บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

ในการพัฒนาซอฟต์แวร์สำหรับสร้างลายมือชื่อดิจิทัลโดยใช้หลักการประมวลผลภาพผู้ศึกษาได้ค้นคว้าเอกสารและงานวิจัยที่เกี่ยวข้องโดยมีรายละเอียดตามหัวข้อที่กำหนดตามลำดับดังนี้

2.1 แนวความคิดเกี่ยวกับลายมือชื่อดิจิทัล

2.1.1 ลายมือชื่อดิจิทัล (Digital Signature)

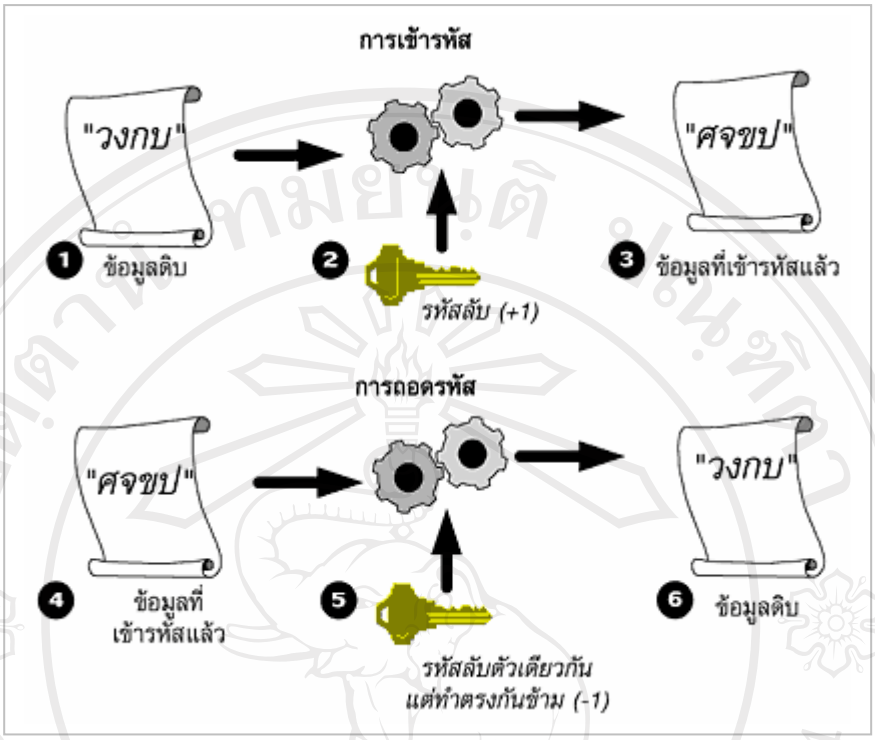
(Wikipedia, 2544:ระบบออนไลน์) ลายมือชื่อดิจิทัล คือ ข้อมูลอิเล็กทรอนิกส์ที่ได้จากการเข้ารหัสข้อมูลโดยการเข้ารหัสข้อมูลจะเป็นชนิด การเข้ารหัสแบบอสมมาตร (asymmetric-key cryptography) ซึ่งเป็นการเข้ารหัสที่ต้องใช้กุญแจที่คู่กัน (กุญแจสองดอก) ได้แก่

1. กุญแจสาธารณะ (Public Key)
2. กุญแจส่วนตัว (Private Key)

กุญแจส่วนตัวและกุญแจสาธารณะจะต้องมีความสัมพันธ์กันคือ ถ้าใช้กุญแจส่วนตัวในการเข้ารหัสจะต้องถอดรหัสโดยใช้กุญแจสาธารณะเท่านั้น ในทางกลับกัน ถ้าใช้กุญแจสาธารณะในการเข้ารหัสจะถอดรหัสได้ต้องใช้กุญแจส่วนตัว ซึ่งกุญแจส่วนตัวและกุญแจสาธารณะจะต้องใช้กันเป็นคู่ ๆ การเข้ารหัสของ ลายมือชื่อดิจิทัล นั้นจะใช้ กุญแจส่วนตัวของผู้ส่งและการถอดรหัสจะใช้กุญแจสาธารณะของผู้ส่งในการรักษาข้อมูลให้เป็นความลับ

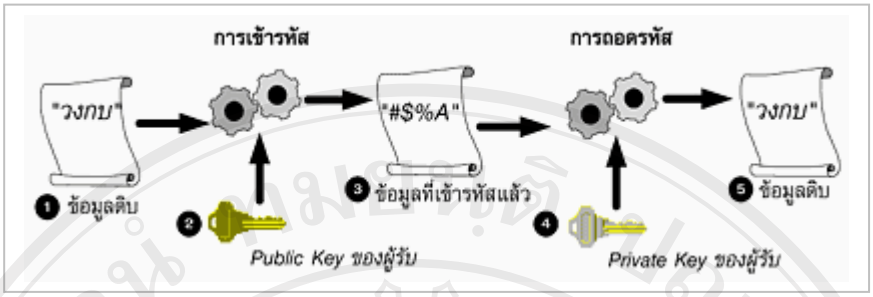
2.1.2 กระบวนการสร้างและลงลายมือชื่อดิจิทัล

การจะเข้าใจการทำงานของลายมือชื่อดิจิทัล ต้องรู้จักกลไกการเข้าและถอดรหัส แบบอสมมาตร (asymmetric) ก่อน โดยปกติการเข้ารหัสที่เราคุ้นเคยกันทั่วไป จะเป็นแบบสมมาตร (symmetric) คือ เอาข้อความที่จะเข้ารหัสมาชุดหนึ่ง ผ่านการเข้ารหัสให้เป็นข้อความใหม่ที่อ่านไม่รู้เรื่อง เช่น เปลี่ยนอักษรทุกตัวเป็นตัวถัดไปหรือบวก 1 เข้าไปที่รหัสของอักษรแต่ละตัว ดังนั้น ก.ไก่ จะกลายเป็น ข.ไข่ อ.อ่างกลายเป็น ฮ.นกฮูก เป็นต้น ดังนั้น คำว่า “วงกบ” จะกลายเป็น “ศจขป” จากนั้นบอกคีย์ที่ใช้การเข้ารหัสนั้น (เช่น ตัวอย่างนี้คือเลข 1) ให้กับผู้รับ ผู้รับก็จะถอดรหัส โดยทำย้อนกลับคือ เอา 1 ไปลบจากรหัสทุกตัว ดังนั้น ศ. ก็จะกลายเป็น ว. ส่วน จ.ก็กลายเป็น ง. ผู้รับก็จะได้คำว่า “วงกบ” กลับมาตามเดิม



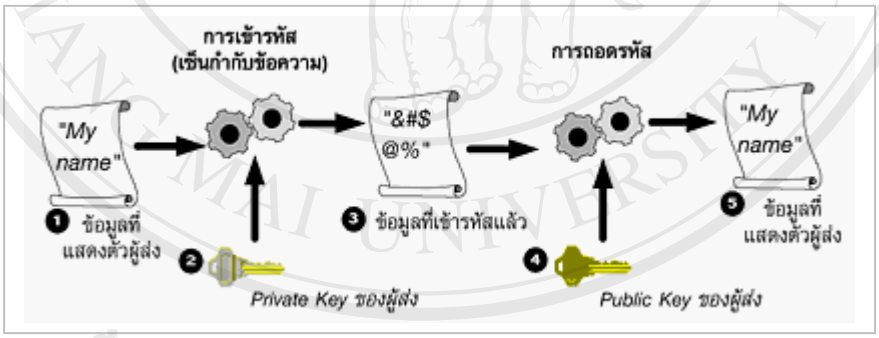
รูป 2.1 แสดงการทำงานของกลไกการเข้าและถอดรหัสแบบสมมาตร

