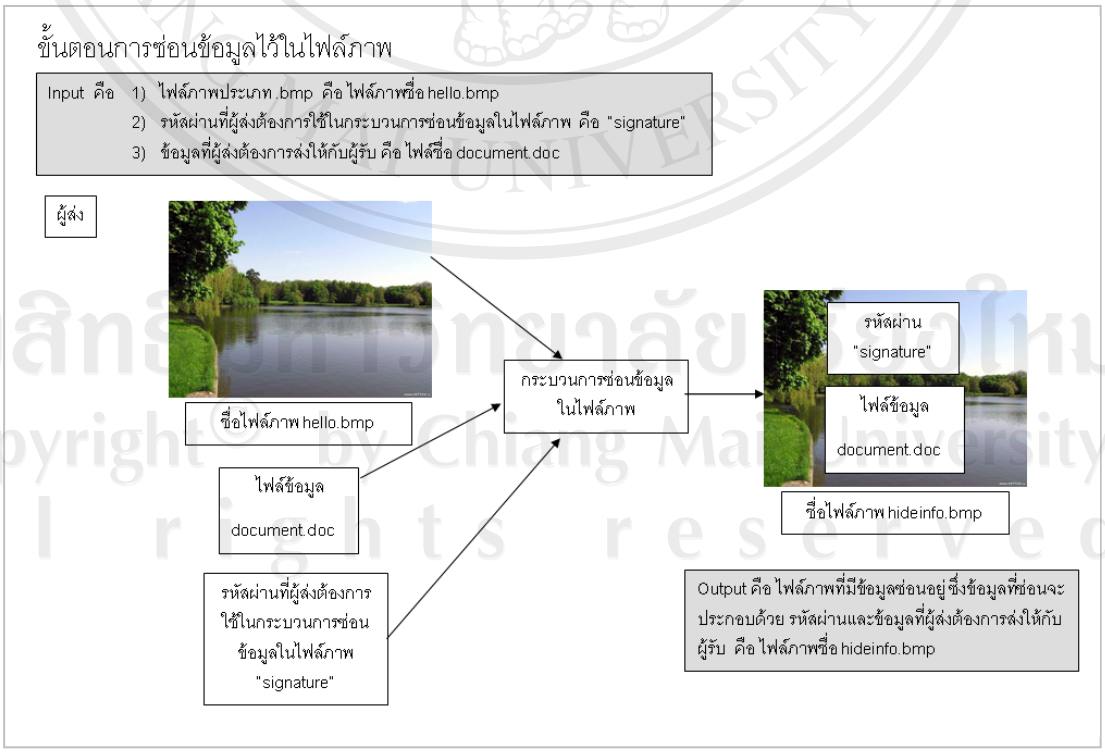
บทที่ 3
การวิเคราะห์และออกแบบระบบ

ซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัล โดยใช้หลักการประมวลผลภาพ เป็นซอฟต์แวร์แบบ Stand Alone (เครื่องเดียว) ที่ได้นำเอาระบบซ่อนข้อมูลในไฟล์ภาพมาประยุกต์ให้ใช้งานร่วมกับการสร้างลายมือชื่อดิจิทัล เพื่อใช้ในการยืนยันตัวตนของผู้ส่ง ในการส่งข้อมูลไปให้ผู้รับว่าข้อมูลนั้นถูกส่งมาจากผู้ส่งจริง พร้อมกับสร้างความปลอดภัยในการส่งข้อมูล โดยผู้รับเท่านั้นที่สามารถเห็นข้อมูลที่ถูกส่งมา

3.1 ขั้นตอนการทำงานระบบซ่อนข้อมูลในไฟล์ภาพ

ระบบซ่อนข้อมูลในไฟล์ภาพ เป็นระบบของการส่งข้อมูลที่เป็นความลับจากผู้ส่งไปให้ผู้รับโดยซ่อนข้อมูลที่ต้องการส่งไว้ในไฟล์ภาพ ซึ่งผู้ส่งกับผู้รับเท่านั้นที่สามารถเห็นข้อมูลที่ถูกซ่อนอยู่ในไฟล์ภาพ ขั้นตอนการทำงานจะแบ่งออกเป็น 2 ขั้นตอน ดังนี้

1. ขั้นตอนการซ่อนข้อมูลไว้ในไฟล์ภาพ เป็นขั้นตอนทางฝั่งผู้ส่ง

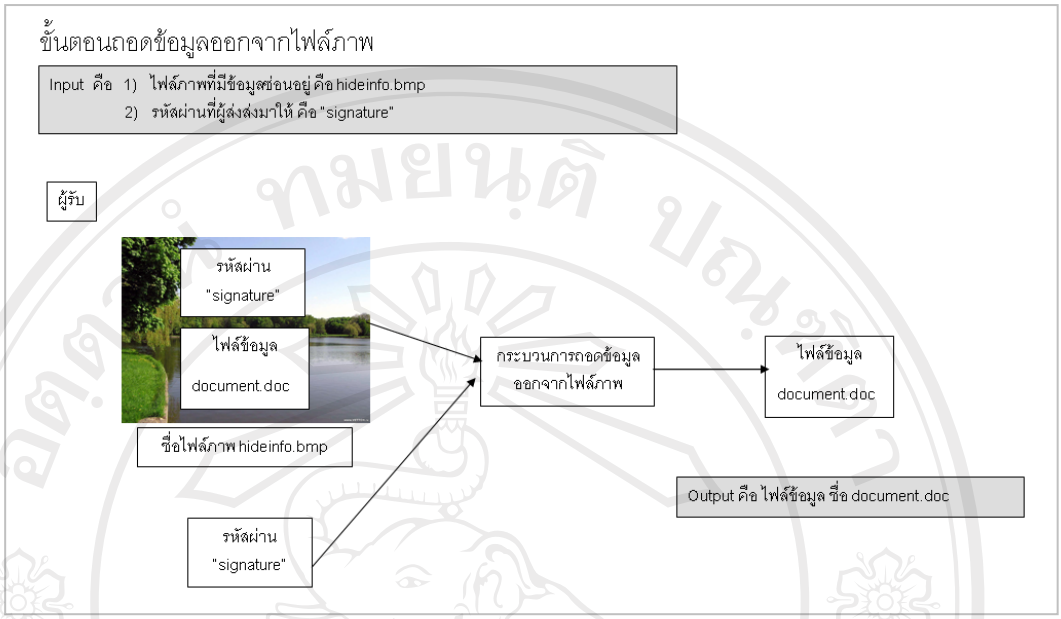


รูป 3.1 แสดงขั้นตอนการซ่อนข้อมูลไว้ในไฟล์ภาพ

จากรูป 3.1 อธิบายได้ดังนี้

1) Input ประกอบด้วย
   (1) ไฟล์ภาพประเภทไฟล์ .bmp จากรูป คือ ไฟล์ภาพชื่อ hello.bmp
   (2) รหัสผ่านที่ผู้ส่งต้องการใช้ในกระบวนการซ่อนข้อมูลในไฟล์ภาพ จากรูป คือ “signature”
   (3) ข้อมูลที่ผู้ส่งต้องการส่งให้กับผู้รับ จากรูป คือ ไฟล์ชื่อ document.doc
2) Output คือ ไฟล์ภาพที่มีข้อมูลซ่อนอยู่ ซึ่งข้อมูลที่ซ่อนจะประกอบด้วยรหัสผ่านและข้อมูลที่ผู้ส่งต้องการส่งให้กับผู้รับ จากรูป คือ ไฟล์ภาพชื่อ hideinfo.bmp
3) Process มีขั้นตอนดังนี้
   (1) ระบบจะรับข้อมูลไฟล์ภาพ คือไฟล์ภาพชื่อ hello.bmp รหัสผ่านที่ที่ผู้ส่งต้องการใช้ในกระบวนการซ่อนข้อมูลในไฟล์ภาพ คือ “signature” และข้อมูลที่ผู้ส่งต้องการส่งให้กับผู้รับ จากรูปคือ ไฟล์ชื่อ document.doc
   (2) นำเอารหัสผ่าน คือ “signature” และ ไฟล์ชื่อ document.doc มาซ่อนไว้ในไฟล์ภาพ โดยให้ทำการตั้งชื่อไฟล์ภาพที่มีข้อมูลซ่อนอยู่ จากรูปตั้งชื่อเป็น hideinfo.bmp
   (3) ผู้ส่งส่งไฟล์ภาพ hideinfo.bmp ไปให้กับผู้รับ โดยอาจส่ง รหัสผ่านคือ “signature” ไปให้กับผู้รับก่อนหรือหลังส่งไฟล์ภาพ hideinfo.bmp ซึ่งขึ้นอยู่กับการตกลงกับผู้รับ

2. ขั้นตอนการถอดข้อมูลออกจากไฟล์ภาพ เป็นขั้นตอนทางฝั่งผู้รับ



รูป 3.2 แสดงขั้นตอนการถอดข้อมูลออกจากไฟล์ภาพ

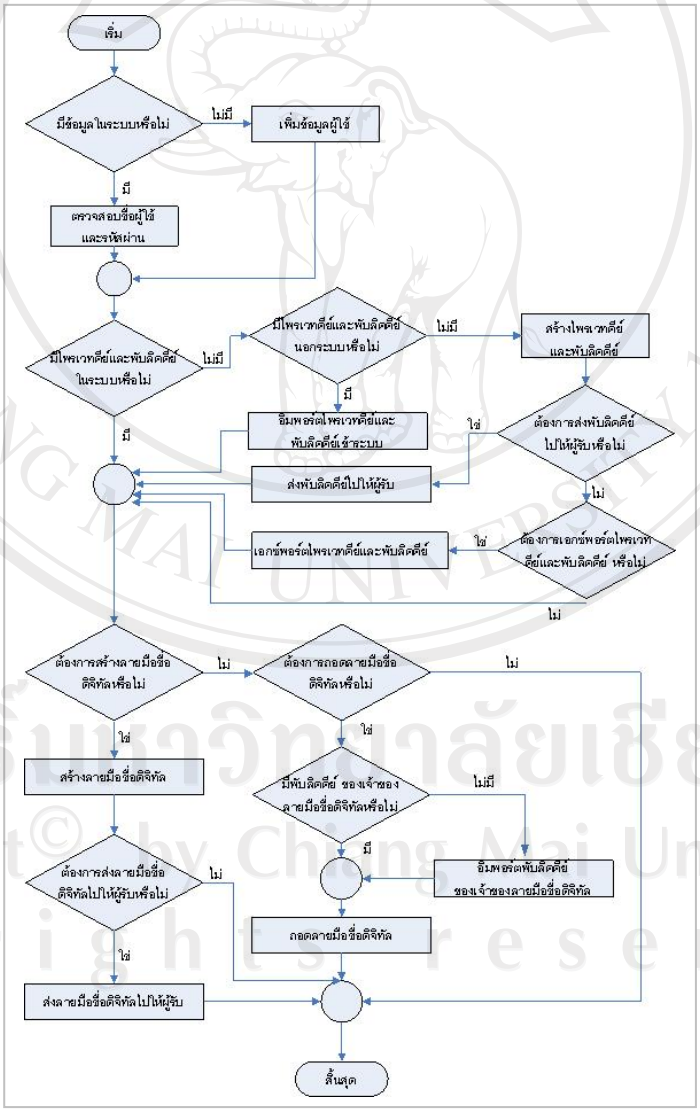
จากรูป 3.2 อธิบายได้ดังนี้

1) Input ประกอบด้วย
   (1) ไฟล์ภาพที่มีข้อมูลซ่อนอยู่ คือ hideinfo.bmp
   (2) รหัสผ่านที่ผู้ส่งส่งมาให้ คือ “signature”
2) Output คือ ไฟล์ข้อมูล ชื่อ document.doc
3) Process มีขั้นตอนดังนี้
   (1) ระบบจะรับข้อมูลไฟล์ภาพ คือไฟล์ภาพชื่อ hello.bmp รหัสผ่านที่ที่ผู้ส่งต้องการใช้ในกระบวนการซ่อนข้อมูลในไฟล์ภาพ คือ “signature” และข้อมูลที่ผู้ส่งต้องการส่งให้กับผู้รับจากรูปคือไฟล์ชื่อ document.doc
   (2) นำรหัสผ่านที่ผู้ส่งส่งมาให้คือ “signature” มาถอดข้อมูลออกจากไฟล์ภาพ ซึ่งจะได้ไฟล์ข้อมูล document.doc

จากระบบซ่อนข้อมูลในไฟล์ภาพข้างต้น เป็นการสร้างความปลอดภัยให้กับการส่งข้อมูลระหว่างผู้ส่งและผู้รับ ผู้ศึกษาได้นำเอาขั้นตอนของระบบนี้มาประยุกต์กับกระบวนการสร้างลายมือชื่อดิจิทัล เพื่อใช้ในการยืนยันตัวตนของผู้ส่ง ว่าข้อมูลที่ส่งเป็นของผู้ส่งจริง และ

สร้างความปลอดภัยให้กับข้อมูลที่ส่งมา ไม่ให้มีการแก้ไข หรือเปลี่ยนแปลงข้อมูลในระหว่างการส่ง ผู้ศึกษาได้นำเอาขั้นตอนการซ่อนข้อมูลในไฟล์ภาพมาใช้ในกระบวนการสร้างไพรเวทคีย์ พับลิคคีย์ และ ลายมือชื่อดิจิทัล ซึ่งจะได้ ไพรเวทคีย์ พับลิคคีย์ และ ลายมือชื่อดิจิทัลเป็นไฟล์ภาพที่มีข้อมูลซ่อนอยู่ โดยไพรเวทคีย์และพับลิคคีย์ จะมีความสัมพันธ์กัน ไพรเวทคีย์จะถูกใช้ในกระบวนการสร้างลายมือชื่อดิจิทัลซึ่งเป็นขั้นตอนทางฝั่งผู้ส่ง และพับลิคคีย์จะถูกใช้ในกระบวนการถอดลายมือชื่อ ดิจิทัล ซึ่งเป็นขั้นตอนทางฝั่งผู้ส่ง

3.2 รายละเอียดการทำงานของซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัล โดยใช้หลักการประมวลผลภาพ



รูป 3.3 แสดงรายละเอียดการทำงานของซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัล โดยใช้หลักการประมวลผลภาพ

จากรูป 3.3 แสดงรายละเอียดการทำงานของซอฟต์แวร์ อธิบายได้ดังนี้

1) การตรวจสอบข้อมูลผู้ใช้ของระบบ กรณีที่ผู้ใช้ยังไม่มีข้อมูลในระบบ สามารถเพิ่มข้อมูลผู้ใช้ในระบบ แต่ถ้าผู้ใช้มีข้อมูลในระบบอยู่แล้ว สามารถทำการล็อกอินเข้าระบบ โดยระบบจะทำการตรวจสอบข้อมูลที่ผู้ใช้กรอกเข้ามาว่าถูกต้องหรือไม่ ถ้าถูกต้องจะสามารถเข้าไปใช้งานในระบบ

