การตรวจสอบความถูกต้องของรูปภาพ โดยใช้เทคนิคลายน้ำดิจิตอล

IMAGE AUTHENTICATION BASED ON DIGITAL WATERMARKING TECHNIQUE

วสิน เสงี่ยมกุล
WASIN SANGIAMKUN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชานิเทศโทรคมนาคม
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2546

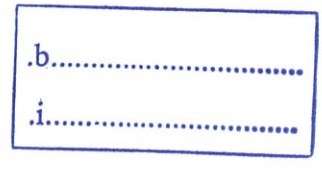
ISBN 974-324-461-1

การตรวจสอบความถูกต้องของรูปภาพ โดยใช้เทคนิคลายน้ำดิจิตอล

IMAGE AUTHENTICATION BASED ON DIGITAL WATERMARKING TECHNIQUE

วศิน เสงี่ยมกุล

WASIN SANGIAMKUN



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2546

ISBN 974-324-461-1

IMAGE AUTHENTICATION BASED ON DIGITAL WATERMARKING TECHNIQUE

WASIN SANGIAMKUN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF SCIENCE PROGRAM IN INFORMATION TECHNOLOGY

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2003

ISBN 974-324-461-1

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การตรวจสอบความถูกต้องของรูปภาพโดยใช้เทคนิคลายน้ำดิจิตอล
IMAGE AUTHENTICATION BASED ON DIGITAL WATERMARKING TECHNIQUES

ชื่อนักศึกษา นายวศิน เสงี่ยมกุล

รหัสประจำตัว 39067032

ปริญญา วิทยาศาสตรมหาบัณฑิต

สาขาวิชา เทคโนโลยีสารสนเทศ

อาจารย์ผู้ควบคุมวิทยานิพนธ์ ผศ.ดร.นพพร โชติกกำธร

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.นพพร	โชติกกำธร	
รศ.ดร.บุญธีร์	เครือตราชู	
รศ.ดร.วิเชียร	เปรมชัยสวัสดิ์	
ผศ.ดร.วรพจน์	กรีสุระเดช	
ดร.ธนารัตน์	ชลิดาพงศ์	

วัน/เดือนปี ที่สอบ 29 เมษายน 2546 เวลา 10.00 น. เป็นต้นไป

สถานที่สอบ ณ ห้อง M21 (ชั้นลอย) อาคารเรียนรวมและปฏิบัติการคณะเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.บุญวัฒน์ อัตชู)

คณบดีบัณฑิตวิทยาลัย

วันที่ 28 **เดือน** พฤษภาคม **พ.ศ.** 2546

หัวข้อวิทยานิพนธ์	การตรวจสอบความถูกต้องของรูปภาพโดยใช้เทคนิคลายน้ำดิจิตอล
นักศึกษา	นายวศิน เสงี่ยมกุล
รหัสประจำตัว	39067032
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2546
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ. ดร. นพพร โชติกกำธร

บทคัดย่อ

ข้อมูลต่างๆในระบบคอมพิวเตอร์ถูกสื่อในรูปแบบดิจิตอล เช่นภาพ เสียง ข้อความ ทำให้เอื้ออำนวยต่อการทำสำเนา ซึ่งนำไปสู่ผลลัพธ์อันไม่พึงประสงค์เช่น การละเมิดลิขสิทธิ์ หรือแก้ไขข้อมูล โดยเฉพาะการบิดเบือนความหมายของรูปภาพบนเครือข่ายอินเตอร์เน็ต งานวิจัยชิ้นนี้ได้เสนอวิธีการใหม่สำหรับตรวจสอบความถูกต้องของรูปภาพ ซึ่งนำแนวคิดพื้นฐานของลายเซ็นดิจิตอล (Digital Signature) และลายน้ำดิจิตอล (Digital Watermark) มาพัฒนาเพื่อใช้ตรวจสอบความถูกต้องของรูปภาพ ที่สามารถระบุพื้นที่บริเวณที่รูปภาพมีการเปลี่ยนแปลงได้ โดยทำการแบ่งรูปภาพออกเป็นบล็อกย่อยๆ แล้วหาลักษณะสำคัญของบล็อกเช่นค่าเฉลี่ยความสว่างมาสร้างเป็นลายเซ็นดิจิตอลโดยใช้ค่าเปรียบเทียบสัมพัทธ์ระหว่างบล็อกข้างเคียง และทำการฝังลายเซ็นลงในภาพต้นฉบับโดยใช้เทคนิคลายน้ำดิจิตอลแบบสเปรดสเปคตรัม ทำให้ลายน้ำที่ได้มีลักษณะทนทานต่อกระบวนการเปลี่ยนแปลงรูปภาพทั่วไปเช่น การเปลี่ยนแปลงค่าความสว่าง การลดขนาดรูปภาพแบบ JPEG การเพิ่มสัญญาณรบกวน ฯลฯ และยังสามารถตรวจสอบการเปลี่ยนแปลงโดยระบุพื้นที่ที่ถูกแก้ไขในรูปภาพได้ นอกจากนี้ยังได้ทำการปรับปรุงวิธีการตรวจสอบรูปภาพดิจิตอลแบบเฉพาะส่วน โดยจะเลือกพื้นที่เฉพาะส่วนที่สำคัญของรูปภาพมาสร้างลายเซ็นดิจิตอล ทำให้สามารถเข้ารหัสลายเซ็นดิจิตอลด้วยกุญแจที่มีขนาดใหญ่กว่าวิธีการเดิม และการทดลองกับรูปภาพที่มีลักษณะความละเอียดและความสว่างแตกต่างกัน แสดงให้เห็นว่าวิธีการนี้สามารถตรวจสอบความถูกต้องของรูปภาพที่ผ่านการแก้ไขเหล่านั้นได้เป็นอย่างดี

Thesis Title	Image Authentication Based on Digital Watermarking Technique
Student	Mr. Wasin Sangaimkun
Student ID.	39067032
Degree	Master of Science
Programme	Information Technology
Year	2003
Thesis Advisor	Asst. Prof. Dr. Nopporn Chotikakamthorn

ABSTRACT

In computer systems, information such as as image, audio and text is represented in digital form making it possible for economical duplication. As a result copyright-violated or modification of content to distort information is greatly simplified. This thesis presents a new method to check an authenticity of digital image, based on the concepts of digital signature and image watermarking. A digital signature, created from some image features such as its mean, standard deviation and correlation, is embedded into an original image by digital watermarking technique based on spread-spectrum principle. The applied watermarking technique is robust against common image modifications such as brightness adjustment, JPEG compression or additive noise. This thesis proposes a technique to verify each part of modified image based on neighboring block relative similarity measure. The method can identify individual blocks that have been altered. In addition, the problem of a short signature key size due to limited embedding bandwidth has been addressed. The use of partial image authentication have been proposed to alleviate the problem. Experimental results show that this method can authenticate most of the sample images correctly.

กิตติกรรมประกาศ

วิทยานิพนธ์ของข้าพเจ้าสำเร็จลุล่วงด้วยดีเช่นนี้ ส่วนหนึ่งก็เพราะได้รับความความช่วยเหลือไม่ทางตรงก็ทางอ้อมจากบุคคลเหล่านี้ ซึ่งข้าพเจ้าขอแสดงความขอบคุณ มา ณ โอกาสนี้

ขอขอบพระคุณบิดา-มารดาของข้าพเจ้า ที่เป็นแรงผลักดัน ให้ทั้งกำลังใจและกำลังทรัพย์แก่ข้าพเจ้าในการทำงานวิจัยนี้

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. นพพร โชติกกำธร อาจารย์ที่ปรึกษา ผู้ซึ่งให้คำแนะนำและแนวคิดต่างๆในงานวิจัยให้แก่ข้าพเจ้าอย่างอดทน อีกทั้งยังให้การสนับสนุนอุปกรณ์และเอกสารที่เกี่ยวข้องกับงานวิจัยได้อย่างดีเยี่ยม

ขอขอบคุณ คุณวรางคณา เงินแก้ว เพื่อนนักศึกษาวิทยานิพนธ์ ผู้คอยให้กำลังใจ ช่วยทำธุระต่างๆ และเผชิญอุปสรรคต่างๆ มาด้วยกัน ทำให้งานวิจัยนี้สำเร็จลุล่วงได้ด้วยดี

งานวิจัยชิ้นนี้ส่วนหนึ่งกระทำภายใต้ห้องปฏิบัติการวิจัยสื่อประสมและระบบเสมือน สำนักวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ (ReCCIT) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ท้ายสุดนี้ ขอขอบคุณ เพื่อนๆ พี่ๆ ทุกคนที่ไม่ได้กล่าวถึงในที่นี้ ที่ให้ความห่วงใย คำแนะนำ และให้ความสะดวกในการทำวิจัย

วศิน เสงี่ยมกุล

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ข้อมูลต่างๆ ในโลกของคอมพิวเตอร์ถูกนำมาใช้งานกันอย่างแพร่หลายในรูปแบบดิจิตอล ไม่ว่าจะเป็น ข้อความ ภาพ เสียง วิดิโอ เป็นต้น โดยข้อมูลดังกล่าวนี้ถูกนำมาใช้งานโดยส่งผ่านทางระบบเครือข่ายอินเตอร์เน็ต ซึ่งได้ขยายตัวแพร่หลายไปทั่วทุกมุมโลก โดยเฉพาะการทำธุรกิจบนอินเตอร์เน็ต ข้อมูลที่ใช้ในคอมพิวเตอร์นั้นเอื้ออำนวยต่อการทำสำเนา ซึ่งนำไปสู่การละเมิดลิขสิทธิ์หรือการปลอมแปลงบิดเบือนข้อมูลที่ส่งถึงกันได้อย่างง่ายดาย โดยเฉพาะรูปภาพบนเครือข่ายอินเตอร์เน็ตนั้น ได้มีการเผยแพร่ภาพตัดต่อของดาราบุคคลที่มีชื่อเสียง หรือการทำสำเนารูปภาพและเผยแพร่โดยไม่ได้รับอนุญาตจากเจ้าของภาพ ทั้งในแง่ที่เป็นการแอบอ้างความเป็นเจ้าของ หรือแก้ไขเปลี่ยนแปลงการสื่อความหมายของรูปภาพนั้น หากว่าความเปลี่ยนแปลงนั้นชัดเจน จนผู้รับสังเกตพิรุธได้ว่าเป็นภาพปลอม คงไม่มีปัญหาในการพิสูจน์ แต่หากเป็นการแก้ไขที่แนบเนียนและน่าเชื่อถือเราจะทราบได้อย่างไรว่ารูปภาพนั้นถูกปลอมแปลงขึ้นมาหรือไม่

วิธีการที่ถูกนำมาใช้ในการปกป้องรูปภาพ คือการซ่อนข้อมูลบางอย่างเข้าไปในภาพเพื่อใช้ในการแก้ปัญหา เช่นซ่อนสัญลักษณ์หรือโลโก้ของเจ้าของภาพ รวมเข้าไปในตัวข้อมูลรูปภาพ ที่รู้จักกันในวิธีการที่เรียกว่าการซ่อนลายน้ำ (Watermarking) แต่วิธีการที่นิยมใช้อยู่ในปัจจุบันถูกออกแบบมาเพื่อใช้ในการป้องกันการละเมิดลิขสิทธิ์เจ้าของภาพเท่านั้น ยังไม่สามารถตรวจสอบการแก้ไขเปลี่ยนแปลงของรูปภาพได้ หรือวิธีการที่ทำได้ยังคงมีจุดอ่อนเช่น จำเป็นต้องใช้ภาพต้นฉบับในการเปรียบเทียบ และไม่ทนทานต่อการเปลี่ยนแปลงแก้ไขรูปภาพในสถานะภาพของการใช้งานจริง

งานวิจัยชิ้นนี้ได้เสนอวิธีการใหม่สำหรับตรวจสอบและพิสูจน์ความถูกต้องของรูปภาพ โดยมีแนวคิดพื้นฐานจากการใช้ลายเซ็นดิจิตอล (Digital signature) และการซ่อนลายน้ำสำหรับรูปภาพแบบดิจิตอล (Digital image watermarking) โดยได้ออกแบบการสร้างลายเซ็นดิจิตอลโดยสร้างจากลักษณะสำคัญบางอย่างของรูปภาพเช่น ส่วนเบี่ยงเบนมาตรฐาน (Standard deviation) ค่าเฉลี่ยความสว่าง (Brightness mean) และค่าคอรีเลชัน (Correlation) เป็นต้น ลักษณะสำคัญดังกล่าวมีคุณสมบัติทนทานต่อกระบวนการเปลี่ยนแปลงพื้นฐานที่มีผลต่อรูปภาพ เช่น การบีบอัดข้อมูลแบบสูญเสีย (Lossy compression) การเพิ่มและลดมาตราส่วน (Scaling) การเพิ่มสัญญานรบกวน (Noise) เป็นต้น และปรับปรุงให้สามารถตรวจเช็คการเปลี่ยนแปลงของพื้นที่แต่ละส่วนในรูปภาพได้ โดยใช้เทคนิคการเปรียบเทียบค่าความคล้ายคลึงกันกับบล็อกข้างเคียงในภาพ และผู้วิจัยได้ประยุกต์ใช้เทคนิคสเปรดสเปคตรัมในการนำลายเซ็นนี้มาซ่อนกลับเข้าไปในรูปภาพต้นฉบับ เพื่อให้ลายเซ็น

ยากต่อการตรวจพบและทำลายโดยผู้ที่ต้องการละเมิดสิทธิ์ ซึ่งส่งผลให้การตรวจสอบสิทธิ์ความเป็นเจ้าของรูปภาพเป็นไปได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

1.2 วัตถุประสงค์ของการวิจัย

1. ศึกษาวิธีการใช้ลายเซ็นดิจิตอลและลายน้ำดิจิตอล เพื่อประยุกต์เข้ากับการตรวจสอบความถูกต้องของรูปภาพดิจิตอล

2. หาวิธีการตรวจสอบรูปภาพที่เหมาะสมกับภาพถ่ายคน สัตว์ สิ่งของ เพื่อตรวจการแก้ไขเปลี่ยนแปลงในรูปภาพ เพื่อรับรองความถูกต้องของรูปภาพ

3. ศึกษาคุณสมบัติและข้อดีข้อเสียของวิธีการตรวจสอบรูปภาพที่พัฒนาขึ้น เมื่อใช้กับรูปภาพที่ผ่านการประมวลผลในลักษณะต่างๆได้แก่ การปลอมแปลงแก้ไข การพิมพ์และสแกน การปรับระดับความเข้มความสว่าง การแปลงฟอร์แมตไฟล์ การปรับความแตกต่างความสว่าง

1.3 สมมุติฐานของการวิจัย

ผู้วิจัยได้นำวิธีการใช้ลายเซ็นดิจิตอลมาประยุกต์ใช้ในการตรวจสอบความถูกต้องของรูปภาพ เนื่องจากเป็นวิธีการที่มีความน่าเชื่อถือและความปลอดภัยสูง ไม่จำเป็นต้องใช้รูปภาพต้นฉบับในการเปรียบเทียบ แต่ข้อมูลรูปภาพมีลักษณะบางประการที่แตกต่างจากข้อมูลตัวอักษร เช่นมีปริมาณข้อมูลมาก มีโอกาสที่จะถูกเปลี่ยนแปลงแก้ไขเมื่อนำไปใช้งานได้ รวมทั้งมีเกณฑ์การตรวจสอบที่คลุมเครือ เนื่องจากถึงแม้รูปภาพจะมีการเปลี่ยนแปลงที่ทำให้ข้อมูลของแต่ละจุด (Pixel) แตกต่างไปจากภาพต้นฉบับแต่สำหรับผู้รับหรือผู้สังเกตแล้วรูปภาพนั้นอาจยังคงสื่อความหมายเดิม หรือไม่อาจจะแยกความแตกต่างนั้นได้ หากว่าเราสามารถเลือกลักษณะเฉพาะของรูปภาพ ที่ไม่ถูกกระทบจากการแก้ไขที่พบได้ทั่วไปซึ่งไม่ทำลายความหมายของภาพไปจากเดิม นำมาสร้างเป็นลายเซ็นดิจิตอล ก็จะทำให้การตรวจสอบมีความถูกต้องสมเหตุสมผลมากยิ่งขึ้น

การใช้ลายเซ็นดิจิตอลสำหรับข้อมูลรูปภาพมีความแตกต่างจากข้อมูลแบบตัวอักษรอีกประการหนึ่งคือ ประเภทฟอร์แมตไฟล์รูปภาพมีความหลากหลาย เช่นไฟล์ประเภท JPEG, BMP, GIF, TIF เป็นต้น และการที่รูปภาพสามารถถูกแก้ไขเปลี่ยนได้ง่าย ทำให้ลายเซ็นดิจิตอลของรูปภาพนั้นๆ มีโอกาสสูญหายได้ จึงจำเป็นต้องซ่อนลายเซ็นดิจิตอลเข้าไปในข้อมูลรูปภาพ โดยวิธีการซ่อนลายน้ำที่ใช้เทคนิคแบบสเปรดสเปคตรัม ซึ่งจะไม่ทำให้ข้อมูลรูปภาพเปลี่ยนแปลงหรือลดคุณภาพลงไปมากนัก อีกทั้งยังมีความทนทานต่อกระบวนการแก้ไขรูปภาพที่พบโดยทั่วไปได้ดี นอกจากนี้วิธีการนี้ยังสามารถที่จะระบุตำแหน่งหรือบริเวณที่รูปภาพถูกแก้ไขได้อีกด้วย

1.4 ทฤษฎีและหลักการที่ใช้ในการวิจัย

1.4.1 รูปภาพดิจิตอล

รูปภาพดิจิตอลที่ใช้อ้างถึงในงานวิจัยนี้มีความหมายในแง่ของฟังก์ชันค่าความสว่างในพิกัดสองมิติ $g(x, y)$ โดยที่ x และ y เป็นพิกัดในแนวนอนและแนวตั้งของจุดภาพ และค่าของ g ในแต่ละจุด (x, y) นั้น แทนความสว่างหรือระดับสีเทา (Gray level) ของภาพ โดยมีระดับสีเทาอยู่ที่ 256 ระดับ มีค่าตั้งแต่ 0 ถึง 255 ซึ่งสามารถแทนด้วยข้อมูล 8 บิต ต่อหนึ่งจุดภาพ

นิยามข้างต้นเป็นความหมายของรูปภาพแบบระดับสีเทา ซึ่งเป็นตัวแทนของรูปภาพอย่างง่าย สะดวกต่อการคำนวณและการทดลอง ดังนั้นงานวิจัยนี้จะอ้างถึงรูปภาพแบบระดับสีเทา อย่างไรก็ตามแนวคิดและวิธีการทั้งหมด ในงานวิจัยนี้สามารถนำไปประยุกต์ใช้กับรูปภาพสีแบบอื่นต่อไปได้

กระบวนการแก้ไขรูปภาพที่ใช้ในงานวิจัยนี้ แบ่งเป็น 2 ประเภท คือการแก้ไขโดยผู้ไม่ประสงค์ดี โดยเพิ่มหรือลบวัตถุในภาพ และการประมวลผลภาพซึ่งพบได้ทั่วไปในการใช้งาน เช่น การบีบอัดข้อมูลแบบ JPEG การพิมพ์และสแกน การปรับระดับความเข้มความสว่าง การปรับความแตกต่างความสว่าง เป็นต้น

1.4.2 ลายเซ็นดิจิตอล

ปัจจุบันนี้ลายเซ็นดิจิตอลได้รับการยอมรับในทางกฎหมายว่า เป็นวิธีการที่เป็นมาตรฐานในการตรวจสอบความถูกต้องของข้อมูลที่อยู่ในรูปดิจิตอลซึ่งใช้ในคอมพิวเตอร์ แนวคิดพื้นฐานก็คือการนำข้อมูลที่ต้องการปกป้อง มาผ่านกระบวนการแปลงที่เรียกว่าแฮชฟังก์ชัน (Hash function) เพื่อให้ได้ตัวแทนของข้อมูลนั้นแต่มีขนาดลดลง แล้วนำมาเข้ารหัสลับโดยอัลกอริทึมแบบ RSA ซึ่งเป็นการเข้ารหัสแบบอสมมาตร จะทำให้ได้ผลลัพธ์เป็นลายเซ็นดิจิตอล ซึ่งจะถูกส่งแนบไปกับข้อมูลนั้นๆ วิธีการนี้เป็นที่นิยมและสามารถใช้กับข้อมูลดิจิตอลที่เป็นตัวอักษรได้อย่างสะดวก เช่นการส่งข้อมูลทางธุรกิจในรูปแบบคอมพิวเตอร์ แต่เมื่อนำมาประยุกต์ใช้กับข้อมูลรูปภาพจำเป็นต้องมีการศึกษาและหาวิธีการที่เหมาะสม ซึ่งงานวิจัยนี้ใช้วิธีการเลือกลักษณะเฉพาะบางอย่างที่สามารถเป็นตัวแทนของรูปภาพ นำมาเข้ารหัสลับ จากนั้นก็จะนำลายเซ็นที่ได้นั้นซ่อนกลับเข้าไปในรูปภาพ

1.4.3 ลายน้ำดิจิตอล

การซ่อนข้อมูล (Data hiding) หรือการซ่อนลายน้ำดิจิตอล (Watermarking) เมื่อใช้กับรูปภาพ หมายถึงการฝังข้อมูล (Embedded) ลงในส่วนที่เป็นเนื้อหาของสื่อดิจิตอล ซึ่งเป็นพาหะ โดยให้กระทบต่อคุณภาพของสื่อพาหะให้น้อยที่สุด และซ่อนเร้นจากการถูกสังเกตพบโดยมนุษย์ เช่น เป็นข้อมูลที่ยากต่อการมองเห็นเมื่อซ่อนอยู่ในภาพ หรือยากต่อการได้ยินเสียงแปลกปลอมเมื่อ

ซ่อนอยู่ในเสียง ข้อมูลที่จะถูกนำมาซ่อนในกรณีนี้ก็คือลายเซ็นดิจิตอลของรูปภาพ โดยประยุกต์วิธีการซ่อนลายน้ำโดยใช้เทคนิคแบบสเปรดสเปคตรัม ซึ่งเป็นเทคนิคในการซ่อนข้อมูลลงในรูปภาพอย่างแนบเนียนและทนทานต่อการเปลี่ยนแปลงแก้ไขได้อย่างมีประสิทธิภาพดีในระดับหนึ่ง

1.5 ขอบเขตการวิจัย

1. ภาพดิจิตอลที่ใช้ในงานวิจัยนี้เป็นภาพ 2 มิติแบบความเข้มสีเทา (Grayscale) ซึ่งได้จากภาพถ่ายของคน สัตว์ หรือวัตถุจริง

2. รูปภาพที่ผ่านการแก้ไขเปลี่ยนแปลง และนำมาตรวจสอบ เป็นภาพที่ถูกแก้ไขโดยกระบวนการแก้ไขรูปภาพดังต่อไปนี้

- การปรับค่าความสว่าง (Brightness adjustment)
- การเพิ่มสัญญาณรบกวน (Noise adding)
- การปรับค่าความแตกต่างความสว่าง (Contrast adjustment)
- การบีบอัดรูปภาพแบบ JPEG (JPEG image compression)
- การแก้ไขบิดเบือนวัตถุในภาพ (Object modification)

3. วิธีการซ่อนลายน้ำใช้สำหรับวัตถุประสงค์ในการตรวจสอบความถูกต้องของรูปภาพเท่านั้น

1.6 ขั้นตอนของการวิจัย

1. ศึกษาค้นคว้างานวิจัยที่เกี่ยวข้องในปัจจุบัน ทดลองนำวิธีการที่มีการวิจัยนั้นประยุกต์ใช้ เพื่อวิเคราะห์และเปรียบเทียบข้อดีข้อเสียของวิธีการต่างๆ

2. กำหนดแนวทาง วัตถุประสงค์ ขอบเขตของงานวิจัย และกำหนดวิธีการที่จะศึกษา

3. หาวิธีการประยุกต์ใช้ลายเซ็นดิจิตอลกับรูปภาพ หาลักษณะเฉพาะที่เหมาะสมสำหรับนำมาสร้างลายเซ็นดิจิตอล และทดสอบวิธีการวัดค่าความสัมพันธ์ระหว่างบล็อกของภาพ เพื่อแก้ปัญหาของวิธีการแบบเดิม

4. พัฒนาการซ่อนลายน้ำสำหรับลายเซ็นดิจิตอลที่ได้ในรูปภาพ และการค้นคืนลายเซ็นดิจิตอล รวมถึงกระบวนการตรวจสอบรูปภาพ

5. ทำการทดลอง สรุปผลและประเมินผลการวิจัย พร้อมทั้งเสนอแนวทางปรับปรุง

6. รวบรวมรายงานการวิจัย และจัดเตรียมวิทยานิพนธ์

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1. พัฒนาวิธีการที่น่าเชื่อถือสำหรับตรวจสอบความถูกต้องของรูปภาพ ซึ่งผ่านกระบวนการแก้ไขเปลี่ยนแปลงได้ โดยไม่จำเป็นต้องใช้ภาพต้นฉบับในขบวนการตรวจสอบ

2. พัฒนาวิธีการตรวจสอบและซ่อนลายเซ็นดิจิตอลในตัวรูปภาพ ให้สามารถตรวจสอบการเปลี่ยนแปลงแก้ไขเฉพาะส่วนพื้นที่ของรูปภาพได้ ทำให้สามารถป้องกันส่วนของรูปภาพบางส่วนที่สำคัญได้ดีขึ้น

3. สามารถเทคนิคที่คิดค้นนี้ไปประยุกต์ใช้ในการตรวจสอบความถูกต้องของรูปภาพที่เผยแพร่กันในระบบอินเตอร์เน็ตหรือสื่อดิจิตอลอื่นได้

1.8 นิยามศัพท์

เพื่อความเข้าใจที่ตรงกันผู้วิจัยขออธิบายนิยามคำศัพท์ที่มักถูกอ้างถึงในวิทยานิพนธ์ดังนี้

1. รูปภาพดิจิตอล หมายถึงรูปภาพดิจิตอลแบบความเข้มสีเทาซึ่งแปลงจากภาพถ่ายที่มีระดับสีธรรมชาติ

2. ลายน้ำดิจิตอล หมายถึงข้อมูลใดๆ ที่ถูกรวมเข้ากับรูปภาพดิจิตอลทำให้ข้อมูลจุดภาพมีการเปลี่ยนแปลงระดับความเข้มความสว่าง แต่ยากต่อการสังเกตเห็น หรือแยกออกจากกัน

3. ลายเซ็นดิจิตอล หมายถึงข้อมูลตัวแทนของต้นฉบับ ในรูปแบบที่ถูกเข้ารหัสด้วยระบบการเข้ารหัสแบบคู่กุญแจส่วนตัว/สาธารณะ สำหรับส่งแนบไปกับข้อมูลต้นฉบับ เพื่อใช้ในการตรวจสอบความถูกต้อง

4. การแก้ไขรูปภาพดิจิตอล หมายถึงกระบวนการเปลี่ยนแปลงข้อมูลความเข้มความสว่างของจุดภาพ ซึ่งอาจจะถูกสังเกตเห็นหรือไม่ก็ได้

5. ค่าสัมพัทธ์ หมายถึงผลจากการคำนวณจากความสัมพันธ์ของลักษณะเฉพาะ ระหว่างบล็อกรูปภาพ

บทที่ 2
หลักการและทฤษฎีที่เกี่ยวข้อง

2.1 การซ่อนข้อมูล

การซ่อนข้อมูลเป็นกระบวนการฝัง (Embedding) ข้อมูลบางอย่างรวมเข้ากับส่วนที่เป็นเนื้อข้อมูลของสื่อดิจิตอลต่างๆ อาทิเช่น ข้อความ เสียง ภาพ ภาพเคลื่อนไหว เป็นต้น โดยกระทบต่อคุณภาพของข้อมูลข่าวสารในสื่อนั้นให้น้อยที่สุด และซ่อนเร้นจากการถูกสังเกตพบโดยมนุษย์หรือวิธีการตรวจจับโดยทั่วไปซึ่งหมายถึง ความยากต่อการมองเห็นเมื่อซ่อนอยู่ในภาพ หรือยากต่อการได้ยินเสียงแปลกปลอม เมื่อซ่อนอยู่ในข้อมูลเสียง แนวคิดนี้มีที่มาจากคำภาษากรีก คำว่า "Steganography" ที่แปลว่าการเขียนที่ซ่อนเร้น การซ่อนข้อมูลที่พบในชีวิตประจำวันเช่น การใช้หมึกล่องหนที่ทำจากน้ำผลไม้ เป็นต้น

2.1.1 ลักษณะของการซ่อนข้อมูล

2.1.1.1 ข้อมูลที่ซ่อนควรถูกรวมไว้ในตัวสื่อ แทนที่จะเก็บในส่วนเฮดเดอร์ไฟล์ เพื่อให้การแยกข้อมูลนั้นออกจากสื่อทำได้ยาก โดยเฉพาะรูปภาพดิจิตอลซึ่งมีรูปแบบของแฟ้มข้อมูลที่มีความหลากหลาย แต่ถ้าหากทราบกุญแจลับหรือรู้วิธีการที่ใช้ซ่อนข้อมูลจะสามารถตรวจสอบการมีอยู่หรือแยกเอาข้อมูลที่ซ่อนอยู่นี้ออกมาได้