วิธีข้างต้นไม่เหมาะที่จะใช้บนอินเทอร์เน็ต เพราะต้องส่งรหัส เช่น +1 ไปให้ผู้รับด้วย ซึ่งอาจถูกขโมยได้ ทำให้ผู้อื่นสามารถอ่านข้อความออก จึงมีการคิดวิธีเข้าและถอดรหัสแบบอสมมาตรขึ้น คือเข้ารหัสด้วยตัวเลขชุดหนึ่ง แต่ถอดรหัสด้วยตัวเลขอีกชุดหนึ่งที่คู่กัน แต่การคำนวณให้ได้รหัสนี้ จะต้องอาศัยวิธีทางคณิตศาสตร์ที่ซับซ้อน วิธีการคือ ทุกคนที่จะรับข้อมูล จะประกาศคีย์หรือตัวเลขชุดที่ใช้ในการเข้ารหัสของตนไว้บนอินเทอร์เน็ต ใครอยากจะส่งข้อมูลให้ผู้รับคนนี้ ก็มาเอาตัวเลขนี้ไปใช้เข้ารหัสข้อมูล แล้วส่งมาให้ ตัวเลขหรือคีย์ชุดดังกล่าวเรียกว่าพับลิคคีย์ มีคุณสมบัติพิเศษ คือ เมื่อเข้ารหัสไปแล้ว จะใช้ถอดรหัสนั้นกลับคืนมาไม่ได้ ข้อความที่เข้ารหัสแล้ว จึงเป็นข้อความลับที่ใครๆ ก็อ่านไม่ได้ นอกจากเจ้าตัวผู้รับที่ผู้ส่งเจาะจงมา ซึ่งจะมีตัวเลขหรือคีย์อีกชุดหนึ่งที่คู่กัน ซึ่งจะใช้สำหรับถอดรหัสข้อความนั้น เรียกว่า ไพรเวทคีย์ วิธีนี้มีข้อดีคือผู้ส่งไม่ต้องส่งรหัสลับมาให้ผู้รับเลย



รูป 2.2 แสดงการทำงานของกลไกการเข้าและถอดรหัสแบบอสมมาตร

ในทางกลับกัน ผู้ส่งอาจใช้ ไพรเวทคีย์ ของตนเองเข้ารหัส แล้วส่งข้อมูลให้ผู้รับก็ได้ วิธีนี้ข้อมูลจะไม่เป็นความลับ เพราะใครๆ ที่ดักฟังข้อมูลที่ส่งได้ก็อาจเอาพับลิคคีย์ ของผู้ส่ง (ที่หาได้บนอินเทอร์เน็ต) มาถอดรหัสเพื่ออ่านได้ แต่ข้อดีคือเป็นการพิสูจน์ว่า ผู้ส่งเป็นคนส่งข้อความนั้นมาเองจริง ๆ เพราะเข้ารหัส ด้วย ไพรเวทคีย์ ของตัวเอง ที่ไม่มีคนอื่นรู้ คนอื่นจึงปลอมแปลง หรือแก้ไขขึ้นมาเองไม่ได้ ซึ่งเหมือนกับเอกสารที่มีลายเซ็นของผู้ส่งกำกับมานั่นเอง



รูป 2.3 แสดงการทำงานของกลไกการเข้าและถอดรหัสแบบอสมมาตร

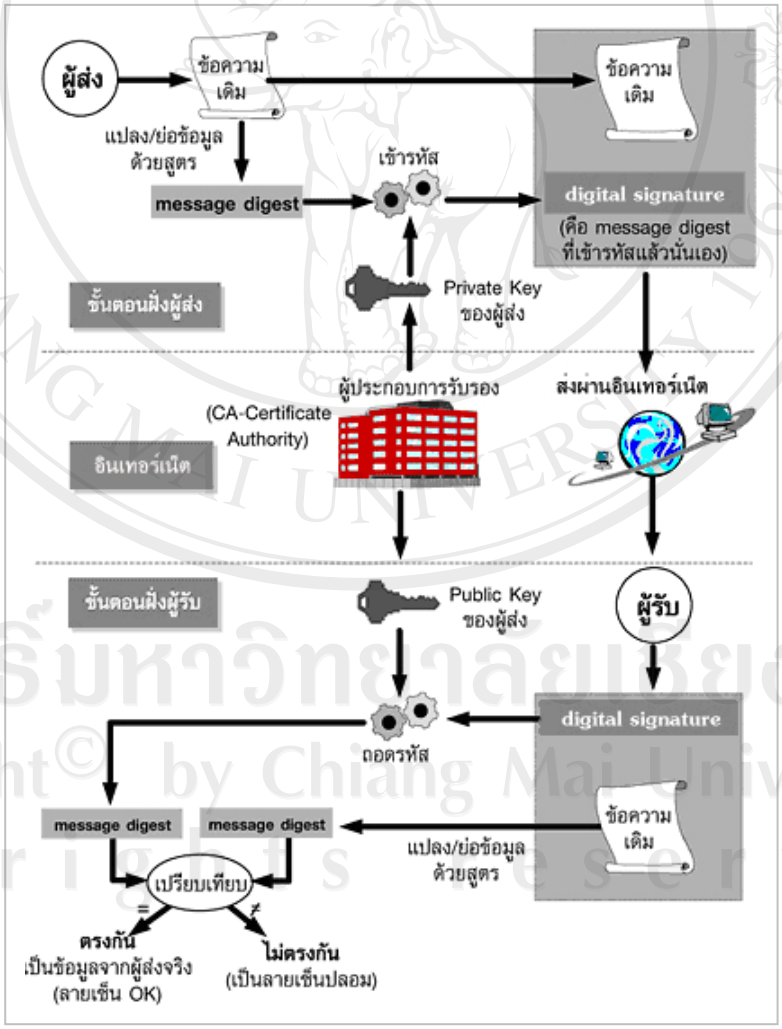
กระบวนการสร้างและลงลายมือชื่อดิจิทัล

1. เริ่มจากการนำข้อมูลอิเล็กทรอนิกส์ต้นฉบับที่จะส่งไปนั้นมาผ่านกระบวนการคณิตศาสตร์ที่เรียกว่า ฟังก์ชันย่อยข้อมูล (Hash Function) เพื่อให้ได้ข้อมูลที่สั้นๆ ที่เรียกว่า ข้อมูลที่ย่อยแล้ว (Digest) ก่อนที่จะทำการเข้ารหัส เนื่องจากข้อมูลต้นฉบับมักจะมีความยาวมากซึ่งจะทำให้กระบวนการเข้ารหัสใช้เวลานานมาก

2. จากนั้นจึงทำการเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่งเอง ซึ่งจุดนี้เปรียบเสมือนการลงลายมือชื่อของผู้ส่งเพราะผู้ส่งเท่านั้นที่มีกุญแจส่วนตัวของผู้ส่งเอง และจะได้ข้อมูลที่เข้ารหัสแล้ว เรียกว่า ลายมือชื่อดิจิทัล

3. จากนั้นก็ทำการส่งลายมือชื่อไปพร้อมกับข้อมูลต้นฉบับไปยังผู้รับ ผู้รับจะทำการตรวจสอบว่าข้อมูลที่ได้รับถูกแก้ไขระหว่างทางหรือไม่ โดยการนำข้อมูลต้นฉบับที่ได้รับมาผ่านกระบวนการย่อยด้วยฟังก์ชันย่อยข้อมูล จะได้ข้อมูลที่ย่อยแล้วชุดที่หนึ่ง

4. นำลายมือชื่อดิจิทัล มาทำการถอดรหัสด้วยกุญแจสาธารณะของผู้ส่ง ก็จะได้ข้อมูลที่ย่อยแล้วชุดที่สองแล้วทำการเปรียบเทียบ ข้อมูลที่ย่อยแล้วทั้งสองชุด ถ้าหากว่าเหมือนกันแสดงว่าข้อมูลที่ได้รับนั้นไม่ได้ถูกแก้ไข แต่ถ้าข้อมูลที่ย่อยแล้วแตกต่างกัน ก็แสดงว่าข้อมูลที่ได้รับถูกเปลี่ยนแปลงข้อมูลระหว่างทาง