2) การสร้างไพรเวทคีย์และพับลิคคีย์ ในกรณีที่ผู้ใช้ระบบยังไม่มีไพรเวทคีย์และพับลิคคีย์ ในระบบ สามารถทำการสร้างไพรเวทคีย์และพับลิคคีย์ ไว้ในระบบได้ และผู้ใช้สามารถเลือกส่งพับลิคคีย์ของตนเองให้กับบุคคลอื่น โดยการส่งอีเมล์ผ่านระบบโดยตรง หรือเลือกทำการเอกซ์พอร์ต (Export) พับลิคคีย์ เพื่อที่จะส่งให้กับบุคคลอื่นภายหลัง ในกรณีที่ผู้ใช้มีไพรเวทคีย์และพับลิคคีย์ อยู่ภายนอกระบบ ผู้ใช้สามารถทำการอิมพอร์ต (Import) ไพรเวทคีย์และพับลิคคีย์เข้าสู่ระบบได้

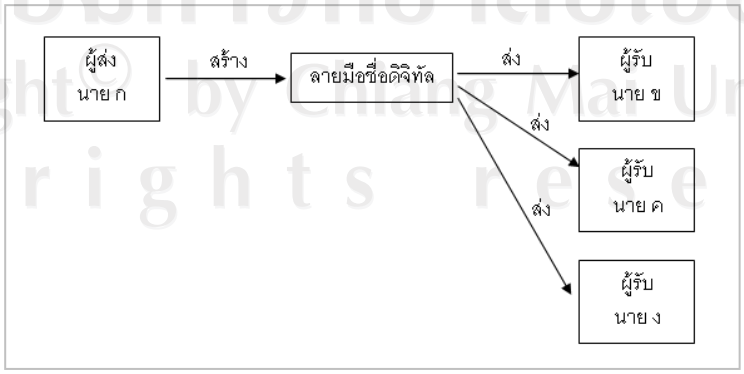
3) การสร้างลายมือชื่อดิจิทัล เป็นขั้นตอนทางฝั่งผู้ส่ง ผู้ส่งสามารถทำการสร้างลายมือชื่อดิจิทัล และส่งลายมือชื่อดิจิทัลให้กับผู้รับโดยสามารถส่งอีเมล์ผ่านระบบโดยตรง

4) การถอดลายมือชื่อดิจิทัล เป็นขั้นตอนทางฝั่งผู้รับ ผู้รับจะต้องมีพับลิคคีย์ของผู้ที่ส่งลายมือชื่อดิจิทัลมาให้ โดยถ้าผู้รับยังไม่ได้นำพับลิคคีย์ของผู้ที่ส่งลายมือชื่อดิจิทัลมาให้เข้าระบบ ผู้รับสามารถทำการอิมพอร์ตพับลิคคีย์ดังกล่าวเข้าสู่ระบบได้ จากนั้นผู้รับจะสามารถทำการถอดลายมือชื่อดิจิทัลได้โดยใช้พับลิคคีย์ของผู้ส่งในการถอด

3.3 ส่วนของการออกแบบระบบ

3.3.1 การออกแบบระบบ

ซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัล โดยใช้หลักการประมวลผลภาพ ผู้ศึกษาได้แบ่งการสร้างลายมือชื่อดิจิทัล ออกเป็น 2 แบบ แสดงดังรูป



รูป 3.4 แสดงการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน

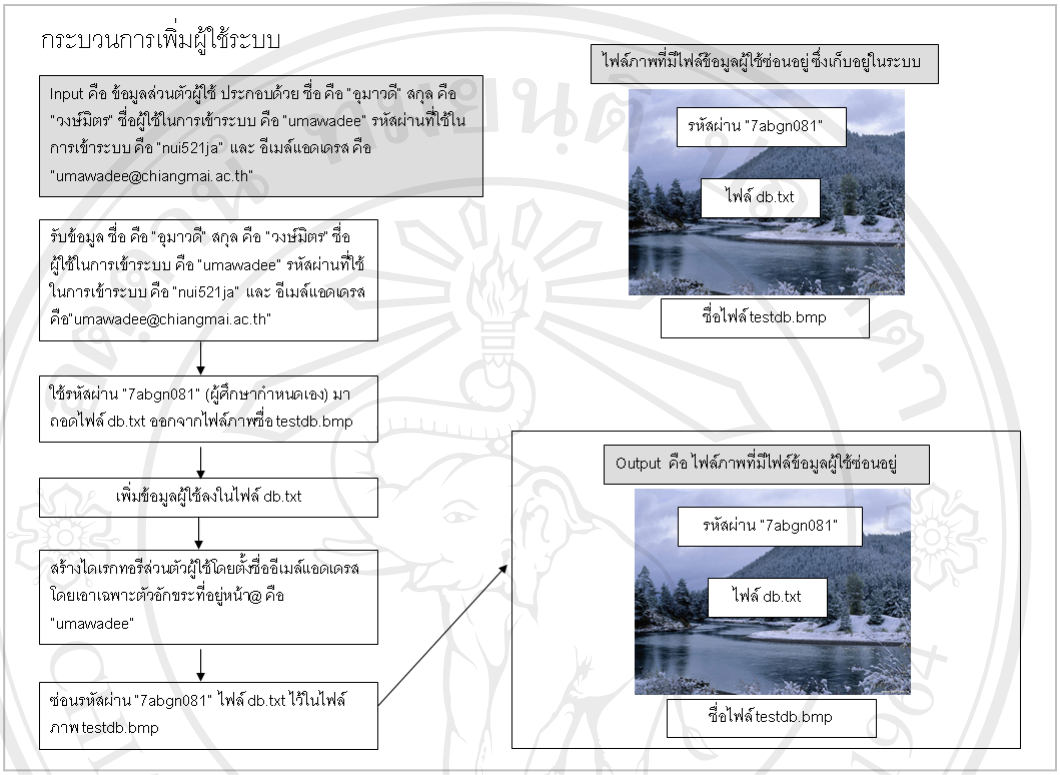
จากรูป 3.4 แสดงการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน เป็นการสร้างลายมือชื่อดิจิทัลเพื่อส่งให้กับผู้รับที่มีพับลิคคีย์ของผู้ส่ง ตั้งแต่ 1 คนขึ้นไป โดยในขั้นตอนการถอดลายมือชื่อดิจิทัลแบบนี้จะใช้เพียงพับลิคคีย์ของผู้ส่งในการถอด ตัวอย่างเช่น นาย ก ส่งลายมือชื่อดิจิทัล ให้กับ นาย ข นาย ค และ นาย ง ซึ่งนาย ข นาย ค และ นาย ง ต้องใช้พับลิคคีย์ของนาย ก ในการถอดลายมือชื่อดิจิทัลซึ่งเป็นกระบวนการในการยืนยันตัวตนของนาย ก ว่าข้อมูลที่ส่งมานั้นเป็นของ นาย ก จริง และสามารถดูข้อมูลที่ถูกส่งมาได้

รูป 3.5 แสดงการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว

จากรูป 3.5 แสดงการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว เป็นการสร้างลายมือชื่อดิจิทัลเพื่อส่งให้กับผู้รับที่มีพับลิคคีย์ของผู้ส่งเพียงคนเดียว โดยในขั้นตอนการถอดลายมือชื่อดิจิทัลแบบนี้จะใช้พับลิคคีย์ของผู้ส่ง และรหัสผ่านที่ผู้รับใช้ในการสร้างไพรเวทคีย์และพับลิคคีย์ของตนเองในการถอดลายมือชื่อดิจิทัล ตัวอย่างเช่น นาย ก ส่งลายมือชื่อให้กับ นาย ข ซึ่งนาย ข ต้องใช้พับลิคคีย์ของนาย ก และ รหัสผ่านที่นาย ข ใช้ในการสร้างไพรเวทคีย์และพับลิคคีย์ของนาย ข เอง ในการถอดลายมือชื่อดิจิทัลซึ่งเป็นกระบวนการในการยืนยันตัวตนของนาย ก ว่าข้อมูลที่ส่งมานั้นเป็นของ นาย ก จริง และ นาย ข เท่านั้นที่สามารถดูข้อมูลที่ถูกส่งมาได้

การออกแบบกระบวนการในระบบได้แบ่งออกเป็น 5 ส่วน ดังนี้

1. กระบวนการตรวจสอบผู้ใช้และเพิ่มผู้ใช้ในระบบ



รูป 3.6 แสดงขั้นตอนการทำงานของการเพิ่มผู้ใช้ในระบบ

จากรูป 3.6 อธิบายได้ดังนี้

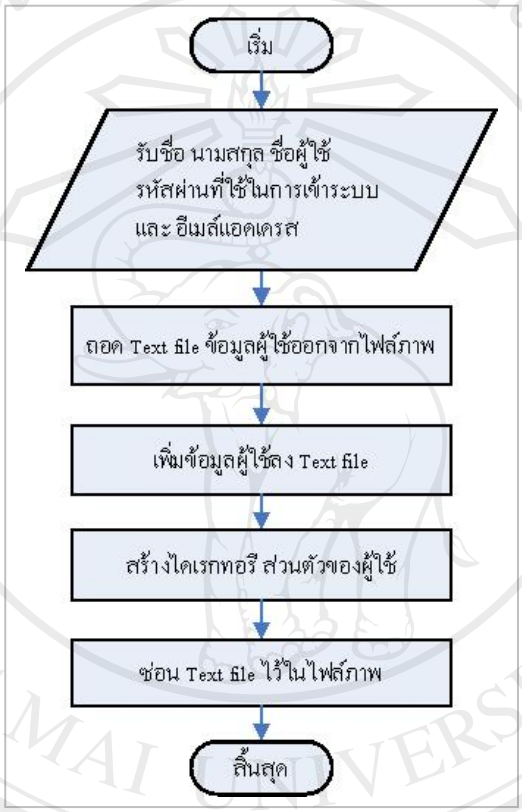
1) Input คือ ข้อมูลส่วนตัวผู้ใช้ ประกอบด้วย ชื่อ คือ “อุมาวดี” สกุล คือ “วงษ์มิตร” ชื่อผู้ใช้ในการเข้าระบบ คือ “umawadee” รหัสผ่านที่ใช้ในการเข้าระบบ คือ “nui521ja” และ อีเมล์แอดเดรส คือ “umawadee@chiangmai.ac.th”
2) Output คือ ไฟล์ภาพ ชื่อ testdb.bmp ซึ่งมีรหัสผ่าน “7abgn081” และ ไฟล์ข้อมูลผู้ใช้ ชื่อ db.txt ซ่อนอยู่
3) Process มีขั้นตอนดังนี้
   (1) รับข้อมูล ชื่อ คือ “อุมาวดี” สกุล คือ “วงษ์มิตร” ชื่อผู้ใช้ในการเข้าระบบคือ “umawadee” รหัสผ่านที่ใช้ในการเข้าระบบ คือ “nui521ja” และ อีเมล์แอดเดรส คือ “umawadee@chiangmai.ac.th”
   (2) ใช้รหัสผ่าน “7abgn081 ”(ผู้ศึกษากำหนดเอง) มาถอดไฟล์ db.txt

ออกจากไฟล์ภาพชื่อ testdb.bmp

(3) เพิ่มข้อมูลผู้ใช้ลงในไฟล์ db.txt

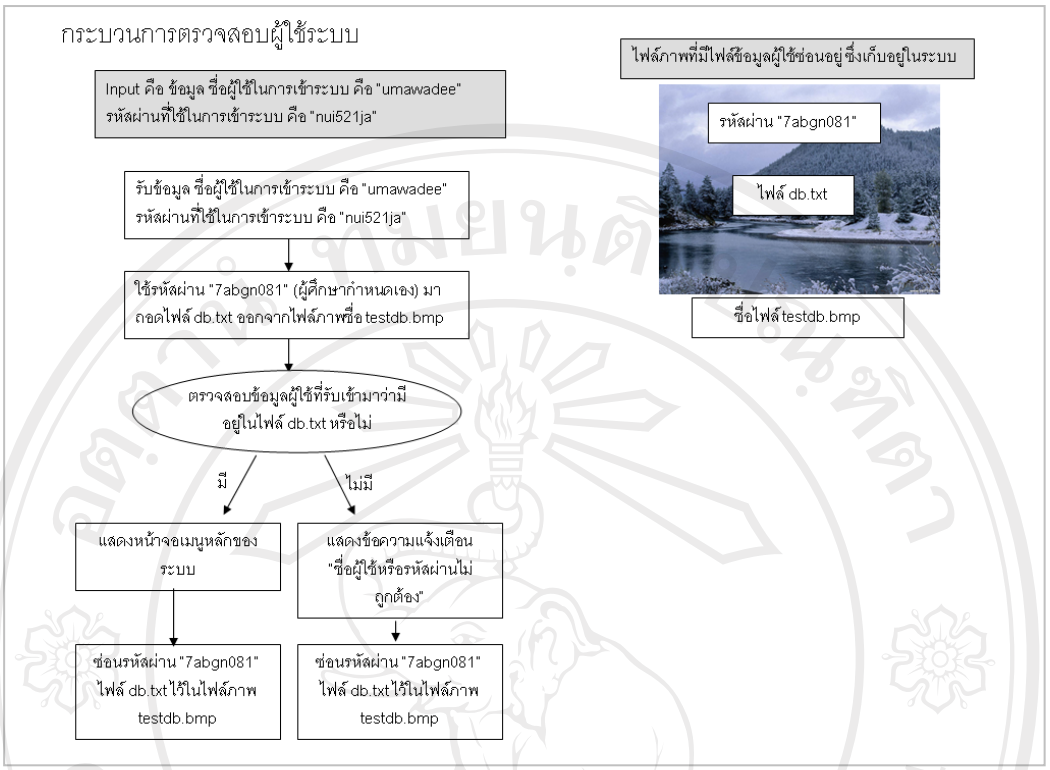
(4) สร้างไดเรกทอรีส่วนตัวผู้ใช้โดยตั้งชื่ออีเมล์แอดเดรส โดยเอาเฉพาะตัวอักขระที่อยู่หน้า@ คือ “umawadee”

(5) ซ่อนรหัสผ่าน “7abgn081 ”ไฟล์ db.txt ไว้ในไฟล์ภาพ testdb.bmp



รูป 3.7 แสดงรายละเอียดการทำงานของการเพิ่มผู้ใช้ในระบบ

จากรูป 3.7 เป็นกระบวนการเพิ่มผู้ใช้ในระบบ สำหรับการเพิ่มผู้ใช้ในระบบจะมีการเก็บข้อมูลของผู้ใช้ คือ ชื่อ นามสกุล ชื่อผู้ใช้ (username) รหัสผ่านที่ใช้ในการเข้าระบบ (password) และ อีเมล์แอดเดรส โดยระบบจะเก็บข้อมูลผู้ใช้ไว้ใน Text file ซึ่ง Text file ดังกล่าวจะถูกซ่อนอยู่ในไฟล์ภาพ โดยขั้นตอนการเก็บข้อมูลผู้ใช้ไว้ใน Text file เริ่มจาก ระบบจะใช้รหัสผ่านที่ผู้ศึกษากำหนดไว้ในระบบ ทำการถอด Text file ออกจากไฟล์ภาพ จากนั้นระบบจะทำการบันทึกข้อมูลผู้ใช้ลง Text file พร้อมทั้งสร้างไดเรกทอรี (Directory) ส่วนตัวของผู้ใช้ เมื่อบันทึกข้อมูลผู้ใช้เสร็จ ระบบจะทำการซ่อน Text file ไว้ในรูปภาพเช่นเดิม