2.1.1.2 การซ่อนข้อมูลนี้ต้องไม่ทำให้สื่อด้อยคุณภาพลงอย่างมีนัยสำคัญ และข้อมูลที่ซ่อนอยู่ควรเป็นที่สังเกตได้ยาก หมายถึงผู้สังเกตจะไม่รู้ถึงการมีอยู่ของข้อมูลที่ซ่อนอยู่นี้ ถึงแม้ว่ามันจะมีอยู่ก็ตาม หรือหากแม้ว่าสามารถสังเกตพบได้ แต่ก็ยากต่อการแยกเอาข้อมูลที่ซ่อนอยู่ออกมาได้ โดยที่ไม่ทำลายคุณภาพของสื่อพาหะ

2.1.1.3 ข้อมูลที่ซ่อนอยู่ควรมีความทนทาน (Robustness) ต่อการแก้ไขเปลี่ยนแปลงหรือการลบทำลาย สำหรับข้อมูลรูปภาพตัวอย่างเช่น การลดทอนคุณภาพจากสัญญาณรบกวน การกรอง การปรับขนาด การตัดบางส่วน การเข้ารหัส การบีบอัดขนาดข้อมูล การพิมพ์ การสแกน และการแปลงสัญญาณ ดิจิตอล/อนาล็อก หรือ อนาล็อก/ดิจิตอล ทั้งนี้ในกรณีของการประยุกต์ใช้งานเพื่อการตรวจสอบความถูกต้องของข้อมูล ความทนทานนี้จะมีขีดจำกัดในระดับหนึ่งเท่านั้น หากว่าการแก้ไขมีปริมาณมากจนทำลายคุณภาพหรือความหมายของสื่อข้อมูลที่ซ่อนอยู่ก็จะถูกทำลายไปด้วย

2.1.2 วัตถุประสงค์ของการซ่อนข้อมูล

การซ่อนข้อมูล มีวัตถุประสงค์หลักที่แตกต่างจากการเข้ารหัส นั่นคือต้องการเพิ่มข้อมูลจำนวนหนึ่งเข้าไปในสื่อที่ทำหน้าที่เป็นเพียงตัวพาหะ ไม่ได้ต้องการให้ตัวสื่อเองเป็นความลับ ข้อมูลที่ถูกเพิ่มเข้าไปในสื่อ มีวัตถุประสงค์การใช้งานอยู่สี่ประเภทใหญ่ [2] ได้แก่

2.1.2.1 การซ่อนข่าวสารลับ (Secret message hiding) มีวัตถุประสงค์เพื่อที่จะส่งข้อมูลข่าวสารลับโดยไม่ต้องการให้เป็นที่น่าสังเกต หรือตรวจจับได้ว่ามีการส่งข่าวสารลับนั้น ความต้องการที่สำคัญคือเทคนิคที่ซ่อนจะต้องทำให้ข้อมูลลับนั้นถูกสังเกตได้ยาก แต่ไม่จำเป็นต้องมีความทนทานต่อการแก้ไข ดังนั้นปริมาณข้อมูลที่ซ่อนได้จะมีมาก

2.1.2.2 การซ่อนเครื่องหมายลิขสิทธิ์ (Copyright watermarking) การประยุกต์ใช้ที่ต้องการความทนทานต่อการถูกแก้ไขทำลายสูง เช่นการซ่อนข้อมูลจำพวกลายเซ็นผู้เขียน เครื่องหมายการค้า เครื่องหมายลายน้ำ เพื่อให้คงอยู่กับสื่อที่ต้องการปกป้องให้ได้มากที่สุด เทคนิคที่ใช้จำเป็นจะต้องมีการทำซ้ำข้อมูล ดังนั้นปริมาณข่าวสารที่ซ่อนได้จึงน้อยกว่าวิธีแรก

2.1.2.3 การตรวจสอบการถูกแก้ไข (Tamper proofing) วัตถุประสงค์ก็เพื่อตอบคำถามเช่นว่า ภาพนี้มีการแก้ไขหรือไม่ แนวคิดก็คือใช้การมีอยู่ของข้อมูลที่ซ่อนเป็นตัวตรวจสอบว่ามีการแก้ไขข้อมูลพาหะหรือไม่ โดยใช้เทคนิคการซ่อนที่มีความทนทานปานกลาง จะทนทานต่อการแก้ไขที่มีปริมาณน้อย แต่จะถูกแก้ไขทำลายได้เมื่อผ่านการแก้ไขปริมาณมาก งานวิจัยนี้มีการใช้การซ่อนข้อมูลเพื่อวัตถุประสงค์จัดอยู่ในประเภทนี้

2.1.2.4 การเพิ่มหมายเหตุ (Caption) เป็นการซ่อนข้อมูลจำพวก คำอธิบายภาพ ชื่อเพลง ผู้แต่ง ที่ไม่ขึ้นกับรูปแบบการจัดเก็บในแฟ้มข้อมูล ซึ่งต้องซ่อนข้อมูลปริมาณมาก และไม่ต้องการความทนทานต่อการถูกแก้ไข สามารถเข้าถึงข้อมูลได้ง่าย และไม่ต้องเป็นความลับ

2.1.3 เทคนิคการซ่อนข้อมูล

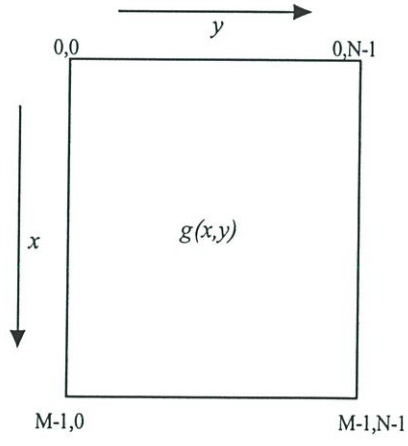
2.1.3.1 เทคนิคการซ่อนข้อมูลในสื่อดิจิตอลแบบข้อความ (Text) จะมีการใช้พื้นที่ข้อมูลส่วนที่ยากต่อการสังเกต เช่นตัวอักขระช่องว่าง โดยการเพิ่มช่องว่างระหว่างคำ หรือช่องว่างบริเวณท้ายบรรทัด วิธีนี้มีความทนทานค่อนข้างต่ำต่อการถูกแก้ไขทำลาย อีกแนวทางหนึ่งคือใช้สไตล์การเขียนที่มีลักษณะเฉพาะ เช่นการใช้คำเสมือนที่แทนกันได้ หรือใช้การสลับการวางตำแหน่งรูปประโยคที่ไม่ทำให้ความหมายต่างไปจากเดิม

2.1.3.2 การซ่อนข้อมูลสำหรับเสียงดิจิตอล เนื่องจากความสามารถในการรับฟังเสียงของมนุษย์ มีความหลากหลายและช่วงความถี่ที่แตกต่างกัน เสียงรบกวนแม้เพียงปริมาณน้อยก็สามารถถูกสังเกตพบได้ อย่างไรก็ตามยังมีช่องว่างในการซ่อนข้อมูลอยู่ โดยใช้ความแตกต่างของความดัง หรือใช้ลักษณะของเฟสซึ่งมนุษย์จะรับได้เฉพาะเฟสที่สัมพันธ์กันเท่านั้น

2.1.3.3 การซ่อนข้อมูลสำหรับรูปภาพดิจิตอล มี 2 แนวทางหลัก คือการมองภาพให้อยู่ในรูปแบบความถี่ (Frequency domain) หรือในรูปแบบอาเรย์ของค่าความสว่างแบบสองมิติ (Spatial domain) จะกล่าวโดยละเอียดในหัวข้อต่อไป

2.2 รูปภาพดิจิตอล

รูปภาพดิจิตอลเริ่มมีการใช้งานครั้งแรกประมาณต้นทศวรรษที่ 1920 [12] เพื่อวัตถุประสงค์หลักในการส่งข้อมูลรูปถ่ายข่าวหนังสือพิมพ์ผ่านระบบสายเคเบิลใต้น้ำของ Bartlane เชื่อมระหว่างลอนดอนกับนิวยอร์ก ข้ามมหาสมุทรแอตแลนติก ซึ่งช่วยลดระยะเวลาการส่งข้อมูลจากเดิม 3 วันเหลือเพียงไม่ถึง 3 ชั่วโมง โดยใช้อุปกรณ์เข้ารหัสดิจิตอลที่ต้นทางและเครื่องพิมพ์แบบดิติตอลที่ปลายทาง รุ่นแรกที่ใช้นั้นสามารถส่งภาพได้ 5 ระดับความสว่าง และพัฒนาจนส่งภาพได้ที่ 15 ระดับความสว่าง พัฒนาการในการสื่อสารภาพแบบดิจิตอลมีต่อเนื่องมาจนกระทั่ง 35 ปีต่อมาเมื่อคอมพิวเตอร์ได้กำเนิดขึ้นจึงเริ่มมีการประมวลผลภาพดิจิตอลโดยคอมพิวเตอร์ ในปี 1964 มีการใช้คอมพิวเตอร์ในการซ่อมแซมเพิ่มคุณภาพของรูปภาพที่ส่งมาจากยานอวกาศ และตั้งแต่นั้นเป็นต้นมาการใช้งานรูปภาพดิจิตอลได้เข้ามาเกี่ยวข้องกับชีวิตประจำวันมากขึ้น ทั้งในวงการแพทย์ วิศวกรรมสถาปัตยกรรม ภาพยนตร์ โฆษณา โดยเฉพาะในปัจจุบันซึ่งเป็นยุคอินเตอร์เน็ต ที่มีการแลกเปลี่ยนข้อมูลข่าวสารในรูปของรูปภาพดิจิตอลกันมากขึ้น



รูปที่ 2.1 ตัวอย่างการแทนรูปภาพแบบดิจิตอล

รูปภาพดิจิตอลที่ใช้ในการวิจัยนี้อ้างถึงความหมายในแง่ของ ฟังก์ชันค่าความสว่างในพิกัดสองมิติ [18] โดยที่รูปภาพขนาดแนวตั้งและแนวนอน $M \times N$ จุดภาพ (Pixel) จะแทนด้วยฟังก์ชัน g(x, y) โดยที่ $x \in 0,\ldots, M\text{-}1$ และ $y \in 0,\ldots, N\text{-}1$ ดังแสดงในรูปที่ 2.1 ค่าของฟังก์ชันและพิกัดของรูปภาพดิจิตอลจะถูกแปลงเป็นค่าจำนวนเต็มไม่ต่อเนื่อง ภาพดิจิตอลสามารถพิจารณาในรูปของเมตริกที่แถวและสดมส์ระบุถึงจุดในภาพ และค่าของเมตริกคือค่าความสว่างตรงตำแหน่งนั้น

ในงานวิจัยนี้จะใช้ภาพที่ถ่ายหรือสแกนมาจากภาพถ่ายของ คน สัตว์ หรือวัตถุที่มีอยู่จริงในธรรมชาติ โดยจะแปลงให้เป็นรูปภาพแบบความเข้มระดับสีเทาที่ 256 ระดับ มีค่าตั้งแต่ 0 ถึง 255 ซึ่งแทนข้อมูลด้วยจำนวนขนาด 8 บิตต่อหนึ่งจุดภาพ

2.2.1 การแก้ไขรูปภาพ

2.2.1.1 การแก้ไขรูปภาพ เป็นกระบวนการที่ทำให้ข้อมูลในรูปภาพมีการเปลี่ยนแปลง [17] ซึ่งพบได้เสมอในการใช้งานรูปภาพ เพื่อทำให้รูปภาพมีคุณภาพดีขึ้น หรือเพื่อเผยแพร่ในรูปแบบไฟล์หรือสื่อประเภทต่างๆ เช่น

1. การบีบอัดข้อมูลแบบสูญเสีย (Lossy compression) เป็นกระบวนการลดปริมาณข้อมูลรูปภาพ วิธีการที่เป็นที่รู้จักแพร่หลายคือการบีบอัดข้อมูลรูปภาพแบบ JPEG
2. การปรับความเข้มความสว่าง (Brightness adjustment) ทำให้ภาพมืดหรือสว่างมากขึ้น โดยการบวกหรือลบระดับความสว่างของทุกๆจุดในรูปภาพ ในปริมาณที่เท่ากัน
3. การปรับความแตกต่าง (Contrast adjustment) ทำให้วัตถุในภาพมีความเด่นชัดมากขึ้น โดยใช้การปรับค่าฮิสโตรแกรมระดับความสว่างของจุดภาพ
4. การเพิ่มสัญญาณรบกวน (Noise adding) มีสัญญาณรบกวนแบบสุ่มเกิดขึ้นในรูปภาพ มักจะเกิดเมื่อภาพดิจิตอลเผยแพร่ผ่านสื่อแบบอนาล็อก เช่นการพิมพ์หรือส่งผ่านสัญญาณวิทยุ

2.2.1.2 การแก้ไขปลอมแปลงรูปภาพโดยเจตนา (Image modification) เกิดจากความจงใจของบุคคลที่สามที่ต้องการเปลี่ยนแปลงแก้ไขข้อมูลรูปภาพเพื่อบิดเบือนความหมายของรูปภาพ ทำให้ผู้รับเกิดการเข้าใจผิด หรือแก้ไขเพื่อแอบอ้างความเป็นเจ้าของ การแก้ไขมักจะเป็นการนำวัตถุจากภาพอื่นเข้ามาแทนที่หรือเพิ่มในรูปภาพ หรือลบวัตถุที่ปรากฏในรูปภาพทิ้งไป [14]

2.2.2 การแยกลักษณะเฉพาะของภาพ

การแยกลักษณะเฉพาะ (Feature extraction) [21] เป็นขั้นตอนหนึ่งในกระบวนการทั่วไป สำหรับประมวลผลรูปภาพ มีวัตถุประสงค์เพื่อแปลความหมายของรูปภาพให้เหมาะสมสำหรับการประมวลผลโดยคอมพิวเตอร์ การแยกลักษณะเฉพาะของรูปภาพมีหลายแบบ เช่น ขอบเขตของพื้นที่ (Region boundary) เส้นขอบ (Edge) ลักษณะพื้นผิว (Texture) หรือ รูปโครงร่าง (Skeletal shape) เป็นต้น ซึ่งในการใช้งานจะต้องมีการเลือกใช้ลักษณะเฉพาะให้เหมาะสมกับงานแต่ละประเภทแตกต่างกันไป สำหรับงานวิจัยนี้เลือกใช้ลักษณะเฉพาะที่เรียกว่า การแบ่งสัดส่วนแบบบล็อก (Block scaling) และคำนวณค่าความสัมพันธ์ระหว่างบล็อก ดูรายละเอียดในบทที่ 3

2.3 ลายน้ำดิจิตอล

2.3.1 นิยามและวัตถุประสงค์การใช้ลายน้ำดิจิตอล

ลายน้ำดิจิตอล (Digital watermark) หมายถึงข้อมูลซึ่งถูกซ่อนเข้าไปในรูปภาพดิจิตอล วัตถุประสงค์ดั้งเดิมในการซ่อนลายน้ำเพื่อปกป้องลิขสิทธิ์ โดยทำการซ่อนสัญลักษณ์ของเจ้าของรูปภาพลงไป ให้มีความทนทานต่อการแก้ไขทำลายสูง ต่อมามีการใช้งานลายน้ำดิจิตอลในลักษณะอื่นมากขึ้น จึงพอสรุปประเภทของลายน้ำได้ 3 ประเภท ตามวัตถุประสงค์ของการใช้งานดังนี้

2.3.1.1 ลายน้ำทนทานสูง (Robust watermark) ลายน้ำประเภทนี้ถูกใช้เพื่อปกป้องลิขสิทธิ์ความเป็นเจ้าของรูปภาพ [3][8] มีความต้านทานต่อการแก้เปลี่ยนแปลงรูปภาพสูง และยากต่อการลบทำลาย ลายน้ำประเภทนี้อาจจะสังเกตจากภาพได้ง่าย แต่การที่จะแยกหรือทำลายลายน้ำโดยหลีกเลี่ยงไม่ทำให้รูปภาพเสียหายนั้นทำได้ยาก โดยทั่วไปเมื่อกล่าวถึงลายน้ำดิจิตอล มักจะหมายถึงลายน้ำประเภทนี้

2.3.1.2 ลายน้ำเปราะบาง (Fragile watermark) เป็นลายน้ำที่ง่ายต่อการสูญหายหรือถูกลบทำลาย ลายน้ำประเภทนี้จะถูกซ่อนให้สังเกตเห็นได้ยาก แต่จะถูกเปลี่ยนแปลงแก้ไขได้ง่าย วัตถุประสงค์ในการใช้งานลายน้ำประเภทนี้ คือเพื่อใช้ตรวจสอบว่ารูปภาพนั้นถูกแก้ไขเปลี่ยนแปลงจากภาพต้นฉบับหรือไม่ [7]

2.3.1.3 ลายน้ำกึ่งเปราะบาง (Semi fragile watermark) ลายน้ำประเภทนี้พัฒนามาจากลายน้ำในข้อ 2.3.1.2 อีกขั้นหนึ่งก็คือเป็นลายน้ำที่มีความทนทานในระดับปานกลาง สามารถถูกแก้ไขเปลี่ยนแปลง ได้โดยที่ยังสามารถตรวจพบลายน้ำได้ [20] [22] วัตถุประสงค์ของการใช้ลายน้ำแบบนี้คือ เพื่อใช้ตรวจสอบว่าภาพถูกแก้ไขเปลี่ยนแปลงในลักษณะใดบ้างมากน้อยเพียงใด ซึ่งขึ้นอยู่กับเทคนิคในการสร้างลายน้ำว่าจะให้มีความทนทานต่อกระบวนการแก้ไขประเภทใด การซ่อนลายน้ำในงานวิจัยนี้มีวัตถุประสงค์จัดอยู่ในลายน้ำประเภทนี้

2.3.2 วิธีการซ่อนลายน้ำดิจิตอลแบบสเปรดสเปคตรัม

ทฤษฎีซึ่งเป็นพื้นฐานของเทคนิคการซ่อนข้อมูลได้ถูกเสนอโดยบทความวิชาการอย่างแพร่หลายในช่วงปี 1996 [5][9] กล่าวถึงการซ่อนข้อมูลดิจิตอลคือการเพิ่มค่าที่ได้จากการรวมเชิงเส้นของฟังก์ชันพื้นฐาน B_i เข้ากับสื่อพาหะ C (Carrier) ผลลัพธ์ทำให้ได้ สื่อที่ซ่อนเร้น S (Stego) สำหรับสื่อรูปภาพ B_i, C และ S นั้น ถูกนิยามในรูปแบบของฟังก์ชัน 2 มิติ ของพิกัดจุด (x, y) การซ่อนหรือการเปลี่ยนแปลงในสื่อพาหะแทนได้ดังนี้

$$\text{Stego-Image(S)} = \text{Original Carrier Image (C)} + \text{Modifications (M)} \qquad (2.1)$$

โดยที่ $\text{Modifications} = \sum m_i B_i(x,y)$ เมื่อ $m_i \in \{-M, -M+1, ..., M-1, M\}$

ปัจจุบันอัลกอริทึมที่มีประสิทธิภาพสูง และเป็นที่นิยมใช้ในการสร้างลายน้ำดิจิตอล มีพื้นฐานมาจากเทคนิคสเปรดสเปคตัม ซึ่งมีการใช้งานกันอย่างแพร่หลายในงานการสื่อสารสัญญาณวิทยุ โดยเฉพาะในภาวะสงคราม แนวคิดคือพยายามส่งสัญญาณข้อความลับไปกับสัญญาณรบกวนซึ่งมีปริมาณมาก แต่กำลังของสัญญาณต่ำเพื่อให้ยากต่อการตรวจจับ วิธีการนี้คือการเข้ารหัสแบบไดเร็คซีเควน [19] โดยมีรายละเอียดดังนี้

ข้อมูลลายน้ำ $\{w_i\}$, $w_i \in \{-1, 1\}$ จะได้รับการกระจาย cr ตัว โดยแต่ละ w_i จะมีการซ้ำกัน cr ครั้ง

$$\{b_j\} = w_1, \ldots, w_1, w_2, \ldots, w_2, \ldots, w_i, \ldots, w_i, \ldots w_N$$

จากนั้นนำมารวมกับภาพต้นฉบับ c_j โดยใช้สูตร

$$s_j = c_j + \alpha\, b_j\, p_j \qquad (2.2)$$

โดยที่ s_j คือภาพที่ถูกซ่อนลายน้ำ

$p_j \in \{-1, 1\}$ คือสัญญาณรบกวนเทียมมีค่าเฉลี่ยเป็น 0

α คือตัวแปรในการปรับค่าแอมปลิจูด ความเข้มกำลังของลายน้ำดิจิตอล

$$w_j = \sum_{i=j\cdot cr}^{(j+1)cr-1} p_i s_i = \sum_{i=j\cdot cr}^{(j+1)cr-1} p_i c_i + \sum_{i=j\cdot cr}^{(j+1)cr-1} p_i^2 \alpha b_i \cong \Delta + cr.\alpha.w_j \qquad (2.3)$$

$$\Delta = mean_i(s_i) \sum_{i=j.cr}^{(j+1)cr-1} p_i \cong 0 \qquad (2.4)$$

การแยกลายน้ำออกจากภาพทำได้โดยการนำสัญญาณรบกวนเทียม (p_j) มาโมดูเลตกับภาพที่ถูกซ่อนลายน้ำ ผลลัพธ์ที่ได้จะถูกพิจารณาแยกเป็นผลรวมของกลุ่มตัวแปรสองกลุ่มตัวแปรจากสมการที่ (2.2) โดยที่พจน์แรกจะมีค่าประมาณเป็น 0 เพราะว่าเป็นผลรวมของค่าสัญญาณรบกวนเทียมที่มีค่าเฉลี่ยเป็นศูนย์

ดังนั้นเราสามารถตัดพจน์แรกทิ้งไปได้ จะทำให้ได้ w_j มีค่าประมาณเท่ากับ $cr * \alpha * m_j$ ซึ่งเราสามารถหาค่า m'_j ที่แม่นยำได้โดยการตรวจค่าเครื่องหมายของ w_j โดยที่ลายน้ำที่ถอดรหัสได้ (m'_j) จะมีค่าดังคำนวณได้จากสมการที่ 2.5

$$m'_j = w'_j = SIGN(w_j) = \{-1, 1\} \qquad (2.5)$$

2.4 การเข้าและถอดรหัสลับแบบใช้กุญแจสาธารณะ

ย้อนไปในประวัติศาสตร์ มนุษย์ได้มีการใช้วิธีการเข้ารหัสข้อมูลในการส่งข้อความข่าวสาร นับเวลาเป็นพันปีแล้ว ตั้งแต่สมัยอียิปต์ กรีก อาณาจักรโรมัน กษัตย์จูเลียส ซีซาร์ มีวิธีส่งข้อความลับโดยฝากจดหมายลับไปกับผู้นำสาร โดยเปลี่ยนตัวอักษร A เป็น D ตัว B เปลี่ยนเป็น E และตัวอักษรอื่นเลื่อนไปอีกสาม (Shift by 3) เช่นกัน ตัวอย่างเช่น ต้องการส่งข้อความ "Hello I Miss You" โดยเข้ารหัสเป็น "Khoor L Plvv Brx" ส่วนผู้รับซึ่งได้มีการตกลงไว้ก่อนแล้วว่าจะใช้วิธีการ "Shift by 3" นี้ในการส่งข้อความก็จะทำการถอดรหัสโดยทำย้อนกลับให้ได้ข้อความเดิม

ตามทฤษฎีการเข้าและถอดรหัสลับแบบดั้งเดิม เมื่อผู้เข้ารหัสเลือกใช้การกุญแจลับเข้ารหัสและกุญแจที่ใช้ในการถอดรหัส พบว่ากุญแจที่ใช้ในการถอดรหัสนี้จะเหมือน หรือถูกแปลงมาจากกุญแจที่ใช้เข้ารหัสลับอย่างง่ายดาย เช่นการเข้าและถอดรหัสแบบ DES จะใช้กระบวนการเดียวกันทั้งตอนเข้าและถอดรหัสแต่ตารางค่าของกุญแจที่ใช้จะผกผันกัน หรือการเข้ารหัสแบบ "Shift by 3" จะใช้การเลื่อนไปและเลื่อนกลับ ซึ่งระบบการเข้าและถอดรหัสที่มีลักษณะเช่นนี้เป็นที่รู้จักกันว่าเป็นระบบกุญแจส่วนตัว (Private-Key systems) เนื่องจากกุญแจที่ใช้จะต้องรักษาเป็นความลับกันระหว่างผู้ส่งและผู้รับข่าวสาร ซึ่งจะให้บุคคลที่สามรู้ไม่ได้เป็นอันขาด มิฉะนั้นระบบจะไม่ปลอดภัยทันที ด้วยลักษณะของกุญแจในการเข้าและถอดรหัสที่เหมือนกันดังกล่าวทำให้ ระบบนี้จึงมีชื่ออีกชื่อหนึ่งว่า การเข้าและถอดรหัสแบบสมมาตร (Symmetry cryptography)

จุดอ่อนประการหนึ่งของระบบกุญแจส่วนตัวคือ จำเป็นต้องมีการตกลงและส่งมอบกุญแจลับที่ใช้กันระหว่างผู้ส่งสื่อกับผู้รับสื่อเสียก่อนที่จะเริ่มส่งข่าวสารกัน การส่งมอบกุญแจนี้ต้องทำให้ปลอดภัยและเป็นความลับมากที่สุด เพื่อป้องกันบุคคลที่สามนำไปใช้ถอดรหัส ซึ่งในทางปฏิบัติแล้วทำได้ยากมาก เช่นการรับส่งข้อมูลทางอิเล็คทรอนิคเมล์ ซึ่งเป็นวิธีการที่ไม่ปลอดภัย

แนวคิดของระบบกุญแจสาธารณะ (Public-Key system) มาจากความคิดที่ว่าน่าจะมีวิธีการเข้าและถอดรหัสลับ ที่ใช้กุญแจในการเข้ารหัสลับไม่เหมือนกับกุญแจที่ผู้รับใช้ถอดรหัส โดยที่ไม่สามารถจะคำนวณหาค่าของกุญแจที่ใช้ในการถอดรหัสจากค่าของกุญแจที่ใช้เข้ารหัสลับได้ (หรือใช้เวลานานมากในการคำนวณหา) วิธีการใช้งาน คือผ่ายรับกำหนดและส่งมอบกุญแจที่ใช้เข้ารหัสไปยังผู้ที่จะส่งข่าวสารลับมาให้ โดยไม่จำเป็นต้องปกปิดเป็นความลับ บุคคลที่สามสามารถรู้กุญแจที่ใช้เข้ารหัสได้ เพราะว่ากุญแจที่ใช้เข้ารหัสนั้นไม่สามารถใช้ในการถอดรหัสได้ จะมีเพียงผู้รับที่เก็บกุญแจสำหรับใช้ถอดรหัสลับไว้เท่านั้น ที่สามารถรับและถอดรหัสข่าวสารจากผู้ส่งดังกล่าวได้ แนวคิดนี้ถูกเสนอโดย Diffie และ Hellman ในปี 1976 ซึ่งวิธีการที่ได้รับการยอมรับว่าเชื่อถือได้ซึ่งการประยุกต์ใช้ตามแนวคิดนี้ ได้มีการพัฒนาขึ้นปลายปี 1977 โดย Reverst, Shamir และ

Adleman ได้แก่วิธีการเข้าและถอดรหัสแบบ RSA ซึ่งเป็นระบบการเข้ารหัสแบบกุญแจสาธารณะที่รู้จักกันอย่างแพร่หลายที่สุด ซึ่งต่อมาได้มีการเสนอวิธีการอื่น อีกหลายวิธีที่มีข้อเด่นและข้อด้อยในการคำนวณแตกต่างกันไป ตัวอย่างเช่น Merkel-Hellman Knapsack วิธีการนี้ใช้พื้นฐานของความยุ่งยากของปัญหาผลรวมเซ็ตย่อย (Subset sum problem : NP Complete) วิธีการของ McEliece ใช้ทฤษฎีการแปลงรหัสแบบอัลจีบรา หรือวิธีการของ ElGamal ที่มีพื้นฐานมาจากการแก้ปัญหาล็อกการิทึมแบบไม่ต่อเนื่องบนสนามจำกัด สำหรับวิธีการเข้าและถอดรหัสลับแบบ RSA ซึ่งงานวิจัยได้นำมาประยุกต์ใช้นี้ ใช้ทฤษฎีทางคณิตศาสตร์บนพื้นฐานของจำนวนเฉพาะ (Prime number) และการแยกตัวประกอบจำนวนเต็มที่มีขนาดใหญ่มาก [6]

หลักการที่ถือเป็นหัวใจสำคัญของการเข้าและถอดรหัสลับแบบกุญแจสาธารณะคือลักษณะที่เป็นฟังก์ชันทางเดียว ขั้นตอนการเข้ารหัสด้วยกุญแจสาธารณะนั้นคำนวณได้ง่ายและไม่เป็นความลับ แต่สำหรับขั้นตอนการถอดรหัสโดยบุคคลอื่นผู้ที่ไม่มีกุญแจสำหรับถอดรหัสของผู้รับที่ถูกต้องแล้วนั้นจะทำได้ยาก ลักษณะที่การเข้ารหัสทำได้ง่ายแต่การถอดรหัสโดยบุคคลที่สามทำได้ยากนี้ เรียกว่าลักษณะเป็นทางเดียว ตัวอย่างของฟังก์ชันทางเดียวนี้ เช่นฟังก์ชัน $f(x) = x^b \bmod n$ โดยกำหนดให้ n เป็นผลคูณของจำตัวเฉพาะ p และ q และให้ b เป็นจำนวนเต็มบวก แต่การนำฟังก์ชันทางเดียวไปใช้กับการเข้าและถอดรหัสได้นั้น จะต้องมีวิธีการแปลงฟังก์ชันกลับได้ มิฉะนั้นผู้รับจะไม่สามารถถอดรหัสได้ การที่ผู้รับรู้ความลับที่ใช้ในการถอดรหัส (กุญแจสำหรับถอดรหัส) ซึ่งจะช่วยให้การถอดรหัสทำได้ง่ายนี้ เปรียบเหมือนกับผู้ใช้ผ่านประตูกล (Trapdoor) ซึ่งเป็นความลับ เราเรียกฟังก์ชันที่มีลักษณะเช่นนี้ว่า ฟังก์ชันทางเดียวประตูลับ (Trapdoor one-way function) จากตัวอย่างฟังก์ชันที่ยกมานี้ใช้เป็นพื้นฐานของวิธีการแบบ RSA ซึ่งจะอธิบายในหัวข้อถัดไป

