บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ปัจจุบันความเจริญก้าวหน้าทางด้านวิทยาศาสตร์และเทคโนโลยีทำให้เกิดการคิดค้นการติดต่อสื่อสารหลากหลายรูปแบบ อินเทอร์เน็ตก็เป็นอีกรูปแบบหนึ่งของเทคโนโลยีการสื่อสารที่มีการใช้งานอย่างกว้างขวางซึ่งเปรียบเสมือนจุดเชื่อมคนจากหลายแห่งทั่วโลกเข้าหากัน ซึ่งทำให้ระยะทางในการติดต่อสื่อสารสั้นลง ไม่ว่าจะอยู่ที่ไหนของโลก การส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์ เป็นการใช้ความสามารถของระบบอินเทอร์เน็ต ซึ่งมีข้อดีคือ ความสะดวก ความรวดเร็ว ความประหยัด ไม่จำกัดระยะทาง ซึ่งปัจจุบันมีการใช้งานอย่างแพร่หลาย

ในการส่งข้อมูลที่อยู่ในรูปแบบกระดาษ ดูเหมือนจะมีข้อได้เปรียบกว่าการส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์กล่าวคือ จะมีความเชื่อถือและมั่นใจได้ว่าผู้ส่งข้อมูลดังกล่าวเป็นบุคคลคนเดียวกับบุคคลที่มีชื่ออยู่ในการส่งข้อมูลจริงๆ โดยการตรวจสอบลายมือชื่อ แต่การส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์นั้นพบว่า ความเชื่อถือและความมั่นใจว่าผู้ส่งข้อมูลเป็นบุคคลคนเดียวกับบุคคลที่มีชื่ออยู่ในการส่งข้อมูลจะมีน้อยกว่า นอกจากนี้พบว่ามีความไม่ปลอดภัยในระหว่างการส่งข้อมูล คืออาจมีการเข้ามาทำลายข้อมูล ปลอมแปลง แก้ไขข้อมูล ขโมยข้อมูล รวมถึง การนำข้อมูลไปเปิดเผยกับผู้ไม่มีสิทธิ์ ซึ่งสิ่งเหล่านี้ได้สร้างผลกระทบและความเสียหายต่อผู้ส่งข้อมูล ผู้รับข้อมูล รวมถึงองค์กรที่เกี่ยวข้อง จากความไม่ปลอดภัยในการส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์ดังกล่าว ทำให้มีการคิดค้นและพัฒนาให้การส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์สามารถยืนยันตัวผู้ส่งได้ คือ ลายมือชื่อดิจิทัล (Digital Signature) โดยการนำเอาหลักการของการเข้ารหัสข้อมูลเข้ามาช่วยในการทำงาน ทำให้สามารถยืนยันตัวผู้ส่งได้ รวมถึงการเพิ่มส่วนของการเข้ารหัสของข้อมูลที่ส่งเพื่อเพิ่มความปลอดภัยในการส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์ ผู้ศึกษาได้ทำการศึกษาหลักการและการทำงานของลายมือชื่อดิจิทัล ประกอบกับได้ศึกษาการประมวลผลภาพในส่วนของการซ่อนข้อมูลบนภาพซึ่งใช้ในการส่งข้อมูลที่เป็นความลับระหว่างผู้ส่งและผู้รับ โดยผู้ส่งและผู้รับเท่านั้นที่สามารถเห็นข้อมูลที่ส่งได้ ทำให้ผู้ศึกษาเกิดแนวคิดในการนำเอาหลักการของการซ่อนข้อมูลบนภาพมาใช้ร่วมกับการสร้างลายมือชื่อดิจิทัล ซึ่งเป็นการสร้างทางเลือกให้กับผู้ใช้ที่ต้องยืนยันตัวผู้ส่งและสร้างความปลอดภัยในการรับส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์

ดังนั้นเพื่อเป็นการทดสอบแนวคิดนี้ว่าสามารถทำให้การส่งข้อมูลผ่านระบบอิเล็กทรอนิกส์ สามารถยืนยันตัวผู้ส่ง และมีความปลอดภัยของข้อมูลที่ส่งได้จริง ผู้ศึกษาจึงเห็นควรให้มีการพัฒนาระบบการสร้างลายมือชื่อดิจิทัลโดยใช้หลักการของการประมวลผลภาพ

1.2 วัตถุประสงค์ของการศึกษา

เพื่อพัฒนาซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัล โดยใช้หลักการประมวลผลภาพ

1.3 ประโยชน์ที่ได้รับจากการศึกษา

1. ได้ซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัล โดยใช้หลักการประมวลผลภาพ
2. สามารถนำไปประยุกต์ใช้กับการส่งจดหมายอิเล็กทรอนิกส์ การส่งข้อมูลโดยใช้สื่ออิเล็กทรอนิกส์อื่น เช่น ซีดี (CD) ยูเอสบี (USB) เป็นต้น การประยุกต์ใช้กับ อี-ออฟฟิศ (e-office) และ การทำธุรกรรมอิเล็กทรอนิกส์อื่นๆ

