การพิสูจน์ความถูกต้องของภาพดิจิตอลบนเว็บโดยใช้ลายน้ำดิจิตอล

WEB-BASED IMAGE AUTHENTICATION USING DIGITAL WATERMARK

โดย

นัดดา ปรัชญานิมิต

NADDA PRUCHYANIMIT

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ภาคเรียนที่ 1 ปีการศึกษา 2549

WEB-BASED IMAGE AUTHENTICATION

USING DIGITAL WATERMARK

NADDA PRUCHYANIMIT

A SYSTEM DEVELOPMENT PROJECT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

FACULTY OF INFORMATION TECNOLOGY

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

1/ 2006

ชื่อหัวข้อ	การพิสูจน์ความถูกต้องของภาพดิจิตอลบนเว็บโดยใช้ลายน้ำดิจิตอล
นักศึกษา	นางสาวนัดดา ปรัชญานิมิต
รหัสนักศึกษา	47066419
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2549
อาจารย์ที่ปรึกษา	รศ.ดร.นพพร โชติกกำธร

บทคัดย่อ

โครงงานนี้จะทำการพัฒนาระบบที่ให้บริการการตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์ โดยผู้ที่จะเข้ามาใช้บริการในระบบนี้แบ่งออกได้เป็นสองประเภท คือ เจ้าของภาพดิจิตอลและบุคคลทั่วไป ในการใช้ระบบผู้ใช้ที่เป็นเจ้าของภาพดิจิตอลเองจำเป็นต้องลงทะเบียนสมัครกับระบบ เพื่อทำการฝังลายน้ำดิจิตอลลงในภาพดิจิตอลหรือตรวจสอบความถูกต้องของภาพดิจิตอลได้ แต่บุคคลทั่วไปจะสามารถนำภาพดิจิตอลมาตรวจสอบได้เพียงอย่างเดียว โดยระบบสามารถให้ผู้ใช้เลือกระดับในการตรวจสอบได้หลายระดับ แล้วระบบจะแจ้งผลมาให้ผู้ใช้บริการตามระดับชั้นที่ผู้ใช้เลือก ซึ่งผลในการตรวจสอบของภาพดิจิตอลจะทำให้ทราบว่าภาพดิจิตอลดังกล่าวได้มีการแก้ไขหรือไม่ ถ้ามีจะอยู่ณ. ตำแหน่งใดบ้าง

Title	Web-based Image Authentication using Digital Watermark
Student	Ms. Nadda Pruchyanimit
Student ID.	47066419
Degree	Master of Science
Program	Information Science
Academic Year	2006
Advisor	Assoc. Prof. Dr. Nopporn Chotikakamthorn

ABSTRACT

A web-based system provides image authentication service by embedding watermark into digital images. Two user groups classified in the system are image owners and guest users. Image owners who register with the system are allowed to embed watermark into owners' digital images or authenticate the digital images. Guest users, who do not need to register with the system, are only allowed to authenticate digital images. The system can support multi-levels of image authentication and show the result based on the level customized by users. The result can be used to verify the authenticity of digital images, and to identify manipulated parts of the image.

กิตติกรรมประกาศ

โครงการพัฒนาระบบงานนี้สำเร็จได้ ด้วยคำแนะนำ คำปรึกษาและความเอาใจใส่จาก รศ.ดร.นพพร โชติกกำธร ซึ่งเป็นอาจารย์ที่ปรึกษา ข้าพเจ้ารู้สึกทราบซึ้งในความอนุเคราะห์ และขอขอบพระคุณเป็นอย่างสูง

ขอกราบขอบพระคุณอาจารย์คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ทุกๆท่านที่ได้ให้ความรู้แก่ข้าพเจ้า

ขอขอบคุณ บัณฑิตวิทยาลัย และคณะเทคโนโลยีสารสนเทศ ที่ได้ให้ความช่วยเหลือในเรื่องต่างๆ ขอขอบคุณเพื่อนๆในรุ่น พี่ๆ ทุกคนที่คอยเป็นกำลังใจในการทำงานตั้งแต่ต้น

สุดท้ายนี้ข้าพเจ้าขอกราบขอบพระคุณ บิดา มารดา และครอบครัวของข้าพเจ้าที่เป็นกำลังใจ และให้การสนับสนุนในทุกเรื่องๆ ทำให้ข้าพเจ้าสามารถทำโครงการพัฒนาระบบงานฉบับนี้สำเร็จลุล่วงด้วยดี

นัดดา ปรัชญานิมิต

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ หน้า

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในสมัยก่อนอาจกล่าวได้ว่า เมื่อมีใครกระทำผิดแล้วต้องขึ้นศาล หลักฐานที่บ่งชี้ชัดถึงการกระทำผิดได้ คือ ภาพ ซึ่งเมื่อได้เห็นภาพพร้อมฟิล์มเนกาทีฟ ศาลก็จะตัดสินถึงความผิดนั้นๆ ได้ โดยการตรวจสอบหลักฐานที่ว่า ภาพไม่สามารถโกหกได้ แต่เมื่อเทคโนโลยีได้เปลี่ยนไปเนื่องจากมีการใช้อินเตอร์เน็ตกันอย่างแพร่หลายโดยผ่านเว็บบราวเซอร์ Mosaic จึงทำให้ผู้คนต่างได้รับข้อมูลข่าวสารต่างๆ จากการใช้บริการ World Wide Web (WWW) และทำให้สื่อดิจิตอลต่างๆ มีการเติบโตอย่างรวดเร็ว ซึ่งผู้ใช้ต่างต้องการที่จะดาวน์โหลดสื่อดิจิตอลมากขึ้น ที่มีทั้งภาพ เสียงและวิดีโอ ด้วยเหตุนี้ จึงทำให้เกิดปัญหาต่างๆ ขึ้นมากมายในเรื่องของการละเมิดลิขสิทธิ์ การเปลี่ยนแปลงหรือแก้ไขข้อมูลต่างๆ ที่อยู่รูปของดิจิตอล เนื่องจากผู้ใช้สามารถแก้ไขหรือทำปลอมแปลงบิดเบือนข้อมูลดิจิตอลได้ด้วยการใช้ซอฟต์แวร์สำเร็จรูปและสามารถส่งถึงกันได้อย่างง่ายดาย จึงนำไปสู่หนทางของการใช้สื่อดิจิตอลในทางที่ผิด โดยมีการเผยแพร่ภาพดิจิตอลที่ถูกตัดต่อของดารา นางแบบหรือบุคคลที่มีชื่อเสียง รวมถึงการทำสำเนาภาพดิจิตอล ซึ่งนำมาเผยแพร่โดยไม่ได้รับอนุญาตจากเจ้าของภาพ ทั้งในแง่ของการแอบอ้างความเป็นเจ้าของหรือการแก้ไขเปลี่ยนแปลงของภาพดิจิตอล ถ้าหากการแก้ไขเปลี่ยนแปลงนั้น สามารถสังเกตได้อย่างชัดเจนว่าเป็นภาพที่ปลอมแปลงขึ้น ก็ไม่จำเป็นต้องมีการพิสูจน์ความถูกต้องของภาพ แต่ถ้าหากเป็นการแก้ไขเปลี่ยนแปลงที่แนบเนียนและน่าเชื่อถือ เราจะทราบได้อย่างไรว่าภาพดิจิตอลนั้นถูกปลอมแปลงขึ้นมาหรือไม่ เพราะฉะนั้นจึงทำให้เกิดคำว่า "ลายน้ำดิจิตอล" ขึ้นในยุคของช่วงปี 1990 โดยที่ผู้คนต่างให้ความสนใจและให้ความสำคัญกับการป้องกันความถูกต้องของข้อมูล แต่เนื่องจากการรับรู้ของมนุษย์ถึงภาพดิจิตอลนั้นมีขีดจำกัด จึงทำให้ไม่สามารถสังเกตถึงความแตกต่างหรือการเปลี่ยนไปเพียงเล็กน้อยได้ด้วยตาเปล่า ดังนั้นลายน้ำดิจิตอลจึงเป็นทางเลือกที่ใช้กันอย่างแพร่หลายกันและมีบทบาทสำคัญในการตรวจสอบความถูกต้องของภาพดิจิตอลโดยเป็นการฝังข้อมูลบางอย่าง (เช่น ตัวอักษร ตัวเลข หรือภาพดิจิตอล) ลงไปในภาพดิจิตอล ซึ่งลายน้ำดิจิตอลจะไม่ปรากฏในภาพดิจิตอล และไม่สามารถที่เอาออกไปได้จากการใช้งานปกติทั่วไป

สำหรับโครงงานนี้ มีแนวคิดพื้นฐานจากการใช้ลายเซ็นดิจิตอล (Digital Signature) ร่วมกับการสร้างลายน้ำดิจิตอลลงในภาพดิจิตอล (Digital Watermark) เพื่อใช้ในการตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์ โดยเป็นการฝังลายเซ็นดิจิตอลลงไปในภาพดิจิตอลด้วยเทคนิคของการฝังลายน้ำดิจิตอล คือ LSB (Least Significant Bit) รวมทั้ง จะสามารถตรวจสอบถึงการ

เปลี่ยนแปลงเฉพาะที่ของภาพดิจิตอลได้ ด้วยการใช้เทคนิคบล็อกที่มีหน้าต่างขนาด 2 x 2 เทียบกับบล็อกข้างเคียง

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

โครงงานฉบับนี้มุ่งหวังเพื่อศึกษาวิธีการใช้ลายเซ็นดิจิตอลและลายน้ำดิจิตอล เพื่อมาประยุกต์ใช้งานในการตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์ ซึ่งในการตรวจสอบนี้ จะเป็นการตรวจสอบความถูกต้องของทั้งภาพดิจิตอล รวมทั้งหาวิธีการตรวจสอบรูปภาพดิจิตอลที่ถูกตัด ในกรณีของการเปลี่ยนแปลงภาพเฉพาะที่ เพื่อต้องการลดปัญหาที่เกิดขึ้นของดารานางแบบหรือบุคคลที่มีชื่อเสียงที่ตกเป็นข่าว เนื่องจากการกระทำของบุคคลที่ไม่ประสงค์ดี

1.3 สมมุติฐานของการศึกษา

การนำลายเซ็นดิจิตอลและลายน้ำดิจิตอลมาประยุกต์ใช้ในการตรวจสอบความถูกต้องของภาพดิจิตอลเป็นวิธีที่น่าเชื่อถือและมีความปลอดภัยสูง ซึ่งข้อมูลภาพดิจิตอลนั้น มีจำนวนปริมาณข้อมูลมาก อีกทั้งบางทีมีการตรวจสอบความถูกต้องของภาพดิจิตอลที่คลุมเครือ ถึงแม้ว่าข้อมูลพิกเซลของภาพดิจิตอลจะเปลี่ยนแปลงไปจากต้นฉบับ โดยที่ความหมายของภาพดิจิตอลยังสื่อถึงความหมายเดิมอยู่ ซึ่งข้อมูลภายในภาพดิจิตอลมีการเปลี่ยนแปลงเกิดขึ้น แต่ในสายตาของผู้รับ ไม่สามารถสังเกตถึงความเปลี่ยนแปลงเพียงเล็กน้อยได้ด้วยตาเปล่า และเนื่องจากการแก้ไขภาพดิจิตอลสามารถทำได้ง่าย จึงทำให้ลายเซ็นดิจิตอลของภาพดิจิตอลนั้นๆ มีโอกาสสูญหายได้ เช่น การแปลงสกุลไฟล์ เป็นต้น จึงจำเป็นที่ต้องฝังลายเซ็นดิจิตอลลงไปในภาพดิจิตอล ซึ่ง จะทำให้การตรวจสอบความถูกต้องได้ละเอียดมากขึ้นอีกด้วยการแบ่งภาพดิจิตอลออกเป็นลำดับชั้น

1.4 ทฤษฎีและหลักการที่ใช้ในโครงงาน

1.4.1 ภาพดิจิตอล

ภาพดิจิตอลสามารถแทนด้วยฟังก์ชันของค่าความสว่างในรูปของ f(x, y) โดยที่ x แสดงถึงพิกัดในแนวนอนและ y แสดงถึงพิกัดในแนวตั้งของจุดภาพ ซึ่ง f คือ ตำแหน่งของภาพที่มีจุด (x, y) แสดงถึงความสว่างหรือระดับสีเทา (Gray level) ของภาพ โดยมีระดับสีเทาอยู่ที่ 256 ระดับ ซึ่งมีค่าตั้งแต่ 0 ถึง 255 และในแต่ละจุดภาพหรือเรียกว่า พิกเซล (Pixel) ซึ่งเป็นหน่วยย่อยที่สุดของภาพดิจิตอลสามารถแทนด้วยข้อมูล 8 บิตต่อหนึ่งพิกเซล

1.4.2 ลายน้ำดิจิตอล

ลายน้ำดิจิตอลเป็นอีกทางเลือกหนึ่งที่ใช้กันแพร่หลายและมีบทบาทสำคัญในการตรวจสอบความถูกต้องของภาพดิจิตอล ซึ่งเป็นการฝังข้อมูล (Embedded) บางอย่างลงไปในภาพดิจิตอล ข้อมูลของลายน้ำดิจิตอลอาจมีลักษณะเป็นตัวอักษร ตัวเลขหรือภาพดิจิตอล ซึ่งลายน้ำดิจิตอลจะไม่ปรากฏในภาพดิจิตอล

1.4.3 ลายเซ็นดิจิตอล

ในการเข้ารหัสเพื่อสร้างลายเซ็นดิจิตอล เป็นการช่วยป้องกันภาพดิจิตอลในการส่งข้อมูลระหว่างผู้ส่งและผู้รับ โดยแนวคิดก็คือ การที่นำข้อมูลภาพดิจิตอลมาผ่านกระบวนการแฮชฟังก์ชัน (Hash Function) เพื่อให้ได้ตัวแทนของข้อมูลที่มีขนาดเล็กลง จากนั้นนำมาเข้ารหัสลับด้วยอัลกอริทึมแบบ RSA ซึ่งเป็นการเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography) แล้วผลลัพธ์ที่ได้ คือ ลายเซ็นดิจิตอล จากนั้นนำลายเซ็นดิจิตอลที่ได้นั้นฝังกลับไปลงไปภาพดิจิตอล

1.5 ขอบเขตของโครงงาน

1. ภาพดิจิตอลที่ใช้ในโครงงานนี้ เป็นภาพสีมีขนาด 24 บิต และเป็นรูปภาพดิจิตอลของดารานางแบบหรือบุคคลที่มีชื่อเสียง ซึ่งจะรองรับสกุลไฟล์ภาพดิจิตอล Bitmap (BMP) เท่านั้น
2. ภาพดิจิตอลที่นำมาฝังลายน้ำดิจิตอล จำเป็นต้องลงทะเบียนกับทางเว็บไซต์ก่อนเสมอ จากนั้นค่อยนำไปตรวจสอบความถูกต้องของภาพดิจิตอล
3. ในการฝังลายน้ำดิจิตอล ใช้เพื่อในการตรวจสอบความถูกต้องของภาพดิจิตอลเท่านั้น
4. ในการตรวจสอบความถูกต้องของภาพดิจิตอล ระบบสามารถให้บริการในการตรวจสอบได้สูงสุด 3 ระดับ
5. ขนาดของรูปภาพดิจิตอลที่ระบบรับได้มากสุด คือ 800 x 600 พิกเซล

1.6 ขั้นตอนการศึกษา

1. ศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องในปัจจุบัน
2. กำหนดแนวทาง วัตถุประสงค์ ขอบเขตของโครงงานและวิธีการที่จะศึกษา
3. หาวิธีการที่จะประยุกต์ใช้ลายเซ็นดิจิตอลกับภาพดิจิตอล รวมทั้งหาวิธีที่เหมาะสมที่ใช้ในการตรวจสอบการตัดภาพดิจิตอล
4. พัฒนาเว็บไซต์ที่มีบริการในการฝังลายเซ็นดิจิตอลลงในภาพดิจิตอลและการตรวจสอบความถูกต้องของภาพดิจิตอล
5. ทำการทดลอง
6. สรุปผลและข้อเสนอแนะ

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. ช่วยลดปัญหาของดารา นางแบบหรือบุคคลที่มีชื่อเสียงที่ตกเป็นข่าวเนื่องจากการกระทำของผู้ที่ไม่ประสงค์นำภาพไปตัดต่อ

2. พัฒนาการฝังลายเซ็นดิจิตอลลงในภาพดิจิตอล ให้สามารถตรวจสอบการเปลี่ยนแปลงแก้ไขภาพดิจิตอลเฉพาะที่ได้

บทที่ 2
หลักการและทฤษฎีที่เกี่ยวข้อง

ในหัวข้อบทนี้จะกล่าวถึงทฤษฎีพื้นฐานต่างๆ ที่เกี่ยวข้องในการวิจัย ซึ่งเนื้อหาจะกล่าวถึง ภาพดิจิตอล ไฟล์รูปภาพดิจิตอล ลายน้ำดิจิตอล การเข้ารหัสและถอดรหัสลับแบบใช้กุญแจสาธารณะและลายเซ็นดิจิตอล

2.1 ภาพดิจิตอล

ภาพดิจิตอลเกิดขึ้นครั้งแรกในวงการหนังสือพิมพ์เมื่อต้นปี 1920 ซึ่งภาพดิจิตอลถูกส่งผ่านระบบสายเคเบิลใต้น้ำของ Bartlane ระหว่างลอนดอนและนิวยอร์ก เพื่อช่วยลดเวลาในการส่งภาพข้ามมหาสมุทรแอนแลนติกที่ปกติใช้เวลามากกว่าหนึ่งอาทิตย์เหลือเพียงไม่เกิน 3 ชั่วโมง ด้วยการใช้อุปกรณ์เข้ารหัสดิจิตอลที่ต้นทางและเครื่องพิมพ์ดิจิตอลที่ปลายทาง จากตอนนั้นถึงบัดนี้พัฒนาการของภาพดิจิตอลมีอย่างต่อเนื่อง โดยเฉพาะในปัจจุบันเป็นยุคของอินเตอร์เน็ต ข่าวสารต่างๆ สามารถส่งผ่านไปมาได้อย่างรวดเร็ว ไม่ว่าจะอยู่ที่ไหนในโลก ดังนั้นภาพดิจิตอลจึงได้มีบทบาทมากขึ้นในชีวิตประจำวัน รวมถึงการใช้ภาพดิจิตอลในวงการอื่นๆ เช่น ด้านทางการแพทย์ สื่อสารมวลชน สถาปัตยกรรม เป็นต้น

รูปที่ 2.1 ภาพดิจิตอลในปี 1921 จากแถบรหัสโดยเครื่องพิมพ์โทรเลข

ภาพดิจิตอลประกอบด้วยจุดภาพ (Pixel) เป็นจำนวนมาก โดยพิกเซลเหล่านี้จะเก็บค่าที่เป็นตัวเลขเพื่อแสดงถึงความสว่างของภาพในแต่ละจุด คุณภาพของภาพจะแปรผันตามจำนวนและขนาดของพิกเซล ซึ่งถ้าเพิ่มจำนวนพิกเซลก็จะทำให้ได้ภาพที่มีความละเอียดมากขึ้นและถ้าเพิ่มจำนวนบิตที่ใช้ในการเก็บค่าความสว่างของพิกเซลก็จะได้ภาพที่มีความคมชัดมากขึ้น ประเภทของภาพดิจิตอล สามารถแบ่งออกได้เป็น 3 แบบด้วยกัน คือ ภาพไบนารี ภาพระดับสีเทาและภาพสี

2.1.1 ภาพไบนารี (Binary images)

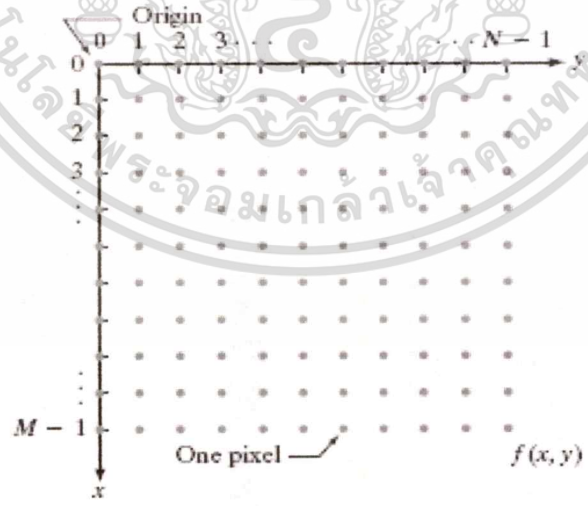
เป็นภาพที่ถูกแสดงด้วยระดับความเข้มเพียง 2 ระดับเท่านั้น ซึ่งระดับแรกจะแสดงถึงข้อมูล (Information) ส่วนอีกระดับจะแสดงถึงพื้นหลัง (Background) ดังนั้นแต่ละพิกเซลจะประกอบไปด้วยบิตเดียวที่มีค่าเป็น 1 หรือ 0

2.1.2 ภาพระดับสีเทา (Gray Scale images)

เป็นภาพที่ถูกแสดงด้วยความเข้มหลายระดับ คือ เป็นภาพที่มีการไล่ความเข้มตั้งแต่สีขาวไปจนถึงสีดำ โดยทั่วไป แต่ละพิกเซลจะประกอบไปด้วย บิตจำนวน N บิต ตั้งแต่ 8 บิตขึ้นไป ภาพระดับสีเทานี้เหมาะสำหรับที่จะใช้ในการแสดงภาพถ่ายโมโนโครม (Monochrome Photographs) และภาพทางการแพทย์ (Medical Image) ที่ใช้ในการเอกซเรย์ (X-ray) ซึ่งให้ความสำคัญในการไล่ความเข้มของระดับสีเทาในการแสดงภาพ

2.1.3 ภาพสี (Color images)

เป็นภาพที่ถูกแสดงด้วยความเข้มหลายระดับและใช้การกรองระดับความสว่างของแต่ละสี โดยมีสีพื้นฐานที่ใช้ด้วยกัน 3 สี คือสีแดง สีเขียวและสีน้ำเงิน ซึ่งจะแสดงด้วยสัญลักษณ์ R(red) G(green) B(blue) ดังนั้นในแต่ละพิกเซลจะประกอบไปด้วยค่า 3 ค่าที่แสดงแต่ละความเข้มของสีพื้นฐาน โดยแต่ละพิกเซลจะมีจำนวนบิตตั้งแต่ 24 บิตขึ้นไป ภาพสีนี้จะเป็นภาพที่มนุษย์สามารถรับรู้ได้ด้วยการมองเห็น



รูปที่ 2.2 การใช้รูปภาพแสดงถึงภาพดิจิตอล

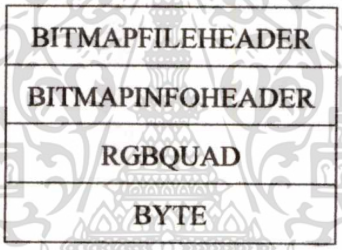
ข้อมูลภาพจะอยู่ในรูปของฟังก์ชันสองมิติ ดังรูปที่ 2.2 โดยที่ภาพดิจิตอลมีขนาด M x N จุดภาพ จะ สามารถเขียนแทนให้อยู่ในรูปของฟังก์ชันทางคณิตศาสตร์ได้เป็น f(x, y) ค่าของฟังก์ชันและพิกัดของภาพดิจิตอลจะถูกแปลงให้เป็นค่าจำนวนเต็มที่ไม่ต่อเนื่อง

2.2 ไฟล์รูปภาพดิจิตอล

ปัจจุบันมีไฟล์รูปภาพดิจิตอลต่างๆ เช่น ไฟล์ BMP (Windows Device Independent Bitmap) เป็นรูปแบบไฟล์มาตรฐานที่ใช้กันทั่วๆ ไปบน Windows ไฟล์ JPEG (Joint Photographic Expert Group) ไฟล์ GIF (Graphic Interchange Format) เป็นต้น

2.2.1 การจัดเก็บภาพดิจิตอล

การจัดเก็บรายละเอียดข้อมูลต่างๆ ลงในไฟล์ภาพดิจิตอลมีรูปแบบที่แตกต่างกันออกไปตามสกุลของไฟล์ภาพดิจิตอล ซึ่งในโครงงานนี้จะขอกล่าวถึงเฉพาะรูปแบบไฟล์รูปภาพดิจิตอลที่เป็นไฟล์ชนิด Bitmap มีสกุลไฟล์ (.bmp) หรือเรียกอีกอย่างว่า Device Independent Bitmap (.dib) เป็นรูปแบบไฟล์มาตรฐานที่ใช้กันทั่วไปในระบบปฏิบัติการ Windows โครงสร้างภายในไฟล์ BMP ประกอบด้วย 4 ส่วนด้วยกัน ดังรูปที่ 2.3



รูปที่ 2.3 โครงสร้างของไฟล์ BMP

Bitmap File Header เป็นส่วนหัวของโครงสร้างไฟล์ จะทำหน้าที่เก็บข้อมูลเกี่ยวกับ ชนิด ขนาด และการวางผังของไฟล์ (Device Independent File) ดังนั้นเมื่อรวมโครงสร้างส่วนหัวของไฟล์ Bitmap ซึ่งมีขนาด 14 ไบต์ ดังรูปที่ 2.4

```
Private Type BITMAPFILEHEADER
    strFileType As String * 2
    IntFileSize As Long
    bytReserved1 As Integer
    bytReserved2 As Integer
    IngBitmapOffset As Long
End Type
```

