว่า Lossy compression algorithm ซึ่งทำให้ขนาดของไฟล์เล็กลงแต่ยังคงคุณภาพของเสียงไว้ได้ในระดับที่ดีมาก เทคโนโลยีนี้ถูกพัฒนาโดยทีมวิศวกรจากยุโรป ประกอบไปด้วย Philips , CCETT , IRT และ Fraunhofer Society ได้รับรองมาตรฐานจาก ISO/IEC ในปี 1991

โครงสร้างของ MP3 นั้นประกอบไปด้วย เฟรม (Frame) ของข้อมูลจำนวนมากมายมาประกอบกัน ซึ่ง MP3 นั้นจะไม่มี header หลัก แต่จะประกอบไปด้วยหลายๆ เฮดเดอร์ (Frame Header)ที่อยู่ใน เฟรม (Frame) โดยภายในแต่ละ เฟรม (Frame) นั้นประกอบไปด้วยส่วนที่เรียกว่า เฮดเดอร์ (Frame Header)และ Data โดยมีรายละเอียดดังนี้

<u>ส่วนหัวของแต่ละโครงสร้าง (Frame header)</u>

เฮดเดอร์ (Frame Header)ประกอบไปด้วยข้อมูลทั้งหมด 32 bits ภายในจะเก็บข้อมูลของ Data ภายในนั้น ซึ่งภายในอาจจะเป็นอิสระต่อกันหรือไม่อิสระต่อกันนั้นขึ้นอยู่กับการจัดการในขั้นตอนการบีบอัด ดังนั้น MP3 อาจไม่สามารถตัดเพียงบาง เฟรม (Frame) ไปใช้ฟังได้ แต่ละ เฟรม (Frame) อาจเหมือนกันหรือไม่เหมือนกันก็ได้ซึ่งก็ขึ้นอยู่กับส่วนของ Data นั้นเอง ตัวอย่างเช่น MPEG สามารถทำ Variable bitrate MPEG(VBR) หรือ Bitrate switching คือการทำให้ Data ในแต่ละ เฟรม (Frame) มี Bitrate ที่แตกต่างกัน

ใน 11 bits แรกของ เฮดเดอร์ (Frame Header)นั้นจะถูกตั้งค่าให้เป็น 1 ทั้งหมด ดังนั้นการเขียนโปรแกรมเพื่อติดต่อกับส่วน เฮดเดอร์ (Frame Header)นั้นสามารถค้นหาได้จากการใช้ประโยชน์จากส่วนนี้(คือการทำการค้นหา Byte ที่มีค่า 255 และตามมาด้วย 1 ทั้งหมด 3 bits จากทางที่มีความหมายมากที่สุด)

โครงสร้างของ เฟรม (Frame) อาจไม่ได้มีเฉพาะ เฮดเดอร์ (Frame Header)และ Data ได้ ถ้าภายใน เฮดเดอร์ (Frame Header)มีการกำหนดค่าที่เรียกว่า Protection bit จะมีการเพิ่มส่วนตรวจสอบ CRC เข้ามาอีก 16 bits ต่อจาก เฮดเดอร์ (Frame Header)และตามด้วย Data ข้อมูลของเสียงที่เก็บใน เฮดเดอร์ (Frame Header)นั้นมีทั้งหมด 13 ชนิด แสดงได้ตามแผนภาพดังนี้

รูปที่ 2.6 แสดงรูปแบบของเฮดเดอร์ (Frame Header)ของไฟล์ MP3

ตารางที่ 2.2 แสดงความหมายของข้อมูลแต่ละชนิดที่เรียงกันใน MP3 ส่วนหัวของแต่ละโครงสร้าง (Frame header)

สัญลักษณ์	ความยาว (bits)	รายละเอียด
A	11	Frame sync (ทุก bit ถูกกำหนดค่าเป็น 1)
B	2	MPEG Audio version ID 00 – MPEG version 2.5 01 – ไม่อนุญาต 10 – MPEG version 2 (ISO/IEC 13818-3) 11 – MPEG version 1 (ISO/IEC 11172-3)

<table>
<tr><th>สัญลักษณ์</th><th>ความยาว (bits)</th><th>รายละเอียด</th></tr>
<tr><td>C</td><td>2</td><td>รายละเอียดของ Layer
00 – ไม่อนุญาต
01 – Layer 3
10 – Layer 2
11 – Layer 1</td></tr>
<tr><td>D</td><td>1</td><td>Protection bit
0 – ได้รับการปกป้องโดย CRC (16bits CRC ต่อจาก ส่วนหัวของแต่ละโครงสร้าง (Frame header))
1 – ไม่ได้รับการปกป้อง</td></tr>
<tr><td>E</td><td>4</td><td>ข้อมูลของ Bitrate
<table>
<tr><th>bits</th><th>V1,L1</th><th>V1,L2</th><th>V1,L3</th><th>V2,L1</th><th>V2, L2 & L3</th></tr>
<tr><td>0000</td><td>free</td><td>free</td><td>free</td><td>free</td><td>free</td></tr>
<tr><td>0001</td><td>32</td><td>32</td><td>32</td><td>32</td><td>8</td></tr>
<tr><td>0010</td><td>64</td><td>48</td><td>40</td><td>48</td><td>16</td></tr>
<tr><td>0011</td><td>96</td><td>56</td><td>48</td><td>56</td><td>24</td></tr>
<tr><td>0100</td><td>128</td><td>64</td><td>56</td><td>64</td><td>32</td></tr>
<tr><td>0101</td><td>160</td><td>80</td><td>64</td><td>80</td><td>40</td></tr>
<tr><td>0110</td><td>192</td><td>96</td><td>80</td><td>96</td><td>48</td></tr>
<tr><td>0111</td><td>224</td><td>112</td><td>96</td><td>112</td><td>56</td></tr>
<tr><td>1000</td><td>256</td><td>128</td><td>112</td><td>128</td><td>64</td></tr>
<tr><td>1001</td><td>288</td><td>160</td><td>128</td><td>144</td><td>80</td></tr>
<tr><td>1010</td><td>320</td><td>192</td><td>160</td><td>160</td><td>96</td></tr>
<tr><td>1011</td><td>352</td><td>224</td><td>192</td><td>176</td><td>112</td></tr>
<tr><td>1100</td><td>384</td><td>256</td><td>224</td><td>192</td><td>128</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td>
<table>
<tr><td>1101</td><td>416</td><td>320</td><td>256</td><td>224</td><td>144</td></tr>
<tr><td>1110</td><td>448</td><td>384</td><td>320</td><td>256</td><td>160</td></tr>
<tr><td>1111</td><td>bad</td><td>bad</td><td>bad</td><td>bad</td><td>bad</td></tr>
</table>
โดย V คือ Version และ L คือ Layer
Free หมายถึง รูปแบบที่อิสระ หากมีการกำหนดในลักษณะนี้ จะหมายถึง Bitrate ที่ใช้นั้นไม่ได้มีกำหนดไว้ในตามตารางนี้ ซึ่ง Bitrate ที่นำมาใช้นั้นจะต้องคงที่ตลอดทั้งเพลง
</td></tr>
<tr><td>F</td><td>2</td><td>Sampling rate frequency
<table>
<tr><th>Bits</th><th>MPEG1</th><th>MPEG2</th><th>MPEG2.5</th></tr>
<tr><td>00</td><td>44100</td><td>22050</td><td>11025</td></tr>
<tr><td>01</td><td>48000</td><td>24000</td><td>12000</td></tr>
<tr><td>10</td><td>32000</td><td>16000</td><td>8000</td></tr>
<tr><td>11</td><td>จอง</td><td>จอง</td><td>จอง</td></tr>
</table>
</td></tr>
<tr><td>G</td><td>1</td><td>Padding bit
0 – เฟรม (Frame) นั้นไม่ถูกเพิ่ม
1 – เฟรม (Frame) นั้นถูกเพิ่ม
Padding นั้นถูกนำมาใช้ในการคำนวณ ความยาวของ เฟรม (Frame) ที่จะได้กล่าวถึงต่อไป</td></tr>
<tr><td>H</td><td>1</td><td>Private bit
เปิดให้ใช้ได้อย่างอิสระสำหรับการโปรแกรมที่ต้องการกำหนดค่าไว้ใน ส่วนหัวของแต่ละโครงสร้าง (Frame header)</td></tr>
<tr><td>I</td><td>2</td><td>Channel Mode
00 – Stereo
01 – Join stereo</td></tr>
</table>

		10 – Dual channel 11 – Single channel
J	2	Mode extension (ใช้สำหรับ Join stereo เท่านั้น)
K	1	Copyright 0 – ไฟล์เสียงไม่มีลิขสิทธิ์ 1 – ไฟล์เสียงมีลิขสิทธิ์
L	1	Original 0 – ไฟล์เสียงนี้เป็นไฟล์แรกที่ไม่ได้ถูกทำซ้ำ 1 – ไฟล์สียงนี้ถูกทำซ้ำ
M	2	Emphasis 00 – none 01 – 50/15 ms 10 – reserved 11 – CCIT J.17

การคำนวณหาขนาดของแต่ละ เฟรม (Frame) นั้น ทำได้โดยใช้สมการดังนี้

สำหรับ MPEG1 Layer 3

Frame LengthInByte = 144 x Bitrate / (SampleRate + padding)

MP3 Data

เป็นส่วนที่เก็บข้อมูลเสียงที่อยู่ในรูปแบบที่ถูกบีบอัดเอาไว้ สำหรับการบีบอัดของข้อมูลเสียงนี้เป็นหนึ่งในวิธีการบีบอัดข้อมูลของ Digital โดยมีความพยายามให้ขนาดของไฟล์นั้นเล็กที่สุดแต่ก็ยังคงรักษาคุณภาพของเสียงเอาไว้ให้คล้ายกับต้นฉบับที่สุด ซึ่ง MPEG นั้นเป็น 1 ในการบีบอัดที่ดีที่สุด

การบีบอัดของ MPEG นั้นใช้กระบวนการที่เรียกว่า Lossy Algorithm ซึ่งทำให้ข้อมูลบางส่วนถูกตัดทิ้งไปและไม่สามารถกู้กลับคืนมาได้ แต่ข้อมูลที่หายไปนั้นคือข้อมูล

เสียงที่ยากจะได้ยินแม้จะเป็นข้อมูลก่อนบีบอัด นั้นคือการตัดข้อมูลส่วนที่เป็นข้อจำกัดของหูของมนุษย์ออกไปนั้นเอง

ID3 tag

ID3 เป็นข้อมูลที่ถูกเพิ่มเติมเข้ามาสำหรับเพิ่มรายละเอียดเกี่ยวกับเสียงนั้นให้กับไฟล์ประเภท MP3 โดยจะเก็บรายละเอียดเกี่ยวกับ ศิลปิน,ชื่อเพลง,ชื่ออัลบัม,ปีที่จัดจำหน่าย,ประเภทของเพลง นอกจากนั้นยังมีพื้นที่ให้กับการเขียน comment เพิ่มเติมอีกด้วย

2.2.2.3 AVI (Audio Video Interleave)

ข้อมูลพื้นฐาน

1 Chunks

```
typedef struct {
        DWORD dwFourCC
        DWORD dwSize
        BYTE data[dwSize] // contains Frame headers or video/audio data
} CHUNK;
```

2 Lists

```
typedef struct {
        DWORD dwList
        DWORD dwSize
        DWORD dwFourCC
        BYTE data[dwSize-4] // contains Lists and Chunks
} LIST;
```

Chunk คือส่วนที่ใช้สำหรับเก็บภาพและเสียง หรือคำบรรยาย โดยใช้ dwFourCC เป็นตัวกำกับหมายเลขของ stream และ ชนิดของข้อมูล โดยใน Lists เองก็ทำหน้าที่เดียวกัน ส่วน dwSize เก็บขนาดของ chunks หรือ Lists

รูปแบบของ AVI โดยทั่วไปจะมี 3 รูปแบบ

- AVI 1.0 เป็นต้นรูปแบบแรก ซึ่งเก่ามาก
- Open-DML เป็นการเพิ่มเติมสำหรับ AVI โดยมีส่วนเพิ่มเติมที่สำคัญคือ

- สร้างไฟล์ขนาดใหญ่มากได้ (มากกว่าที่ NTFS อนุญาต)

- ลด overhead ลง 33%

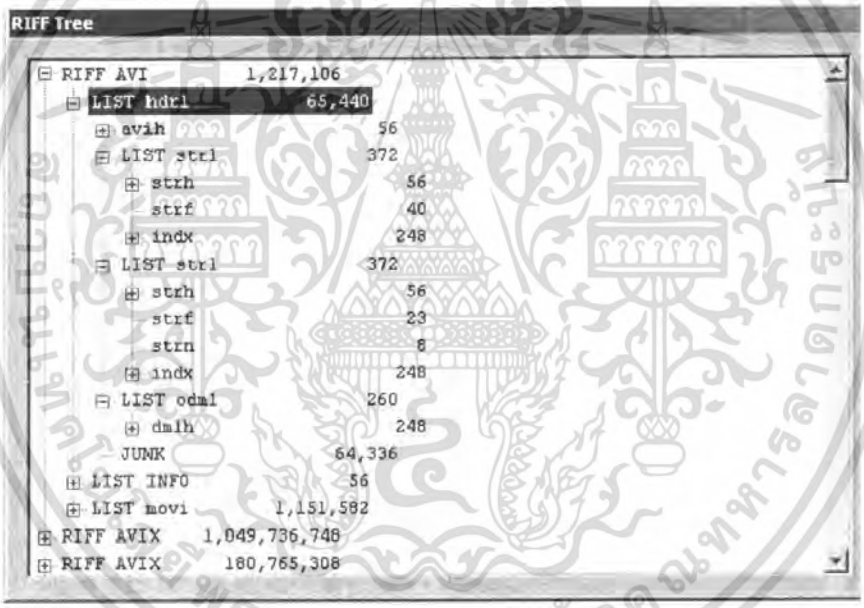
- Hybride-Files เก็บเพียง 1 RIFF List สามารถเป็นได้ทั้ง 2 แบบข้างต้น

<u>แผนผังของ AVI</u>

RIFF-List ที่ dwFourCC เป็น AVI จะเรียกว่า RIFF-AVI-List และ RIFF-List ที่ dwFourCC เป็น AVIX จะเรียกว่า RIFF-AVIX-List โดยทุกๆ ไฟล์ AVI จะมีโครงสร้างดังนี้

ส่วนหัวของแต่ละโครงสร้าง (Frame header)

ส่วนของ เฮดเดอร์ (Frame Header)จะมีลักษณะดังนี้



รูปที่ 2.7 แสดงรูปแบบของ AVI ส่วนหัวของแต่ละโครงสร้าง (Frame header)

โดยรายละเอียดต่างๆใน เฮดเดอร์ (Frame Header)มีดังนี้

MainAVI Frame header (avih)

typedef struct

{

DWORD dwMicroSecPerเฟรม (Frame); // เฟรม (Frame) display rate (or 0)

DWORD dwMaxBytesPerSec; // max. transfer rate

```
        DWORD dwPaddingGranularity; // pad to multiples of this
        // size;
        DWORD dwFlags; // the ever-present flags
        DWORD dwTotalเฟรม (Frame)s; // # เฟรม (Frame)s in file
        DWORD dwInitialเฟรม (Frame)s;
        DWORD dwStreams;
        DWORD dwSuggestedBufferSize;
        DWORD dwWidth;
        DWORD dwHeight;
        DWORD dwReserved[4];
} MainAVIHeader;
```

dwMicroSecPerเฟรม (Frame) เก็บข้อมูลของไฟล์วิดีโอในหน่วย ไมโครวินาที ซึ่งค่านี้สามารถละทิ้งได้ แต่ควรเขียนอย่างถูกต้องด้วย ทุกๆตัวเขียน AVI

dwMaxBytesPerSec ข้อมูลที่มี data rate สูงที่สุดในไฟล์

dwPaddingGranularity ข้อมูลถูกเพิ่มเข้าเป็นจำนวนกี่เท่า

dwFlags

- AVIF_HASINDEX ไฟล์มีอินเดกซ์
- AVIF_MUSTUSEINDEX การบังคับให้ทั้งวิดีโอและเสียงเวลาทำการเล่นต้องใช้อินเดกซ์
- AVIF_ISINTERLEAVED stream มีคุณสมบัติในการแทรกและถูกแทรก
- AVIF_WASCAPTUREFILE ไฟล์สามารถถูกบันทึกได้
- AVIF_COPYRIGHT บอกถึงลิขสิทธิ์
- AVIF_TRUSTCKTYPE(Open-DML เท่านั้น) flag นี้ช่วย keyเฟรม (Frame) flag ในอินเดกซ์นั้นดูน่าเชื่อถือ

dwTotalเฟรม (Frame)

เก็บค่าจำนวนเฟรมทั้งหมดของวิดีโอในรายการ RIFF-AVI

dwStreams

จำนวนของ stream ในไฟล์

dwSuggestedBufferSize

ขนาดของ Buffer ที่จะไปรองรับ Chucks ของไฟล์

dwWidth

ความกว้างของ Video stream

dwHeight

ความสูงของ Video stream

The Stream Header list – general

มี strl – List สำหรับทุกๆ Stream ถ้าหมายเลขของ strl – Lists ข้างใน hdrl – List นั้น แตกต่างจาก MainAVIHeader::dwStreams จะต้องมีการแจ้งเตือน Error

The StreamHeaders list element: strh

```
typedef struct {
        FOURCC fccType;
        FOURCC fccHandler;
        DWORD dwFlags;
        WORD wPriority;
        WORD wLanguage;
        DWORD dwInitialเฟรม (Frame)s;
        DWORD dwScale;
        DWORD dwRate; /* dwRate / dwScale == samples/second */
        DWORD dwStart;
        DWORD dwLength; /* In units above... */
        DWORD dwSuggestedBufferSize;
        DWORD dwQuality;
        DWORD dwSampleSize;
        RECT rcเฟรม (Frame);
} AVIStreamHeader;
```

โดยแต่ละตัวมีรายละเอียดดังนี้

1. fccType มีค่าได้ดังนี้

- 'vids' – วิดีโอ
- 'auds' – เสียง
- 'txts' – คำบรรยาย

2. fccHandler

FourCC ของ codec ที่จะใช้

3. dwFlags

โดยมี flag ที่ทำการประกาศไว้ดังนี้

- AVISF_DISABLED – stream จะไม่ทำงานเอง

- AVISF_VIDEO_PALCHANGES – stream คือสัญญาณวิดีโอที่มีการเปลี่ยนแปลงไปเรื่อยๆในขณะที่กำลังทำงาน

4. dwInitialFrames คือ จำนวน block แรกของ เฟรม (Frame) ที่ปรากฏในไฟล์

5. swRate / dwScale = samples / second(เสียง) หรือ เฟรม (Frame)s / second(วิดีโอ)

6. dwStart

เวลาเริ่มต้นทำงานของ Stream ในกรณีของเสียงแบบที่ bitrate มีการเปลี่ยนแปลง ตัวเลขนี้จะบอกจำนวนของ เฟรม (Frame) ที่ไม่มีเสียงที่จะต้องเล่นก่อนที่จะเริ่ม stream

7. dwLength

ขนาดของ stream ใน 1 หน่วย

8. dwSuggestedBufferSize

ขนาดของ buffer ที่จำเป็นในการเก็บในแต่ละกล่องข้อมูลของ stream ซึ่งค่านี้สามารถเป็น 0 ได้ ถ้ามี Application ไหนแนะนำ

9. dwQuality

บอกคุณภาพของไฟล์ (ไม่สำคัญ)

10. dwSampleSize

จำนวนของ byte ของ 1 stream อะตอม

The stream Header list element: strf

โครงสร้างของ strf ขึ้นอยู่กับชนิดของสื่อ สัญญาณ Video ใช้ BITMAPONFOส่วนหัวของแต่ละโครงสร้าง (FRAME HEADER)