2.5 วิธีการเข้าและถอดรหัสลับแบบ RSA

ชื่อของวิธีการนี้มาจากชื่อต้นของนักคณิตศาสตร์สามคนที่ร่วมกันคิดค้นได้แก่ Revest, Shamir และ Adelman [4] ได้ถูกประกาศเผยแพร่ในปี 1978 วิธีการนี้มีพื้นฐานการคำนวณทางคณิตศาสตร์ในสาขาทฤษฎีตัวเลข กับวิธีการหาค่าตัวประกอบจำนวนเฉพาะ ใช้ตัวดำเนินการทางคณิตศาสตร์ mod ในการคำนวณ (เป็นการคำนวณหาค่าจำนวนเศษที่เหลือจากการหาร) วิธีการเข้าและถอดรหัสแบบ RSA มีรายละเอียดดังนี้

กำหนดให้ e และ d เป็นกุญแจที่ใช้เข้าและถอดรหัสตามลำดับ ข้อความ P จะถูกเข้ารหัสโดย

$$C = P^e \bmod n. \qquad (2.6)$$

การถอดรหัสทำได้โดย

$$P = C^d \bmod n. \qquad (2.7)$$

จากทฤษฎีทางคณิตศาสตร์ ตัวดำเนินการมอดูลัสจะไม่มีผลต่อลำดับก่อนหลังในการยกกำลัง ทำให้เราสามารถสลับตำแหน่งของค่ายกกำลัง e และ d ได้โดยให้ผลลัพธ์ที่เท่ากันดังสมการที่ 2.8

$$P = C^d \bmod n = (P^e)^d \bmod n = (P^d)^e \bmod n. \qquad (2.8)$$

ดังนั้นกุญแจที่ใช้เข้าและถอดรหัสนี้ จะมีลักษณะเป็นคู่ซึ่งสามารถสลับลำดับกันได้ หมายถึงกุญแจทั้งคู่นี้สามารถนำไปใช้ได้ทั้งการเข้าและการถอดรหัส ซึ่งมีประโยชน์อย่างมากสำหรับการนำไปใช้กับลายเซ็นดิจิตอล

2.5.1 อัลกอริทึมเข้ารหัส RSA

2.5.1.1 กุญแจที่ใช้ในการเข้ารหัสประกอบด้วยจำนวนเต็มสองค่าคือ (e, n) และกุญแจที่ใช้ในการถอดรหัสคือ (d, n) ขั้นตอนแรกคือ การหาค่า n ลักษณะของค่า n นี้จะเป็นจำนวนเต็มที่มีขนาดใหญ่มาก เกิดจากการคูณกันของจำนวนเฉพาะสองค่าคือ p และ q โดยปกติแล้ว p และ q ในแต่ละตัวจะเป็นตัวเลขประมาณ 100 หลัก ผลคูณได้แก่ค่า n จะมีขนาดประมาณ 200 หลัก สามารถแทนได้ด้วยเลขฐาน 2 ขนาด 512 บิต ซึ่งจำนวนที่ใหญ่ขึ้นของค่า n จะป้องกันให้วิธีการนี้ปลอดภัยจากการถอดรหัสได้ดียิ่งขึ้น

2.5.1.2 จากนั้นค่า e จะถูกเลือกโดยใช้ค่า $(p\text{-}1) * (q\text{-}1)$ มาทำการคำนวณหาค่าจำนวนเฉพาะสัมพัทธ์ (Relative prime) ให้ได้จำนวนเฉพาะ e ที่มีคุณสมบัติไม่มีตัวประกอบร่วมกับค่า $(p\text{-}1) * (q\text{-}1)$ ซึ่งในทางปฏิบัตินั้นจะเลือกค่าจำนวนเฉพาะที่มีขนาดใหญ่กว่าค่า $(p\text{-}1)$ และ $(q\text{-}1)$ ทั้งคู่

2.5.1.3 การหาค่าของ d ที่มีคุณสมบัติเป็นจำนวนเต็มและ $(e*d - 1)$ ที่หารด้วย $(p\text{-}1) * (q\text{-}1)$ ลงตัว ในทางคณิตศาสตร์ สามารถเขียนอยู่ในรูปของ $e * d \equiv 1 \bmod (p\text{-}1) * (q\text{-}1)$ โดยเรียก d ว่าเป็นตัวคูณผกผัน ของ e (Multiplicative inverse of e) นิยมใช้ Extended Euclidean Algorithm [15] ในการหาค่าของ d

2.5.2 ตัวอย่างการคำนวณของอัลกอริทึม RSA

2.5.2.1 สมมุติการคำนวณกุญแจขนาด 8 บิต เลือก $p = 11$ และ $q = 23$ จะได้ค่า $n = p * q = 253$

2.5.2.2 คำนวณค่า $(p\text{-}1) * (q\text{-}1) = 10 * 22 = 220$ จำนวนเฉพาะที่มีขนาดใหญ่ไล่ลงมาจาก 255 (จำนวนขนาด 8 บิต) ที่ไม่มีตัวประกอบร่วมกับ 220 คือ 251 จะได้ค่า $e = 251$

2.5.2.3 หาค่าของ d โดยใช้วิธีการหาค่าที่ทำให้ $(e*d - 1)$ หารด้วย $((p-1) * (q-1))$ ลงตัว ในที่นี้ d มีค่าเท่ากับ 71 จะทำให้ได้ $(251 * 71) - 1 = 17820$ ซึ่งหารกับ $(p-1) * (q-1)$ ที่มีค่า 220 ได้ลงตัว (81)

2.5.2.4 ดังนั้นจะได้ ค่า $e = 251$, $d = 71$ และ $n = 253$ ซึ่งสามารถแสดงได้ตามตัวอย่างการเข้าและถอดรหัส ข้อมูล P = 100 ดังต่อไปนี้

การเข้ารหัส

$$C = P^e \bmod n$$

$$C = 100^{251} \bmod 253$$

$$C = 78$$

การถอดรหัส

$$P = C^d \bmod n$$

$$P = 78^{71} \bmod 253$$

$$P = 100$$

จากตัวอย่างนี้จะได้กุญแจสำหรับเข้ารหัสคือ $(e, n) = (251, 255)$ กุญแจสำหรับถอดรหัสคือ $(d, n) = (71, 255)$ ในกรณีที่ทำการเข้ารหัสข้อความ เช่น P = "RSA" เมื่อแปลงเป็นรหัส ASCII ได้ 82, 83, 65 และนำมาเข้ารหัสจะได้ข้อความเข้ารหัสเป็น 21, 61, 241 ในการใช้งานจริงขนาดของ e, d และ n จะเป็นจำนวนขนาด 512 บิต หรือมากกว่านั้นเพื่อความปลอดภัยที่น่าเชื่อถือได้

ในทางปฏิบัติแล้วการยกกำลังจำนวนเต็ม e และ d (การดำเนินการแบบ $z = x^b \bmod n$) ขนาด 512 บิต จะมีวิธีการทางคณิตศาสตร์ช่วยในการคำนวณ โดยใช้วิธียกกำลังสองและคูณ โดยให้ b แทนด้วย

$$b = \sum_{i=0}^{l-1} b_i 2^i \qquad (2.9)$$

วิธีการยกกำลังสองและคูณ (Square-and-Multiply) เพื่อหาค่า $z = x^b \bmod n$

1: $z = 1$

2 : for $i = l - 1$ downto 0 do

3 : $z = z^2 \bmod n$

4 : if $b_i = 1$ then $z = z * x \bmod n$

สำหรับปัญหาในการหาค่าจำนวนเฉพาะ p, q ขนาดใหญ่ (ตั้งแต่ 64 บิตขึ้นไป) จะใช้วิธีการของ Solovay-Strassen ซึ่งใช้พื้นฐานแนวคิดจากทฤษฎีจำนวนตัวเลข (Number theory) และ

จาโคบีฟังก์ชัน (Jacobi function) เพื่อทดสอบความน่าจะเป็นที่ตัวเลขจำนวนเต็มใดๆ จะเป็นจำนวนเฉพาะ โดยการทดสอบซ้ำหลายครั้งเพื่อให้ได้ค่าความน่าจะเป็นที่ยอมรับได้ [15]

กุญแจคู่ที่ใช้ในการเข้าและถอดรหัส (*e, d*) สามารถใช้สลับที่ในการเข้าและถอดรหัสได้ แต่จะต้องมีกุญแจตัวใดตัวหนึ่งเป็นความลับและอีกตัวเปิดเผยให้แก่สาธารณะ ซึ่งทำให้มีการใช้งานกุญแจสาธารณะนี้เป็น 2 รูปแบบคือ

1. กุญแจที่ใช้เข้ารหัสเป็นกุญแจสาธารณะ กุญแจที่ใช้ถอดรหัสเป็นความลับแสดงว่าผู้รับเป็นเจ้าของกุญแจคู่นี้ ข้อความที่เข้ารหัสจะอ่านได้โดยผู้รับเพียงคนเดียว การใช้งานแบบนี้ มีไว้เพื่อให้ข้อความที่ส่งไปถึงผู้รับนั้นเป็นความลับ โดยที่บุคคลอื่นที่ไม่รู้กุญแจสำหรับถอดรหัสจะไม่สามารถเข้าใจข่าวสารที่ถูกส่งไปได้เลย

2. กุญแจที่ถอดรหัสเป็นกุญแจสาธารณะ รูปแบบนี้ผู้ส่งจะต้องเก็บกุญแจที่ใช้เข้ารหัสเป็นความลับ โดยที่จะมีเพียงผู้ส่งที่เป็นเจ้าของกุญแจคู่นี้เท่านั้นที่สามารถเข้ารหัสข้อความที่ผู้รับรับได้ การใช้งานแบบนี้จะทำให้ผู้ส่งสามารถยืนยันความเป็นเจ้าของของข้อความที่ส่งไปได้ ซึ่งนำไปสู่การใช้งานลายเซ็นดิจิตอลนั่นเอง

2.6 ลายเซ็นดิจิตอล

2.6.1 นิยามและวัตถุประสงค์การใช้งาน

ในชีวิตประจำวันลายเซ็นที่เกิดจากลายมือชื่อของผู้เซ็น ถูกเซ็นลงไปกับเอกสารเพื่อใช้ในการยืนยันความเป็นเจ้าของและความรับผิดชอบในเอกสารชิ้นนั้นๆ เช่นการส่งจดหมาย การถอนเงินจากธนาคาร การรับรองสัญญาต่างๆ แต่สำหรับลายเซ็นดิจิตอลแล้ว ข้อมูลเอกสารจะอยู่ในรูปแบบของสื่ออิเล็คทรอนิค ลักษณะของลายเซ็นดิจิตอลมีความแตกต่างจากลายเซ็นในชีวิตประจำวันดังนี้

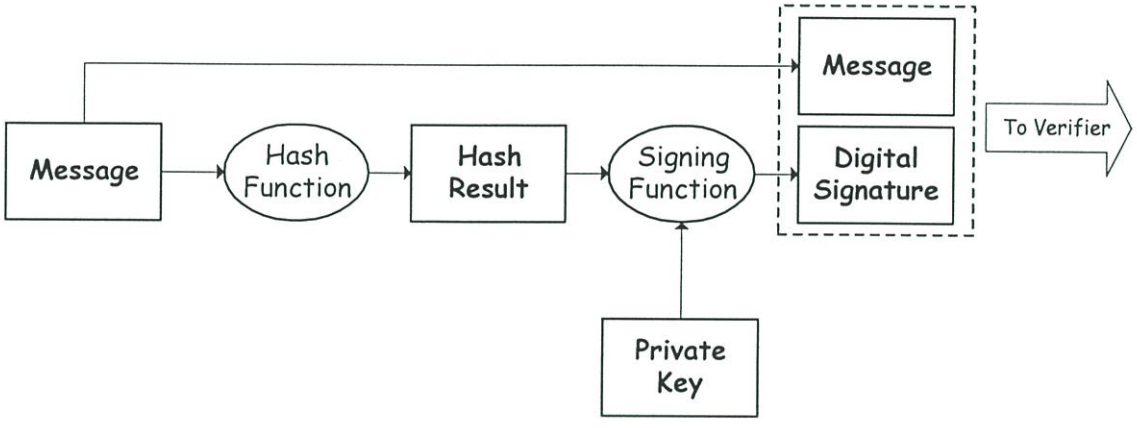
1. การเซ็นลายเซ็นดิจิตอลเกิดจากการใช้ข้อมูลตัวแทนของสื่อที่จะรับรองมาเข้ารหัสโดยใช้กุญแจลับของผู้เซ็น

2. ลายเซ็นดิจิตอลไม่ได้ถูกเซ็นลงในตัวสื่อดิจิตอล แต่จะถูกผนวกเข้ากับสื่อนั้น และประการที่สองการตรวจสอบลายเซ็นดิจิตอลนั้น ทำโดยใช้วิธีการที่เป็นที่รู้กันในสาธารณะ ต่างจากลายเซ็นในชีวิตประจำวันที่ใช้วิธีเปรียบเทียบกับลายเซ็นที่รับรอง เช่นการเปรียบเทียบลายเซ็นในสลิปซ์กับลายเซ็นที่อยู่หลังบัตรเครดิต

แบบแผนการใช้ลายเซ็นดิจิตอลแบ่งออกเป็น 2 ส่วนใหญ่ คือขั้นตอนการเซ็นและขั้นตอนการตรวจสอบลายเซ็น โดยมีพื้นฐานจากการประยุกต์เทคนิคการเข้าและถอดรหัสลับแบบใช้กุญแจสาธารณะ (Public-Key cryptography)

2.6.2 ขั้นตอนการสร้างลายเซ็นดิจิตอล

วิธีการสร้างลายเซ็นดิจิตอล ใช้แนวคิดในใช้ข้อมูลที่ต้องการส่ง นำมาสร้างลายเซ็นดิจิตอลเซ็นผนวกเข้ากับกุญแจเฉพาะตัวของผู้ทำการเซ็น สมาคมอเมริกันบาร์ (America Bar Association) ได้กำหนดมาตรฐานแล้วขั้นตอนในการใช้ลายเซ็นดิจิตอล [10] มีรายละเอียดสามารถแสดงได้ดังรูปที่ 2.2



รูปที่ 2.2 โครงสร้างมาตรฐานของกระบวนการสร้างลายเซ็นดิจิตอล

จากรูปที่ 2.2 การสร้างลายเซ็นดิจิตอลมีขั้นตอนดังต่อไปนี้

1. นำข้อความมาคำนวณแปลงเป็นข้อมูลตัวแทน ที่มีขนาดเล็กและมีเอกลักษณ์ (Unique) โดยผ่านฟังก์ชันแฮช (Hash function) ซึ่งเป็นฟังก์ชันแบบหนึ่งต่อหนึ่ง (One-to-One) และเป็นฟังก์ชันทางเดียว (One way) โดยจะทำให้ข้อมูลที่ได้ออกมาเป็นมีขนาดเล็กกว่าข้อความที่นำมาคำนวณ แต่ยังคงความแตกต่างของข้อความต้นฉบับไว้ได้ และไม่สามารถนำผลลัพธ์ที่ได้จากฟังก์ชันแฮชนี้มาดำเนินการย้อนกลับเพื่อให้ได้ข้อความต้นฉบับได้ ในทางปฏิบัติฟังก์ชันแฮชนี้จะแตกต่างกันไปขึ้นอยู่กับลักษณะประเภทของสื่อที่นำมาคำนวณ

2. นำผลลัพธ์ของฟังก์ชันแฮช (Hash result) จากขั้นตอนแรกมาเข้ารหัสโดยใช้วิธีการเข้ารหัสแบบกุญแจสาธารณะ หรือเรียกว่าฟังก์ชันการเซ็น (Signing function) โดยที่ผู้สร้างลายเซ็นจะใช้กุญแจส่วนตัวในการเข้ารหัส ซึ่งเป็นการรับรองว่ามีผู้สร้างลายเซ็นเพียงผู้เดียวเท่านั้นที่เซ็นได้ ผลลัพธ์ที่ได้ในขั้นนี้เรียกว่าลายเซ็นดิจิตอล

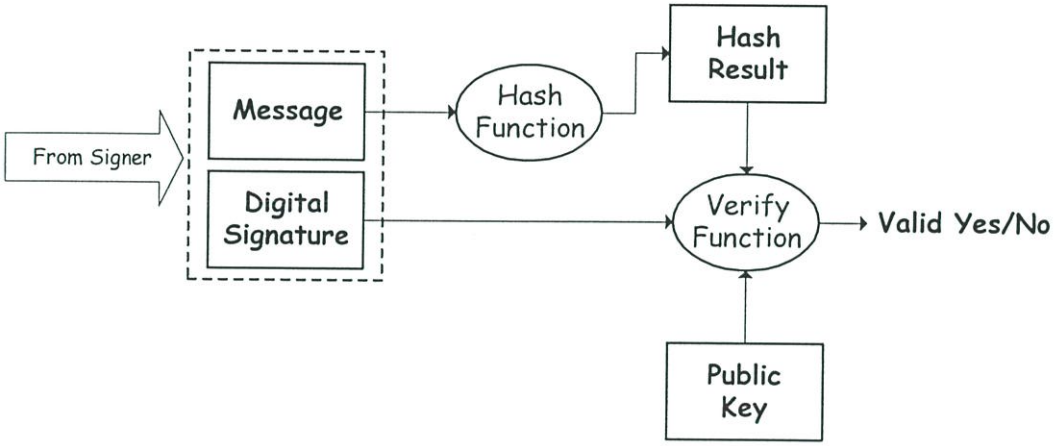
3. นำลายเซ็นดิจิตอลที่ได้มาแนบและส่งไปกับข้อความต้นฉบับ ซึ่งอาจจะส่งไปในแบบเฮดเดอร์ของไฟล์ หรือข้อมูลที่แนบไปกับจดหมายอิเล็คทรอนิค เพื่อใช้ยืนยันความถูกต้องของข่าวสาร โดยที่การส่งกุญแจสาธารณะที่ใช้ในการตรวจสอบลายเซ็นสามารถส่งไปพร้อมกับข้อมูลหรือ ส่งไปให้ผู้รับที่ตกลงกันไว้ก่อนก็ได้

2.6.3 ขั้นตอนการตรวจสอบลายเซ็นดิจิตอล

วิธีการตรวจสอบลายเซ็นดิจิตอล แสดงได้ดังรูปที่ 2.3 โดยที่กระบวนการตรวจสอบลายเซ็นดิจิตอล มีขั้นตอนดังต่อไปนี้

1. เมื่อผู้รับได้รับข้อความที่แนบลายเซ็นดิจิตอลมาแล้ว จะทำการแยกเอาลายเซ็นมาถอดรหัสโดยใช้กุญแจสาธารณะเพื่อให้ได้เป็นผลลัพธ์การแฮชของผู้สร้างลายเซ็น

2. ผู้รับนำข้อความที่ได้รับมาผ่านฟังก์ชันแฮช แบบเดียวกับที่ใช้ในการสร้างลายเซ็นจะทำให้ได้ผลลัพธ์การแฮชของข้อความที่ได้รับ



รูปที่ 2.3 โครงสร้างมาตรฐานของกระบวนการตรวจสอบลายเซ็นดิจิตอล

3. นำผลลัพธ์การแฮชจากข้อที่ 1 และ 2 มาเปรียบเทียบกัน หากว่าตรงกันจะสามารถยืนยันได้ว่าข้อมูลที่ผู้รับได้รับนั้นถูกส่งโดยผู้สร้างลายเซ็นจริง (Signer authentication) และเป็นข้อความที่ถูกต้อง (Message authentication) แต่หากว่าผลลัพธ์การแฮชทั้งคู่ไม่ตรงกันก็จะมีประเด็นสองประเด็นคือ เจ้าของกุญแจสาธารณะไม่ได้เป็นผู้สร้างลายเซ็นนี้ หรืออีกประเด็นคือข้อความที่ผู้รับได้รับไม่ใช่ข้อความต้นฉบับ มีการปลอมแปลงแก้ไข

จากวิธีการสร้างและตรวจสอบลายเซ็นดิจิตอลที่กล่าวมานี้ ในทางปฏิบัติแล้วจะต้องมีองค์กร หรือหน่วยงานที่ดูแลการขึ้นทะเบียนคู่กุญแจที่ใช้เข้าและถอดรหัส และมอบกุญแจส่วนตัว รวมถึงวิธีการสร้างลายเซ็นให้กับเจ้าของลายเซ็นแต่ละคน ซึ่งจะต้องเก็บไว้เป็นความลับ ส่วนกุญแจสาธารณะที่ใช้ในการตรวจสอบลายเซ็น และวิธีการทำฟังก์ชันแฮชและการตรวจสอบลายเซ็นจะถูกเผยแพร่ให้กับผู้ที่รับสื่อ ซึ่งในปัจจุบันได้มีบริษัทที่ได้รับอนุญาติให้สามารถดูแลจัดการ การรักษาความปลอดภัยของข้อมูลโดยใช้เทคนิคลายเซ็นดิจิตอล อย่างถูกต้องตามกฎหมายแล้วในอเมริกาและยุโรป

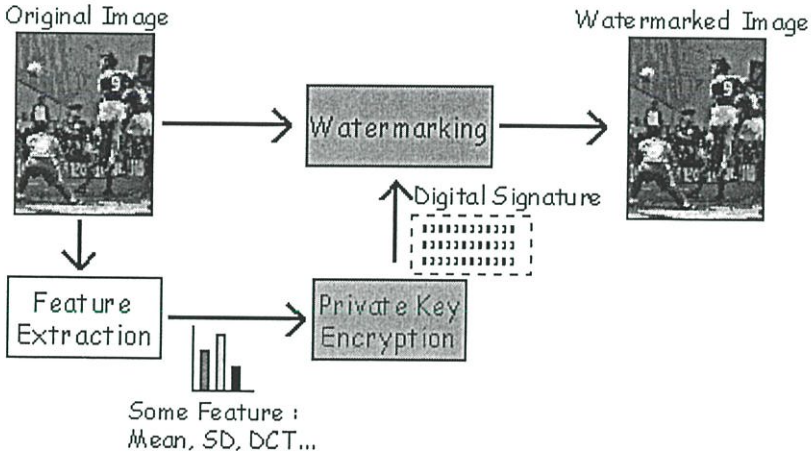
บทที่ 3
การตรวจสอบความถูกต้องของรูปภาพ

3.1 การประยุกต์ใช้ลายเซ็นดิจิตอลกับรูปภาพ

เนื่องลายเซ็นดิจิตอลเป็นมาตรฐานที่นิยมใช้ในการพิสูจน์ความเป็นเจ้าของ และความถูกต้องของเอกสารดิจิตอล อีกทั้งยังมีความน่าเชื่อถือสูง ดังนั้นขอบเขตและแนวทางในการพัฒนาวิธีการตรวจสอบความถูกต้องในงานวิจัยนี้ จึงได้ดำเนินไปตามแนวคิดของการใช้ลายเซ็นดิจิตอลเป็นพื้นฐาน โดยได้นำกระบวนการในการสร้างและตรวจสอบลายเซ็นดิจิตอลแบบทั่วไปมาประยุกต์ให้ใช้ได้กับข้อมูลรูปภาพ ระบบการตรวจสอบรูปภาพโดยใช้ลายเซ็นดิจิตอลนั้น แบ่งได้เป็นสองส่วนใหญ่ มีรายละเอียดดังนี้

3.1.1 การสร้างลายเซ็นดิจิตอลสำหรับรูปภาพ

กระบวนการสำหรับฝั่งของผู้ส่ง หรือเจ้าของรูปภาพ ดังรูปที่ 3.1 มีขั้นตอนหลัก 3 ขั้นตอนดังต่อไปนี้



รูปที่ 3.1 ขั้นตอนการสร้างลายเซ็นดิจิตอลร่วมกับการซ่อนลายน้ำในรูปภาพ

1. การแยกลักษณะเฉพาะของรูปภาพ (Feature extraction) เป็นการสร้างผลลัพธ์การแฮช (Hash result) จากรูปภาพต้นฉบับ ซึ่งฟังก์ชันแฮชสำหรับรูปภาพในที่นี้ จะเป็นการดึงลักษณะเฉพาะของรูปภาพออกมา เช่นความเข้มเฉลี่ยของภาพ ค่าความแปรปรวนของภาพเป็นต้น ซึ่งจะทำให้ได้ข้อมูลจำนวนหนึ่ง ที่จะเป็นตัวแทนของภาพต้นฉบับ และคงเอกลักษณ์ของภาพต้นฉบับอยู่แต่มีปริมาณน้อยพอที่จะซ่อนเข้าไปในภาพได้ โดยที่ไม่ทำให้ภาพนั้นด้อยคุณภาพลง

2. การสร้างลายเซ็นดิจิตอล (Digital signature signing) เป็นการนำลักษณะเฉพาะที่แยกได้ ไปเข้ารหัสลับ (Encryption) ด้วยวิธีการเข้ารหัสแบบ RSA ซึ่งเป็นพื้นฐานของการสร้างลายเซ็นดิจิตอล โดยใช้กุญแจส่วนตัวของผู้สร้างลายเซ็นในการเข้ารหัส เพื่อให้เป็นลายเซ็นที่สร้างได้เฉพาะเจ้าของกุญแจ ผลลัพธ์ที่ได้ในขั้นนี้จะได้เป็นลายเซ็นดิจิตอล ที่มีข้อมูลลักษณะเฉพาะของรูปภาพและเอกลักษณ์ของตัวผู้เซ็นเองบรรจุอยู่

3. การซ่อนลายน้ำดิจิตอล (Watermarking) เป็นการนำลายเซ็นดิจิตอลที่ได้ มาซ่อนกลับเข้าไปในรูปภาพต้นฉบับ ให้กระทบกระเทือนต่อคุณภาพของภาพต้นฉบับน้อยที่สุด ซึ่งจะทำให้ยากต่อการสังเกตพบลายเซ็นดิจิตอล และมีความทนทานต่อกระบวนการแก้ไขรูปภาพพื้นฐาน โดยการประยุกต์ใช้เทคนิคแบบสเปรดสเปคตรัม ในการซ่อนข้อมูลดิจิตอล

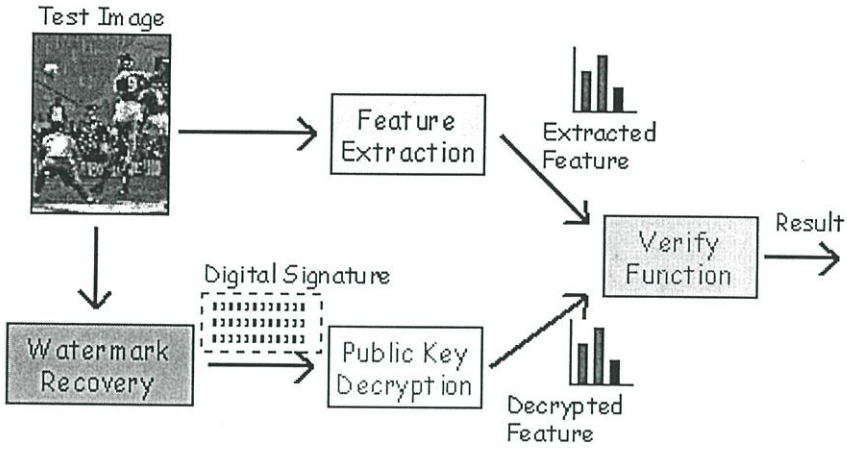
3.1.2 การค้นคืนและการตรวจสอบลายน้ำดิจิตอลในรูปภาพ

เป็นกระบวนการสำหรับฝั่งของผู้รับ เมื่อต้องการตรวจสอบความถูกต้องของรูปภาพ มีขั้นตอนหลัก 3 ขั้นตอนดังต่อไปนี้

1. การค้นคืนลายน้ำดิจิตอล (Watermark recovery) ขั้นตอนนี้เป็นการค้นหาตำแหน่งของลายน้ำที่ซ่อนอยู่ และแยกข้อมูลลายน้ำออกมาจากรูปภาพ เป็นการประยุกต์ใช้วิธีการทำคอร์รีเลชันร่วมกับเทคนิคการค้นคืนลายน้ำดิจิตอลแบบสเปรดสเปคตรัม ซึ่งจะได้ผลลัพธ์เป็นลายเซ็นดิจิตอลที่ซ่อนมากับรูปภาพ [16]

2. การถอดรหัสลายเซ็นดิจิตอล (Decryption) เป็นการนำลายเซ็นดิจิตอลมาถอดรหัสลับด้วยกุญแจสาธารณะที่เป็นคู่กุญแจของเจ้าของลายเซ็น ซึ่งจะได้เป็นลักษณะเฉพาะของรูปภาพที่เป็นต้นฉบับในการสร้างลายเซ็นดิจิตอล