1.4 แผนการดำเนินงาน ขอบเขต และวิธีการศึกษา

1. แผนการดำเนินงาน

ขั้นตอนในการพัฒนาซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพ

1) ศึกษาหลักการสร้างและการทำงานของลายมือชื่อดิจิทัล
2) ศึกษาการประมวลผลภาพพร้อมทั้งการซ่อนข้อมูลในไฟล์ภาพ
3) ศึกษาการเข้ารหัสและการถอดรหัสเพื่อนำมาประยุกต์ใช้กับการสร้างลายมือชื่อดิจิทัล
4) วิเคราะห์และออกแบบระบบการสร้างลายมือดิจิทัลโดยใช้หลักการประมวลผลภาพ
5) ออกแบบขั้นตอนการทำงานของการสร้างลายมือดิจิทัลโดยใช้หลักการประมวลผลภาพ
6) ออกแบบหน้าจอการใช้งานของการสร้างลายมือดิจิทัลโดยใช้หลักการประมวลผลภาพ
7) เขียนโปรแกรมการสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพ
8) ทดสอบการใช้งานซอฟต์แวร์การสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพ

9) ตรวจสอบและปรับปรุงซอฟต์แวร์การสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพ
10) ทำแบบสอบถามความพึงพอใจผู้ใช้งานซอฟต์แวร์
11) จัดทำเอกสารประกอบการใช้งานซอฟต์แวร์การสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพ

2. ขอบเขต

การพัฒนาซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพจะใช้วิธีการซ่อนข้อมูลในไฟล์ภาพ (Steganography) สำหรับไฟล์ภาพที่ใช้จะเป็นไฟล์ภาพประเภท .bmp

ระบบการสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพประกอบด้วย

1) ส่วนของการล็อกอินเข้าสู่ระบบเพื่อความปลอดภัยในการใช้งานและเป็นการแยกข้อมูลของผู้ใช้แต่ละคนออกจากกัน
2) ส่วนของการสร้าง ไพรเวทคีย์ (Private Key) และ พับลิคคีย์ (Public Key) โดยคีย์ทั้งคู่จะเป็นไฟล์ภาพ
   (1) ไพรเวทคีย์ คือ คีย์ส่วนตัว โดยคีย์นี้ใช้ในกระบวนการสร้างลายมือชื่อดิจิทัลของผู้ใช้
   (2) พับลิคคีย์ คือ คีย์สาธารณะ โดยคีย์นี้ใช้สำหรับยืนยันตัวผู้ใช้และเป็นคีย์ในการถอดข้อมูลที่ซ่อนอยู่ในลายมือชื่อดิจิทัลของผู้ใช้ออกมา
3) ส่วนของการ อิมพอร์ต/เอกซ์พอร์ต (Import/Export) ไพรเวทคีย์ และพับลิคคีย์ ส่วนนี้ผู้ใช้สามารถทำการ เอกซ์พอร์ต ไพรเวทคีย์ และ พับลิคคีย์ เพื่อ อิมพอร์ตลงเครื่องอื่น
4) ส่วนของการ อิมพอร์ต/เอกซ์พอร์ต พับลิคคีย์ ของบุคคลอื่น ผู้ใช้สามารถทำการอิมพอร์ต/เอกซ์พอร์ต พับลิคคีย์ ของบุคคลอื่นได้
5) ส่วนของการสร้างลายมือชื่อดิจิทัล ผู้ใช้จะใช้ ไพรเวทคีย์ ในการสร้างลายมือชื่อดิจิทัลโดยลายมือชื่อดิจิทัลจะเป็นไฟล์ภาพและมีการซ่อนข้อมูลส่วนตัวของผู้ใช้และข้อมูลที่ผู้ใช้ต้องการส่งให้กับบุคคลอื่นไปด้วย
6) ส่วนของการตรวจสอบลายมือชื่อดิจิทัลและการถอดข้อมูลออกจากลายมือชื่อดิจิทัล เมื่อบุคคลอื่นส่งไฟล์ภาพที่เป็นลายมือชื่อดิจิทัลมาให้ ผู้ใช้ต้องใช้พับลิคคีย์ของบุคคลที่ส่งลายมือชื่อดิจิทัลมาให้นั้นในการยืนยันลายมือชื่อดิจิทัลและใช้ในการถอดข้อมูลที่ถูกส่งมาออกจากลายมือชื่อดิจิทัลดังกล่าว

7) ส่วนของการส่งอีเมล์ ผู้ใช้สามารถใช้ส่วนนี้ในการส่งอีเมล์พร้อมแนบไฟล์ พับลิคคีย์ รวมถึง ใช้ส่งอีเมล์พร้อมแนบไฟล์ที่เป็นลายมือชื่อดิจิทัล ไปให้บุคคลอื่นได้
8) แกลอรี่ภาพ สำหรับให้ผู้ใช้เลือกภาพที่จะใช้ในการสร้าง ไพรเวทคีย์ พับลิคคีย์ และลายมือชื่อดิจิทัล