รูปที่ 2.4 โครงสร้างส่วนหัวของไฟล์ Bitmap

- strFileType ระบุประเภทของไฟล์ ซึ่งเป็น BM หรือ 4D42h
- IngFileSize ระบุขนาดของไฟล์เป็นไบต์
- byteReserved1 ไบต์ที่มีค่าสงวนเป็น 0
- byteReserved2 ไบต์ที่มีค่าสงวนเป็น 0
- IngBitmapOffset ระบุ byte Offset จากโครงสร้าง BITMAPFILEHEADER

Bitmap Information Header จะทำหน้าที่กำหนดขนาด ประเภทของการบีบอัดข้อมูลและรูปแบบสีของ Bitmap และเมื่อรวมโครงสร้างส่วนหัวของภาพดิจิตอลในไฟล์ Bitmap ซึ่งมีขนาด 40 ไบต์ ดังรูปที่ 2.5

```
Private Type BITMAPINFOHEADER
    biSize As Long
    biWidth As Long
    biHeight As Long
    biPlanes As Integer
    biBitCount As Integer
    biCompression As Long
    biSizeImage As Long
    biXPelsPerMeter As Long
    biYPelsPerMeter As Long
    biClrUsed As Long
    biClrImportant As Long
End Type
```

รูปที่ 2.5 โครงสร้างส่วนหัวของภาพดิจิตอลในไฟล์ Bitmap

- biSize ระบุจำนวนไบต์ที่โครงสร้าง BITMAPINFOHEADER ต้องการ
- biWidth ระบุความกว้างในหน่วนพิกเซล
- bitHeight ระบุความสูงในหน่วยพิกเซล
- biplanes ระบุจำนวน Planes ซึ่งตั้งค่าเป็น 1
- ByBitCount ระบุจำนวนของบิตต่อพิกเซล เช่น 1 4 8 หรือ 24
- BiCompression ระบุประเภทของการบีบอัด
- BiSizeImage ระบุขนาดของภาพ Bitmap ในหน่วยไบต์
- BiXPelsPerMeter ระบุความละเอียดในแนวนอนในหน่วยพิกเซลต่อเมตร

- BiYPelsPerMeter ระบุความละเอียดในแนวตั้งในหน่วยพิกเซลต่อเมตร
- biClrUsed ระบุจำนวนของสีจากตารางสีที่ใช้จริง
- biClrImportant ระบุจำนวนสี ที่มีความสำคัญในการแสดงภาพดิจิตอล

RGBQUAD จะทำหน้าที่เก็บส่วนประกอบต่างๆ ซึ่งเป็นสีใน Bitmap หรือเรียกว่าตารางสี (Color Table) หรือเรียกอีกอย่างว่า แผ่นเทียบสี (Palette) ดังนั้นเมื่อรวมโครงสร้างแผ่นเทียบสีในไฟล์ Bitmap ซึ่งแต่ละสีมีขนาด 1 ไบต์ รวมกันจึงเป็น 4 ไบต์ ดังรูปที่ 2.6

```
Private Type RGBQUAD
    rgbBlue As Byte
    rgbGreen As Byte
    rgbRed As Byte
    rgbReserved As Byte
End Type
```

รูปที่ 2.6 โครงสร้างแผ่นเทียบสีในไฟล์ Bitmap

- rgbBlue ระบุค่าไบต์ของสีฟ้า ซึ่งมีค่าสีอยู่ระหว่าง 0-255
- rgbGreen ระบุค่าไบต์ของสีเขียว ซึ่งมีค่าสีอยู่ระหว่าง 0-255
- rgbRed ระบุค่าไบต์ของสีแดง ซึ่งมีค่าสีอยู่ระหว่าง 0-255
- rgbReserved ระบุค่าไบต์ที่สงวนเป็น 0

BYTE จะทำหน้าที่เก็บข้อมูลไบต์ของภาพดิจิตอลลงในไบต์อาเรย์ ดังรูปที่ 2.6

```
Dim BMPData() As Byte
```

รูปที่ 2.7 ตัวข้อมูลภาพดิจิตอลที่เก็บลงในไบต์อาเรย์

ข้อมูลในไฟล์ภาพ Bitmap ประกอบด้วยไบต์ที่ต่อเนื่องกันและเก็บลงในอาเรย์ ดังรูปที่ 2.7 ซึ่งข้อมูลพิกเซลของภาพดิจิตอลจะถูกเก็บเริ่มจากมุมล่างซ้ายและสแกนไล่มาทีละบรรทัดขึ้นมาขึ้นข้างบนด้วยการสแกนจากซ้ายไปขวา ดังนั้นทั้งบรรทัดล่างสุดจะถูกเก็บลงในอาเรย์ก่อน จนถึงพิกเซลสุดท้ายที่อยู่ทางมุมขวามือของภาพดิจิตอลจะถูกเก็บลงอาเรย์เป็นตัวสุดท้าย

2.3 ลายน้ำดิจิตอล

2.3.1 ประเภทของลายน้ำดิจิตอล

ลายน้ำดิจิตอลที่มนุษย์สามารถรับรู้ได้ สามารถแบ่งออกได้เป็น 2 ประเภท คือ ลายน้ำดิจิตอลที่สามารถมองเห็นได้ (Visible Watermark) และลายน้ำดิจิตอลที่ไม่สามารถมองเห็นได้ (Invisible Watermark)

2.3.1.1 ลายน้ำดิจิตอลที่สามารถมองเห็นได้

เป็นลายน้ำดิจิตอลที่ใช้กันมากบนเว็บไซต์และลายน้ำดิจิตอลดังกล่าว มีลักษณะเป็นชื่อหรือสัญลักษณ์ต่างๆ เช่น ชื่อหรือสัญลักษณ์ของบริษัทวางทับบนภาพดิจิตอล ดังรูปที่ 2.8 ซึ่งลายน้ำดิจิตอลนี้มีความคล้ายคลึงกับลายน้ำในกระดาษที่ใช้กันในธนบัตรหรือภาพวาด ดังนั้นลายน้ำดิจิตอลที่มองเห็นได้จะมีประโยชน์ในกรณีที่สื่อถึงสิทธิความเป็นเจ้าของได้อย่างชัดเจน

รูปที่ 2.8 ลายน้ำดิจิตอลที่สามารถมองเห็นได้

2.3.1.2 ลายน้ำดิจิตอลที่ไม่สามารถมองเห็นได้

ลายน้ำดิจิตอลชนิดนี้นิยมใช้กันแพร่หลายซึ่งเป็นการฝังข้อมูลบางอย่างเข้าไปในภาพดิจิตอลซึ่งจะไม่สามารถมองเห็นตัวข้อมูลที่ฝังเข้าไปได้ เช่น ข้อความแสดงลิขสิทธิ์ หรือซีเรียลนัมเบอร์ เป็นต้น ลายน้ำดิจิตอลที่ไม่สามารถมองเห็นจะมีข้อได้เปรียบกว่าลายน้ำดิจิตอลที่สามารถมองเห็น เพราะภาพดิจิตอลที่ได้หลังจากการฝังลายน้ำดิจิตอลไม่ถูกลดคุณค่าและความสวยงามลง ซึ่งคุณสมบัตินี้จะมีค่าแปรผกผันกับความคงทนของสัญญาณลายน้ำดิจิตอลที่ถูกใส่เอาไว้ในตัวข้อมูล ดังรูปที่ 2.9

รูปที่ 2.9 ลายน้ำดิจิตอลที่ไม่สามารถมองเห็นได้

2.3.2 คุณสมบัติของลายน้ำดิจิตอล

คุณสมบัติของลายน้ำดิจิตอลมีความเกี่ยวข้องกับการนำลายน้ำดิจิตอลไปใช้งาน ดังนั้น หน้าที่ของลายน้ำดิจิตอลก็จะแตกต่างกันไปตามชนิดของงานที่นำไปใช้ ซึ่งลายน้ำดิจิตอลที่ดี ควรมีคุณสมบัติ ดังนี้

- **ความสามารถในการซ่อนข้อมูล (Imperceptibility)** เมื่อฝังลายน้ำดิจิตอลลงไปในภาพดิจิตอลแล้ว ควรจะมองไม่เห็นถึงความแตกต่างจากภาพดิจิตอลต้นฉบับกับภาพดิจิตอลที่ฝังลายน้ำดิจิตอล ซึ่งแสดงถึงว่าลายน้ำดิจิตอลที่ดีจะต้องไม่ปรากฏในภาพดิจิตอล
- **ความทนทาน (Robustness)** เมื่อฝังลายน้ำดิจิตอลลงไปในภาพดิจิตอลแล้ว ข้อมูลลายน้ำดิจิตอลควรจะคงทนอยู่ในสื่อนั้นๆ ไม่ว่าจะเกิดอะไรขึ้นกับสื่อนั้นก็ตาม รวมทั้งการถูกโจมตีจากผู้ที่ต้องการจะทำลายสื่อเหล่านี้ เช่น การบีบอัดภาพดิจิตอล การกรองภาพดิจิตอล ช่องการสื่อสารที่มีสัญญาณรบกวน การแก้ไขหรือเปลี่ยนแปลงภาพดิจิตอล การตัดพื้นที่บางส่วนของภาพดิจิตอล เป็นต้น
- **ปริมาณข้อมูลที่สามารถบรรจุได้ (Capacity)** สื่อที่จะสร้างลายน้ำดิจิตอล ควรจะสามารถบรรจุข้อมูลได้มากที่สุดเท่าที่จะเป็นไปได้

จะเห็นได้ว่า คุณสมบัติที่สำคัญทั้งสามที่กล่าวมาข้างต้น จะเป็นปฏิภาคซึ่งกันและกัน โดยที่ถ้าต้องการให้ข้อมูลมีความทนทานและสามารถบรรจุปริมาณข้อมูลได้มาก ข้อมูลนั้นก็จะมีความสามารถในการซ่อนข้อมูลได้ต่ำ ในทางกลับกัน ถ้าต้องการข้อมูลที่มีความสามารถในการซ่อนข้อมูลได้สูงและบรรจุปริมาณข้อมูลได้มาก ข้อมูลนั้นจะมีความทนทานที่ต่ำ ซึ่งในโครงงานนี้จะกล่าวถึงลายน้ำดิจิตอลที่ใช้งานทางด้านการตรวจสอบความถูกต้องของภาพดิจิตอล ซึ่งลายน้ำดิจิตอลควรที่จะตรวจสอบถึงการแก้ไขหรือการเปลี่ยนแปลงใดๆ ของภาพดิจิตอลได้

คุณสมบัติของการตรวจสอบความถูกต้องของภาพดิจิตอลที่มีประสิทธิภาพ ควรมีดังนี้

- ต้องสามารถบอกได้ว่าภาพดิจิตอลได้มีการแก้ไขหรือเปลี่ยนแปลงหรือไม่
- ต้องสามารถระบุถึงการเปลี่ยนแปลงใดๆ ที่เกิดขึ้นในภาพดิจิตอลได้
- ต้องสามารถรวมข้อมูลที่แสดงถึงความถูกต้องของภาพดิจิตอลเข้าในภาพดิจิตอลต้นทางได้ ไม่ใช่แยกกันคนละไฟล์
- การฝังข้อมูลบางอย่างลงไปเพื่อตรวจสอบความถูกต้องของภาพดิจิตอลจะต้องไม่ปรากฏในภาพดิจิตอลภายใต้การใช้งานปกติ
- อนุญาตให้ลายน้ำดิจิตอลที่ฝังอยู่ในภาพดิจิตอลสามารถอยู่ในรูปของการบีบอัดข้อมูลภาพดิจิตอลแบบ Lossy ได้ เช่น JPEG

2.3.3 วัตถุประสงค์การนำลายน้ำดิจิตอลไปใช้งาน

ลายน้ำดิจิตอลสามารถนำไปใช้ประโยชน์ได้มากมายหลายรูปแบบ ดังนั้นรูปแบบการนำไปใช้ก็มีความแตกต่างกันเช่นเดียวกัน

2.3.3.1 การป้องกันลิขสิทธิ์ (Copyright Protection)

ในปัจจุบันสื่อต่างๆ อย่างภาพดิจิตอลหรือเสียงเพลงสามารถถูกคัดลอกได้โดยง่าย ถึงแม้ว่าผู้ผลิตสื่อเหล่านั้นจะมีเอกสารมารับรองสิทธิ์การเป็นเจ้าของสื่อก็ตาม ลายน้ำดิจิตอลสามารถเข้ามาช่วยได้ โดยการฝังข้อมูลเกี่ยวกับสิทธิ์การเป็นเจ้าของสื่อนั้นลงไปสื่อนั้นโดยตรง ซึ่งถ้าหากว่าอุปกรณ์ที่ใช้ในการคัดลอกมีส่วนตรวจจับข้อมูลลายน้ำดิจิตอลอยู่แล้วก็จะสามารถกำหนดได้ว่าไม่อนุญาตให้ทำการคัดลอกสื่อที่มีข้อมูลลายน้ำดิจิตอลตามที่กำหนดให้

2.3.3.2 การตรวจสอบความถูกต้อง (Authentication)

เนื่องจากปัจจุบันสื่อดิจิตอลต่างๆ สามารถแก้ไขได้ง่าย เช่น ไม่ว่าจะลบหรือแก้ไขรายละเอียดใดๆ ของภาพดิจิตอลก็สามารถทำได้โดยง่าย ซึ่งหากภาพดิจิตอลนี้มีความเกี่ยวข้องกับกระบวนการทางกฎหมาย ก็อาจจะทำให้ตัดสินพลาดได้ ซึ่งลายน้ำดิจิตอลก็จะสามารถช่วยแก้ไขปัญหานี้ได้ โดยฝังข้อมูลรายละเอียดเกี่ยวกับสื่อนั้นๆ ลงไปในสื่อ และก่อนที่จะฝังข้อมูลเข้าไปจำเป็นต้องมีการเข้ารหัสแบบอสมมาตร เช่น ลายเซ็นดิจิตอล ซึ่งหากมีบุคคลมาทำการแก้ไขสื่อนั้นๆ ผู้รับสื่อก็สามารถตรวจสอบรายละเอียดของสื่อได้ โดยจากข้อมูลของลายน้ำดิจิตอล

2.3.3.3 การเพิ่มข้อมูลประกอบ (Data Annotation)

เป็นการเพิ่มข้อมูลรายละเอียดเกี่ยวกับสื่อนั้นๆ เพื่อให้ผู้ใช้งานสามารถค้นหาข้อมูลเกี่ยวกับสื่อนั้นต่อได้ เช่น ข้อมูลเกี่ยวกับป้ายประกาศที่เป็นรูปภาพ เมื่อผู้พบเห็นทำการคัดลอกโดยใช้สแกนเนอร์ หรือกล้องดิจิตอล ก็จะสามารถพบกับข้อมูลประกอบที่เพิ่มเข้าไปได้

2.3.3.4 การพิสูจน์ความเป็นเจ้าของ (Proof of Ownership)

โดยปกติแต่ละประเทศจะมีการจดลิขสิทธิ์แก่สื่อต่างๆ เช่น รูปภาพ เพลง เนื่องจากสื่อเหล่านี้ถือเป็นทรัพย์สินทางปัญญา แต่ว่าปัญหาที่เกิดขึ้น คือ การจดลิขสิทธิ์เหล่านี้ จะต้องมีการชำระค่าจดลิขสิทธิ์ ซึ่งอาจจะเป็นราคาจำนวนมาก ดังนั้นลายน้ำดิจิตอลจึงมีบทบาท โดยการฝังข้อมูลลงบางอย่างลงไป เมื่อมีการคัดลอกเกิดขึ้น ก็สามารถใช้ลายน้ำดิจิตอลแสดงถึงความเป็นเจ้าของได้

2.3.4 ลักษณะลายน้ำดิจิตอลที่ใช้ในการตรวจสอบความถูกต้อง

ลายน้ำดิจิตอลที่ใช้ในการตรวจสอบความถูกต้อง สามารถแบ่งออกเป็น 3 ลักษณะ ได้แก่ ลายน้ำเปราะบาง (Fragile Watermark) ลายน้ำกึ่งเปราะบาง (Semi Fragile Watermark) และ ลายน้ำคงทน (Robust Watermark) โดยมีรายละเอียด ดังนี้

2.3.4.1 ลายน้ำเปราะบาง

เป็นลายน้ำดิจิตอลเปราะบางที่ถูกทำลายได้ง่ายหรือผิดเพี้ยนได้ง่าย เมื่อค่าของพิกเซลต่างๆ เกิดการเปลี่ยนแปลงเนื่องจากกระบวนการประมวลผลภาพด้วยวิธีต่างๆ ทั้งที่เจตนาหรือไม่เจตนา ลายน้ำดิจิตอลประเภทนี้จะถูกซ่อนให้สังเกตได้ยาก ดังนั้นจึงนำมาใช้สำหรับการตรวจสอบความถูกต้องในด้านรายละเอียดของข้อมูลภาพว่าภาพดิจิตอลนี้ถูกแก้ไขเปลี่ยนแลงจากภาพต้นฉบับมาหรือไม่

2.3.4.2 ลายน้ำกึ่งเปราะบาง

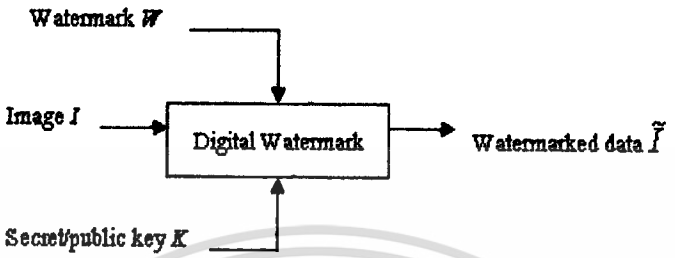
เป็นลายน้ำดิจิตอลกึ่งเปราะบางที่มีความคงทนในระดับปานกลาง สามารถแก้ไขเปลี่ยนแปลง ก็ยังสามารถตรวจพบลายน้ำดิจิตอล ดังนั้นจึงนำมาใช้เพื่อตรวจสอบว่าภาพดิจิตอลถูกแก้ไขเปลี่ยนแปลงในลักษณะใดบ้าง มากหรือน้อยเพียงใด ซึ่งขึ้นอยู่กับเทคนิคที่ใช้สร้างลายน้ำดิจิตอลว่ามีความคงทนต่อการแก้ไขแบบใด

2.3.4.3 ลายน้ำคงทน

เป็นลายน้ำดิจิตอลคงทนต่อการทำลายหรือผิดเพี้ยน สามารถทนต่อการแก้ไขเปลี่ยนแปลงภาพดิจิตอลได้สูง เช่น การบีบอัดภาพดิจิตอล การตัด การซูมภาพดิจิตอล การกรองภาพดิจิตอล การแก้ไขหรือเปลี่ยนแปลงภาพดิจิตอลต่างๆ ลายน้ำดิจิตอลประเภทนี้ อาจจะสังเกตลายน้ำดิจิตอลได้ง่าย แต่หลังจากที่นำภาพดิจิตอลไปประมวลผลต่างๆ แล้ว ลายน้ำดิจิตอลจะยังคงอยู่ไม่เสียหายแต่อย่างใด ดังนั้นจึงนำมาใช้งานในด้านการตรวจสอบความเป็นเจ้าของ

2.3.5 การสร้างลายน้ำดิจิตอลลงในรูปภาพดิจิตอล

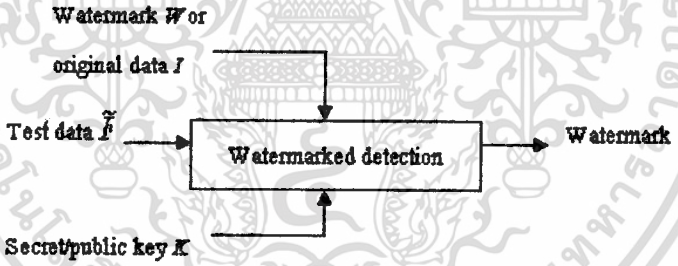
โครงสร้างของการสร้างลายน้ำดิจิตอล แบ่งออกได้เป็น การฝังลายน้ำดิจิตอล (Embedding watermark) และการดึงลายน้ำดิจิตอล (Extracting watermark)



รูปที่ 2.10 การฝังลายน้ำดิจิตอลลงไปในภาพดิจิตอล

อินพุต คือ ข้อมูลที่ต้องการฝังเป็นลายน้ำดิจิตอล ภาพดิจิตอลและกุญแจส่วนตัวหรือกุญแจสาธารณะ

เอาต์พุต คือ ภาพดิจิตอลที่มีการฝังลายน้ำดิจิตอล



รูปที่ 2.11 การดึงลายน้ำดิจิตอลออกจากภาพดิจิตอล

อินพุต คือ ภาพดิจิตอลที่มีการฝังลายน้ำดิจิตอล ภาพดิจิตอลต้นฉบับและกุญแจส่วนตัวหรือกุญแจสาธารณะ

เอาต์พุต คือ ข้อมูลที่ฝังเป็นลายน้ำดิจิตอล

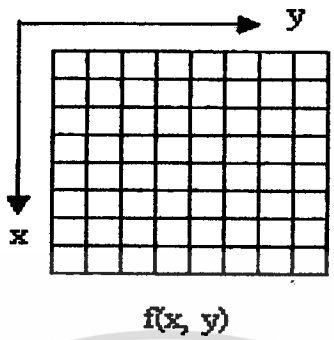
2.3.6 การเข้าถึงภาพดิจิตอล

การเข้าถึงภาพดิจิตอลสามารถเข้าถึงได้ 2 วิธี คือ Spatial domain และ Frequency domain

2.3.6.1 Spatial domain

เป็นวิธีที่จะฝังข้อมูลลายน้ำดิจิตอลเข้าไปในพิกเซลของภาพดิจิตอลโดยตรง ซึ่งในแต่ละพิกเซลของภาพดิจิตอลก็จะแทนด้วย f(x, y) ดังรูปที่ 2.12 ซึ่งบอกถึงระดับความเข้มของแสงในภาพ

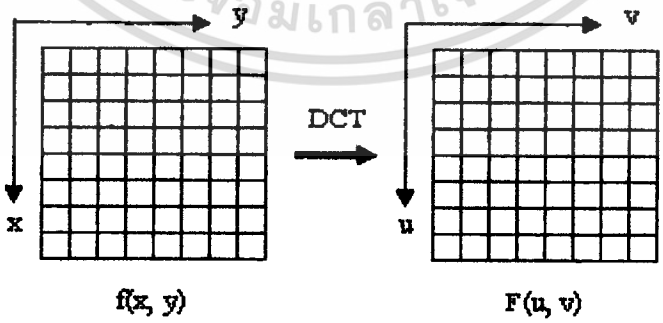
ดิจิตอล สามารถนำเทคนิคของ Least Significant Bit (LSB) มาใช้ในการฝังลายน้ำดิจิตอล วิธีนี้ใช้กันมากกับประเภทของลายน้ำแบบ Fragile Watermark



รูปที่ 2.12 Spatial domain

2.3.6.2 Frequency domain

เป็นวิธีการฝังข้อมูลลายน้ำดิจิตอลให้อยู่ในรูปของโดเมนความถี่ ซึ่งวิธีนี้จะมีความคงทนต่อการบีบอัดข้อมูล การตัดภาพดิจิตอล มากกว่าใช้วิธี Spatial domain แต่วิธีนี้จำเป็นต้องแปลงให้อยู่ในรูปของโดเมนความถี่ก่อน โดยนำฟังก์ชั่นทางคณิตศาสตร์มาใช้ในการแปลงจาก Spatial domain (ภาพดิจิตอลปกติ) เป็นโดเมนความถี่ด้วย Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) ดังรูปที่ 2.13 และสามารถนำเทคนิคของ Least Significant Bit (LSB) หรือ Spread Spectrum (SS) มาใช้ในการฝังลายน้ำดิจิตอล วิธีนี้นำมาใช้งานกันมากในด้านของการตรวจสอบความถูกต้องของข้อมูลภาพดิจิตอล ดังนั้นการสร้างลายน้ำดิจิตอลในโดเมนความถี่จะทำให้ข้อมูลลายน้ำดิจิตอลทนทานต่อการกรองสัญญาณความถี่ต่ำ การกรองสัญญาณความถี่สูงและการบีบอัดข้อมูลภาพดิจิตอล



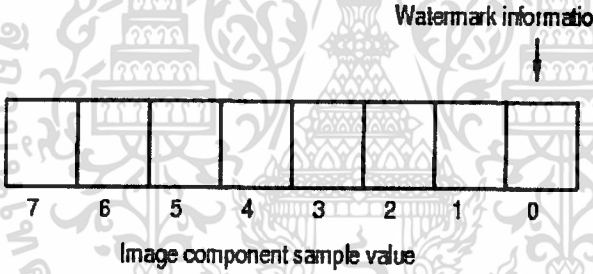
รูปที่ 2.13 การแปลงภาพดิจิตอลจาก Spatial domain ไปเป็น Frequency domain ด้วย DCT