3. การดึงลักษณะเฉพาะของรูปภาพที่ทดสอบ (Feature extraction) ภาพที่นำมาทดสอบจะถูกแยกเอาลักษณะเฉพาะออกมา โดยใช้วิธีเดียวกันกับขั้นตอนการสร้างลายเซ็นดิจิตอล การตรวจสอบ (Verification) ในขั้นนี้ ลักษณะเฉพาะที่ได้จากทั้งสองวิธี จะถูกนำมาเปรียบเทียบกัน ซึ่งผลลัพธ์ที่ได้จะเป็นค่าความเหมือน และตำแหน่งบริเวณที่ภาพถูกเปลี่ยนแปลงแก้ไข โดยขั้นตอนทั้งหมดที่กล่าวนี้ แสดงดังรูปที่ 3.2



รูปที่ 3.2 ขั้นตอนการตรวจสอบลายเซ็นดิจิตอลในรูปภาพ

3.2 การสร้างลายเซ็นดิจิตอลจากรูปภาพ

ในหัวข้อนี้เป็นรายละเอียดของขั้นตอนการสร้างลายเซ็นดิจิตอลจากรูปภาพ ซึ่งสามารถแบ่งได้เป็น 2 ส่วนหลักได้แก่ การแยกเอาลักษณะเฉพาะของรูปภาพและการเข้ารหัสลับ โดยใช้กุญแจส่วนตัวของผู้สร้าง ในขั้นแรกจะเป็นการอธิบายวิธีการสร้างลักษณะเฉพาะของรูปภาพ ซึ่งงานวิจัยนี้ ได้สร้างข้อมูลที่เรียกว่า ลักษณะเฉพาะของรูปภาพแบบค่าสัมพัทธ์ระหว่างบล็อก มีรายละเอียดดังนี้

3.2.1 ลักษณะเฉพาะแบบสัมพัทธ์ระหว่างบล็อกข้างเคียง

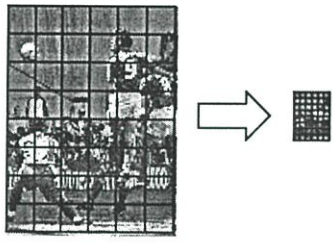
ลักษณะเฉพาะแบบสัมพัทธ์ระหว่างบล็อกข้างเคียงนี้ เป็นลักษณะเฉพาะของรูปภาพแบบใหม่ ที่ใช้ในการสร้างลายเซ็นดิจิตอลในงานวิจัย โดยใช้พื้นฐานการเขียนรหัสแบบบล็อก (Block coding) คือลักษณะเฉพาะแต่ละค่าจะได้มาจากการประมวลผลรูปภาพที่แบ่งเป็นบล็อก ลักษณะเฉพาะแบบค่าสัมพัทธ์ระหว่างบล็อก จะมีคุณสมบัติในการตรวจสอบการแก้ไขรูปภาพแบบแยกส่วนเป็นพื้นที่ตำแหน่งต่างๆ ของภาพได้ การใช้ค่าสัมพัทธ์ทำให้ตำแหน่งของบล็อกมีผลต่อการสร้างลักษณะเฉพาะ และการเปลี่ยนแปลงความเข้มความสว่างของบล็อกทุกบล็อก จะไม่ทำให้ลักษณะเฉพาะเปลี่ยนแปลง ซึ่งทำได้โดยเปรียบเทียบลักษณะเฉพาะของบล็อกที่พิจารณา กับบล็อกข้างเคียงในภาพ โดยกำหนดให้ รูปภาพดิจิตอลขนาด $M \times N$ จุดภาพ แทนด้วย $g(x, y) \in 0 \ldots 255$ โดยที่ $x \in 0,\ldots,M\text{-}1, y \in 0,\ldots,N\text{-}1$ โดยวิธีการแยกลักษณะเฉพาะมีขั้นตอน 6 ขั้นตอนดังนี้

1. แบ่ง $g(x, y)$ ออกเป็นบล็อกสี่เหลี่ยมจตุรัสขนาด B×B ที่ไม่ซ้อนทับกัน ให้แต่ละบล็อกแทนด้วย $g_{i,k}(m, n)$ เมื่อ $i \in \{0 \ldots P\text{-}1\}$ (กำหนดให้ $P = \lfloor M/B \rfloor$) และ $k \in \{0 \ldots Q\text{-}1\}$

(กำหนดให้ Q = $\lfloor N/B \rfloor$) จากนั้นให้คำนวณหาค่าเฉลี่ย (Mean) ของระดับความเข้มความสว่างสำหรับแต่ละบล็อก $g_{i,k}$ โดยใช้สมการที่ 3.1

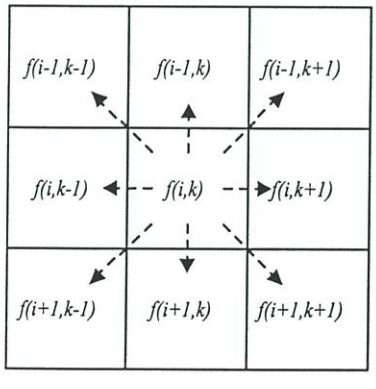
$$f(i,k) = \frac{\sum_{m=0}^{B-1}\sum_{n=0}^{B-1} g_{i,k}(m,n)}{B \times B} \qquad (3.1)$$

ลักษณะเฉพาะแบบค่าเฉลี่ยความเข้มของบล็อก แทนด้วย $f(i, k)$ โดยมีนิยามดังสมการที่ 3.1 คำนวณค่า $f(i,j)$ จากสมการที่ 3.1 ทุกๆ บล็อก i, k จะได้เป็นลักษณะเฉพาะ ที่จะเป็นตัวแทนของรูปภาพ ซึ่งขนาดของ f คือ $P \times Q$ จุดภาพ แสดงได้ดังรูปที่ 3.3



รูปที่ 3.3 ลักษณะค่าเฉลี่ยความเข้มความสว่างแบบบล็อกของรูปภาพ

2. หาค่าสัมพัทธ์ระหว่างค่า $f(i, k)$ กับ $f(i+d_1 , k+d_2)$ ของบล็อกข้างเคียง โดยที่ $d_1 , d_2 \in \{-1, 0, 1\}$ แต่ละบล็อกจะมีความสัมพันธ์กับบล็อกที่อยู่ข้างเคียงดังรูปที่ 3.4 โดยที่ลูกศรทั้งแปดแทนรูปแบบความสัมพันธ์ที่เป็นไปได้



รูปที่ 3.4 รูปแบบความสัมพันธ์ระหว่างบล็อกข้างเคียงที่เป็นไปได้ของบล็อก i, k

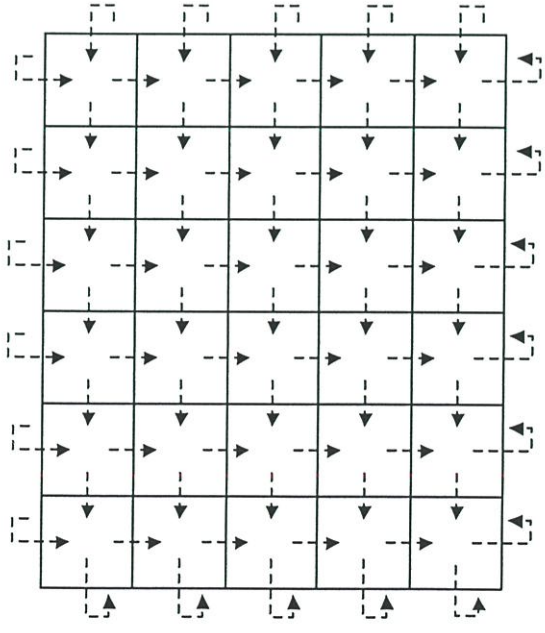
3. ลักษณะเฉพาะแบบสัมพัทธ์แทนด้วยฟังก์ชัน $f'(i, k, d_1, d_2)$ โดยกำหนดให้ MAX_f คือค่าสูงสุดที่เป็นไปได้ของ $f(i, k)$ สำหรับภาพแบบ 8 bits/pixel แล้วจะมีค่า MAX_f เท่ากับ 255 ซึ่งนิยามลักษณะเฉพาะแบบสัมพัทธ์ได้ดังสมการที่ 3.2

$$f'(i,k,d_1,d_2) = \frac{f(i,k) - f(i+d_1,k+d_2)}{MAX_f} \qquad (3.2)$$

โดยที่ค่าของ $f'(i, k, d_1, d_2)$ เป็นสมาชิกของจำนวนจริงมีค่าตั้งแต่ –1 ถึง 1 และเพื่อให้ความสัมพันธ์ของบล็อกข้างเคียง มีลักษณะเป็นวงวนในกรณีที่เป็นบล็อกที่อยู่รอบนอกสุด จะใช้หลักในการพิจารณาคู่ความสัมพันธ์ ดังนี้

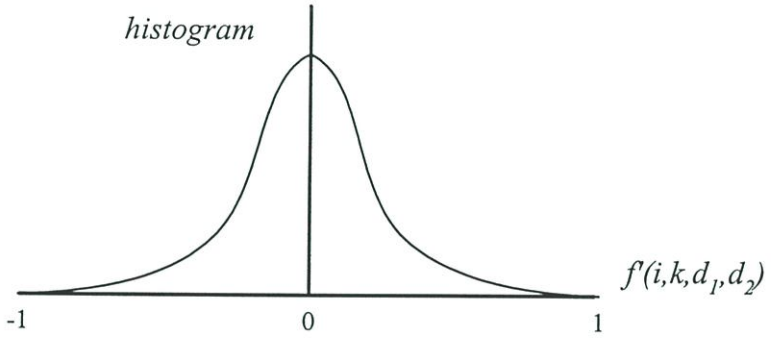
- ในกรณีที่ $i+d_1$ มีค่ามากกว่า P ให้เป็นค่า 0 และถ้าหากว่า $i+d_1$ มีค่าน้อยกว่า 0 ให้ปรับเป็นค่า P
- ในกรณีที่ $k+d_2$ มีค่ามากกว่า Q ให้เป็นค่า 0 และถ้าหากว่า $k+d_2$ มีค่าน้อยกว่า 0 ให้ปรับเป็นค่า Q

4. ในทางปฏิบัติ เราไม่จำเป็นต้องแทนความสัมพันธ์ทุกด้าน เพราะการแบ่งบล็อกเป็นแบบสมมาตร ซึ่งจะมีคู่ความสัมพันธ์ที่ตรงข้ามกัน เช่นด้านบนกับด้านล่าง ด้านซ้ายกับด้านขวา ดังนั้นจะมี 4 คู่ความสัมพันธ์ แต่เราจะเลือกใช้เพียงสองคู่เท่านั้น เพื่อลดความสัมพัทธ์ที่ซ้ำซ้อนและปริมาณข้อมูล ผู้วิจัยเลือกใช้ความสัมพันธ์ทางด้านขวาและด้านล่าง ซึ่งแทนด้วยฟังก์ชัน $f'(i, k, 0,1)$ และ $f'(i, k, 1,0)$ ตามลำดับ แสดงได้ด้วยลูกศรเส้นประดังรูปที่ 3.5



รูปที่ 3.5 ตัวอย่างความสัมพันธ์ระหว่างบล็อกข้างเคียงแบบ $f'(i, k, 0,1)$ และแบบ $f'(i, k, 1,0)$

5. ผลลัพธ์ของลักษณะเฉพาะแบบสัมพัทธ์ข้างต้นจะอยู่ในรูปของจำนวนจริง เพื่อให้สามารถเข้ารหัสและซ่อนในรูปภาพแบบดิจิตอลได้ ดังนั้นจึงมีการแทนค่า $f'(i, k, d_1, d_2)$ ด้วยข้อมูลขนาด 4 บิต โดยกำหนดให้ $E(x)$ เป็นฟังก์ชันการแปลงจำนวนจริง x ที่มีค่าตั้งแต่ –1 ถึง 1 ให้อยู่ในรูปของจำนวนเต็ม 16 ระดับที่มีค่าตั้งแต่ 0 ถึง 15 ซึ่งจะแทนได้ด้วยจำนวนเต็มฐานสอง 4 บิต ดังแสดงในรูปที่ 3.6

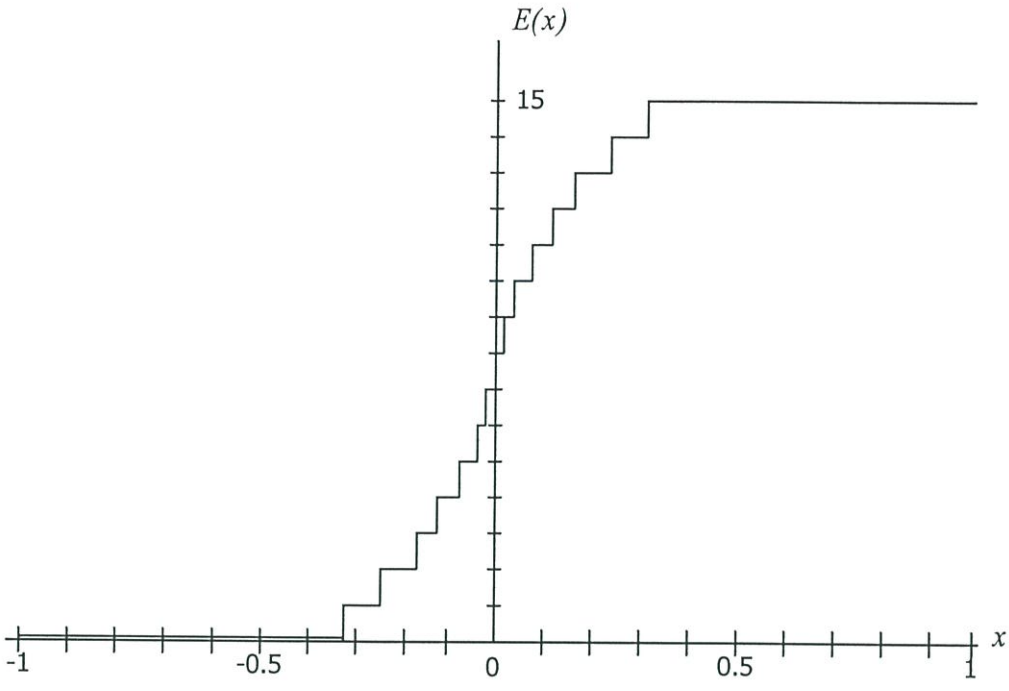


รูปที่ 3.6 เส้นกราฟแสดงการแจกแจงของค่า $f'(i, k, d_1, d_2)$ สำหรับภาพถ่ายดิจิตอล

จากรูปที่ 3.6 แสดงการแจกแจงของค่า $f'(i, k, d_1, d_2)$ (ได้จากสถิติในการทดลอง) สำหรับรูปภาพดิจิตอล จะพบว่าค่า $f'(i, k, d_1, d_2)$ ส่วนใหญ่จะอยู่ในช่วง –0.2 ถึง 0.2 กราฟการแจกแจงจะมีลักษณะเป็นรูประฆังคว่ำ ดังนั้นเพื่อปรับให้ผลลัพธ์การเข้ารหัสมีการแจกแจงแบบปกติ ระดับค่า Threshold ที่ใช้ในการแปลงจะมีแนวโน้มลักษณะเป็นแบบล็อกการิทึม (logarithm) ดังแสดงในตารางที่ 3.1 และรูปที่ 3.7

ตารางที่ 3.1 ระดับค่า Threshold สำหรับการแปลงค่า $f'(i, k, d_1, d_2)$

$x = f'(i, k, d_1, d_2)$	*Coding E(x)*
$-1 \le x \le -0.32$	0000
$-0.32 < x \le -0.24$	0001
$-0.24 < x \le -0.16$	0010
$-0.16 < x \le -0.12$	0011
$-0.12 < x \le -0.08$	0100
$-0.08 < x \le -0.04$	0101
$-0.04 < x \le -0.02$	0110
$-0.02 < x \le 0.00$	0111
$0.00 < x \le 0.02$	1000
$0.02 < x \le 0.04$	1001
$0.04 < x \le 0.08$	1010
$0.08 < x \le 0.12$	1011
$0.12 < x \le 0.16$	1100
$0.16 < x \le 0.24$	1101
$0.24 < x \le 0.32$	1110
$0.32 < x \le 1.00$	1111



รูปที่ 3.7 เส้นกราฟแสดงการแปลงค่าของ $E(x)$ แบบขั้นบันได

ผลลัพธ์ที่ได้ในขั้นนี้ ในแต่ละบล็อกจะได้ลักษณะเฉพาะเป็นจำนวนเต็มขนาด 4 บิต 2 ชุด ซึ่งคือความสัมพันธ์ 2 ด้าน รวมมีขนาด 8 บิต ต่อข้อมูล 1 บล็อก

6. ขั้นตอนสุดท้ายในการสร้างลักษณะเฉพาะ คือการเพิ่มข้อมูลตำแหน่งบล็อกลงไป โดยทำการเลื่อนบิตข้อมูลที่ได้จากการแปลง $E(x)$ ในข้อ 5 ไปเท่ากับตำแหน่งบล็อกในแนวคอลัมน์รวมกับแนวแถว ดังสมการที่ (3.3)

$$\text{Feature}\ (i,\ k) = \text{BitRotate}(E(x)\ ,\ i+k\ ) \qquad (3.3)$$

ตัวอย่างเช่น ลักษณะเฉพาะ $E(f'(i,\ k,\ 0,1))$, $E(f'(i,\ k,\ 1,0))$ เท่ากับ 1001 1010 โดยที่ $i = 3$ และ $k=2$ จะถูกเลื่อนไปทางขวาแบบหมุน 3+2 = 5 ตำแหน่ง ได้ผลลัพธ์ เป็น 1101 0100

การเพิ่มข้อมูลตำแหน่งบล็อกลงไปนี้ เพื่อให้สามารถตรวจสอบการแก้ไขรูปภาพแบบสลับตำแหน่งบริเวณพื้นที่ของรูปภาพได้ ลักษณะเฉพาะซึ่งเป็นตัวแทนขนาดเล็กของรูปภาพนี้จะถูกนำไปเข้ารหัสลับในขั้นตอนต่อไป

3.2.2 การเข้ารหัสลับแบบ RSA Public-key Encryption

การเข้ารหัสแบบ RSA ได้ถูกนำมาประยุกต์เพื่อใช้ในการเข้ารหัสลักษณะเฉพาะ โดยในการทดลองสำหรับงานวิจัยนี้จะใช้กุญแจที่มีขนาด 16 บิต ด้วยเหตุผล 2 ประการ ประการแรกคือเป็นขนาดข้อมูลที่สามารถเขียนโปรแกรมคำนวณได้ง่ายโดยใช้ตัวแปรจำนวนเต็มในการแทน และง่ายต่อการประยุกต์ใช้กับลักษณะเฉพาะ ในที่นี้มีขนาดเป็นจำนวนเท่าของ 4 บิต และก่อนที่จะทำขั้นตอนการเข้ารหัสนี้ เราจะต้องได้คู่กุญแจสาธารณะมาก่อน โดยจะต้องมีคุณสมบัติตามข้อกำหนดของวิธีการแบบ RSA

ขั้นตอนในการเข้ารหัสมีดังนี้ [15]

1. สิ่งที่ต้องใช้ในการเข้ารหัสประกอบไปด้วย ข้อมูลของลักษณะเฉพาะ(f) กุญแจส่วนตัวสำหรับเข้ารหัส (d) และค่าโมดูโล (m) ซึ่งเป็นตัวหารเอาเศษในขั้นตอนการคำนวณ

2. แบ่งข้อมูลลักษณะเฉพาะออกเป็นกลุ่มโดยแต่ละกลุ่มมีขนาดเท่ากับขนาดของกุญแจคือ 16 บิต ในที่นี้บล็อกหนึ่งบล็อกจะมีข้อมูลลักษณะเฉพาะ 8 บิต ดังนั้นจะแบ่งข้อมูลเป็นกลุ่มละ 2 บล็อก สำหรับบล็อกที่เหลือเศษจะแทนบิตที่เหลือด้วย 0 ทำการเข้ารหัสเป็นกลุ่มๆ ไป

3. ในแต่ละกลุ่ม ให้ทำการเข้ารหัสข้อมูลโดยใช้วิธีการแบบ RSA โดยมีขั้นตอนดังอัลกอริทึมในรูปที่ 3.8 ฟังก์ชันนี้ใช้ทั้งในขั้นตอนการเข้ารหัสและการถอดรหัส ซึ่งมีอัลกอริทึมเหมือนกัน แต่สิ่งที่แตกต่างกันระหว่างการใช้ฟังก์ชันนี้คือ ข้อมูลที่ส่งผ่านตัวแปร *Plain* ซึ่งจะเป็นข้อมูลที่ต้องการเข้ารหัสหรือถอดรหัส และตัวแปร ***Key*** ซึ่งแทนกุญแจส่วนตัว หรือกุญแจสาธารณะสำหรับใช้ในการเข้าหรือถอดรหัสตามลำดับ

4. นำข้อมูลที่เข้ารหัสแล้วในแต่ละกลุ่มมารวมกันอีกครั้ง ซึ่งเรียกว่าลายเซ็นดิจิตอล ข้อมูลลายเซ็นนี้จะถูกนำไปรวมเข้ากับรูปภาพโดยวิธีการที่เรียกว่า การซ่อนลายน้ำดิจิตอล ซึ่งจะกล่าวถึงในหัวข้อต่อไป

```
% rsa : Encryption/Decryption Function (RSA Algorithm)
%   Cipher = rsa(Plain, Key, Modulo)
%     is RSA encryption/decryption for Plain text with Key and Modulo
%   Cipher : MxN doubles : Cipher Text
%   Plain  : MxN doubles : Plain Text or Message
%   Key    : Positive Integer    : Key for encryption or decryption
%   Modulo : Positive Integer    : Modulo

function Cipher = rsa(Plain, Key, Modulo)
   Cipher = ones(size(Message));
   KeyBinary = dec2bin(Key);
   KeyBitLength = length(KeyBinary);
   for index = 1:KeyBitLength,
      Cipher = mod(Cipher.*Cipher, Modulo);
      if KeyBinary(index) == '1'
         Cipher = mod(Cipher.*Message, Modulo);
      end; % if
   end; % for
```

รูปที่ 3.8 อัลกอริทึมที่ทำการเข้าและถอดรหัสโดยใช้วิธีการแบบ RSA

3.3 การซ่อนข้อมูลลายเซ็นดิจิตอลลงในรูปภาพ

การประยุกต์ใช้ลายเซ็นดิจิตอลเพื่อตรวจสอบความถูกต้องของรูปภาพ มีส่วนสำคัญอีกส่วนหนึ่งได้แก่ กระบวนการเซ็นลายเซ็นดิจิตอล เนื่องจากความจำเป็นของข้อมูลรูปภาพที่จะต้องซ่อนลายเซ็นดิจิตอลรวมเข้ากับตัวสื่อ การซ่อนข้อมูลลายเซ็นดิจิตอลลงในรูปภาพ หรือที่เรียกว่าการเซ็นหรือการสร้าง/ซ่อนลายน้ำดิจิตอล (Digital watermarking) โดยใช้พื้นฐานมาจากเทคนิคการซ่อนข้อมูลแบบสเปรดสเปคตรัม [11] สามารถแบ่งขั้นตอนย่อย ออกเป็น 4 ขั้นตอนดังนี้

3.3.1 การกระจายบิตข้อมูล

กระบวนการกระจายบิตข้อมูล (Data bit spreading) ลายเซ็นดิจิตอลที่ถูกสร้างในหัวข้อที่ 3.2 จะถูกแปลงให้อยู่ในรูปสายลำดับของค่าไบนารี โดยที่แปลงจากจำนวนฐานสอง ให้ค่า 0 แปลงเป็น –1 และค่า 1 แปลงเป็น +1 แทนด้วยสัญลักษณ์ $w_{i,\,k,\,b} \in \{+1, -1\}$, $i \in \{0 \ldots P\text{-}1\}$, $k \in \{0 \ldots Q\text{-}1\}$ และ $b \in \{0 \ldots 7\}$ โดยที่ ค่า b จะเป็นตัวระบุตำแหน่งของบิต

ตัวอย่าง ค่าฐานสองของลายเซ็นดิจิตอล

1 0 1 1 0 1 0 1 1 1 0 0 0 1 0 0

แปลงเป็น

+1 -1 +1 +1 -1 +1 -1 +1 +1 +1 -1 -1 -1 +1 -1 -1

การกระจายบิตข้อมูลจะทำให้ข้อมูลแต่ละบิตมีความซ้ำซ้อน มีวัตถุประสงค์เพื่อเพิ่มความทนทานต่อการถูกแก้ไขทำลาย โดยให้ค่าระดับความซ้ำซ้อนแทนด้วย cr ซึ่งในที่นี้ค่า cr จะขึ้นอยู่กับขนาดของสื่อพาหะที่ใช้ซ่อนข้อมูล มีสูตรในการคำนวณหาค่า cr ดังนี้

cr = size of host signal / size of signature

การกระจายบิตข้อมูลซึ่งใช้ค่า cr นี้มีแนวทาง 2 แบบที่มีคุณสมบัติต่างกันดังนี้

1. การทำซ้ำทีละบิต วิธีนี้แต่ละบิตจะถูกกระจายซ้ำๆ กัน cr บิตโดยเรียงติดกัน การทำซ้ำในรูปแบบนี้จะทำให้ข้อมูลมีความทนทานต่อการแก้ไขแบบสุ่ม เนื่องจากแต่ละบิตข้อมูลจะถูกกระจายเป็นกลุ่มที่พื้นที่ติดต่อกัน สัญญาณรบกวนที่กระจายเป็นบริเวณกว้าง จะมีผลกระทบต่อบิตในแต่ละกลุ่มเพียงเล็กน้อย โดยที่ไม่กระทบต่อค่าความซ้ำโดยรวมของแต่ละบิตมากนัก ตัวอย่างเช่น

Signature = 1 0 0 1 0 1 1 0, cr = 4

sb = 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0

2. การทำซ้ำเป็นกลุ่ม ข้อมูลจะถูกทำซ้ำกันเป็นกลุ่มบิต จำนวน cr ครั้ง วิธีนี้จะทำให้ข้อมูลมีความทนทานต่อการแก้ไขที่เกิดขึ้นกระจายเป็นบริเวณแคบ เฉพาะกลุ่ม เนื่องจากบิตข้อมูลซ้ำของแต่ละบิตถูกกระจายไปทั่วทั้งพื้นที่ของสื่อพาหะ การแก้ไขที่เกิดขึ้นเฉพาะที่หรือเฉพาะกลุ่มก็จะไม่กระทบกระเทือนข้อมูลแต่ละบิตมากนัก ตัวอย่างเช่น

Signature = 1 0 0 1 0 1 1 0, cr = 4

sb = 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0

สำหรับการนำมาใช้งานในงานวิจัยนี้จะใช้การกระจายแบบที่ 2 คือกระจายเป็นกลุ่มเพราะวัตถุประสงค์หลักคือ เพื่อป้องกันการแก้ไขรูปภาพที่เกิดขึ้นเฉพาะบริเวณ ซึ่งวิธีนี้จะทำให้รักษาข้อมูลที่ซ่อนไว้ได้ดีกว่าวิธีแรก แสดงตัวอย่างวิธีการกระจายบิต $w_{i,\,k,1}$ ดังรูปที่ 3.9

1	1	0	0	1
1	0	1	1	0
0	1	0	0	1
1	1	1	1	0
1	0	1	0	1

1	1	0	0	1	1	1	0	0	1	1	1	0	0	1
1	0	1	1	0	1	0	1	1	0	1	0	1	1	0
0	1	0	0	1	0	1	0	0	1	0	1	0	0	1
1	1	1	1	0	1	1	1	1	0	1	1	1	1	0
1	0	1	0	1	1	0	1	0	1	1	0	1	0	1
1	1	0	0	1	1	1	0	0	1	1	1	0	0	1
1	0	1	1	0	1	0	1	1	0	1	0	1	1	0
0	1	0	0	1	0	1	0	0	1	0	1	0	0	1
1	1	1	1	0	1	1	1	1	0	1	1	1	1	0
1	0	1	0	1	1	0	1	0	1	1	0	1	0	1

รูปที่ 3.9 บิตที่ถูกกระจาย (Spreading Code)

ข้อมูลบิตของลักษณะเฉพาะ จะถูกแบ่งออกเป็นกลุ่มย่อย แต่ละกลุ่มมีขนาดเท่ากับ 4 บิต โดยที่ข้อมูลนี้จะถูกซ่อนไว้ในรูปภาพใช้พื้นที่เท่ากับบล็อก ดังนั้นค่า cr ของบิตที่จะต้องทำซ้ำจึงมีค่าเท่ากับ $cr = \lfloor BlockSizes / 4 \rfloor$

3.3.2 สัญญาณรบกวนเทียม

สัญญาณรบกวนเทียม (Psudo noise) คือ ข้อมูลสายลำดับของค่าไบนารี {+1,-1} เป็นข้อมูลสุ่มที่มีการแจกแจงความถี่แบบปกติ แทนด้วย $p_{x,\ y} \in \{+1,\ -1\}$, $x \in \{1...M-1\}$, $y \in \{1...N-1\}$ โดยที่ค่าเฉลี่ยของ $p_{x,y}$ มีค่าประมาณ 0