รูป 2.4 กระบวนการสร้างและลงลายมือชื่อดิจิทัล

โปรแกรมสำหรับสร้างลายมือชื่อดิจิทัลมีอยู่หลายโปรแกรม แต่ที่นิยมใช้คือ Pretty Good Privacy (PGP) ซึ่งเป็นโปรแกรมช่วยในการรักษาความลับของเนื้อความในอีเมล์และไฟล์ได้โดยการเข้ารหัสเพื่อให้ผู้รับที่ระบุไว้เท่านั้นสามารถเปิดอ่านได้ นอกจากนี้ยังสามารถเซ็นรับรองข้อความในอีเมล์ และไฟล์เพื่อให้แน่ใจว่าข้อความและไฟล์เหล่านั้นไม่ได้ถูกปลอมแปลงมาด้วย PGP อาศัยหลักการของการเข้ารหัสซึ่งเป็นที่ยอมรับและรู้จักกันดีคือ การเข้ารหัสแบบอสมมาตร ซึ่งประกอบด้วยกุญแจ 2 ชุดสำหรับการติดต่อสื่อสารกันอย่างปลอดภัย ชุดหนึ่งเรียกว่ากุญแจส่วนตัว หรือ ไพรเวทคีย์ ส่วนอีกชุดหนึ่งเรียกว่า กุญแจสาธารณะหรือพับลิคคีย์ ในการส่งอีเมล์ถึงผู้รับ ผู้ส่งต้องใช้พับลิคคีย์ของผู้รับในการเข้ารหัส ซึ่งผู้รับเท่านั้นที่สามารถถอดรหัสด้วยไพรเวทคีย์ของตนเองเพื่ออ่านข้อความ นอกจากนี้ ผู้ส่งยังสามารถใช้ไพรเวทคีย์ของตนเองในการเซ็นรับรองอีเมล์ไปยังผู้รับ เมื่อผู้รับได้รับอีเมล์ก็จะใช้ พับลิคคีย์ของผู้ส่งในตรวจสอบให้แน่ใจว่ามาจากผู้ส่งจริงโดยไม่ได้ถูกลักลอบแก้ไขเปลี่ยนแปลงระหว่างทาง
(http://thaicert.nectec.or.th/paper/encryption/pgp.php : 7 กุมภาพันธ์ พ.ศ. 2551)

2.1.3 ประโยชน์และการประยุกต์ใช้ลายมือชื่อดิจิทัล

ประโยชน์ของลายมือชื่อดิจิทัล

1. สามารถ ระบุตัวบุคคล และ เป็นกลไกการป้องกันการปฏิเสธความรับผิดชอบ
2. สามารถป้องกันข้อมูลที่ส่งไปไม่ให้ถูกแก้ไข หรือ หากถูกแก้ไขไปจากเดิมก็สามารถรู้ได้

(CAT-CA (Certification Authority), 2544:ระบบออนไลน์) การประยุกต์ใช้ลายมือชื่อดิจิทัล

1. การส่งจดหมายอิเล็กทรอนิกส์ (Electronic Mail) โดยนำลายมือชื่อดิจิทัลแนบไปกับการส่งข้อมูลระหว่างผู้ส่งและผู้รับผ่านจดหมายอิเล็กทรอนิกส์ เพื่อเพิ่มความปลอดภัยในการส่งข้อมูล และสามารถยืนยันตัวตนของผู้ส่งได้
2. Online Banking, Trading, Shopping สำหรับ Online Banking หรือ ธนาคารออนไลน์ คือการให้บริการของทางธนาคารผ่านระบบอินเทอร์เน็ต เช่น บริการโอนเงิน บริการสอบถามสถานะเช็ค บริการชำระสินค้าและบริการ บริการชำระบัตรเครดิต เป็นต้น มีการนำเอาลายมือชื่อดิจิทัลไปใช้เพื่อให้ความคุ้มครองผู้ใช้บริการในด้านความปลอดภัยของข้อมูลของผู้ใช้ และ ใช้ในการยืนยันตัวตนของธนาคารและผู้ใช้บริการ สำหรับ Trading และ shopping เป็นการค้าขายสินค้าและบริการ และ การซื้อสินค้าและบริการ ผ่านระบบอินเทอร์เน็ต มีการนำลายมือชื่อดิจิทัลมาใช้เพื่อสร้างความปลอดภัยของข้อมูลที่ส่งผ่านระบบอินเทอร์เน็ตระหว่างผู้ซื้อและผู้ขาย และใช้ในการยืนยันตัวตนของผู้ซื้อและผู้ขาย

3. E-Government หรือ รัฐบาลอิเล็กทรอนิกส์ คือการให้บริการของภาครัฐผ่านระบบอินเทอร์เน็ต มีการนำลายมือชื่อดิจิทัลเข้ามาใช้ในส่วนของการสร้างความปลอดภัยของการให้บริการต่าง ๆ ของภาครัฐ ไม่ว่าจะเป็นการส่งผ่านข้อมูล และการยืนยันตัวตน ระหว่างภาครัฐกับผู้ใช้บริการ

4. Web Based Application คือ Application ที่ใช้งานผ่านระบบอินเทอร์เน็ต มีการนำลายมือชื่อดิจิทัลไปช่วยในส่วนของการส่งผ่านข้อมูลบนระบบอินเทอร์เน็ต เพื่อให้การส่งผ่านข้อมูลมีความปลอดภัย และสามารถยืนยันตัวตนของผู้ส่งข้อมูลได้

5. VPN หรือ เครือข่ายเสมือนส่วนตัว มีการนำเอาลายมือชื่อดิจิทัลไปใช้ในการสร้างความปลอดภัยในการส่งแพ็กเก็ตข้อมูลผ่านเครือข่ายเฉพาะขององค์กร โดยการเข้ารหัสแพ็กเก็ตข้อมูลก่อนทำการส่ง และเมื่อไปถึงฝั่งรับ จะมีการถอดรหัสเพื่อตรวจสอบแพ็กเก็ตข้อมูลที่ส่งมา

2.2 แนวความคิดเกี่ยวกับการประมวลผลภาพ (Image Processing)

2.2.1 การประมวลผลภาพ

(Wikipedia, 2544:ระบบออนไลน์) การประมวลผลภาพ เป็นการประยุกต์ใช้งานการประมวลผลสัญญาณบนสัญญาณ 2 มิติ เช่น ภาพนิ่ง (ภาพถ่าย) หรือ ภาพวีดิทัศน์ (วีดิโอ) และยังรวมถึงสัญญาณ 2 มิติอื่นๆ ที่ไม่ใช่ภาพด้วย เมื่อหลายสิบปีมาแล้ว การประมวลผลภาพนั้น จะอยู่ในรูปของการประมวลผลสัญญาณแอนะล็อก (analog) โดยใช้อุปกรณ์ปรับแต่งแสง (optics) ซึ่งวิธีเหล่านั้นก็ไม่ได้หายสาบสูญ หรือเลิกใช้ไป ยังมีใช้เป็นส่วนสำคัญ สำหรับการประยุกต์ใช้งานบางอย่าง เช่น ฮอโลกราฟี (holography) แต่เนื่องจากอุปกรณ์คอมพิวเตอร์ในปัจจุบัน ราคาถูกลงและเร็วขึ้นมาก การประมวลผลภาพดิจิทัล (Digital Image Processing) จึงได้รับความนิยมมากกว่า เพราะการประมวลผลที่ทำได้ซับซ้อนขึ้น แม่นยำ และง่ายในการลงมือปฏิบัติ

2.2.2 การประมวลผลภาพดิจิทัล

วนัสนันท์ ทองกฤษณ์ (2547) การประมวลผลภาพดิจิทัลเป็นซับคลาส (Subclass) ของการประมวลผลสัญญาณ กล่าวคือ การประมวลผลสัญญาณภาพดิจิทัลเป็นการประมวลผลสัญญาณที่มีอินพุตของระบบเป็นภาพเท่านั้น โดยวัตถุประสงค์ของการประมวลผลภาพแบ่งออกเป็นสองประเภทใหญ่ ๆ คือ การปรับปรุงคุณภาพเพื่อให้มนุษย์สามารถมองเห็นรายละเอียดของภาพได้ชัดเจนมากขึ้น (Image Quality Improvement) และเพื่อให้เครื่องคอมพิวเตอร์สามารถตีความภาพได้ (Computer Interpretation)