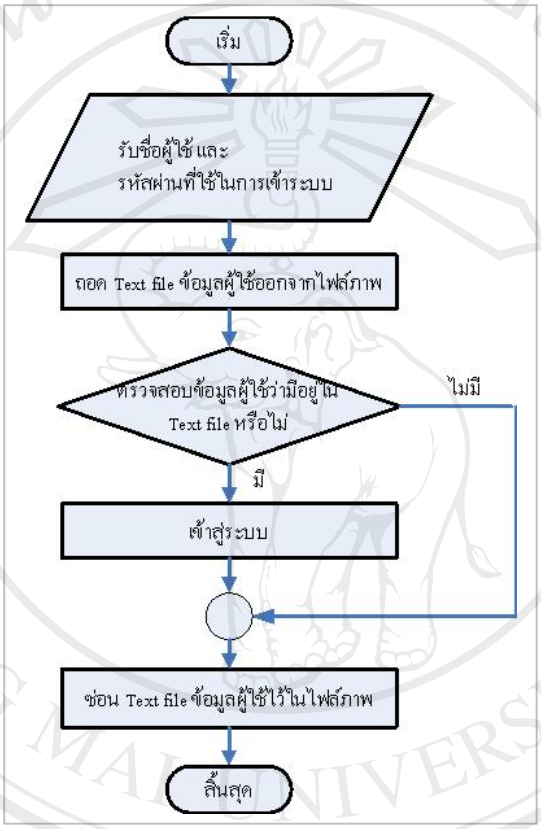


รูป 3.8 แสดงขั้นตอนการทำงานของการตรวจสอบผู้ใช้ในระบบ

จากรูป 3.8 อธิบายได้ดังนี้

1) Input คือ ข้อมูลส่วนตัวผู้ใช้ ประกอบด้วย ชื่อ คือ “อุมาวดี” สกุล คือ “วงษ์มิตร” ชื่อผู้ใช้ในการเข้าระบบ คือ “umawadee” รหัสผ่านที่ใช้ในการเข้าระบบ คือ “nui521ja” และ อีเมล์แอดเดรส คือ “umawadee@chiangmai.ac.th”
2) Output คือ ไฟล์ภาพ ชื่อ testdb.bmp ซึ่งมีรหัสผ่าน “7abgn081” และไฟล์ข้อมูลผู้ใช้ ชื่อ db.txt ซ่อนอยู่
3) Process มีขั้นตอนดังนี้
   (1) รับข้อมูล ชื่อผู้ใช้ในการเข้าระบบ คือ “umawadee” รหัสผ่านที่ใช้ในการเข้าระบบ คือ “nui521ja”
   (2) ใช้รหัสผ่าน “7abgn081 ” (ผู้ศึกษากำหนดเอง) มาถอดไฟล์ db.txt ออกจากไฟล์ภาพชื่อ testdb.bmp

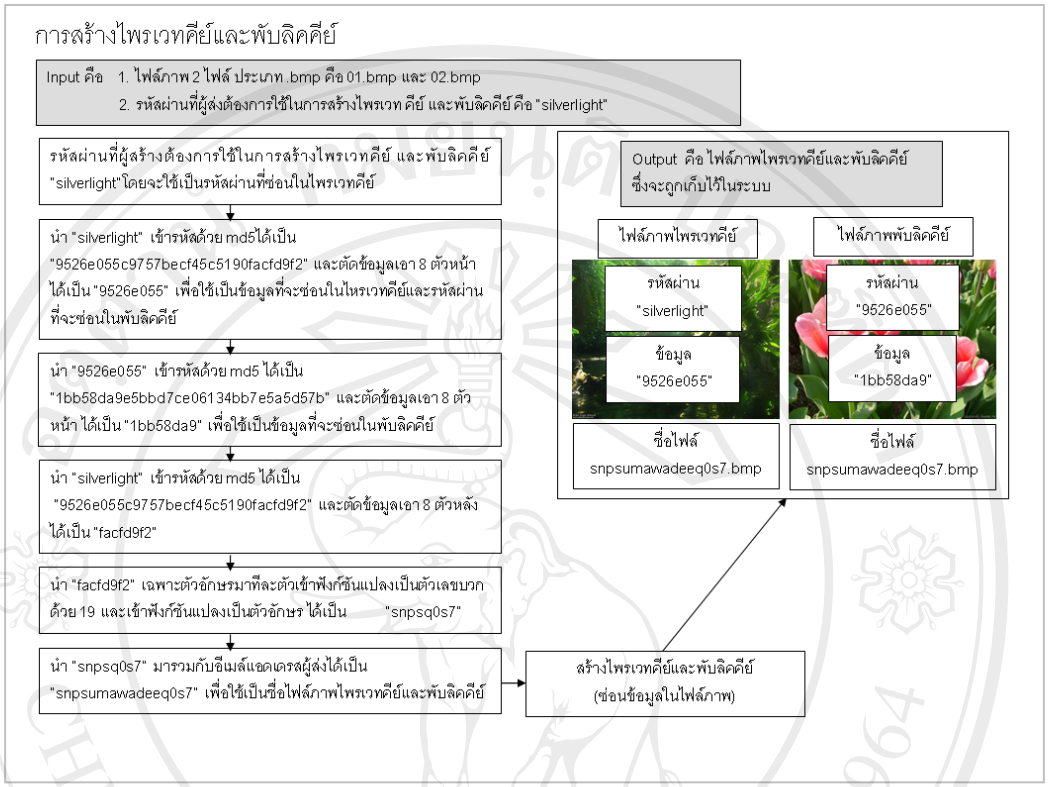
(3) ตรวจสอบข้อมูลผู้ใช้ที่รับเข้ามาว่ามีอยู่ในไฟล์ db.txt หรือไม่ ถ้ามี แสดงหน้าจอเมนูหลักของระบบและซ่อนรหัสผ่าน “7abgn081” ไฟล์ db.txtไว้ในไฟล์ภาพ testdb.bmp ถ้าไม่มี แสดงข้อความแจ้งเตือน “ชื่อผู้ใช้หรือรหัสผ่านไม่ถูกต้อง” และซ่อนรหัสผ่าน “7abgn081 ” ไฟล์ db.txt ไว้ในไฟล์ภาพ testdb.bmp



รูป 3.9 แสดงรายละเอียดการทำงานของการตรวจสอบผู้ใช้ในระบบ

จากรูป 3.9 แสดงรายละเอียดการทำงานของกระบวนการตรวจสอบข้อมูลของผู้ใช้ในระบบในกรณีที่ผู้ใช้มีข้อมูลอยู่ในระบบแล้ว ระบบจะทำการถอด Text file ออกจากไฟล์ภาพเพื่อทำการตรวจสอบข้อมูลผู้ใช้ ที่ผู้ใช้ได้ทำการกรอกเข้ามาว่ามีอยู่ในระบบหรือไม่ ถ้ามี ผู้ใช้จะสามารถเข้าสู่ระบบได้ และ ระบบจะทำการซ่อน Text file ไว้ในรูปภาพเช่นเดิม แต่ถ้าไม่มีระบบจะทำการซ่อน Text file ไว้ในรูปภาพเช่นเดิม

2. กระบวนการสร้างไพรเวทคีย์และพับลิคคีย์



รูป 3.10 แสดงขั้นตอนการทำงานของการสร้างไพรเวทคีย์และพับลิคคีย์

จากรูป 3.10 อธิบายได้ดังนี้

1) Input คือ

(1) ไฟล์ภาพ 2 ไฟล์ ประเภท .bmp คือ 01.bmp และ 02.bmp

(2) รหัสผ่านที่ผู้ส่งต้องการใช้ในการสร้างไพรเวทคีย์และพับลิคคีย์ คือ “silverlight”

2) Output คือไฟล์ภาพไพรเวทคีย์ที่มีข้อมูลซ่อนอยู่ ซึ่งข้อมูลที่ซ่อนจะประกอบด้วยรหัสผ่าน คือ “silverlight” และข้อมูล คือ “9526e055” และไฟล์ภาพพับลิคคีย์ที่มีข้อมูลซ่อนอยู่ ซึ่งข้อมูลที่ซ่อนจะประกอบด้วยรหัสผ่าน คือ “9526e055” และ ข้อมูล คือ “1bb58da9”

3) Process มีขั้นตอนดังนี้

(1) รหัสผ่านที่ผู้สร้างต้องการใช้ในการสร้างไพรเวทคีย์และพับลิคคีย์ “silverlight”โดยจะใช้เป็นรหัสผ่านที่ซ่อนในไพรเวทคีย์

(2) นำ “silverlight” เข้ารหัสด้วย md5ได้เป็น “9526e055c9757becf45c5190facfd9f2” และตัดข้อมูลเอา 8 ตัวหน้าได้เป็น “9526e055” เพื่อใช้เป็นข้อมูลที่จะซ่อนในไพรเวทคีย์และรหัสผ่านที่จะซ่อนในพับลิคคีย์

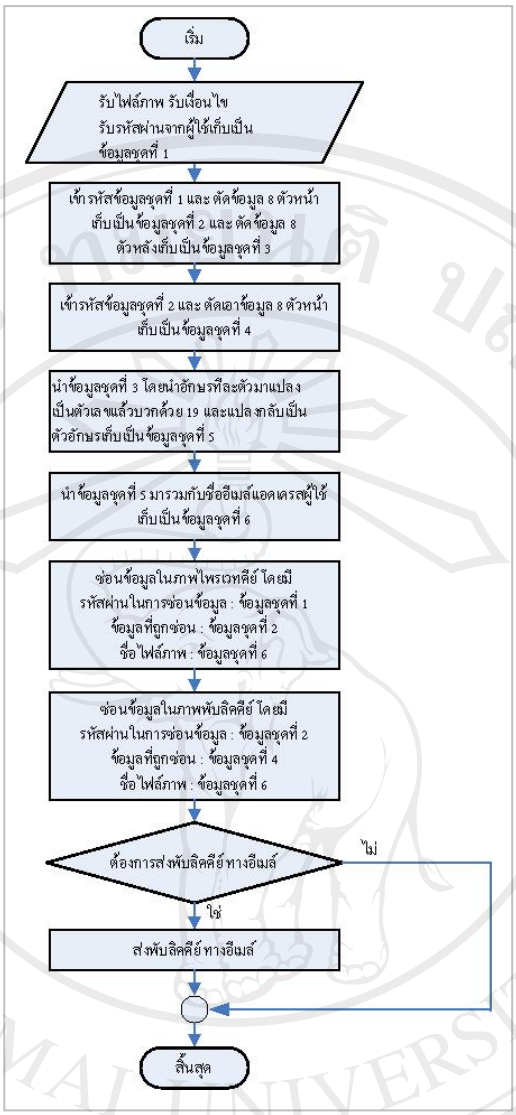
(3) นำ “9526e055” เข้ารหัสด้วย md5 ได้เป็น “1bb58da9e5bbd7ce06134bb7e5a5d57b” และตัดข้อมูลเอา 8 ตัวหน้า ได้เป็น “1bb58da9” เพื่อใช้เป็นข้อมูลที่จะซ่อนในพับลิคคีย์

(4) นำ “silverlight” เข้ารหัสด้วย md5 ได้เป็น “9526e055c9757becf45c5190facfd9f2” และตัดข้อมูลเอา 8 ตัวหลังได้เป็น “facfd9f2”

(5) นำ “facfd9f2” เฉพาะตัวอักษรมาทีละตัวเข้าฟังก์ชันแปลงเป็นตัวเลขบวกด้วย 19 และเข้าฟังก์ชันแปลงเป็นตัวอักษร ได้เป็น “snpsq0s7”

(6) นำ “snpsq0s7” มารวมกับอีเมล์แอดเดรสผู้ส่งได้เป็น “snpsumawadeeq0s7” เพื่อใช้เป็นชื่อไฟล์ภาพไพรเวทคีย์และพับลิคคีย์

(7) สร้างไพรเวทคีย์และพับลิคคีย์ (ซ่อนข้อมูลในไฟล์ภาพ)

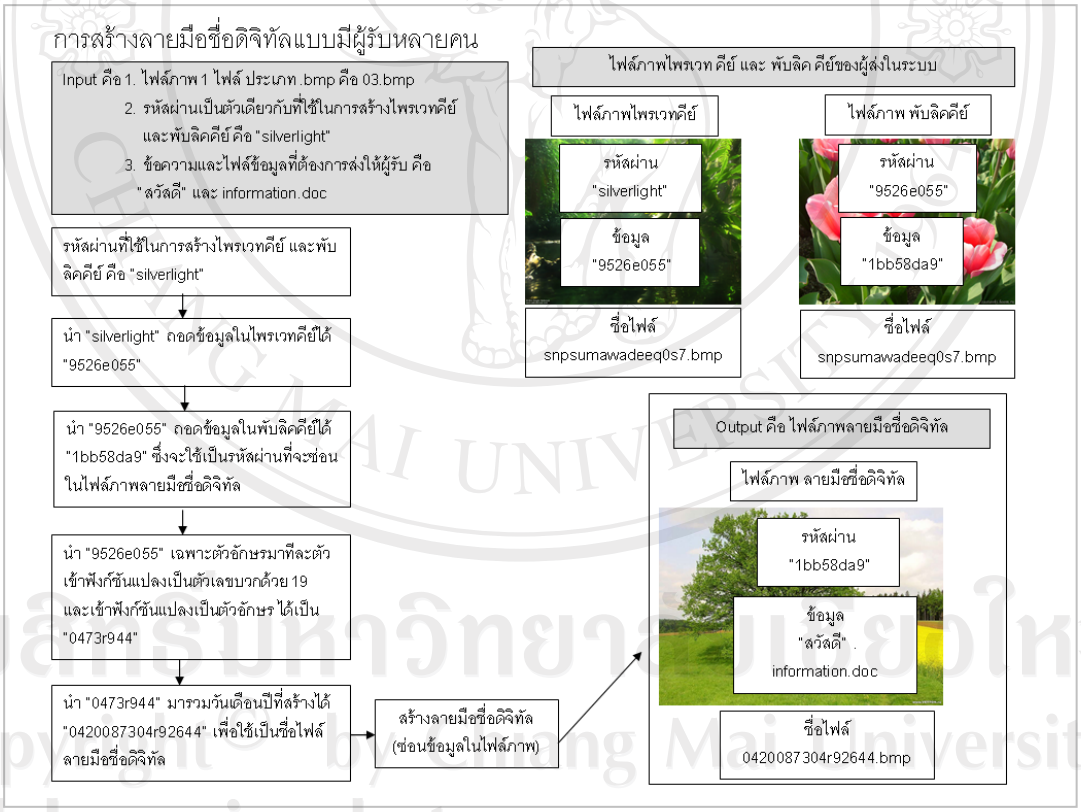


รูป 3.11 แสดงรายละเอียดการทำงานของการสร้างไพรเวทคีย์และพับลิคคีย์

จากรูป 3.11 แสดงรายละเอียดการทำงานของการสร้างไพรเวทคีย์ ที่ใช้ในการสร้างลายมือชื่อดิจิทัล และ การสร้างพับลิคคีย์ที่ใช้ในการถอดลายมือชื่อดิจิทัล โดยกระบวนการในการสร้างคีย์ทั้งสอง ระบบจะรับข้อมูลการเลือกไฟล์ภาพประเภท .bmp ที่ผู้ใช้เลือกไฟล์ภาพจากภายนอก หรือเลือกจากแกลอรี่ภาพของระบบ รับรหัสผ่านที่ผู้ใช้กรอกเข้ามาเพื่อใช้ในกระบวนการสร้างคีย์ทั้งคู่รับเงื่อนไขจากผู้ใช้ว่าต้องการสร้างไพรเวทคีย์และพับลิคคีย์ เพื่อเก็บไว้ในระบบ หรือสร้างแล้วให้ส่งพับลิคคีย์ ไปให้ผู้รับทางอีเมล์ จากนั้นระบบจะนำเอารหัสผ่านที่ผู้ใช้กรอกมาเก็บไว้เป็นข้อมูลชุดที่หนึ่ง และนำมาเข้ารหัสแบบทางเดียว (One-Way Encryption) คือ md5 พร้อมทั้งตัดเอาข้อมูล 8 ตัวหน้า เก็บไว้เป็นข้อมูลชุดที่สองและตัดเอา