สัญญาณรบกวนเทียมนี้ เกิดจากค่าตั้งต้นในการสร้างลำดับการสุ่ม ซึ่งผู้สร้างจะต้องเก็บค่าไว้เพื่อใช้ลำดับการสุ่มเดียวกันนี้ในการตรวจหาลายน้ำและตรวจสอบอีกครั้ง ดังรูปที่ 3.10

```
-1  -1   1   1   1  -1   1   1   1   1  -1   1   1   1  -1
 1  -1   1   1   1   1  -1   1  -1  -1  -1  -1   1   1  -1
-1   1   1  -1  -1  -1  -1   1  -1  -1   1   1  -1  -1  -1
-1   1   1   1  -1   1   1  -1   1  -1   1   1   1   1   1
-1   1   1  -1  -1  -1  -1   1   1   1  -1   1  -1   1  -1
 1  -1   1  -1   1   1  -1  -1  -1   1   1  -1   1   1  -1
-1  -1  -1   1   1   1  -1   1   1   1  -1  -1   1   1  -1
-1   1   1  -1  -1  -1   1  -1   1   1  -1   1  -1  -1   1
 1   1   1  -1  -1   1  -1   1  -1   1  -1  -1   1  -1   1
 1   1  -1  -1   1  -1   1  -1  -1  -1  -1   1  -1  -1   1
```

รูปที่ 3.10 ตัวอย่างสัญญาณรบกวนเทียม $p_{x,y}$ ขนาด 10 x 15 Pixels

3.3.3 การซ่อนลายน้ำดิจิตอล

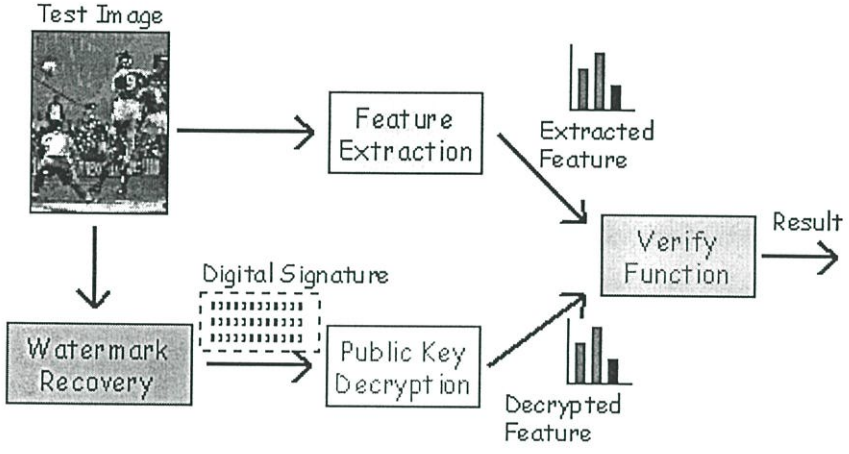
ขั้นตอนนี้เป็นการสร้างข้อมูลลายน้ำจากการรวมกันของข้อมูลลายเซ็นดิจิตอลกับสัญญาณรบกวนเทียม ลายเซ็นดิจิตอลที่ถูกกระจายบิตข้อมูล จะถูกนำมาคูณแบบโมดูเลตกับสัญญาณรบกวนเทียม โดยใช้สมการที่ 3.4

$$g(x,y)' = g(x,y) + \alpha_b \cdot w_{i,\ k,\ b} \cdot p_{x,\ y} \qquad (3.4)$$

โดยที่ค่า α_b ในที่นี้ เป็นค่าสัมประสิทธ์ในการกำหนดแอมปลิจูดของลายน้ำ มีค่าตั้งแต่ 2 ถึง 5 ซึ่งเป็นช่วงที่ไม่ทำให้ลายน้ำเด่นชัดจนสังเกตได้ง่าย และมีความทนทานต่อการเปลี่ยนแปลงแก้ไขได้ดี ค่า α_b นี้ จะมีค่าขึ้นกับค่า b เนื่องจากค่า b แทนตำแหน่งบิตของค่าลักษณะเฉพาะในแต่ละบล็อก ค่า α สูงสุดสำหรับบิตตำแหน่งที่มีค่ามากที่สุดจะเท่ากับ 6 ส่วนบิตที่สำคัญรองลงมาจะมีค่า 5, 4 และ 3 ตามลำดับ ซึ่งวิธีการนี้จะทำให้บิตของลักษณะเฉพาะทั้ง 4 บิต ได้รับการป้องกันที่เหมาะสมกับความสำคัญของบิต

3.4 การค้นคืนลายเซ็นดิจิตอลจากรูปภาพ

กระบวนการนี้เป็นการตรวจสอบว่ามีข้อมูลลายน้ำดิจิตอลซ่อนอยู่ในรูปภาพหรือไม่ และทำการแยกเอาข้อมูลนั้นออกมาจากรูปภาพ ในการนี้ผู้รับจะต้องใช้รูปแบบสัญญาณรบกวนเทียมที่ใช้ในการสร้างลายน้ำดิจิตอล นำมาทำการตรวจหาลายน้ำดิจิตอล โดยการโมดูเลตสัญญาณรบกวนนี้ กลับเข้าไปในรูปภาพอีกครั้ง และสร้างลักษณะเฉพาะของรูปภาพขึ้นมาใหม่ เพื่อใช้เทียบกับลักษณะเฉพาะที่ได้จากการถอดรหัสลายเซ็นดิจิตอลมีขั้นตอนแสดงดังรูปที่ 3.11



รูปที่ 3.11 ขั้นตอนการตรวจสอบลายเซ็นดิจิตอลในรูปภาพ

3.4.1 การตรวจหาลายน้ำดิจิตอลในรูปภาพ

เทคนิคในการตรวจหาลายน้ำนี้ใช้หลักการของการหาค่าคอร์รีเลชัน (Correlation) ของสัญญาณรบกวนเทียมกับข้อมูลรูปภาพ หากว่ารูปภาพมีลายน้ำที่เกิดจากสัญญาณรบกวนเทียมที่ใช้ทดสอบจริง ค่าคอร์รีเลชันของภาพนี้จะมีค่าสูงกว่าปกติ สามารถคำนวณโดยใช้สมการที่ 3.5

$$r = \frac{\sum (x - \bar{x})(y - \bar{y})}{\sqrt{\sum (x - \bar{x})^2 \sum (y - \bar{y})^2}} \qquad (3.5)$$

สมการที่ 3.5 แสดงสูตรในการคำนวณหาค่าคอร์รีเลชัน ระหว่างสัญญาณรบกวนเทียมและรูปภาพที่ผู้รับได้รับ โดยให้ r คือค่าคอร์รีเลชัน มีค่าตั้งแต่ –1 ถึง 1 และกำหนดให้ y คือสัญญาณรบกวนเทียม และ x คือค่าความสว่างของรูปภาพ ค่าคอร์รีเลชันที่ได้สำหรับรูปภาพที่ไม่ได้รับการซ่อนลายเซ็นดิจิตอลไว้ จะมีค่าอยู่ที่ประมาณ 0 แต่สำหรับภาพที่ซ่อนลายเซ็นดิจิตอลไว้ ค่าที่ได้จะใกล้เคียง 1 หรือ –1

ในการนำหลักการนี้มาใช้ตรวจหาลายน้ำที่ซ่อนอยู่ในรูปภาพแบบแบ่งเป็นบล็อกๆ นั้น จำเป็นต้องทำการค้นหาพิกัดตำแหน่งของบล็อกในรูปภาพก่อน โดยทำการสแกนหาค่าคอร์รีเลชันของบล็อก เริ่มตั้งแต่จุดพิกัด (0, 0) และทำการเลื่อนทั้งในแนวตั้งและแนวนอน ไปจนกระทั่งพิกัดที่ (B, B) ซึ่ง B เป็นขนาดบล็อกที่ใช้ ค่าคอร์รีเลชันที่ได้จะมีทั้งหมด B^2 ค่า พิกัดที่เป็นตำแหน่งของบล็อกลายน้ำดิจิตอลจะให้ค่าคอร์รีเลชันที่มีค่าสัมบูรณ์มากที่สุด โดยค่า Threshold ที่เป็นเกณฑ์ในการตัดสินว่ามีลายน้ำซ่อนอยู่หรือไม่จะมีค่าเท่ากับ ค่าคอร์รีเลชันที่มากเป็นอันดับสองและค่าคอร์รีเลชันที่มากเป็นอันดับสามรวมกัน

3.4.2 การกู้คืนลายเซ็นดิจิตอล

การกู้คืนลายเซ็นดิจิตอล สามารถทำได้โดยการโมดูเลตสัญญาณรบกวนนี้กับรูปภาพดิจิตอลอีกครั้ง จากหลักการในข้อ 2.5 ในบทที่ 2 เพื่อให้สัญญาณรบกวนนี้ไปหักล้างกับสัญญาณรบกวนที่แฝงอยู่กับลายน้ำ จึงสามารถดึงข้อมูลลายน้ำดิจิตอลออกมากได้ โดยอาศัยเครื่องหมายของผลรวมค่าเฉลี่ยจากการโมดูเลต ค่าที่ได้จะเป็นลายเซ็นดิจิตอลซึ่งได้มาจากรูปภาพที่ต้องสงสัย

3.5 การตรวจสอบลายเซ็นดิจิตอล

การตรวจสอบรูปภาพแยกได้เป็น 2 ลักษณะ คือตรวจสอบความเป็นเจ้าของรูปภาพหรืออีกนัยหนึ่งคือเจ้าของลายเซ็นดิจิตอล และการตรวจสอบความถูกต้องของรูปภาพ โดยที่การตรวจสอบความเป็นเจ้าของนั้น ได้รับการรับรองโดยวิธีการเข้ารหัสแบบใช้กุญแจสาธารณะอยู่แล้ว ดังนั้นในหัวข้อนี้ จะกล่าวถึงขั้นตอนในการตรวจสอบความถูกต้องของรูปภาพ ว่ามีการถูกแก้ไขหรือไม่อย่างไร โดยผู้รับรูปภาพจะนำรูปภาพที่มีลายเซ็นดิจิตอล มาดำเนินการตรวจสอบดังต่อไปนี้

3.5.1 ขั้นตอนการตรวจสอบลายเซ็นดิจิตอล

1. นำลายเซ็นดิจิตอลที่ได้มาทำการถอดรหัสโดยกุญแจสาธารณะของผู้ส่ง ซึ่งจะได้ผลลัพธ์เป็นลักษณะเฉพาะรุ่น ที่ถูกสร้างมาพร้อมกับรูปภาพต้นฉบับ ขั้นตอนการถอดรหัสนี้มีวิธีการเหมือนกับขั้นตอนการเข้ารหัสในหัวข้อ 3.2.2 แต่จะเปลี่ยนกุญแจที่ใช้เป็นกุญแจสาธารณะซึ่งเป็นคู่กันกับกุญแจส่วนตัวของผู้ส่ง

2. นำรูปภาพที่ผู้รับได้รับไปผ่านกระบวนการแยกลักษณะเฉพาะ เพื่อให้ได้ลักษะเฉพาะรุ่น ของภาพที่ทำการตรวจสอบ โดยนำรูปภาพที่ถูกแยกเอาลายเซ็นดิจิตอลออกไปแล้วไปแยกลักษณะเฉพาะ ตามขั้นตอนการแยกลักษณะเฉพาะในหัวข้อ 3.2.1

3. นำลักษณะเฉพาะทั้งสองรุ่นมาเปรียบเทียบกัน โดยใช้ฟังก์ชันการเปรียบเทียบลักษณะเฉพาะ และแสดงผลการเปรียบเทียบให้ผู้ใช้ทราบ

3.5.2 ฟังก์ชันการเปรียบเทียบลักษณะเฉพาะ

ขั้นตอนนี้จะเป็นการนำลักษณะเฉพาะที่ได้จากการถอดรหัสลายเซ็นดิจิตอล มาเปรียบเทียบกับลักษณะเฉพาะที่สร้างจากรูปภาพที่ผู้รับมีอยู่ เทคนิคในการเปรียบเทียบนี้จะทำกับลักษณะเฉพาะในแต่ละด้านของทุกๆ บล็อก แสดงได้ตารางที่ 3.2

ตารางที่ 3.2 การเปรียบเทียบความแตกต่างของค่าลักษณะเฉพาะขนาด 4 บิต

0															
0	**1**														
1	0	**2**													
1	1	0	**3**												
2	1	1	0	**4**											
2	2	1	1	0	**5**										
3	2	2	1	1	0	**6**									
3	3	2	2	1	1	0	**7**								
4	3	3	2	2	1	1	0	**8**							
4	4	3	3	2	2	1	1	0	**9**						
5	4	4	3	3	2	2	1	1	0	**10**					
5	5	4	4	3	3	2	2	1	1	0	**11**				
6	5	5	4	4	3	3	2	2	1	1	0	**12**			
6	6	5	5	4	4	3	3	2	2	1	1	0	**13**		
7	6	6	5	5	4	4	3	3	2	2	1	1	0	**14**	
7	7	6	6	5	5	4	4	3	3	2	2	1	1	0	**15**

ฟังก์ชันที่ใช้เปรียบเทียบค่าลักษณะเฉพาะที่ได้ จะทำการคำนวณหาค่าใช้จ่ายหรือระดับความเปลี่ยนแปลงของค่าลักษณะเฉพาะที่อยู่ในรูปการปรับค่าเป็น 16 ระดับ โดยจะถือว่ามีความเปลี่ยนแปลงเมื่อเป็นการเปลี่ยนที่มากกว่า 2 ระดับขั้น ซึ่งค่าการเปรียบเทียบจะอยู่ในช่วง 0 ถึง 7 ตัวอย่างเช่น

ลักษณะเฉพาะ $f(i,\ k,0,1)$ หมายถึงลักษณะเฉพาะสัมพัทธ์กับบล็อกด้านบนของบล็อกที่ $i,\ k$ ซึ่งได้จากการถอดรหัสจากลายเซ็นดิจิตอล เปรียบเทียบกับ ลักษณะเฉพาะ $f'(i,\ k,\ 0,\ 1)$ ซึ่งหมายถึงลักษณะเฉพาะสัมพัทธ์กับบล็อกด้านบนของบล็อกที่ $i,\ k$ ที่ได้จากการสร้างใหม่จากรูปภาพที่ทดสอบ โดยที่เราจะทำการเปรียบเทียบ $f(i,k,0,1)$ กับ $f'(i,k,1,0)$

กรณีที่ $f(i,\ k,1,0) = 7$ และ $f'(i,\ k,1,0) = 8$ ผลการเปรียบเทียบจะได้ค่าความแตกต่างเท่ากับ 0 ซึ่งหมายถึง การเปลี่ยนแปลงไม่ถือว่าแตกต่างกันอย่างมีนัยสำคัญ

กรณีที่ $f(i, k,1,0) = 6$ และ $f'(i, k,1,0) = 8$ ผลการเปรียบเทียบจะได้ค่าความแตกต่างเท่ากับ 1 ซึ่งหมายถึง การเปลี่ยนแปลงนี้แตกต่างกันอย่างมีนัยสำคัญเท่ากับ 1

สำหรับภาพที่ไม่มีการเปลี่ยนแปลงใดๆ ฟังก์ชันการเปรียบเทียบนี้จะให้ค่าเท่ากับ 0 และในทางกลับกันกรณีมีการแก้ไข ค่าสูงสุดที่ได้จะเท่ากับ 7 การแสดงผลลัพธ์การเปรียบเทียบนี้จะแทนระดับความแตกต่างด้วยความเข้มของเส้นระหว่างลักษณะเฉพาะทั้งสองบล็อกนั้น

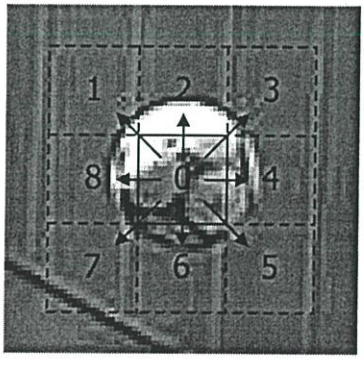
3.6 การตรวจสอบความถูกต้องของรูปภาพแบบเฉพาะส่วน

การแบ่งรูปภาพออกเป็นบล็อกๆ เป็นเทคนิคสำคัญของงานวิจัยนี้ ซึ่งขนาดของบล็อกที่ใช้นั้นขึ้นอยู่กับลักษณะ ของรูปภาพนั้นๆ ว่ามีรายละเอียดมากน้อยเพียงใด หากว่าวัตถุในภาพมีขนาดเล็ก เพื่อให้การตรวจสอบ เป็นไปอย่างสมเหตุสมผล ขนาดของบล็อกก็จำเป็นต้องมีขนาดเล็กตามลงมาด้วย เช่นบล็อกขนาด 20x20x 30x30, 40x40 จะทำให้ค่า cr สำหรับกระจายบิตให้ซ้ำกันมีค่าน้อย ทำให้ลายน้ำมีความทนทานต่อการเปลี่ยนแปลงแก้ไขรูปภาพน้อยลง

ดังนั้นผู้วิจัยจึงได้พัฒนาวิธีการตรวจสอบรูปภาพแบบเฉพาะส่วนขึ้นมา โดยใช้วิธีสร้างลายเซ็นดิจิตอลจากพื้นที่เฉพาะส่วนสำคัญของรูปภาพที่ต้องการจะปกป้อง จากนั้นนำมาซ่อนลงไปในรูปภาพโดยซ่อนลงในพื้นที่รอบๆ ซึ่งเป็นพื้นหลัง จะทำให้สามารถซ่อนลายน้ำดิจิตอลที่มีขนาดใหญ่กว่าขนาดของบล็อกได้

3.6.1 การสร้างลายเซ็นดิจิตอลแบบเฉพาะส่วน

ตัวอย่างการสร้างลายเซ็นดิจิตอลจากรูปภาพเฉพาะส่วนแสดงได้ดัง รูปที่ 3.12 มีรายละเอียดดังต่อไปนี้



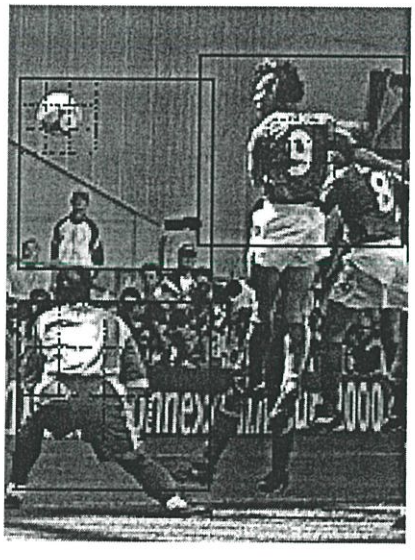
รูปที่ 3.12 ลายเซ็นดิจิตอลจากรูปภาพเฉพาะส่วนลูกบอล

1. ให้ทำการเลือกวัตถุที่ต้องการจะปกป้องในรูปภาพ เช่นรูปลูกบอล จากนั้นทำการกำหนดขนาดบล็อกที่ใกล้เคียงกับขนาดลูกบอลหรือครอบคลุมพื้นที่ส่วนใหญ่ของลูกบอลได้ (บล็อกขนาด 20x20 จุด)

2. กำหนดให้บล็อกดังกล่าวเป็นบล็อกหมายเลข 0 จากนั้นคำนวณหาลักษณะเฉพาะแบบสัมพัทธ์ (ดูหัวข้อ 3.2.1) ของบล็อกที่ 0 กับบล็อกข้างเคียง 8 บล็อก จะได้ 8 ความสัมพันธ์ แทนด้วยข้อมูล 32 บิต

3. นำลักษณะเฉพาะทำคำนวณจากบล็อกทั้ง 9 บล็อก ผนวกเข้ากับข้อมูลขนาดบล็อกและตำแหน่งของบล็อก มาสร้างลายเซ็นดิจิตอลโดยวิธีการในหัวข้อ 3.2.2 จะทำให้ลายเซ็นดิจิตอลมีขนาด 300 บิต ซึ่งประกอบด้วย ลักษณะเฉพาะสัมพัทธ์ขนาด 32 บิต 9 บล็อก และขนาดบล็อก 4 บิต และตำแหน่งบล็อกแนวตั้ง 4 บิต ตำแหน่งบล็อกแนวนอน 4 บิต ทำให้สามารถใช้กุญแจสาธารณะที่มีขนาด 128 ถึง 300 บิตในการเข้ารหัสลายเซ็นดิจิตอลได้

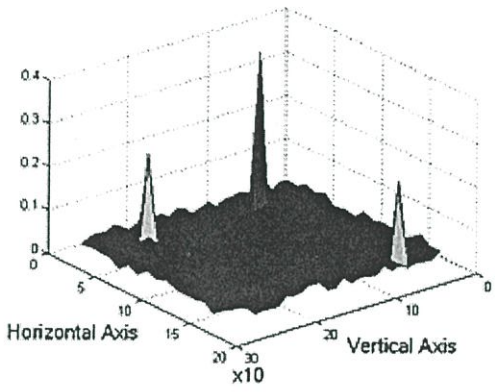
ขั้นตอนต่อมาคือการนำลายเซ็นดิจิตอลมาซ่อนลงในรูปภาพโดยใช้เทคนิคแบบสเปรดสเปคตรัมในหัวข้อที่ 3.3 โดยใช้ค่า cr ประมาณ 400 ถึง 800 เพื่อให้ลายน้ำมีความทนทานต่อการแก้ไข ซึ่งจะต้องใช้สัญญาณรบกวนเทียมขนาดประมาณ 120,000 บิต ถึง 240,000 บิต มีลักษณะการซ่อนแสดงได้ดังรูปที่ 3.13 โดยที่ เส้นประคือตำแหน่งของบล็อกที่ใช้สร้างลายเซ็นดิจิตอล และเส้นทึบแสดงขอบเขตของสัญญาณรบกวนเทียม จะเห็นได้ว่าวิธีการนี้สามารถใช้บล็อกขนาดที่แตกต่างกันเพื่อปกป้องรายละเอียดในภาพที่มีขนาดต่างกันได้



รูปที่ 3.13 ตัวอย่างการซ่อนลายเซ็นดิจิตอลแบบเฉพาะส่วน

3.6.2 การตรวจสอบลายเซ็นดิจิตอลแบบเฉพาะส่วน

วิธีการตรวจสอบจะใช้เทคนิคในการค้นคืนลายน้ำดิจิตอลจากข้อ 3.4.1 และ 3.4.2 สำหรับภาพตัวอย่างในรูปที่ 3.13 เมื่อนำมาตรวจหาลายน้ำดิจิตอลจะให้ผลของค่าคอร์รีเลชันแสดงได้ดังรูปที่ 3.14 เมื่อหาลายเซ็นดิจิตอลได้แล้ว จะนำมาตรวจสอบโดยใช้วิธีการในหัวข้อ 3.5



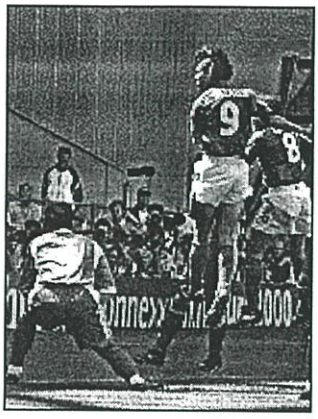
รูปที่ 3.14 กราฟแสดงค่าคอร์รีเลชันของภาพซึ่งมีการซ่อนลายเซ็นดิจิตอลไว้ 3 ตำแหน่ง

จากวิธีการนี้ทำให้การตรวจสอบรูปภาพมีประสิทธิภาพมากยิ่งขึ้น สามารถใช้กุญแจสาธารณะที่มีขนาดใหญ่ในการเข้ารหัส และใช้กับรูปภาพที่มีวัตถุสำคัญขนาดแตกต่างกันได้ แต่วิธีการนี้ยังต้องอาศัยมนุษย์ในการตัดสินใจว่าจะเลือกปกป้องบริเวณใดของรูปภาพ และจะจัดวางตำแหน่งของการซ่อนลายเซ็นตรงบริเวณใดของรูปภาพ

3.7 ความแม่นยำของการตรวจสอบรูปภาพ

จากผลการตรวจสอบรูปภาพที่ได้ซึ่งแสดงอยู่ในรูปบล็อกของบริเวณที่ถูกแก้ไข สำหรับการเปลี่ยนแปลงแก้ไขวัตถุในภาพ ผู้วิจัยได้ทำการวัดประสิทธิภาพของวิธีการตรวจสอบ เพื่อให้เห็นความแม่นยำของผลการทดลองได้อย่างชัดเจน โดยใช้การเปรียบเทียบระหว่างจุดภาพของบริเวณระบุได้จากขั้นตอนการตรวจสอบ กับจุดภาพของบริเวณที่ได้รับการแก้ไขจริงในรูปภาพ โดยที่รูปที่ 3.15 (a) และ3.15 (b) จะแสดงรูปภาพ “Inzaghi” ที่ใช้เป็นตัวอย่างภาพต้นฉบับและภาพที่ถูกแก้ไขในหัวข้อนี้

(a)



(b)

รูปที่ 3.15 (a) ภาพ "Inzaghi" ต้นฉบับ
(b) ภาพ "Inzaghi" ที่ถูกแก้ไขโดยนำพื้นหลังมาทับลูกบอล

3.7.1 จุดเปลี่ยนแปลงที่ตรวจสอบได้

หมายถึงจุดภาพของบริเวณที่ระบุได้จากขั้นตอนการตรวจสอบ เป็นจุดภาพทั้งหมดในบล็อกที่มีเส้นการเปลี่ยนแปลงล้อมรอบทั้ง 4 ด้าน สำหรับรูปภาพดิจิตอลขนาด $M \times N$ จุดภาพ $g(x, y)$ โดยที่ $x \in 0,\ldots,M\text{-}1$, $y \in 0,\ldots,N\text{-}1$ จะแทนจุดเปลี่ยนแปลงจากการตรวจสอบ โดยใช้สัญลักษณ์ $p(x, y)$ โดยที่ $p(x, y) \in 0, 1$ ค่า 0 หมายถึงไม่มีการเปลี่ยนแปลง และค่า 1 หมายถึงมีการเปลี่ยนแปลง แสดงตัวอย่างในรูปที่ 3.16 จะเป็นภาพที่ถูกตัดพื้นหลังมาทับรูปลูกบอล ซึ่งเมื่อตรวจสอบด้วยวิธีการในหัวข้อ 3.5 แล้วจะได้ผลลัพธ์เป็นบล็อกที่ถูกแก้ไข ดังนั้นจุดทั้งหมดในบล็อกที่แสดงจะเป็น จุดเปลี่ยนแปลงที่ตรวจสอบได้

รูปที่ 3.16 ผลการตรวจสอบภาพ "Inzaghi" ที่ถูกลบลูกบอล

3.7.2 จุดเปลี่ยนแปลงจริง

จุดเปลี่ยนแปลงจริง หมายถึงจุดภาพของบริเวณที่ได้รับการแก้ไขจริงในรูปภาพ เกิดจากการนำภาพต้นฉบับมาเปรียบเทียบกับภาพที่ตรวจสอบ จุดที่มีค่าความสว่างไม่เหมือนกับภาพต้นฉบับจะนับเป็นจุดภาพที่ได้รับการแก้ไขจริง รูปที่ 3.17 ส่วนที่แรงเงาของภาพที่ถูกแก้ไขเป็นบริเวณที่มีจุดภาพแตกต่างไปจากภาพต้นฉบับ แทนจุดเปลี่ยนแปลงจริงโดยใช้สัญลักษณ์ $q(x, y)$ โดยที่ $q(x, y) \in 0, 1$ ค่า 0 หมายถึงไม่มีการเปลี่ยนแปลง และค่า 1 หมายถึงมีการเปลี่ยนแปลง

รูปที่ 3.17 จุดเปลี่ยนแปลงจริง ในภาพ "Inzaghi" ที่ถูกลบลูกบอล

3.7.3 สมการหาค่าความแม่นยำ

ขั้นตอนต่อไปนี้เป็นการนำข้อมูลของจุดภาพที่มีการเปลี่ยนแปลง ทั้ง 2 ประเภทมาทำการคำนวณหาเปอร์เซ็นความแม่นยำในการระบุตำแหน่งของรูปภาพที่ถูกแก้ไขเปลี่ยนแปลง โดยใช้สมการที่ 3.6 หาอัตราส่วนระหว่าง จำนวนสมาชิกจุดภาพของพื้นที่ระบุได้จากการตรวจสอบที่ตรงกับจุดภาพที่เปลี่ยนแปลงไปจริง ต่อจำนวนสมาชิกของจุดภาพที่ระบุได้จากการตรวจสอบ คิดเป็นเปอร์เซ็นความแม่นยำ มีค่าตั้งแต่ 0% ถึง 100%

$$Accuracy = \frac{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} p(x,y)\cdot q(x,y)}{\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} p(x,y)} \times 100 \qquad (3.6)$$

จะเห็นได้ว่าถ้ารูปภาพไม่มีการเปลี่ยนแปลงแก้ไข ค่า $q(x, y)$ จะมีค่าเป็น 0 ไม่ว่าการตรวจสอบจะให้ผลเป็นอย่างไร ค่าความแม่นยำนี้จะมีค่าเป็น 0 เสมอ ในอีกกรณีหนึ่งถ้าหากว่าจุดเปลี่ยนที่ตรวจสอบได้ ตรงกับจุดเปลี่ยนแปลงจริง $p(x, y) \cdot q(x, y) = p(x, y)$ ผลลัพธ์จะมีค่าเป็น 100% หมายความว่าสามารถระบุจุดภาพบริเวณที่ถูกแก้ไขได้ทั้งหมด