ที่มาของการประมวลผลภาพดิจิทัลเริ่มต้นจากแอพพลิเคชันแรกของอุตสาหกรรมหนังสือพิมพ์ โดยเป็นการส่งข้อมูลภาพที่ถูกเข้ารหัส (Coding) ด้วยอุปกรณ์การพิมพ์พิเศษ ที่มีจุดประสงค์ในการลดเวลาส่งถ่ายข้อมูลผ่านสายเคเบิล การส่งภาพผ่านสายเคเบิลใต้น้ำครั้งแรกระหว่างเมืองลอนดอน ประเทศอังกฤษ ไปสู่ เมืองนิวยอร์ก ประเทศสหรัฐอเมริกา ทำให้ระยะเวลาในการส่งผ่านข่าวแทนการส่งแบบดั้งเดิมที่ใช้เวลาเป็นอาทิตย์กลายเป็นใช้เวลาน้อยกว่าสามชั่วโมง อุปกรณ์ปลายทางจะทำการถอดรหัสข้อมูล (Decoding) แล้วสร้างเป็นภาพเหมือนต้นฉบับขึ้นมา วิธีการเข้ารหัสแบบนี้เรียกว่า รูปแบบฮาฟโทน (Halftone Pattern)

หลังจากนั้นเทคโนโลยีการประมวลผลภาพดิจิทัลก็ถูกพัฒนาเพิ่มขึ้นเรื่อยๆ ประวัติการพัฒนาของเทคโนโลยีด้านนี้ผูกติดกับการพัฒนาดิจิทัลคอมพิวเตอร์เป็นอย่างมาก เนื่องจากการประมวลผลภาพนั้นมีความต้องการเนื้อที่ในการเก็บข้อมูลและความเร็วในการประมวลผลสูง ทำให้การพัฒนาขึ้นอยู่กับความเร็วของหน่วยประมวลผลกลาง (Central Processing Unit, CPU) หน่วยความจำสำรอง (Data Storage) และการส่งถ่ายข้อมูล (Data Transmission)

หลังจากที่เทคโนโลยีคอมพิวเตอร์ได้รุดหน้าถึงขั้นที่เราสามารถประมวลผลภาพได้อย่างรวดเร็ว ก็ได้มีการนำเอาทฤษฎีการประมวลผลภาพไปประยุกต์ใช้กับงานด้านอวกาศ ไม่ว่าจะเป็นการส่งผ่านภาพถ่ายดวงจันทร์ผ่านยานอวกาศ โดยภาพที่ส่งมานั้นถูกประมวลผลด้วยคอมพิวเตอร์เพื่อทำการแก้ไขส่วนข้อมูลที่ผิดเพี้ยน อันเกิดขึ้นในกระบวนการส่งภาพหรือรับภาพ นอกจากนี้ก็ได้มีการนำเทคโนโลยีไปใช้กับงานด้านภาพทางการแพทย์ (Medical Imaging) งานด้านการสำรวจโลกสำรวจอวกาศ การนำมาใช้ในอุตสาหกรรม เช่น การตรวจสอบความสมบูรณ์ของผลิตภัณฑ์ งานด้านอาชญากรรม งานสำรวจสภาพอากาศและพยากรณ์อากาศ งานด้านธรณีวิทยา เช่น การตรวจสอบการสั่นสะเทือนของเปลือกโลก

2.2.3 รูปร่างของภาพ (Image Shape)

วัตถุที่มีอยู่ตามธรรมชาติและที่มนุษย์สร้างขึ้นมีรูปร่างที่แตกต่างกันไป ทั้งที่เป็นรูปทรงเรขาคณิตและไม่เป็นรูปทรงเรขาคณิต ในศาสตร์ของการประมวลผลภาพนั้น การกำหนดขอบเขตของภาพทุกภาพให้อยู่ในรูปสี่เหลี่ยม (Rectangular image model) เป็นวิธีที่นิยมใช้กันมากที่สุด เนื่องจากทำให้การอ่านภาพ การจัดเก็บข้อมูลภาพในหน่วยความจำ และการแสดงภาพออกทางอุปกรณ์ต่าง ๆ เป็นไปได้อย่างมีประสิทธิภาพ

การเก็บข้อมูลภาพลงหน่วยความจำของคอมพิวเตอร์สามารถทำได้โดยการจองหน่วยความจำของเครื่องไว้ในรูปของตัวแปรอะเรย์ (array) โดยค่าในแต่ละช่องของอะเรย์แสดงถึงคุณสมบัติของจุดภาพ (pixel) และตำแหน่งของช่องอะเรย์เป็นตัวกำหนดตำแหน่งของจุดภาพ สมมุติให้ Image เป็นตัวแปรแบบอะเรย์ขนาด M X N (M แถว และ N คอลัมน์) ที่ใช้เก็บภาพขนาด

M x N จุด (M จุดในแนวนอน และ N จุดในแนวตั้ง) ค่าสี (หรือความสว่าง ในกรณีที่เป็นภาพ grey level) ของจุดภาพในแถวที่ 5 คอลัมน์ที่ 4 จะตรงกับค่าของ Image(5,4) จะเห็นว่าเราใช้ตำแหน่งของจุดภาพทั้งสองแกนเป็นตัวชี้ค่าข้อมูลในอะเรย์ จากการใช้หน่วยความจำเพื่อการเก็บภาพในลักษณะที่กล่าวมา เนื้อที่ในการเก็บภาพสามารถคำนวณได้จาก M x N x g เมื่อ g เป็นจำนวนเต็มที่แทนจำนวนบิตของข้อมูลในแต่ละจุดภาพ ตัวอย่างถ้า g มีค่าเท่ากับ 8 บิต เราจะสามารถเก็บความแตกต่างของระดับสีที่เป็นไปสูงสุด 256 ระดับ ค่า M และ N จะเป็นตัวบอกถึงความละเอียดของภาพ สำหรับคอมพิวเตอร์ทั่วไปในระบบ VGA (Video Graphic Array) จะมีขนาด 640x480 800x600 และ 1024x768 จุด เป็นต้น การกำหนดความละเอียดจะขึ้นอยู่กับงานที่จะใช้ ในงานบางอย่างใช้ความละเอียดแค่ 30x50 จุด ก็พอแล้ว แต่ในงานบางชนิดใช้ความละเอียดถึง 1000x1000 จุด ก็ยังไม่พอ ปกติแล้วในการเก็บข้อมูลภาพโดยเครื่องมือต่าง ๆ จะเก็บตามมาตรฐานของโทรทัศน์ซึ่งมีอัตราส่วน x ต่อ y เท่ากับ 4 :3 สำหรับเครื่องมือเก็บข้อมูลภาพที่ไม่เป็นไปตามอัตราส่วน 4 :3 เมื่อนำภาพนี้ไปแสดงในจอภาพมาตรฐานจะทำให้ภาพที่แสดงนั้นมีขนาดของจุดภาพไม่เป็นสีเหลี่ยมจัตุรัสเช่นในบางระบบอาจจะใช้ความละเอียดในการแสดงเท่ากับ 640x512 ซึ่งจะทำให้ขนาดของจุดภาพที่ได้มีขนาดของด้านกว้างมีความยาวมากกว่าด้านสูง ซึ่งลักษณะดังกล่าวนี้เป็นหัวข้อที่ต้องสนใจสำหรับการเขียนโปรแกรมทางด้านกราฟิกและการจัดการข้อมูลจำนวนสีสูงสุดที่เป็นไปได้ของแต่ละจุดภาพขึ้นอยู่กับจำนวนบิตที่ใช้ เมื่อมีการกำหนดให้ขนาดของบิตต่อจุด มากขึ้นจะทำให้จำนวนของสีมากขึ้นด้วย สำหรับการแสดงข้อมูลภาพที่มีขนาด 1 บิตและ 8 บิตนั้นจะมีการทำงานที่จะใกล้เคียงกันเนื่องจากหน่วยประมวลผลจะไม่สามารถจัดการกับข้อมูลที่เป็นบิตเดี่ยว ๆ ได้ดังนั้นในการแสดงข้อมูลออกทางจอภาพตัวโปรเซสเซอร์จะทำการคัดลอกข้อมูลทั้ง 8 บิต (1 Byte) ส่งให้กับจอภาพซึ่งในกรณีที่ Pixel มีขนาด 1 บิต เมื่อโปรเซสเซอร์จะทำงานกับบิตแรกที่ต้องการแล้วก็จะทำการคัดลอกข้อมูลชุดใหม่ทันทีโดยที่ไม่เกี่ยวกับข้อมูลอีก 7 บิตที่เหลือส่วนในกรณี Pixel ที่มีขนาด 8 บิต โปรเซสเซอร์จะทำการคัดลอกข้อมูลจุดใหม่ก็ต่อเมื่อโปรเซสเซอร์ทำงานกับทุกบิตแล้ว ตัวอย่างสำหรับระบบที่มีความละเอียดเท่ากับ 800x600 และมีขนาด 16 บิตต่อ Pixel จะสามารถแสดงสีได้ทั้งหมด 65536 ระดับและต้องใช้เนื้อที่ในการเก็บเท่ากับ 800x600x16 บิต