ข้อมูล 8 ตัวหลังเก็บไว้เป็นข้อมูลชุดที่สาม จากนั้นนำข้อมูลชุดที่สองมาเข้ารหัสแบบทางเดียว และตัดเอาข้อมูล 8 ตัวหน้าเก็บไว้เป็นข้อมูลชุดที่สี่ จากนั้นระบบจะนำข้อมูลชุดที่สามโดยเอาตัวอักษรแต่ละตัวในข้อมูลชุดนี้มาเข้าฟังก์ชันแปลงเป็นตัวเลขแล้วบวกกับค่าคงที่คือ 19 และแปลงตัวเลขให้กลับเป็นตัวอักษรเก็บเป็นข้อมูลชุดที่ห้า และนำข้อมูลชุดที่ห้ามาต่อกับชื่ออีเมล์แอดเดรสของผู้ใช้ จะได้เป็นข้อมูลชุดที่หก จากนั้นระบบจะทำการซ่อนข้อมูลชุดที่สองไว้ในไพรเวทคีย์ โดยมีข้อมูลชุดที่หนึ่งเป็นรหัสผ่านในการซ่อนข้อมูลดังกล่าวไว้ในไพรเวทคีย์ และทำการซ่อนข้อมูลชุดที่สี่ไว้ในพับลิคคีย์ โดยมีข้อมูลชุดที่สองเป็นรหัสผ่านในการซ่อนข้อมูลดังกล่าวในพับลิคคีย์ และใช้ข้อมูลชุดที่หก สำหรับการตั้งชื่อไฟล์ภาพไพรเวทคีย์และพับลิคคีย์ และในกรณีที่มีการระบุเงื่อนไขจากผู้ใช้ว่า ต้องการส่งพับลิคคีย์ ไปให้ผู้รับผ่านทางอีเมล์ ระบบจะทำการส่งพับลิคคีย์ไปให้ผู้รับทางอีเมล์

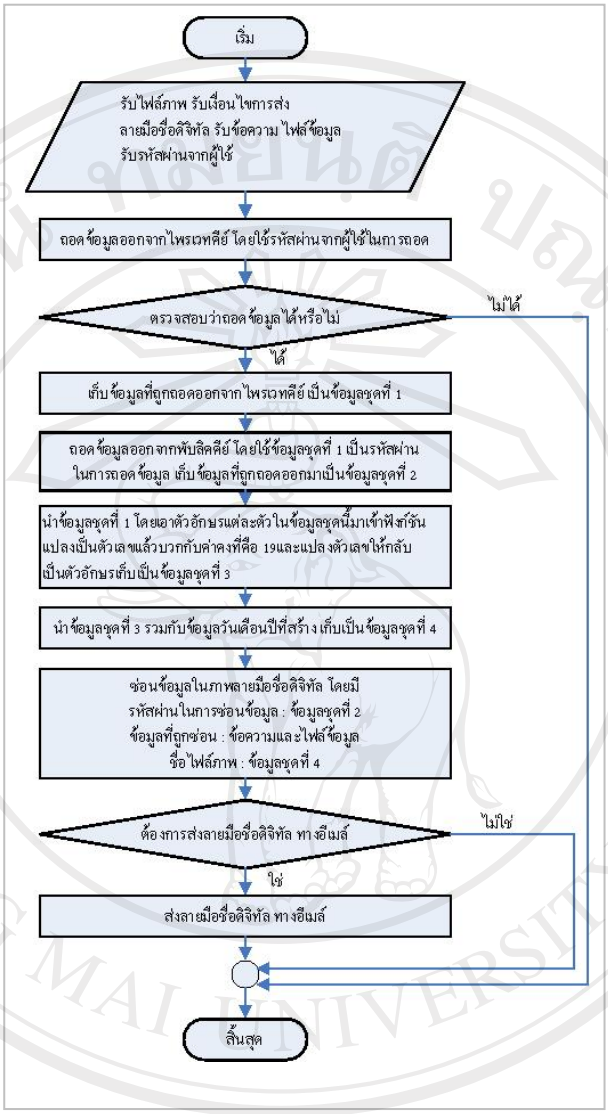
3. กระบวนการสร้างลายมือชื่อดิจิทัล เป็นขั้นตอนทางฝั่งผู้ส่ง



รูป 3.12 แสดงขั้นตอนการทำงานของการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน

จากรูป 3.12 อธิบายได้ดังนี้

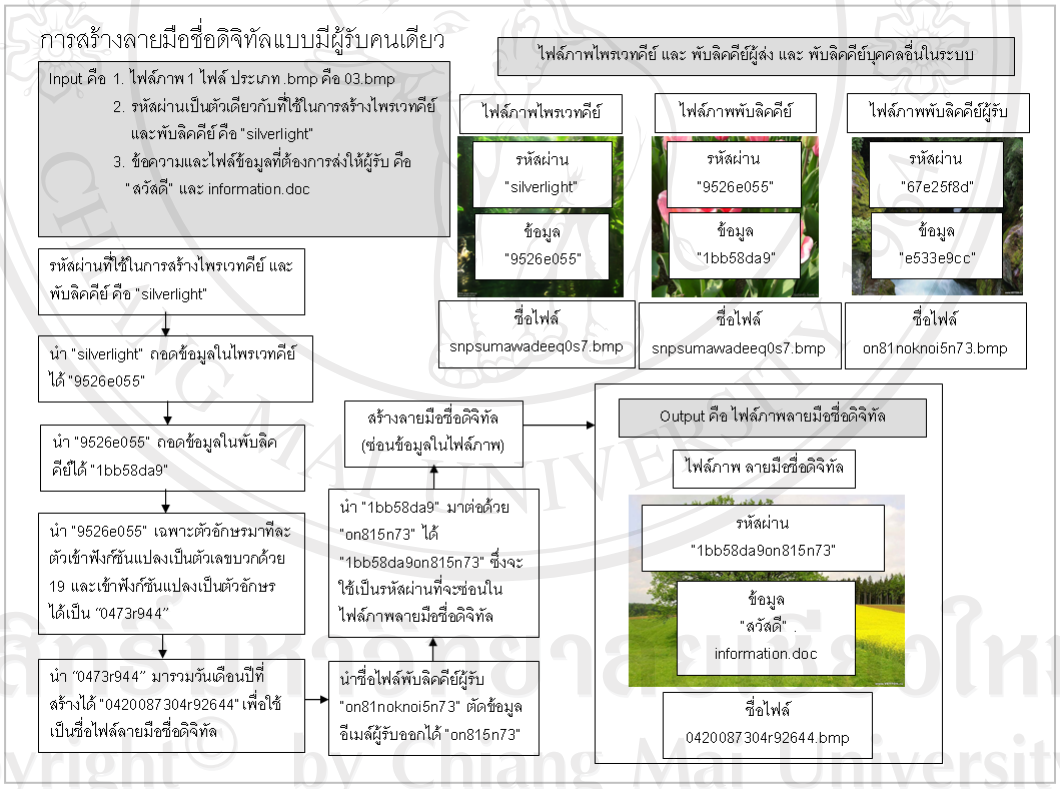
1) Input คือ
   (1) ไฟล์ภาพ 1 ไฟล์ ประเภท .bmp คือ 03.bmp
   (2) รหัสผ่านที่ผู้ส่งต้องการใช้ในการสร้างไพรเวทคีย์และพับลิคคีย์ คือ “silverlight”
   (3) ข้อความและไฟล์ข้อมูลที่ต้องการส่งให้ผู้รับ คือ “สวัสดี” และ information.doc
2) Output คือ ไฟล์ภาพลายมือชื่อดิจิทัลที่มีข้อมูลซ่อนอยู่ ซึ่งข้อมูลที่ซ่อนจะประกอบด้วย รหัสผ่าน คือ “1bb58da9” และข้อมูล คือ “สวัสดี” และไฟล์ information.doc
3) Process มีขั้นตอนดังนี้
   (1) รหัสผ่านที่ใช้ในการสร้างไพรเวทคีย์ และพับลิคคีย์ คือ “silverlight”
   (2) นำ “silverlight” ถอดข้อมูลในไพรเวทคีย์ได้ “9526e055”
   (3) นำ “9526e055” ถอดข้อมูลในพับลิคคีย์ได้ “1bb58da9” ซึ่งจะใช้เป็นรหัสผ่านที่จะซ่อนในไฟล์ภาพลายมือชื่อดิจิทัล
   (4) นำ “9526e055” เฉพาะตัวอักษรมาทีละตัวเข้าฟังก์ชันแปลงเป็นตัวเลขบวกด้วย 19 และเข้าฟังก์ชันแปลงเป็นตัวอักษร ได้เป็น “0473r944”
   (5) นำ “0473r944” มารวมวันเดือนปีที่สร้างได้ “0420087304r92644” เพื่อใช้เป็นชื่อไฟล์ลายมือชื่อดิจิทัล
   (6) สร้างลายมือชื่อดิจิทัล (ซ่อนข้อมูลในไฟล์ภาพ)



รูป 3.13 แสดงรายละเอียดการทำงานของการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน

จากรูป 3.13 แสดงรายละเอียดการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน ระบบจะรับข้อมูลไฟล์ภาพประเภท .bmp ที่ผู้ใช้เลือกจากภายนอกระบบ หรือเลือกจากแกลอรี่ภาพของระบบ รับข้อความและไฟล์ข้อมูลที่ผู้ใช้ต้องการที่จะซ่อนไว้ในลายมือชื่อดิจิทัล และรหัสผ่านซึ่งจะต้องเป็นตัวเดียวกับที่ใช้สร้างไพรเวทคีย์และพับลิคคีย์ พร้อมทั้งเงื่อนไขจากผู้ใช้ว่าต้องการสร้างลายมือชื่อดิจิทัล เพื่อเก็บไว้ในระบบ หรือสร้างแล้วให้ส่งลายมือชื่อดิจิทัล ไปให้ผู้รับทางอีเมล์ด้วย จากนั้นระบบจะนำรหัสผ่านที่ผู้ใช้กรอกเข้ามาเป็นรหัสผ่านในการถอดข้อมูลออกจากไพรเวทคีย์ ของผู้ใช้ ซึ่งจะได้ข้อมูลที่ซ่อนอยู่ในไพรเวทคีย์ เก็บไว้เป็นข้อมูลชุด

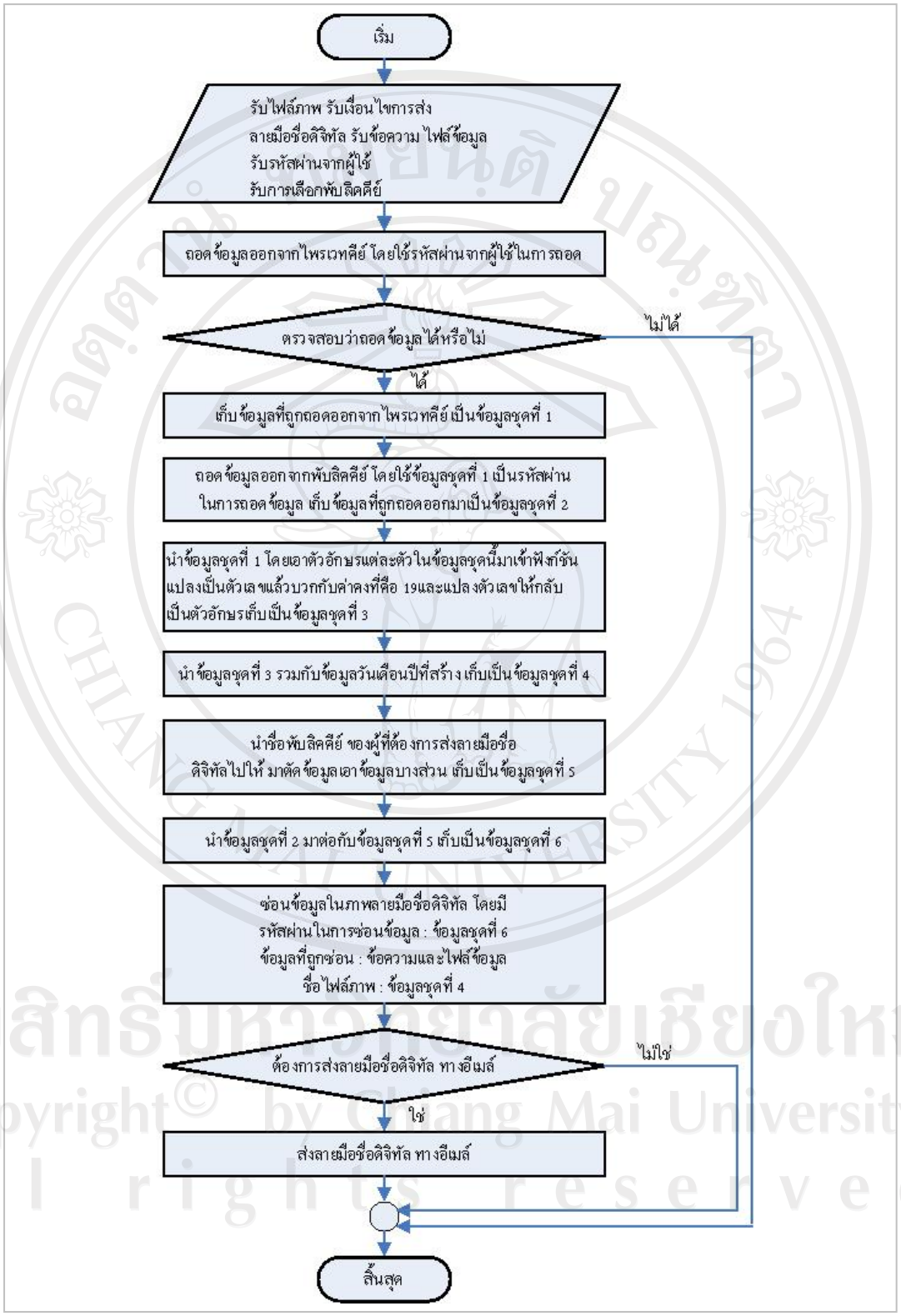
ที่หนึ่ง จากนั้นนำข้อมูลชุดที่หนึ่งมาเป็นรหัสผ่านในการถอดข้อมูลจากพับลิคคีย์ของผู้ใช้ จะได้ข้อมูลที่ซ่อนอยู่ในพับลิคคีย์ เก็บไว้เป็นข้อมูลชุดที่สอง จากนั้นนำข้อมูลชุดที่หนึ่งโดยเอาตัวอักษรแต่ละตัวในข้อมูลชุดนี้มาเข้าฟังก์ชันแปลงเป็นตัวเลขแล้วบวกกับค่าคงที่คือ 19 และแปลงตัวเลขให้กลับเป็นตัวอักษรเก็บเป็นข้อมูลชุดที่สาม จากนั้นจะนำข้อมูลชุดที่สามมารวมกับข้อมูลวันเดือนปีที่สร้างจะได้เป็นข้อมูลชุดที่สี่ จากนั้นระบบจะทำการซ่อนข้อความและไฟล์ข้อมูลที่ผู้ใช้ระบุ เข้าไปไว้ในไฟล์ภาพที่ผู้ใช้ได้ทำการเลือกเพื่อสร้างเป็นลายมือชื่อดิจิทัล โดยใช้ข้อมูลชุดที่สองเป็นรหัสผ่านที่ใช้ในการซ่อนข้อความและไฟล์ข้อมูลในลายมือชื่อดิจิทัล และใช้ข้อมูลชุดที่สี่เป็นชื่อของไฟล์ภาพที่เป็นลายมือชื่อดิจิทัล ในกรณีที่มีการระบุว่า ต้องการส่งลายมือชื่อดิจิทัล ไปให้ผู้รับผ่านทางอีเมล์ ระบบจะทำการส่งลายมือชื่อดิจิทัลไปให้ผู้รับทางอีเมล์