The stream Header *list element: indx*

ใน chunk นี้ระดับของอินเดกซ์

The stream Header list element: strn

ส่วนนี้ทำการเก็บชื่อของ stream โดยชื่อนั้นจะเก็บอยู่ในรูปแบบ ASCII และต้องไม่ใช่ UTF-8

AVI Indexes

อินเดกซ์ในรูปแบบเก่า

ซึ่งเป็นรูปแบบของ AVI 1.0 ซึ่งจะวางไว้ต่อจาก movi List ใน RIFF AVI List โดยมีรูปแบบของข้อมูลดังนี้

AVIINDEXENTRY index_entry[n]

typedef struct {

```
        DWORD ckid;
        DWORD dwFlags;
        DWORD dwChunkOffset;
        DWORD dwChunkLength;
} AVIINDEXENTRY;
```

Ckid

เก็บค่า chunk ID โดยใช้ 4 ตัวอักษร

dwFlags

โดยมี flag ดังนี้

- AVIIF_KEYเฟรม (Frame) ระบุว่า chunk นี้เป็น keyเฟรม (Frame) หรือไม่
- AVIIF_LIST ระบุว่าตัวนี้เป็น LIST ไม่ใช่ Chunk
- AVIIF_FIRSTPART chuck ต้องการ เฟรม (Frame) ต่อท้ายถึงจะใช้งานได้
- AVIIF_LASTPART chunk นี้ต้องการมี เฟรม (Frame) ถึงจะใช้งานได้
- AVIIF_NOTIME ไม่ใช้เวลาสำหรับการปรับตัวเข้ากับ chunk ที่เหมาะสม

dwChunkOffset

Header ของ chunk ที่สอดคล้องกัน

dwChunkLength

เก็บขนาดของ chunk ในรูปแบบของ byte

Open-DML index

มีลักษณะโครงสร้างดังนี้

```
typedef struct _aviindex_chunk {
        FOURCC fcc;
        DWORD cb;
        WORD wLongsPerEntry;
        BYTE bIndexSubType;
        BYTE bIndexType;
        DWORD nEntriesInUse;
        DWORD dwChunkId;
        DWORD dwReserved[3];
        struct _aviindex_entry {
                DWORD adw[wLongsPerEntry];
        } aIndex [ ];
```

} AVIINDEXCHUNK;

Fcc,cb

Headerของ chunk แบบเดียวกับ dwFourCC และ dwSize ใน โครงสร้างของ Chunk

wLongsPerEntry

ทุกๆ aIndex ที่ I จะมีขนาด 4 x wLongsPerEntry bytes (โดยโครงสร้างของ aIndex[i] นั้นขึ้นอยู่กับลักษณะพิเศษของอินเดกซ์)

bIndexType, bIndexSubType

บอกลักษณะรูปแบบของอินเดกซ์

nEntriesInUse

จำนวนของ aIndex ที่ใช้ (aIndex[0] ... aIndex[nEntriesInUse-1])

dwChunkId

ID ของ stream อินเดกซ์

Upper Level Index(Super Index)

โดย upper level index ทำหน้าที่ในการระบุไปยัง index chunk อื่นๆ โดยมีลักษณะโครงสร้างดังต่อไปนี้

```
typedef struct _avisuperindex_chunk {
        FOURCC fcc;
        DWORD cb;
        WORD wLongsPerEntry;
        BYTE bIndexSubType;
        BYTE bIndexType;
        DWORD nEntriesInUse;
        DWORD dwChunkId;
        DWORD dwReserved[3];
        struct _avisuperindex_entry {
                __int64 qwOffset;
                DWORD dwSize;
                DWORD dwDuration;
        } aIndex[ ];
} AVISUPERINDEX;
```

โดยต้องกำหนดค่าต่างๆดังนี้

bIndexType = AVI_INDEX_OF_INDEXES

bIndexSubType = [AVI_INDEX_2FIELD | 0]

wLongsPerEntry = 4

โดยในอาเรย์ aIndex นั้นจะประกอบด้วยค่าเหล่านี้

qwOffset

ตำแหน่งของ index chunk ที่ชี้ไปในไฟล์

dwSize

ขนาดของ chunk ที่มีการระบุถึง

dwDuration

ช่วงเวลาที่ระบุไว้ใน AVI stream Header ในกรณีของวิดีโอที่หรือเสียงที่มีการเปลี่ยนแปลง bitrate โดยปกติจะหมายถึงจำนวน เฟรม (Frame)

The Standard Index

ในอินเดกซ์นี้จะเก็บ Pointer ที่ชี้ไปยัง วิดีโอ,เสียง,คำบรรยาย โดยจะอยู่ในรูปแบบดังต่อไปนี้

```
typedef struct _avistdindex_chunk {
        FOURCC fcc;
        DWORD cb;
        WORD wLongsPerEntry;
        BYTE bIndexSubType;
        BYTE bIndexType;
        DWORD nEntriesInUse;
        DWORD dwChunkId;
        __int64 qwBaseOffset;
        DWORD dwReserved3;
        struct _avistdindex_entry {
                DWORD dwOffset;
                DWORD dwSize;
        } aIndex[ ];
} AVISTDINDEX;
```

bIndexSubType เป็น 0

bIndexType เป็น AVI_INDEX_OF_CHUNKS

qwBaseOffset

ค่านี้ถูกกำหนดเป็น AVISTDINDEX ในทุกๆ dwOffset

dwOffset , dwSize

ระบุถึงตำแหน่ง (qwBaseOffset + dwOffset) ในส่วนของข้อมูล ซึ่งจะมี nEntriesInUse เป็นคู่ ซึ่งใช้สำหรับวิดีโอและเสียง และนอกจากนั้น Bit ที่ 31 ของ dwSize ใช้สำหรับการระบุประเภทของ เฟรม (Frame) bit นี้จะไม่ใช่ keyเฟรม (Frame) ถ้ามีการกำหนดค่าให้กับ bit นี้

The movi – Lists

เป็นส่วนที่เก็บข้อมูล วิดีโอ, เสียง, คำบรรยาย โดยสามารถจัดกลุ่มให้เป็น rec – List ดังนี้

LIST movi

LIST rec

01wb

01wb

02wb

03wb

03wb

03wb

00dc

00dc

LIST rec

01wb

02wb

LIST rec

...

ix01

ix02

ix03

....

โดย chunk Header ID ถูกกำหนดดังนี้

..wb เสียง

..dc วิดีโอ

..tx คำบรรยาย

ix.. กล่องอินเดกซ์มาตราฐาน

Subtitles in AVI files

เป็นส่วนของการเก็บคำบรรยาย โดยสามารถใช้ VSFilter สำหรับการเลือกโหลดคำบรรยาย โดยรายละเอียดของ Header มีดังนี้

```
char[4]; // 'GAB2'
BYTE 0x00;
WORD 0x02; // unicode
DWORD dwSize_name; // length of stream name in bytes
char name[dwSize_name]; // zero-terminated subtitle stream
name encoded in UTF-16
WORD 0x04;
DWORD dwSize; // size of SRT/SSA text file
char data[dwSize]; // cntirc SRT/SSA file
Stream Header chunk
typedef struct {
        FOURCC fccType; // "txts"
        FOURCC fccHandler; // 00 00 00 00
        DWORD dwFlags;
        WORD wPriority;
        WORD wLanguage;
        DWORD dwInitialเฟรม (Frame)s;
        DWORD dwScale;
        DWORD dwRate; // dwRate / dwScale == duration in seconds
        DWORD dwStart;
        DWORD dwLength; // In units above..., should be 1
        DWORD dwSuggestedBufferSize;
        DWORD dwQuality;
        DWORD dwSampleSize; // = 0 -> treated as VBR
        RECT rcเฟรม (Frame); // 0, 0, 0, 0
} AVIStream Header;
```

Stream format chunk

chunk นี้มีขนาด 0

Stream name chunk

chunk strn จะไม่ถูกเลือกจาก VSfilter ดังนั้นจึงไม่จำเป็นต้องเขียนหรืออ่าน

2.3 การเข้าและถอดรหัสลับ

การเข้ารหัสข้อมูล (Encryption) หมายถึง วิธีการที่ทำเปลี่ยนแปลงข้อมูลเพื่อไม่ให้สามารถแปลความได้จากบุคคลที่เราไม่ต้องการให้เขาเข้าใจข้อมูล ส่วนการถอดรหัสข้อมูล นั้นจะมีวิธีการที่ตรงกันข้ามกับการเข้ารหัสข้อมูล กล่าวคือการถอดรหัส (Decryption) หมายถึง วิธีการที่ทำการเปลี่ยนแปลงข้อมูลที่ได้จากการเข้ารหัสข้อมูล เป็นข้อมูลก่อนที่จะถูกทำการเข้ารหัส การที่จะทำให้ข้อมูลเป็นความลับ จุดหลักคือ ต้องไม่ให้ข้อมูลความลับนี้ถูกอ่านโดยบุคคลอื่น แต่ให้ถูกอ่านได้โดยบุคคลที่เราต้องการให้อ่านได้เท่านั้น โดยการนำเอาข้อความเดิมที่สามารถอ่านได้ (Plain text,Clear Text) มาทำการเข้ารหัสก่อน เพื่อเปลี่ยนแปลงข้อความเดิมให้ไปเป็นข้อความที่เราเข้ารหัส (Ciphertext) ก่อนที่จะส่งต่อไปให้บุคคลที่เราต้องการที่จะติดต่อด้วย เพื่อป้องกันไม่ให้บุคคลอื่นสามารถที่จะแอบอ่านข้อความที่ส่งมาโดยที่ข้อความที่เราเข้ารหัสแล้ว

2.3.1 ความต้องการของเทคโนโลยีการเข้ารหัสข้อมูล

การรักษาความลับ (Confidentiality)

คือความสามารถในการที่จะรักษาความลับที่ไม่ให้ผู้อื่นที่ไม่มีสิทธิ์เข้าถึงข้อมูลภายในระบบได้

การระบุตัวบุคคลได้ (Authenticity)

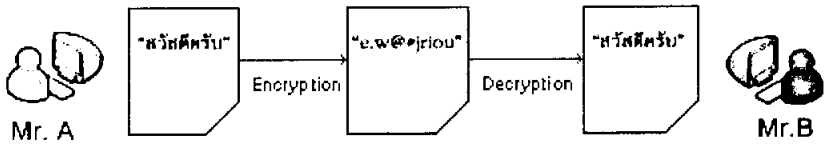
คือการที่เราสามารถที่จะระบุตัวตนของผู้ที่การเข้าถึงข้อมูลภายในระบบได้

การรักษาความลับ (Integrity)

คือความสามารถในการรักษาความถูกต้องและสมบูรณ์ของข้อมูล

การป้องกันการปฏิเสธความรับผิดชอบ (Non-repudiation)

คือความสามารถในการป้องกันการปฏิเสธความรับผิดชอบของการเข้าถึงข้อมูลภายในระบบ



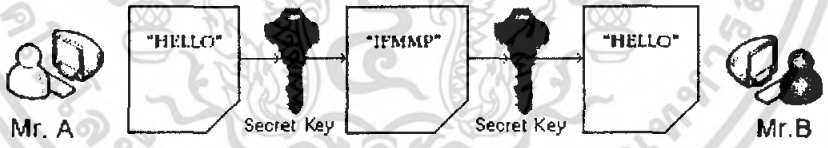
รูปที่ 2.8 แสดงการเข้ารหัสข้อมูล (Encryption)

2.3.2 ระบบการเข้ารหัสลับ (Cryptography)

ระบบการเข้ารหัสลับ (Cryptography) เป็นกระบวนการสำหรับการแปรรูปข้อมูลอิเล็กทรอนิกส์ธรรมดาให้อยู่ในรูปที่บุคคลทั่วไปไม่สามารถอ่านเข้าใจได้ ซึ่งโดยทั่วไปแล้วการเข้ารหัสจะกระทำก่อนการจัดเก็บข้อมูลหรือก่อนการส่งข้อมูล โดยการนำข้อมูลอิเล็กทรอนิกส์ธรรมดากับกุญแจ (Key) ซึ่งเป็นตัวเลขสุ่มใดๆ มาผ่านกระบวนการทางคณิตศาสตร์ ผลที่ได้ก็คือข้อมูลที่เข้ารหัส ขั้นตอนที่กล่าวมานี้จะเรียกว่า "การเข้ารหัส" (Encryption) และเมื่อต้องการอ่านข้อมูล ก็นำเอาข้อมูลที่เข้ารหัสกับกุญแจมาผ่านกระบวนการทางคณิตศาสตร์ ผลลัพธ์ที่ได้ก็คือข้อมูลดั้งเดิม ซึ่งขั้นตอนนี้จะเรียกว่า "การถอดรหัส" (Decryption)
จะเห็นได้ว่ากุญแจเป็นตัวแปรที่สำคัญสำหรับระบบเข้ารหัส ดังนั้นระบบเข้ารหัสสามารถแบ่งตามวิธีการใช้กุญแจได้เป็น 2 วิธีดังนี้

2.3.2.1 ระบบเข้ารหัสแบบกุญแจสมมาตร (Symmetric-key cryptography หรือ Secret key Cryptography)

คือ การเข้ารหัสข้อมูลด้วยกุญแจเดี่ยว (Secret Key) ทั้งผู้ส่งและผู้รับ โดยวิธีการนี้ผู้รับกับผู้ส่งต้องตกลงกันก่อนว่าจะใช้รูปแบบไหนในการเข้ารหัสข้อมูล ซึ่งรูปแบบไหนในการเข้ารหัสข้อมูลที่ผู้รับกับผู้ส่งตกลงกันแท้ที่จริงก็คือ กุญแจลับ (Secret Key) นั่นเอง เช่น ผู้ส่งกับผู้รับตกลงจะใช้เทคนิคการแทนที่ตัวอักษรที่อยู่ถัดไป 1 ตำแหน่ง เช่น ถ้าเห็นตัวอักษร A ก็ให้เปลี่ยนไปเป็น B หรือเห็นตัวอักษร B ก็ให้เปลี่ยนไปเป็น C เป็นต้น นั้นก็คือผู้ส่งกับผู้รับตกลงใช้รูปแบบนี้เป็นกุญแจลับดูตัวอย่างดังรูป



รูปที่ 2.9 แสดงการเข้ารหัสแบบกุญแจสมมาตร (Symmetric-key cryptography)

จากรูป ถ้า Mr. A ได้ตกลงกับ Mr. B ว่ากุญแจลับที่จะใช้เข้ารหัสและถอดรหัสคือ การเปลี่ยนตัวอักษรจากเดิมถัดไป1ตำแหน่ง ถ้า Mr. A ต้องการส่งคำว่า HELLO ไปให้ Mr. B ขั้นตอนจะเป็นดังนี้

1. Mr. A สร้างข้อความว่า "HELLO" ขึ้นมา
2. Mr. A ใช้กุญแจลับมาทำการเข้ารหัสข้อความ โดยการเปลี่ยนตัวอักษรจากเดิมถัดไป 1 ตำแหน่ง ดังนั้น ตัวอักษร H จะเปลี่ยนไปเป็นตัวอักษร E จะเปลี่ยนไปเป็นตัวอักษร F ตัวอักษร L ทั้ง 2 ตัว จะเปลี่ยนไปเป็นตัวอักษร M ทั้งสองตัว และสุดท้ายตัวอักษร O จะ

เปลี่ยนไปเป็นตัวอักษร P เพราะฉะนั้นหลังจากการทำการเข้ารหัสข้อความที่ Mr. A ต้องการส่งด้วยกุญแจลับแล้ว ข้อความว่า HELLO จะเปลี่ยนไปเป็นข้อความที่เข้ารหัส (Ciphertext) ว่า "IFMMP"

3. Mr. A ส่งข้อความที่เข้ารหัสไปให้ Mr. B

4. หลังจากที่ Mr. B ได้รับข้อความที่เข้ารหัสจาก Mr. A แล้ว Mr. B จะต้องทำการถอดรหัสข้อครามนี้ก่อน หรือที่เรียกว่า Decrypt โดยการถอดรหัสข้อความนี้ Mr. B จะต้องใช้กุญแจลับที่ได้ตกลงกันไว้แล้วกับ Mr. A มาทำการถอดรหัส เพราะฉะนั้นกุญแจลับที่ได้ตกลงกันกับ Mr. A ว่า Mr. A จะทำการเข้ารหัสโดยการเปลี่ยนตัวอักษรจากเดิมไปเป็นตัวอักษรที่อยู่ถัดไป 1 ตำแหน่ง ดังนั้น Mr. B จะต้องเอาข้อความเข้ารหัส IFMMP มาถอดรหัส โดยการเปลี่ยนจากตัวอักษร I ไปเป็นตัวอักษร H และตัวอักษร F จะไปเป็นตัวอักษร E และตัวอักษร M ทั้งสองตัวจะเปลี่ยนไปเป็นตัวอักษร O หลังจากนั้น Mr. B ก็จะทราบว่าข้อความที่ Mr. A ส่งมา คือ ข้อความว่า "HELLO"

จากตัวอย่างที่ได้อธิบายมานี้จะเป็นหลักการแบบง่ายๆ ทำให้เห็นการทำงานของการเข้ารหัสแบบสมมาตร หรือกุญแจเดี่ยว เพราะฉะนั้นหลักการเข้ารหัสแบบสมมาตรนี้จะใช้กุญแจลับ Secret Key) ทำการเข้ารหัสและถอดรหัสข้อความ

<u>ข้อดีของการเข้ารหัสแบบสมมาตร</u>

1. การเข้ารหัสและถอดรหัสข้อมูลใช้เวลาน้อย เพราะว่าอัลกอริทึมที่ใช้ไม่ได้สลับซับซ้อน
2. ขนาดของข้อมูลหลังจากทำการเข้ารหัสแล้ว มีการเปลี่ยนแปลงไม่มาก หรือพูดอีกนัยหนึ่งว่า ข้อมูลหลังจากทำการเข้ารหัสแล้ว จะมีขนาดไม่ใหญ่ไปกว่าเดิมมากนัก

<u>ข้อเสียของการเข้ารหัสแบบสมมาตร</u>

1. การจัดการกับกุญแจลับที่ยุ่งยาก เพราะ Mr. A ต้องจำให้ได้ด้วยว่า ถ้าจะติดต่อกับ Mr. B ต้องใช้กุญแจลับดอกไหน หรือติดต่อกับนายขาวต้องใช้กุญแจลับดอกไหน
2. การกระจายกุญแจลับ เนื่องจากการเข้ารหัสวิธีนี้ต้องใช้กุญแจลับ 1 ดอกต่อผู้รับ 1 คน ดังนั้นถ้า Mr. A ต้องติดต่อกับคนมากๆ Mr. A ก็ต้องส่งกุญแจลับที่ใช้ไปให้กับทุกคน

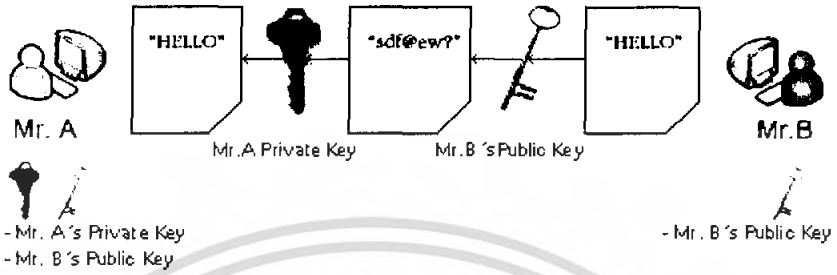
สำหรับวิธีการเข้ารหัสแบบนี้ ก็จะมีมาตรฐานมารองรับเหมือนกัน มาตรฐานที่ว่าก็คือ มาตรฐาน DES (Digital Encryption Standard) หรือเรียกว่า “เดส” ที่มาของ DES เกิดขึ้นมาจากทีมพัฒนาของบริษัท IBM เมื่อราวๆปลายยุค 1960 ทำการพัฒนาระบบเข้ารหัสและถอดรหัสนี้ โดยหลักการทำงานจะทำการแบ่งข้อมูลที่จะทำการเข้าหรือถอดรหัสออกเป็นบล็อก (block) โดยที่แต่ละบล็อกจะทีขนาด 64 บิต และจำนวนความยาวของ