3. วิธีการศึกษา

การเก็บรวบรวมข้อมูล

1) ศึกษาหลักการสร้างและการทำงานของลายมือชื่อดิจิทัลว่ามีการสร้างและทำงานอย่างไร โดยเริ่มต้นจากผู้ส่งจนกระทั่งถึงผู้รับ
2) ศึกษาการเข้ารหัสและการถอดรหัสเพื่อนำมาประยุกต์ใช้กับการสร้างลายมือชื่อดิจิทัล
3) ศึกษาการประมวลผลภาพพร้อมทั้งการซ่อนข้อมูลในไฟล์ภาพว่ามีวิธีใดบ้างเพื่อหาทางนำมาประยุกต์ใช้กับการสร้างลายมือชื่อดิจิทัล
4) วิเคราะห์และออกแบบระบบการสร้างลายมือดิจิทัลโดยใช้หลักการประมวลผลภาพว่าควรจะมีลำดับขั้นตอนและการทำงานอย่างไร
5) ออกแบบขั้นตอนการทำงานของการสร้างลายมือดิจิทัลโดยใช้หลักการประมวลผลภาพ
6) ออกแบบหน้าจอของการสร้างลายมือดิจิทัลโดยใช้หลักการประมวลผลภาพให้มีการใช้งานที่ง่ายและไม่ซับซ้อน
7) เขียนโปรแกรมสำหรับสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพ
8) ทดลองใช้งาน และประเมินระบบการสร้างลายมือดิจิทัลโดยใช้หลักการประมวล ผลภาพที่จัดทำขึ้น โดยกลุ่มผู้ที่ทดลองใช้งาน คือ เจ้าหน้าที่ของสถานบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่ เพื่อทำการปรับแต่งและแก้ไขข้อผิดพลาดในส่วนต่าง ๆ

1.5 สถานที่ใช้ในการดำเนินการศึกษาและรวบรวมข้อมูล

1. สถานบริการเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่
2. สำนักหอสมุด มหาวิทยาลัยเชียงใหม่
3. สาขาวิชาเทคโนโลยีสารสนเทศและการจัดการ บัณฑิตวิทยาลัย (โครงการพิเศษ) มหาวิทยาลัยเชียงใหม่

1.6 เครื่องมือที่ใช้ในการศึกษา

1. ฮาร์ดแวร์

เครื่องคอมพิวเตอร์ส่วนบุคคล เพื่อใช้ในการศึกษาและพัฒนาระบบมีคุณสมบัติดังนี้

1) หน่วยประมวลผลกลางแบบเพนเทียมโฟ ความเร็ว 3 กิกะเฮิร์ทซ์
2) หน่วยความจำขนาด 512 เมกะไบต์
3) ฮาร์ดดิสก์ ขนาดความจุ 80 กิกะไบต์

2. ซอฟต์แวร์

1) ระบบปฏิบัติการวินโดวส์เอ็กซ์พี
2) โปรแกรมไมโครซอฟท์วิชวลเบสิก 6.0 (Microsoft Visual Basic 6.0)

1.7 นิยามศัพท์

1. ลายมือชื่อดิจิทัล

คือ ไฟล์ภาพที่มีข้อมูลซึ่งประกอบด้วย รหัสผ่าน ข้อความและไฟล์ข้อมูล ที่ผู้ส่งต้องการส่งให้ผู้รับซ่อนอยู่

2. ไพรเวทคีย์ และ พับลิคคีย์

ไพรเวทคีย์ คือ คีย์ส่วนตัว เป็นไฟล์ภาพที่มีข้อมูลซึ่งประกอบด้วย รหัสผ่าน และชุดของตัวอักษรและตัวเลขซ่อนอยู่

พับลิคคีย์ คือ คีย์สาธารณะ เป็นไฟล์ภาพที่มีข้อมูลซึ่งประกอบด้วย รหัสผ่าน และชุดของตัวอักษรและตัวเลขซ่อนอยู่

โดยไพรเวทคีย์ และ พับลิคคีย์ จะมีความสัมพันธ์กันคือ ข้อมูลที่ซ่อนอยู่ในไฟล์ภาพไพรเวทคีย์จะเป็นรหัสผ่านของไฟล์ภาพพับลิคคีย์ ไพรเวทคีย์จะใช้ในกระบวนการสร้างลายมือชื่อดิจิทัลของผู้ส่ง และ พับลิคคีย์จะใช้ในกระบวนการถอดลายมือชื่อดิจิทัล ซึ่งจะเป็นกระบวนการทางฝั่งผู้รับในการตรวจสอบลายมือชื่อดิจิทัลว่าเป็นของผู้ส่งจริงและถอดข้อมูลที่ซ่อนอยู่ในไฟล์ภาพลายมือชื่อดิจิทัลออกมา