รูป 3.14 แสดงขั้นตอนการทำงานของการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว

จากรูป 3.14 อธิบายได้ดังนี้

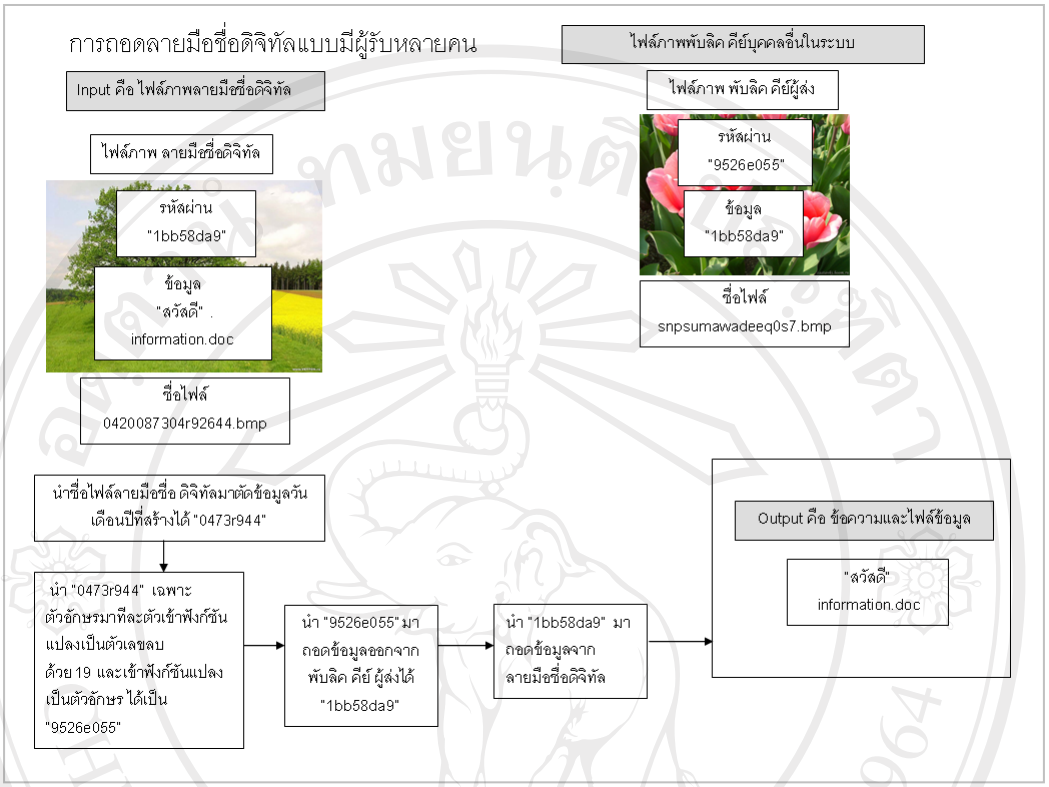
1) Input คือ
   (1) ไฟล์ภาพ 1 ไฟล์ ประเภท .bmp คือ 03.bmp
   (2) รหัสผ่านที่ผู้ส่งต้องการใช้ในการสร้างไพรเวทคีย์ และพับลิคคีย์ คือ “silverlight”
   (3) ข้อความและไฟล์ข้อมูลที่ต้องการส่งให้ผู้รับ คือ “สวัสดี” และ information.doc
2) Output คือ ไฟล์ภาพลายมือชื่อดิจิทัลที่มีข้อมูลซ่อนอยู่ ซึ่งข้อมูลที่ซ่อนจะประกอบด้วย รหัสผ่าน คือ “1bb58da9on815n73” และข้อมูลคือ “สวัสดี” และไฟล์ information.doc
3) Process มีขั้นตอนดังนี้
   (1) รหัสผ่านที่ใช้ในการสร้างไพรเวทคีย์ และพับลิคคีย์ คือ “silverlight”
   (2) นำ “silverlight” ถอดข้อมูลในไพรเวทคีย์ได้ “9526e055”
   (3) นำ “9526e055” ถอดข้อมูลในพับลิคคีย์ได้ “1bb58da9”
   (4) นำ “9526e055” เฉพาะตัวอักษรทีละตัวเข้าฟังก์ชันแปลงเป็นตัวเลขบวกด้วย 19 และเข้าฟังก์ชันแปลงเป็นตัวอักษรได้เป็น“0473r944”
   (5) นำ “0473r944” มารวมวันเดือนปีที่สร้างได้ “0420087304r92644” เพื่อใช้เป็นชื่อไฟล์ลายมือชื่อดิจิทัล
   (6) นำชื่อไฟล์พับลิคคีย์ผู้รับ “on81noknoi5n73” ตัดข้อมูลอีเมล์ผู้รับออกได้ “on815n73”
   (7) นำ “1bb58da9” มาต่อด้วย “on815n73” ได้ “1bb58da9on815n73” ซึ่งจะใช้เป็นรหัสผ่านที่จะซ่อนในไฟล์ภาพลายมือชื่อดิจิทัล
   (8) สร้างลายมือชื่อดิจิทัล (ซ่อนข้อมูลในไฟล์ภาพ)



รูป 3.15 แสดงรายละเอียดการทำงานของการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว

จากรูป 3.15 แสดงรายละเอียดการสร้างลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว ระบบจะรับข้อมูลไฟล์ภาพ ประเภท .bmp ที่ผู้ใช้เลือกจากภายนอกระบบ หรือเลือกจากแกลอรี่ภาพของระบบ รับข้อความและไฟล์ข้อมูลที่ผู้ใช้ต้องการที่จะซ่อนไว้ในลายมือชื่อดิจิทัล รับการเลือกพับลิคคีย์ ของผู้ที่ต้องการส่งลายมือชื่อดิจิทัลไปให้ และ รหัสผ่านซึ่งจะต้องเป็นตัวเดียวกับที่ใช้สร้างไพรเวทคีย์และพับลิคคีย์ พร้อมทั้งเงื่อนไขจากผู้ใช้ว่าต้องการสร้างลายมือชื่อดิจิทัล เพื่อเก็บไว้ในระบบ หรือสร้างแล้วให้ส่งลายมือชื่อดิจิทัล ไปให้ผู้รับทางอีเมล์ด้วย จากนั้นระบบจะนำรหัสผ่านที่ผู้ใช้กรอกเข้ามาเป็นรหัสผ่านในการถอดข้อมูลออกจากไพรเวทคีย์ ของผู้ใช้ ซึ่งจะได้ข้อมูลที่ซ่อนอยู่ในไพรเวทคีย์ เก็บไว้เป็นข้อมูลชุดที่หนึ่ง จากนั้นนำข้อมูลชุดที่หนึ่งมาเป็นรหัสผ่านในการถอดข้อมูลจากพับลิคคีย์ ของผู้ใช้ จะได้ข้อมูลที่ซ่อนอยู่ในพับลิคคีย์ เก็บไว้เป็นข้อมูลชุดที่สอง จากนั้นนำข้อมูลชุดที่หนึ่งโดยเอาตัวอักษรแต่ละตัวในข้อมูลชุดนี้มาเข้าฟังก์ชันแปลงเป็นตัวเลขแล้วบวกกับค่าคงที่คือ 19 และแปลงตัวเลขให้กลับเป็นตัวอักษรเก็บเป็นข้อมูลชุดที่สาม จากนั้นจะนำข้อมูลชุดที่สามมารวมกับข้อมูลวันเดือนปีที่สร้างจะได้เป็นข้อมูลชุดที่สี่ จากนั้นระบบจะทำการเอาชื่อของพับลิคคีย์ ของผู้ที่ต้องการส่งลายมือชื่อดิจิทัลไปให้ มาตัดข้อมูลชื่ออีเมล์แอดเดรสออกเก็บเป็นข้อมูลชุดที่ห้า จากนั้นเอาข้อมูลชุดที่สองมาต่อกับข้อมูลชุดที่ห้า ซึ่งจะได้เป็นข้อมูลชุดที่หก จากนั้นระบบจะทำการซ่อนข้อความและไฟล์ข้อมูลที่ผู้ใช้ระบุ เข้าไปไว้ในไฟล์ภาพที่ผู้ใช้ได้ทำการเลือกเพื่อสร้างเป็นลายมือชื่อดิจิทัล โดยใช้ข้อมูลชุดที่หกเป็นรหัสผ่านที่ใช้ในการซ่อนข้อความและไฟล์ข้อมูลในลายมือชื่อดิจิทัล และใช้ข้อมูลชุดที่สี่เป็นชื่อของไฟล์ภาพที่เป็นลายมือชื่อดิจิทัล ในกรณีที่มีการระบุว่า ต้องการส่งลายมือชื่อดิจิทัล ไปให้ผู้รับผ่านทางอีเมล์ ระบบจะทำการส่งลายมือชื่อดิจิทัลไปให้ผู้รับทางอีเมล์

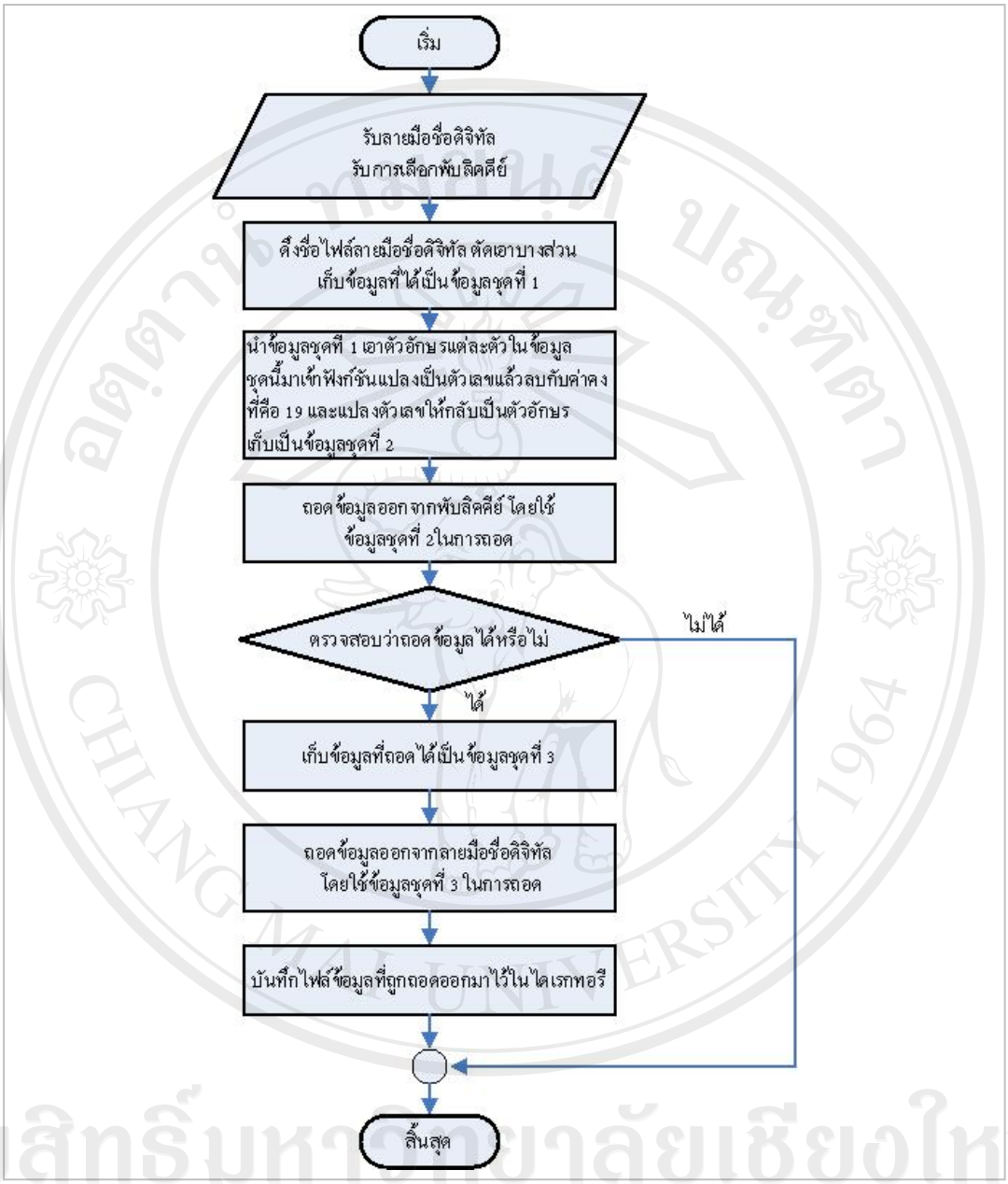
4. กระบวนการถอดลายมือชื่อดิจิทัล เป็นขั้นตอนฝั่งผู้รับ