กุญแจลับจะมีขนาด 128 บิตในช่วงแรก หลังจากนั้นทางบริษัท IBM ก็ได้เพิ่มทุนให้ทำการพัฒนาและปรับปรุงต่อเรื่อยๆมา โดยในครั้งนี้ได้มีที่ปรึกษาจากสำนักงานความมั่นคงแห่งชาติ (National Security Agency: NSA) ของสหรัสอเมริกาเข้าร่วมด้วย ผลที่ได้จากการพัฒนานี้ ทำให้ระบบ DES สามารถทนทานต่อผู้ต้องการเจาะรหัส (cryptanalysis) ได้ และขณะเดียวกัน ก็ได้ทำการลดความยาวของกุญแจลงเหลือแค่ 56 บิต จากเดิม 128 บิต เหตุผลที่ต้องลดความยาวของกุญแจลับลง ก็เพราะว่าสำนักงานความมั่นคงแห่งชาติของสหรัสอเมริกา เกรงว่าจะไม่สามารถตรวจสอบข้อมูลที่เข้ารหัสด้วยความยาวของกุญแจลับที่ 128 บิตได้ ซึ่งการลดความยาวของกุญแจลับก็โดนกระแสต่อต้านจากกลุ่มธุรกิจองค์กรต่างๆมากมาย เพราะพวกกลุ่มธุรกิจองค์กรต่างๆเหล่านี้ต้องการให้ข้อมูลมีความลับมากๆ เพราะยิ่งกุญแจลับมีความยาวมากเท่าไหร่ ข้อมูลที่เข้ารหัสก็ยิ่งต้องใช้เวลาในการถอดรหัสออกนานมากขึ้น ทำให้ข้อมูลมีความปลอดภัยมากขึ้นอีก แต่รัฐบาลสหรัฐก็ออกมาโต้ว่า ด้วยความยาวกุญแจลับขนาด 56 บิตนี้ ก็ทำให้ต้องใช้เวลาในการถอดรหัสนานมากทีเดียว แต่ในปัจจุบันนี้ มีเครื่องคอมพิวเตอร์ที่มีประสิทธิภาพสูง สามารถที่จะถอดรหัสที่ใช้กุญแจขนาด 56 บิตได้ในเวลาแค่ 56 ชั่วโมง และมีแนวโน้มว่าจะสามารถถอดรหัสโดยใช้เวลาลดลงกว่านี้ได้อีก แต่สำหรับข้อมูลที่เข้ารหัสด้วยกุญแจขนาด 128 บิต ในปัจจุบันยังถือว่าปลอดภัยอยู่มาก เพราะว่ายังไม่สามารถถอดรหัสได้เร็วเกินที่จะรอคอยได้ เพราะกว่าจะถอดรหัสได้ ข้อมูลเหล่านั้นก็อาจจะไม่มีประโยชน์ต่อการนำกลับไปใช้งานได้อีกแล้ว ซึ่งในปัจจุบันนี้ก็ได้มีมาตรฐานที่เรียกว่า 3DES เกิดขึ้นมาแล้ว โดยมาตรฐานนี้จะใช้กุญแจลับที่มีขนาดความยาว 168 บิต แต่สำหรับธุรกิจองค์กรใดที่จะใช้มาตรฐานนี้จะต้องทำเรื่องขออนุญาตจากรัฐบาลสหรัสอเมริกาก่อน ถ้าได้รับอนุญาตจากรัฐบาลอเมริการจึงจะสามารถนำมาใช้งานได้

2.3.2.2 ระบบเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric-key cryptography หรือ Public Key Technology)

ระบบการเข้ารหัสแบบนี้ได้ถูกคิดค้นโดย นายวิทฟิลด์ ดิฟฟี (Whitfield Diffie) ซึ่งเป็นนักวิจัยแห่งมหาวิทยาลัยสแตนฟอร์ด สหรัสอเมริกา ในปี พ.ศ. 2518 โดยการเข้ารหัสแบบนี้จะใช้หลักกุญแจคู่ทำการเข้ารหัสและถอดรหัส โดยกุญแจคู่ที่ว่านี้จะประกอบไปด้วย กุญแจส่วนตัว (privatc key) และกุญแจสาธารณะ (public key) โดยหลักการทำงานจะทำดังนี้ ถ้าใช้กุญแจลูกใดเข้ารหัส ก็ต้องใช้กุญแจอีกลูกหนึ่งถอดรหัส สำหรับการเข้ารหัสและถอดรหัสด้วยกุญแจคู่นี้จะใช้ฟังก์ชั่นทางคณิตศาสตร์เข้ามาช่วยโดย

ที่ฟังก์ชั่นทางคณิตศาสตร์ที่นำมาใช้ ได้รับการพิสูจน์แล้วว่าจะมีเฉพาะกุญแจคู่ของมันเท่านั้นที่จะสามารถถอดรหัสได้ ไม่สามารถนำกุญแจคู่อื่นมาถอดรหัสได้อย่างเด็ดขาด



รูปที่ 2.10 การเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric-key cryptography or Public Key Technology)

จากรูปการเข้ารหัสแบบนี้จะมี Mr. A คนเดียวที่อ่านได้ จะมีขั้นตอนดังนี้

1. Mr. A ต้องมีกุญแจคู่1คู่ขึ้นมาก่อน คือ กุญแจส่วนตัวกับกุญแจสาธารณะ โดยที่กุญแจสาธารณะของ Mr. A นี้ ใครๆก็สามารถที่จัดหามาได้รวมถึง Mr. B ด้วย หรือ Mr. A ส่งกุญแจนี้ไปให้ Mr. B ก่อน

2. หลังจาก Mr. B มีกุญแจสาธารณะของ Mr. A Mr. B จะใช้กุญแจสาธารณะของ Mr. A เข้ารหัสข้อความที่ต้องการจะส่ง

3. Mr. B ส่งข้อความเข้ารหัสไปให้ Mr. A

4. Mr. A ได้รับข้อความเข้ารหัสจาก Mr. B Mr. A จะต้องใช้กุญแจส่วนตัว นำมาใช้ในการถอดข้อความเข้ารหัสของ Mr. B หลังจากนั้น Mr. A จึงสามารถอ่านข้อความเข้ารหัสจาก Mr. B ได้ หรือในทางกลับกันถ้า Mr. B ต้องการส่งข้อความลับให้กับ Mr. A Mr. B ก็แค่ใช้กุญแจสาธารณะของ Mr. A ทำการเข้ารหัสข้อมูลแล้วส่งไปให้ดำ พอ Mr. A ได้ข้อความเข้ารหัสจาก Mr. B Mr. A ก็จะใช้กุญแจส่วนตัวของตัวเองถอดรหัสข้อความลับจาก Mr. B เพราะฉะนั้นจะมีแต่ Mr. A เท่านั้นที่สามารถอ่านข้อความลับที่ถูกส่งมาจาก Mr. B ได้

หลักการการคำนวณกุญแจสาธารณะ

Public key เกิดจากหลักคณิตศาสตร์ที่เรียกว่า ฟังก์ชันทางเดียว (one-way function) กลุ่มของฟังก์ชันทางเดียวส่วนหนึ่งมีความเกี่ยวข้องกับเลขจำนวนเฉพาะ (prime number) เลขที่หารได้เฉพาะ 1 และตัวมันเอง ตัวอย่างเช่น เลขจำนวนเฉพาะสองตัวมาคูณกัน สมมติเป็น 5 กับ 7 ได้ 35 ทีนี้ลองหาอีกจำนวนนึงเช่น 11,927 x 20,903 คำตอบคือ 249,310,081 การคูณ 11,927 กับ 20,903 นี้ทำได้ง่ายกว่าหาตัวประกอบของ 249,310,081 เพราะฉะนั้นยิ่งเลขจำนวณเฉพาะมีค่ามากเท่าไหร่ยิ่งจะแยกตัวประกอบยากขึ้นเท่านั้น

แนวคิดเรื่อง public key ไม่ได้เป็นของใหม่ คนแรกที่คิดเรื่องนี่คือ Whitfield Diffie และ Martin Hellman ซึ่งเสนอวิธีการแบบ public key นี้ใน National Computer Conference ปี 1976 และตีพิมพ์ใน IEEE Transaction on Information Theory สามารถอธิบาย algorithm ได้ดังนี้

1. ให้ A และ B กำหนดค่า n และ g โดยที่ $1 < g < n$ เลขทั้งสองไม่จำเป็นต้องปกปิด

2. A สุ่มเลขที่มีค่ามากๆ มาตัวนึง กำหนดให้เป็นค่า x และหาค่า $X = g^x \bmod n$ เก็บค่า x เป็นความลับ

3. B ทำเหมือนกัน สุ่มเลขที่มีค่ามากๆ มาตัวนึง กำหนดให้เป็นค่า y และหาค่า $Y = g^y \bmod n$ เก็บค่า y เป็นความลับ

4. ทีนี้ A กับ B แลกค่า X และ Y กัน

5. A คำนวณหาค่า $k = Y^x \bmod n$

6. B คำนวณหาค่า $k' = X^y \bmod n$

7. ค่า k และ k' จะมีค่าเท่ากัน และเท่ากับ $g^{xy} \bmod n$

ผลการทดลอง Yoshijo's Diffie-Hellman algorithms

$1<g<n$

$1<2<5$

A (assign x=5): X = 2^5 = 32 mod 5 = 2

B (assign y =7): Y = 2^7 = 128 mod 5 = 3

A: k = 3^5 mod 5 = **3**

B: k' = 2^7 mod 5 = **3**

k = k' = 2^(5*7) mod 5 = **3**

ผลการทดลอง Yoshijo's RSA Cryptosystem

p = 47, q = 71

m ในที่นี้ ให้เท่ากับ ตัวอักษร A (ASCII = 65)

n = p*q = 3337 (RSA Values)

phi = (p-1)(q-1) = 3220

e = 79 (สุ่มค่า)

gcd(e, p-1) = gcd(79, 46) = 1 (79 และ 46 ไม่มีตัวประกอบร่วมใดๆ ยกเว้น 1)

gcd(e, q-1) = gcd(79, 70) = 1 (79 และ 70 ไม่มีตัวประกอบร่วมใดๆ ยกเว้น 1)

gcd(e, phi) = gcd(e, (p-1)(q-1)) = gcd(79, 3337) = 1

Private Key: d = c^-1(mod(p-1)(q-1))

c*d = 1 (mod phi)

d = c^-1 mod phi

d = 79^-1 mod 3220

79d = 1 mod 3220

79d - 1 = mod 3220

หาค่า d ใดๆ ที่ ผลลัพธ์ของ 79d -1 จะต้อง mod ด้วย 3220 แล้วออกมาเป็นจำนวนเต็ม

d = {1,2,3...} ...d=1019

79*1019 - 1 = 80500 mod 3220

= 25

d = 1019

n = 3337

e = 79

Encrypting:

formulas: c = m^e(mod n) (นำ message(m) มา เข้ารหัส ด้วย encryption (e) กับ public key(n))

c = 65^79 mod 3337

c = 1.660179989012795634718125103458 4e+143 mod 3337

c = 541

Decrypting:

formulas: m = c^d(mod n) (นำ cypher text(c) มา ถอดรหัสด้วย private key (d) ที่สามารถถอด public key(n) ของตนเองได้)

m = 541^1019 mod 3337

m = 1.342805599519496305148314481531 6e+2785 mod 3337

m = 65

ASCII Character "A" = 65

ค่า k และ k' ที่ว่านี้นอกจาก A และ B แล้วคนอื่นไม่มีทางหาได้เพราะค่าที่คนอื่นมีโอกาสรู้มีเพียง n, g, X และ Y โอกาสที่จะหาค่า x จาก X (หรือ y จาก Y) ทำได้ด้วยการหา inverse ของ X ซึ่งเรียกว่า discrete logarithm และ discrete logarithm นี่ไม่ได้คำนวณได้ยากมากหรือทำไม่ได้เลย เพราะ บางทีdiscrete logarithm จะไม่มีคำตอบ

หลังจาก Diffie-Hellman เสนอวิธีการของ public key ได้ไม่นานนักก็เกิด RSA cryptosystem ซึ่งตีพิมพ์โดย Ron Rivest, Adi Shamir, และ Leonard Adleman ในปี 1978 ความปลอดภัยของ algorithm นี้ขึ้นกับความยากในการแยกตัวประกอบของเลขจำนวนเฉพาะที่มีค่ามากๆ ดังแสดงในรูปข้างล่าง

RSA Cryptosystem

Public Key:

- n คำนวณจากเลขจำนวนเฉพาะสองตัว p และ q คูณกัน - ทั้ง p และ q ต้องเก็บเป็นความลับ ปกติจะทำลายทิ้งหลังจากหา key ได้เพราะไม่ได้ใช้ในการเข้า/ถอดรหัส
- c เป็นจำนวนที่ไม่มีตัวประกอบร่วมกับ (p-1)(q-1)

Private Key: $d = e^{-1}(\text{mod}(p-1)(q-1))$

Encrypting: $c = m^{e}(\text{mod } n)$

Decrypting: $m = c^{d}(\text{mod } n)$

ทั้งสามคนคิดว่าวิธีการนี้ปลอดภัยมากและเชื่อว่าต้องใช้เวลานับล้านปีกว่าจะแยกตัวประกอบของเลขจำนวน 129 หลักออกไม่ว่าจะใช้คอมพิวเตอร์ที่ทรงพลังขนาดไหนก็ตาม ปัญหาการแยกตัวประกอบ 129 ตัวนี้เป็นที่รู้จักกันดีในวงการนักคณิตศาสตร์และคอมพิวเตอร์ว่า "*RSA 129*" เลขที่ว่านี้คือ "114 381 625 757 888 867 669 235 779 967 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541" เลขนี้ตีพิมพ์เป็นปริศนาในคอลัมน์ Mathematical Games ใน Scientific American โดย Martin Gardner ในปี 1977 (ก่อน RSA จะตีพิมพ์) ไม่มีใครในยุคนั้นสามารถหาคำตอบได้เลยจนกระทั่งในปี 1993 จึงมีคนพยายามแก้ปริศนานี้อีกครั้ง Paul Leyland, Michael Graff และ Derek Atkins เป็นผู้ที่พยายามจะแก้ปัญหานี้โดยได้รับการสนับสนุนจากอาสาสมัครมากกว่า 600 คนทั่วโลกให้ run โปรแกรมที่เขียนโดย K. Lenstra ในเวลากลางคืนเพื่อช่วยกันหาคำตอบผ่านทาง Internet ในที่สุดในเดือนเมษายนปี 1994 ปริศนาก็ถูกแก้ออกเป็นเลขจำนวนเฉพาะขนาด 64 และ 65 หลักคือ "3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577" กับ "32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533" และยังถอดรหัสออกมาเป็นข้อความได้ว่า "The magic words are Squeamish and Ossifrage" เรื่องนี้สอนให้รู้ว่า 129 หลักยังไม่ปลอดภัยพอ

อย่างไรก็ตามปัจจุบัน RSA ใช้ key เป็นตัวเลขขนาด 1024 bits (ประมาณ 309 หลัก) เป็นอย่างน้อย จึงยอมรับกันว่า RSA cryptosystem ปลอดภัยไปจนกว่าจะมีคนคิดวิธีแยกตัวประกอบได้ง่ายและเร็วกว่าวิธีที่มีทั้งหมดในปัจจุบัน หรือไม่ก็จนกว่า cryptanalyst จะหาจุดอ่อนของ RSA ได้

ข้อดีของระบบเข้ารหัสแบบกุญแจอสมมาตร

1. การจัดการกับกุญแจทำได้ง่าย เพราะว่า Mr. A ไม่ต้องจำเลยว่าได้ใช้กุญแจคู่ไหนกับใคร Mr. A แค่ใช้กุญแจส่วนตัวของตัวเองทำการถอดรหัสข้อมูลที่ Mr. B ส่งมาให้ หรือเอากุญแจส่วนตัวเข้ารหัสส่งไปให้ Mr. B Mr. B ก็สามารถที่จะอ่านได้ ซึ่งวิธีนี้จะง่ายมากครับ เพราะ Mr. A ใช้แค่กุญแจส่วนตัวของตัวเองดอกเดียวก็สามารถติดต่อกับ Mr. B หรือใครๆ ก็ได้ตามต้องการ

2. การกระจายกุญแจลับ เนื่องจากการเข้ารหัสโดยวิธีนี้ ใช้แค่กุญแจสาธารณะเพียงดอกเดียวในการเข้ารหัสและถอดรหัส และกุญแจสาธารณะของ Mr. A ก็สามารถที่จะเปิดเผยให้กับใครก็ได้ที่ต้องการจะติดต่อด้วย ไม่ว่าจะเป็น Mr. B นายขาว เหล่านี้เป็นต้น เพราะฉะนั้นการแจกจ่ายกุญแจสาธารณะของ Mr. A ไปให้กับคนสักพันคน หรือหมื่นคน จะไม่เป็นปัญหาอีกต่อไป

ข้อเสียของระบบเข้ารหัสแบบกุญแจอสมมาตร

1. การเข้ารหัสและถอดรหัสข้อมูลใช้เวลามาก เพราะว่าอัลกอริทึมที่ใช้ค่อนข้างจะสลับซับซ้อนมาก
prime number generator การหาเลขจำนวนเฉพาะที่มีค่ามากๆ ต้องใช้วิธีการที่ยุ่งยาก และเสียเวลามาก และสมการ exponential ในการเข้าและถอดรหัสก็เป็นเหตุผลนึงที่ทำให้ทำงานช้า เพราะต้วยกกำลังเป็นเลขที่มีค่าเยอะ

2. ใช้ operation ที่ซับซ้อนมากกว่าเยอะ อย่างพวก xor, shift จึงทำงานได้ช้ากว่า

3. ขนาดของข้อมูลหลังจากทำการเข้ารหัสแล้ว มีการเปลี่ยนแปลงมาก หรือพูดอีกนัยหนึ่งว่า ข้อมูลหลังจากทำการเข้ารหัสแล้ว จะมีขนาดใหญ่กว่าเดิมมากขึ้น เพราะฉะนั้นจะเป็นปัญหาในการใช้งาน

2.3.3 การประยุกต์ใช้การเข้ารหัสโดยใช้กุญแจสาธารณะ

การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography)

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัสคือ

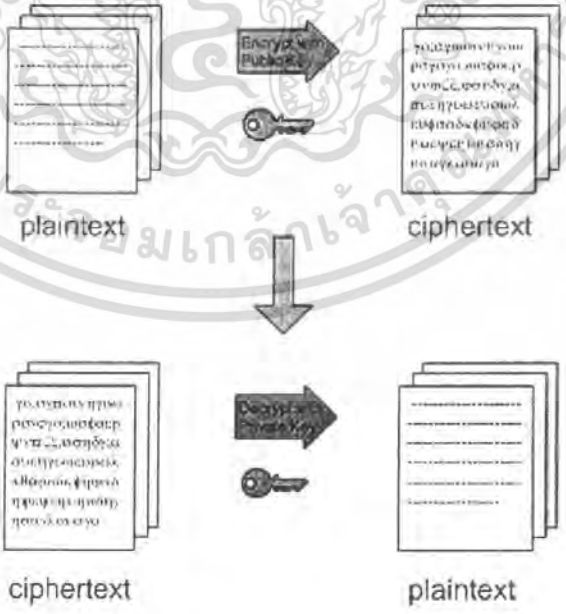
- กุญแจสาธารณะ (public key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้อื่นๆ ทราบหรือเปิดเผยได้
- กุญแจส่วนตัว (private key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

กระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

1. ผู้ใช้แต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัส
2. กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้คนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง
3. เมื่อจะส่งข้อมูลออกไปหาผู้ใช้คนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะก่อนถูกส่งออกไป
4. เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา

<u>การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication)</u>

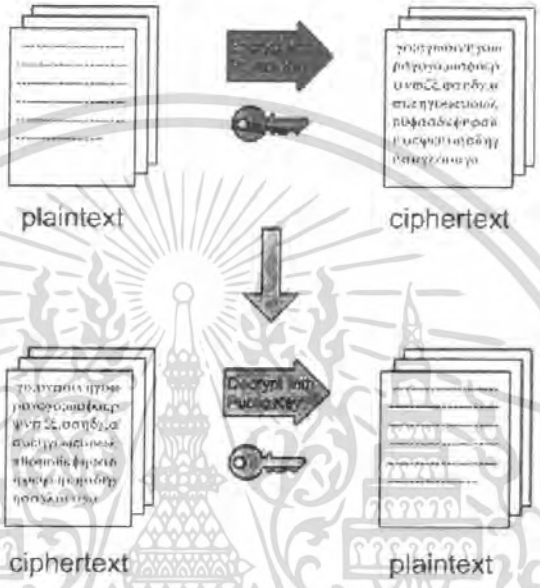
การประยุกต์ใช้ในการเข้ารหัสข้อมูล (Encryption) เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้



รูปที่ 2.11 แสดงระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจ

การประยุกต์ใช้ในการพิสูจน์ตัวตน (Authentication)

เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง แล้วนำข้อมูลนั้นส่งไปยังผู้รับ ซึ่งผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัสออกมา ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง

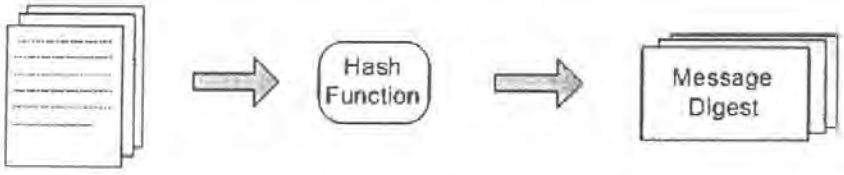


รูปที่ 2.12 แสดงระบบของการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตน

การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิคส์ (Digital Signature)

เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ดังนี้

1. เมื่อผู้ใช้ต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชั่นทางคณิตศาสตร์ที่เรียกว่า "แฮชฟังก์ชัน" ได้เมสเซสไดเจสต์ (Message Digest) ออกมา

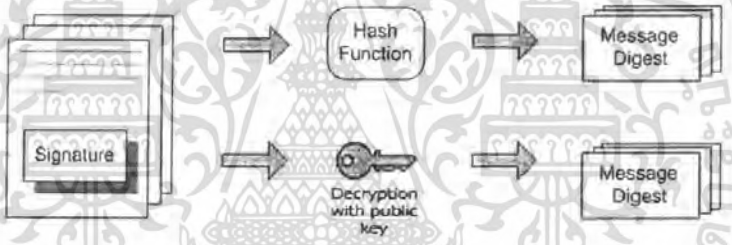


รูปที่ 2.13 แสดงการส่งข้อมูลเข้าไปใน Hash function

2. การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอลยินยอมที่จะให้ผู้รับ สามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

รูปที่ 2.14 แสดงการเข้ารหัสเมสเซสไดเจสต์ด้วยกุญแจส่วนตัวเพื่อเป็นการลงลายเซ็น

3. การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นอิเล็กทรอนิกส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง



รูปที่ 2.15 แสดงขั้นตอนการเปรียบเทียบความถูกต้อง

2.4 การซ้อนลายน้ำดิจิตอล

2.4.1 Steganography

Steganography เป็นกลไกในการติดต่อสื่อสารที่สามารถซ่อนการมีอยู่ของตัวเองแตกต่างกับการเข้ารหัส (Cryptography) ซึ่งสามารถตรวจพบ แล้วเข้าแทรกแซงได้ (แต่มีกลไกช่วยรับประกันความถูกต้อง และยืนยันได้ว่าข้อมูลมิได้ถูกเปลี่ยนไป ยากต่อการ decipher)

จุดมุ่งหมายของ Steganography คือซ่อนข้อมูลอย่างหนึ่งไว้ในข้อมูลอีกอย่างหนึ่ง โดยมิให้ผู้อื่นเห็นสิ่งที่ซ่อนเอาไว้ ดั่งคำที่ว่า การจะซ่อนใบไม้ ซ่อนในป่า การประยุกต์ใช้ในงานด้านลิขสิทธิ์มี 2 ลักษณะคือ Watermarking และ Fingerprinting

เป็นเทคนิคที่ใช้หลักการการบีบอัดข้อมูลดิจิตอล เนื่องจากข้อมูลดิจิตอล เช่น เสียง และภาพ จะมีความซ้ำซ้อนของข้อมูลสูง ทำให้มีขนาดใหญ่ หลักการการบีบอัดจึงทำการลดความซ้ำซ้อน แต่ก็ทำให้สูญเสียคุณภาพไปบ้าง (lossy compression techniques) แต่การประยุกต์ใช้ของ

หลักการ Steganography แทนที่จะลดความซ้ำซ้อนลง แต่กลับนำข้อมูลไปแทรกแทนไว้ในพื้นที่ที่จะบีบอัดแทน

โดยการทำ Steganography กับไฟล์สื่อดิจิตอล อาศัยการโจมตีจุดอ่อนของการรับรู้ของประสาทสัมผัสของมนุษย์ HAP (Human Auditory Perception) เช่น หูมนุษย์ได้ยินความถี่สูงสุด 20 kHz แต่จะซ่อนข้อมูลในช่วงความถี่ที่สูงกว่านั้น ทำให้ไม่สามารถได้ยินหรือ แยกแยะได้

<u>การประยุกต์ใช้ในงาน</u>

- ซ่อนข้อมูลลิขสิทธิ์ (Copyrights message) ไว้บนไฟล์ เพื่ออ้างสิทธิ์ในการฟ้องร้องดำเนินคดี
- เพื่อยืนยันสิทธิความเป็นเจ้าของข้อมูล
- เพื่อทำให้งานทุกชิ้นมีลายมือชื่อเป็นของตัวเอง
- เพื่อป้องกันข้อมูลดิจิตอลนั้น และสามารถตรวจสอบถึงความถูกต้องของข้อมูล
- เพื่อทำเครื่องหมายประจำตัวให้ข้อมูล โดยเก็บข้อมูลเพิ่มเติมเกี่ยวกับงานนั้นไว้ด้วย

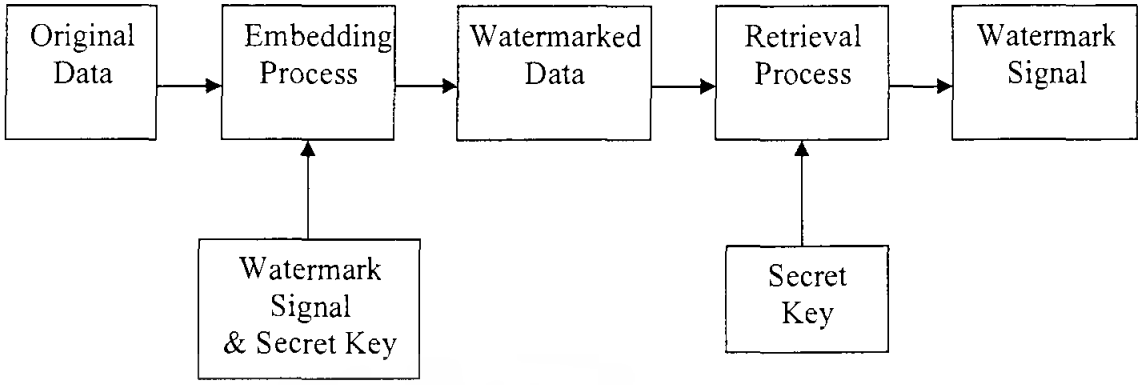
2.4.2 Digital watermarking

หลักการในการทำภาพพิมพ์ลายน้ำดิจิตอล

โดยทั่วไปเทคนิคในการทำภาพพิมพ์ลายน้ำดิจิตอลทั้งหลาย ล้วนแต่มีรูปแบบที่คล้ายคลึงกัน วางอยู่บนหลักการเดียวกันนั่นคือเป็นการใส่สัญญาณชนิดใดชนิดหนึ่งเข้าไปในตัวข้อมูลมัลติมีเดียก่อนที่จะทำการเผยแพร่ ซึ่งสัญญาณนี้อาจถูกเปลี่ยนแปลงแก้ไขหรือตรวจสอบได้โดยผู้ที่เป็นเจ้าของหรือผู้ที่ได้รับอนุญาต

<u>หลักการทั่วไป</u>

การทำภาพพิมพ์ลายน้ำดิจิตอลทุกประเภทจะต้องประกอบด้วยขั้นตอนทั่วๆ ไปที่เหมือนกันคือ การใส่ลายน้ำดิจิตอล (Watermark Embedding) และการตรวจสอบ (detection) หรือการนำลายน้ำดิจิตอลออก (Watermark Retrieval) ดังแสดงในรูปที่1 ข้อมูลมัลติมีเดียจะผ่านกระบวนการใส่สัญญาณลายน้ำ โดยสัญญาณที่ใส่เข้าไปจะมีค่าขึ้นอยู่กับกุญแจลับ (secret key) ที่ใช้ในการเข้ารหัส เพื่อที่ว่าจะได้มีเพียงผู้ที่ถือกุญแจลับนี้เท่านั้นที่จะสามารถเปลี่ยนแปลงแก้ไขสัญญาณลายน้ำดังกล่าวได้ เช่นเดียวกันกับในกระบวนการตรวจสอบสัญญาณลายน้ำ ซึ่งจำเป็นต้องใช้กุญแจลับในการนำสัญญาณลายน้ำที่ถูกต้องกลับคืนมา [1]



รูปที่ 2.16 *แสดงกระบวนการใส่และถอดลายน้ำดิจิตอล*

ในการแบ่งแยกประเภทของเทคนิคการทำภาพพิมพ์ลายน้ำดิจิตอลนั้น เราอาจใช้ตำแหน่งที่ทำการใส่สัญญาณลายน้ำเป็นหลัก ใช้ลักษณะวิธีการของกระบวนการใส่ลายน้ำดิจิตอล หรือกระบวนการตรวจสอบลายน้ำดิจิตอลเป็นหลักก็ได้ ในส่วนนี้ ได้ยกตัวอย่างเทคนิคการทำภาพพิมพ์ลายน้ำดิจิตอลที่โดดเด่นและเป็นที่ยอมรับกันโดยทั่วไปถึงความมีประสิทธิภาพมา 3 เทคนิคคือ เทคนิคการกล้ำความลึกของสัญญาณ เทคนิคการนับจำนวนซีโรทรีของค่าสัมประสิทธิ์ และเทคนิคการกระจายแถบความถี่

2.5 CSS และ DeCSS

CSS (Content Scrambling System)

เป็นระบบในการป้องกันการคัดลอก DVD (DVD Copy Control Association) โดยใช้ในการเล่นข้อมูลบน DVD ซึ่งต้องประกอบด้วย 3 ส่วน คือ แผ่น DVD , เครื่องเล่น DVD และเครื่องคอมพิวเตอร์

ซึ่งบนแผ่น DVD จะมีส่วนที่เรียกว่า Hidden area ซึ่งเก็บข้อมูล Encrypted content โดย DVD-R ทั่วไปจะทำการปิดส่วนนี้ไว้เพื่อไม่ให้สามารถเขียนข้อมูลลงไปในพื้นที่นี้ได้ และเครื่องที่ไม่ได้รับอนุญาตก็ไม่สามารถเข้าไปอ่านข้อมูลได้เช่นกัน โดยข้อมูล Encrypted content ก็คือ Encrypted Disk Keys

เครื่องเล่น DVD จะเก็บ player Key หรือ Master Key ซึ่งใช้ในการ Decrypt Disk Key

ทั้งหมดใช้เพื่อ Scrambling ข้อมูลภายในแผ่น DVD นั้น และถึงแม้จะทำการคัดลอก DVD ไปแต่ส่วนของ Disk Key จะไม่ถูกนำไปด้วยเนื่องจากอยู่ในส่วน Hidden area

ขั้นตอนการทำงานของDVD Player ที่เล่น DVD ที่มี CSS

2.5.1 ทำการใส่แผ่น DVD เข้าไปในเครื่องเล่น DVD (DVD Player)

2.5.2 DVD Player ทำการหาข้อมูลลับบนแผ่น DVD ที่เรียกว่า Secured Disc Key แล้วทำการโหลดข้อมูลขึ้นมา

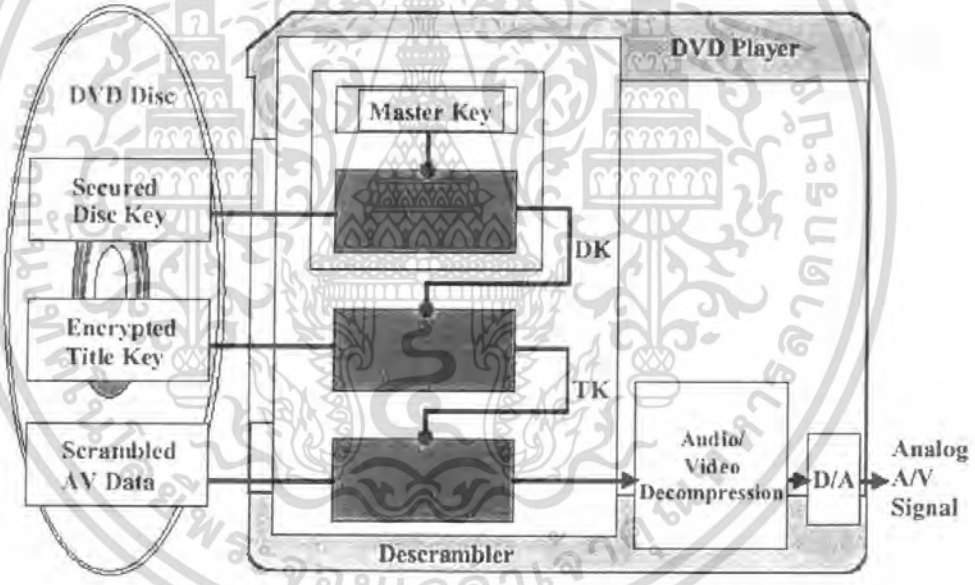
2.5.3 Secured Disc Key ถูกถอดรหัสด้วย Master Key ที่มีประจำอยู่แล้วบน DVD Player ทำให้ได้ Key ใหม่ที่ชื่อว่า DK

2.5.4 DVD Player ทำการหาข้อมูลที่เรียกว่า Title key ซึ่งเป็นข้อมูลที่ถูกเข้ารหัสเอาไว้

2.5.5 ถอดรหัส Title key ด้วย DK ทำให้ได้ Key ใหม่ที่ชื่อว่า TK

2.5.6 DVD Player ทำการหาข้อมูล AV ที่ถูก Scramble เอาไว้ ซึ่งข้อมูลนี้ถูก De Scramble ด้วย TK ทำให้เราได้ข้อมูลภาพและเสียงที่ถูกบีบอัดไว้

2.5.7 ส่งข้อมูลภาพและเสียงที่ถูกบีบอัดไปสู่กระบวนการ Decompression เพื่อแปลงเป็นสัญญาณภาพและเสียงต่อไป



รูปที่ 2.17 แสดงการทำงานของ CSS(Content Scrambling System)

การทำงานของ DeCSS

โดยกระบวนการทำงานของ DeCSS คือทำการหา Master Key ที่เหมาะสมกับ Secured Disk key ที่พบ ซึ่งจะทำให้ได้ DK และนำไปใช้ในการถอดรหัสในขั้นต่อไป

บทที่ 3
การออกแบบและพัฒนา

ในส่วนของการออกแบบและการพัฒนานั้นจะต้องมีการพิจารณาถึง การแก้ปัญหาจากการศึกษาระบบจัดการลิขสิทธิ์สื่อดิจิตอลในปัจจุบัน โดยในขั้นตอนการทำงานต่างๆ นั้นได้มีการพิจารณาอย่างเหมาะสม

3.1 โครงสร้างพื้นฐานของโครงงาน

3.1.1 วางโครงสร้างของต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล

จากการศึกษาระบบจัดการลิขสิทธิ์สื่อดิจิตอล จะเห็นว่าองค์ประกอบของระบบจัดการลิขสิทธิ์สื่อดิจิตอลนั้น ประกอบด้วย 4 ข้อ

1. Encryption กระบวนการการเข้ารหัส
2. Access control (conditional access) เงื่อนไขการใช้งาน หรือการเข้าถึงข้อมูล
3. Copy control or copy prevention การป้องกันการคัดลอก หรือทำซ้ำข้อมูล
4. Identification and tracing การพิสูจน์ตัวตนเพื่อการใช้งาน หรือการตรวจสอบข้อมูล

โดยในการออกแบบจะนำองค์ประกอบ 4 ข้อมาพัฒนาและปรับปรุงจุดประสงค์ไปจากเดิม

Encryption

จากเดิมนำมาใช้เพื่อการเข้ารหัส เพื่อแปลงข้อมูลสื่อดิจิตอลไม่ให้สามารถอ่านได้ หรือ เข้าใช้งานได้ แต่เราจะนำมาประยุกต์ใช้ในการเข้ารหัส เพื่อแปลงข้อมูลที่จะซ่อนในสื่อดิจิตอล เพื่อความปลอดภัยต่อการบุกรุก ปกปิดเป็นความลับไม่ให้สามารถรับรู้ได้โดยง่าย และยังนำมาประยุกต์ในการยืนยันตัวตนด้วยการเข้ารหัสแบบกุญแจสาธารณะ

Access control

จากเดิมใช้การสร้างรูปแบบไฟล์เฉพาะ เพื่อบังคับใช้กับโปรแกรมเล่นสื่อดิจิตอลเฉพาะ แต่จะใช้การยืนยันตัวตน เพื่อพิสูจน์ความเป็นเจ้าของและการเข้าใช้งาน

Copy control and protection

จากเดิมกำหนดจำนวนในการคัดลอก หรือห้ามไม่ให้คัดลอกไปเลย แต่เนื่องจากเราสร้างระบบจัดการกับตัวไฟล์สื่อดิจิตอล เช่น การลดลดคุณภาพของไฟล์ เป็นต้น ไว้แล้วจึงทำให้ถึงแม้จะคัดลอกไปได้ แต่ถ้าไม่สามารถยืนยันตัวตนได้ ก็ไม่สามารถใช้งานสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์นี้ คุณภาพสูงได้ สรุปคือ เป็นการใช้ความรู้ของผู้ใช้มาช่วยลดการคัดลอกหรือทำซ้ำ

Identification and tracing

ก็ยังคงไว้ตามเดิม โดยสร้างระบบการยืนยันตัวตนโดยตรวจสอบจาก ข้อมูลที่ซ่อนอยู่บนไฟล์สื่อดิจิตอล ถ้ามีการละเมิดก็ใช้การตรวจสอบเป็นหลักฐานเพื่อดำเนินคดีต่อไป และ ยังสามารถตรวจสอบการเปลี่ยนแปลงของไฟล์ได้จากการซ้อนลายมือชื่อดิจิตอล