บทที่ 4
ขั้นตอนการทดลองและผลการทดลอง

ในบทนี้จะเป็นการอธิบายถึงการทดลอง ตั้งแต่ขั้นตอนในการทดลองและสภาพแวดล้อมที่กำหนด โดยการนำรูปภาพดิจิตอลที่ได้จากกล้องถ่ายภาพดิจิตอล หรือการสแกนภาพถ่าย มาทำการซ่อนลายน้ำดิจิตอล และจำลองการแก้ไขเปลี่ยนแปลงรูปภาพด้วยวิธีที่ต่างกัน จากนั้นนำไปตรวจสอบความถูกต้องของรูปภาพโดยใช้ข้อมูลจากลายน้ำแบบลักษณะเฉพาะสัมพัทธ์ เพื่อรวบรวมและวิเคราะห์ผลการทดลอง โดยมีรายละเอียดดังนี้

4.1 การเตรียมการทดลอง

ในส่วนนี้จะกล่าวถึง ข้อกำหนดและขั้นตอนในการเตรียมข้อมูลรูปภาพ วิธีการที่ใช้ในการทดลอง รวมถึงแนวทางในการตรวจสอบความถูกต้องของรูปภาพ ที่ได้จากการทดลองดังนี้

4.1.1 การเตรียมรูปภาพดิจิตอล

รูปภาพที่นำมาใช้เป็นต้นฉบับในการทดลอง จะมีลักษณะเป็นภาพที่มีต้นกำเนิดจากรูปถ่ายของคน หรือวัตถุจริงตามธรรมชาติ ซึ่งได้จากการสแกนหรือถ่ายจากกล้องดิจิตอล และใช้โปรแกรมประมวลผลภาพ แปลงให้เป็นภาพความเข้มสีเทา 256 ระดับ (Grayscale 8 bits/pixel Bitmap format) ซึ่งตัวแทนภาพดิจิตอลที่นำมาแสดงตัวอย่างในการทดลองนี้ ประกอบไปด้วยภาพ 2 ภาพ ได้แก่ ภาพ "Twin" เป็นภาพที่ได้จากการสแกนจากภาพถ่าย แสดงดังรูปที่ 4.1 และภาพ "Baresi" เป็นภาพที่เผยแพร่ทางอินเตอร์เน็ต แสดงดังรูปที่ 4.2

รูปที่ 4.1 ภาพ "Twin" มีขนาด 682x508 pixels

รูปที่ 4.2 ภาพ "Baresi" มีขนาด 476x764 pixels

4.1.2 การเตรียมข้อมูลสำหรับสร้างลายเซ็นดิจิตอล

การเตรียมข้อมูลเพื่อสร้างลายเซ็นดิจิตอล มีตัวแปรสำหรับใช้สร้างลายเซ็นดิจิตอลจากรูปภาพ รวมถึงกุญแจสาธารณะ ซึ่งมีข้อกำหนดในการเตรียมข้อมูลดังนี้

1. ขนาดของบล็อกที่ใช้เข้ารหัส มีขนาด 40x40 pixels

2. ความสัมพันธ์ของบล็อกข้างเคียง จะใช้ 2 ด้านความสัมพันธ์ คือบล็อกถัดไปทางด้านขวา และด้านล่าง แทนด้วย $f'(i, k, 0,1)$ และ $f'(i, k, 1,0)$ ตามลำดับ

3. การซ่อนลายน้ำ จะใช้กำลังของสัญญาณ [2, 3, 4, 5] สำหรับการซ่อนข้อมูลความสัมพันธ์ขนาด 4 บิต ($\alpha_i = [2, 3, 4, 5]$)

4. กุญแจสาธารณะสำหรับเข้ารหัสลายเซ็นดิจิตอล จะใช้กุญแจขนาด 16 บิต โดยทำการสุ่มคู่กุญแจสำหรับผู้ส่งและผู้รับจำนวน 1 คู่

4.1.3 ข้อกำหนดรายละเอียดของอุปกรณ์

1. เครื่องคอมพิวเตอร์ การทดลองนี้ใช้คอมพิวเตอร์ PC ยี่ห้อ "Powell" CPU Pentium III 1 กิกะเฮิร์ซ หน่วยความจำ 512 เมกกะไบต์ ใช้เนื้อที่ดิสต์เก็บข้อมูลการทดลองประมาณ 50 เมกกะไบต์

2. เครื่องสแกนเนอร์สำหรับใช้แปลงรูปภาพ เป็นไฟล์ดิจิตอล เป็นของยี่ห้อ HP รุ่น ScanJet 4C ใช้ความละเอียดในการสแกน 300 dpi (จุดต่อตารางนิ้ว) ระดับความสว่าง 50%

3. เครื่องพรินเตอร์ HP LaserJet 4100 PCL 6 สำหรับพิมพ์ภาพดิจิตอลลงสู่กระดาษ ที่ความละเอียด 300 dpi ความเข้มหมึกพิมพ์ปกติ

4.1.4 ข้อกำหนดรายละเอียดของซอฟต์แวร์

1. MATLAB 5.3.1 (R11.1) เป็นเครื่องมือสำหรับเขียนโปรแกรม จำลองขั้นตอนการทำงานของการตรวจสอบรูปภาพ ในส่วนของการคำนวณ โดยเฉพาะส่วนของการเข้ารหัสและถอดรหัส รวมถึงการเข้าถึงการอ่านเขียนแฟ้มข้อมูลรูปภาพ

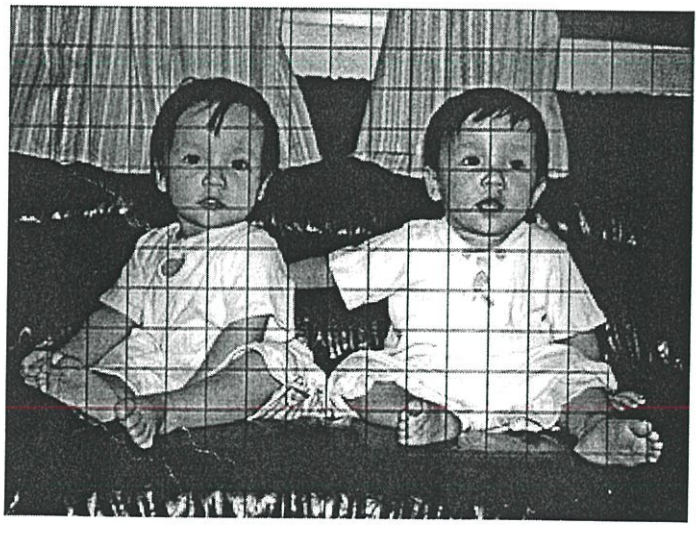
2. Adobe PhotoShop 5.5 โปรแกรมสำหรับแก้ไขเปลี่ยนแปลงรูปภาพที่ผ่านการซ่อนลายเซ็นดิจิตอลแล้ว รวมทั้งใช้ในเข้าถึงไฟล์รูปภาพในการพิมพ์รูปภาพและสแกนรูปภาพ

4.2 ขั้นตอนการทดลองและการตรวจสอบผล

การทดลองในงานวิจัยนี้ ผู้วิจัยได้ทำการจำลองกระบวนการรับส่งข้อมูลรูปภาพ ระหว่างผู้รับและผู้ส่ง โดยมีการปรับเปลี่ยนค่าตัวแปรต่างๆ ที่คาดว่าจะมีผลกระทบต่อประสิทธิภาพของเทคนิคการตรวจสอบรูปภาพที่ใช้ โดยทำการทดสอบและวัดผลกับรูปภาพที่ผ่านการแก้ไขเปลี่ยนแปลงระหว่างการส่ง ในลักษณะที่ต่างกัน ซึ่งขั้นตอนการทดลองมีตัวอย่างรายละเอียดดังนี้

4.2.1 การสร้างลักษณะเฉพาะสัมพัทธ์จากรูปภาพ

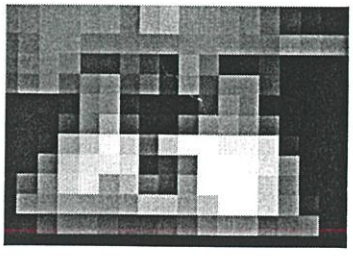
1. ทำการแบ่งภาพออกเป็นบล็อกขนาดที่เท่ากัน แล้วทำการคำนวณค่าเฉลี่ยความสว่างของแต่ละบล็อก ดังรูปที่ 4.3 และรูปที่ 4.4



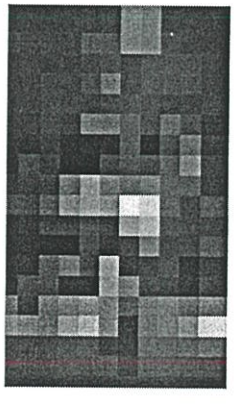
รูปที่ 4.3 ภาพที่ถูกแบ่งเป็นบล็อกขนาด 40x40 ในภาพ “Twin”

รูปที่ 4.4 ภาพที่ถูกแบ่งเป็นบล็อกขนาด 40x40 ในภาพ "Baresi"

2. จากนั้นคำนวณค่าเฉลี่ยของทุกๆบล็อกซึ่งจะได้ผลลัพธ์คล้ายกับรูปภาพที่ถูกย่อยขนาดลงด้วยอัตราส่วน 1 ต่อ Block Size ในที่นี้คือ 40 แสดงตัวอย่างผลลัพธ์ของการหาค่าเฉลี่ยในรูปแบบภาพขยาย 10 เท่าได้ดังรูปที่ 4.5 โดยตารางสี่เหลี่ยมแทนค่าเฉลี่ยของแต่ละบล็อก มีข้อมูลดังแสดงเป็นตัวอย่างในรูปที่ 4.6



(a)



(b)

รูปที่ 4.5 ผลลัพธ์ของการหาค่าเฉลี่ยแบบบล็อกของรูปภาพ (a) "Twin" และ (b) "Baresi"

131	144	150	152	162	170	154	195	204	176	175	168 . . .
113	133	153	153	137	145	154	159	163	171	173	167 . . .
115	140	151	133	75	77	114	88	43	179	138	64 . . .
101	125	146	104	136	162	101	124	70	167	109	167 . . .
22	25	43	53	156	169	66	32	33	45	96	181 . . .
29	28	34	79	152	197	99	43	55	126	185	192 . . .
22	22	47	190	215	236	211	131	219	240	243	236 . . .
28	32	125	211	227	230	221	79	98	161	245	247 . . .
55	99	162	218	230	190	207	147	114	190	244	250 . . .
55	141	151	185	182	179	187	211	212	196	220	244 . . .
29	34	77	117	113	100	89	89	98	118	159	172 . . .
24	24	30	35	40	44	43	42	41	43	46	50 . . .

รูปที่ 4.6 ตัวอย่างค่าเฉลี่ยแบบบล็อกของภาพ "Twin"

3. หาค่าความสัมพันธ์ของบล็อกข้างเคียงโดยใช้ความสัมพันธ์ 2 ทิศทาง จากสมการที่ 3.2 (ในบทที่ 3) ทำการเข้ารหัสของค่าความสัมพันธ์แต่ละความสัมพันธ์ ให้อยู่ในรูปของจำนวนเต็ม 4 บิต จะได้เป็นค่าลักษณะเฉพาะสัมพัทธ์ของรูปภาพ มีตัวอย่างดังรูปที่ 4.7 (a) และรูปที่ 4.7 (b)

2	3	5	10	5	1	8	13	9	5	11
14	4	14	4	4	2	3	11	5	9	8
6	10	5	10	4	9	1	10	5	7	7
5	8	4	6	2	11	2	9	10	14	13
5	9	10	3	5	10	11	3	5	10	13
4	2	5	4	3	12	5	1	13	9	9
11	4	3	10	6	2	15	8	2	7	7
2	3	14	9	0	1	14	3	2	7	7
5	3	2	6	10	12	9	9	8	6	11
4	2	10	1	5	3	3	11	12	5	7
4	8	10	8	11	2	5	7	9	12	15
1	14	4	0	7	9	0	14	6	1	15
5	10	2	9	0	15	2	10	7	1	13
2	7	9	2	0	11	11	5	13	2	11
14	0	9	4	8	13	4	10	9	10	14
1	2	10	6	7	15	0	4	12	5	5
13	11	7	14	3	14	0	14	5	3	12
11	8	10	13	3	13	4	9	11	7	5
7	12	13	11	7	12	13	11	8	1	10

รูปที่ 4.7 (a) ตัวอย่างค่าลักษณะสัมพัทธ์แบบบล็อก ในทิศทางด้านขวา

8	10	4	10	4	1	3	8	1	11	6
14	7	3	13	14	10	15	7	10	2	8
4	12	12	2	6	4	5	10	8	14	13
5	5	11	8	5	11	2	11	7	14	10
6	13	9	5	4	1	9	1	12	12	11
10	10	5	3	15	15	8	7	5	2	6
5	0	1	3	10	2	5	1	3	4	12
6	6	2	0	0	4	9	1	14	10	5
8	2	1	6	1	9	1	0	12	5	3
15	13	13	15	14	14	7	2	11	7	5
5	5	11	7	12	9	15	14	13	1	5
10	12	8	0	3	0	5	13	6	7	6
5	9	5	13	14	11	0	5	10	10	5
8	10	2	0	0	8	11	4	8	0	2
3	0	5	10	4	14	3	3	5	6	12
11	7	14	13	11	11	3	9	9	14	6
9	3	7	10	5	1	2	14	9	11	9
5	10	3	10	5	10	6	6	5	10	5
15	15	15	15	15	15	3	14	15	15	15

รูปที่ 4.7 (b) ตัวอย่างค่าลักษณะสัมพัทธ์แบบบล็อก ในทิศทางด้านล่าง

4.2.2 การสร้างลายเซ็นดิจิตอล

เป็นการนำลักษณะเฉพาะ ที่ได้จากขั้นตอนแรกมาเข้ารหัสด้วยวิธีการแบบ RSA โดยขั้นแรกจะทำการสร้างคู่กุญแจส่วนตัวและกุญแจสาธารณะของผู้ส่งและผู้รับตามลำดับ จากนั้นทำการเข้ารหัสบล็อก 2 บล็อกต่อการเข้ารหัสกุญแจ 16 บิตหนึ่งครั้ง แสดงดังตัวอย่างในรูปที่ 4.8 และ รูปที่ 4.9 ตามลำดับ

Private Key = 1 1 1 1 1 0 0 0 0 0 1 1 0 1 0 1

Public Key = 0 1 0 1 0 0 1 0 1 0 1 1 1 1 0 1

Modulo = 1 1 1 1 1 0 0 0 0 1 0 0 0 1 0 1

รูปที่ 4.8 คู่กุญแจส่วนตัวและกุญแจสาธารณะขนาด 16 บิต

239	43	59	43	59	1	179	239	1	88	39
113	84	179	233	113	43	37	84	43	167	239
59	188	188	167	39	59	126	43	239	113	233
126	126	88	239	126	88	167	88	84	113	43
39	233	163	126	59	1	163	1	188	188	88
43	43	126	179	37	37	239	84	126	167	39
126	0	1	179	43	167	126	1	179	59	188
39	39	167	0	0	59	163	1	113	43	126
239	167	1	39	1	163	1	0	188	126	179
37	233	233	37	113	113	84	167	88	84	126
126	126	88	84	188	163	37	113	233	1	126
43	188	239	0	179	0	126	233	39	84	39
126	163	126	233	113	88	0	126	43	43	126
239	43	167	0	0	239	88	59	239	0	167
179	0	126	43	59	113	179	179	126	39	188
88	84	113	233	88	88	179	163	163	113	39
163	179	84	43	126	1	167	113	163	88	163
126	43	179	43	126	43	39	39	126	43	126
37	37	37	37	37	37	179	113	37	37	37

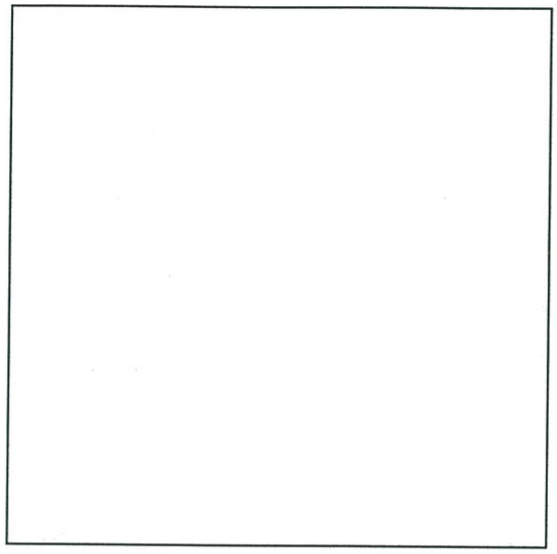
รูปที่ 4.9 ตัวอย่างลายเซ็นดิจิตอล

4.2.3 การซ่อนลายน้ำดิจิตอล

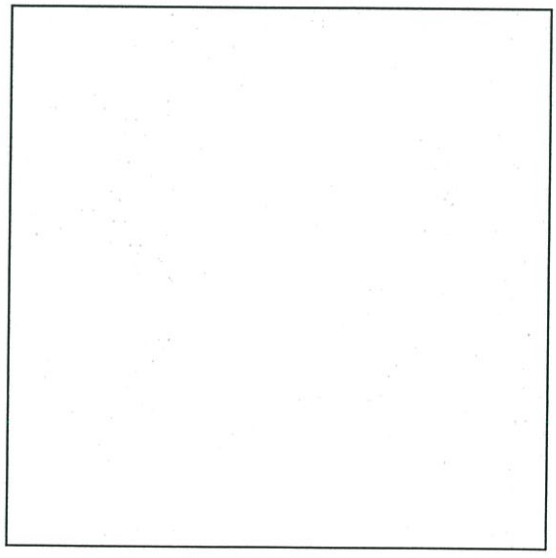
ขั้นตอนนี้จะนำลายเซ็นดิจิตอลที่ได้ มาซ่อนลายน้ำเข้าไปในรูปภาพ โดยเริ่มจากการสุ่มสัญญาณรบกวนเทียมขึ้นมาก่อน แสดงตัวอย่างดังรูปที่ 4.10 รูปที่ 4.11 และ รูปที่ 4.12 ตามลำดับ

1.0151	1.0151	1.0151	-0.9753	-0.9753	1.0151	1.0151
1.0151	-0.9753	-0.9753	1.0151	1.0151	-0.9753	1.0151
1.0151	-0.9753	1.0151	1.0151	1.0151	-0.9753	-0.9753
1.0151	-0.9753	-0.9753	-0.9753	-0.9753	-0.9753	-0.9753
1.0151	1.0151	-0.9753	1.0151	-0.9753	1.0151	-0.9753
-0.9753	1.0151	1.0151	-0.9753	-0.9753	1.0151	-0.9753
1.0151	1.0151	-0.9753	-0.9753	-0.9753	1.0151	1.0151
1.0151	-0.9753	1.0151	1.0151	-0.9753	1.0151	-0.9753
-0.9753	-0.9753	1.0151	-0.9753	1.0151	-0.9753	1.0151
-0.9753	1.0151	1.0151	1.0151	-0.9753	1.0151	-0.9753

รูปที่ 4.10 ตัวอย่างสัญญาณรบกวนเทียม



รูปที่ 4.11 ลายน้ำดิจิตอลขนาด 1 บล็อก ค่ากำลัง (Amplitude) เฉลี่ยเท่ากับ 5



รูปที่ 4.12 ลายน้ำดิจิตอลขนาด 1 บล็อก ค่ากำลัง (Amplitude) เฉลี่ยเท่ากับ 10

เมื่อซ่อนลายน้ำดิจิตอลเข้าไปในรูปภาพเรียบร้อยแล้ว จากนั้นเราจะบันทึกแฟ้มรูปภาพที่ถูกป้องกันนี้ เพื่อนำไปจำลองการเปลี่ยนแปลงแก้ไขรูปภาพในขั้นตอนต่อไป

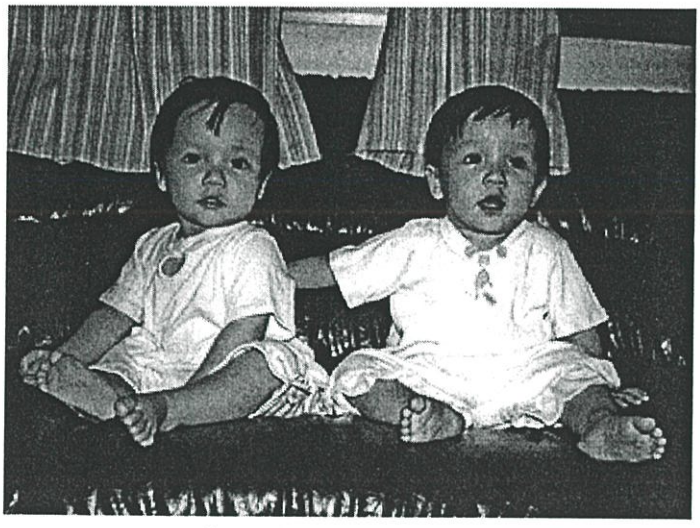
4.2.4 การแก้ไขรูปภาพ

4.2.4.1 การเพิ่มสัญญาณรบกวน (Noise adding)

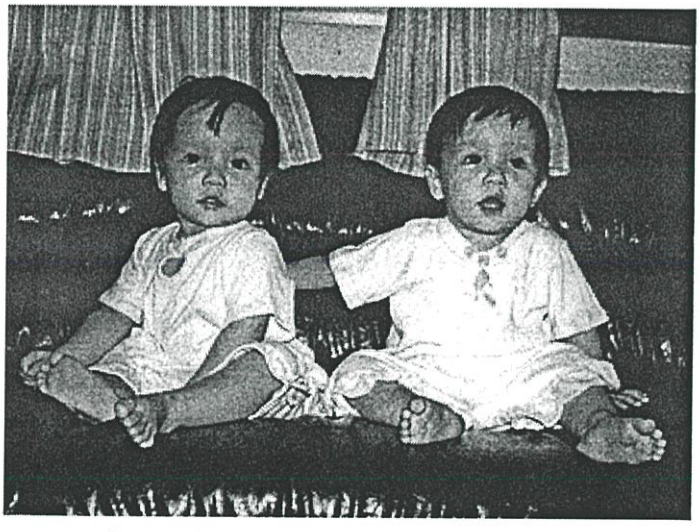
เทคนิคการซ่อนลายน้ำแบบสเปรดสเปคตรัมที่ใช้ในงานวิจัยนี้ มีแนวคิดพื้นฐานมาจากการซ่อนข้อมูลลงไปในรูปภาพ ให้มีลักษณะคล้ายกับสัญญาณรบกวนกำลังต่ำ แต่สำหรับในการใช้งานจริง รูปภาพอาจถูกเปลี่ยนแปลง โดยมีสัญญาณรบกวนที่เกิดจากข้อจำกัดหรือความบกพร่องทางอุปกรณ์ที่เกี่ยวข้อง เช่นสแกนเนอร์ พรินเตอร์ ในการทดลองนี้ จะนำรูปภาพที่มีลายน้ำดิจิตอลซ่อนอยู่ มาเพิ่มสัญญาณรบกวนแบบสุ่มเทียม ที่มีการแจกแจงแบบเกาส์เซียน (Gaussian) และมีค่าเฉลี่ยของกำลังสัญญาณ (Amplitude) ที่ 5 และ 10 ตามลำดับ ดังรูปที่ 4.13 (a) 4.13 (b) และ รูปที่ 4.14 (a) 4.14 (b)

รูปที่ 4.13 (a) ภาพ "Baresi" ที่ถูกเปลี่ยนแปลงโดยสัญญาณรบกวนที่กำลังเท่ากับ 5

รูปที่ 4.13 (b) ภาพ "Baresi " ที่ถูกเปลี่ยนแปลงโดยสัญญาณรบกวนที่กำลังเท่ากับ 10



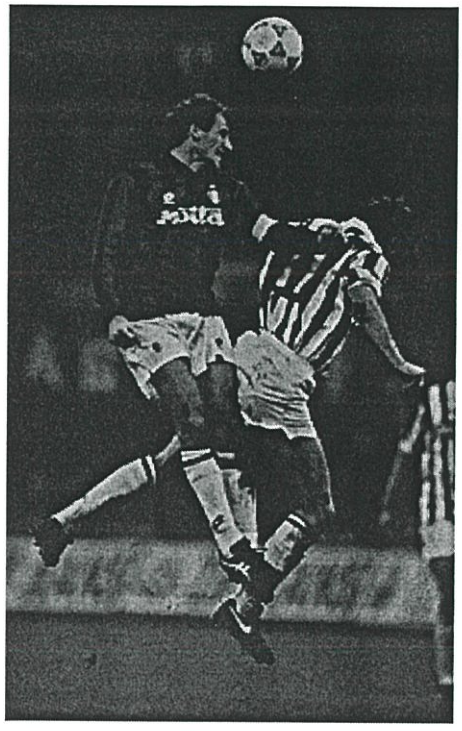
รูปที่ 4.14 (a) แสดงภาพ "Twin" ที่ถูกเปลี่ยนแปลงโดยสัญญาณรบกวน ที่กำลังเท่ากับ 5



รูปที่ 4.14 (b) แสดงภาพที่ถูกเปลี่ยนแปลงโดยสัญญาณรบกวน ที่กำลังเท่ากับ 10

4.2.4.2 การปรับค่าความสว่าง (Brightness adjustment)

การทดลองนี้จะทำการแก้ไขความสว่างของของรูปภาพ โดยการบวกค่าความสว่างของทุกๆ จุดภาพ ด้วยจำนวนเต็มคงที่ค่าหนึ่ง ที่มีค่าอยู่ในช่วง -20, -10, 10 และ 20 ระดับความเข้มสีเทา แสดงตัวอย่างได้ดังรูปที่ 4.15 (a) 4.15 (b)



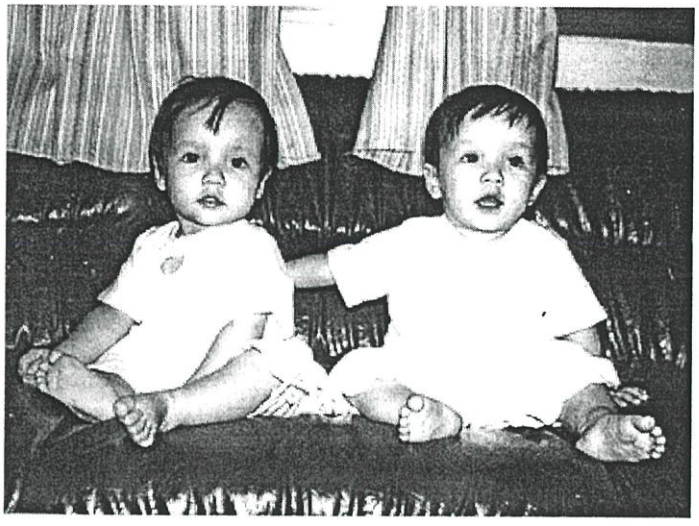
รูปที่ 4.15 (a) ภาพ "Baresi" ที่ถูกปรับค่าความสว่าง -20

รูปที่ 4.15 (b) ภาพ "Baresi " ที่ถูกปรับค่าความสว่าง +20

4.2.4.3 การปรับความแตกต่างของความสว่าง (Contrast adjustment)

เป็นการเพิ่มหรือลดความแตกต่างของความสว่างในรูปภาพ โดยให้ค่าความแตกต่างตั้งแต่ –20, -10, 10 และ 20 ระดับ ดังรูปที่ 4.16 (a) และ 4.16 (b)

รูปที่ 4.16 (a) ภาพ "Twin" ที่ถูกปรับความแตกต่างค่าความสว่าง -20



รูปที่ 4.16 (b) ภาพ "Twin" ที่ถูกปรับความแตกต่างค่าความสว่าง +20

4.2.4.4 การบีบอัดรูปภาพแบบ JPEG (JPEG compression)

ฟอร์แมตไฟล์ที่มีการลดขนาดข้อมูลรูปภาพมีด้วยกันหลายแบบตัวอย่าง เช่น GIF, TIF และ PNG แต่ที่เลือกใชไฟล์แบบ JPEG ในการทดลองเพราะว่าเป็นรูปแบบการบีบอัดข้อมูลแบบสูญเสียซึ่งทำให้รูปภาพถูกแก้ไขเปลี่ยนแปลง ดังนั้นจึงได้ทำการบันทึกภาพเป็นไฟล์ประเภท JPEG โดยกำหนดดีกรีของการบีบอัดขนาดแบบ JPEG ที่ 95%, 90%, 80% แล้วแปลงภาพเหล่านั้นกลับมาเป็นภาพแบบ BMP อีกครั้ง เพื่อนำไปตรวจสอบ แสดงดังรูปที่ 4.17 (a, b, c)

(a)

(b)

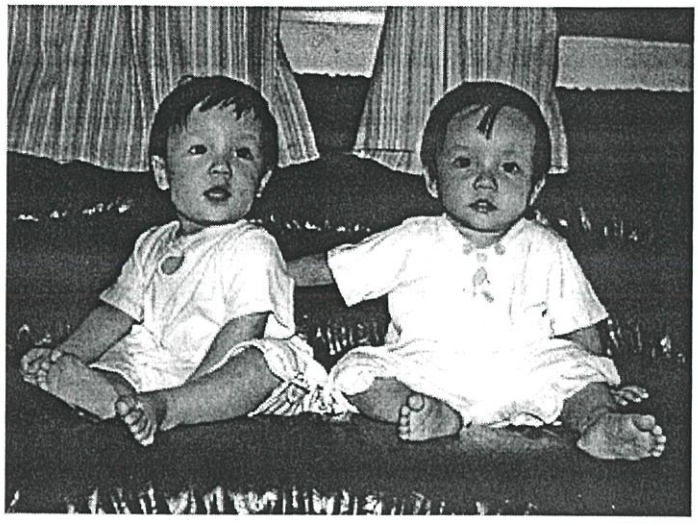
(c)

รูปที่ 4.17 (a, b, c) ภาพ "Baresi" ที่ทำการบีบอัดข้อมูลแบบ JPEG ที่ระดับ 95%, 90% และ 80% ตามลำดับ