รูป 3.16 แสดงขั้นตอนการทำงานของการถอดลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน

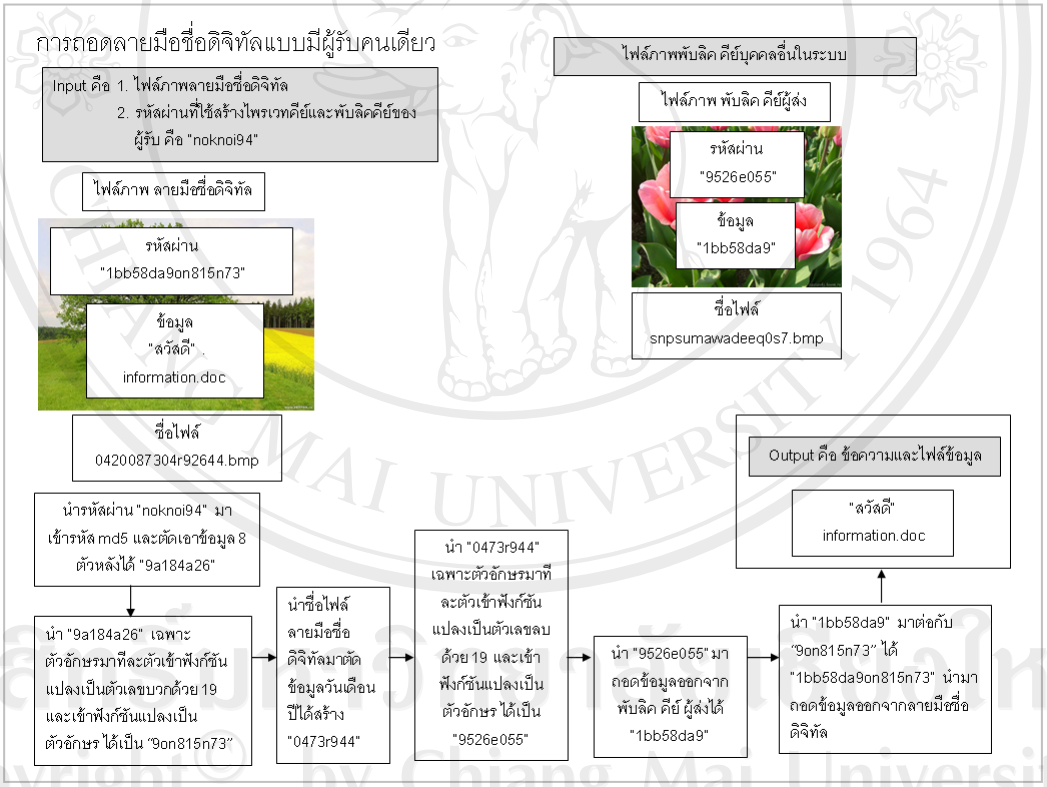
จากรูป 3.16 อธิบายได้ดังนี้

1) Input คือไฟล์ภาพลายมือชื่อดิจิทัล คือ 0420087304r92644.bmp
2) Output คือ ข้อความ คือ “สวัสดี” และไฟล์ข้อมูล คือ information.doc
3) Process มีขั้นตอนดังนี้
   (1) นำชื่อไฟล์ลายมือชื่อ ดิจิทัลมาตัดข้อมูลวันเดือนปีที่สร้างได้ “0473r944”
   (2) นำ “0473r944” เฉพาะตัวอักษรทีละตัวเข้าฟังก์ชันแปลงเป็นตัวเลขลบด้วย 19 และเข้าฟังก์ชันแปลงเป็นตัวอักษรได้เป็น “9526e055”
   (3) นำ “9526e055”มาถอดข้อมูลออกจากพับลิคคีย์ ผู้ส่งได้ “1bb58da9”
   (4) นำ “1bb58da9” มาถอดข้อมูลจากลายมือชื่อดิจิทัล



รูป 3.17 แสดงรายละเอียดการทำงานของการถอดลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน

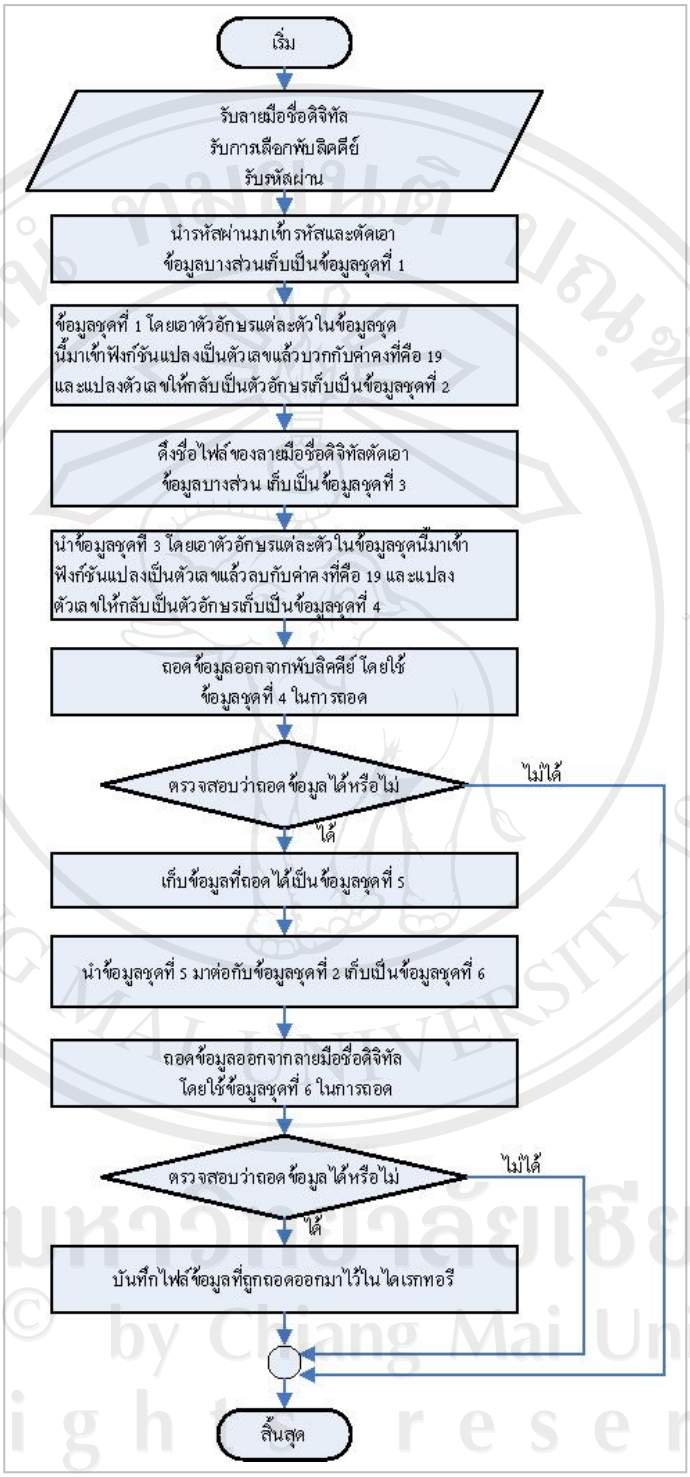
จากรูป 3.17 แสดงรายละเอียดการถอดลายมือชื่อดิจิทัลแบบมีผู้รับหลายคน ระบบจะรับข้อมูลการเลือกลายมือชื่อดิจิทัล และ พับลิคคีย์ ของบุคคลที่เป็นเจ้าของลายมือชื่อดิจิทัล ระบบจะดึงชื่อไฟล์ของลายมือชื่อดิจิทัลมาตัดเอาข้อมูลวันเดือนปีที่สร้างออกเก็บเป็นข้อมูลชุดที่หนึ่ง นำข้อมูลชุดที่หนึ่งโดยเอาตัวอักษรแต่ละตัวในข้อมูลชุดนี้มาเข้าฟังก์ชันแปลงเป็นตัวเลขแล้วลบกับค่าคงที่คือ 19 และแปลงตัวเลขให้กลับเป็นตัวอักษรเก็บเป็นข้อมูลชุดที่สอง จากนั้นระบบจะใช้ข้อมูลชุดที่สองเป็นรหัสผ่านที่ใช้ในการถอดข้อมูลที่ซ่อนอยู่ในพับลิคคีย์ ของผู้ที่เป็นเจ้าของลายมือชื่อดิจิทัล ถ้าพับลิคคีย์ เป็นของเจ้าของลายมือชื่อดิจิทัลจริง จะสามารถถอดข้อมูลที่ถูกซ่อนอยู่ในพับลิคคีย์ ได้ ระบบจะเก็บเป็นข้อมูลชุดที่สาม จากนั้นระบบจะนำข้อมูลชุดที่สามมาเป็นรหัสผ่านในการถอดข้อมูลออกจากลายมือชื่อดิจิทัล ระบบจะให้ผู้ใช้ทำการเลือกไฟล์ข้อมูลเพื่อทำการบันทึกไว้ที่ไดเรกทอรีที่ต้องการ



รูป 3.18 แสดงขั้นตอนการทำงานของการถอดลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว

จากรูป 3.18 อธิบายได้ดังนี้

1) Input คือ
   (1) ไฟล์ภาพลายมือชื่อดิจิทัล คือ 0420087304r92644.bmp
   (2) รหัสผ่านที่ใช้สร้างไพรเวทคีย์และพับลิคคีย์ของผู้รับ คือ “noknoi94”
2) Output คือ ข้อความ คือ “สวัสดี” และไฟล์ข้อมูล คือ information.doc
3) Process มีขั้นตอนดังนี้
   (1) นำรหัสผ่าน “noknoi94” มาเข้ารหัส md5 และตัดเอาข้อมูล 8 ตัวหลัง ได้ “9a184a26”
   (2) นำ “9a184a26” เฉพาะตัวอักษรทีละตัวเข้าฟังก์ชันแปลงเป็นตัวเลข และนำมาบวกด้วย 19 และเข้าฟังก์ชันแปลงเป็นตัวอักษรได้เป็น “9on815n73”
   (3) นำชื่อไฟล์ลายมือชื่อดิจิทัลมาตัดข้อมูลวันเดือนปีได้เป็น “0473r944”
   (4) นำ “0473r944” เฉพาะตัวอักษรทีละตัวเข้าฟังก์ชันแปลงเป็นตัวเลข ลบด้วย 19 และเข้าฟังก์ชันแปลงเป็นตัวอักษรได้เป็น “9526e055”
   (5) นำ “9526e055”มาถอดข้อมูลออกจากพับลิคคีย์ ผู้ส่งได้ “1bb58da9”
   (6) นำ“1bb58da9” มาต่อกับ “9on815n73” ได้“1bb58da9on815n73” นำมาถอดข้อมูลออกจากลายมือชื่อดิจิทัล



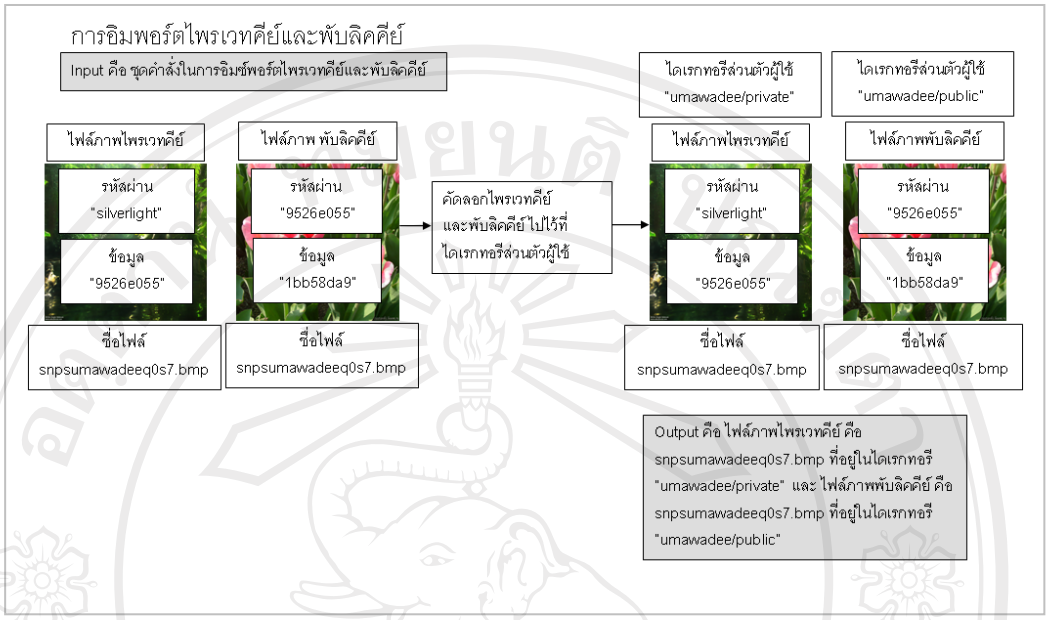
รูป 3.19 แสดงรายละเอียดการทำงานของการถอดลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว

จากรูป 3.19 แสดงรายละเอียดการถอดลายมือชื่อดิจิทัลแบบมีผู้รับคนเดียว ระบบจะรับข้อมูลการเลือกลายมือชื่อดิจิทัล และ พับลิคคีย์ของบุคคลที่เป็นเจ้าของลายมือชื่อดิจิทัล และรับข้อมูลรหัสผ่านซึ่งเป็นตัวเดียวกับที่ใช้สร้างไพรเวทคีย์และพับลิคคีย์ จากที่ผู้ใช้ ระบบจะนำรหัสผ่านดังกล่าวมาเข้ารหัสแบบทางเดียว คือ md5 ตัดเอาข้อมูล 8 ตัวหลัง เก็บเป็นข้อมูลชุดที่หนึ่ง นำข้อมูลชุดที่หนึ่งโดยเอาตัวอักษรแต่ละตัวในข้อมูลชุดนี้มาเข้าฟังก์ชันแปลงเป็นตัวเลขแล้วบวกกับค่าคงที่คือ 19 และแปลงตัวเลขให้กลับเป็นตัวอักษรเก็บเป็นข้อมูลชุดที่สอง จากนั้นระบบจะดึงเอาชื่อไฟล์ของลายมือชื่อดิจิทัลตัดเอาข้อมูลวันเดือนปีที่สร้างออกเก็บเป็นข้อมูลชุดที่สาม นำข้อมูลชุดที่สามโดยเอาตัวอักษรแต่ละตัวในข้อมูลชุดนี้มาเข้าฟังก์ชันแปลงเป็นตัวเลขแล้วลบกับค่าคงที่คือ 19 และแปลงตัวเลขให้กลับเป็นตัวอักษรเก็บเป็นข้อมูลชุดที่สี่ จากนั้นระบบจะใช้ข้อมูลชุดที่สี่เป็นรหัสผ่านในการถอดข้อมูลที่ซ่อนอยู่ในพับลิคคีย์ ของผู้ที่เป็นเจ้าของลายมือชื่อดิจิทัล ถ้าพับลิคคีย์ เป็นของเจ้าของลายมือชื่อดิจิทัลจริง จะสามารถถอดข้อมูลที่ถูกซ่อนอยู่ในพับลิคคีย์ได้ ระบบจะเก็บเป็นข้อมูลชุดที่ห้า จากนั้นระบบจะนำข้อมูลชุดที่ห้ามาต่อกับข้อมูลชุดที่สองได้เป็นข้อมูลชุดที่หก เพื่อใช้เป็นรหัสผ่านในการถอดข้อมูลออกจากลายมือชื่อดิจิทัล ถ้าลายมือดิจิทัลนั้นถูกส่งมาให้ผู้ใช้จริง จะสามารถถอดข้อมูลที่ซ่อนไว้ในลายมือชื่อดิจิทัลได้ ระบบจะให้ผู้ใช้ทำการเลือกไฟล์ข้อมูลเพื่อทำการบันทึกไว้ที่ไดเรกทอรีที่ต้องการ