3.2 รายละเอียดโปรแกรมที่พัฒนา (Software Specification)

3.2.1 รายละเอียดส่วนนำเข้า

- ผู้ใช้ ใช้งานผ่านโปรแกรมเล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ หรือสื่อดิจิตอลทั่วไปได้
- ผู้ใช้งานจะต้องทำการลงทะเบียนเพื่อยืนยันตัวตนกับ ผู้ให้บริการ

3.2.2 รายละเอียดส่วนนำออก

- ผู้ใช้งานที่สามารถยืนยันสิทธิ์ได้สามารถเล่นสื่อดิจิตอล ได้คุณภาพสูง
- โปรแกรมผลิตไฟล์สื่อดิจิตอลที่มีระบบจัดการลิขสิทธิ์ได้

3.2.3 รายละเอียดฟังก์ชัน

- ชุดโปรแกรมสามารถซ่อนข้อมูลสำคัญในสื่อดิจิตอลโดยการทำ Steganography ได้
- ชุดโปรแกรมสามารถ Encryption ข้อมูลสำคัญที่ซ่อนในสื่อดิจิตอลได้
- ชุดโปรแกรมสามารถสร้าง Access Control โดยการกำหนดให้มีการยืนยันสิทธิ์ผู้ใช้เพื่อจะได้รับคุณภาพสูงได้
- ชุดโปรแกรมสามารถสร้างลายมือชื่อดิจิตอลให้กับสื่อดิจิตอลได้
- ชุดโปรแกรมสามารถตรวจสอบความถูกต้อง และการเปลี่ยนแปลงข้อมูลได้
- ชุดโปรแกรมสามารถตรวจสอบลิขสิทธิ์ของไฟล์สื่อดิจิตอล ได้

3.2.4 โครงสร้างของซอฟต์แวร์ (Design)

แบ่งการทำงานเป็น 2 ส่วน คือ โปรแกรมเล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ และโปรแกรมสร้างสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์

- โปรแกรมเล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ โดยพัฒนาจากการเขียนโปรแกรมติดต่อสื่อดิจิตอลประเภทเพลงและภาพยนต์ (เพลง MP3 และ ภาพยนต์ AVI)
- โปรแกรมสร้างสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์

3.2.5 ขอบเขตและข้อจำกัดของโครงสร้าง

- โปรแกรมทำงานบนระบบปฏิบัติการ Windows XP SP2

- การเล่นไฟล์สื่อดิจิตอลที่มีการจัดการด้วยต้นแบบระบบจัดการลิขสิทธิ์ของโครงการนั้นต้องเป็นโปรแกรมเล่นสื่อดิจิตอลที่โครงการพัฒนาขึ้นเท่านั้น
- โปรแกรมสามารถติดต่อไฟล์สื่อดิจิตอลได้ 2 ประเภท คือ MP3 และ AVI

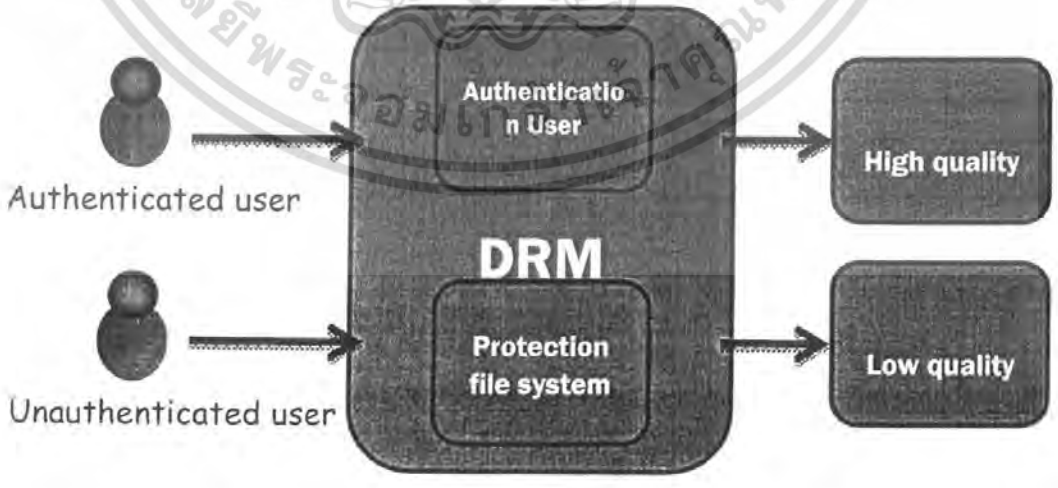
3.2.6 เครื่องมือที่ใช้การพัฒนา

- Java/Netbeans IDE - เนื่องจากการพัฒนาชุดโปรแกรมนั้น ต้องเขียนติดต่อเข้าถึงระดับหน่อยความจำซึ่งทำได้สะดวก และยังมีแหล่งความรู้แบบ open source เพื่อใช้ในการพัฒนาจึงเลือกใช้ภาษาจาวาเป็นภาษาพื้นฐานในการพัฒนาโปรแกรม
- Microsoft Windows XP Service Pack 2 -โครงงานนี้ได้ใช้ระบบต้นแบบเป็น Microsoft Windows XP Service Pack 2 เนื่องจากเป็นระบบปฏิบัติการที่มีการใช้งานและโดนบุกรุกมากที่สุดในปัจจุบัน นอกจากนี้แล้วชุดโปรแกรมนี้ยังสามารถติดตั้งและทดสอบการทำงานได้
- HxD เป็นโปรแกรมในการช่วยดูเลขฐาน 16 เนื่องจากไฟล์สื่อดิจิตอลโดยทั่วไปจะเก็บรูปแบบนี้

3.3 การออกแบบและพัฒนาซอฟแวร์

3.3.1 การออกแบบต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล

ออกแบบต้นระบบจัดการลิขสิทธิ์สื่อดิจิตอล เพื่อจัดการลิขสิทธิ์บนสื่อดิจิตอลโดยที่ยังคงความสามารถในการใช้งานทั่วไปของไฟล์ดิจิตอลไว้ และยึดหลักการที่ว่า "ผู้ซื้อจะสามารถเล่นสื่อดิจิตอลได้คุณภาพสูง แต่ผู้ละเมิดลิขสิทธิ์จะเล่นได้คุณภาพต่ำ" ใช้การยืนยันตัวตนของผู้ใช้งานเพื่อกำหนดสิทธิ์การเข้าใช้งานสื่อดิจิตอล ดังรูป

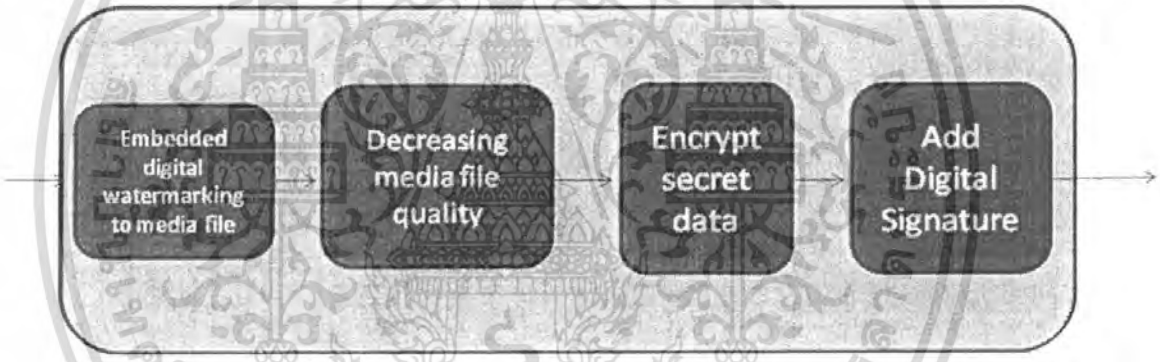


รูปที่ 3.1 ต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล

3.3.2 การพัฒนาระบบจัดการลิขสิทธิ์สื่อดิจิตอล

การพัฒนาในส่วน File Protection System ซึ่งเป็นการสร้างระบบเพื่อการป้องกันการใช้งานในตัวข้อมูลนั้น โดยมีลำดับขั้นตอนในการทำงานอธิบายได้ด้วยแผนภาพดังนี้

รูปที่ 3.2 แสดงการจัดการไฟล์สื่อดิจิตอลในระบบจัดการลิขสิทธิ์สื่อดิจิตอล



รูปที่ 3.3 แสดงขั้นตอนกาจัดการไฟล์สื่อดิจิตอล

โดยในส่วนนี้เป็นการสร้างระบบป้องกันการละเมิดลิขสิทธิ์บนตัวข้อมูลดิจิตอล โดยจากรูปที่ 3.2 แสดงให้เห็นว่าในส่วน File Protection System แบ่งขั้นตอนการทำงานออกเป็น 4 ส่วน ดังนี้

1. **การซ้อนลายน้ำดิจิตอล (Embedded digital watermarking)** โดยในส่วนนี้ทำหน้าที่ในการรวม digital watermarking ที่ใช้สำหรับการตรวจสอบสิทธิ์เข้าไปรวมไว้บนข้อมูลสื่อดิจิตอลโดยใช้การทำ Steganography ในการซ้อนข้อมูล
2. **การลดทอนคุณภาพของสื่อดิจิตอล (Decreasing quality)** ทำการลดทอนคุณภาพของข้อมูลในสื่อดิจิตอลลงโดยการนำข้อมูลบางอย่างเข้าไปแทนข้อมูลปกติ ทำให้ผลลัพธ์ที่ได้นั้นผิดแปลกไปจากข้อมูลสื่อดิจิตอลดั้งเดิม

3. การสร้างและการเข้ารหัสข้อมูลสำคัญ (Embedded Secret data) เป็นการแทรกข้อมูลบางอย่าง เพื่อใช้ในการตรวจสอบความเป็นเจ้าของ และการทำกระบวนการย้อนเพื่อเพิ่มคุณภาพข้อมูลในสื่อดิจิตอล โดยจะเก็บโดยเข้าเข้ารหัสลับแบบกุญแจสาธารณะ เพื่อความปลอดภัย

4. การใส่ลายมือดิจิตอล (Digital signature) เป็นการแทรกลายมือชื่อดิจิตอลเพื่อใช้ในการตรวจสอบการเปลี่ยนแปลงของสื่อดิจิตอลได้

3.3.3 การพัฒนาโปรแกรม

3.2.3.1 โปรแกรมผลิตสื่อดิจิดอลที่มีการจัดการลิขสิทธิ์

การเขียนโปรแกรมเข้าถึงส่วนต่างๆภายในข้อมูล MP3 โดยพิจารณาจากลักษณะโครงสร้างของ MP3 ซึ่งมีลักษณะดังรูปต่อไปนี้

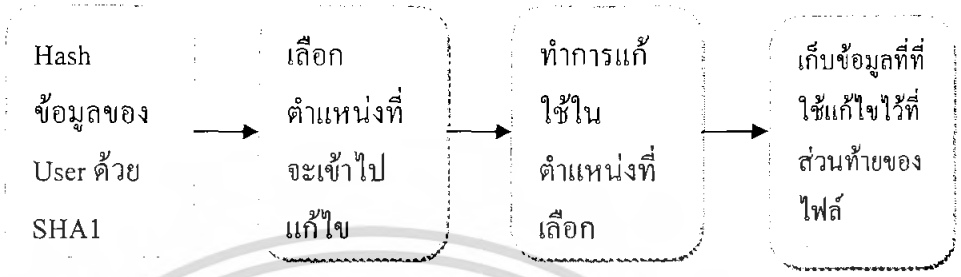
รูปที่ 3.4 แสดงรูปแบบของเฮดเดอร์ (Frame Header) ของไฟล์ MP3

ตำแหน่งที่แทนด้วยอักษร A นั้นเป็นส่วนที่เรียกว่า Frame sync โดย A ทั้งหมด 11 bits จะถูกกำหนดค่าให้เป็น 1 ทั้งหมด เพื่อให้สามารถเขียนโปรแกรมเพื่อติดต่อเข้าไปได้ และนอกจากนั้นถ้าพิจารณาที่ B ซึ่งมี 2 bits พบว่าค่า 00 คือ MPEG version 2.5 และ 01 เป็นค่าที่ไม่อนุญาตให้ใช้ ดังนั้นจึงสามารถเพิ่มเงื่อนไขเพิ่มเติมว่าต้องพบ 1 ทั้งหมด 12 bits ได้ ซึ่งในทางปฏิบัติแล้วยังไม่เพียงพอ เพราะภายใน MP3 นั้นยังมีส่วนของ Data ที่อาจจะมีค่าเดียวกันนี้รวมอยู่ด้วย ดังนั้นถ้ามีเงื่อนไขเพียง Frame sync อาจทำให้ได้ เฮดเดอร์ (Frame Header) ที่ผิดตำแหน่งได้ ดังนั้นจึงควรเขียนโปรแกรมเข้าไปตรวจสอบค่าภายในนั้นของ เฮดเดอร์ (Frame Header) แล้วตรวจสอบดูว่าตรงกับข้อมูลจริงๆหรือไม่ เช่น ค่า Bitrates นั้นสามารถคำนวณหาได้ ค่า Sample Rate ก็เช่นกัน จึงควรคำนวณหาค่าเหล่านี้แล้วนำมาเปรียบเทียบกับข้อมูลจริงๆ และการที่จะไปยัง เฟรม (Frame) ถัดไป ควรจะมีการตรวจสอบก่อนว่า ความยาวของ เฟรม (Frame) เดิมนั้นเป็นเท่าไร และมีการทำ CRC หรือไม่ เพื่อที่จะคำนวณหาตำแหน่งถัดไปได้อย่างไม่ผิดพลาด

ขั้นตอนการลดคุณภาพสื่อดิจิตอล

สื่อดิจิตอลประเภทเพลง (MP3) และประเภทภาพยนตร์ (AVI)

- การลดคุณภาพสื่อดิจิตอล มีกระบวนการทำงานหลักดังนี้



รูปที่ 3.5 แสดงหลักการลดคุณภาพของไฟล์สื่อดิจิตอล

การลดคุณภาพเสียง มีกระบวนการทำงานหลัก อธิบายเป็นขั้นตอนได้ดังนี้

1. ทำการ Hash ข้อมูลของผู้ใช้โดยใช้ SHA1 ในลักษณะดังต่อไปนี้ SHA1(username salt password) โดย salt คือ username ต่อกับ password ได้ผลลัพธ์เป็นชุดข้อมูลขนาด 20 byte

2. ทำการแบ่งข้อมูลเสียงออกเป็น 16 ส่วน

3. ทำการดึงข้อมูลทั้ง 16 ส่วนขึ้นมาทีละ 1 ส่วนมา เพื่อทำการเลือก เฟรม (Frame) เข้าไปแก้ไข โดยพิจารณาตำแหน่ง เฟรม (Frame) จากการรับค่าข้อมูลที่ได้จากการ Hash ในข้อ 1.

4. แก้ไขข้อมูลในส่วน MP3Data ใน เฟรม (Frame) ที่เลือกจากข้อ 3. โดยการลบด้วยค่าที่ได้จากการ Hash ในข้อ 1.

5. นำค่า Hash ในข้อ 1. มาแทรกไว้ ณ. ตำแหน่งหลังสุดของ เฟรม (Frame) สุดท้ายที่มีการจัดพื้นที่ไว้ก่อน เพื่อเก็บไว้ใช้ตรวจสอบความเป็นเจ้าของต่อไป

การลดคุณภาพภาพยนตร์ มีกระบวนการทำงานหลัก อธิบายเป็นขั้นตอนได้ดังนี้

1. ทำการ Hash ข้อมูลของผู้ใช้โดยใช้ SHA1 ในลักษณะดังต่อไปนี้ SHA1(username salt password) โดย salt คือ username ต่อกับ password ได้ผลลัพธ์เป็นชุดข้อมูลขนาด 20 byte

2. ทำการโหลดข้อมูลขึ้นมาครั้งละ 160000 byte

โดยในแต่ละครั้งที่มีการโหลดข้อมูลขึ้นมาจะถูกแก้ไขด้วยคำสั่งดังนี้

- ข้อมูลตำแหน่งที่ 4 ของชุดข้อมูลนั้นลบออกด้วย 1
- ข้อมูลในตำแหน่งที่ 5 – 8 ของชุดข้อมูลนั้น บวกด้วยค่าในแต่ละตำแหน่งที่ได้จากการ Hash ข้อมูลในข้อ 1.

3. นำค่า Hash ในข้อ 1. มาแทรกไว้ ณ. ตำแหน่งหลังสุดของ เฟรม (Frame) สุดท้ายที่มีการจัดพื้นที่ไว้ก่อน เพื่อเก็บไว้ใช้ตรวจสอบความเป็นเจ้าของต่อไป

โดยจะแตกต่างกันที่การเลือกตำแหน่งของสื่อดิจิตอลประเภทเพลง (MP3) จะได้ตำแหน่งที่ไม่คงที่ แต่ประเภทภาพยนตร์ (AVI) จะกำหนดตำแหน่งไว้ตายตัวเนื่องจากความซับซ้อนของโครงสร้างทำให้ไม่สามารถเข้าไปแก้แบบไม่มีระบบได้ แต่ยังคงแก้ไขแบบมีเอกลักษณ์ เพราะค่าที่นำเข้าไปแก้ไขจะต้องมาจากข้อมูลของแต่ละเจ้าของ เพื่อให้เกิดรูปแบบเฉพาะตัว

โดยสร้างโปรแกรม เพื่อรับคำสั่งผ่าน Command line เนื่องจากใช้การสร้างไฟล์สื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ในฝั่งผู้ผลิต โดยอัตโนมัติ โดยโปรแกรมผลิตสื่อดิจิตอลนี้จะทำการสร้างไฟล์สื่อดิจิตอลเมื่อมีการสั่งซื้อสื่อดิจิตอลผ่าน ISAG Store webpage ซึ่งจะรับตัวแปร 4 ตัว คือ username, password, public key และชื่อไฟล์สื่อดิจิตอล และจะรับตัวแปร 3 ตัว คือ username, password และชื่อไฟล์สื่อดิจิตอล เมื่อเป็นการซื้อสื่อดิจิตอลครั้งแรก เพราะทาง sever จะทำการสร้างคู่กุญแจสาธารณะ เพื่อใช้ในการสร้างไฟล์สื่อดิจิตอล โดยคู่กุญแจสาธารณะที่สร้างจะทำการส่งไปให้ผู้ใช้ทางอีเมล์

<u>ขั้นตอนการทำงานของระบบจัดการสื่อดิจิตอล</u>

สื่อดิจิตอลประเภทเพลง (MP3)

1. ทำการลดคุณภาพสื่อดิจิตอล
2. ตรวจสอบว่าผู้ใช้ได้ใส่ Public Key เข้ามาให้หรือไม่ ถ้าไม่มีแสดงว่าเป็นซื้อสื่อดิจิตอลครั้งแรก ระบบจะทำการสร้างคู่กุญแจสาธารณะขึ้นมา แล้วส่งไปให้ผู้ใช้ผ่านทางหน้าเว็บบราวเซอร์
3. โปรแกรมจะใช้ Private Key ไปใช้เป็น Key ในการเข้ารหัสลับข้อมูลลับที่ใช้ในการตรวจสอบว่าสื่อดิจิตอลนี้เป็นของผู้ผลิต โดยในที่นี้จะใช้คำว่า “ISAG Music DRM” เป็นข้อมูลลับ เมื่อทำการเข้ารหัสแล้วจะนำข้อมูลไปแทรกไว้ ณ ตำแหน่งท้ายสุดของ เฟรม (Frame)

4. โปรแกรมจะทำการสร้างลายมือชื่อดิจิตอล โดยใช้ Private Key แล้วนำเอาข้อมูลลายมือชื่อดิจิตอลไปแทรกไว้ ณ ตำแหน่งหลังข้อมูลที่เข้ารหัสลับในข้อที่ 3.