2.3.7 เทคนิคการฝังและการดึงลายน้ำดิจิตอล

ในที่นี้จะกล่าวถึง 2 เทคนิคที่ใช้กันแพร่หลาย คือ Least Significant Bit (LSB) และ Spread Spectrum (SS)

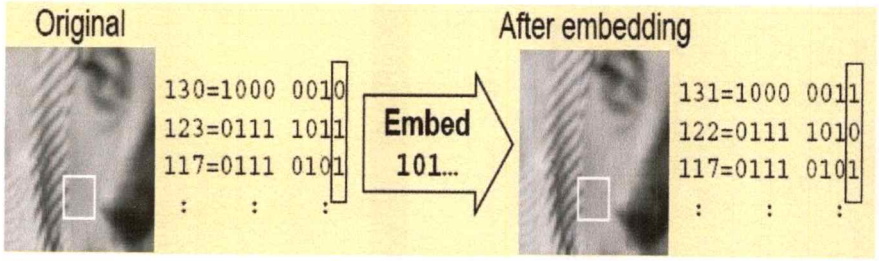
2.3.7.1 Least Significant Bit (LSB)

เป็นวิธีที่สามารถทำได้ง่าย เพียงแค่นำข้อมูลแต่ละบิตของข้อมูลลายน้ำดิจิตอลเข้าไปเก็บในบิตที่มีความสำคัญน้อยที่สุดของแต่ละไบต์ข้อมูลในภาพ ข้อดีของวิธีนี้ คือ ข้อมูลสามารถแทรกเข้าไปในภาพดิจิตอลได้มาก โดยไม่มีผลกระทบต่อการรับรู้ของมนุษย์ เนื่องจากบริเวณที่จะบรรจุข้อมูลลงไปนั้นเป็นบริเวณที่มีความสำคัญน้อยที่สุด ดังรูปที่ 2.14 จึงทำให้มีการเปลี่ยนแปลงน้อยที่สุด จึงทำให้ภาพก่อนและหลังทำการฝังลายน้ำดิจิตอลด้วยวิธีนี้ ไม่มีความแตกต่างที่สังเกตเห็นได้เลย อีกทั้งยังสามารถใส่ข้อมูลลงไปได้ในปริมาณที่มาก เช่น ภาพที่มีข้อมูลแต่ละพิกเซลมีขนาด 24 บิต โดยมีขนาดภาพ 20 x 20 พิกเซล จะสามารถบรรจุข้อมูลได้มากถึง 1200 บิต หรือ 150 ไบต์ ภาพดิจิตอลที่มีข้อมูลแต่ละพิกเซลมีขนาด 24 บิต เราสามารถใส่ข้อมูลลายน้ำดิจิตอลเข้าไปได้ 3 บิต ถ้าเราต้องการบรรจุตัวอักษร A เข้าไปเก็บในภาพ เราจำเป็นต้องใช้จำนวนพิกเซลทั้งหมด 3 พิกเซล



รูปที่ 2.14 รูปแบบการฝัง LSB

แต่เนื่องจากการสร้างลายน้ำดิจิตอลด้วยเทคนิคนี้เป็นการแก้ไขบิต ดังรูปที่ 2.15 ข้อเสียของวิธีนี้ คือจะทำให้ข้อมูลมีความทนทานต่ำ ซึ่งเมื่อใดที่ภาพดิจิตอลมีการแก้ไขหรือเปลี่ยนแปลงไปจากเดิม เช่น การตัดส่วนใดส่วนหนึ่งของภาพ หรือการปรับเปลี่ยนแปลงความเข้มแสงหรือสี ก็จะทำให้ข้อมูลที่ใส่ลงไป มีการเปลี่ยนแปลงไปได้ จึงทำให้การพิสูจน์ลายน้ำดิจิตอลก็จะล้มเหลว และถ้าหากมีการลบบิตค่าสุดท้าย LSB จะทำให้ภาพดิจิตอลที่มีลายน้ำดิจิตอลฝังอยู่ก็จะถูกทำลายด้วย



รูปที่ 2.15 การฝังข้อมูลแบบ LSB

2.3.7.2 Spread Spectrum (SS)

เป็นเทคนิคมอดูเลชันที่ใช้กันในระบบสื่อสารดิจิตอล ซึ่งสามารถนำมาประยุกต์ใช้กับการฝังลายน้ำดิจิตอลเข้าไปในภาพดิจิตอลได้เป็นอย่างดี ด้วยเทคนิคนี้เป็นการใช้สัญญาณรบกวนซึ่งเป็นหัวใจหลักของวิธีการกระจายแถบความถี่ จึงจะทำให้ลายน้ำดิจิตอลมีความคงทน ลบออกยาก และปลอดภัย เทคนิคการกระจายแถบความถี่

2.4 การเข้ารหัสและถอดรหัสลับแบบใช้กุญแจสาธารณะ (Public Key Cryptography)

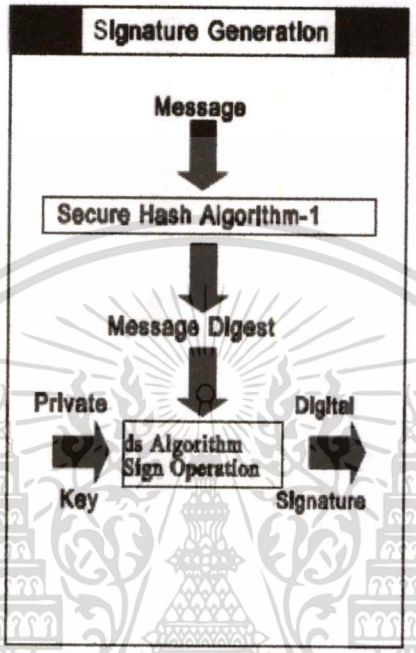
การรหัสแบบกุญแจสาธารณะหรืออสมมาตร เป็นการเข้าและถอดรหัสด้วยกุญแจที่ต่างกัน ด้วยการใช้คู่กุญแจ คือ กุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) โดยที่ไม่สามารถจะคำนวณหาค่าของกุญแจที่ใช้ในการถอดรหัสจากค่ากุญแจที่ใช้เข้ารหัสลับได้ หรืออาจจะต้องใช้เวลานานมากในการคำนวณหา โดยที่ข้อมูลจากผู้ส่งจะถูกเข้ารหัสด้วยกุญแจส่วนตัวและจะถูกถอดรหัสได้เพียงการใช้กุญแจสาธารณะ ที่เป็นคู่ของมันเท่านั้น ซึ่งการเข้ารหัสแบบนี้สามารถเปิดเผยกุญแจที่ถอดรหัสได้ แต่กุญแจส่วนตัวต้องเก็บไว้กับตัวคนเดียว ห้ามให้คนอื่นรู้ การเข้ารหัสแบบกุญแจอสมมาตรช่วยรักษาความปลอดภัยของข้อมูลได้เป็นอย่างดี นำไปสู่การเข้ารหัสและถอดรหัสลับแบบใช้กุญแจสาธารณะด้วยวิธีการเข้ารหัสแบบ RSA ซึ่งมาจากคนคิด 3 คน ชื่อ R. Rivest A.Sharmir และ L. Adleman ในปี 1978 ด้วยหลักการทางคณิตศาสตร์ของจำนวนเฉพาะ (Prime number) และการแยกตัวประกอบของจำนวนที่มีขนาดใหญ่ โดยใช้ mod ในการคำนวณเพื่อให้หาค่าจำนวนเศษที่เหลือจากการหาร ซึ่งการเข้ารหัสและถอดรหัสแบบ RSA เป็นระบบการเข้ารหัสแบบกุญแจสาธารณะที่รู้จักกันแพร่หลายที่สุด

2.5 ลายเซ็นดิจิตอล

การใช้ลายเซ็นดิจิตอลบนภาพดิจิตอล มีหลักการเหมือนกับการใช้ลายเซ็นที่ใช้ในเอกสารทั่วไป ที่สามารถพิสูจน์ได้ว่าลายเซ็นของใครจึงสามารถระบุถึงตัวบุคคลได้และไม่สามารถปลอมแปลงได้ โดยมีพื้นฐานจากการประยุกต์เทคนิคการเข้าและถอดรหัสลับแบบใช้กุญแจสาธารณะด้วยการใช้คู่กุญแจที่แตกต่างกัน คือ กุญแจส่วนตัวและกุญแจสาธารณะ ซึ่งมีมาตรฐานในการสร้าง

ลายเซ็นดิจิตอลนี้ พัฒนาขึ้นมาโดย NSA (National Security Agency) ในประเทศสหรัฐอเมริกาและได้รับการรับรองจาก NIST (National Institute of Standards and Technology)

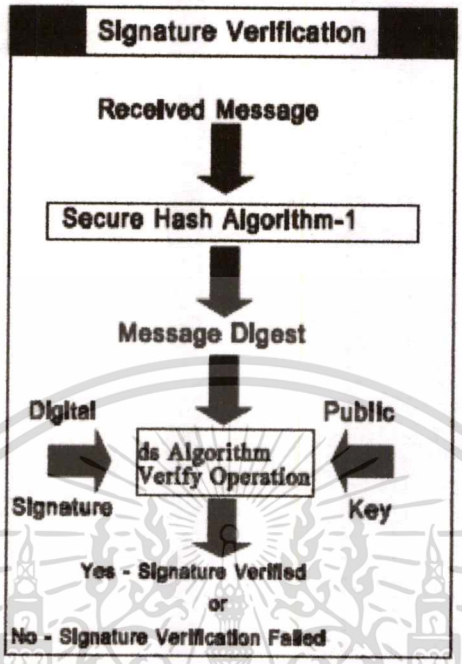
2.5.1 ขั้นตอนการสร้างลายเซ็นดิจิตอล



รูปที่ 2.16 การสร้างลายเซ็นดิจิตอล

1. เริ่มจากนำข้อความต้นฉบับที่ต้องการจะส่งนั้น มาผ่านกระบวนการทางคณิตศาสตร์ ที่เรียกว่า ฟังก์ชันแฮช (Hash function) เพื่อให้ได้ข้อความตัวแทนที่มีขนาดเล็กและมีเอกลักษณ์ ที่เรียกว่า ข้อความที่ย่อยแล้ว (Message Digest) โดยที่ฟังก์ชันนี้เป็นลักษณะแบบหนึ่งต่อหนึ่ง (One-to-One) และเป็นฟังก์ชันทางเดียว (One way) ทำให้ข้อความที่ได้มีขนาดเล็กกว่าข้อความที่นำมาคำนวณ แต่ยังคงความแตกต่างของข้อความต้นฉบับไว้ได้ และไม่สามารถนำผลลัพธ์ของฟังก์ชันนี้มาดำเนินการย้อนกลับเพื่อให้ได้ข้อความต้นฉบับ
2. จากนั้นนำข้อความที่ย่อยแล้วมาเข้ารหัสโดยใช้วิธีการเข้ารหัสแบบกุญแจสาธารณะ ที่ใช้กันแพร่หลาย คือ RSA โดยที่ผู้ส่งจะต้องใช้กุญแจส่วนตัวในการเข้ารหัส ซึ่งเป็นการรับรองว่ามีผู้สร้างลายเซ็นดิจิตอลเพียงคนเดียวเท่านั้น ผลลัพธ์ที่ได้ ก็คือ ลายเซ็นดิจิตอล
3. นำลายเซ็นดิจิตอลที่ได้มา แนบและส่งไปกับข้อความต้นฉบับ เพื่อใช้ยืนยันความถูกต้องของข่าวสาร โดยที่การส่งกุญแจสาธารณะที่ใช้ในการตรวจสอบลายเซ็นดิจิตอลไปพร้อมกับข้อความ หรือส่งไปให้ผู้รับไว้ก่อนก็ได้

2.5.2 ขั้นตอนการตรวจสอบลายเซ็นดิจิตอล



รูปที่ 2.17 การตรวจสอบลายเซ็นดิจิตอล

1. เมื่อผู้รับได้รับข้อความที่แนบมาพร้อมกับลายเซ็นดิจิตอลแล้ว จะต้องทำการแยกลายเซ็นดิจิตอลออกจากข้อความเพื่อมาถอดรหัส โดยใช้กุญแจสาธารณะเพื่อให้ได้ผลลัพธ์ของการแฮชของผู้สร้างลายเซ็น
2. ผู้รับนำข้อความที่ผ่านฟังก์ชันแฮชด้วยอัลกอริทึมเดียวกันกับที่ใช้ในการสร้างลายเซ็นดิจิตอล จะทำให้ได้ผลลัพธ์ของการแฮชของข้อความที่ได้รับ
3. จากนั้นนำผลของการแฮชในข้อที่ 1 และ 2 มาเปรียบเทียบกัน เพื่อตรวจสอบความถูกต้องของข้อความ ซึ่งถ้าหากผลที่ได้ตรงกัน แสดงว่าสามารถยืนยันได้ว่าข้อความที่ผู้รับได้รับถูกส่งโดยผู้สร้างลายเซ็นดิจิตอลจริง และเป็นข้อความที่ถูกต้อง แต่ถ้าหากว่าผลของการแฮชทั้งคู่ที่ออกมาไม่ตรงกัน แสดงว่า ข้อความที่ผู้รับได้รับไม่ใช่ข้อความต้นฉบับ มีการปลอมแปลงเกิดขึ้น

2.5.3 การแฮชข้อมูล

เป็นการสร้างข้อความย่อยเพื่อใช้เป็นตัวแทนของข้อความต้นฉบับโดยผ่านกระบวนการทางคณิตศาสตร์ ที่เรียกว่า ฟังก์ชันแฮช (Hash function) โดยข้อความย่อยนี้จะมีความยาวอยู่ระหว่าง 128 ถึง 256 บิตและจะไม่ขึ้นอยู่กับขนาดความยาวของข้อความต้นฉบับ ซึ่งอัลกอริทึมที่ใช้กันมากในการทำฟังก์ชันแฮช คือ SHA-1 เป็นอัลกอริทึมที่แก้ไขเพิ่มเติมมาจาก SHA (Secure Hash

Algorithm) ซึ่งได้รับการพัฒนาขึ้นมาเพื่อมาใช้งานร่วมกับการสร้างลายเซ็นดิจิตอล การสร้างข้อความย่อยด้วยอัลกอริทึมของ SHA-1 จะมีขนาดข้อความย่อย 160 บิต

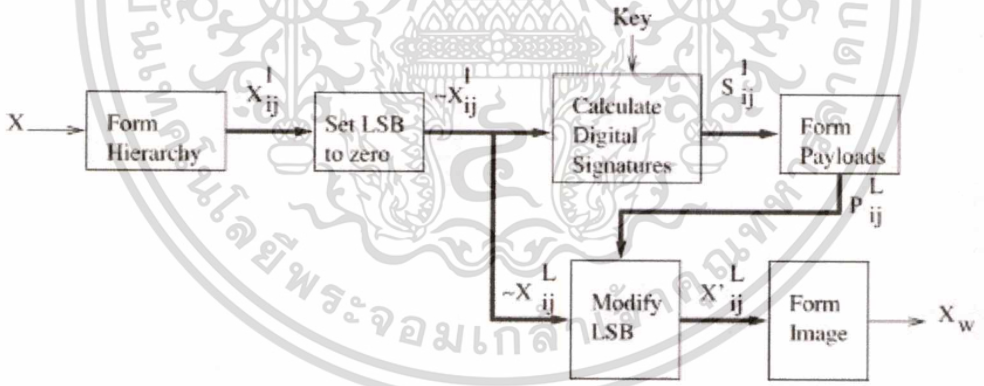
บทที่ 3
การตรวจสอบความถูกต้องของภาพดิจิตอล

3.1 การสร้างลายน้ำดิจิตอลแบบแบ่งลำดับชั้น

วิธีการสร้างลายน้ำดิจิตอลแบบแบ่งลำดับชั้น (Hierarchical Based Watermarking) เป็นการฝังและดึงลายน้ำดิจิตอลในลำดับชั้น ซึ่งจะสามารถตรวจสอบความถูกต้องของภาพดิจิตอลที่มีการแก้ไขเปลี่ยนแปลงทั้งภาพดิจิตอลหรือการแก้ไขเฉพาะที่ของภาพดิจิตอลได้ โดยมีแนวคิดจากการสร้างลายน้ำดิจิตอลแบบเปราะบางด้วยกุญแจสาธารณะของ Wong ที่คิดวิธีการฝังลายเซ็นดิจิตอลในบิต MSB (Most Significant Bit) ของบล็อกในภาพดิจิตอลเข้าไปใน LSB ของบล็อกเดียวกัน เพื่อช่วยในการตรวจสอบความถูกต้องของภาพดิจิตอล

3.1.1 การฝังลายน้ำดิจิตอลแบบแบ่งลำดับชั้น

กระบวนการฝังลายน้ำดิจิตอลของวิธีนี้ ดังรูปที่ 3.1 ประกอบไปด้วยสามขั้นตอนหลัก คือ การจัดบล็อกในลำดับชั้น การคำนวณลายเซ็นดิจิตอลและการฝังลายน้ำดิจิตอล เป็นภาพรวมของกระบวนการฝังลายน้ำดิจิตอล โดยค่า X คือภาพดิจิตอลที่มีขนาด M x N

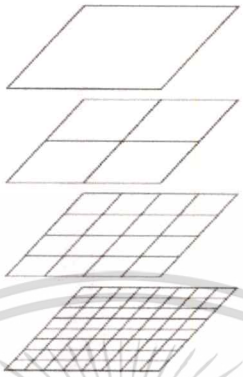


รูปที่ 3.1 ภาพรวมของกระบวนการฝังลายน้ำดิจิตอล

3.1.1.1 การจัดบล็อกในลำดับชั้น

ขั้นตอนแรกเริ่มจากการแบ่งภาพดิจิตอลออกเป็นบล็อกย่อยๆ ที่ไม่เหมือนกันและมีขนาด 2 x 2 บล็อก ขึ้นเป็นลำดับชั้น ซึ่งแต่ละบล็อกก็จะถูกแบ่งไปเรื่อยๆ จนได้ลำดับชั้นที่เหมาะสม ดังรูปที่ 3.2 เช่น ภาพดิจิตอลรูปหนึ่งถือเป็นหนึ่งบล็อกในลำดับชั้นที่หนึ่ง จากนั้นหนึ่งบล็อกถูกแบ่งออกเป็นบล็อกย่อยๆ ที่มีขนาด 2 x 2 บล็อก จะได้ 4 บล็อกติดกันในลำดับชั้นที่สอง และบล็อกแต่ละบล็อกในลำดับชั้นที่สองก็จะถูกแบ่งลงไปอีกในลำดับชั้นที่ 3 จะได้ 16 บล็อก ซึ่ง X^l_{ij} โดยที่ ij

คือ ตำแหน่งของพิกเซลบล็อก I คือ ชั้นของลำดับชั้นที่บล็อกนั้นๆ อยู่ ดังนั้นเมื่อจัดบล็อกในลำดับชั้นได้เหมาะสมแล้ว ในแต่ละบล็อกจะตั้งค่า LSB ของแต่ละพิกเซลในบล็อกนั้นๆ ให้เป็น 0 ซึ่งจะได้เป็น $\sim X_{ij}^{l}$ เอาไว้ใส่ข้อมูลของลายน้ำดิจิตอลเพื่อใช้ในการฝังลายน้ำดิจิตอลลงในภาพดิจิตอล

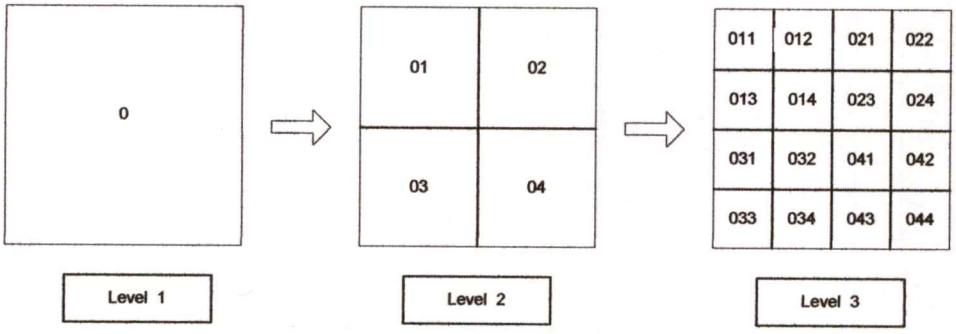


รูปที่ 3.2 การแบ่งภาพดิจิตอลออกเป็นบล็อกในลำดับชั้น

3.1.1.2 การคำนวณลายเซ็นดิจิตอล

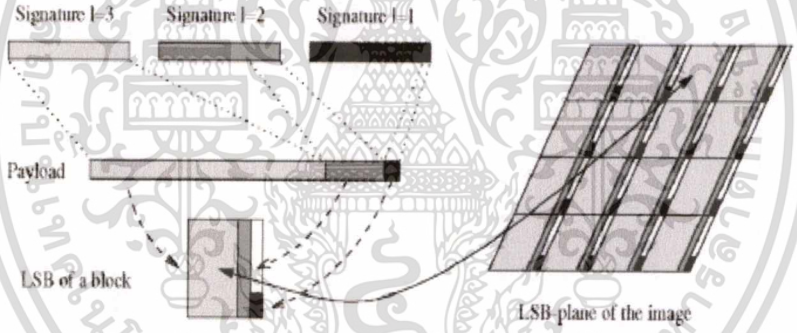
ขั้นตอนที่สองเป็นการนำข้อมูลภาพดิจิตอลแต่ละบล็อกในแต่ละลำดับชั้นมาเข้าฟังก์ชันแฮช เพื่อคำนวณหาลายเซ็นดิจิตอล เมื่อได้ข้อมูลที่ผ่านฟังก์ชันแฮชแล้ว นำมาเข้ารหัสข้อมูลด้วยการใช้กุญแจคู่แบบ Public Key Cryptography พร้อมด้วยการใช้กุญแจส่วนตัว (Private Key) ซึ่งในการเข้ารหัสไปพร้อมกับข้อมูลที่ได้จากการแฮช ผลที่ได้ คือ ลายเซ็นดิจิตอล S_{ij}^{l} ของแต่ละบล็อกในแต่ละลำดับชั้น ซึ่งจะได้อยู่ในรูปของข้อมูลที่เป็นบิตที่ต่อๆ กัน (Bit String) ดังนั้นในแต่ละชั้นจะมีข้อมูลลายเซ็นดิจิตอลที่แตกต่างกัน ดังรูปที่ 3.3 โดยเริ่มจากบล็อกใหญ่ของลำดับชั้นบนสุดจะมีลายเซ็นดิจิตอล 0 ของ Level 1 พอมาถึงชั้นที่สอง Level 2 ก็จะมีลายเซ็นดิจิตอลของแต่ละบล็อก คือ 01, 02, 03 และ 04 ซึ่งอยู่ในลำดับชั้นนี้ และในลำดับชั้นที่ Level 3 ก็จะมีลายเซ็นดิจิตอลของแต่ละบล็อก คือ 011, 012, 013, 014 โดยที่ 0 เป็นลายเซ็นดิจิตอลของลำดับชั้นที่หนึ่ง ต่อด้วยลายเซ็นดิจิตอลของชั้นที่สองก็คือ 1 และต่อท้ายด้วยลายเซ็นดิจิตอลของชั้นที่สาม ก็คือ 1 เลยได้เป็น 011 ที่เป็นลายเซ็นดิจิตอลของสามชั้นต่อกัน เป็นต้น ซึ่งจะสังเกตเห็นว่า แต่ละบล็อกของชั้นต่ำสุดจะมีลายเซ็นดิจิตอลของชั้นที่สูงกว่าพร้อมกับลายเซ็นดิจิตอลของชั้นมันเอง โดยข้อมูลลายเซ็นดิจิตอลจะสะสมเรื่อยมา

เมื่อได้ลายเซ็นดิจิตอลของแต่ละบล็อกและลำดับชั้นแล้ว ก็จะนำมาสร้างข้อมูล Payload เพื่อที่จะนำไปฝังลงในบล็อกที่ย่อยที่สุดในลำดับชั้นที่ต่ำสุด โดยเรียง Payload ที่ได้จากลายเซ็นดิจิตอล 0, 01, 011



รูปที่ 3.3 ลายเซ็นดิจิตอลของแต่ละบล็อกในแต่ละลำดับชั้น

ดังนั้นเมื่อได้ S_{ij}^{l} ของแต่ละบล็อกในแต่ละลำดับชั้นแล้ว ข้อมูลลายเซ็นดิจิตอลในแต่ละบล็อกของลำดับชั้นที่ย่อยที่สุด จะประกอบไปด้วยลายเซ็นดิจิตอลของชั้นที่หนึ่ง สองและสาม เป็นต้น ในการจัดรวมเป็นข้อมูล Payload ของลายเซ็นดิจิตอลในแต่ละบล็อกของทุกชั้นมาต่อกันเป็น P_{ij}^{L} ซึ่ง L คือ จำนวนชั้นทั้งหมดในลำดับชั้น



รูปที่ 3.4 การฝังข้อมูล Payload ลงในแต่ละบล็อกของภาพดิจิตอลด้วยเทคนิค LSB

ในโครงสร้างของข้อมูล Payload จะประกอบไปด้วย ดังรูปที่ 3.5 เพื่อจะนำไปฝังลายน้ำดิจิตอลในขั้นต่อไป