5. กระบวนการอิมพอร์ตและเอกซ์พอร์ตคีย์ต่าง ๆ ในระบบ

กระบวนการอิมพอร์ต เป็นกระบวนการคัดลอกคีย์ที่ผู้ใช้ต้องการ เข้าสู่ระบบ กระบวนการเอกซ์พอร์ต เป็นกระบวนการคัดลอกคีย์ ไปเก็บไว้ในไดเรกทอรีสำหรับเก็บคีย์ที่ถูกเอกซ์พอร์ต โดยแบ่งออกเป็น 4 ส่วน ดังนี้

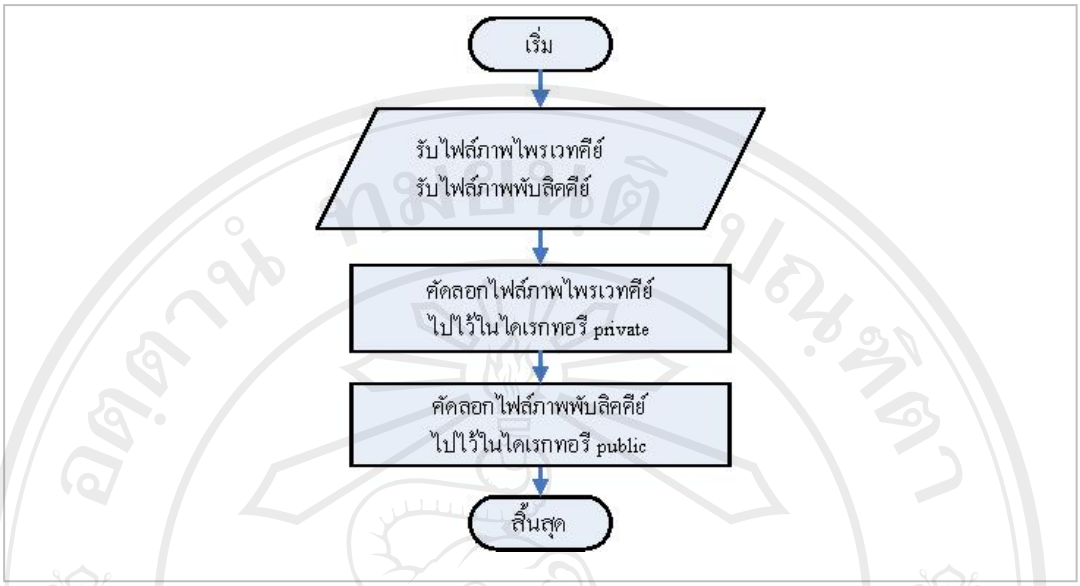
1. กระบวนอิมพอร์ตไพรเวทคีย์และพับลิคคีย์



รูป 3.20 แสดงขั้นตอนการทำงานของการอิมพอร์ตไพรเวทคีย์และพับลิคคีย์

จากรูป 3.20 อธิบายได้ดังนี้

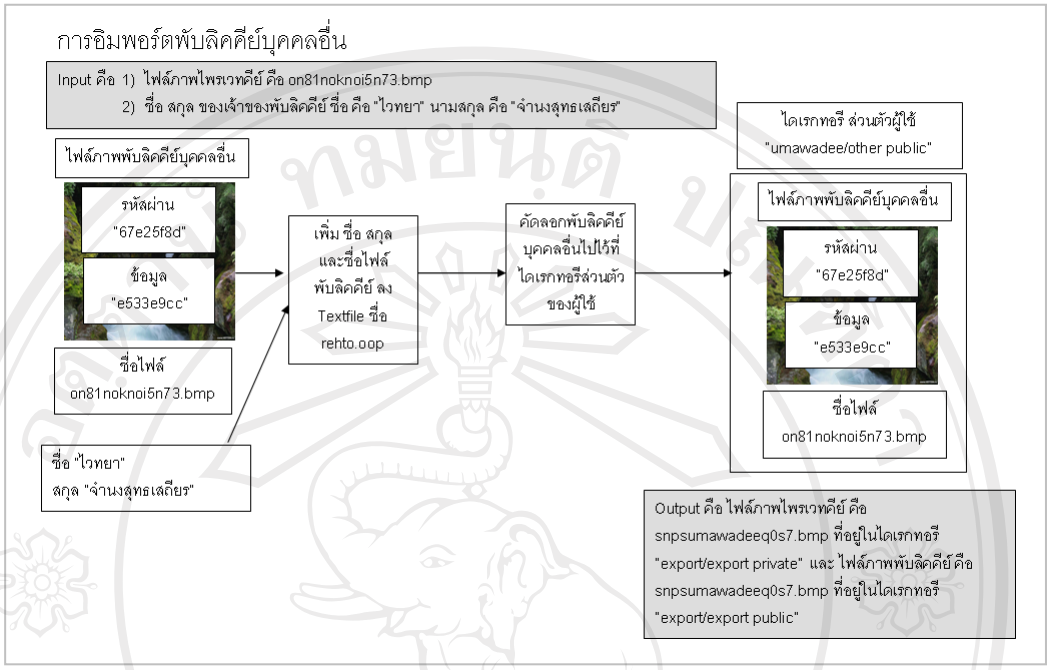
1) Input คือ
   (1) ไฟล์ภาพไพรเวทคีย์ คือ snpsumawadeeq0s7.bmp
   (2) ไฟล์ภาพพับลิคคีย์ คือ snpsumawadeeq0s7.bmp
2) Output คือ ไฟล์ภาพไพรเวทคีย์ คือ snpsumawadeeq0s7.bmp และ ไฟล์ภาพพับลิคคีย์ คือ snpsumawadeeq0s7.bmp ที่อยู่ในไดเรกทอรีส่วนตัวของผู้ใช้ คือ “umawadee/private”
3) Process คือ คัดลอกไพรเวทคีย์และพับลิคคีย์ไปไว้ที่ไดเรกทอรีส่วนตัวของผู้ใช้คือ “umawadee/public”



รูป 3.21 แสดงรายละเอียดการทำงานของการอิมพอร์ตไพรเวทคีย์และพับลิคคีย์

จากรูป 3.21 แสดงรายละเอียดการทำงานของการอิมพอร์ตไพรเวทคีย์และพับลิคคีย์ ระบบจะทำการรับข้อมูลไฟล์ภาพที่เป็นไพรเวทคีย์และพับลิคคีย์ ที่ผู้ใช้ระบุเข้ามาและทำการคัดลอกไฟล์ภาพที่เป็นไพรเวทคีย์ไปเก็บไว้ในไดเรกทอรี private ที่อยู่ในไดเรกทอรีส่วนตัวของผู้ใช้ และทำการคัดลอกไฟล์ภาพที่เป็นพับลิคคีย์ไปเก็บไว้ในไดเรกทอรี public ที่อยู่ในไดเรกทอรีส่วนตัวของผู้ใช้

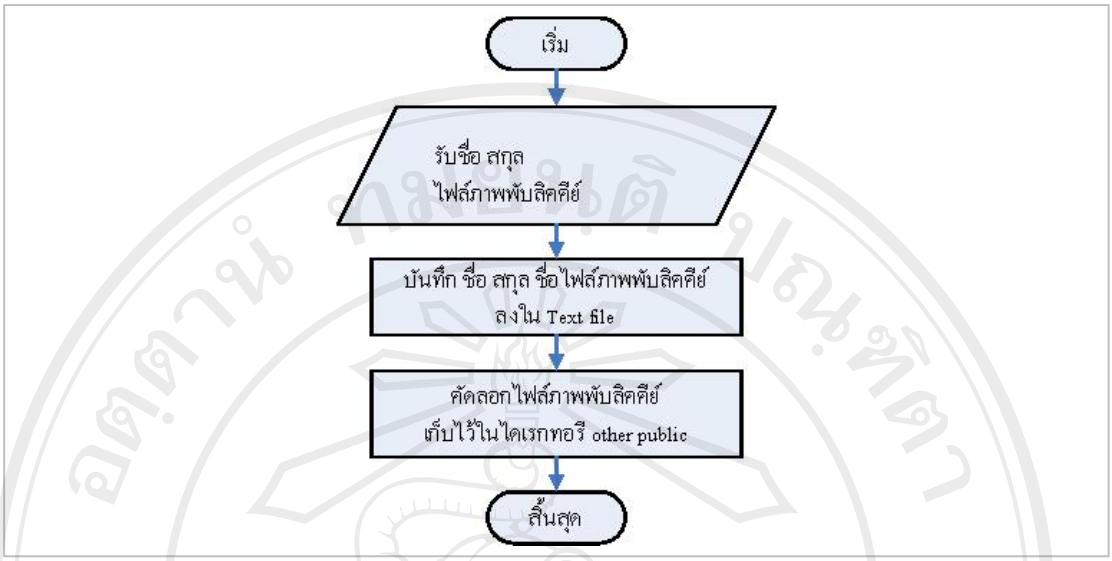
2. กระบวนการอิมพอร์ตพับลิคคีย์บุคคลอื่น



รูป 3.22 แสดงขั้นตอนการทำงานของการอิมพอร์ตพับลิคคีย์บุคคลอื่น

จากรูป 3.22 อธิบายได้ดังนี้

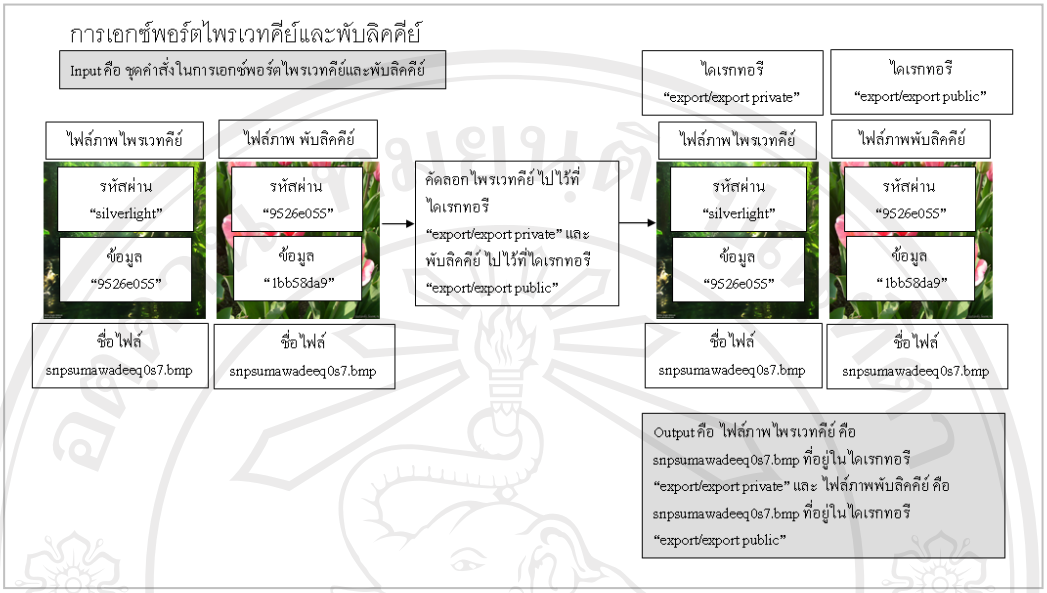
1) Input คือ
   (1) ไฟล์ภาพไพรเวทคีย์ คือ on81noknoi5n73.bmp
   (2) ชื่อ สกุล ของเจ้าของพับลิคคีย์ ชื่อ คือ “ไวทยา” นามสกุล คือ “จำนงสุทธเลถียร”
2) Output คือ ไฟล์ภาพพับลิคคีย์ คือ on81noknoi5n73.bmp ที่อยู่ในไดเรกทอรีส่วนตัวของผู้ใช้ คือ “umawadee/other public”
3) Process คือ
   (1) เพิ่ม ชื่อ สกุล และชื่อไฟล์พับลิคคีย์ ลง Textfile ชื่อ rehto.oop
   (2) คัดลอกพับลิคคีย์บุคคลอื่นไปไว้ที่ไดเรกทอรีส่วนตัวของผู้ใช้ คือ “umawadee/other public”



รูป 3.23 แสดงรายละเอียดการทำงานของการอิมพอร์ตพับลิคคีย์บุคคลอื่น

จากรูป 3.23 แสดงรายละเอียดการทำงานของการอิมพอร์ตพับลิคคีย์บุคคลอื่น ระบบจะทำการรับข้อมูลไฟล์รูปภาพที่เป็นพับลิคคีย์บุคคลอื่น พร้อมทั้ง ชื่อ สกุล ของผู้เป็นเจ้าของพับลิคคีย์ โดยนำชื่อ สกุล และ ชื่อไฟล์ภาพพับลิคคีย์ บันทึกลงใน Text file ที่เก็บข้อมูลไฟล์ภาพพับลิคคีย์ บุคคลอื่น และทำการคัดลอกไฟล์ภาพพับลิคคีย์ เก็บไว้ในไดเรกทอรี other public ที่อยู่ในไดเรกทอรีส่วนตัวของผู้ใช้