สื่อดิจิตอลประเภทภาพยนตร์ (AVI)

1. ทำการลดคุณภาพสื่อดิจิตอล

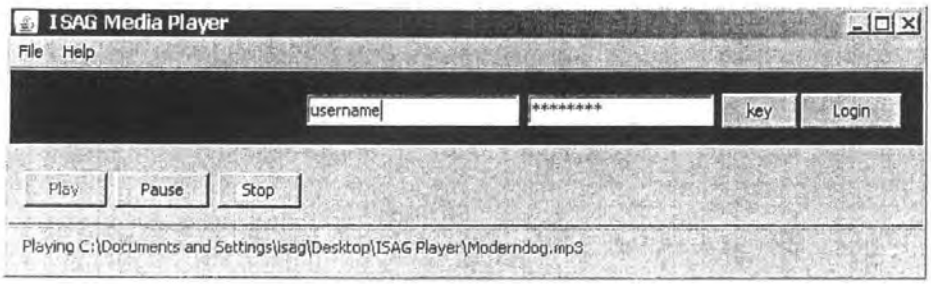
2. ตรวจสอบว่าผู้ใช้ได้ใส่ Public Key เข้ามาให้หรือไม่ ถ้าไม่มีแสดงว่าเป็นซื้อสื่อดิจิตอลครั้งแรก ระบบจะทำการสร้างคู่กุญแจสาธารณะขึ้นมา แล้วส่งไปให้ผู้ใช้ทางหน้าเว็บบราวเซอร์

3. โปรแกรมจะใช้ Private Key ไปใช้เป็น Key ในการเข้ารหัสลับข้อมูลลับที่ใช้ในการตรวจสอบว่าสื่อดิจิตอลนี้เป็นของผู้ผลิต โดยในที่นี้จะใช้คำว่า "ISAG Video DRM" เป็นข้อมูลลับ เมื่อทำการเข้ารหัสแล้วจะนำข้อมูลไปเพิ่มไว้ ณ ตำแหน่งท้ายสุดของ เฟรม (Frame) สุดท้าย

4. โปรแกรมจะทำการสร้างลายมือชื่อดิจิตอล โดยใช้ Private Key แล้วนำเอาข้อมูลลายมือชื่อดิจิตอลไปแทรกไว้ ณ ตำแหน่งต่อจากข้อมูลที่เข้ารหัสลับในข้อที่ 3.

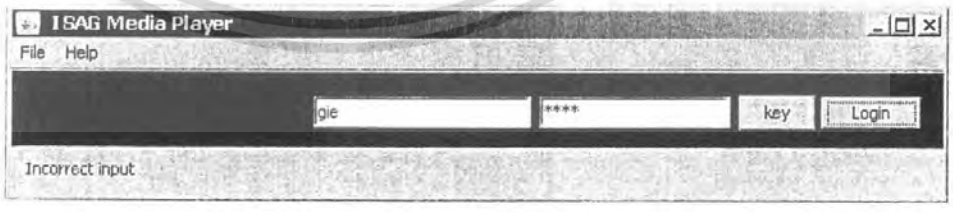
3.2.3.2 โปรแกรมเล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์

- พัฒนาโปรแกรมให้สามารถเล่นสื่อดิจิตอลประเภทเพลง(MP3) และประเภทภาพยนตร์ (AVI) โดยเขียนมี User interface ให้ใช้งานได้ง่าย โดยมีฟังค์ชัน พื้นฐาน คือ Play, Pause, Stop
- โดยใช้ Library หลัก คือ Java Sound และ MP3 SPI กับสื่อดิจิตอลประเภทเพลง
- โดยใช้ Library หลัก คือ JMF และ Fob4JMF กับสื่อดิจิตอลประเภทภาพยนตร์
- พัฒนาโปรแกรมให้สามารถตรวจสอบความเป็นเจ้าของ และการเปลี่ยนแปลงของไฟล์สื่อดิจิตอล ผ่านการยืนยันตัวตน โดยใช้ username และ password ทำการ Login เข้าใช้งานโปรแกรม และโปรแกรมจะร้องขอให้ผู้ใช้ใส่ คู่กุญแจสาธารณะ(ที่ได้รับจากอีเมล์ยืนยันการสั่งซื้อเพลงครั้งแรก) เมื่อผู้ใช้คนนั้นเข้าใช้โปรแกรมครั้งแรก

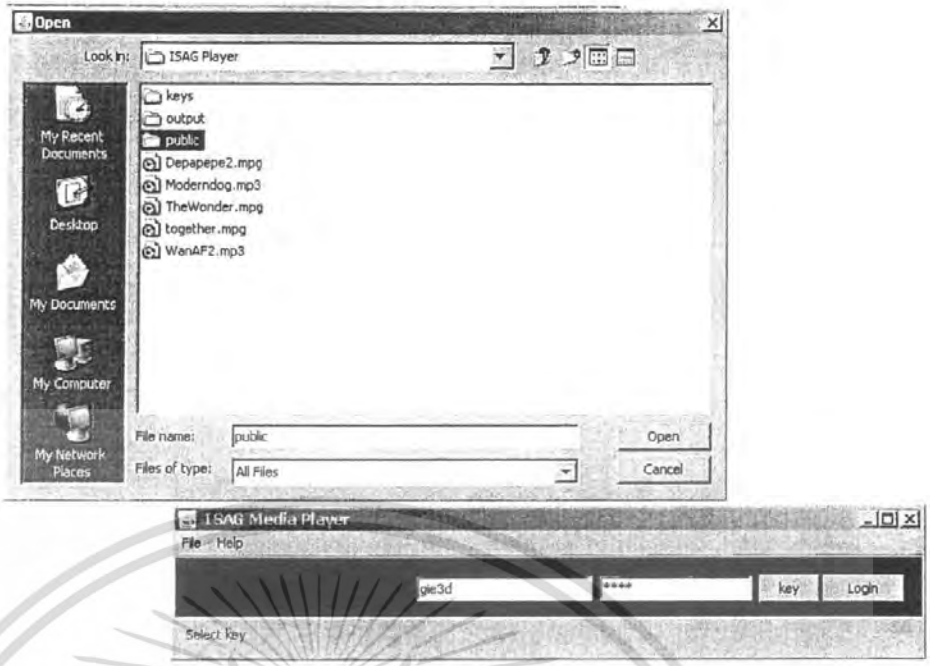


รูปที่ 3.6 แสดงหน้าต่างโปรแกรม ISAG Player

รูปที่ 3.7 แสดงการเล่นสื่อดิจิตอลประเภทภาพยนตร์ โดยไม่ได้ Login

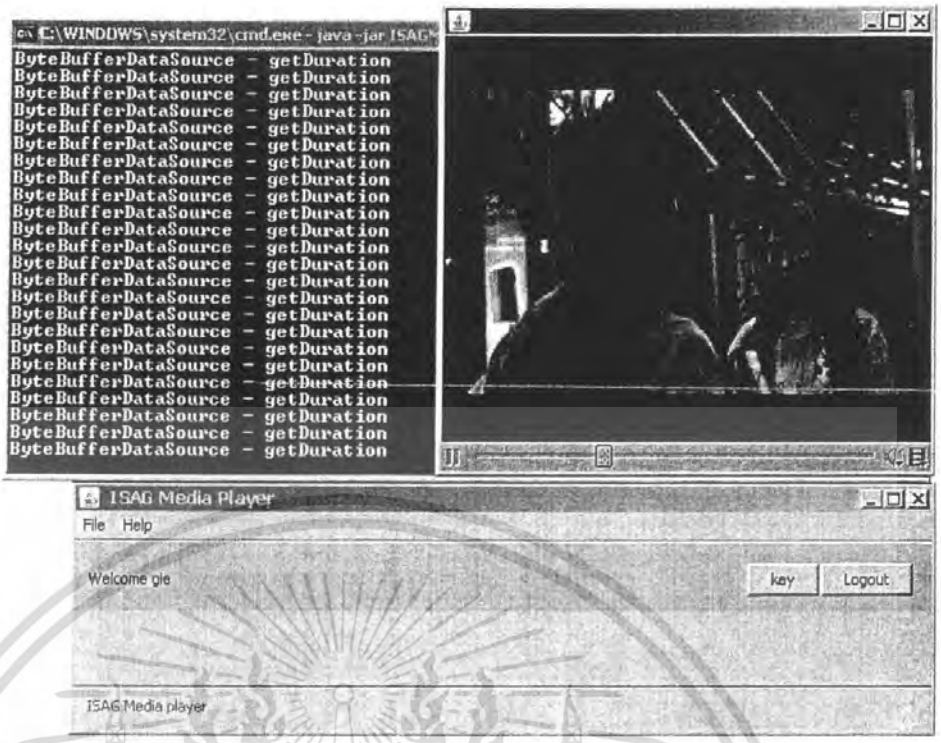


รูปที่ 3.8 แสดงเมื่อทำการ Login ไม่ถูกต้อง

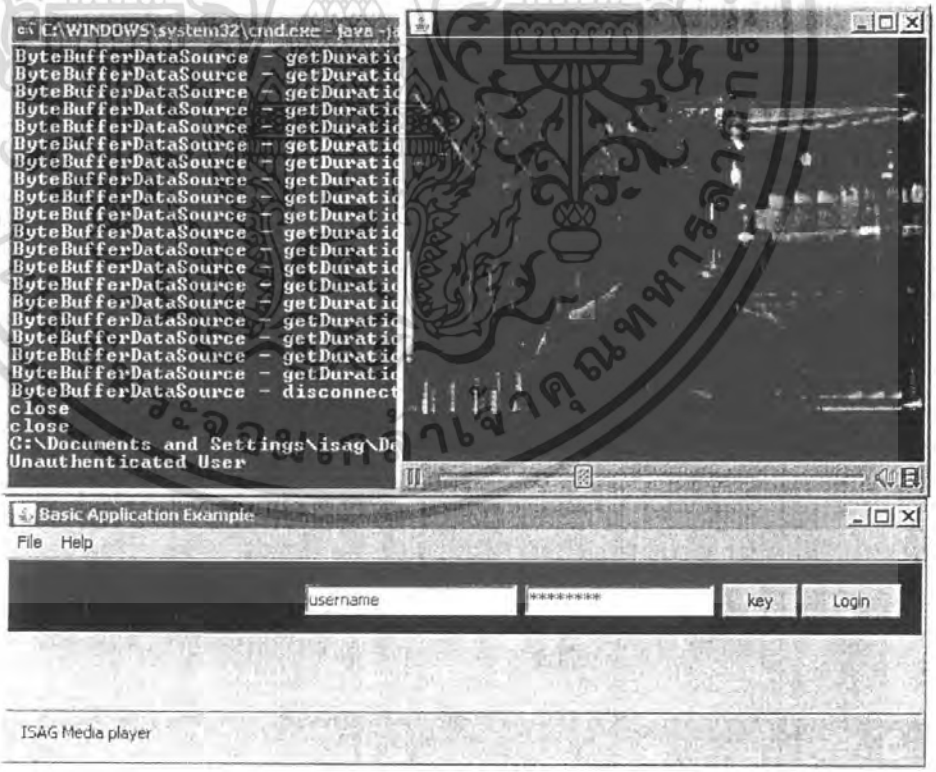


รูปที่ 3.9 แสดงการ Browse ไฟล์กุญแจสาธารณะ

รูปที่ 3.10 แสดงเมื่อทำการ Login แล้ว



รูปที่ 3.11 แสดงหลักการกู้คุณภาพกลับของไฟล์สื่อดิจิตอล



รูปที่ 3.12 แสดงหลักการกู้คุณภาพกลับของไฟล์สื่อดิจิตอล

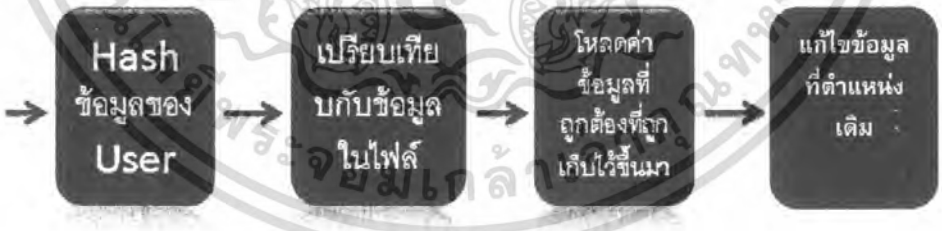
รูปที่ 3.13 แสดงหลักการกู้คุณภาพกลับของไฟล์สื่อดิจิตอล

- โปรแกรมสามารถย้อนกระบวนการลดคุณภาพสื่อดิจิตอล เพื่อให้สามารถใช้งานสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ได้คุณภาพสูง เมื่อผู้ใช้งานสามารถยืนยันตัวตนได้เรียบร้อย

<u>ขั้นตอนการย้อนกระบวนการลดคุณภาพ</u>

สื่อดิจิตอลประเภทเพลง (MP3) และประเภทภาพยนตร์ (AVI)

- กระบวนการย้อนกลับ มีกระบวนการทำงานหลักดังรูป



รูปที่ 3.14 แสดงหลักการกู้คุณภาพกลับของไฟล์สื่อดิจิตอล

<u>สื่อดิจิตอลประเภทเพลง (MP3)</u>

การแก้ไขไฟล์ที่ถูกลดคุณภาพมีกลับมามีคุณภาพเดิม มีกระบวนการทำงานอธิบายเป็นขั้นตอนได้ดังนี้

1. ทำการตรวจสอบความเป็นเจ้าของก่อนโดยการเทียบค่า Hash จากการยืนยันตัวตน กับค่า Hash ที่แทรกไว้ในสื่อดิจิตอล

2. โดยทำการ Hash โดยใช้ SHA-1 ในการ Hash และได้ output มาเป็น array of byte มีสมาชิกทั้งหมด 20 ไบต์ โดยทำการ Hash ค่า Username ต่อกับ Password ที่ Hash ด้วย MD5 ของ user คนนั้น เพื่อนำมาใช้ระบุตำแหน่งของ เฮดเดอร์ (Frame Header) แต่ละเฟรม (Frame)

3. นำค่าที่ได้จากการ Hash แล้วมาแก้ไขข้อมูล จากตำแหน่งที่กำหนดไว้ โดยทำการนำค่าของตำแหน่งนั้นลบออกด้วยค่าของ ไบต์ที่ตำแหน่งนั้น ซึ่งจะทำให้ในไฟล์นั้นๆ ของแต่ละ User มีการแก้ไขที่ต่างกันในแต่ละ User

ประเภทภาพยนตร์ (AVI)

การแก้ไขไฟล์ที่ถูกลดคุณภาพมีกลับมามีคุณภาพเดิม มีกระบวนการทำงานหลักอธิบายเป็นขั้นตอนได้ดังนี้

1. ทำการตรวจสอบความเป็นเจ้าของก่อนโดยการเทียบค่า Hash จากการยืนยันตัวตน กับค่า Hash ที่แทรกไว้ในสื่อดิจิตอล

2. โดยทำการ Hash โดยใช้ SHA-1 ในการ Hash และได้ output มาเป็น array of byte มีสมาชิกทั้งหมด 20 ไบต์ โดยทำการ Hash ค่า Username ต่อกับ Password ที่ Hash ด้วย MD5 ของ user คนนั้น เพื่อนำมาใช้ระบุตำแหน่งของ เฮดเดอร์ (Frame Header) แต่ละเฟรม (Frame)

3. นำค่าที่ได้จากการ Hash แล้วมาเข้าสู่กระบวนการในการเลือกตำแหน่ง เฮดเดอร์ (Frame Header) ที่จะเข้าไปแก้ไขข้อมูล โดยบวกเข้าไปอีก 10 ไบต์จากตำแหน่งที่ได้เพื่อไม่ให้ทับ Meta data ใน เฮดเดอร์ (Frame Header) ซึ่งจะทำให้ในไฟล์นั้นๆของแต่ละ User มีการแก้ไขที่ต่างกันในแต่ละ User

โดยจะแตกต่างกันที่การเลือกตำแหน่งของสื่อดิจิตอลประเภทเพลง (MP3) จะได้ตำแหน่งที่ไม่คงที่ แต่ประเภทภาพยนตร์ (AVI) จะกำหนดตำแหน่งไว้ตายตัวเนื่องจากความซับซ้อนของโครงสร้างทำให้ไม่สามารถเข้าไปแก้แบบไม่มีระบบได้ แต่ยังคงแก้ไขแบบมีเอกลักษณ์ เพราะค่าที่นำเข้าไปแก้ไขจะต้องมาจากข้อมูลของแต่ละเจ้าของ เพื่อให้เกิดรูปแบบเฉพาะตัว

ขั้นตอนการทำงานของระบบจัดการสื่อดิจิตอล

สื่อดิจิตอลประเภทเพลง (MP3) และประเภทภาพยนตร์ (AVI)

1. ตรวจสอบลายมือชื่อสาธารณะ ในไฟล์สื่อดิจิตอลก่อนว่าถูกต้องหรือไม่ โดยการใช้ Public Key ที่ได้รับทางอีเมล์

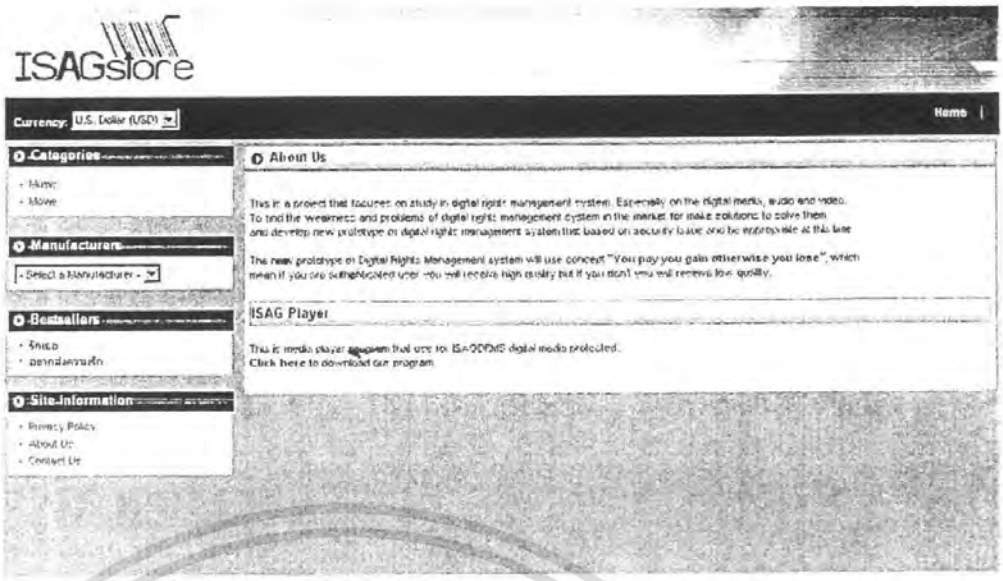
2. โปรแกรมจะนำเอา Public Key ไปใช้ถอดรหัสลับ ข้อมูลสำคัญที่ใช้ในการตรวจสอบ