Sync Bit	Level	Block ID	Height of block	Width of block	Signature of each level

รูปที่ 3.5 โครงสร้างภายในของข้อมูล Payload

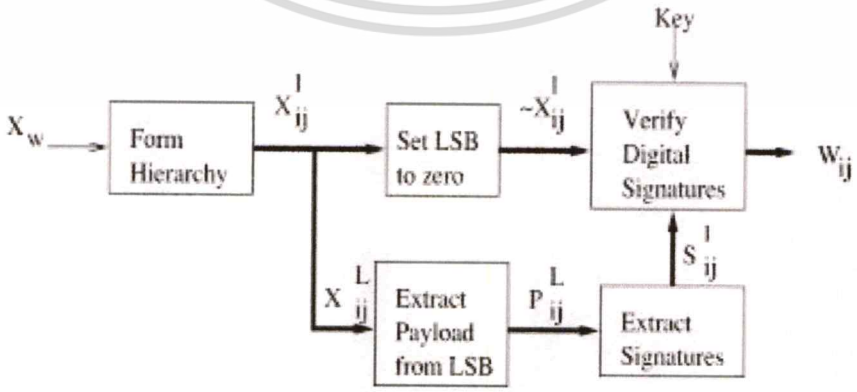
- Sync Bit คือ บิตที่ถูกกำหนดขึ้น เพื่อใช้ในการหาความสอดคล้องของบล็อกและบล็อกข้างเคียงของภาพดิจิตอล โดยกำหนดให้เป็น “1111111111111111”
- Level คือ ลำดับชั้นที่เหมาะสมในการแบ่งภาพดิจิตอลเพื่อนำไปฝังลายน้ำดิจิตอล
- Block ID คือ ตัวเลขเพื่อกำหนดหมายเลขของบล็อก ใช้ในการตรวจสอบความถูกต้องของภาพดิจิตอล
- Height of Block คือ ความสูงของบล็อก
- Width of Block คือ ความกว้างของบล็อก
- Signature of each level คือ ลายเซ็นดิจิตอลของแต่ละบล็อกในลำดับชั้นของมันเอง ที่มีการสะสมเรื่อยมา

3.1.1.3 การฝังลายน้ำดิจิตอล

ขั้นตอนสุดท้าย คือการฝังลายน้ำดิจิตอลโดยฝังที่บิต LSB ในแต่ละบล็อกของลำดับชั้นล่างสุดที่ตอนแรกเคยตั้งค่าให้เป็นศูนย์ ~ X_{ij}^{L} ฝังด้วยบิตของ Payload P_{ij}^{L} ที่ได้จากคำนวณลายเซ็นดิจิตอลของแต่ละบล็อกในแต่ละลำดับชั้นที่ต่อกันจะได้เป็น X'^{L}_{ij} ซึ่งเป็นการฝังด้วยเทคนิค LSB เป็นการฝังลายน้ำดิจิตอลเข้าไปโดยตรงในพิกเซลของภาพดิจิตอลที่เป็นบล็อกย่อยๆ ที่สุดในลำดับชั้น และผลที่ได้ คือ ภาพดิจิตอลที่ทำการฝังลายน้ำดิจิตอล X_w

3.1.2 การดึงลายน้ำดิจิตอลแบบแบ่งลำดับชั้น

กระบวนการดึงลายน้ำดิจิตอลของวิธีนี้ ดังรูปที่ 3.6 ประกอบไปด้วยสามขั้นตอน ซึ่งมีลักษณะคล้ายคลึงกับการฝังลายน้ำดิจิตอล คือ การจัดบล็อกในลำดับชั้น การดึงลายเซ็นดิจิตอลออกจากบล็อกและการตรวจสอบความถูกต้องของลายเซ็นดิจิตอล เป็นภาพรวมของกระบวนการดึงลายน้ำดิจิตอล โดยค่า X_w คือ ภาพดิจิตอลที่มีการฝังลายน้ำดิจิตอลไว้แล้ว



รูปที่ 3.6 ภาพรวมของกระบวนการดึงลายน้ำดิจิตอล

3.1.2.1 การจัดบล็อกในลำดับชั้น

ขั้นตอนแรกใช้การแบ่งภาพดิจิตอล X_w ออกเป็นบล็อกย่อยๆ และทำการจัดกลุ่มบล็อกขึ้นเป็นลำดับชั้นโดยรวมบล็อกที่ไม่เหมือนกันขนาด 2 x 2 บล็อก เช่นเดียวกันกับการฝังลายน้ำดิจิตอลดังที่กล่าวในหัวข้อ 3.1.1.2 และทำการตั้งค่า LSB ของแต่ละพิกเซลในแต่ละบล็อกให้เป็นศูนย์ จะได้เป็น $\sim X_{ij}^{l}$

3.1.2.2 การดึงลายเซ็นดิจิตอลออกจากบล็อก

ขั้นตอนที่สองจะทำการดึงข้อมูล Payload ออกจาก LSB ของแต่ละบล็อกในชั้นล่างสุดของลำดับชั้น X_{ij}^{L} ซึ่งข้อมูล Payload ที่ได้ P_{ij}^{L} ที่ประกอบไปด้วยลายเซ็นดิจิตอลของแต่ละบล็อกและลำดับชั้นที่ต่อกัน จากนั้นก็ต้องดึงลายเซ็นดิจิตอลของแต่ละชั้นและแต่ละบล็อกออกมา S_{ij}^{l} ซึ่งกระบวนการที่ใช้ในการดึงลายเซ็นดิจิตอลเป็นการทำย้อนกลับของการฝังลายน้ำดิจิตอลเพื่อที่จะกู้ลายเซ็นดิจิตอลคืนกลับมาของทุกบล็อกในแต่ละลำดับชั้น

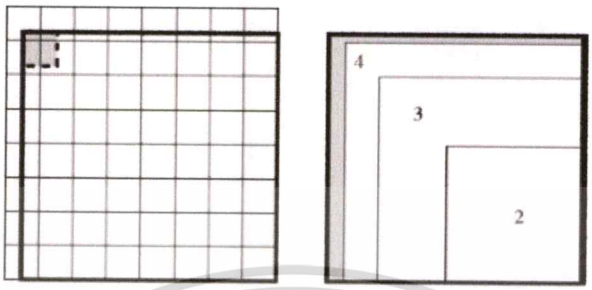
3.1.2.3 การตรวจสอบความถูกต้องของลายเซ็นดิจิตอล

ขั้นตอนสุดท้าย คือ การตรวจสอบความถูกต้องของลายเซ็นดิจิตอลว่าภาพดิจิตอลนั้นได้มีการแก้ไขเปลี่ยนแปลงหรือไม่ โดยจะทำการถอดลายเซ็นดิจิตอลออกมาของแต่ละบล็อกในแต่ละลำดับชั้น จากนั้นจะต้องทำการถอดรหัสด้วยกุญแจสาธารณะ (Public Key) เพื่อจะให้ได้ข้อมูลมาเพื่อมาเปรียบเทียบกับข้อมูลที่เข้าแฮชฟังก์ชันในตอนแรกว่าเท่ากันหรือไม่ โดยเทียบกันทีละบิต ถ้ามีบิตใดบิตหนึ่งเปลี่ยนแปลงไปจากเดิม แสดงว่าภาพดิจิตอลได้มีการแก้ไขเกิดขึ้นและผลที่ได้จากขั้นตอนนี้ คือ ความถูกต้องของข้อมูลลายน้ำดิจิตอลว่ามีจุดที่แก้ไขหรือเปลี่ยนแปลงหรือไม่ แล้วถ้ามีจะอยู่ ณ ตำแหน่งใดของบล็อกของลำดับชั้น

3.2 การตัดภาพดิจิตอล

การตัดภาพดิจิตอลออกเป็นส่วนย่อยเป็นการแก้ไขที่สามารถทำได้ง่ายที่สุด โดยขอบเขตสี่เหลี่ยมที่เล็กกว่าของภาพดิจิตอลรูปใหญ่จะถูกดึงขึ้นมาและส่วนที่เหลือของภาพดิจิตอลจะถูกตัดทิ้งออกไป ปัญหาที่เกิดขึ้นส่วนใหญ่ในการตรวจจับการตัดภาพดิจิตอลเกิดจากอัลกอริทึมในการตรวจจับลายน้ำดิจิตอลจะผิดพลาดในการตรวจสอบความถูกต้อง เนื่องจากเกิดความสูญเสียจังหวะของความสอดคล้อง (Loss of synchronization) ในขอบเขตของบล็อกจึงมีการใช้ "Sliding Window" ทำเป็นหน้าต่างเลื่อนในการค้นหา โดยจะช่วยเอาความสอดคล้องของขอบเขตบล็อกกลับคืนมา ดังนั้น ในลำดับชั้นก็สามารถใช้หน้าต่างเลื่อนในการค้นหาได้เช่นเดียวกัน ซึ่งจะสามารถตรวจจับการตัดภาพดิจิตอลได้ ดังรูปที่ 3.7 โดยในลำดับชั้นล่างสุดจะใช้หน้าต่างเลื่อนในการค้นหาด้วยขนาดบล็อก O x P และเมื่อภาพดิจิตอลในลำดับชั้นล่างสุดได้จังหวะความสอดคล้องของ

ขอบเขตบล็อกกลับคืนมา ก็จะสามารถใช้ “Sliding-Block Window” หน้าต่างเลื่อนแบบบล็อกในการค้นหาซึ่งจะมีขนาด 2 x 2 บล็อก ในการใช้หน้าต่างเลื่อนแบบบล็อกนี้จะสามารถจัดบล็อกขึ้นค้นหาในลำดับชั้นที่สูงขึ้นได้ จากการค้นหาจากบล็อกข้างเคียง



รูปที่ 3.7 การตรวจจับการตัดภาพดิจิตอล

บทที่ 4
การวิเคราะห์และออกแบบระบบ

4.1 การออกแบบแผนภาพการไหลข้อมูล (Data Flow Diagram)

ในการออกแบบระบบมักจะนำเสนอระบบด้วยแผนภาพเพื่อช่วยให้สามารถเข้าใจกระบวนการทำงานของระบบโดยรวมได้ง่ายยิ่งขึ้น ซึ่งแผนภาพการไหลข้อมูลนี้ แสดงถึงการไหลของข้อมูลทั้งอินพุตและเอาต์พุต โดยการวิเคราะห์ระบบนี้จะมองจากบนลงล่าง ซึ่งเป็นการไหลข้อมูลจากภาพกว้างๆ ของระบบก่อนและค่อยลงลึกสู่รายละเอียดของตัวระบบมากขึ้น เพื่อเป็นการกำหนดขอบเขตการทำงานของระบบ ซึ่งจะมีการแบ่งระดับของแผนภาพต่างๆ ดังนี้

4.1.1 แผนภาพการไหลข้อมูลระดับคอนเท็ค (Context Diagram)

แผนภาพระดับคอนเท็คนี้ เป็นแผนภาพระดับสูงสุด ที่แสดงถึงลักษณะโดยรวมของระบบ โดยมีตัวประมวลผลเพียงหนึ่งตัว ซึ่งเป็นการทำงานแทนทั้งระบบ ดังรูปที่ 4.1

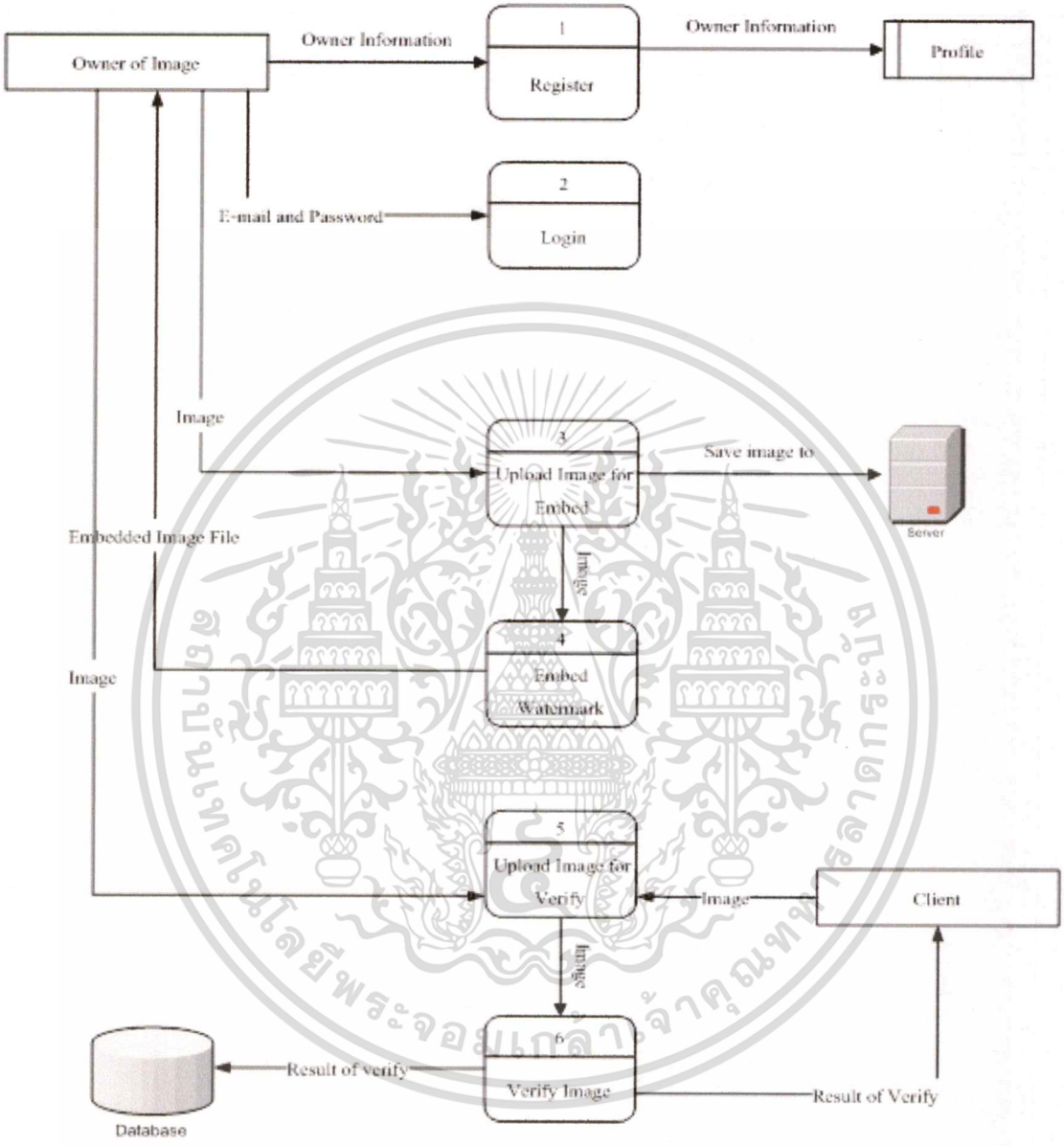
รูปที่ 4.1 คอนเท็คไดอะแกรมของระบบที่ให้บริการการพิสูจน์ความถูกต้องของภาพดิจิตอล

- Owner of image หมายถึง ระบบภายนอกซึ่งเป็นผู้ใช้บริการที่เป็นเจ้าของภาพดิจิตอลที่เข้ามาใช้งานระบบ
- Client หมายถึง ระบบภายนอกซึ่งเป็นผู้ใช้บริการที่ต้องการส่งภาพดิจิตอลมายังระบบเพื่อทำการตรวจสอบ
- Web base Image Authentication หมายถึง ตัวระบบที่ให้บริการการพิสูจน์ความถูกต้องของภาพดิจิตอล

4.1.2 แผนภาพการไหลข้อมูลระดับศูนย์ (Level 0)

แผนภาพระดับศูนย์นี้ เป็นแผนภาพที่แสดงถึงรายละเอียดเพิ่มเติมในแผนภาพระดับคอนเท็ค และมีการแตกขั้นตอนทำให้เห็นการทำงานชัดเจนยิ่งขึ้น ซึ่งจะประกอบไปด้วย ระบบ

ภายนอกหรือเอนติที เส้นการไหลของข้อมูล กระบวนการ และแหล่งเก็บข้อมูลต่างๆ จะแสดงให้เห็นในแผนภาพระดับนี้ ดังรูปที่ 4.2



รูปที่ 4.2 แผนภาพการไหลข้อมูลในระดับศูนย์ของระบบ

โดยเริ่มจากเจ้าของรูปภาพมีความประสงค์ที่ต้องการใช้บริการของระบบผ่านเว็บไซต์ เพื่อที่จะให้ระบบทำการฝังลายน้ำดิจิตอลลงในภาพดิจิตอลที่ต้องการ จึงจำเป็นต้องสมัครเป็นสมาชิกกับระบบก่อน จากนั้นสมาชิกกรอกอีเมลและรหัสผ่านเพื่อเข้าสู่ระบบ และทำการอัปโหลดรูปภาพที่ต้องการฝังลายน้ำดิจิตอลเข้าสู่ระบบ ระบบจะทำการฝังข้อมูลลายน้ำดิจิตอลลงในภาพดังกล่าว จากนั้นส่งไฟล์ภาพดิจิตอลกลับมายังเจ้าของรูปภาพ ในกรณีที่ลูกค้าไม่ได้เป็น

สมาชิกก็สามารถที่ใช้บริการของระบบได้ แต่ทำได้แค่เพียงตรวจสอบภาพดิจิตอลอย่างเดียวเท่านั้น โดยอัปโหลดภาพดิจิตอลที่ต้องการตรวจสอบ ระบบจะทำการตรวจสอบให้ ซึ่งจะบอกได้ว่าภาพดิจิตอลได้มาจากเจ้าของภาพจริงหรือไม่ หรือภาพดิจิตอลนี้มีการแก้ไขหรือไม่ เมื่อระบบตรวจสอบเสร็จแล้ว ก็จะส่งผลลัพท์ให้กับลูกค้า

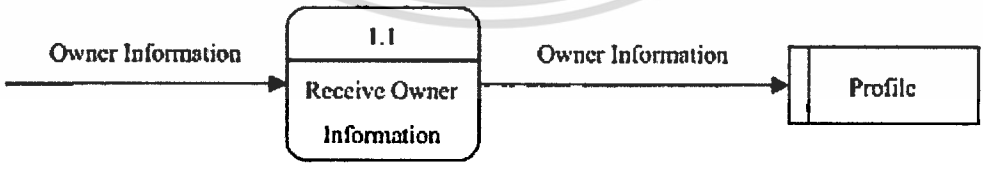
โดยจะแบ่งกระบวนการออกเป็น 6 ส่วนย่อยๆ ได้ดังนี้

1. Register ทำหน้าที่จัดการข้อมูลของเจ้าของภาพที่มาใช้บริการกับระบบ โดยเจ้าของภาพจะมาลงทะเบียนสมัครสมาชิกผ่านทางเว็บไซต์ของผู้ให้บริการตรวจสอบความถูกต้องของรูปภาพ
2. Login ทำหน้าที่ตรวจสอบเจ้าของรูปภาพที่เป็นสมาชิกว่ามีสิทธิ์เข้าสู่ระบบหรือไม่
3. Upload Image for Embed ทำหน้าที่อัปโหลดรูปภาพเข้าสู่ระบบ เพื่อเตรียมไว้ใช้ในการฝังลายน้ำดิจิตอล
4. Embed Watermark ทำหน้าที่นำรูปภาพที่ได้จากเจ้าของภาพมาฝังลายน้ำดิจิตอลลงในภาพ
5. Upload Image for Verify ทำหน้าที่อัปโหลดรูปภาพเข้าสู่ระบบเพื่อเตรียมไว้ใช้ในการตรวจสอบความถูกต้องของภาพดิจิตอล
6. Verify Image ทำหน้าที่ตรวจสอบความถูกต้องของภาพดิจิตอล

4.1.3 แผนภาพการไหลข้อมูลระดับลูกของแต่ละขบวนการที่แสดงในระดับศูนย์ (Level 1)

เป็นการแตกขั้นตอนย่อยเพื่อเพิ่มรายละเอียดในระดับลูกจากแผนภาพระดับศูนย์ โดยจะแสดงการไหลข้อมูลของแต่ละกระบวนการมากขึ้น ซึ่งเป็นการแตกกระบวนการ และมองลึกลงไปในรายละเอียดของแต่ละกระบวนการ แบ่งออกเป็น 6 กระบวนการ มีดังต่อไปนี้

กระบวนการที่ 1

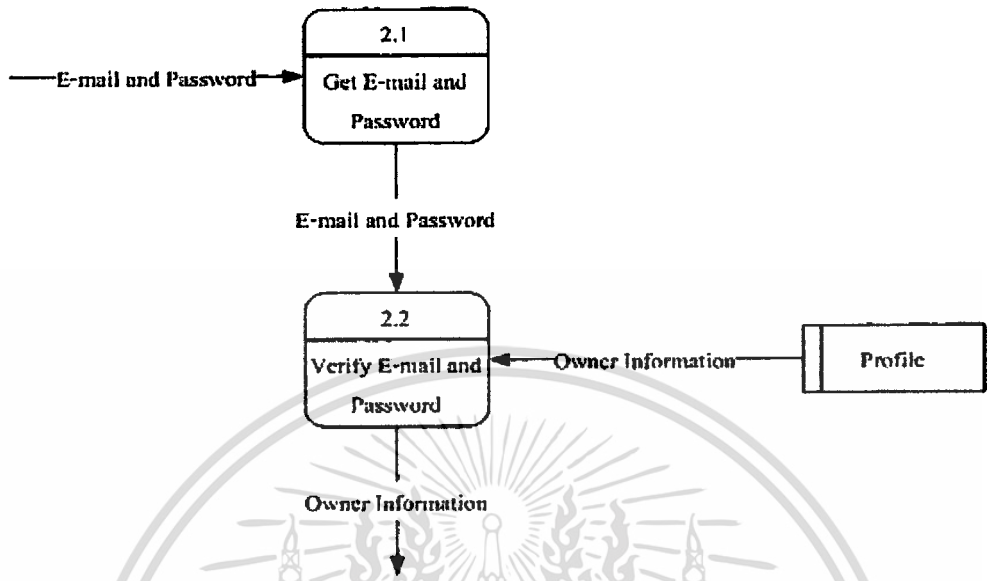


รูปที่ 4.3 แผนภาพการไหลข้อมูล Level 1 (Register)

จากรูปที่ 4.3 แสดงถึงการไหลข้อมูล Level 1 จะมีการทำงานเพียงหนึ่งส่วน ดังต่อไปนี้

1.1 Receive Owner Information ทำหน้าที่รับข้อมูลส่วนตัวของเจ้าของภาพที่มาใช้บริการกับระบบผ่านจากหน้าเว็บ จากนั้นระบบจะข้อมูลส่วนตัวของสมาชิกลงไปเก็บในแหล่งข้อมูล Profile

กระบวนการที่ 2



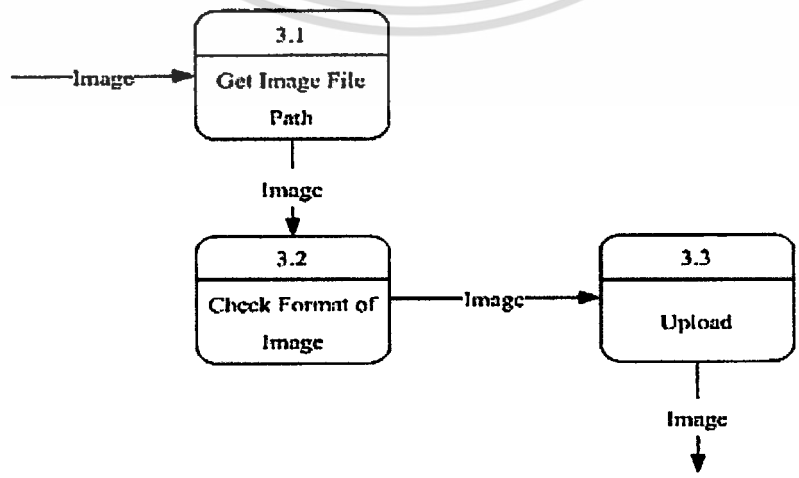
รูปที่ 4.4 แผนภาพการไหลข้อมูล Level 1 (Login)

จากรูปที่ 4.4 แสดงถึงการไหลข้อมูล Level 1 จะแบ่งการทำงานออกเป็น 2 ส่วน ดังต่อไปนี้

2.1 Get E-mail and Password ทำหน้าที่รับข้อมูลอีเมลและรหัสผ่านของเจ้าของภาพที่ป้อนเข้ามาในระบบ

2.2 Verify E-mail and Password ทำหน้าที่ตรวจสอบข้อมูลอีเมลและรหัสผ่านที่เจ้าของภาพส่งเข้ามาในระบบว่ามีสิทธิ์ที่จะเข้าสู่ระบบหรือไม่ โดยเอาข้อมูลที่เก็บในแหล่งข้อมูล Profile มาเทียบเพื่อยืนยันตัวตน

กระบวนการที่ 3



รูปที่ 4.5 แผนภาพการไหลข้อมูล Level 1 (Upload Image for Embed)