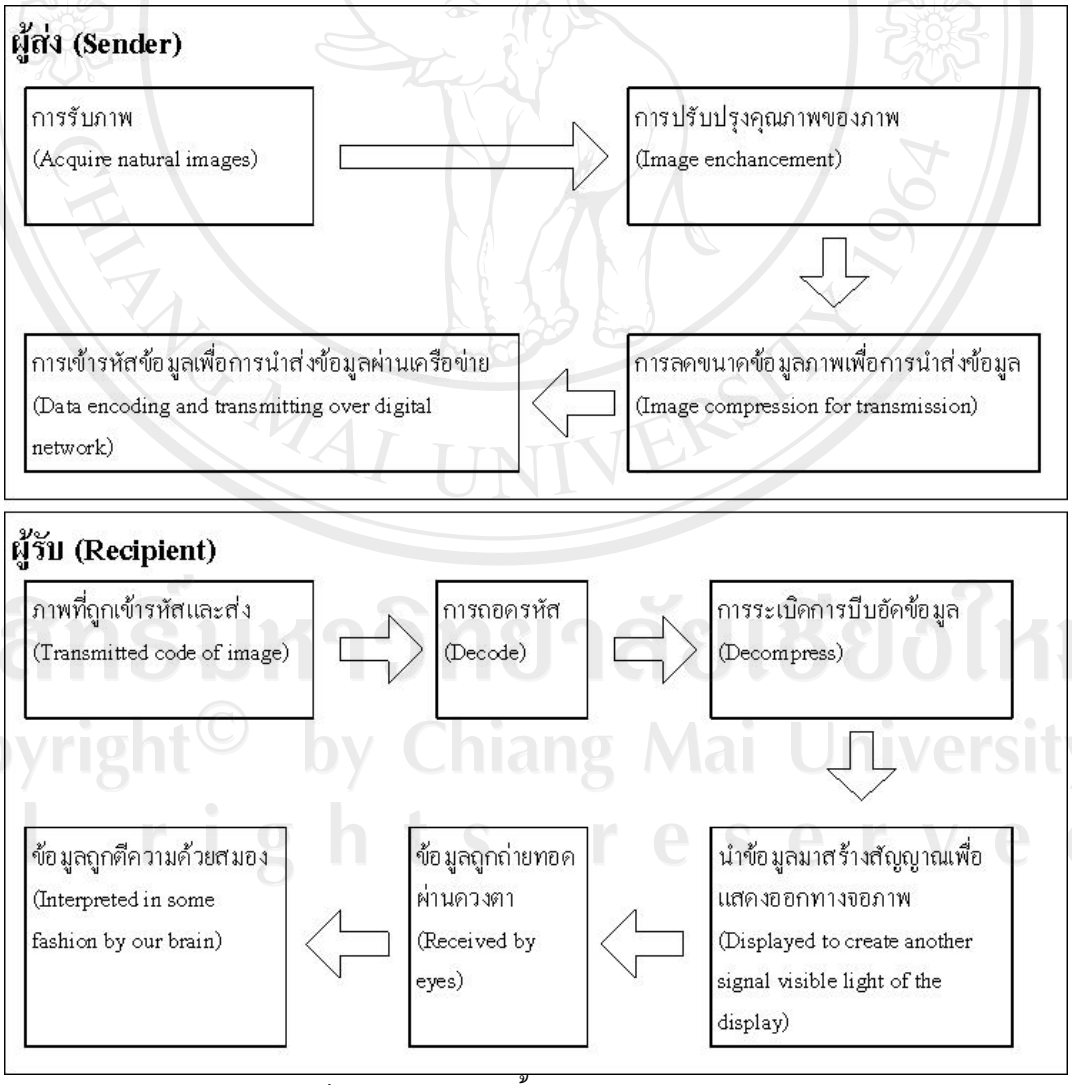
2.2.4 มาตรฐานของสี

มาตรฐานของสีที่ใช้อยู่ในปัจจุบันมีอยู่หลายระบบด้วยกัน ทั้งนี้จะขึ้นอยู่กับการนำไปใช้ แต่โดยทั่วไปแล้วทุกมาตรฐานจะมีแนวคิดเดียวกันคือ การแทนจุดสีด้วยจุดที่อยู่ภายในสเปส 3 มิติ โดยจะมีแกนอ้างอิงสำหรับจุดสีนั้นในสเปสซึ่งแต่ละแกนจะมีความเป็นอิสระต่อกัน ตัวอย่างเช่นในระบบ RGB จะมีแกนสีคือ แกนสีแดง เขียว และน้ำเงินในระบบ HLS จะมีแกนเป็น ค่าสี (hue)

ความสว่าง (lightness) และความบริสุทธิ์ของสี (saturation) ตัวอย่างระบบสีที่นิยมใช้กันได้แก่ ระบบ RGB HSV (Hue Saturation Value) และ HLS (Hue Lightness Saturation)

2.2.5 ขั้นตอนในการประมวลผลสัญญาณภาพดิจิทัล

เริ่มตั้งต้นตั้งแต่การรับสัญญาณภาพจากธรรมชาติเข้าระบบซึ่งอินพุตของระบบนี้คือรูปภาพนั่นเอง ส่วนเอาต์พุตของการประมวลผลภาพถูกแบ่งออกเป็นสองประเภทขึ้นอยู่กับวัตถุประสงค์ของการประมวลผล กล่าวคือ หากการประมวลผลคือการปรับปรุงคุณภาพของภาพอินพุตให้ดีขึ้นเพื่อให้มนุษย์สามารถมองเห็นรายละเอียดภายในภาพได้ชัดเจนมากขึ้น เอาต์พุต คือภาพที่ถูกปรับคุณภาพแล้วนั่นเอง แต่หากวัตถุประสงค์คือ การทำให้คอมพิวเตอร์สามารถรู้จำภาพได้ เอาต์พุตของระบบอาจเป็นข้อมูลองค์ประกอบลักษณะสำคัญของภาพที่ได้ผ่านขั้นตอนการแยกส่วน (Segmentation) เพื่อนำไปเป็นอินพุตให้กับโปรแกรมรู้จำของคอมพิวเตอร์ต่อไป



รูป 2.5 แสดงไดอะแกรมสรุปขั้นตอนการประมวลผลภาพดิจิทัล

จากรูปเป็นไดอะแกรมสรุปขั้นตอนการประมวลผลภาพดิจิทัล แต่ถึงแม้ขั้นตอนในการประมวลผลภาพมีอยู่หลายขั้นตอน แต่ไม่ได้หมายความว่าทุกขั้นตอนในไดอะแกรมจะถูกนำมาใช้ทั้งหมด ขั้นตอนแต่ละชั้นตอนนั้นมีวัตถุประสงค์เฉพาะ ดังนั้นในการทำงานกับภาพนั้นเราอาจเลือกใช้เฉพาะบางขั้นตอนตามต้องการได้ ทั้งนี้ทั้งนั้นผลลัพธ์ที่ได้จากการเลือกใช้ขั้นตอนที่ต่างกันก็ย่อมต่างกันไปด้วย