3. ถ้าตรวจสอบแล้วผ่าน ก็จะทำการย้อนกระบวนการการลดคุณภาพสื่อดิจิตอล

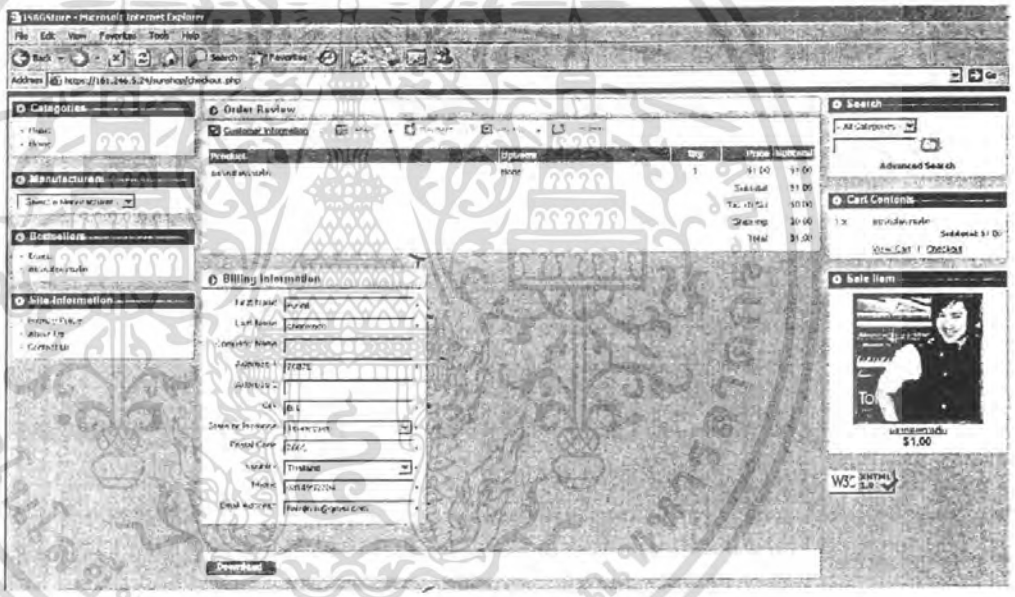
3.2.3.3 พัฒนาร้านค้าสื่อดิจิตอลออนไลน์ ISAG Store

- สร้างเพื่อใช้ในการสาธิต การทำงานของต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลผ่านการดาวน์โหลด ไฟล์สื่อดิจิตอล
- โดยพัฒนาเวปเซฟเวอร์ Apache2 บนระบบปฏิบัติการ Windows XP service pack II และติดตั้ง PHPMyAdmin และ MySQL เพื่อจัดการเกี่ยวกับฐานข้อมูลของเวปเซฟเวอร์
- ผู้ใช้งานต้องสมัครสมาชิก และทำการ Login ก่อนจึงจะสามารถสั่งซื้อสื่อดิจิตอลจาก ISAG Store ได้
- เมื่อทำการสั่งซื้อเพลง จะต้องทำการยืนยันตัวตนอีกครั้ง แทนระบบการจ่ายเงินจริงผ่านบัตรเครดิต หรือระบบจ่ายเงินออนไลน์ทั่วไป
- ทำการเขียน PHP Script เพื่อไปติดต่อกับโปรแกรมสร้างไฟล์สื่อดิจิตอล โดยจะส่งค่าตัวแปร คือ username, password ที่ทำการ Hash และชื่อไฟล์สื่อดิจิตอล เมื่อสร้างไฟล์สื่อดิจิตอลเสร็จจะเข้าสู่หน้าเวปเพื่อให้ทำการดาวน์โหลดต่อไป ดังตัวอย่างรูปหน้าเวป ISAG Store

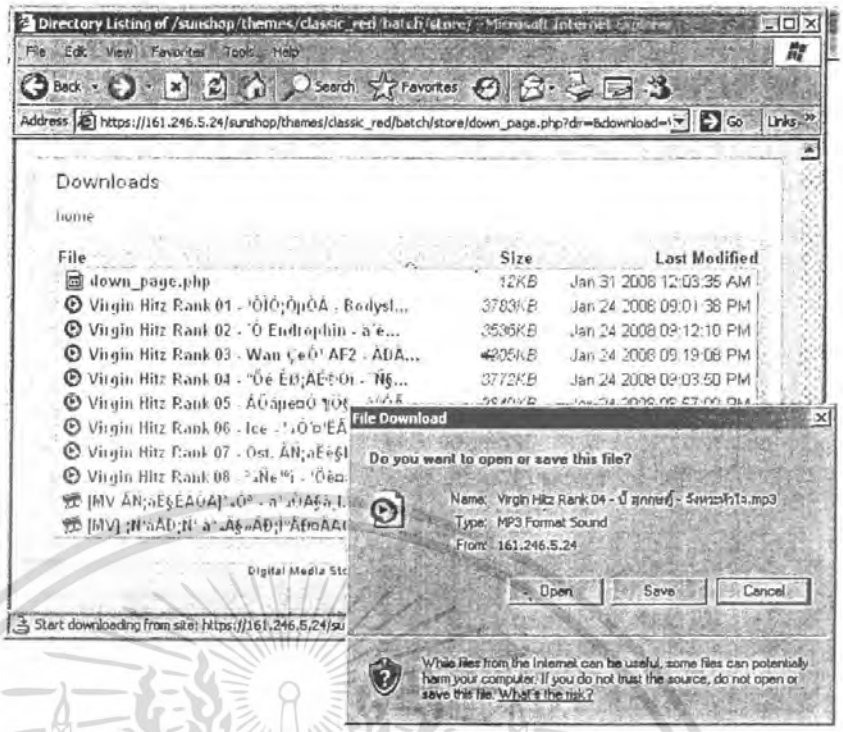
รูปที่ 3.15 แสดงหน้าแรกเวป ISAG Store



รูปที่ 3.16 แสดงหน้า About Us ของเวป ISAG Store



รูปที่ 3.17 แสดงหน้าcart เวป ISAG Store แสดงรายการที่ซื้อเพื่อจะ download



รูปที่ 3.18 แสดงหน้า download เวป ISAG Store

ขั้นตอนการซื้อสื่อดิจิตอลผ่าน ISAG Store ดังรูป

รูปที่ 3.19 แสดงการทำงานของ ISAG Store

1. ต้องสมัครเป็นสมาชิก โดยจะใช้ Username และ Password ในการ Login เข้าใช้งานเวป

2. เลือกสื่อดิจิตอลที่ต้องการจะซื้อ รายการซื้อจะแสดงทางหน้าเวป cart

3. เมื่อทำการกด Download จะต้องทำการยืนยันตัวตนแทนการจ่ายเงินผ่านบัตรเครดิต หรือระบบชำระเงินออนไลน์ทั่วไป

4. เมื่อยืนยันตัวผ่านเวปจะทำการเรียกโปรแกรมผลิตสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ ให้สร้างสื่อดิจิตอล ถ้าเป็นการซื้อครั้งแรกจะทำการสร้างคู่กุญแจสาธารณะแล้วส่ง Public Key ไปให้ผู้ใช้ทางอีเมล์โดยอัตโนมัติ

5. เมื่อเข้าหน้า Download จะเห็นรายการสื่อดิจิตอลที่สั่งซื้อ กดที่ Link แล้ว Browser จะทำการ Download ไฟล์สื่อดิจิตอลให้ทำที

บทที่4

การทดลองและผลการทดลอง

4.1 ขั้นตอนเขียนโปรแกรมติดต่อสื่อดิจิตอล

4.1.1 การเขียนโปรแกรมเข้าถึงภายในสื่อดิจิตอลประเภทเพลง (MP3)

โดยพิจารณาจากลักษณะโครงสร้างของ MP3 ซึ่งมีลักษณะดังรูปต่อไปนี้

รูปที่ 4.1 แสดงรูปแบบของ MP3เฮดเดอร์ (Frame Header)

ตำแหน่งที่แทนด้วยอักษร A นั้นเป็นส่วนที่เรียกว่า Frame sync โดย A ทั้งหมด 11 bits จะถูกกำหนดค่าให้เป็น 1 ทั้งหมด เพื่อให้สามารถเขียนโปรแกรมเพื่อติดต่อเข้าไปได้ และนอกจากนั้นถ้าพิจารณาที่ B ซึ่งมี 2 bits พบว่าค่า 00 คือ MPEG version 2.5 และ 01 เป็นค่าที่ไม่อนุญาติให้ใช้ ดังนั้นจึงสามารถเพิ่มเงื่อนไขเพิ่มเติมว่าต้องพบ 1 ทั้งหมด 12 bits ได้ ซึ่งในทางปฏิบัติแล้วยังไม่เพียงพอ เพราะภายใน MP3 นั้นยังมีส่วนของ Data ที่อาจจะมีค่าเดียวกันนี้รวมอยู่ด้วย ดังนั้นถ้ามีเงื่อนไขเพียง Frame sync อาจทำให้ได้เฮดเดอร์(Frame Header) ที่ผิดตำแหน่งได้ ดังนั้นจึงควรเขียนโปรแกรมเข้าไปตรวจสอบค่าภายในนั้นของเฮดเดอร์(Frame Header) แล้วตรวจสอบดูว่าตรงกับข้อมูลจริงๆหรือไม่ เช่น ค่า Bitrates นั้นสามารถคำนวณหาได้ ค่า Sample Rate ก็เช่นกัน จึงควรคำนวณหาค่าเหล่านี้แล้วนำมาเปรียบเทียบกับข้อมูลจริงๆ

และการที่จะไปยังเฟรม(Frame) ถัดไป ควรจะมีการตรวจสอบก่อนว่า ความยาวของเฟรม (Frame) เดิมนั้นเป็นเท่าไร และมีการทำ CRC หรือไม่ เพื่อที่จะคำนวณหาตำแหน่งถัดไปได้อย่างไม่ผิดพลาด

4.2 ขั้นตอนการทดลองลดคุณภาพสื่อดิจิตอล

4.2.1 ขั้นตอนการลดและกู้คืนคุณภาพเสียง

- **การลดคุณภาพเสียง**

  เมื่อนำไฟล์สื่อดิจิตอลที่ทำการลดคุณภาพแล้ว ไปเล่นด้วยโปรแกรม Media Player ทั่วไป จะเล่นได้แต่ภาพจะมีจุดสีเพี้ยนและเสียงจะมี noise

- **การแก้ไขไฟล์ที่ถูกลดคุณภาพมีกลับมามีคุณภาพเดิม**

  เมื่อนำไฟล์สื่อดิจิตอลที่ทำการลดคุณภาพแล้ว ไปเล่นด้วยโปรแกรม ISAG Player และทำการยืนยันตัวตนของผู้ใช้ได้ว่าเป็นเจ้าของไฟล์สื่อดิจิตอล จะเล่นได้คุณภาพสูง

4.2.2 ขั้นตอนการลดและกู้คืนคุณภาพภาพยนตร์

- **การลดคุณภาพภาพยนตร์**

  เมื่อนำไฟล์สื่อดิจิตอลที่ทำการลดคุณภาพแล้ว ไปเล่นด้วยโปรแกรม Media Player ทั่วไป จะเล่นได้แต่ภาพจะมีจุดสีเพี้ยนและเสียงจะมี noise

- **การแก้ไขไฟล์ที่ถูกลดคุณภาพมีกลับมามีคุณภาพเดิม**

  เมื่อนำไฟล์สื่อดิจิตอลที่ทำการลดคุณภาพแล้ว ไปเล่นด้วยโปรแกรม ISAG Player และทำการยืนยันตัวตนของผู้ใช้ได้ว่าเป็นเจ้าของไฟล์สื่อดิจิตอล จะเล่นได้คุณภาพสูง

4.2.3 ขั้นตอนทดลองการทำ Steganography ด้วย MP3Stego

เป็นการทำการทดลองเกี่ยวกับ Steganography ในการ แทรกข้อมูลลับเข้าไปในไฟล์ digital ในขณะที่ทำการบีบอัด .Wav เป็น .Mp3 โดยอาศัยหลักการข้อจำกัดในการรับรู้ของ

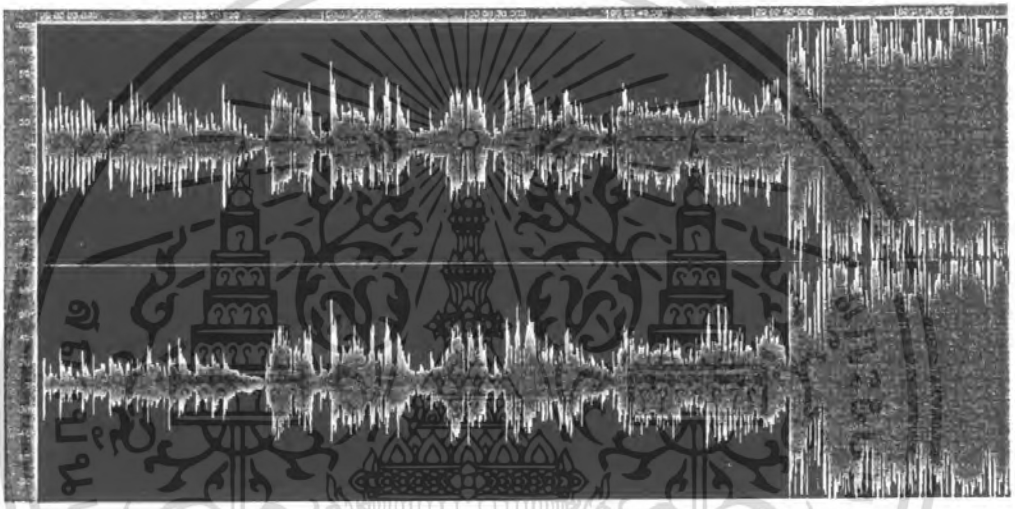
มนุษย์ หรือ HAP (Human Auditory Perception) โดยในการทดลองได้ทำการทดลองผ่านโปรแกรม MP3Stego ในการทดลองเพื่อศึกษาถึงกระบวนการและขั้นตอนในการทำงาน สิ่งที่ได้ทำไปคือเขียน GUI ด้วยภาษา C# เพื่อเขียน Batch file เข้าไปสั่งงานในโปรแกรม (เดิมทีการสั่งงานเป็นแบบ command line ซึ่งไม่สะดวกต่อการใช้งาน) และได้ทำการปรับรุงให้เหมาะสมกับการใช้งานมากยิ่งขึ้น คือมีการตรวจสอบความถูกต้องของข้อมูลที่แทรกเอาไว้ในตัวไฟล์ mp3 โดยการเรียกข้อความนั้นคือมาดู โดยโปรแกรมมีหน้าจอการทำงานดังนี้

รูปที่ 4.2 แสดงโปรแกรมที่ทดลองเขียนติดต่อกับ MP3Stego

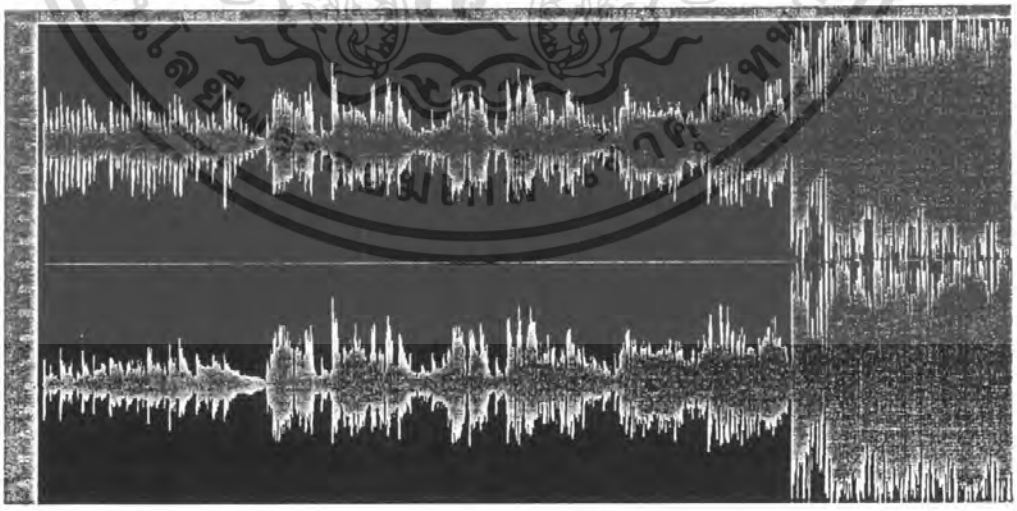
รูปที่ 4.3 การทำงานของโปรแกรม MP3Stego

4.3 ผลการทดลองลดคุณภาพสื่อดิจิตอล

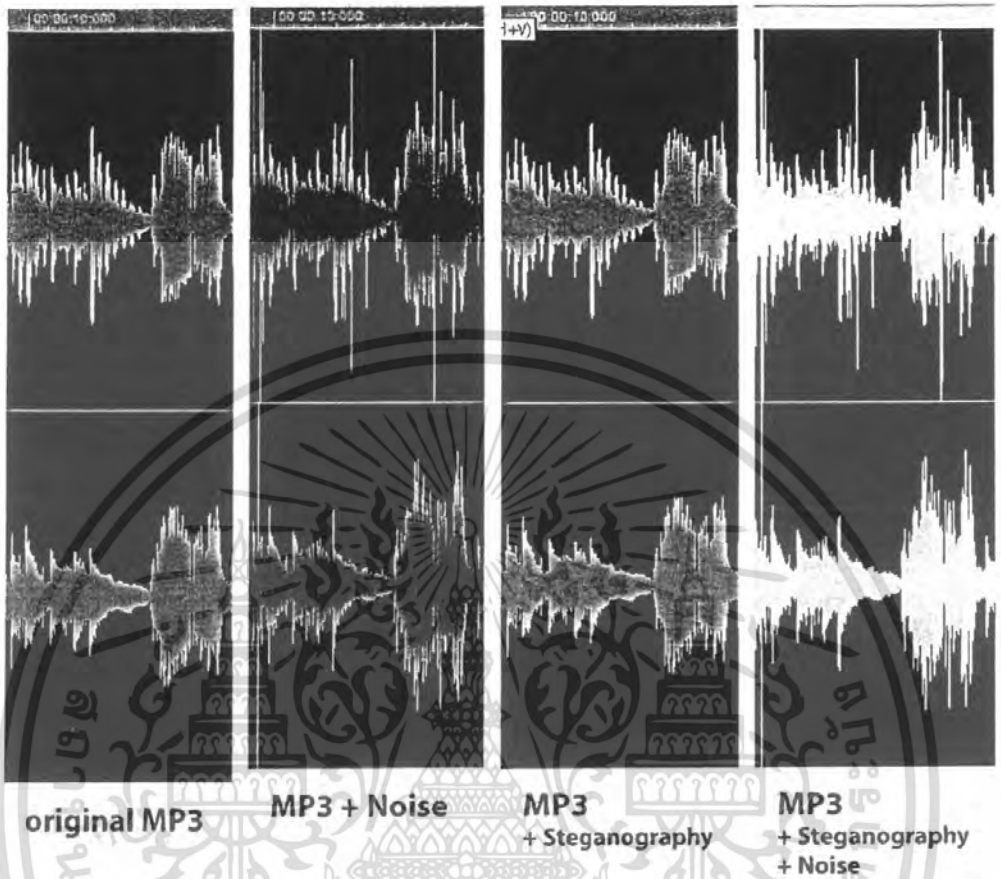
โดยผลจากการลดคุณภาพไฟล์สื่อดิจิตอล นอกจากการทดลองโดยการเล่นด้วยโปรแกรมเล่นสื่อดิจิตอล เพื่อใช้ประสาทรับรู้ของมนุษย์ในการรับชม และรับฟังนั้นอาจแยกแยะได้ไม่ดีพอ ประสาทรับรู้ของมนุษย์แต่ละคนมีข้อจำกัด และไม่เป็นมาตรฐาน ผลการทดลองจึงแสดงด้วยการใช้การเปรียบเทียบรูปแบบของคลื่น ของเสียง(Sound Wave Form)