4.2.4.5 การแก้ไขเปลี่ยนแปลงวัตถุในภาพ

เป็นการใช้โปรแกรมประมวลผลภาพ โดยทำการย้ายพื้นที่ของภาพบางส่วน ไปทับพื้นที่ที่เป็นส่วนของวัตถุในภาพ โดยมีการแก้ไขแตกต่างกันขึ้นอยู่กับลักษณะรูปภาพ มีรายละเอียดดังนี้

1. ภาพ "Twin" ทำการสลับใบหน้าของเด็กฝาแฝดแต่ละคน โดยตัดพื้นที่บริเวณใบหน้าของเด็กทางซ้ายก๊อปปี้ (Copy) ไปแทนที่บริเวณใบหน้าของเด็กทางขวา และนำภาพใบหน้าของเด็กทางขวามาแทนที่บริเวณใบหน้าของเด็กทางซ้ายดังรูปที่ 4.18



รูปที่ 4.18 ภาพ "Twin" ที่ทำการสลับใบหน้าของเด็กฝาแฝดแต่ละคน

2. ภาพ "Baresi" ทำการตัดพื้นที่ฉากหลังบริเวณซึ่งเป็นภาพฝูงชนเบลอๆ มาแทนที่รูปลูกฟุตบอลเพื่อทำให้ลูกฟุตบอลเสมือนว่าหายไป แสดงดังรูปที่ 4.19

รูปที่ 4.19 ภาพ "Baresi" ที่ถูกลบลูกฟุตบอล

4.3 ผลการทดลอง

4.3.1 ประสิทธิภาพของการซ่อนลายน้ำ

ก่อนที่จะทำการซ่อนและตรวจสอบความถูกต้องของรูปภาพ ผู้วิจัยได้ทำการทดลองและวัดประสิทธิภาพของการซ่อนลายน้ำที่ใช้เทคนิคแบบสเปรดสเปคตรัม โดยทำการซ่อนลายน้ำดิจิตอลโดยใช้วิธีการที่พัฒนาขึ้น (ดูรายละเอียดของวิธีการในหัวข้อที่ 3.3) ที่สร้างจากข้อมูลขนาด 8 บิต ลงในรูปภาพดิจิตอล และทำการปรับค่าขนาดของบล็อก(Block size) ค่าบิตซ้ำ (Cr) ซึ่งจะแปรผันตามขนาดบล็อก และปรับค่ากำลังสัญญาณรบกวนเฉลี่ยต่อบิต (Watermark amplitude) จำนวน 100 ครั้งสำหรับแต่ละเงื่อนไข และเปรียบเทียบบิตข้อมูลที่ได้กับบิตข้อมูลตั้งต้น จะได้เปอร์เซ็นต์ความผิดพลาดของการกู้คืนข้อมูลจากลายน้ำดิจิตอลดังตารางที่ 4.1 และ 4.2

ตารางที่ 4.1 เปอร์เซ็นต์ความผิดพลาดของการกู้ข้อมูล 8 บิต/บล็อก จากลายน้ำดิจิตอล ในภาพ "Twin"

BLOCK SIZE	CR BIT	WATERMARK AMPLITUDE				
		3	4	5	6	7
20x20	50	28.90%	10.24%	3.03%	2.32%	1.02%
40x40	200	22.35%	5.24%	0.84%	0.34%	0.00%
60x60	450	15.43%	1.47%	0.12%	0.07%	0.00%
80x80	800	7.36%	0.76%	0.09%	0.00%	0.00%
100x100	1250	1.54%	0.06%	0.00%	0.00%	0.00%
120x120	1800	0.78%	0.00%	0.00%	0.00%	0.00%

ตารางที่ 4.2 เปอร์เซ็นต์ความผิดพลาดของการกู้ข้อมูล 8 บิต/บล็อก จากลายน้ำดิจิตอล ในภาพ "Baresi"

BLOCK SIZE	CR BIT	WATERMARK AMPLITUDE				
		3	4	5	6	7
20x20	50	30.12%	11.03%	3.54%	2.40%	1.10%
40x40	200	22.01%	4.77%	0.75%	0.28%	0.00%
60x60	450	16.11%	1.71%	0.14%	0.08%	0.00%
80x80	800	8.39%	0.86%	0.08%	0.00%	0.00%
100x100	1250	1.48%	0.03%	0.00%	0.00%	0.00%
120x120	1800	0.46%	0.00%	0.00%	0.00%	0.00%

4.3.2 ผลลัพธ์จากการตรวจสอบความถูกต้อง

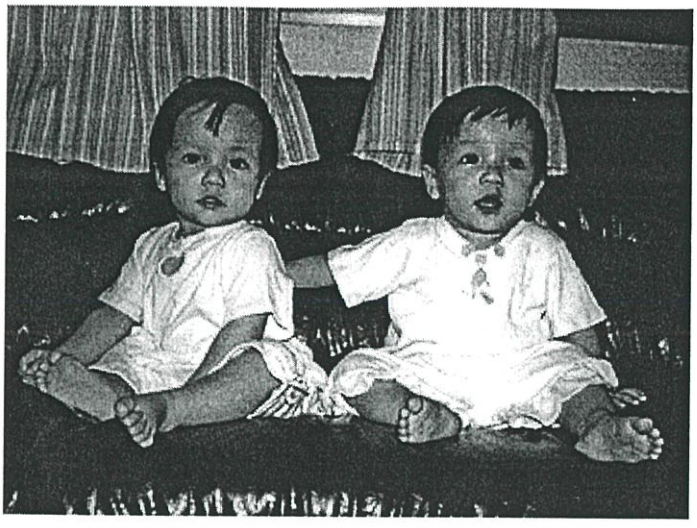
หลังจากที่ได้ทดลองตามขั้นตอนที่วางไว้เรียบร้อยแล้ว ต่อมาจะนำรูปภาพที่ซ่อนลายน้ำไว้มาตรวจสอบ ผลการตรวจสอบรูปภาพที่ได้มีดังนี้

4.3.2.1 ผลลัพธ์จากรูปภาพที่ถูกเพิ่มสัญญาณรบกวน

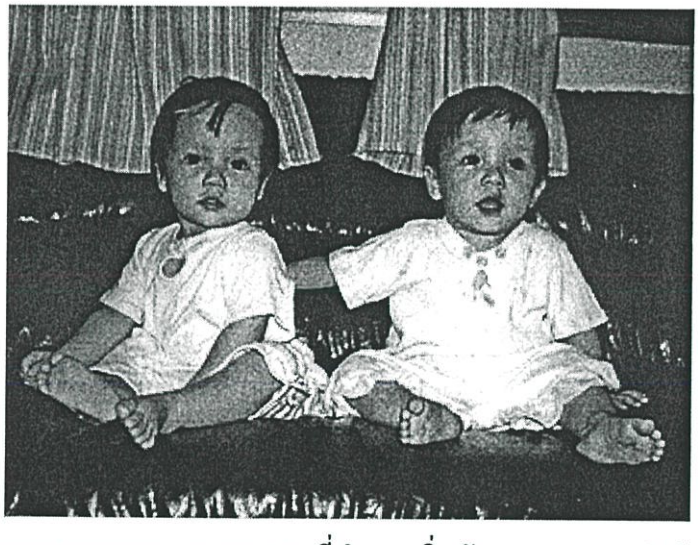
ภาพผลลัพธ์ที่ได้จะมีบล็อกที่กู้คืนลายน้ำผิดพลาดเล็กน้อย ซึ่งค่าการเปรียบเทียบที่ผิดพลาดนี้ไม่อยู่ในระดับที่กำหนดไว้ในฟังก์ชั่นการเปรียบเทียบ (ดูรายละเอียดจากหัวข้อ 3.5.2) จึงไม่พบว่ามีการแสดงความผิดพลาดของรูปภาพที่ถูกแก้ไข จากรูปที่ 4.20 (a) 4.20 (b) และรูปที่ 4.21 (a) 4.21 (b)

รูปที่ 4.20 (a) ภาพการตรวจสอบภาพ "Baresi" ที่ถูกเปลี่ยนแปลงโดยสัญญาณรบกวนระดับ 5

รูปที่ 4.20 (b) ภาพการตรวจสอบภาพ "Baresi" ที่ถูกเปลี่ยนแปลงโดยสัญญาณรบกวนระดับ 10



รูปที่ 4.21 (a) ภาพการตรวจสอบภาพ "Twin" ที่ทำการเพิ่มสัญญาณรบกวนกำลัง 5



รูปที่ 4.21 (b) ภาพการตรวจสอบภาพ "Twin" ที่ทำการเพิ่มสัญญาณรบกวนกำลัง 10

4.3.2.2 ผลลัพธ์จากรูปภาพที่ถูกปรับค่าความสว่าง

ภาพผลลัพธ์ที่ได้จะพบว่าการปรับค่าความสว่างรูปภาพที่ระดับ –20, -10, +10, +20 นั้นจะได้ผลการตรวจสอบที่แสดงว่าภาพนี้ยังเป็นภาพที่ถูกต้องเหมือนภาพต้นฉบับ ดังรูปที่ 4.22 (a, b, c, d) และรูปที่ 4.23 (a, b, c, d)

(a)

(b)

(c)

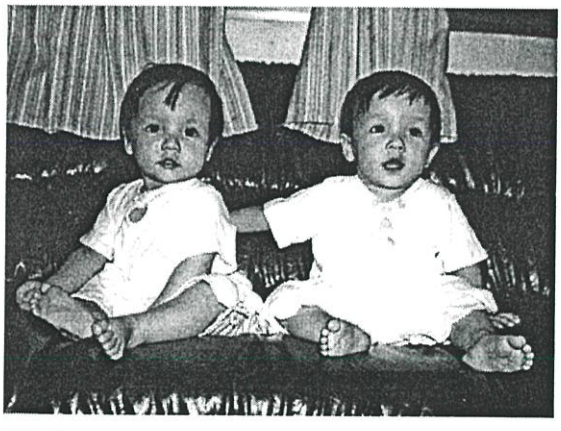
(d)

รูปที่ 4.22 (a, b, c, d) ภาพการตรวจสอบภาพ "Baresi" ที่ทำการปรับค่าความสว่าง –20, -10, +10, +20 ตามลำดับ

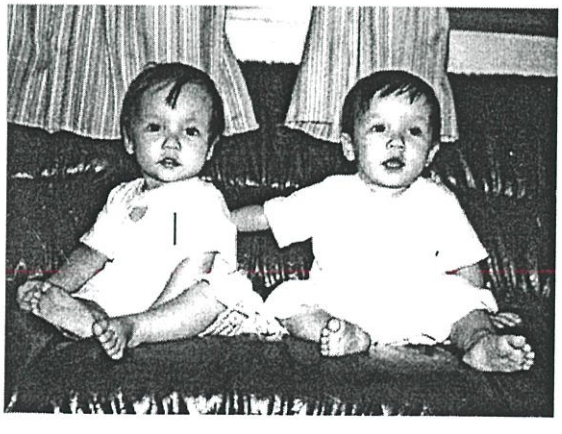
(a)

(b)

(c)



(d)

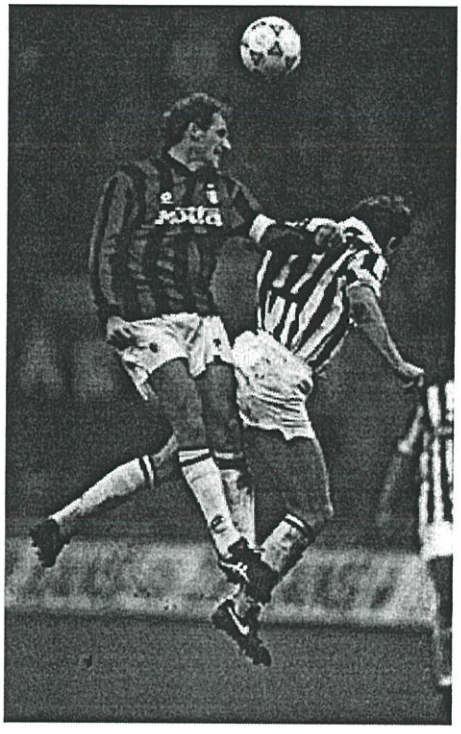


รูปที่ 4.23 (a, b, c, d) ภาพการตรวจสอบภาพ "Twin" ที่ทำการปรับค่าความสว่าง –20, -10, +10, +20 ตามลำดับ

4.3.2.3 ผลลัพธ์จากรูปภาพที่ถูกปรับความแตกต่างของความสว่าง

การแก้ไขลักษณะนี้จะทำให้ได้ผลลัพธ์การตรวจสอบที่ถูกต้อง ดังรูปที่ 4.24 (a, b, c, d) และ 4.25 (a, b, c, d)

(a)



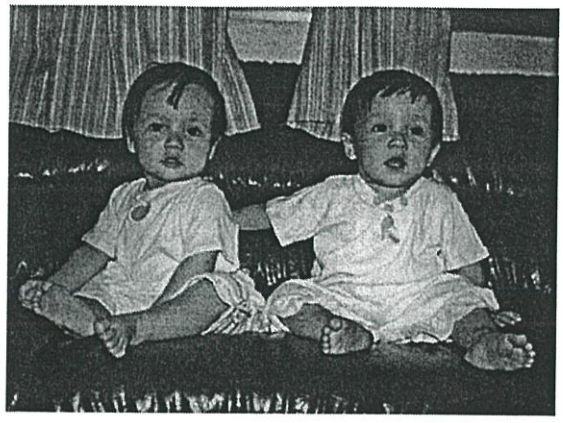
(b)

(c)

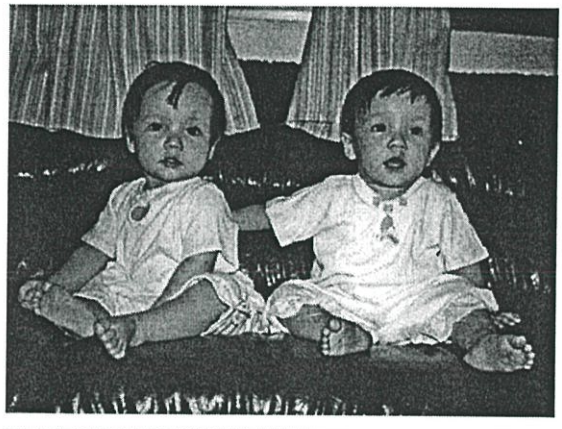
(d)

รูปที่ 4.24 (a, b, c, d) ภาพการตรวจสอบภาพ "Baresi" ที่ทำการปรับค่าความแตกต่างของความสว่าง –20, -10, +10, +20 ตามลำดับ

(a)



(b)



(c)

(d)

รูปที่ 4.25 (a, b, c, d) ภาพการตรวจสอบภาพ "Twin" ที่ทำการปรับค่าความแตกต่างของความสว่าง –20, -10, +10, +20 ตามลำดับ

4.3.2.4 ผลลัพธ์จากรูปภาพที่ถูกบีบอัดข้อมูลภาพแบบ JPEG

ผลการตรวจสอบภาพจะให้ผลว่าภาพเป็นภาพที่ถูกต้อง เมื่ออัตราการบีบอัดอยู่ที่ระดับ 80-100% ดังรูปที่ 4.26 (a, b, c) และรูปที่ 4.27 (a, b, c)

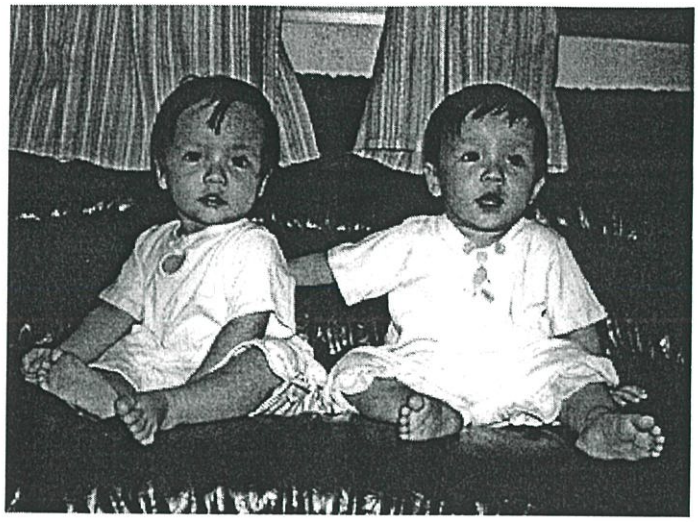
(a)

(b)

(c)

รูปที่ 4.26 (a, b, c) ภาพการตรวจสอบภาพ "Baresi" ที่ทำการบีบอัดข้อมูลแบบ JPEG ที่ระดับ 80%, 90% และ 95% ตามลำดับ

(a)



(b)

(c)

รูปที่ 4.27 (a, b, c) ภาพการตรวจสอบภาพ "Twin" ที่ทำการบีบอัดข้อมูลแบบ JPEG ที่ระดับ 80%, 90% และ 95% ตามลำดับ

4.3.2.5 ผลลัพธ์จากรูปภาพที่ถูกแก้ไขบิดเบือนวัตถุในภาพ

ในกรณีนี้เราสามารถตรวจพบว่าบริเวณรอยเส้นประที่เกิดขึ้นจะเป็นบริเวณที่ภาพไม่ถูกต้อง ซึ่งอาจจะมีการแก้ไขโดยการลบวัตถุในภาพไป หรือเปลี่ยนตำแหน่งของวัตถุในภาพ แสดงดังรูปที่ 4.28 และรูปที่ 4.29

รูปที่ 4.28 ภาพการตรวจสอบ ภาพ "Baresi" ที่ถูกลบลูกบอล

รูปที่ 4.29 ภาพการตรวจสอบ ภาพ "Twin" ที่ถูกสลับใบหน้า

ตัวอย่างภาพที่นำมาใช้ในการทดลองอื่นๆ นั้น ได้นำมารวบรวมไว้ในภาคผนวก ข. และผลการทดลองทั้งหมดจะนำไปสรุปในบทต่อไป

4.3.3 การปรับปรุงผลลัพธ์จากการตรวจสอบความถูกต้อง

จากผลลัพธ์จากการตรวจสอบซึ่งแสดงเป็นเส้นระหว่างบล็อกที่มีการเปลี่ยนแปลงจะพบว่าจะมีเส้นเกิดขึ้นจากความผิดพลาดในการตรวจสอบเกิดขึ้น เส้นดังกล่าวถูกนำมาปรับปรุงให้มีความสมเหตุสมผลกับลักษณะการแก้ไขรูปภาพมากขึ้นโดยสามารถแบ่งการปรับปรุงเส้นผลลัพธ์ที่เกิดขึ้นได้ 2 ขั้นตอนดังนี้

1. พิจารณาในแต่ละบล็อกเส้นที่เกิดขึ้นในบล็อกเพียงด้านเดียวจากสี่ด้านจะถูกตัดทิ้งไป และบล็อกที่มีเส้นการเปลี่ยนแปลงเกิดขึ้น 3 จากทั้งหมดสี่ด้าน จะถูกเติมเส้นให้ครบทั้ง 4 ด้าน เพื่อให้เป็นบล็อกที่มีการแก้ไขอย่างสมบูรณ์ ดังรูปที่ 4.30

รูปที่ 4.30 ภาพการตรวจสอบ ภาพ "Twin" ซึ่งตัดเส้นที่ผิดพลาดบล็อกละหนึ่งเส้นจากรูป 2.23 (b)

2. กลุ่มของบล็อกที่ถูกแก้ไขที่อยู่ใกล้เคียงกันจะถูกรวมเข้าเป็นบล็อกใหญ่เดียวกัน โดยจะทำการตัดเส้นการแก้ไขของบล็อกภายในทิ้งไปคงเหลือไว้เฉพาะเส้นของบล็อกภายนอกที่ล้อมเป็นพื้นที่ของรูปภาพที่มีการแก้ไขไว้เท่านั้น ดังรูปที่ 4.31

รูปที่ 4.31 ภาพการตรวจสอบ ภาพ "Twin" ซึ่งรวมกลุ่มของบล็อกที่ถูกแก้ไขเป็นบล็อกเดี่ยวกันจากรูป 2.29

จากขั้นตอน 2 ขั้นตอนดังกล่าวสามารถนำมาเขียนอัลกอริทึมสำหรับใช้งานจริงได้ดังรูปที่ 4.32

```
function Result = trim(Right, Down)
[Row, Col] = size(Right);
Block = zeros(Row, Col);
for r = 1 : Row,
   for c = 1 : Col,
      Lines = Right(r, c-1) + Right(r, c) + . . .
              Down(r-1, c) + Down(r, c);
      if Lines = 1 then
         Right(r, c) = 0
         Down(r, c) = 0
      elsif Lines >= 3 then
         Right(r, c-1) = 1;
         Right(r, c) = 1;
         Down(r-1, c) = 1;
         Down(r, c) = 1;
         Block(r, c) = 1;
      end if
   end
end
for r = 1 : Row,
   for c = 1 : Col,
      if Block(r, c) = 1,
         Right(r, c-1) = Right(r, c-1) + 1;
         Right(r, c) = Right(r, c) + 1;
         Down(r-1, c) = Down(r-1, c) + 1;
         Down(r, c) = Down(r, c) + 1;
      end if
   end
end
for r = 1 : Row,
   for c = 1 : Col,
      if Right(r, c)>1,
         Right(r, c) = 0;
      end if
      if Down(r, c)>1,
         Down(r, c) = 0;
      end if
   end
end
```

รูปที่ 4.32 อัลกอริทึมสำหรับปรับปรุงผลลัพธ์การตรวจสอบรูปภาพ

4.3.4 อัตราความผิดพลาดของการตรวจสอบความถูกต้อง

ในหัวข้อนี้จะเป็นการวัดค่าความผิดพลาดในการตรวจสอบของเทคนิคการตรวจสอบความถูกต้องของรูปภาพ ทั้งแบบการตรวจสอบทั่วทั้งภาพและการตรวจสอบรูปภาพเฉพาะส่วน โดยวัดจากจำนวนเส้นที่เกิดขึ้นเมื่อตรวจสอบลายเซ็นดิจิตอลของรูปภาพที่ผ่านกระบวนการแก้ไขรูปภาพพื้นฐานประเภทต่างๆในระดับการแก้ไขต่างๆกัน โดยขั้นตอนนี้ทำการทดลองกับกลุ่มตัวอย่างภาพดิจิตอลจำนวน 27 ภาพ (ดูในภาคผนวก ข) ผลลัพธ์แสดงได้ดังตารางที่ 4.3, 4.4, 4.5 และ 4.6

ตารางที่ 4.3 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดระหว่างวิธีการตรวจสอบรูปภาพแบบปกติและแบบเฉพาะส่วนสำหรับภาพที่ผ่านกระบวนการปรับค่าความสว่าง

ระดับการปรับค่าความสว่าง	Line Error Detection Rate (%)	
	Full Image Authentication	Partial Image Authentication
1. ± 5 ระดับความสว่าง	0.0%	00%
2. ± 10 ระดับความสว่าง	0.2%	0.0%
3. ± 20 ระดับความสว่าง	1.2%	0.4%
4. ± 30 ระดับความสว่าง	3.5%	1.2%
5. ± 40 ระดับความสว่าง	8.5%	6.5%

ตารางที่ 4.4 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดระหว่างวิธีการตรวจสอบรูปภาพแบบปกติและแบบเฉพาะส่วนสำหรับภาพที่ผ่านกระบวนการปรับค่าความแตกต่างความสว่าง

ระดับการปรับค่าความแตกต่างความสว่าง	Line Error Detection Rate (%)	
	Full Image Authentication	Partial Image Authentication
1. ± 5 ระดับความสว่าง	0.0%	0.0%
2. ± 10 ระดับความสว่าง	0.6%	0.2%
3. ± 20 ระดับความสว่าง	3.4%	1.8%
4. ± 30 ระดับความสว่าง	10.5%	6.7%
5. ± 40 ระดับความสว่าง	23.5%	14.0%

ตารางที่ 4.5 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดระหว่างวิธีการตรวจสอบรูปภาพแบบปกติและแบบเฉพาะส่วนสำหรับภาพที่มีการเพิ่มสัญญาณรบกวน

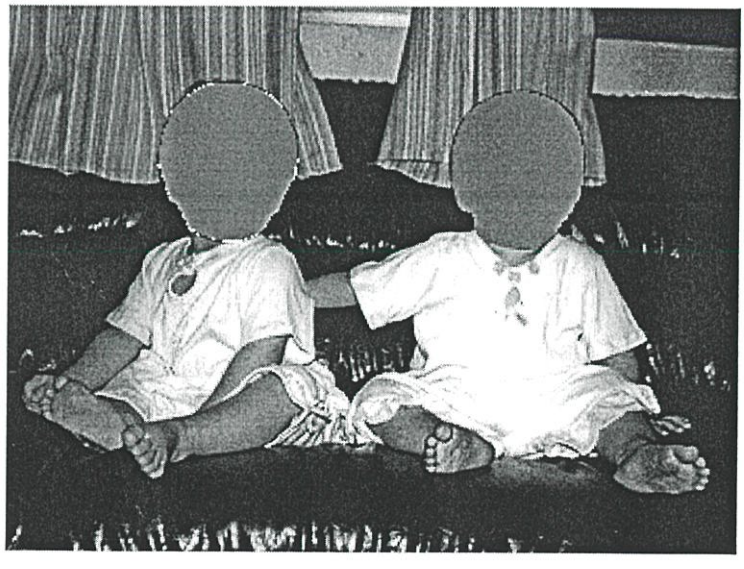
ระดับสัญญาณรบกวนในภาพ	Line Error Detection Rate (%)	
	Full Image Authentication	Partial Image Authentication
1. สัญญาณรบกวน 5	0.0%	0.0%
2. สัญญาณรบกวน 10	0.2%	0.0%
3. สัญญาณรบกวน 15	0.6%	0.2%
4. สัญญาณรบกวน 20	1.9%	0.8%
5. สัญญาณรบกวน 25	2.3%	1.2%

ตารางที่ 4.6 เปรียบเทียบอัตราส่วนการตรวจสอบที่ผิดพลาดระหว่างวิธีการตรวจสอบรูปภาพแบบปกติและแบบเฉพาะส่วนสำหรับภาพที่ผ่านกระบวนการบีบอัดแบบ JPEG

ระดับการบีบอัดรูปภาพแบบ JPEG	Line Error Detection Rate (%)	
	Full Image Authentication	Partial Image Authentication
1. JPEG 90	0.0%	0.0%
2. JPEG 80	0.0%	0.0%
3. JPEG 70	1.8%	0.2%
4. JPEG 60	3.5%	1.3%
5. JPEG 50	5.6%	3.0%

4.3.5 ความแม่นยำของการตรวจสอบรูปภาพที่ถูกแก้ไขเปลี่ยนแปลงวัตถุ

สำหรับการแก้ไขชนิดที่มีการเปลี่ยนแปลงวัตถุภายในภาพ ผู้วิจัยได้ทำการวัดค่าความแม่นยำของการระบุพื้นที่ที่ถูกแก้ไข โดยใช้วิธีการคำนวณในหัวข้อ 3.7 ตัวอย่างพื้นที่ของจุดเปลี่ยนแปลงจริงของรูป "Twin" แสดงได้ดังรูปที่ 4.32 นำมาคำนวณกับจุดเปลี่ยนแปลงที่ได้จากการตรวจสอบดังรูปที่ 4.31 และทำการทดลองเพิ่มเติมกับรูปภาพอื่นๆ อีกจำนวน 20 ภาพ (ดูในภาคผนวก ข) ได้ผลการทดลองแสดงดังตารางที่ 4.7



รูปที่ 4.33 จุดที่ถูกแก้ไขเปลี่ยนแปลงจริงเมื่อเทียบกับภาพต้นฉบับของรูปภาพ "Twin"

ตารางที่ 4.7 ค่าความแม่นยำของการตรวจสอบรูปภาพที่ถูกแก้ไขจำแนกตามลักษณะรูปภาพ

ประเภทรูปภาพ	ค่าความแม่นยำ
1. ภาพที่มีรายละเอียดมาก ภาพที่ 1, 3, 4, 5 12, 13, 14, 16, 18, 20	92.35%
2. ภาพที่มีรายละเอียดน้อย ภาพที่ 2, 6, 7, 8, 9, 10, 11, 15, 17, 19	85.84%
3. ภาพที่มีความสว่างแตกต่างกันมาก ภาพที่ 2, 3, 8, 10, 11, 12, 13, 14, 16, 17	89.28%
4. ภาพที่มีความสว่างแตกต่างกันน้อย ภาพที่ 1, 4, 5, 6, 7, 9, 15, 16, 18, 19, 20	84.57%
5. ค่าเฉลี่ยจากรูปภาพทั้งหมด 20 ภาพ	87.26%

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

เนื่องจากคุณสมบัติทั่วไปของรูปภาพดิจิตอลที่ยอมให้มีการแก้ไขเปลี่ยนแปลงข้อมูลความสว่างของจุดภาพได้ในระดับหนึ่งที่ไม่ทำให้คุณภาพหรือความหมายของภาพที่ต้องการสื่อของภาพเสียไป อีกประการหนึ่งรูปภาพดิจิตอลมีปริมาณข้อมูลมาก ซึ่งไม่สะดวกต่อการนำภาพต้นฉบับมาใช้ในการเปรียบเทียบ ทำให้เกิดปัญหาของการตรวจสอบความถูกต้องของรูปภาพดิจิตอล ที่ไม่สามารถใช้การเปรียบเทียบข้อมูลในระดับบิตเหมือนข้อมูลดิจิตอลประเภทอื่นได้