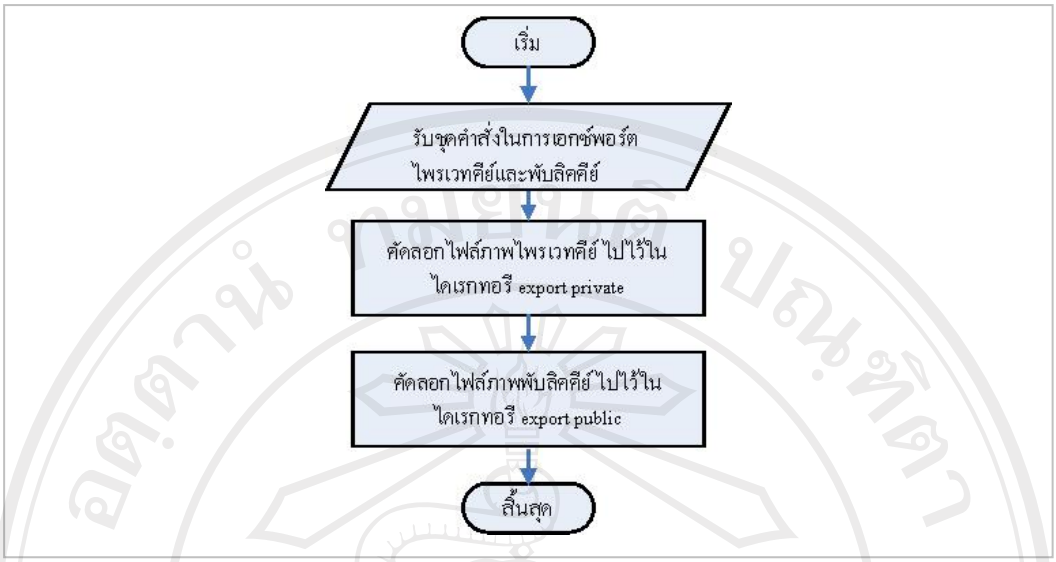
3. กระบวนการเอกซ์พอร์ตไพรเวทคีย์และพับลิคคีย์



รูป 3.24 แสดงขั้นตอนการทำงานของการเอกซ์พอร์ตไพรเวทคีย์และพับลิคคีย์

จากรูป 3.24 อธิบายได้ดังนี้

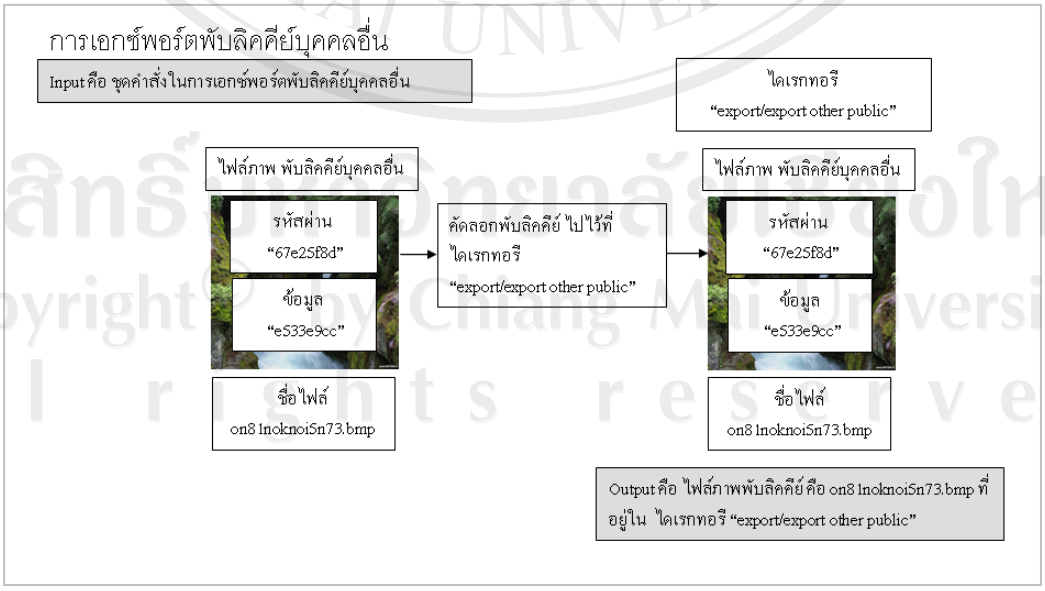
1) Input คือ ชุดคำสั่งในการเอกซ์พอร์ตไพรเวทคีย์และพับลิคคีย์
2) Output คือ ไฟล์ภาพไพรเวทคีย์ คือ snpsumawadeeq0s7.bmp ที่อยู่ในไดเรกทอรี "export/export private" และ ไฟล์ภาพพับลิคคีย์ คือ snpsumawadeeq0s7.bmp ที่อยู่ในไดเรกทอรี "export/export public"
3) Process คือ คัดลอกไพรเวทคีย์ คือ snpsumawadeeq0s7.bmp ไปไว้ที่ไดเรกทอรี "export/export private" และพับลิคคีย์ คือ snpsumawadeeq0s7.bmp ไปไว้ที่ไดเรกทอรี "export/export public"



รูป 3.25 แสดงรายละเอียดการทำงานของการเอกซ์พอร์ตไพรเวทคีย์และพับลิคคีย์

จากรูป 3.25 แสดงรายละเอียดการทำงานของการเอกซ์พอร์ตไพรเวทคีย์และพับลิคคีย์ ซึ่งเป็นกระบวนการที่ระบบทำการคัดลอกไฟล์ภาพไพรเวทคีย์ที่อยู่ในไดเรกทอรีส่วนตัวของผู้ใช้ ไปเก็บไว้ในไดเรกทอรี export private ของระบบ และ คัดลอกไฟล์ภาพพับลิคคีย์ทีอยู่ในไดเรกทอรีส่วนตัวของผู้ใช้ ไปเก็บไว้ในไดเรกทอรี export public ของระบบ

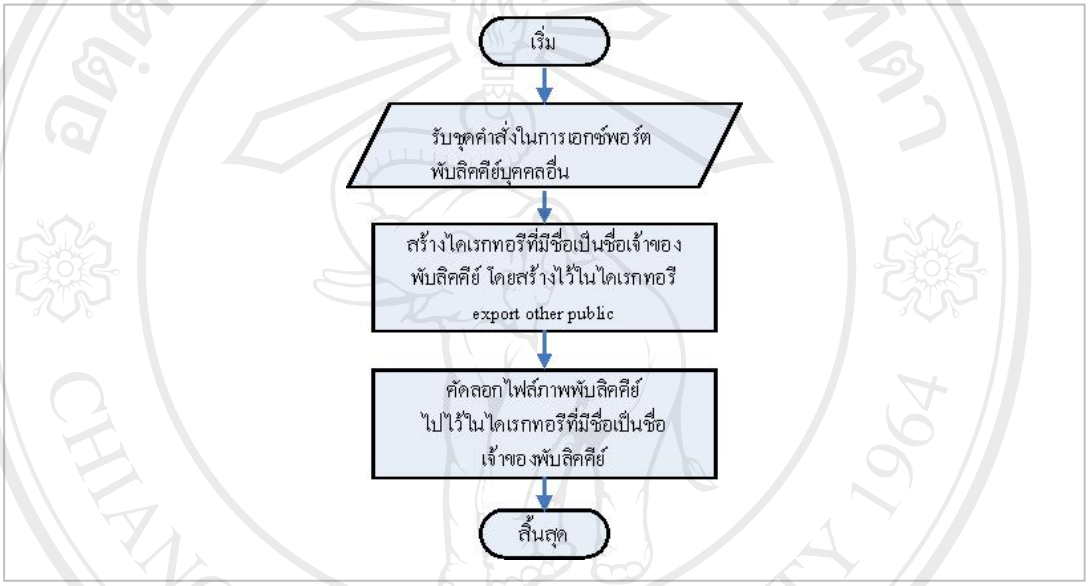
4. กระบวนการเอกซ์พอร์ตพับลิคคีย์บุคคลอื่น



รูป 3.26 แสดงขั้นตอนการทำงานของการเอกซ์พอร์ตพับลิคคีย์บุคคลอื่น

จากรูป 3.26 อธิบายได้ดังนี้

1) Input คือ ชุดคำสั่งในการเอกซ์พอร์ตพับลิคคีย์บุคคลอื่น
2) Output คือ ไฟล์ภาพพับลิคคีย์ คือ on81noknoi5n73.bmp ที่อยู่ในไดเรกทอรี “export/export other public”
3) Process คือ คัดลอกพับลิคคีย์ คือ on81noknoi5n73.bmpไปไว้ที่ไดเรกทอรี “export/export other public”



รูป 3.27 แสดงขั้นตอนการทำงานของการเอกซ์พอร์ตพับลิคคีย์บุคคลอื่น

จากรูป 3.27 แสดงขั้นตอนการทำงานของการเอกซ์พอร์ตพับลิคคีย์บุคคลอื่นซึ่งเป็นกระบวนการที่ระบบทำการสร้างไดเรกทอรีโดยชื่อไดเรกทอรีเป็นชื่อของเจ้าของพับลิคคีย์ โดยสร้างไว้ในไดเรกทอรี export other public ของระบบ จากนั้นทำการคัดลอกไฟล์ภาพพับลิคคีย์บุคคลอื่น ที่อยู่ไดเรกทอรีส่วนตัวของผู้ใช้ ไปเก็บไว้ในไดเรกทอรีที่มีชื่อเป็นชื่อของเจ้าของพับลิคคีย์

3.3.2 วิธีการ โมดูล และ โปรแกรม ที่ใช้ในการพัฒนาระบบ

1. วิธีการเข้ารหัสข้อมูล (Encryption) ที่ผู้ศึกษาใช้ คือการเข้ารหัสข้อมูลแบบทางเดียว โดยเลือกใช้การเข้ารหัส MD5 มีสูตรดังนี้

b1 = MD5(S+RA) c(i) = p1 XOR b1

b2 = MD5(S+c(1)) c(2) = p2 XOR b2

.

.

bi = MD5(S+c(i-1)) c(i) = pi XOR bi

ค่าของ String ที่ได้จะประกอบด้วย c(1)+c(2)+…+c(i)

S คือ Share Secret

RA คือ Pseudo-random 128-bit Request Authenticator

p1, p2,.... คือ การนำ ข้อมูลเข้า ไปไว้ใน 16 ไบต์

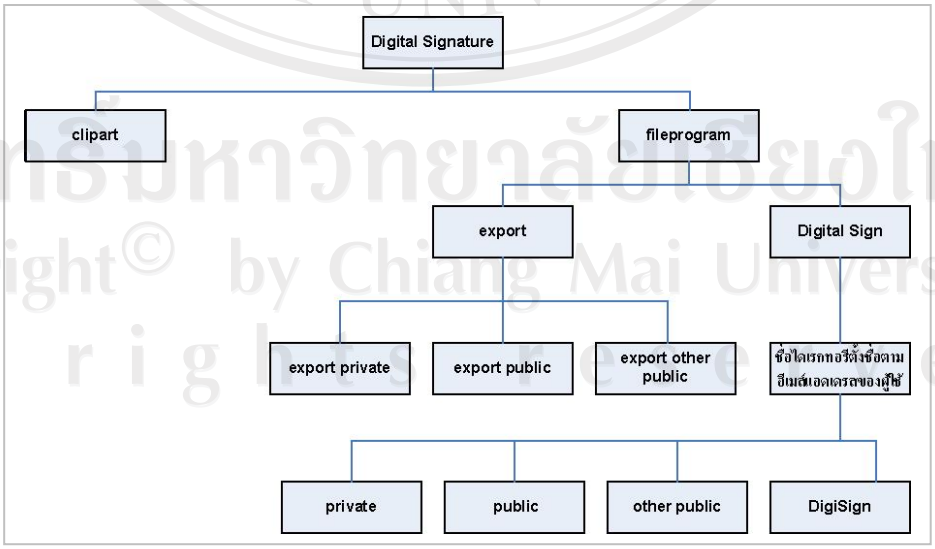
c(1), c(2),... คือ Ciphertext blocks

2. วิธีการซ่อนข้อมูลในรูปภาพ ที่ผู้พัฒนาเลือกใช้ คือ การซ่อนข้อมูลไว้ในบิตที่มีนัยสำคัญต่ำสุด (Least Significant Bit : LSB) คือบิตขวามือเป็นบิตที่มีค่าประจำหลักน้อยที่สุด

3. โมดูลในการส่งอีเมล์ คือ SMTP ของ Ostrosoft

4. โปรแกรม Smile Help ในการสร้าง Help ของระบบ

3.3.3 โครงสร้างของการเก็บข้อมูล ในระบบ



รูป 3.28 แสดงโครงสร้างของการเก็บข้อมูลในระบบ

จากรูป 3.28 การออกแบบโครงสร้างของการเก็บข้อมูลในระบบ มีรายละเอียด ดังนี้

ระบบจะประกอบด้วย 2 ไดเรกทอรี หลัก คือ fileprogram และ Clipart

1. fileprogram เป็นไดเรกทอรีที่เก็บไฟล์ที่ต้องใช้ในกระบวนการต่าง ๆ ของระบบ และ ไดเรกทอรีส่วนตัวของผู้ใช้ โดยไดเรกทอรีนี้จะมีไดเรกทอรีย่อย 2 ไดเรกทอรี คือ Digital Sign และ export

1) Digital Sign เป็นไดเรกทอรี ที่เก็บ ไดเรกทอรีส่วนตัวของผู้ใช้ ซึ่งในแต่ละไดเรกทอรีส่วนตัวของผู้ใช้ จะประกอบด้วยไดเรกทอรีย่อย 4 ไดเรกทอรี ดังนี้

- DigiSign เก็บข้อมูลที่ถูกถอดออกมาจากลายมือชื่อดิจิทัล แต่ข้อมูลจะถูกลบไปเมื่อผู้ใช้ไม่ได้ทำการบันทึกข้อมูลดังกล่าว หรือข้อมูลจะถูกย้ายไปยังไดเรกทอรี ที่ผู้ใช้ได้ทำการเลือกไว้
- Other Public เก็บไฟล์ภาพที่เป็นพับลิคคีย์ของบุคคลอื่น และเก็บไฟล์นามสกุล .txt ที่มีข้อมูลของพับลิคคีย์ของบุคคลอื่น
- Private เก็บไฟล์ภาพ ที่เป็น ไพรเวทคีย์ ของผู้ใช้
- Public เก็บไฟล์ภาพ ที่เป็น พับลิคคีย์ ของผู้ใช้

2) export เป็นไดเรกทอรีที่เก็บไฟล์ภาพ คีย์ ต่าง ๆ ที่ผู้ใช้ทำกาเอกซ์พอร์ต โดยมีไดเรกทอรีย่อย 3 ไดเรกทอรี่ ดังนี้

- export other public เก็บไฟล์ภาพพับลิคคีย์ของบุคคลอื่นที่ผู้ใช้ได้ทำการเอกซ์พอร์ต
- export private เก็บไฟล์ภาพไพรเวทคีย์ของผู้ใช้ที่ผู้ใช้ได้ทำการเอกซ์พอร์ต
- export public เก็บไฟล์ภาพพับลิคคีย์ของผู้ใช้ที่ผู้ใช้ได้ทำการเอกซ์พอร์ต

นอกจากไดเรกทอรี่ Digital Sign และ export แล้ว จะมีไฟล์ภาพที่มีไฟล์ข้อมูลผู้ใช้ซ่อนอยู่ ซึ่งไฟล์นี้ใช้สำหรับกรณีตรวจสอบผู้ใช้ของระบบ เพิ่มและแก้ไขข้อมูลผู้ใช้

2. Clipart เป็นไดเรกทอรี่ที่เก็บไฟล์ภาพที่ใช้แสดงในแกลอรี่ภาพ สำหรับให้ผู้ใช้เลือกในการสร้าง ไพรเวทคีย์ พับลิคคีย์ และ ลายมือชื่อดิจิทัล