รูปที่ 4.4 แสดง wave form ของไฟล์ waveที่ทดลอง

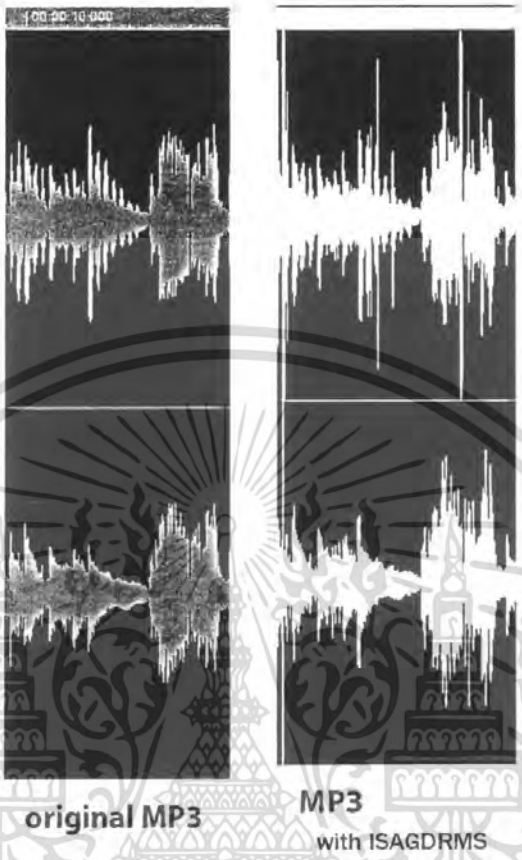


รูปที่ 4.5 แสดง wave form ของไฟล์ waveที่ตัดมาทดลอง



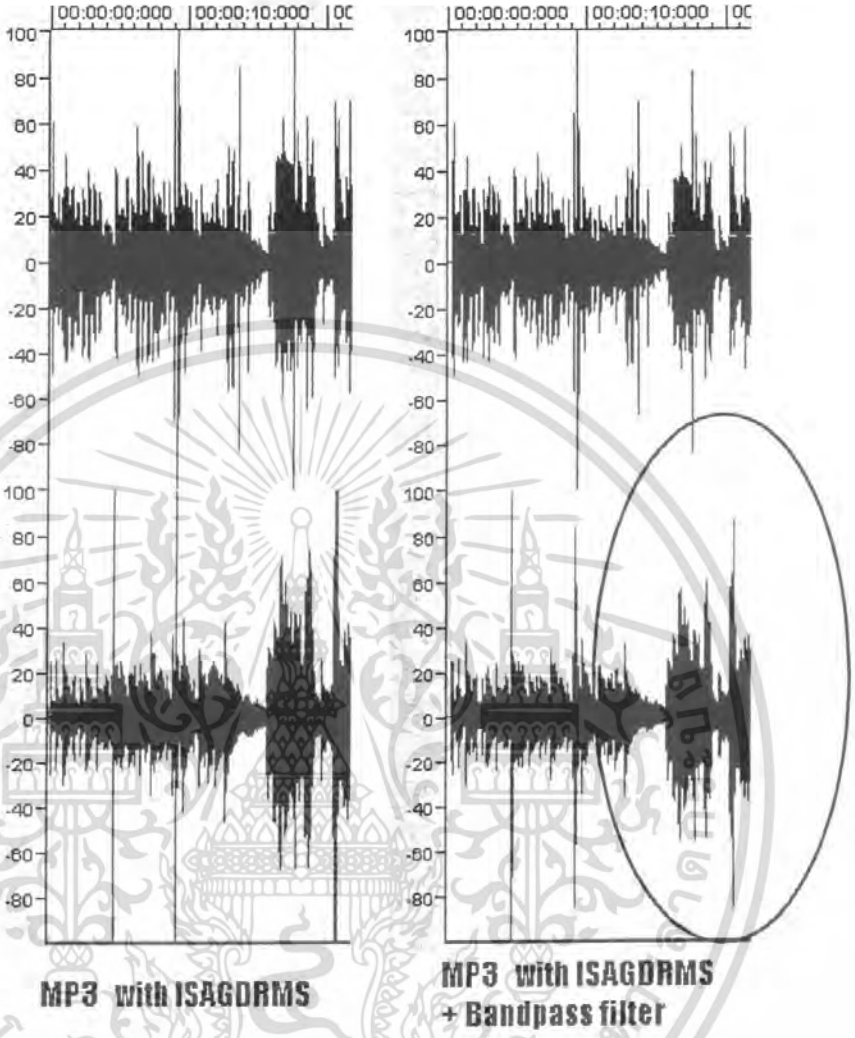
รูปที่ 4.6 แสดงการเปรียบเทียบ wave form ของไฟล์ที่ทดลอง

โดยจากรูปข้างบน จะเห็นว่า wave form ของไฟล์ MP3 ธรรมดา กับไฟล์ MP3 ที่เกิดจากการ compress ด้วยการทำ Steganography โดยการ แทรก Text file เข้าไป ไม่มีความแตกต่างเลย เป็นการพิสูจน์แล้วว่า หลักการที่ซ่อนการมีอยู่ของข้อมูลเป็นจริงตามทฤษฎี



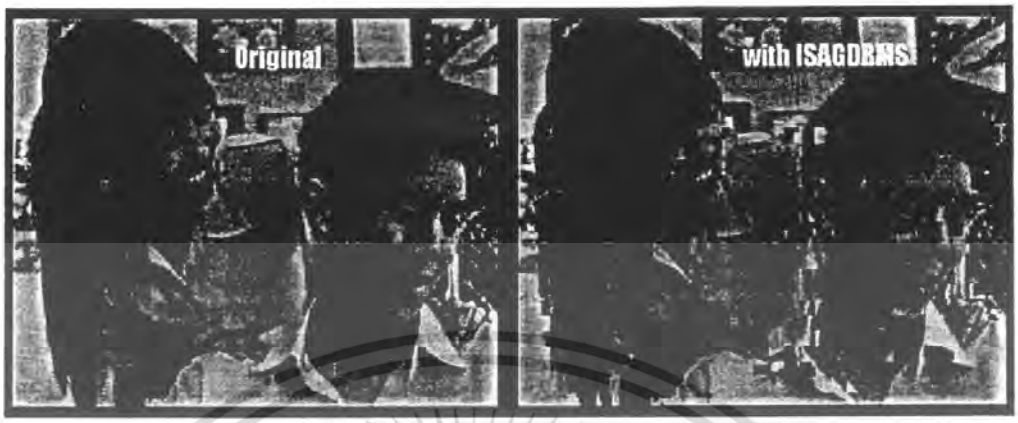
รูปที่ 4.7 แสดงการเปรียบเทียบ wave form ของไฟล์ที่ทดลอง

โดยจากรูปข้างบน ไฟล์ MP3 ธรรมดา กับไฟล์ MP3 ที่ผ่านกระบวนการจัดการลิขสิทธิ์แล้ว จะเห็นว่า wave form มีความแตกต่างกัน และเมื่อเล่นด้วย Media Player ทั่วไปจะฟังแล้วมี noise แต่เล่นด้วย ISAG Player และยืนยันตัวตนได้ก็จะเล่นได้คุณภาพสูง



รูปที่ 4.8 แสดงการเปรียบเทียบ wave form ของไฟล์ที่ทดลอง

โดยจากรูปข้างบน ไฟล์ MP3 ที่ผ่านกระบวนการจัดการลิขสิทธิ์ กับไฟล์ MP3 ที่ผ่านกระบวนการจัดการลิขสิทธิ์ที่นำไปผ่าน Amplification filter ด้วยโปรแกรมแต่งเสียงทั่วไป จะเห็นว่า wave form มีความแตกต่างกัน โดยจะมี Amplitude ที่ต่ำลง และเมื่อเล่นด้วย Media Player ทั่วไปจะฟังแล้วยังคงมี noise อยู่ไม่สามารถทำให้ noise ลดลงได้



รูปที่ 4.9 แสดงการเปรียบเทียบ ภาพจากไฟล์สื่อดิจิตอล

โดยจากรูปข้างบน ไฟล์ AVI ธรรมดา กับไฟล์ AVI ที่ผ่านกระบวนการจัดการลิขสิทธิ์แล้ว จะเห็นว่าภาพที่เห็น มีความแตกต่างกันโดยเมื่อเล่นด้วย Media Player ทั่วไปภาพมีจุดสีเพี้ยนแล้วเสียงจะมี noise แต่เล่นด้วย ISAG Player และยืนยันตัวตนได้ก็จะเล่นได้คุณภาพสูง

4.4 ผลการทดลองเปรียบเทียบสื่อดิจิตอลที่การจัดการลิขสิทธิ์

4.4.1 การทดลองลดคุณภาพไฟล์สื่อดิจิตอลประเภทเพลง แสดงด้วยการใช้การเปรียบเทียบรูปแบบของคลื่น ของเสียง(Sound Wave Form) ของไฟล์ MP3 ธรรมดา กับไฟล์ MP3 ที่มีการจัดการด้วย ISAGDRMS

- การทำ Steganography จะเห็นว่า wave form ไม่มีความแตกต่างเลย เป็นการพิสูจน์แล้วว่า หลักการที่ซ่อนการมีอยู่ของข้อมูลเป็นจริงตามทฤษฎี
- ผ่านกระบวนการจัดการลิขสิทธิ์แล้ว จะเห็นว่า wave form มีความแตกต่างกัน และเมื่อเล่นด้วย Media Player ทั่วไปจะฟังแล้วมี noise แต่เล่นด้วย ISAG Player และยืนยันตัวตนได้ก็จะเล่นได้คุณภาพสูง

4.4.2 การทดลองลดคุณภาพไฟล์สื่อดิจิตอลประเภทภาพยนตร์ แสดงด้วยการใช้การเปรียบเทียบรูปภาพที่ Capture จากไฟล์ AVI ธรรมดา กับไฟล์ AVI ที่มีการจัดการด้วย ISAGDRMS อีก 3 ไฟล์ที่เป็นภาพยนตร์เรื่องเดียวกันแต่เจ้าของต่างกัน โดยจะเปรียบเทียบภาพช่วงเวลาเดียวกัน

- ผ่านกระบวนการจัดการลิขสิทธิ์แล้ว จะเห็นว่า ภาพ จะมีจุดเพี้ยนของสี มีความแตกต่างกัน ทั้ง 3 ภาพที่เจ้าของต่างกัน ดังรูป

รูปที่ 4.10 แสดงการเปรียบเทียบภาพจากไฟล์สื่อดิจิตอล

- เมื่อเล่นด้วย Media Player ทั่วไปจะมีจุดเพี้ยนของสี และ noise ในเสียง แต่เล่นด้วย ISAG Player และยืนยันตัวตนได้ก็จะเล่นได้คุณภาพสูง

บทที่ 5
บทสรุป

5.1 สรุปการพัฒนา

จากการศึกษาและวิเคราะห์เพื่อแก้ปัญหาต่างๆของระบบจัดการลิขสิทธิ์สื่อดิจิตอล ทำให้ออกแบบต้นระบบจัดการลิขสิทธิ์สื่อดิจิตอล เพื่อจัดการลิขสิทธิ์บนสื่อดิจิตอลโดยที่ยังคงความสามารถในการใช้งานทั่วไปของไฟล์ดิจิตอลไว้ และยึดหลักการที่ว่า "ผู้ซื้อจะสามารถเล่นสื่อดิจิตอลได้คุณภาพสูง แต่ผู้ละเมิดลิขสิทธิ์จะเล่นได้คุณภาพต่ำ" ใช้การยืนยันตัวตนของผู้ใช้งานเพื่อกำหนดสิทธิ์การเข้าใช้งานสื่อดิจิตอล

ทำการทดลองสร้างไฟล์สื่อดิจิตอลที่มีการจัดการด้วยระบบจัดการลิขสิทธิ์สื่อดิจิตอลแล้วนำไปเล่นด้วยโปรแกรมเล่นสื่อดิจิตอลทั่วไปได้คุณภาพต่ำ แต่เล่นด้วย ISAG Player และสามารถยืนยันตัวตนได้เล่นได้คุณภาพสูง

- ออกแบบต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอล
- ทำการเขียนโปรแกรมที่นำต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลนี้มาใช้ โดยแบ่งออกเป็น 2 ส่วน คือ
    1. โปรแกรมสร้างสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์
    2. โปรแกรมเล่นสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์
- สาธิตการใช้งานสื่อดิจิตอลที่มีการจัดการลิขสิทธิ์ และรูปของระบบการจัดการลิขสิทธิ์สื่อดิจิตอล ด้วยระบบซื้อสื่อดิจิตอลผ่านร้านค้าสื่อดิจิตอลออนไลน์ ISAG Store
- สร้างระบบการยืนยันตัวตนโดยตรวจสอบจาก ข้อมูลที่ซ่อนอยู่บนไฟล์สื่อดิจิตอล ถ้ามีการละเมิดก็ใช้การตรวจสอบเป็นหลักฐานเพื่อดำเนินคดีต่อไป และ ยังสามารถตรวจสอบการเปลี่ยนแปลงของไฟล์ได้จากการทำลายมือชื่อดิจิตอล

5.2 ปัญหาและอุปสรรค

5.2.1 การศึกษาข้อมูลพื้นฐานของระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่มีอยู่ในปัจจุบันทำได้ยาก เนื่องจากปกปิดเป็นความลับ

5.2.2 การเขียนโปรแกรมติดต่อไฟล์ดิจิตอลทำได้ยาก และทำให้งานได้ล่าช้ากว่าแผนที่วางไว้

5.2.3 เกิดปัญหาการเลือกใช้ภาษาในการเขียน เปลี่ยนจาก C# ซึ่งติดปัญหาการแก้ไข Library ซึ่งทำได้ยาก เป็น Java ระหว่างการพัฒนา เนื่องจาก Java มี Open source ช่วยให้การพัฒนาได้ดีมากกว่า

5.2.4 เกิดปัญหาฮาร์ดดิสเสียระหว่างการพัฒนา ทำให้ข้อมูลที่เกี่ยวข้องกับโครงงานหายไปแต่เพียงส่วนน้อย

5.2.5 เกิดปัญหาในตัวโปรแกรมเล่นสื่อดิจิตอลที่พัฒนาขึ้นในส่วนการเล่นภาพยนตร์ สามารถแก้ไขให้เล่นได้คุณภาพสูงได้ แต่มีปัญหา codec ไม่สามารถหา format ของเสียงเจอทำให้เล่นได้ภาพที่สมบูรณ์แต่เสียงไม่ออก

5.2.6 เปลี่ยนจาก AVI format เป็น MPG เนื่องจะความหลากหลายในมาตรฐานของ AVI และ Library ที่ใช้ไม่สามารถทำให้ AVI ทำงานได้สมบูรณ์

5.3 แนวทางการพัฒนาต่อ

5.3.1 พัฒนาระบบจัดการลิขสิทธิ์นี้ ให้ใช้ได้กับ file format ที่หลากหลายขึ้น หรือใช้ได้กับสื่อดิจิตอลประเภทอื่น

5.3.2 พัฒนาวิธีการลดคุณภาพ และการกู้กลับ เพิ่มเติม

5.3.3 พัฒนาให้สามารถ plug-in กับ media player อื่นๆได้

5.3.4 สร้างการป้องกันการคัดลอกสื่อดิจิตอล(Copy protection)

5.3.5 พัฒนาและปรับปรุงให้โปรแกรมเล่นสื่อดิจิตอลสมบูรณ์ สวยงามมากขึ้น

5.4 ข้อสรุปและข้อเสนอแนะ

เนื่องจากการศึกษาชี้ให้เห็นว่าระบบจัดการลิขสิทธิ์สื่อดิจิตอลในปัจจุบัน นั้นมันสร้างปัญหาให้กับผู้ใช้งาน ทั้งการบังคับการใช้งานต่างๆ การใช้รูปแบบไฟล์เฉพาะ การที่ต้องอาศัยอินเตอร์เน็ตตลอดเวลา รวมถึงกระทำต่อทรัพย์สินของผู้ใช้โดยไม่บอก ซึ่งอาจก่อให้เกิดความเสียหายได้ ทำให้การนำหลักการของระบบจัดการลิขสิทธิ์สื่อดิจิตอล มาใช้งานลดน้อยลง หรือที่มีใช้อยู่ก็เริ่มทยอยเลิกใช้ไป ทำให้ระบบจัดการลิขสิทธิ์สื่อดิจิตอล เหมือนเป็นเทคโนโลยีที่ใกล้ตาย

ด้วยเหตุผลข้างต้น ต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลที่ได้ทำการออกแบบและพัฒนาขึ้นนั้น ประยุกต์ให้เหมาะสมกับลักษณะการใช้งานในปัจจุบันมากขึ้น โดยมีแนวคิดหลักคือ คงความสามารถในการใช้งาน และผู้ที่เป็นเจ้าของต้องเล่นได้คุณภาพสูง แต่ผู้ที่ละเมิดลิขสิทธิ์จะเล่นได้แต่ได้คุณภาพต่ำ ซึ่งต้นแบบระบบจัดการลิขสิทธิ์สื่อดิจิตอลนี้ยังสามารถนำไปพัฒนาต่อยอดได้ ทั้งรูปแบบการลดคุณภาพสื่อดิจิตอล และเพิ่มการจัดการการป้องกันการคัดลอกเพิ่มเติมเพื่อให้เกิดความปลอดภัยมากยิ่งขึ้น

บรรณานุกรม

CENTER FOR DEMOCRACY & TECHNOLOGY, **Evaluating DRM:Building a Marketplace for the Convergent World**, 1634 I St., NW, Suite 1100, Washington, DC 20006, http://www.cdt.org, , September 2006 – Version 1.0, 20060907drm.pdf

DMAG, **Protection of MP3 Music Files Using Digital Rights Management and Symmetric Ciphering**, Dept. AC, Campus Nord Mòdul D6, E-08034 Barcelona, Spain DRM_Sys.pdf

Gregory Kesden Fall 2000, **Content Scrambling System (CSS)**, Carnegie Mellon University, 15-412, css.ppt

Worakit, IIT_NU 48 G-2, **การเข้ารหัสและการถอดรหัสข้อมูล**, encryp.pdf

OpenDML February 28, 1996, **AVI File Format Extensions**, Version 1.02, odmlff2-avidef.pdf

Praveen Sripada, March 2006, Department of Signal Processing and Telecommunications, Sweden Masters Thesis Report, Blekinge Tekniska Högskola, **MP3 DECODER in Theory and Practice**, MP3_Decoder.pdf

Frank Hartung and Friedhelm Ramme, 2000, Ericsson Research, **SELECTED PAPERS FROM ISS, Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications**, DRM_watermark_00883493.pdf

Gallery of CSS Descramblers .[Online]

Available : http://www.cs.cmu.edu/~dst/DeCSS/Gallery/

Available : http://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html

DRM Documentation .[Online]

Available : http://en.wikipedia.org/wiki/Digital_rights_management

Available : http://www.eff.org/IP/DRM/

Microsoft's DRM .[Online]

Available : http://www.microsoft.com/windows/windowsmeda/forpros/drm/default.mspx

Apple's DRM(Fairplay) .[Online]

Available : http://www.roughlydrafted.com/RD/RDM.Tech.Q1.07/2A351C60-A4E5-4764-A083-FF8610E66A46.html

File format .[Online]

Available : http://www.dv.co.yu/mpgscript/mpeghdr.htm

Available : http://www.mpgedit.org/mpgedit/mpeg_format/MP3Format.html

Available : http://www.virtualsciencefair.org/2004/chia4a0/public_html/aviresearch.htm,avi.pdf

Copy Protection for DVD Video, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999, No. 00771077

Laurence Boney, Ahmed H. Tewfik, Khaled N. Hamdy, Department of Electrical Engineering, University of Minnesota, Minneapolis, ***Digital Watermarks for Audio Signals, IEEE* No. 00535015**