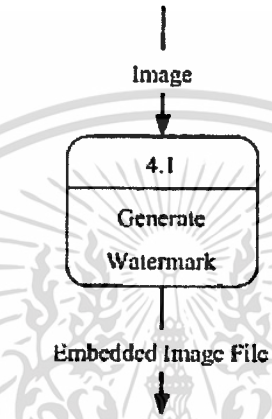
จากรูปที่ 4.5 แสดงถึงการไหลข้อมูล Level 1 จะแบ่งการทำงานออกเป็น 3 ส่วน ดังต่อไปนี้

3.1 Get Image File Path ทำหน้าที่รับข้อมูล Path ของไฟล์รูปภาพ

3.2 Check Format of Image ทำหน้าที่ตรวจสอบสกุลของไฟล์ภาพ

3.3 Upload ทำหน้าที่อัปโหลดรูปภาพที่เจ้าของภาพเลือกเอาไว้ อัปโหลดเข้าระบบ

กระบวนการที่ 4

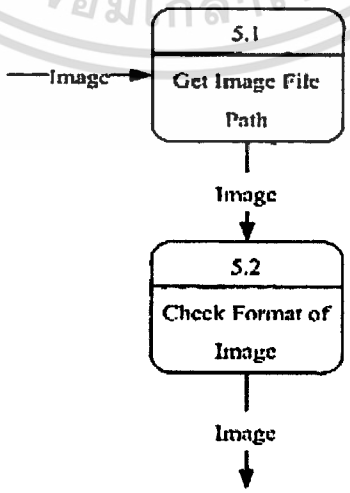


รูปที่ 4.6 แผนภาพการไหลข้อมูล Level 1 (Embed Watermark)

จากรูปที่ 4.6 แสดงถึงการไหลข้อมูล Level 1 มีการทำงานดังนี้

4.1 Generate Watermark ทำหน้าที่รับรูปภาพมา และทำการสร้างลายน้ำดิจิตอลขึ้นมาเพื่อที่จะนำไปฝังลงในรูปภาพ

กระบวนการที่ 5



รูปที่ 4.7 แผนภาพการไหลข้อมูล Level 1 (Upload Image for Verify)

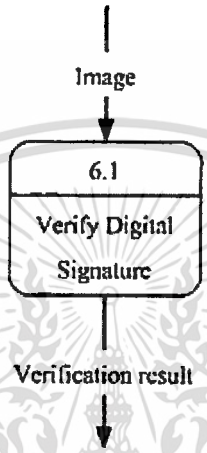
จากรูปที่ 4.7 แสดงถึงการไหลข้อมูล Level 1 จะแบ่งการทำงานออกเป็น 3 ส่วน ดังต่อไปนี้

5.1 Get Image File Path ทำหน้าที่รับข้อมูล Path ของไฟล์รูปภาพ

5.2 Check Format of Image ทำหน้าที่ตรวจสอบสกุลของไฟล์ภาพ

5.3 Upload ทำหน้าที่อัปโหลดรูปภาพที่เข้าของภาพเลือกเอาไว้ อัปโหลดเข้าระบบ

กระบวนการที่ 6



รูปที่ 4.8 แผนภาพการไหลข้อมูล Level 1 (Verify Image)

จากรูปที่ 4.8 แสดงถึงการไหลข้อมูล Level 1 มีการทำงานดังนี้

6.1 Verify Digital Signature ทำหน้าที่ตรวจสอบลายเซ็นดิจิตอลว่าถูกต้องหรือไม่

4.2 การออกแบบฐานข้อมูล

ในขั้นการออกแบบฐานข้อมูลนี้ มีเอนทิตี Profile คือ ข้อมูลเจ้าของภาพดิจิตอลที่สมัครเป็นสมาชิก ซึ่งมีพจนานุกรมข้อมูลของฐานข้อมูลสำหรับระบบให้บริการการพิสูจน์ความถูกต้องของภาพดิจิตอล

ตารางที่ 4.1 Profile

Attribute Name	Contents	Type	Format	Range	PK or FK	FK Referenced Table
FirstName	ชื่อสมาชิก	Char(25)	Xxxxxx	NA		
LastName	นามสกุลสมาชิก	Char(25)	Xxxxxx	NA		
BOD	วันเกิดของสมาชิก	DateTime	99999999	NA		
Sex	เพศของสมาชิก	Char(1)	X	M,F		

ตารางที่ 4.1 (ต่อ)

Attribute Name	Contents	Type	Format	Range	PK or FK	FK Referenced Table
Address	ที่อยู่ของสมาชิก	Char(50)	Xxxxxx	NA		
PhoneNo	เบอร์โทรศัพท์สมาชิก	Char(10)	(99) 999-9999	NA		
Email	อีเมลของสมาชิก	Char(30)	xxxxxx	NA	PK	
Password	รหัสผ่านของสมาชิก	Char(10)	xxxxxx	NA		
PrivateKey	กุญแจลับ	Char(1024)	xxxxxx	NA		
PublicKey	กุญแจสาธารณะ	Char(1024)	xxxxxx	NA		
userType	ประเภทของสมาชิก	Char(1)	X	P,C		

4.3 ภาพรวมของการทำงานในฟังก์ชันหลัก

การทำงานภายในระบบนี้สามารถแบ่งออกได้เป็น 2 ฟังก์ชันหลักที่สำคัญ คือ การฝังลายน้ำดิจิตอลลงในภาพดิจิตอลและการตรวจสอบความถูกต้องของภาพดิจิตอล ซึ่งภายใน 2 ฟังก์ชันหลักนี้ ยังมีกระบวนการทำงานย่อยๆ ซึ่งจะอธิบายถึงกระบวนการทำงานภายในของฟังก์ชันหลักดังต่อไปนี้

4.3.1 การฝังลายน้ำดิจิตอล

ฟังก์ชัน Upload Image

เป็นฟังก์ชันที่ทำหน้าที่รับภาพดิจิตอลจากผู้ใช้มายังที่เซิร์ฟเวอร์และตรวจสอบสกุลไฟล์ภาพดิจิตอลว่าเป็น BMP มีขั้นตอนการทำงาน ดังนี้

เลือกรูปที่ต้องการ

ตรวจสอบว่ามีรูปอยู่จริงตาม Path ที่กำหนด

ตรวจสอบว่าเป็นรูปสกุลไฟล์ BMP หรือไม่

ถ้าเป็น - ทำการอัปโหลดรูปเข้าสู่ระบบ

ถ้าไม่เป็น - แจ้งเตือนผู้ใช้

ฟังก์ชัน ReadImgUpload

เป็นฟังก์ชันที่ทำการอ่านภาพดิจิตอลที่ได้จากการอัปโหลด และทำการแปลงพิกเซลความกว้างและความสูงของภาพดิจิตอลให้เป็นเลขคู่ จากนั้นทำการแปลงค่าบิตสุดท้ายของสีฟ้าในแต่ละพิกเซลให้เป็นศูนย์ มีขั้นตอนการทำงาน ดังนี้

อ่านภาพดิจิตอลจาก Path ที่กำหนดอยู่ในเซิร์ฟเวอร์

ตรวจสอบความสูงของภาพดิจิตอลว่าเป็นเลขคู่หรือไม่

ถ้าเป็น – กำหนดค่าพิกเซลเดิม

ถ้าไม่เป็น – กำหนดค่าพิกเซลลบหนึ่ง

ตรวจสอบความกว้างของภาพดิจิตอลว่าเป็นเลขคู่หรือไม่

ถ้าเป็น – กำหนดค่าพิกเซลเดิม

ถ้าไม่เป็น – กำหนดค่าพิกเซลลบหนึ่ง

อ่านค่าสีน้ำเงิน (B) ของแต่ละพิกเซลจาก RGB ของภาพดิจิตอล

แล้วทำการเปลี่ยนค่าบิตสุดท้ายของสีฟ้าให้เป็นศูนย์

ฟังก์ชัน FindLevelImg

เป็นฟังก์ชันที่หาว่าภาพดิจิตอลสามารถแบ่งได้กี่ลำดับชั้น มีขั้นตอนการทำงาน ดังนี้

อ่านค่าพิกเซลความกว้างและความสูงของภาพดิจิตอล

นำพิกเซลของความสูงและความกว้างของภาพดิจิตอลมา mod ด้วย 2 ไปเรื่อยๆ โดยที่ผลลัพธ์ยังเป็น 0 และพิกเซลความกว้าง x ความสูงของบล็อกจะต้องรองรับข้อมูล Payload ทั้งหมด จากนั้น นำค่าจำนวนครั้งที่มากที่สุด คือ จำนวนลำดับชั้นที่เหมาะสมของภาพดิจิตอลที่จะแบ่งได้

ฟังก์ชัน WriteWM

เป็นฟังก์ชันที่ฝังลายน้ำดิจิตอลลงในภาพดิจิตอลโดยมีข้อมูล Payload ที่ภายในประกอบไปด้วย SyncData (ขนาด 16 บิต คือ “1111111111111111”) + level (ขนาด 8 บิต) + blockID (ขนาด 16 บิต) + Height (ขนาด 16 บิต) + Width (ขนาด 16 บิต) + [level x Signature (ขนาด 1024 บิต)] มีขั้นตอนการทำงาน ดังนี้

แปลงข้อมูลภาพดิจิตอลให้เป็นไบต์

นำข้อมูลที่ได้เข้าแฮชฟังก์ชัน ด้วย SHA1 ผลลัพธ์ที่ได้ นำไปเข้ารหัสข้อมูล ด้วย RSA พร้อมกุญแจส่วนตัว ซึ่งจะได้ลายเซ็นดิจิตอล

นำลายเซ็นดิจิตอลที่ได้ แปลงเป็นไบนารี

จากนั้นนำลายเซ็นดิจิตอลที่ได้ มาต่อกับข้อมูล Payload ซึ่งจะได้ข้อมูล Payload ใหม่

นำข้อมูล Payload ใหม่มาฝังลงภาพดิจิตอล

ทำขั้นตอนดังกล่าวทั้งหมดกับทุกๆ บล็อกในแต่ละลำดับชั้น

4.3.2 การตรวจสอบความถูกต้องของภาพดิจิตอล

ฟังก์ชัน Upload Image

เป็นฟังก์ชันที่ทำหน้าที่รับภาพดิจิตอลจากผู้ใช้มายังที่เซิร์ฟเวอร์และตรวจสอบสกุลไฟล์ภาพดิจิตอลว่าเป็น BMP มีขั้นตอนการทำงาน ดังนี้

เลือกรูปที่ต้องการ

ตรวจสอบว่ามีรูปอยู่จริงตาม Path ที่กำหนด

ตรวจสอบว่าเป็นรูปสกุลไฟล์ BMP หรือไม่

ถ้าเป็น - ทำการอัปโหลดรูปเข้าสู่ระบบ

ถ้าไม่เป็น - แจ้งเตือนผู้ใช้

ฟังก์ชัน ReadImgUpload

เป็นฟังก์ชันที่ทำการอ่านภาพดิจิตอลที่ได้จากการอัปโหลด และทำการแปลงพิกเซลความกว้างและความสูงของภาพดิจิตอลให้เป็นเลขคู่ จากนั้นทำการแปลงค่าบิตสุดท้ายของสีฟ้าในแต่ละพิกเซลให้เป็นศูนย์ มีขั้นตอนการทำงาน ดังนี้

อ่านภาพดิจิตอลจาก Path ที่กำหนดอยู่ในเซิร์ฟเวอร์

ตรวจสอบความสูงของภาพดิจิตอลว่าเป็นเลขคู่หรือไม่

ถ้าเป็น – กำหนดค่าพิกเซลเดิม

ถ้าไม่เป็น – กำหนดค่าพิกเซลลบหนึ่ง

ตรวจสอบความกว้างของภาพดิจิตอลว่าเป็นเลขคู่หรือไม่

ถ้าเป็น – กำหนดค่าพิกเซลเดิม

ถ้าไม่เป็น – กำหนดค่าพิกเซลลบหนึ่ง

อ่านค่าสีน้ำเงิน (B) ของแต่ละพิกเซลจาก RGB ของภาพดิจิตอล

แล้วทำการเปลี่ยนค่าบิตสุดท้ายของสีฟ้าให้เป็นศูนย์

ฟังก์ชัน FindMin

เป็นฟังก์ชันที่หาค่าของตำแหน่งพิกเซลในแกน x หรือ y ที่น้อยที่สุด จากค่าของตำแหน่ง SyncData ทุกตัวที่พบในแกน x หรือ y โดยหาค่าน้อยที่สุดจากชุดอะเรย์ใน dataInt โดยการเปรียบเทียบข้อมูลทีละตัวจนครบ

ฟังก์ชัน FindMinL2

เป็นฟังก์ชันที่หาค่าของตำแหน่งพิกเซลในแกน x หรือ y ที่รองจากค่าที่น้อยที่สุด จากค่าของตำแหน่ง SyncData ทุกตัวที่พบในแกน x หรือ y โดยหาค่าน้อยที่สุดจากชุดอะเรย์ใน dataInt โดยการเปรียบเทียบข้อมูลทีละตัวจนครบ

ฟังก์ชัน Verify

เป็นฟังก์ชันที่ใช้ในการตรวจสอบความถูกต้องของภาพดิจิตอลในแต่ละลำดับชั้น มีขั้นตอนการทำงาน ดังนี้

อ่านไฟล์ภาพดิจิตอล โดยเรียกใช้ ฟังก์ชัน ReadImgUpload2

ดึง LSB บิตของสีฟ้าของแต่ละพิกเซลในภาพดิจิตอลออกมา เพื่อเอาข้อมูล Payload

สแกนหาตำแหน่งของ SyncData

หาตำแหน่งของ (minX, minX2) (minY, minY2) ของบล็อก โดยเรียกใช้ฟังก์ชัน FindMin ในการหา min X และ minY และ ใช้ฟังก์ชัน FindMinL2 ในการหา minX2 และ minY2 เพื่อจะได้ทราบขอบเขตของความกว้าง x สูงของบล็อก

หา Level ขนาด 8 บิตในข้อมูล Payload ที่ต่อจาก SyncData ของบล็อก

สร้างโครงสร้าง tree ให้เป็นลำดับชั้น ซึ่งมี 3 ลำดับ ได้แก่ ชั้นที่ 1 คือ root ชั้นที่สอง คือ parent และชั้นที่สาม คือ child

ในขั้นของการตรวจสอบความถูกต้องของภาพดิจิตอล จะทำกระบวนการดังกล่าวกับทุกบล็อกในแต่ละลำดับชั้นที่มีลายน้ำดิจิตอลฝังอยู่ ดังต่อไปนี้

เอาข้อมูลตำแหน่ง (StartX, StartY) และ (EndX, EndY) ของบล็อกไปหาลายเซ็นดิจิตอล

ตัดเอาเฉพาะลายเซ็นดิจิตอลของลำดับชั้นที่ต้องการ

แปลงข้อมูลลายเซ็นดิจิตอลจาก String เป็น Byte

นำข้อมูลของขอบเขตภาพดิจิตอล มาเปลี่ยนค่าบิตสุดท้ายของสีฟ้าให้เป็นศูนย์ แล้วนำไปเข้าแฮชฟังก์ชัน ซึ่งจะได้ข้อมูลแฮช

นำข้อมูลแฮชที่ได้ ลายเซ็นดิจิตอล และกุญแจสาธารณะ มาตรวจสอบความถูกต้องว่าข้อมูลถูกต้องหรือไม่ถูกต้อง

ถ้าตรวจสอบว่าข้อมูลถูกต้อง – แสดงว่าภาพไม่มีการแก้ไข

ถ้าตรวจสอบว่าข้อมูลไม่ถูกต้อง – แสดงว่าภาพมีการแก้ไขเกิดขึ้น

การแสดงผลการตรวจสอบ

ถ้าบล็อกที่แสดงสีเขียว คือ ส่วนที่ถูกต้อง

ถ้าบล็อกที่แสดงสีแดง คือ ส่วนที่มีการดัดแปลงแก้ไข

ถ้าบล็อกที่ไม่มีสี คือ บริเวณที่ไม่สามารถตรวจสอบได้

4.3.3 กระบวนการสร้างลายเซ็นดิจิตอล

คลาสและฟังก์ชันที่จำเป็นสำหรับการสร้างลายเซ็นดิจิตอลของ .NET Framework ซึ่งภายในสามารถแบ่งหน้าที่ออกได้ขั้นตอน คือ ขั้นตอนการ Hash ข้อมูล และกระบวนการสร้างลายเซ็นดิจิตอล มีดังต่อไปนี้

- SHA1Managed
- RSACryptoServiceProvider

1. SHA1Managed

เป็นคลาสที่เอาไว้ย่อหรือสรุป (Hash) ข้อมูลขนาดใหญ่เพื่อให้ได้ข้อมูลที่มีขนาดที่เล็กลง (Message Digest) ด้วยอัลกอริทึม SHA-1 (Secure Hash Algorithm) ซึ่งจะมีฟังก์ชันให้เรียกใช้ คือ ฟังก์ชัน ComputeHash(DataImgBlock) ซึ่งจะได้ข้อมูลที่ย่อย HashImgData แล้วมีขนาด 160 บิต ดังนั้นผลของการ Hash ข้อมูลภาพดิจิตอลของสองชุดจะตรงกันก็ต่อเมื่อตัวข้อมูลภาพดิจิตอลต้องตรงกันด้วย ดังนั้นถ้ามีการเปลี่ยนแปลงเพียงเล็กน้อยกับตัวข้อมูลภาพดิจิตอลก็ทำให้ผลลัพธ์จากการ Hash ผิดพลาดเช่นเดียวกัน

2. RSACryptoServiceProvider

เป็นคลาสที่เอาไว้สร้างลายเซ็นดิจิตอล ด้วยอัลกอริทึมของ RSA ซึ่งเป็นการเข้ารหัสแบบ Asymmetric Encryption เพื่อที่จะตรวจสอบความถูกต้องของข้อมูล โดยมีฟังก์ชันให้เรียกใช้ คือ ฟังก์ชัน SignHash (HashImgData, "SHA1") ซึ่งจะได้ Signature ที่มีขนาด 128 ไบต์ หรือ 1024 บิต ซึ่งจะต้องขึ้นอยู่กับขนาดของ Private Key ที่ใช้ว่ามีขนาดเท่าไร สามารถอธิบายถึงการทำงานของฟังก์ชันนี้ได้ด้วย

$$H_{ij}^{l} = Hash(\tilde{X}_{ij}^{l} \| [top])$$
$$S_{ij}^{l} = SignHash(H_{ij}^{l}, Key_{private})$$

ในทางกลับกัน เวลาที่จะต้องการตรวจสอบจึงต้องใช้ฟังก์ชัน VerifyHash (HashImgData, "SHA1", Signature) ซึ่งจะได้ผลออกมาเป็นถูกหรือผิด (Boolean)

$$True\ or\ False = VerifyHash(\hat{S}_{ij}^{l}, Key_{public})$$

เมื่อผลออกว่าถูก แสดงว่าการตรวจสอบลายเซ็นดิจิตอลแล้วถูกต้อง ภาพดิจิตอลดังกล่าวไม่ได้มีการแก้ไข แต่ถ้าผลออกว่าผิด แสดงว่ามีการปลอมแปลงเกิดขึ้น

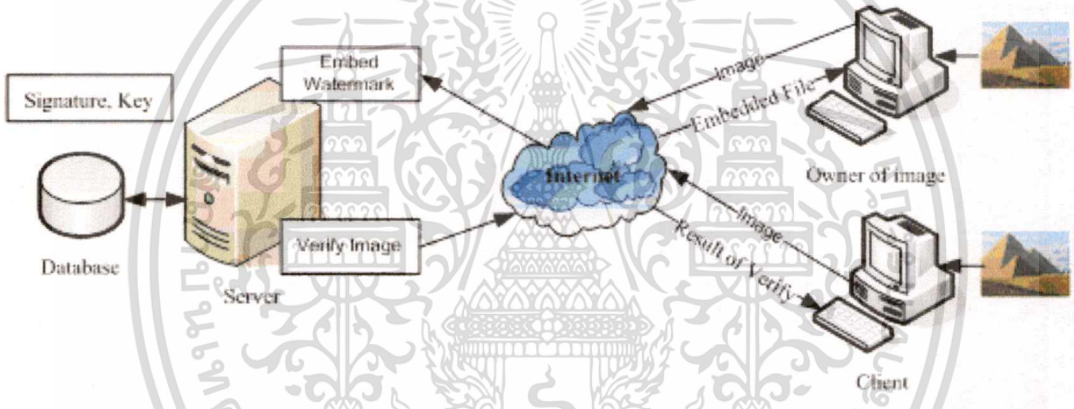
$$Verified = \begin{cases} True, & if\ \hat{H}_{ij}^{l} = \mathrm{H}(\widetilde{X}_{ij}^{l}) \\ False, & Otherwise \end{cases}$$

บทที่ 5
การพัฒนาระบบ

5.1 เครื่องมือในการพัฒนาระบบ

ในการพัฒนาระบบได้ใช้เครื่องมือในการเขียนโปรแกรม Microsoft Visual Studio .NET โดยใช้ ASP.NET เพื่อประมวลผลออกหน้าเว็บได้ ซึ่งโค้ดภายในเขียนด้วย VB.NET และเชื่อมโยงกับ Microsoft SQL Server 2000 ในการดูแลและจัดการฐานข้อมูล

5.2 โครงสร้างระบบ



รูปที่ 5.1 ภาพรวมของระบบพิสูจน์ความถูกต้องของภาพดิจิตอล

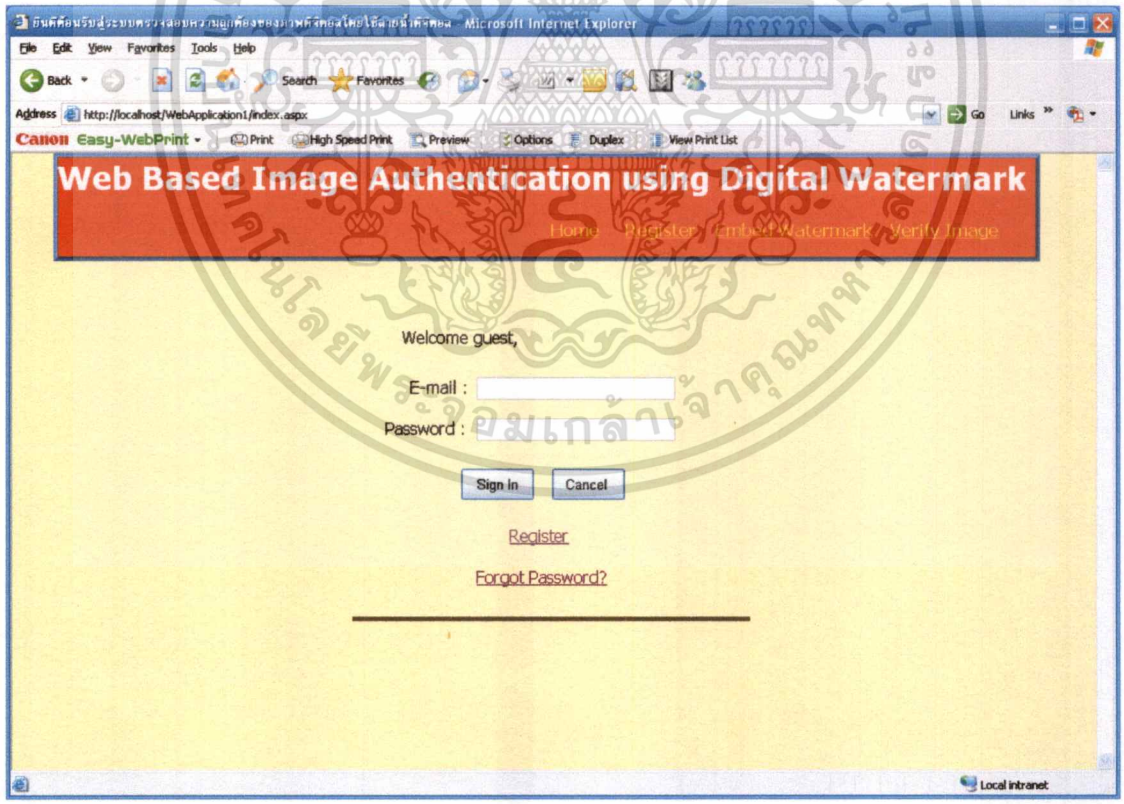
โครงสร้างของระบบ เป็นระบบที่ให้บริการการตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์ ดังนั้นการติดต่อสื่อสารของระบบจึงเป็นในลักษณะของไคลเอนท์เซิร์ฟเวอร์ (Client-Server) โดยการทำงานและการประมวลผลต่างๆ ของระบบจะทำอยู่บนฝั่งเซิร์ฟเวอร์ แล้วค่อยส่งผลไปยังไคลเอนท์ ซึ่งภายในระบบจะมองลูกค้าออกเป็น 2 มุม คือ อย่างแรกในมุมของเจ้าของภาพดิจิตอลซึ่งเป็นคนอัปโหลดภาพดิจิตอลต้นฉบับเข้าสู่ระบบ ซึ่งสามารถแบ่งออกได้เป็น 2 อย่าง คือ สมาชิกส่วนบุคคลหรือสมาชิกส่วนของบริษัท และอย่างที่สองในมุมของบุคคลทั่วไปที่ต้องการเอาภาพดิจิตอลมาตรวจสอบความถูกต้องกับระบบ โดยแสดงภาพรวมของระบบ ดังรูปที่ 5.1 ดังนั้นแนวทางในการพัฒนาระบบผ่านเว็บจะเริ่มจาก ผู้ที่เป็นเจ้าของภาพดิจิตอลจะเข้ามาใช้บริการในระบบนี้จำเป็นต้องลงทะเบียนสมัครเป็นสมาชิกกับระบบก่อนจึงจะเข้าใช้ระบบได้ ซึ่งข้อมูลต่างๆ ของผู้ใช้จะถูกบันทึกลงในฐานข้อมูลของระบบ จากนั้นเมื่อผู้ใช้ต้องการเข้าใช้ระบบก็จะทำการล็อกอินเข้าผ่านทางหน้าเว็บด้วยชื่ออีเมลผู้ใช้และรหัสผ่านเพื่อเป็นการยืนยันตัวตนในการ