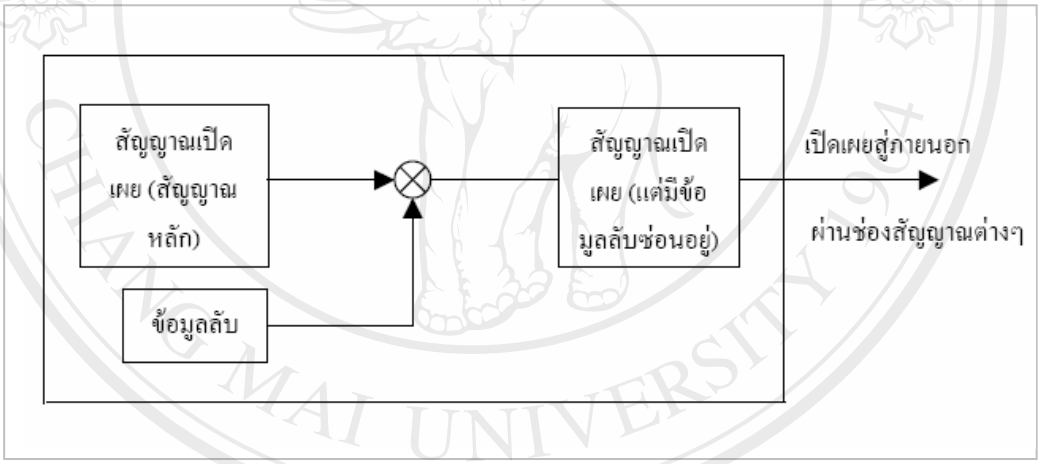
2.3 การซ่อนข้อมูล (Steganography) และ การซ่อนข้อมูลไว้ในภาพ

2.3.1 การสื่อสารข้อมูล

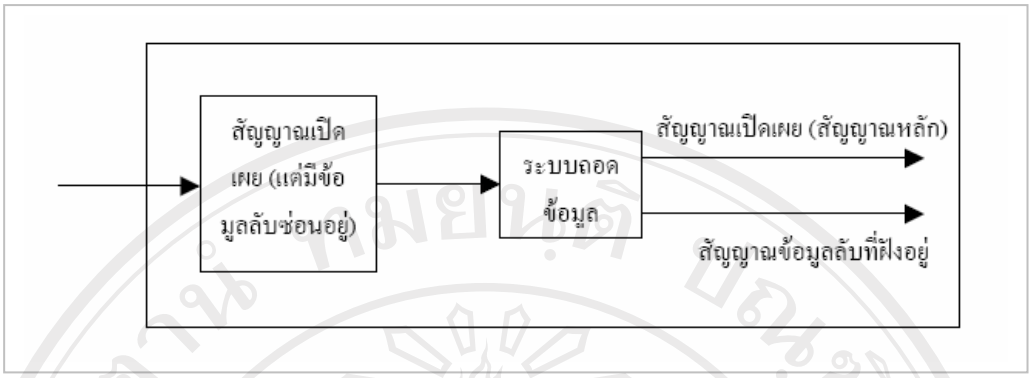
การสื่อสารข้อมูลโดยทั่วไป สามารถแบ่งแยกประเภทออกได้เป็นสองรูปแบบ กล่าวคือ การสื่อสารแบบเปิดเผย และ การสื่อสารแบบปกปิด โดยการสื่อสารแบบเปิดเผยนั้นคือ การสื่อสารโดยทั่วไปที่เรากระทำอยู่ เป็นการสื่อสารที่บุคคล(หรืออุปกรณ์)สองกลุ่มติดต่อแลกเปลี่ยนข้อมูลกันโดยไม่สนใจพิจารณาว่าจะมีบุคคลที่สามเข้ามาฟังหรือรับทราบข้อมูลที่สื่อสารกันอยู่หรือไม่ ในทางตรงกันข้าม การสื่อสารแบบปกปิด จะเป็นการสื่อสารที่บุคคล(หรืออุปกรณ์) ติดต่อส่งข้อมูลเฉพาะให้แก่กันและกัน โดยอาศัยวิธีการบางประการเพื่อป้องกันมิให้บุคคลที่สาม ที่ไม่เกี่ยวข้องสามารถเข้าถึงข้อมูลนั้นได้ วิธีการสื่อสารแบบปกปิดนี้ ยังสามารถแบ่งอย่างกว้างๆออกได้เป็นสองประเภท คือ การสื่อสารแบบปกปิดประเภทไม่ซ่อนเร้นและการสื่อสารแบบปกปิดประเภทซ่อนเร้น ตัวอย่างของการสื่อสารแบบปกปิดประเภทไม่ซ่อนเร้น ก็คือวิธีการเข้ารหัสข้อมูล (Encryption) นั่นเอง การสื่อสารประเภทนี้ข้อมูลจะถูกเข้ารหัสโดยยอมให้บุคคล (หรืออุปกรณ์) สองฝ่ายที่เกี่ยวข้องเท่านั้นที่สามารถถอดรหัสและเข้าใจความหมายที่แท้จริงของข้อมูลข่าวสารได้ โดยที่บุคคลที่สามที่ไม่เกี่ยวข้องและไม่ได้รับอนุญาต แม้จะรู้เห็นว่ามีการติดต่อส่งข้อมูลระหว่างบุคคลทั้งสองฝ่ายเกิดขึ้น ก็จะไม่สามารถถอดรหัสข้อมูลหรือรับทราบเนื้อหาของข้อมูลนั้นได้ อย่างไรก็ตามด้วยวิธีการสื่อสารประเภทนี้ความลับหรือความเป็นส่วนตัวของข้อมูลของการสื่อสารแบบปกปิด จะขึ้นกับวิธีการและกุญแจ (Key) ที่ใช้ในการเข้า/ถอดรหัส ดังนั้นจึงอาจเป็นไปได้ที่บุคคลที่สามที่ไม่เกี่ยวข้องจะสามารถถอดรหัสเข้าไปถึงเนื้อหาจริงได้ ด้วยเหตุนี้จึงเกิดแนวคิดการเข้ารหัสแบบปกปิดอีกประเภทหนึ่งคือ การเข้ารหัสข้อมูลแบบซ่อนเร้นหรือการซ่อนข้อมูลเกิดขึ้น กล่าวคือเป็นการสื่อสารแบบปกปิดประเภทนี้ไม่ยอมแม้แต่จะให้บุคคลที่สามทราบได้ว่ามีการสื่อสารเกิดขึ้นระหว่างบุคคล (หรืออุปกรณ์) สองกลุ่ม

2.3.2 หลักการและวิธีการซ่อนข้อมูล

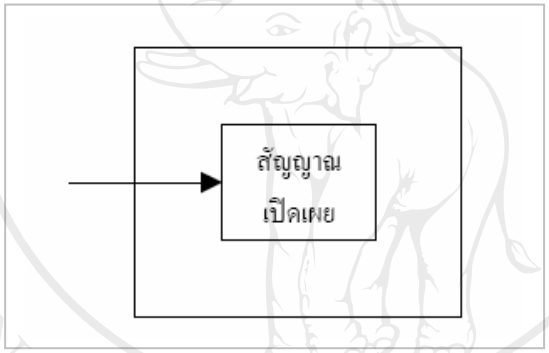
เพื่อที่จะซ่อนเร้นข้อมูลลับโดยมิให้บุคคลที่สามรับรู้ ผู้ทำการสื่อสารทั้งสองฝ่ายจะใช้วิธีการลวงให้บุคคลที่สาม เข้าใจว่ามีการสื่อสารแบบเปิดเผยขึ้นระหว่างบุคคลทั้งสองฝ่าย โดยที่ความเป็นจริงแล้ว บุคคลที่เกี่ยวข้องทั้งสองฝ่ายได้ทำการซ่อนข้อมูลที่สัมผัสหรือรับรู้ไม่ได้ (ไม่เห็น ไม่ได้ยิน ไม่เข้าใจ) เข้าไปในข้อมูลการสื่อสารแบบเปิดเผย วิธีการที่จะซ่อนข้อมูลประเภทนี้โดยทั่วไปแล้ว จะอาศัยช่องโหว่ที่ว่าสัญญาณทั่วไปที่เกิดตามธรรมชาติ เช่น สัญญาณข้อมูล สัญญาณภาพ สัญญาณวิดีโอ หรือ สัญญาณเสียง จะมีสัญญาณรบกวน (Noise) ที่ไม่พึงประสงค์เข้ามาปนในสัญญาณหลักและยากต่อการขจัดหรือทำลายออกไป ดังนั้นถ้าสามารถแปลงข้อมูลลับที่ต้องการสื่อสารให้อยู่ในรูปของ สัญญาณรบกวนเสมือน (Pseudo Noise) และ ออกแบบวิธีโดยทำการปนสัญญาณเสมือนนี้เข้าไปในสัญญาณข้อมูลเปิดเผย (สัญญาณหลัก) ที่แนบเนียนได้ ก็จะเป็นการยากที่บุคคลที่สามจะแยกแยะหรือรับรู้ได้ถึงข้อมูลที่ซ่อนเร้นอยู่