เข้าใช้ระบบ ซึ่งเจ้าของภาพดิจิตอลจะทำการอัปโหลดภาพดิจิตอลมายังระบบ เพื่อทำการฝังลายน้ำดิจิตอลลงในตัวภาพดิจิตอล แล้วเก็บข้อมูลบางส่วนลงในฐานข้อมูลของระบบและส่งไฟล์รูปภาพที่ทำการฝังแล้วมาให้เจ้าของภาพดาวน์โหลด เมื่อลูกค้าต้องการนำภาพดิจิตอลมาตรวจสอบ ก็จะทำการอัปโหลดภาพที่ต้องการตรวจสอบเข้าสู่ระบบ ระบบจะทำการตรวจสอบภาพดิจิตอลนั้นและแจ้งผลในการตรวจสอบให้ลูกค้าทราบว่าภาพดิจิตอลนั้นๆ ได้มีการแก้ไขหรือไม่ ถ้ามีจะอยู่ณ. ตำแหน่งใดบ้าง

5.3 หน้าจอการทำงานของโปรแกรม

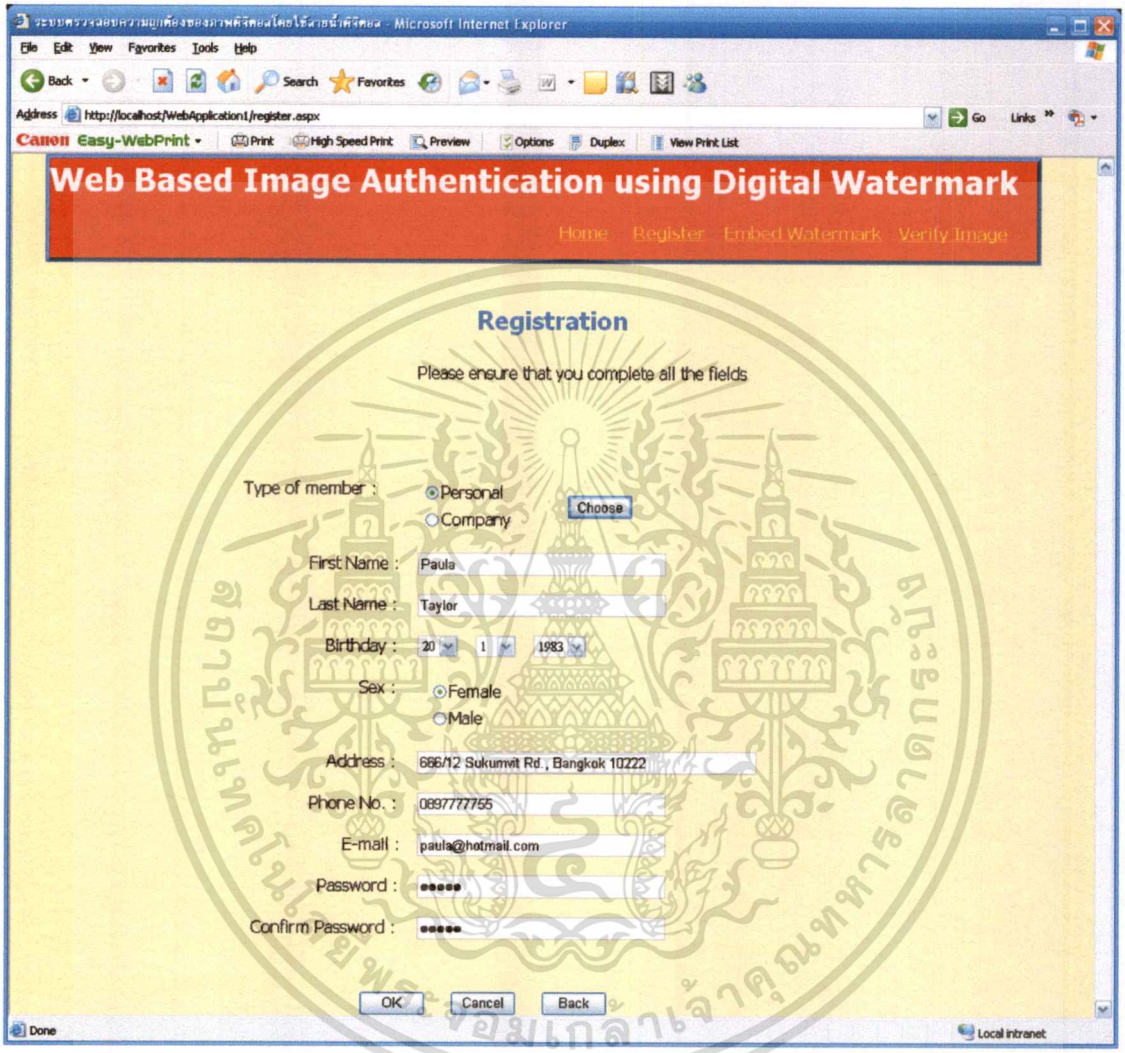
5.3.1 หน้าจอให้บริการ

จากการที่ได้วิเคราะห์และออกแบบระบบจนได้ส่วนติดต่อผู้ใช้งาน โดยผู้ที่จะใช้บริการของนี้ คือ เจ้าของภาพและลูกค้าทั่วไป ซึ่งเจ้าของภาพดิจิตอลจำเป็นต้องลงทะเบียนสมัครเป็นสมาชิกก่อน แต่ถ้าเป็นลูกค้าทั่วไป ก็สามารถอัปโหลดรูปภาพเข้าตรวจสอบได้เลย โดยไม่ต้องสมัครสมาชิก เมื่อเข้าเว็บไซต์ จะพบเว็บไซต์หน้าแรกของระบบ ดังรูปที่ 5.2

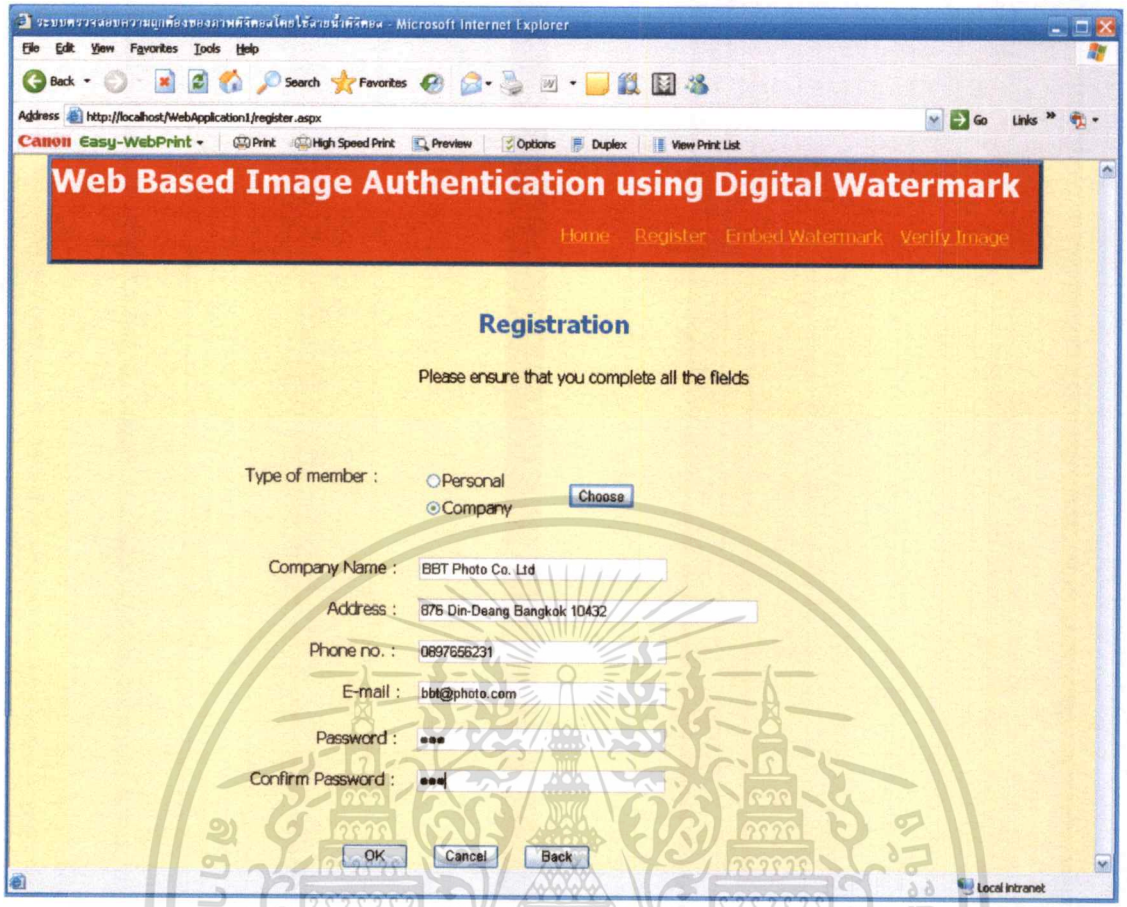


รูปที่ 5.2 หน้าแรกของระบบให้บริการการตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์

เพื่อต้องการสมัครสมาชิกกับระบบให้เจ้าของภาพดิจิตอลคลิกลงทะเบียน จากนั้นเจ้าของภาพดิจิตอลกรอกรายละเอียดส่วนตัว ซึ่งระบบมีตัวเลือกให้เลือกประเภทของสมาชิกว่าเป็นส่วนตัวหรือส่วนของบริษัท ดังรูปที่ 5.3 และ 5.4 ตามลำดับ

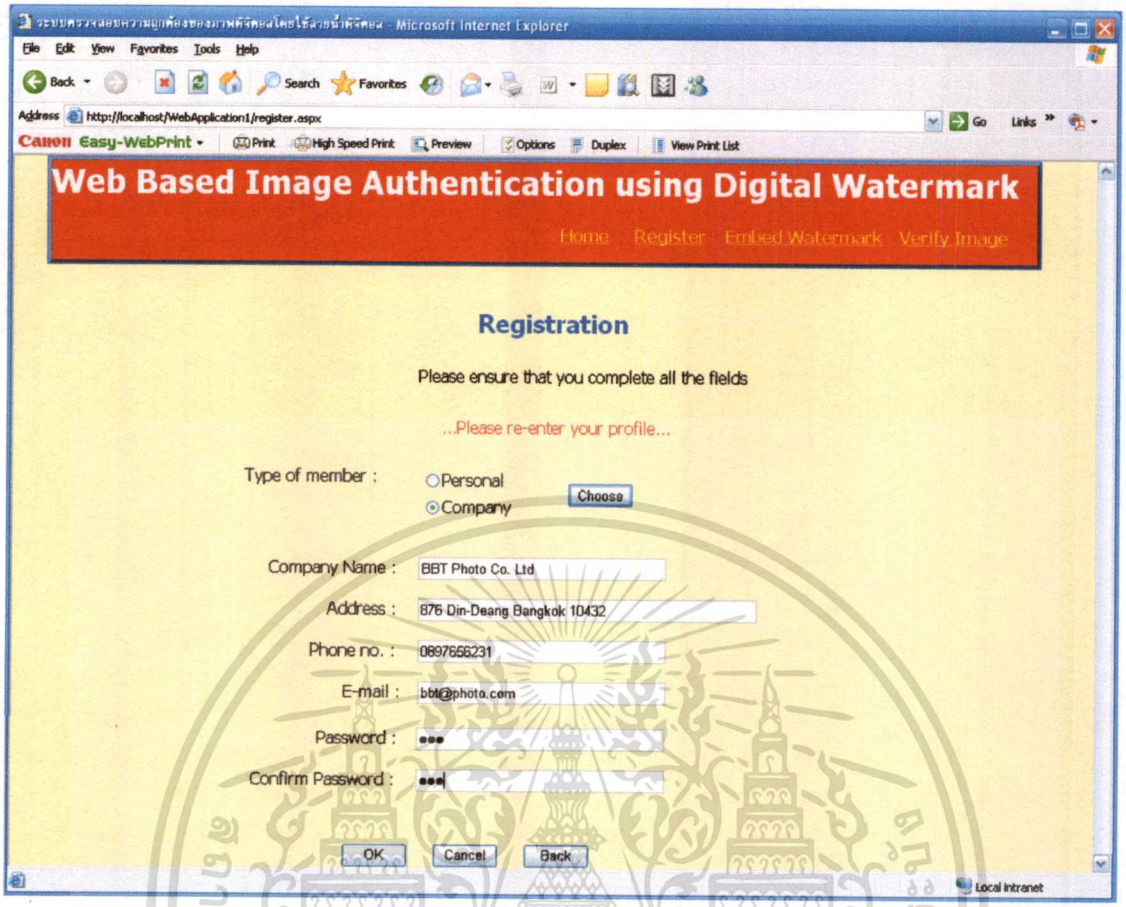


รูปที่ 5.3 หน้าจอการลงทะเบียนสมัครสมาชิกส่วนตัว



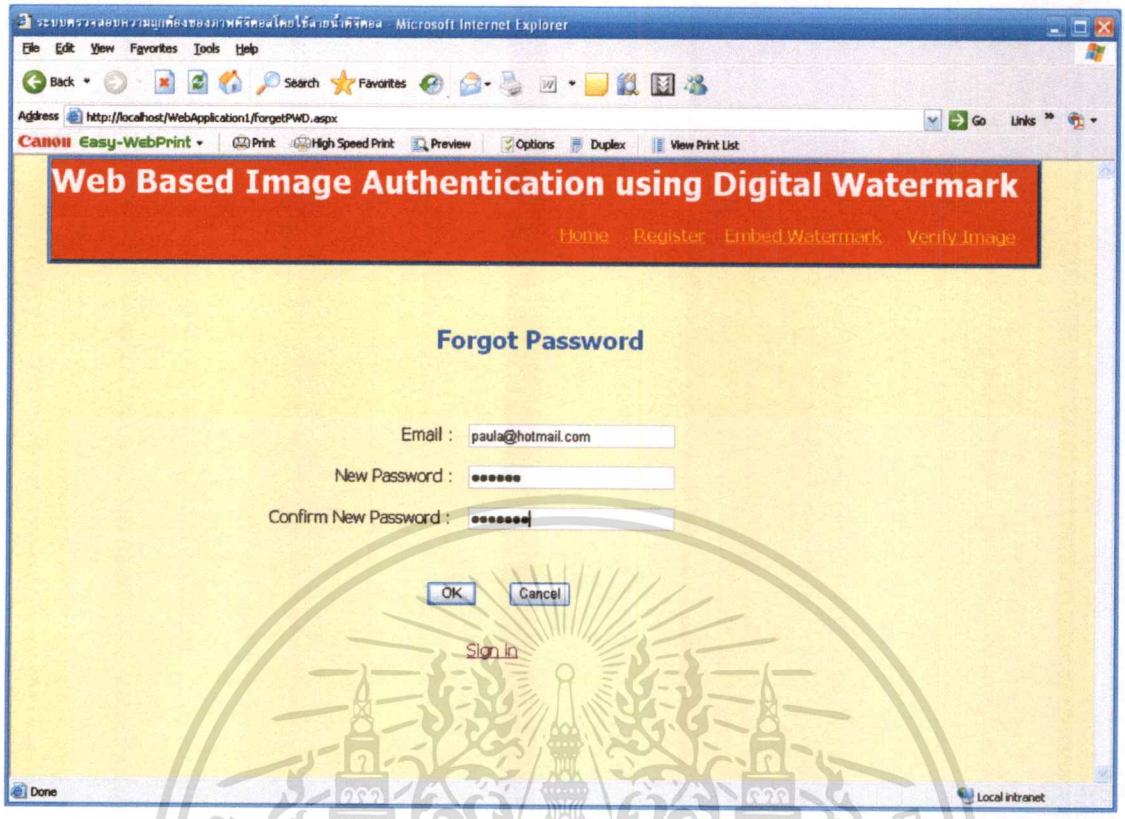
รูปที่ 5.4 หน้าจอการลงทะเบียนสมัครสมาชิกส่วนของบริษัท

เมื่อใดที่สมาชิกกรอกรายละเอียดส่วนตัวไม่ถูกต้อง เช่น รหัสผ่านและยืนยันรหัสผ่านไม่ตรงกัน ระบบจะใช้สมาชิกกรอกรายละเอียดส่วนตัวใหม่ ดังรูปที่ 5.5

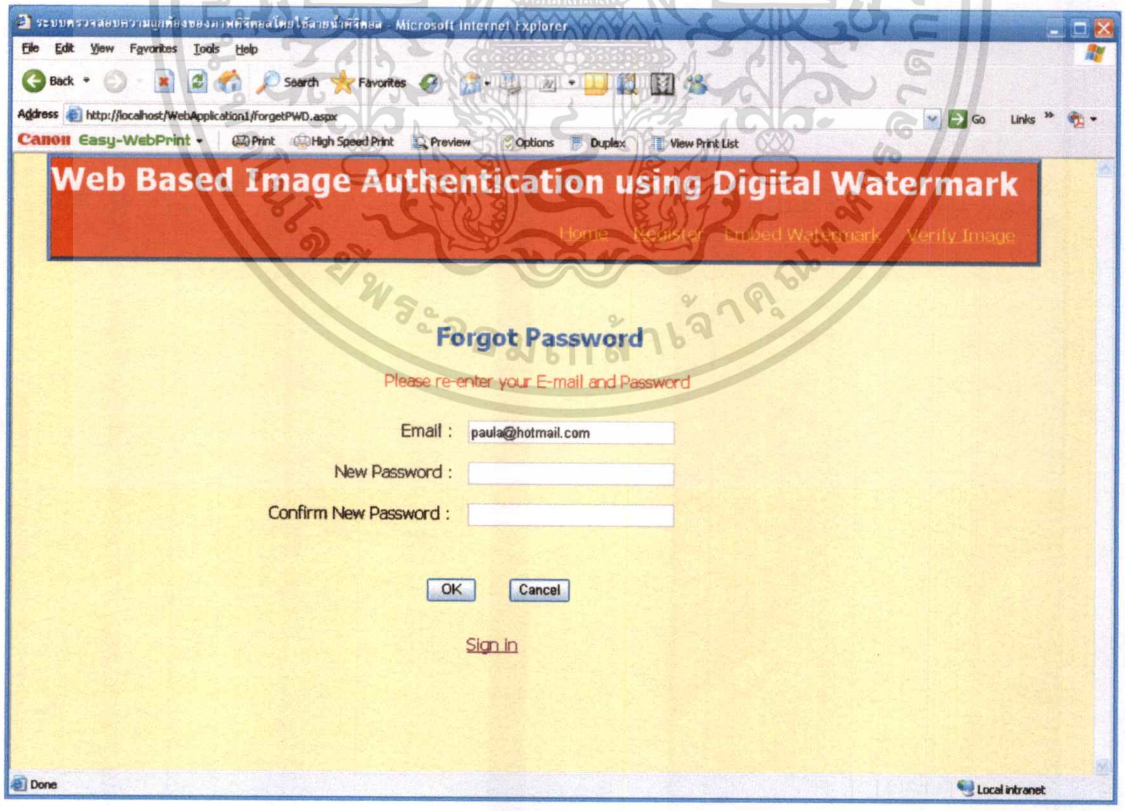


รูปที่ 5.5 หน้าจอการกรอกรายละเอียดส่วนตัวไม่ถูกต้อง

ในการใช้งานผ่านเว็บไซต์ ถ้าสมาชิกผู้ใดลืมรหัสผ่านให้คลิก Forgot Password ที่หน้าแรกของเว็บ แล้วกรอกรหัสผ่านใหม่ ดังรูปที่ 5.6 ระบบจะปรับรหัสผ่านใหม่ให้กับสมาชิก ดังรูปที่ 5.7