รูป 2.6 แสดงถึงแบบจำลองระบบการซ่อนข้อมูลลับเข้าไปในสัญญาณหลัก
ระบบการซ่อนข้อมูลด้านผู้ส่ง



รูป 2.7 แสดงถึงแบบจำลองระบบการซ่อนข้อมูลลับเข้าไปในสัญญาณหลัก ระบบการถอดข้อมูลด้านผู้รับ (ที่ต้องการส่งข้อมูลให้)



รูป 2.8 ข้อมูลเปิดเผยที่บุคคลที่สามรับได้เป็นแค่สัญญาณเปิดเผยทั่วไปไม่มีความหมายอะไร

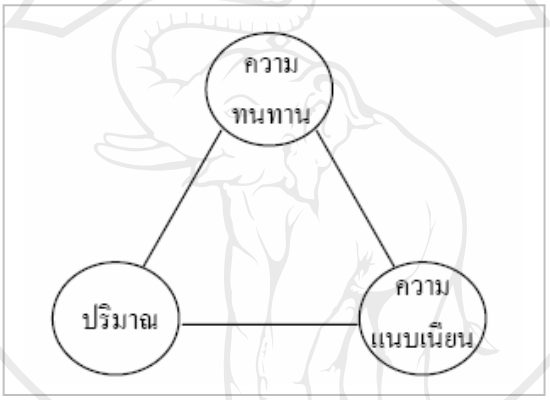
2.3.3 ข้อพิจารณาทั่วไปในการออกแบบระบบ

การออกแบบระบบการซ่อนข้อมูล โดยทั่วไปจะมีข้อพิจารณาอยู่หลายประการตามแต่จุดประสงค์และความมุ่งหมายของการใช้ประโยชน์ เช่น

1. ความแนบเนียน ความแนบเนียน หมายถึง การที่ระบบซ่อนข้อมูลสามารถซ่อนข้อมูลลับได้โดยไม่ทำให้ข้อมูลเดิม(สัญญาณหลัก)เกิดความเสียหายในระดับที่สายตามนุษย์หรือเครื่องจักร อุปกรณ์ ไม่สามารถตรวจจับหรือรับรู้ได้ เช่นถ้าฝังข้อมูลลับลงบนภาพ ภาพที่ถูกฝังเรียบร้อยแล้วจะต้องมีลักษณะเช่นเดียวกับภาพเดิมที่ไม่ได้ถูกฝังข้อมูล หรือไม่มีการสูญเสียคุณภาพทางสายตา เป็นต้น

2. ปริมาณ ปริมาณ หมายถึง ปริมาณของข้อมูลลับที่สามารถฝังเข้าไปในข้อมูลหลักได้

3. ความทนทาน เนื่องจากในขั้นตอนการซ่อนฝังข้อมูลลับลงในข้อมูลหลัก ข้อมูลลับจะถูกแปลงเปลี่ยนไปในรูปของสัญญาณรบกวนที่มีพลังงานต่างซึ่งอาจเป็นไปได้ที่สัญญาณข้อมูลลับจะถูกทำลายหรือกำจัดไปได้โดยง่าย ดังนั้นในการออกแบบระบบการซ่อนข้อมูลจะต้องพิจารณาด้วยว่าจะใช้วิธีการใดจึงจะสามารถซ่อนฝังข้อมูลลับให้ติดแน่นอยู่ในสัญญาณหลักได้อย่างไรก็ตามความยากในการออกแบบระบบซ่อนข้อมูลจะอยู่ตรงประเด็นที่ว่า ทำอย่างไรจึงจะสามารถออกแบบระบบให้เป็นไปตามความต้องการตามข้อกำหนดทั้งสามข้อได้ ในขณะที่ความต้องการทั้งสามมีความขัดแย้งกันอยู่



รูป 2.9 ความขัดแย้งระหว่างความต้องการด้านความทนทาน ปริมาณ และ ความแนบเนียน

ตัวอย่างเช่น ถ้าต้องการระบบซ่อนข้อมูลที่ฝังข้อมูลลับได้ในปริมาณมากนั้น เสมือนกับว่า ระบบจะต้องใส่สัญญาณรบกวนเข้าไปในสัญญาณหลักมากขึ้น หรืออีกนัยหนึ่งจะหมายความว่าระบบจะสูญเสียความแนบเนียน (สัญญาณเดิมถูกรบกวนมากขึ้น) ไปนั่นเอง

2.3.4 แนวทางการนำไปใช้ประโยชน์

เป็นที่คาดกันว่าหลักการของการซ่อนข้อมูลจะสามารถนำไปประยุกต์ใช้ประโยชน์ได้ในหลายทิศทาง เช่น

1. การสื่อสารทางลับ เป็นการส่งข้อมูลลับผ่านระบบการสื่อสารแบบเปิดเผยโดยที่ลวงไม่ให้ผู้ที่ไม่เกี่ยวข้องรับทราบได้ ซึ่งอาจกระทำโดยซ่อนข้อมูลลับในสื่อทั่วไป เช่นซ่อนฝังในรูปภาพ หรือ เสียง แล้วส่งผ่านทางอินเทอร์เน็ต

2. การป้องกันสิทธิและทรัพย์สินทางปัญญา ข้อมูลลับจะถูกฝังเข้าไปในสัญญาณที่มีค่าทรัพย์สินทางปัญญาและต้องการที่จะได้รับการคุ้มครอง เช่น สัญญาณภาพดิจิทัลและเสียงเพลง

โดยมีวัตถุประสงค์ที่จะนำข้อมูลลับดังกล่าวไปใช้ยืนยันความเป็นเจ้าของดั่งเดิมที่แท้จริง แน่นอนในกรณีนี้ข้อมูลลับจะต้องถูกฝังให้มีความทนทาน ไม่ว่าสัญญาณข้อมูลหลักจะถูกเปลี่ยนแปลงเพียงใด (จนถึงระดับที่สัญญาณหลักยังคงคุณค่าอยู่ได้) ข้อมูลลับจะต้องคงอยู่และสามารถถอดกลับมาใช้ยืนยันได้

3. ใช้ยืนยันความเป็นของแท้ เนื่องจากในอนาคตจะมีความเป็นไปได้สูงที่ข้อมูลเอกสารที่มีความสำคัญ จะถูกนำมาใช้หรือเก็บหรือส่งผ่านระบบเครือข่ายคอมพิวเตอร์แน่นอน ปัญหาที่จะตามมาก็คือจะเกิดความเสี่ยงอย่างยิ่งที่จะมีผู้ปลอมแปลงหรือเปลี่ยนแปลงรายละเอียดข้อมูลเดิม ซึ่งอาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้ ในกรณีนี้อาจจะประยุกต์ใช้หลักการของการซ่อนข้อมูล โดยซ่อนหรือฝังข้อมูลหรือรหัสลับที่มีความอ่อนแอ ที่จะถูกทำลายได้โดยง่ายเมื่อมีการแก้ไขหรือเปลี่ยนแปลงข้อมูลหลักแม้แต่เพียงเล็กน้อย

4. ข้อมูลเสริม ในบางกรณีถึงแม้จะไม่เป็นการปกปิดข้อมูลโดยตั้งใจ แต่อาจจะเป็นการดีที่จะซ่อนข้อมูลเสริมบางอย่างไว้ที่ข้อมูลหลัก เมื่อยามที่มีความต้องการใช้งาน จึงค่อยเปิดหรือถอดรหัสข้อมูลนั้นๆออกมา ตัวอย่างของความเป็นไปได้ในการประยุกต์ใช้คือ อักษรอธิบาย (Caption) ที่ปรากฏอยู่ด้านล่างของสัญญาณวิดีโอนั่นเอง

การซ่อนข้อมูลมีหลักการพื้นฐานอยู่บนความคิดที่จะซ่อนปกปิดรายละเอียดของข้อมูลลับ โดยไม่ประสงค์ให้บุคคลที่สามรู้ได้แม้แต่การเปิดเผยว่าได้มีการสื่อสารเกิดขึ้นแล้ว เทคนิคการซ่อนข้อมูลสามารถนำมาประยุกต์ใช้งานให้เป็นประโยชน์ได้ในหลายๆรูปแบบ โดยการออกแบบการซ่อนข้อมูลจะต้องพิจารณาถึงวัตถุประสงค์ของการนำไปใช้งานแล้วแต่กรณีไป อย่างไรก็ตามข้อพิจารณาส่วนใหญ่ยังคงอยู่บนหลักการที่ว่า จะสร้างความแนบเนียนได้อย่างไร จะสามารถซ่อนข้อมูลได้มากน้อยเพียงใด และต้องการความแข็งแกร่งทนทานของข้อมูลมากน้อยแค่ไหน

2.3.5 การซ่อนข้อมูลไว้ในภาพ

เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งให้กับผู้รับ ซ่อนไว้ในไฟล์ภาพ เพื่อไม่ให้บุคคลอื่นทราบข้อมูลดังกล่าว

การซ่อนข้อมูลในไฟล์ภาพแบ่งเป็น 2 แบบ คือ

1. การซ่อนข้อมูลที่ต้องการเพียงอย่างเดียว
2. การซ่อนข้อมูลที่ต้องการพร้อมกับรหัสผ่าน

การซ่อนข้อมูลแบบที่ 2 จะมีความปลอดภัยของข้อมูลมากกว่า เนื่องจากในการถอดข้อมูลออกจากไฟล์ภาพจะต้องมีรหัสผ่านซึ่งจะต้องตรงกับรหัสผ่านที่ถูกซ่อนอยู่ในไฟล์ภาพถึงจะสามารถถอดข้อมูลออกจากไฟล์ภาพได้

วิธีการซ่อนข้อมูลในไฟล์ภาพแบ่งออกได้เป็น 2 วิธี คือ

1. การซ่อนข้อมูลไว้ที่ค่าพิกเซลของไฟล์ภาพ

(Least Significant Bit : LSB) คือ บิตที่อยู่ขวามือสุดเป็นบิตที่มีค่าประจำหลักน้อยที่สุด (เป็นวิธีที่นิยมใช้มากที่สุด) หรือ บิตที่มีนัยสำคัญสูงสุด (Most Significant Bit : MSB) คือ บิตที่อยู่ซ้ายมือสุดเป็นบิตที่มีค่าประจำหลักมากที่สุดของพิกเซลของไฟล์ภาพ

การซ่อนข้อมูลไว้ที่บิตที่มีค่าประจำหลักน้อยที่สุดหรือบิตที่อยู่ขวามือสุด เช่น ถ้าต้องการซ่อน “G” โดยใช้ไฟล์ภาพที่มีขนาด 8 ไบต์ จะต้องเปลี่ยนไฟล์ภาพให้อยู่ในรูป ไบนารี ดังนี้

10010101 00001101 11001001 10010110

00001111 11001011 10011111 00010000

จะเห็นว่าบิตที่เป็นตัวหนาจะเป็นบิตที่มีค่าประจำหลักน้อยที่สุดหรือบิตที่อยู่ขวามือสุด จากนั้นจะทำการเปลี่ยน “G” เป็นไบนารี คือ 01000111 และจะนำค่าแต่ละบิตไปแทนที่ค่าบิตที่อยู่ขวามือสุดของแต่ละไบต์ของไฟล์ภาพ ซึ่งแสดงบิตดังกล่าวด้วยตัวเอียง ดังนี้

10010101 00001101 11001000 10010110

00001110 11001011 10011111 00010001

2. การซ่อนข้อมูลไว้ที่ค่าอื่นๆ ที่ไม่ใช่ค่าของพิกเซลของไฟล์ภาพ

(Aelphaeis Mangarae, 2549:ระบบออนไลน์) การซ่อนข้อมูลในภาพ สามารถซ่อนข้อมูลไว้ในประเภทของไฟล์ภาพ ไม่ว่าจะเป็นประเภทไฟล์ .bmp ประเภทไฟล์ .jpg ประเภทไฟล์ .png หรือ ประเภทไฟล์อื่น สำหรับประเภทของไฟล์ภาพที่ดีที่สุดสำหรับการซ่อนข้อมูลคือประเภทไฟล์ .bmp เนื่องมาจากเป็นไฟล์ภาพที่มีขนาดใหญ่และมีคุณภาพสูง มีพื้นที่ว่างที่สามารถซ่อนข้อมูลมากกว่าไฟล์ภาพประเภทอื่น โดยไม่ทำให้ขนาดของไฟล์และคุณภาพของไฟล์เปลี่ยน ทั้งนี้ขนาดของข้อมูลที่จะซ่อนต้องมีความเหมาะสมกับพื้นที่ว่างที่สามารถซ่อนข้อมูลได้ของไฟล์ภาพด้วย

จากการศึกษาการทำงานของลายมือชื่อดิจิทัลและได้ทดลองใช้งานโปรแกรม PGP ผู้ศึกษาได้เลือกใช้โปรแกรม PGP เป็นต้นแบบของกระบวนการสร้างลายมือชื่อดิจิทัล และได้นำเอาการซ่อนข้อมูลในไฟล์ภาพมาประยุกต์ใช้กับกระบวนการสร้างลายมือชื่อดิจิทัล โดยมีการเปลี่ยนแปลงลักษณะของไพรเวทคีย์ พับลิคคีย์ และลายมือชื่อดิจิทัล คือ สร้างออกมาเป็นไฟล์ภาพแทนชุดของอักขระที่โปรแกรม PGP สร้าง ออกมา ในการส่งข้อมูล ชุดของอักขระจะเป็นที่สังเกตได้ง่ายว่าได้ผ่านการเข้ารหัสข้อมูลมา ทำให้เป็นที่น่าสนใจแก่ผู้ที่ไม่ประสงค์ดี ในการที่จะหาวิธีการต่าง ๆ เพื่อทำการถอดรหัสข้อมูลดังกล่าว แต่ถ้าเป็นไฟล์ภาพจะสังเกตด้วยตาเปล่าได้ยาก เนื่องจากไฟล์ภาพที่มีข้อมูลซ่อนอยู่จะไม่แตกต่างจากไฟล์ภาพต้นฉบับ ซึ่งส่งผลดีต่อการส่งข้อมูล สำหรับประเภทของไฟล์ภาพที่นำมาใช้ คือ ประเภทไฟล์ .bmp เนื่องจากเป็นไฟล์รูปภาพที่มีขนาดใหญ่

และมีคุณภาพสูง มีพื้นที่ว่างที่สามารถซ่อนข้อมูลมากกว่าไฟล์รูปภาพนามสกุลอื่นโดยไม่ทำให้ขนาดของไฟล์และคุณภาพของไฟล์เปลี่ยน เลือกใช้การซ่อนข้อมูลแบบซ่อนข้อมูลที่ต้องการพร้อมกับรหัสผ่านไว้ในไฟล์ภาพ เนื่องจากต้องการสร้างความปลอดภัยให้กับข้อมูลที่ซ่อนอยู่ในไฟล์ภาพ และเลือกใช้วิธีการซ่อนข้อมูลไว้ที่บิตที่มีนัยสำคัญต่ำสุด ซึ่งเป็นวิธีที่นิยมใช้มากที่สุด