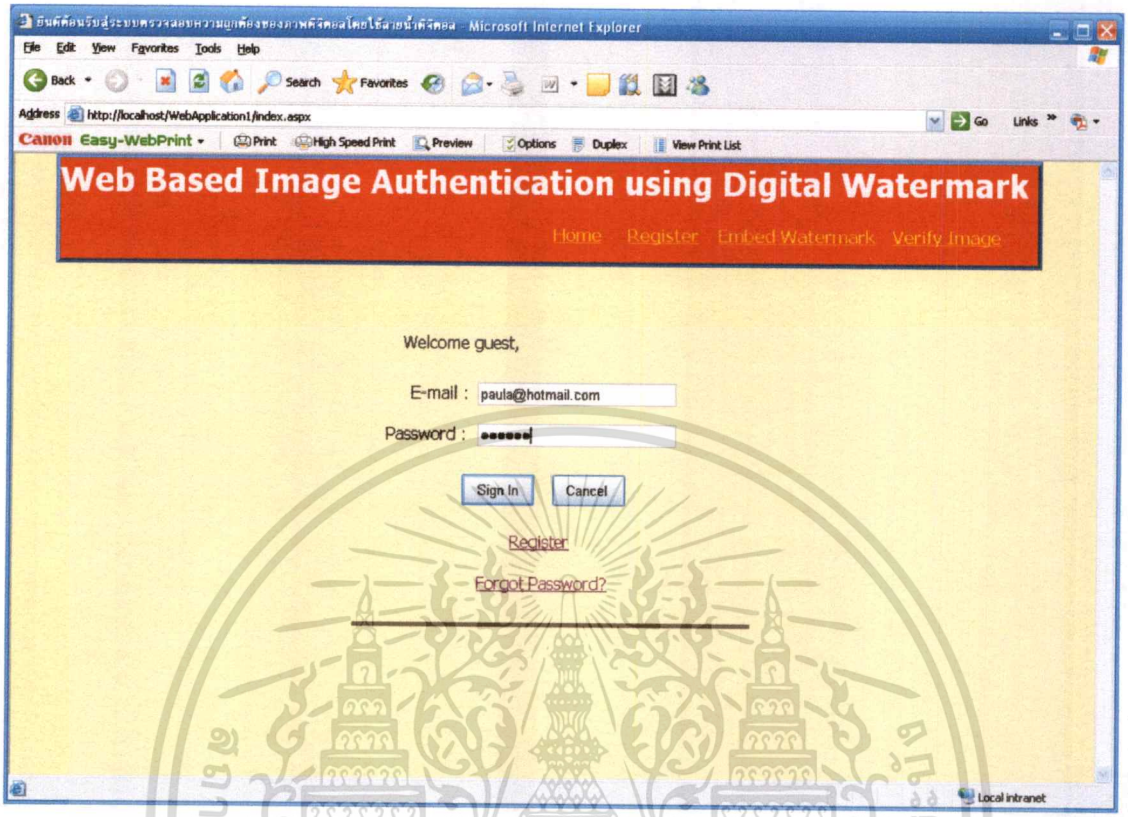


รูปที่ 5.6 หน้าจอลืมรหัสผ่านของสมาชิก



รูปที่ 5.7 หน้าจอแสดงผลการปรับรหัสผ่านใหม่ของสมาชิก

จากหน้าแรกของเว็บนั้น กรอกอีเมลและรหัสผ่านของสมาชิกเพื่อเข้าสู่ระบบ ดังรูป 5.8

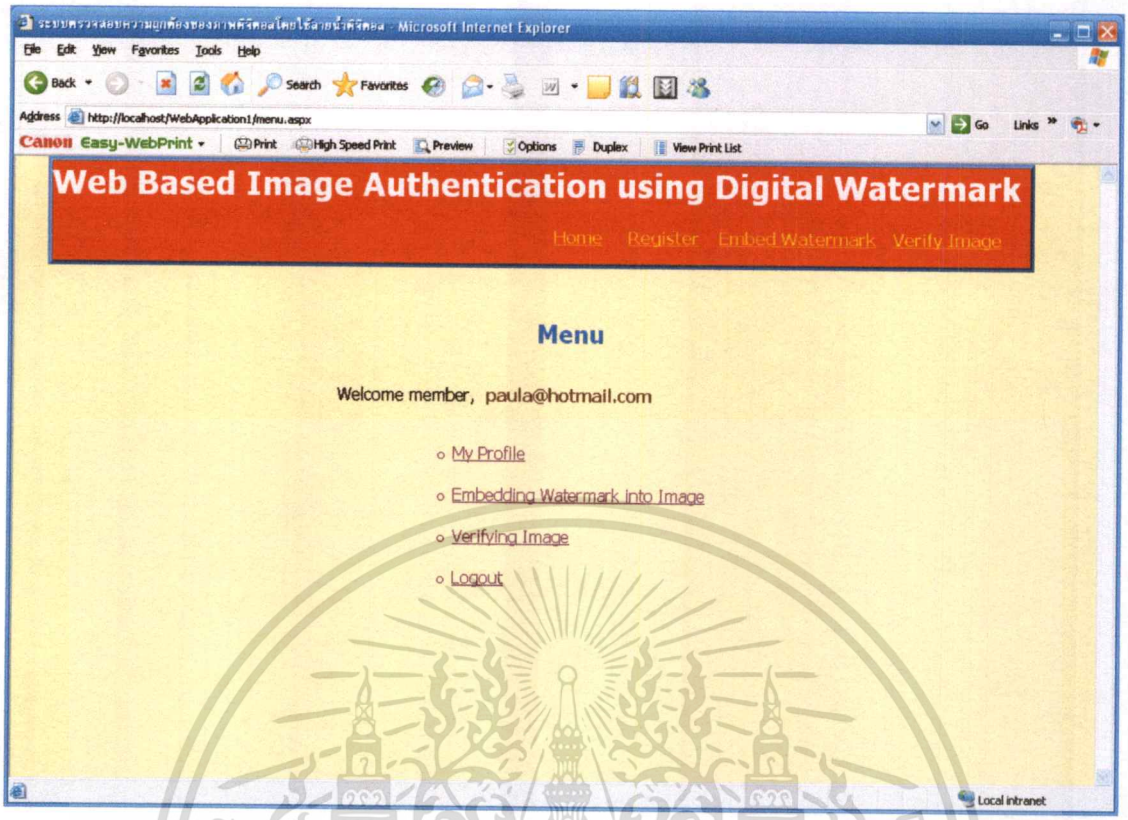


รูปที่ 5.8 หน้าจอเข้าสู่ระบบ

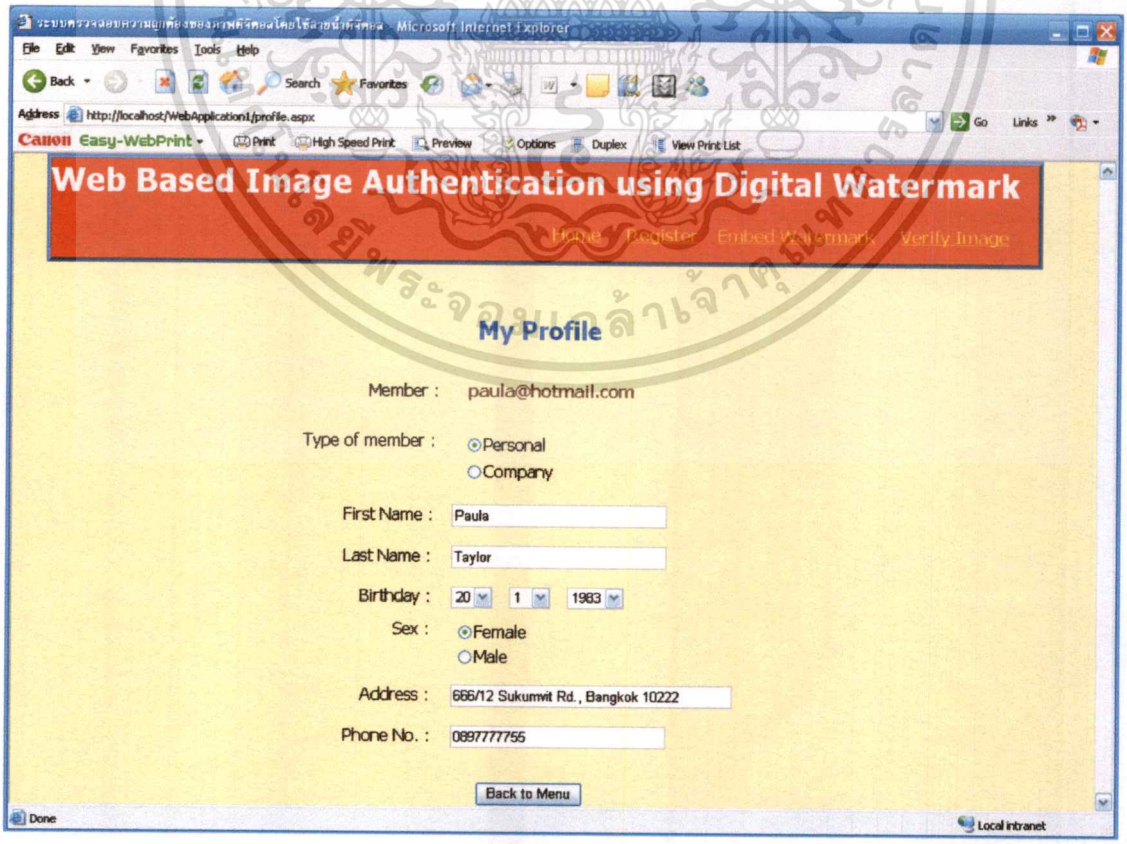
ซึ่งจะพบหน้าเมนูหลักของระบบที่ให้บริการสมาชิก ดังรูปที่ 5.9 มีดังนี้

- My Profile
- Embedding Watermark into Image
- Verifying Image
- Logout

ในการแสดงรายละเอียดข้อมูลส่วนตัวของสมาชิก ดังรูปที่ 5.10

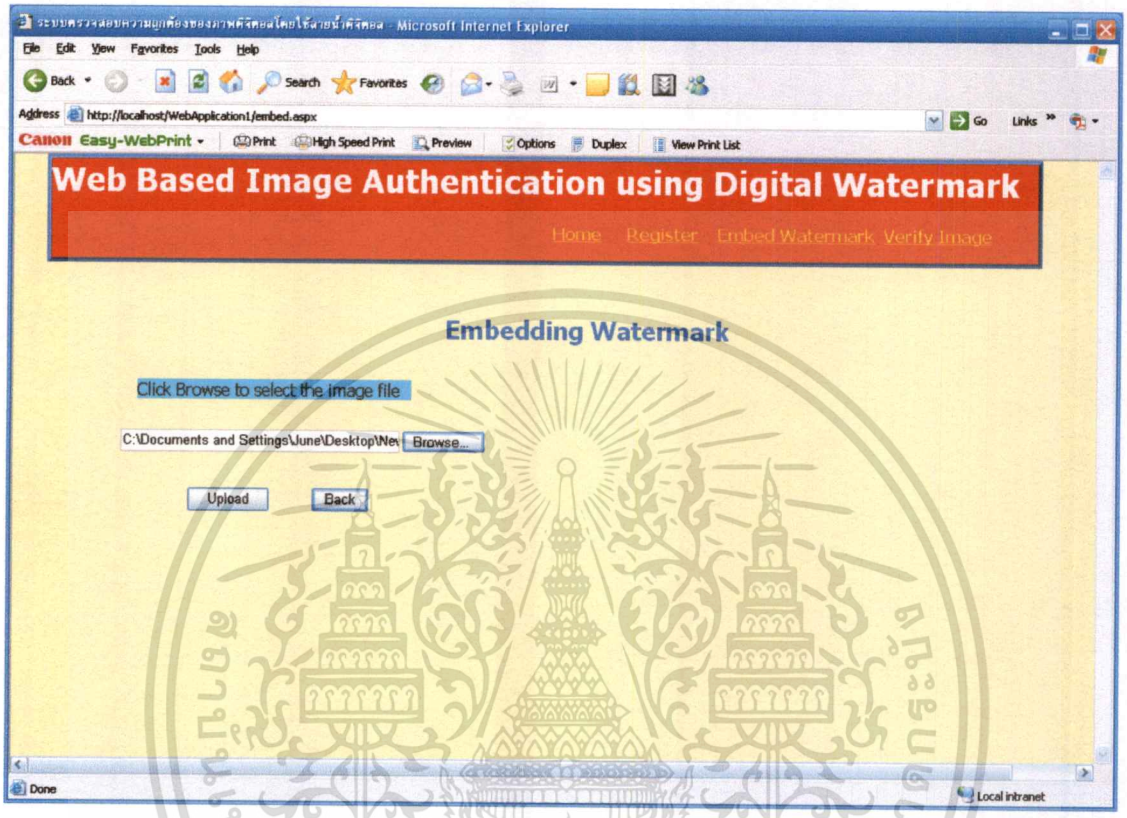


รูปที่ 5.9 หน้าจอเมนูหลักที่ให้บริการแก่สมาชิก

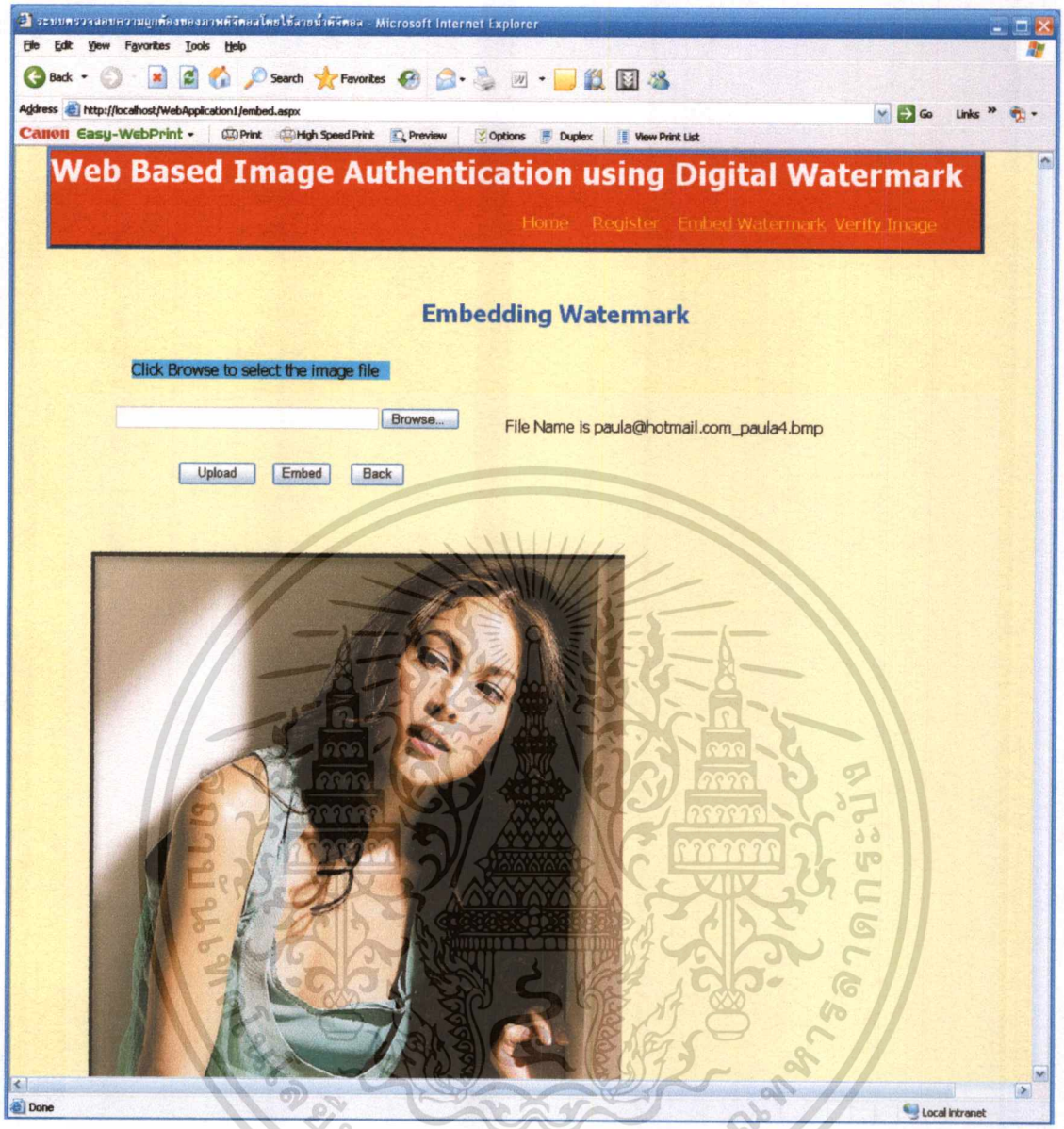


รูปที่ 5.10 หน้าจอข้อมูลส่วนตัวของสมาชิก

เมื่อคลิกฝังลายน้ำดิจิตอลลงภาพดิจิตอล สมาชิกที่เป็นเจ้าของภาพต้องเลือกรูปภาพดิจิตอลที่ต้องการอัปโหลด ดังรูปที่ 5.11 และคลิกปุ่ม Upload เพื่ออัปโหลดรูปภาพดิจิตอลเข้าสู่ระบบ ดังรูปที่ 5.12

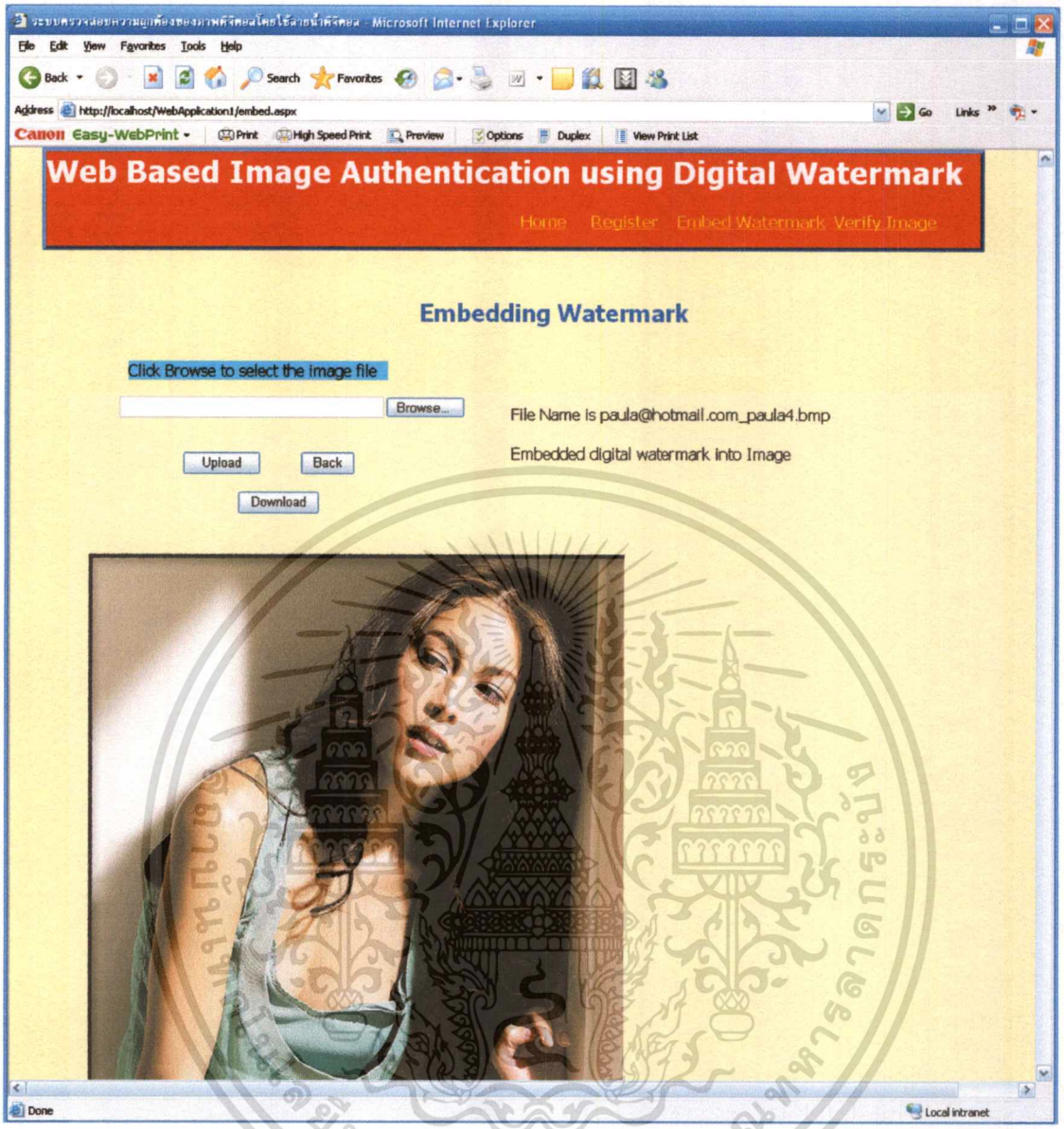


รูปที่ 5.11 หน้าจอการฝังลายน้ำดิจิตอลลงภาพดิจิตอล



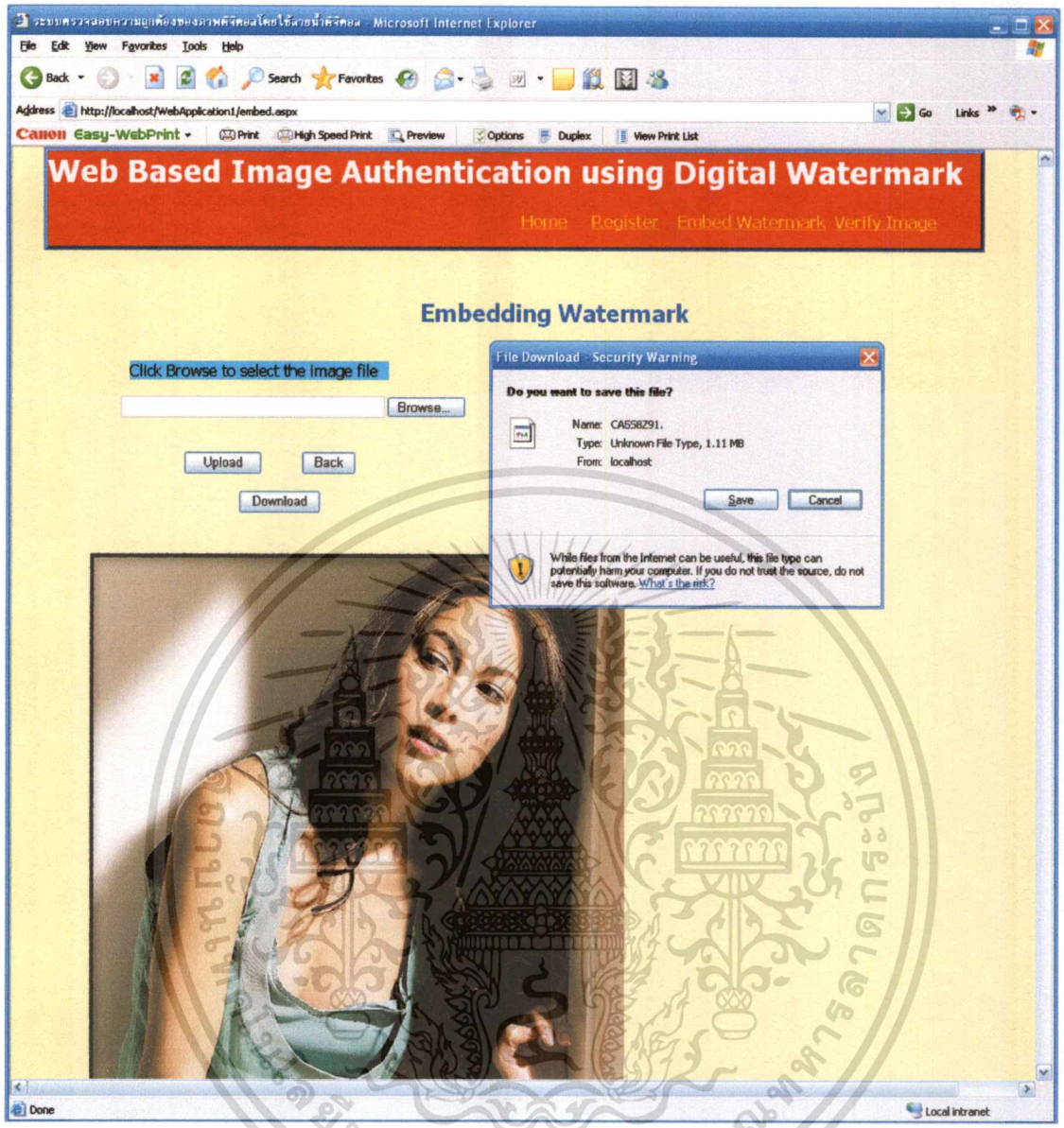
รูปที่ 5.12 หน้าจอการอัปโหลดรูปภาพเพื่อฝังลายน้ำดิจิตอล

จากนั้นแล้วกดปุ่ม Embed ระบบจะทำการสร้างลายน้ำดิจิตอลแล้วนำมาฝังลงในภาพดิจิตอล ดังรูปที่ 5.13



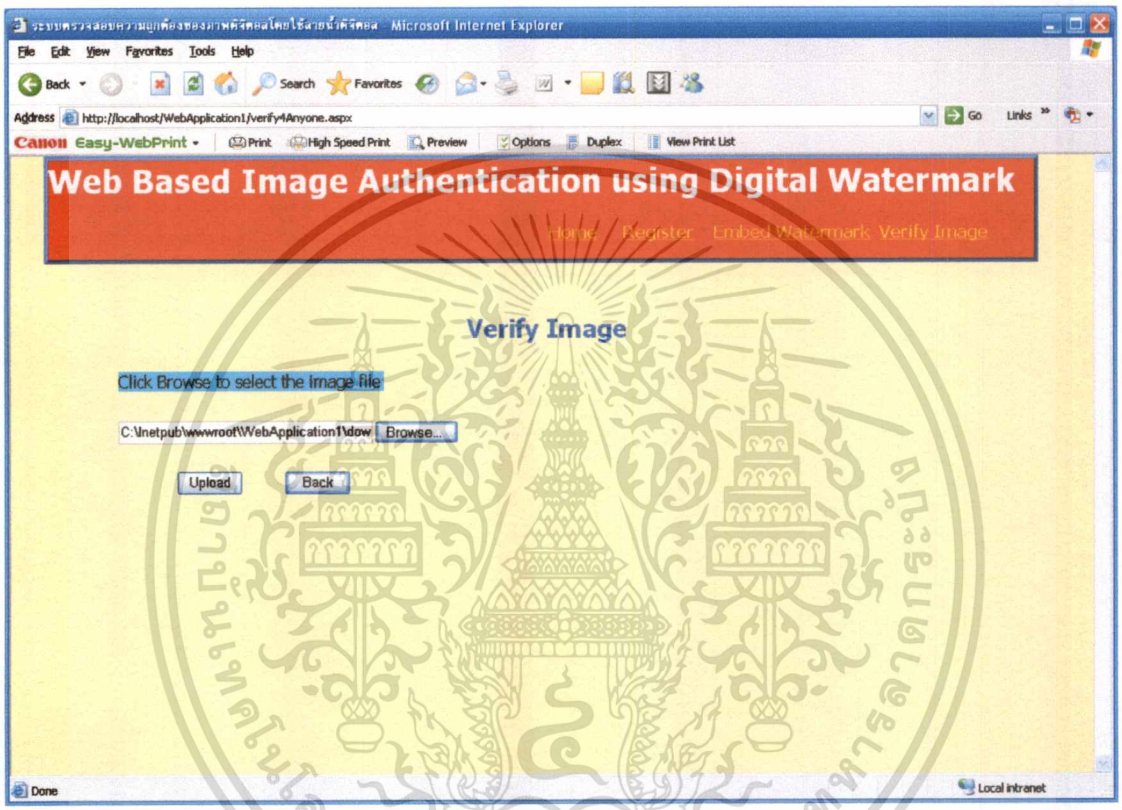
รูปที่ 5.13 หน้าจอแสดงผลการฝังลายน้ำดิจิตอลลงในภาพดิจิตอล

จากนั้นเมื่อคลิกปุ่ม Download เพื่อให้เจ้าของภาพดิจิตอลสามารถดาวน์โหลดไฟล์รูปภาพที่ทำการฝังลายน้ำดิจิตอลลงในภาพดิจิตอลกลับไปได้ ดังรูปที่ 5.14 และเมื่อคลิกปุ่ม Back จะกลับไปหน้าจอหลักของระบบ



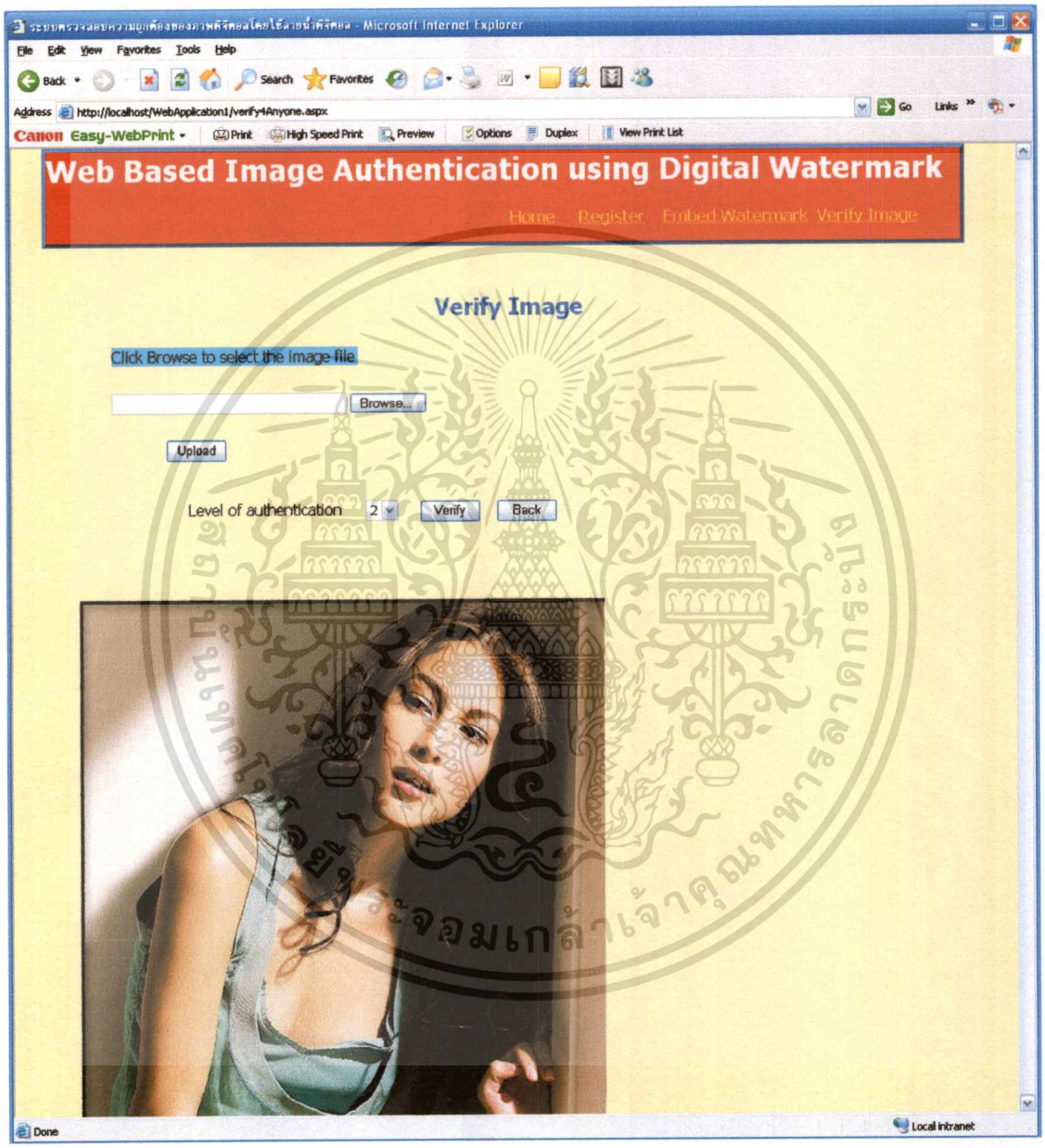
รูปที่ 5.14 หน้าจอแสดงให้ดาวน์โหลดไฟล์รูปภาพดิจิตอลที่ได้ทำการฝังลายน้ำดิจิตอล

ในส่วนของการตรวจสอบความถูกต้องของภาพดิจิตอล ทั้งเจ้าของภาพดิจิตอลและบุคคลทั่วไป สามารถที่จะนำรูปภาพดิจิตอลมาตรวจสอบได้ โดยเจ้าของภาพสามารถคลิก Verifying Image จากหน้าจอหลัก ส่วนบุคคลทั่วไปที่ไม่ได้สมัครเป็นสมาชิกก็สามารถตรวจสอบได้เช่นเดียวกัน โดยคลิกที่ลิงค์ในหน้าแรกของเว็บ ซึ่งจะเข้าสู่ในหน้าตรวจสอบความถูกต้องของภาพ ซึ่งทั้งเจ้าของภาพและลูกค้าทั่วไปต้องเลือกไฟล์รูปที่ต้องการตรวจสอบความถูกต้องก่อน ดังรูป 5.15



รูปที่ 5.15 หน้าจอการตรวจสอบความถูกต้องของภาพดิจิตอล

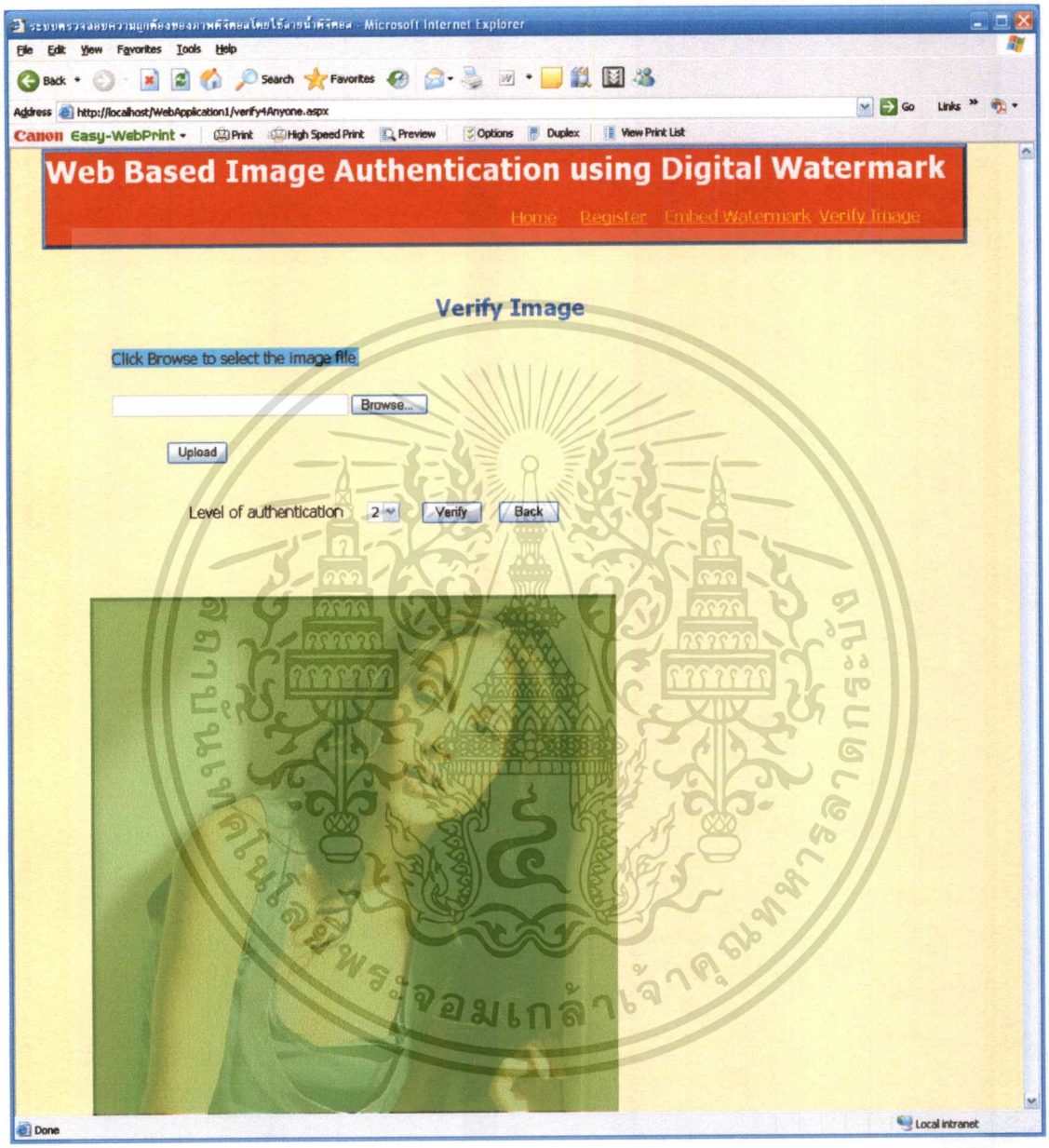
จากนั้นคลิกปุ่ม Upload เพื่ออัปโหลดรูปภาพดิจิตอลที่ต้องการตรวจสอบความถูกต้องของภาพดิจิตอล ดังรูปที่ 5.16



รูปที่ 5.16 หน้าจอการอัปโหลดรูปภาพเพื่อตรวจสอบความถูกต้องของภาพดิจิตอล

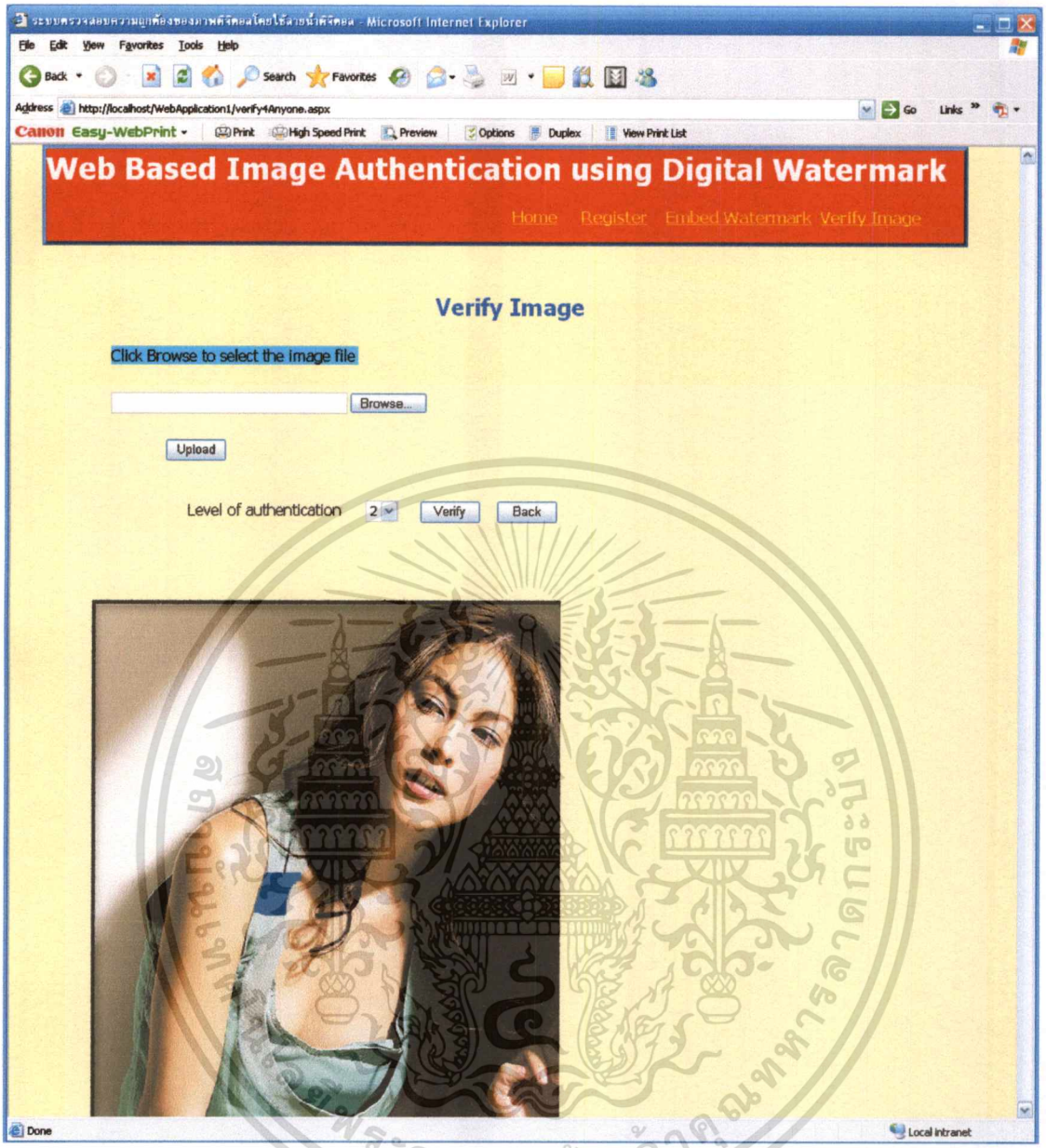
และทำการเลือกระดับที่ต้องการตรวจสอบ ซึ่งมีอยู่ด้วยกัน 3 ระดับ เมื่อเลือกระดับได้แล้ว ให้คลิกปุ่ม Verify ซึ่งผลของการตรวจสอบสามารถจำแนกออกเป็นสองสีในการแสดงผล คือ สีเขียวสีแดง และไม่แสดงสี

- ถ้าผลออกเป็นสีเขียว แสดงว่าบล็อกของรูปภาพดังกล่าว “ถูกต้อง” ไม่มีการแก้ไขหรือเปลี่ยนแปลงข้อมูลภายในภาพดิจิตอลแต่อย่างใด ดังรูปที่ 5.17



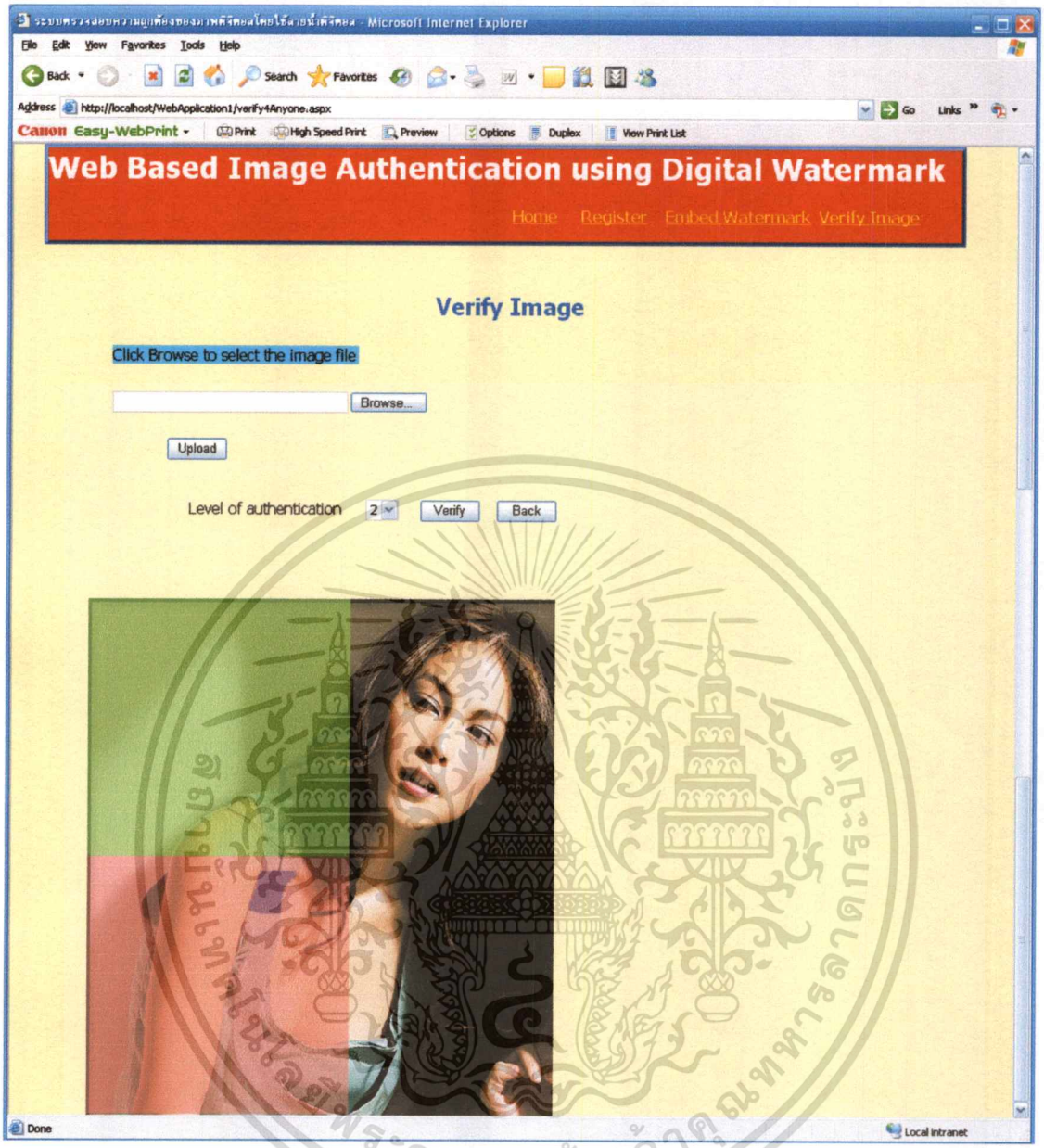
รูปที่ 5.17 หน้าจอแสดงผลการตรวจสอบความถูกต้องของภาพดิจิตอลในกรณีที่ถูกต้อง

จากนั้นลองทดสอบโดยให้อัปโหลดภาพดิจิตอลที่มีการแก้ไขเกิดขึ้น ทั้งมีการตัดภาพดิจิตอลและการแก้ไขเปลี่ยนแปลงภายในภาพดิจิตอล ดังรูปที่ 5.18



รูปที่ 5.18 หน้าจอการอัปโหลดรูปภาพที่มีการแก้ไขเพื่อตรวจสอบความถูกต้องของภาพดิจิตอล

- ถ้าผลออกเป็นสีแดง แสดงว่าบล็อกของรูปภาพดังกล่าว “ไม่ถูกต้อง” มีการแก้ไขหรือเปลี่ยนแปลงข้อมูลภายในภาพดิจิตอลเกิดขึ้น ดังรูปที่ 5.19
- ถ้าผลออกเป็นไม่แสดงสี แสดงว่าบล็อกของรูปภาพดังกล่าว “มีการตัดภาพดิจิตอล” เกิดขึ้น จึงทำให้ระบบไม่สามารถตรวจสอบความถูกต้องของภาพดิจิตอลได้ เนื่องจากมีข้อมูลไม่ครบที่จะตรวจสอบได้



รูปที่ 5.19 หน้าจอแสดงผลการตรวจสอบความถูกต้องของภาพดิจิตอลในกรณีที่ไม่ถูกต้อง

บทที่ 6
สรุปผลและข้อเสนอแนะ

เนื่องจากคุณสมบัติของภาพดิจิตอลที่ยอมให้มีการแก้ไขเปลี่ยนแปลงข้อมูลพิกเซลได้ในระดับหนึ่ง โดยที่ไม่ได้ทำให้คุณภาพหรือความหมายของภาพเปลี่ยนไป อีกทั้งรูปภาพดิจิตอลมีปริมาณข้อมูลมาก จึงไม่สะดวกที่จะนำภาพต้นฉบับมาใช้ในการเปรียบเทียบ จึงทำให้เกิดปัญหาของการตรวจสอบความถูกต้องของภาพดิจิตอล จากการวิเคราะห์และออกแบบระบบที่ให้บริการการตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บ มีขั้นตอนการพัฒนาระบบหลายขั้นตอน เริ่มจากการกำหนดวัตถุประสงค์ของการพัฒนาระบบ ศึกษาทฤษฎีและหลักการที่ใช้ในระบบ โดยเริ่มต้นศึกษาลักษณะไฟล์รูปภาพดิจิตอล ลายน้ำดิจิตอล ลายเซ็นดิจิตอล การสร้างลายน้ำดิจิตอลแบบแบ่งลำดับชั้น การหาวิธีที่เหมาะสมในการตรวจสอบการตัดภาพดิจิตอล การวิเคราะห์และออกแบบระบบ และการนำระบบไปใช้งาน

6.1 สรุปผล

ในการพัฒนาระบบงานนี้ โดยใช้เครื่องมือในการพัฒนา คือ Microsoft Visual Studio .NET 2003 ให้แสดงผลออกหน้าเว็บด้วย ASP.NET เชื่อมต่อกับ SQL Server 2000 เพื่อที่จะสร้างระบบที่สามารถฝังลายน้ำดิจิตอลลงในภาพดิจิตอล และสามารถตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์ได้ โดยนำจุดเด่นของวิธีการสร้างลายเซ็นดิจิตอลมาประยุกต์ใช้กับเทคนิคการฝังลายน้ำดิจิตอลเปราะบาง ร่วมกับการสร้างลายน้ำดิจิตอลแบบแบ่งลำดับชั้น ซึ่งการพัฒนาโครงงานนี้ จะสามารถระบุถึงการแก้ไขเฉพาะที่ของภาพดิจิตอลได้ โดยจะช่วยลดปัญหาในการตกแต่งภาพดิจิตอลที่ผิดแปลกไปจากต้นฉบับของบุคคลที่มีชื่อเสียง เช่น ดารา นางแบบหรือบุคคลที่มีชื่อเสียงที่ต้องตกเป็นข่าวเนื่องจากผู้ไม่ประสงค์ดีนำภาพดิจิตอลไปตกแต่ง ซึ่งเจ้าของภาพจะต้องสมัครสมาชิกกับระบบและระบบจะให้บริการการฝังลายน้ำดิจิตอลลงในภาพดิจิตอล รวมทั้งการตรวจสอบความถูกต้องของภาพดิจิตอล ส่วนบุคคลทั่วไป ก็สามารถตรวจสอบความถูกต้องของภาพดิจิตอลผ่านทางเว็บไซต์ได้ โดยที่ไม่ต้องสมัครสมาชิก

6.2 ข้อเสนอแนะ

สำหรับโครงงานพัฒนาระบบงานนี้ ยังมีส่วนที่น่าจะพัฒนาเพิ่มเติมให้มีประสิทธิภาพมากขึ้นต่อไปอีก

1. เนื่องจากระบบถูกพัฒนาขึ้นในลักษณะของไคลเอนท์เซิร์ฟเวอร์ ดังนั้นการประมวลผลจึงอยู่ที่เซิร์ฟเวอร์เป็นตัวหลัก โดยที่เซิร์ฟเวอร์จะมีฐานข้อมูลไว้คอยจัดเก็บข้อมูลต่างๆ ซึ่งใน

ฐานข้อมูลมีการเก็บข้อมูลกุญแจลับและกุญแจสาธารณะของเจ้าของภาพแต่ละคนไว้ ซึ่งถ้ามีคนประสงค์ร้ายเอากุญแจลับไปทำอะไรกับภาพ ก็จะสามารถทำได้ง่าย และรวมถึงถ้าเซิร์ฟเวอร์ล่มหรือเป็นอะไรไป ทุกคนก็จะใช้ระบบไม่ได้ ดังนั้นควรจะต้องเก็บกุญแจลับไว้ที่เจ้าของภาพเพื่อให้เจ้าของภาพรู้ได้เพียงคนเดียว

2. ระบบควรจะรองรับสกุลของไฟล์รูปภาพได้มากกว่านี้
3. ระบบควรจะรองรับระดับการตรวจสอบภาพดิจิตอลได้มากนี้
4. เนื่องจากระบบมีการใช้ Sync bit เพื่อใช้สำหรับการหาความสอดคล้องของระหว่างบล็อก ซึ่ง Sync bit เป็นบิตที่ถูกกำหนดค่าเป็น 1 จำนวน 16 ตัว นั่นหมายถึงสีขาว ดังนั้นเมื่อภาพดิจิตอลมีการแก้ไขเปลี่ยนแปลงเกิดขึ้น โดยทำการลบหรือระบายสีด้วยสีขาวเมื่อใด จะส่งผลให้ในการตรวจสอบความถูกต้องของระบบผิดพลาด ดังนั้นระบบควรจะเปลี่ยน Sync bit ให้ Unique

บรรณานุกรม

Federal Information Processing Standards Publication 180-1. 1997. **Secure Hash Standard.** [Online]. Available : http://www.itl.nist.gov/fipspubs/fip180-2.htm.

Federal Information Processing Standards Publication 186. 1994. **Digital Signature Standard.** [Online]. Available : http://www.itl.nist.gov/fipspubs/fip180-2.htm.

Ingemar J. Cox, Matthew L. Miller and Jeffrey A. Bloom. 2001. **Digital Watermarking,** 1st ED. San Francisco: Morgan Kaufmann Publishers.

M. U. Celik, G. Sharma, E. Saber and A.M. Tekalp. 2002. **Hierarchical Watermarking for Secure Image Authentication with Localization.** IEEE Transactions on Image Processing. vol.11. no.6. pp. 585-595.

M. Wu and B. Liu. 1998. **Watermarking for Image Authentication.** IEEE Transaction on Image Processing. vol.2. pp.437-441

Rafael C. Gonzalez and Richard E. Woods. 2001. **Digital Image Processing.** 2nd ED. New Jersey: Prentice-Hall

Stefan Katzenbeisser and Fabien A.P. Peticolas. 2000. **Information Hiding Techniques for Steganography and Digital Watermarking.** Boston: Artech House.

Stefan Hetzl. 1998. **The .bmp file format.** [Online]. Available: http://www.fortunecity.com/skyscrapper/windows/364/bmpffrmt.html.

Virtual Science Fair. 2004. **Specifics of the .BMP File Format.** [Online]. Available: http://www.virtualsciencefair.org/2004/chia4a0/public_html/bmpresearch.htm.

ประวัติผู้เขียน

นางสาวนัดดา ปรัชญานิมิต เกิดเมื่อวันที่ 1 มิถุนายน พ.ศ. 2525 ที่จังหวัดกรุงเทพมหานคร สำเร็จการศึกษาปริญญาตรีวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยอัสสัมชัญ พ.ศ. 2546 และเข้าศึกษาต่อในระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ในปีการศึกษา 2547 ภาคการศึกษาที่ 2