มาตรฐานการรักษาความปลอดภัยของข้อมูลดิจิตอลโดยใช้ลายเซ็นดิจิตอลนับว่าเป็นแนวคิดที่ได้รับการยอมรับว่าเป็นวิธีการตรวจสอบข้อมูลดิจิตอลที่น่าเชื่อถือ แต่ไม่สามารถนำมาใช้ได้กับข้อมูลรูปภาพได้โดยตรง เนื่องมาจากปัญหาดังกล่าวข้างต้น แนวคิดอื่นนอกเหนือจากนี้คือใช้วิธีการซ่อนลายน้ำดิจิตอล ซึ่งมีการใช้งานกันอย่างแพร่หลายกับรูปภาพดิจิตอล โดยทำการซ่อนข้อมูลสัญลักษณ์บางอย่างลงไปในภาพ เพื่อใช้ปกป้องลิขสิทธิ์แสดงความเป็นเจ้าของ แต่ก็มีจุดอ่อนในการที่จะลบทำลายหรือทำปลอมขึ้นมาได้ง่าย ซึ่งผู้วิจัยเห็นว่าพอจะมีแนวทางในการพัฒนาการตรวจสอบรูปภาพดิจิตอลโดยปรับปรุงขั้นตอนการสร้างลายเซ็นดิจิตอล รวมไปถึงกระบวนการเซ็นและตรวจสอบลายเซ็นดิจิตอลสำหรับรูปภาพ โดยประยุกต์เทคนิคการซ่อนลายน้ำดิจิตอลลงในรูปภาพมาใช้ในการการตรวจสอบความถูกต้องของรูปภาพอย่างมีประสิทธิภาพได้

งานวิจัยนี้ได้นำเสนอวิธีการซ่อนข้อมูลลงในรูปภาพดิจิตอล มีวัตถุประสงค์เพื่อใช้ตรวจสอบความถูกต้องของรูปภาพ โดยสร้างลายเซ็นดิจิตอลจากข้อมูลลักษณะเฉพาะแบบสัมพัทธ์ และซ่อนในรูปภาพโดยใช้เทคนิคแบบสเปรดสเปคตรัม เป็นการนำจุดเด่นของวิธีการใช้ลายเซ็นดิจิตอลซึ่งเป็นมาตรฐานของวิธีการรักษาความปลอดภัยของข้อมูลแบบดิจิตอล มาประยุกต์ใช้ร่วมกับเทคนิคการซ่อนลายน้ำแบบสเปรดสเปคตรัม ซึ่งเป็นวิธีการซ่อนข้อมูลลงในภาพให้มีลักษณะคล้ายกับสัญญาณรบกวน ทำให้วิธีการตรวจสอบแบบใหม่นี้ มีวิธีการดังต่อไปนี้

1. สร้างลักษณะเฉพาะจากรูปภาพที่แบ่งเป็นบล็อก และใช้ค่าความสัมพันธ์ของค่าเฉลี่ยของแต่ละบล็อกที่อยู่ข้างเคียงกัน ในการแทนรูปภาพดิจิตอล ทำให้ได้ลักษณะเฉพาะของรูปภาพที่สามารถแทนตำแหน่งของแต่ละบล็อกที่สัมพันธ์กันอยู่ในภาพได้ และไม่ขึ้นกับการปรับค่าความมืดหรือความสว่างของภาพ ซึ่งจะถูกนำไปใช้เปรียบเทียบในการตรวจสอบความถูกต้อง

2. มีการนำลักษณะเฉพาะของรูปภาพต้นฉบับมาสร้างเป็นลายเซ็นดิจิตอล และใช้การเข้ารหัสกุญแจสาธารณะแบบ RSA ทำให้ลายเซ็นดิจิตอลนี้มีความปลอดภัยและนำไปใช้ตรวจสอบความถูกต้องของรูปภาพดิจิตอลได้

3. มีการซ่อนลายเซ็นดิจิตอลรวมเข้าเป็นเนื้อเดียวกันกับรูปภาพดิจิตอล โดยใช้เทคนิคแบบสเปรดสเปคตรัม ซึ่งเป็นวิธีการหนึ่งที่มีประสิทธิภาพและความทนทานต่อการเปลี่ยนแปลงแก้ไขสูง ทำให้ยากต่อการลบหรือทำลายลายเซ็นดิจิตอล โดยที่ไม่ทำให้รูปภาพเสียหาย

เมื่อผนวกเอาลักษณะเด่นของแนวคิดต่างๆ ที่นำมาประยุกต์ใช้ร่วมกันนี้ ผู้วิจัยคาดว่าวิธีการใหม่ที่ทำการพัฒนาขึ้นนี้จะสามารถใช้ตรวจสอบความถูกต้องของรูปภาพดิจิตอลอย่างมีประสิทธิภาพ โดยสามารถระบุได้ว่าบริเวณใดหรือบล็อกใดของภาพที่มีการเปลี่ยนแปลงแก้ไข และสามารถตรวจสอบภาพที่ผ่านการแก้ไขโดยวิธีการต่างๆ ได้หลากหลายขึ้น และจากผลการทดลองผู้วิจัยสามารถวิเคราะห์และสรุปผลได้ดังนี้

5.1 สรุปผลการวิจัย

จากประโยชน์ที่คาดว่าจะได้รับในบทที่ 1 สามารถประยุกต์ใช้ลายเซ็นดิจิตอลร่วมกับการซ่อนลายน้ำดิจิตอล เพื่อนำมาตรวจสอบความถูกต้องของรูปภาพได้ และเมื่อทำการทดลองแล้ว ผลการทดลองเป็นที่ยอมรับได้ตามเป้าหมายที่วางไว้ วิธีการตรวจสอบที่พัฒนาขึ้นนี้สามารถตรวจสอบรูปภาพคน สัตว์ หรือวัตถุสิ่งของได้ โดยสามารถตรวจสอบการมีอยู่หรือสูญหายไปของวัตถุในรูปภาพ ซึ่งขึ้นอยู่กับขนาดของบล็อกที่ใช้ในการเข้ารหัส ซึ่งขนาดของวัตถุที่จะทำการตรวจสอบในภาพจะต้องมีขนาดไม่เล็กไปกว่าขนาดของบล็อก มิฉะนั้นจะไม่สามารถแยกได้ว่าการแก้ไขนั้นเกิดขึ้นที่บล็อกใด ปัจจัยที่มีผลต่อการตรวจสอบนั้นได้แก่ความทนทานต่อการแก้ไขเปลี่ยนแปลงรูปภาพ วิธีการนี้มีความทนทานต่อการแก้ไขรูปภาพในลักษณะต่างๆ แตกต่างกันไป ซึ่งทำให้มีความเหมาะสมในการใช้ตรวจสอบความถูกต้องของข้อมูลที่ผ่านการเปลี่ยนแปลงแก้ไขโดยวิธีการต่างๆ ไม่เท่ากัน จากผลการทดลองในบทที่ 4 ผู้วิจัยได้มาวิเคราะห์และสรุปแยกเป็นประเด็นใหญ่ๆ ตามลักษณะการแก้ไขรูปภาพได้ 5 ประเด็นดังต่อไปนี้ โดยเรียงลำดับตามความทนทานจากมากไปหาน้อย

1. การเพิ่มสัญญาณรบกวน การเพิ่มสัญญาณรบกวนลงในรูปภาพ การแก้ไขลักษณะนี้มีที่มาจากสาเหตุสองประการคือ หนึ่งเกิดจากการแปลงจากภาพดิจิตอลเป็นอนาล็อกแล้วแปลงกลับเป็นภาพดิจิตอลอีกครั้งหนึ่ง เช่นการพิมพ์ภาพออกทางเครื่องพิมพ์ แล้วสแกนกลับมาเป็นไฟล์ดิจิตอลอีกครั้งหนึ่ง ส่วนอีกประการนั้นเกิดจากวิธีการซ่อนลายน้ำดิจิตอลเอง ซึ่งเทคนิคสเปรดสเปคตรัมที่ใช้ในงานวิจัยนี้ จะทำให้ลายน้ำดิจิตอลมีลักษณะเป็นสัญญาณรบกวนกำลังต่ำซ่อนอยู่ในรูปภาพ จากผลการทดลองเมื่อนำรูปภาพที่มีลายน้ำดิจิตอล กลับมาตรวจสอบความถูกต้องของรูปภาพทันที จะให้ผลลัพธ์ที่ถูกต้อง 100% ซึ่งการซ่อนลายน้ำนี้สามารถทำซ้ำกันได้ประมาณ 4-6 ครั้ง โดยใช้กำลังของสัญญาณรบกวนกำลังต่ำ ในกรณีที่สัญญาณรบกวนในภาพเกิดจากการแปลงดิจิตอล-อนาล็อก-ดิจิตอล นั้นขึ้นอยู่กับกำลังของสัญญาณรบกวนและการแจกแจงของ

สัญญาณรบกวนว่าเป็นการแจกแจงแบบเกาซ์ ที่มีค่าเฉลี่ยใกล้เคียง 0 หรือไม่ ซึ่งสัญญาณรบกวนที่มีค่าเฉลี่ยใกล้เคียง 0 นั้นจะไม่มีผลกระทบต่อลายน้ำดิจิตอล ซึ่งจากผลการทดลองการตรวจสอบจะให้ผลลัพธ์ถูกต้องเมื่อสัญญาณรบกวนมีค่าไม่เกิน 20

2. การปรับค่าความสว่าง การแก้ไขลักษณะนี้เป็นการปรับค่าความสว่างของทุกๆ จุดสีในภาพ ซึ่งจะไม่มีผลกระทบต่อลายน้ำดิจิตอล จนกว่าค่าที่ปรับนี้จะเกินขีดจำกัดค่าหนึ่งซึ่งขึ้นอยู่กับรูปภาพด้วยว่าเป็นภาพที่มีความสว่างหรือมืดมากน้อยแค่ไหน แต่โดยเฉลี่ยแล้วรูปภาพดิจิตอลทั่วไปที่ผ่านการปรับแต่งค่าความสว่างเพิ่มหรือลดเพื่อให้ได้ภาพที่มีคุณภาพดีขึ้นนั้น จะไม่ทำให้ลายน้ำดิจิตอลมีการเปลี่ยนแปลง ผลการตรวจสอบจะให้ผลถูกต้อง 100% เมื่อระดับการปรับค่ามีไม่เกิน 25 ระดับความเข้ม

3. การปรับค่าความแตกต่างของความสว่าง การแก้ไขรูปภาพแบบนี้เป็นการปรับคุณภาพของรูปภาพให้มีความชัดเจนขึ้น เป็นการปรับฮิสโตแกรมของค่าความสว่างจุดภาพให้กระจายตัวกันอย่างเหมาะสม ซึ่งผลกระทบต่อลายน้ำดิจิตอลนั้น ขึ้นอยู่กับความแตกต่างของค่าความสว่างของภาพก่อนและหลังการปรับค่า โดยจะต้องไม่เกินค่าความแตกต่างของลักษณะเฉพาะในตารางการเปรียบเทียบซึ่งเป็นขั้นตอนการตรวจสอบลายน้ำ โดยที่การแก้ไขลักษณะนี้จะมีเปอร์เซ็นต์การตรวจสอบได้ถูกต้องเมื่อการปรับค่ามีไม่เกินบวกลบ 15 ระดับความเข้ม

4. การบีบอัดข้อมูลภาพแบบ JPEG เป็นการแก้ไขที่เกิดจากการแปลงฟอร์แมตไฟล์รูปภาพ ซึ่งพบได้ทั่วไป วิธีการนี้ทำให้คุณภาพของรูปภาพด้อยลง และจะทำลายข้อมูลลายน้ำดิจิตอลที่ซ่อนอยู่ในรูปภาพ การทำลายนี้ขึ้นอยู่กับระดับการบีบอัดของอัลกอริทึม ผลการทดลองแสดงให้เห็นว่าการตรวจสอบรูปภาพสามารถทำได้ถูกต้องประมาณ 95% กับภาพที่ใช้ระดับการบีบอัด 8-10 (สำหรับการบีบอัดตั้งแต่ระดับ 1-10 จากมากไปน้อย)

5. การแก้ไขเปลี่ยนแปลงวัตถุในภาพ การแก้ไขแบบนี้มีความหลากหลายและซับซ้อนกว่าวิธีอื่น ซึ่งไม่สามารถจำกัดหรือระบุได้ชัดเจนว่ามีขั้นตอนอย่างไรบ้าง แต่โดยทั่วไปแล้วจะมีผลให้ข้อมูลหรือวัตถุที่อยู่ในภาพมีการเปลี่ยนแปลง ไม่ว่าจะเป็นการสลับตำแหน่ง ลบ หรือเพิ่มบริเวณพื้นที่บางส่วนของรูปภาพ ในการทดลองซึ่งใช้วิธีการสลับพื้นที่บางส่วนของภาพ และย้ายพื้นที่บางส่วนของภาพไปทับอีกส่วนหนึ่งนั้น จะมีผลกระทบกับข้อมูลลายน้ำดิจิตอลและรูปภาพมากที่สุดในบรรดาวิธีที่ใช้ทดลอง แต่จากผลการตรวจสอบนั้น สามารถระบุได้ว่ารูปภาพบริเวณบล็อกใดบ้างที่ถูกแก้ไข ซึ่งความถูกต้องของการตรวจสอบนั้น ขึ้นอยู่กับปริมาณพื้นที่ที่ถูกแก้ไขในภาพ จะต้องมีปริมาณไม่ต่ำกว่า 85% ของขนาดบล็อก

การตรวจสอบความถูกต้องของรูปภาพดิจิตอล ที่ถูกแก้ไขโดยไม่อาศัยภาพต้นฉบับในการเปรียบเทียบนั้น เป็นขั้นตอนที่ยากต่อการแยกแยะโดยคอมพิวเตอร์ และยังต้องอาศัยสายตาของมนุษย์ในการตัดสินใจอย่างถูกต้องว่าภาพที่ได้รับการแก้ไขนั้น ถูกทำให้คุณภาพเปลี่ยนแปลงถึงขั้น

ที่เรียกว่าทำให้ภาพเสียหายหรือเปลี่ยนแปลงความหมายของรูปภาพหรือไม่ ทำให้มีกฎเกณฑ์การพิจารณาที่ไม่แน่นอนตายตัว ขึ้นกับตัวบุคคลแตกต่างกันไป อย่างไรก็ตามคอมพิวเตอร์สามารถช่วยงานที่เกี่ยวข้องกับรูปภาพจำนวนมากเช่นการตรวจสอบรูปภาพในเครือข่ายอินเตอร์เน็ตหรือฐานข้อมูล ทำให้สามารถทำได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

5.2 ข้อเสนอแนะสำหรับการพัฒนาในอนาคต

จากผลการทดลอง พบว่าวิธีการที่ได้พัฒนานี้มีข้อจำกัดบางประการ และมีจุดที่ควรปรับปรุงให้มีประสิทธิภาพมากขึ้นต่อไปอีกดังนี้

1. ข้อจำกัดของเทคนิคการซ่อนลายน้ำแบบสเปรดสเปคตรัม ทำให้วิธีการนี้สามารถตรวจสอบรูปภาพที่ผ่านการแก้ไข ที่ไม่ซับซ้อนมากนัก เช่นการปรับค่าความสว่างของรูปภาพ หรือการเข้ารหัสภาพแบบ JPEG เป็นต้น ผู้วิจัยมีความเห็นว่าต่อไปเมื่อมีการพัฒนาวิธีการซ่อนลายน้ำที่ประสิทธิภาพดีขึ้น จะทำให้สามารถตรวจสอบความถูกต้องของรูปภาพดิจิตอลที่ถูกแก้ไขเปลี่ยนแปลงได้ได้ซับซ้อนมากยิ่งขึ้น

2. ในงานวิจัยนี้ใช้การเข้ารหัสบล็อกที่กำหนดขนาดตายตัวเท่ากันหมดทั้งรูปภาพ ซึ่งอาจไม่เหมาะสมเมื่อนำไปใช้กับภาพที่มีรายละเอียดสูง ซึ่งบางบริเวณของภาพอาจจะมีรายละเอียดที่เล็กหรือใหญ่ไม่เท่ากัน อาจจะต้องมีการปรับขนาดบล็อกให้แปรผันกับเนื้อหาของรูปภาพ ซึ่งรูปภาพหนึ่งๆ สามารถใช้การเข้ารหัสบล็อกได้หลายๆ ขนาดในภาพเดียวกัน เพื่อให้สามารถตรวจสอบรายละเอียดของรูปภาพได้ยืดหยุ่นมากขึ้น ผู้วิจัยมีความเห็นว่าน่าจะมีการใส่ข้อมูลขนาดของบล็อกในแต่ละบริเวณลงในลักษณะเฉพาะที่นำไปสร้างลายเซ็นดิจิตอล อาจเป็นทางเลือกหนึ่งที่เป็นไปได้

3. ปรับปรุงเทคนิคในการเข้ารหัสกุญแจสาธารณะของข้อมูลลักษณะเฉพาะให้ใช้กับกุญแจที่มีขนาดใหญ่ขึ้น เนื่องจากข้อจำกัดของขนาดบล็อก และความยุ่งยากในการเข้าและถอดรหัสข้อมูลโดยให้กุญแจสาธารณะที่มีขนาดใหญ่ ในการวิจัยนี้จึงใช้กุญแจขนาดเล็กพอที่ใช้ในการทดลอง เพื่อเป็นแนวคิดในการปรับปรุงต่อไป จะต้องพิจารณาขนาดกุญแจที่เหมาะสมในการประยุกต์ใช้งานจริงอีกด้วย

4. ควรมีการพัฒนาขั้นตอนการตรวจสอบความถูกต้องของรูปภาพดิจิตอล ที่ทำให้ผู้ใช้สามารถพิจารณาและตัดสินได้ว่าภาพถูกแก้ไขไปมากน้อยในระดับใด ได้ง่ายและชัดเจนยิ่งขึ้น อาจมีการสร้างแบบจำลองหรือสมการในการวัดค่าความเปลี่ยนแปลงของรูปภาพออกมาเป็นตัวเลขเป็นค่ามาตรฐานใช้ในการเปรียบเทียบกับรูปภาพต่างๆได้

เอกสารอ้างอิง

[1] Aura, T. "Practical Invisible in Digital Communication." In Proc. of the HUT Seminar on Network Security '95, Espoo, Finland. Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology, November 1995. pp. .

[2] Bender, W. et. al. "Techniques for Data Hiding." IBM System Journal., vol.35, no.3&4, 1996. pp. 313-336.

[3] Chang-Hsing, L. and Yeuan-Kuen, L. "An Adaptive Digital Image Watermarking Technique for Copyright Protection." IEEE Transactions On Consumer Electronics., vol.45, no.4, November 1999. pp. 1006-1015.

[4] Charles P.Pfleeger. **Security In Computing**. 2nd Ed. Prentice Hall, Inc. 1997. pp. 91-95.

[5] Comiskey, B.O. and J.R. Smith, "Modulation and Information Hiding in Images." In Proc. of Information Hiding, 1st International Workshop, Cambridge, U.K. Lecture Notes in Computer Science, Vol. 1174, 1996.

[6] Douglas, S.R. **Cryptography Theory and Practice**. Florida : CRC Press, Inc. 1995.

[7] Fridrich, J. "Image Watermarking for Tamper Detection." IEEE International Conference On Image Processing., vol.2, 1998. pp.404-408.

[8] Fridrich , J and Goljan, M. "Robust Hash Functions for Digital Watermarking." Information Technology : Coding And Computing., 2000. pp.178-183.

[9] Hartung, F. and Girod, B. "Watermarking of Uncompressed and Compressed Video." Signal Precessing, Cambridge,U.K., vol. 66, no. 3, May 1998. pp. 283-301

[10] Information security committee electronic commerce and section of science & technology, American Bar Association. "Digital Signature Guideline." [Online]. Available : http://www.abanet.org/scitech/ec/isc/digital_signature.html. August 1, 1996.

[11] Ingemar, C. J. et. al. "Secure Spread Spectrum Watermarking for Multimedia." IEEE Transactions On Image Processing., vol.6, no.12, December 1997. pp. 1673-1687.

[12] Jain, A. K. **Fundamentals Of Digital Image Processing**. New Jersey : Prentice-Hall, Inc. 1989.

[13] Koch, E. and Zhao, J. "Toward robust and hidden image copyright labeling." IEEE Workshop

on Nonlinear Signal and Image Processing., I. Pitas Editor, 1995. pp.452-455.

[14] Lynn, P. A. **Digital Signal Processing With Computer Applications.** New York : John Wiley & Sons. 1994.

[15] Manber, U. **Introduction To Algorithms (A Creative Approach).** Addison-Wesley Inc. 1989. pp. 294-297.

[16] Piva, A. et. al. "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image" IEEE International Conference On Image Processing., Firenze, Italy, vol.1, 1997. pp.520-523.

[17] Porat ,B. **A Course In Digital Signal Processing.** US. : John Wiley & Sons, Inc. 1997.

[18] Rao, K.R. and Hwang ,J.J. **Techniques & Standards For Image, Video & Audio Coding.** New Jersey, US. : Prentice-Hall International, Inc. 1996.

[19] Rodger, E. et. al. **Digital Communications And Spread Spectrum Systems.** New York, US. : Macmillan Publishing Company. 1985.

[20] Schneider, M and Chang ,S. "A Robust Content Based Digital Signature for Image Authentication." IEEE Transactions On Image Processing., vol.3, 1996. pp.227-230.

[21] Umbaugh, S.E. **Computer Vision and Image Processing.** International Ed. NJ., US. : Prentice-Hall International, Inc. 1998.

[22] Won-Gyum, K. et. al. "An Image Watermarking Scheme with Hidden Signatures." IEEE International Conference On Image Processing., vol.2, 1999. pp.206-210.

ภาคผนวก

ภาคผนวก ก.

ตัวอย่างโปรแกรม

การทดลองที่ทำในงานวิจัย ได้ประยุกต์ใช้โปรแกรม MATLAB รุ่น 5.3.129215a (R11.1) เขียนโปรแกรม ในการทำกระบวนการสร้างลายเซ็นดิจิตอล และซ่อนข้อมูลลงในรูปภาพดิจิตอล รวมทั้งการตรวจสอบความถูกต้องของรูปภาพดิจิตอล

ก.1 การหาค่าเฉลี่ยของภาพแบ่งเป็นบล็อก

```
function Result = Block(Picture,BlockSize,Row,Col)
Result = Picture((Row-1).*BlockSize+1:Row.*BlockSize,
                 (Col-1).*BlockSize+1:Col.*BlockSize);
```

```
function Result = bavg(X, BlockSize)
[Row, Col] = size(X);
BlockPerRow = floor(Row / BlockSize);
BlockPerCol = floor(Col / BlockSize);
Result = zeros(BlockPerRow, BlockPerCol);
for r = 1 : BlockPerRow,
   for c = 1 : BlockPerCol,
      Result(r,c) =  round(mean2(block(X,BlockSize,r,c)));
   end
end
```

ก.2 การหาความสัมพันธ์ระหว่างบล็อก

```
function code = encode(X, Y)
ratio = similar(X,Y);
x = int8(round(ratio*100));
if x <= -32, code = 0;
elseif x <= -24, code = 1;
elseif x <= -16, code = 2;
elseif x <= -12, code = 3;
elseif x <= -8, code = 4;
elseif x <= -4, code = 5;
elseif x <= -2, code = 6;
elseif x <= 0, code = 7;
elseif x <= 2, code = 8;
elseif x <= 4, code = 9;
elseif x <= 8, code = 10;
elseif x <= 12, code = 11;
elseif x <= 16, code = 12;
elseif x <= 24, code = 13;
elseif x <= 32, code = 14;
else code = 15; end;
```

```
function Result = Relate(feature)
[m,n] = size(feature);
Result = zeros(m, n);
feature = cat(1,feature(m,:),feature);
feature = cat(2,feature(:,n),feature);
feature(m+2,:) = feature(2,:);
feature(:,n+2) = feature(:,2);
for r = 2:m+1,
   for c = 2:n+1,
      Result(r-1,c-1) = encode(feature(r,c), feature(r,c+1));
      Result(r-1,c-1) = bitshift(Result(r-1,c-1),4) +
                        encode(feature(r,c), feature(r+1,c));
      Result(r-1,c-1) = bitrotate(Result(r-1,c-1),r+c-2,8);
   end;
end;
```

ก.3 การเข้า/ถอดรหัสกุญแจสาธารณะแบบ RSA

```
% rsa_pq(bits) : find the optimal p and q for data [bits] bits.
%     [p,q] = rsa_pq(bits)
%     p : prime number p
%     q : prime number q
function [p,q] = rsa_pq(bits)
MaxModulo = 2.^bits;
prime_table = primes(MaxModulo);
len = length(prime_table);
i = floor(len / 10);
% find prime number "p"
p = floor(MaxModulo / prime_table(i));
while ~isprime(p) & i<len,
   i = i + 1;
   p = floor(MaxModulo / prime_table(i));
end;
% find prime number "q"
q = prime_table(i);


% rsa_key(p,q) : generate Key for RSA Algorithm
%    [PrivateKey, PublicKey, Modulo] = rsa_key(p,q)
%    PrivateKey :
%    PublicKey :
%    Modulo :
function [PrivateKey, PublicKey, Modulo] = rsa_key(p,q)
Modulo = p .* q;
prime_table = primes(Modulo);
len = length(prime_table);
p_q_ = (p-1) .* (q-1);
% find Private key
i = len;
while mod(p_q_,prime_table(i)) == 0,
   i = i - 1;
end;
PrivateKey = prime_table(i);
```

```
% find Public key
PublicKey = prime_table(floor(len/3));
while mod(PrivateKey.*PublicKey-1,p_q_) > 0,
   PublicKey = PublicKey + 1;
end;


% rsa : Encryption/Decryption with RSA Algorithm
%   Cipher = rsa(Plain, Key, Modulo)
%     is RSA encryption/decryption for Plain text with Key and Modulo
%   Cipher : MxN doubles : Cipher Code
%   Plain  : MxN doubles : Plain Text or Code
%   Key    : integer+    : Private key for encryption or Public key for
decryption
%   Modulo : integer+    : Modulo in algorithm
%
function Cipher = rsa(Plain, Key, Modulo)
Message = double(Plain);
mx = max(max(Message)); % find largest value of message
if length(factor(Modulo)) ~= 2
   error('RSA Modulo error ! : Modulo is not factor of 2 prime number')
elseif mx > Modulo
   error('RSA Modulo error ! : Modulo is less than some value of
Message ')
else
   Cipher = ones(size(Message));
   KeyBinary = dec2bin(Key);
   KeyBitLength = length(KeyBinary);
   for index = 1:KeyBitLength,
      Cipher = mod(Cipher.*Cipher, Modulo);
      if KeyBinary(index) == '1'
         Cipher = mod(Cipher.*Message, Modulo);
      end; % if
   end; % for
end; % if
```

ก.4 การตรวจหาลายน้ำดิจิตอลในรูปภาพ

```
% Correlation Function
function result = Corr(X,Y)
[m,n] = size(X);
d = m.*n-1;
X_ = mean(mean(X));
Vx = (X - X_);
Sx = sqrt(sum(sum(Vx.^2)) ./ d);

Y_ = mean(mean(Y));
Vy = Y - Y_;
Sy = sqrt(sum(sum(Vy.^2)) ./ d);

if (Sx.*Sy) == 0
   result = 0;
else
   result = (sum(sum(Vx.*Vy))./(Sx.*Sy)) ./ d;
end;
```

```
function Result = detect(img, noise);
[M, N] = size(img);
[m, n] = size(noise);
d = 10;
a = M-m+1;
b = N-n+1;
Result = zeros(round(a / d), round(b / d));
x = 0;
for i = 1:d:a,
   x = x + 1;
   y = 0;
   for j = 1:d:b,
      y = y + 1;
      Result(x, y) = corr(img(i:i+m-1, j:j+n-1), noise);
   end;
end;
```

ก.5 การเปรียบเทียบลักษณะเฉพาะสัมพัทธ์

```
function Right = compare(X,Y)
[m,n] = size(X);
comp = ...
[0,0,1,1,2,2,3,3,4,4,5,5,6,6,7,7;
 0,0,0,1,1,2,2,3,3,4,4,5,5,6,6,7;
 1,0,0,0,1,1,2,2,3,3,4,4,5,5,6,6;
 1,1,0,0,0,1,1,2,2,3,3,4,4,5,5,6;
 2,1,1,0,0,0,1,1,2,2,3,3,4,4,5,5;
 2,2,1,1,0,0,0,1,1,2,2,3,3,4,4,5;
 3,2,2,1,1,0,0,0,1,1,2,2,3,3,4,4;
 3,3,2,2,1,1,0,0,0,1,1,2,2,3,3,4;
 4,3,3,2,2,1,1,0,0,0,1,1,2,2,3,3;
 4,4,3,3,2,2,1,1,0,0,0,1,1,2,2,3;
 5,4,4,3,3,2,2,1,1,0,0,0,1,1,2,2;
 5,5,4,4,3,3,2,2,1,1,0,0,0,1,1,2;
 6,5,5,4,4,3,3,2,2,1,1,0,0,0,1,1;
 6,6,5,5,4,4,3,3,2,2,1,1,0,0,0,1;
 7,6,6,5,5,4,4,3,3,2,2,1,1,0,0,0;
 7,7,6,6,5,5,4,4,3,3,2,2,1,1,0,0];
X_Right = X+1;
Y_Right = Y+1;
for i=1:m
   for j=1:n
      Right(i,j) = comp(X_Right(i,j),Y_Right(i,j));
   end;
end;
```

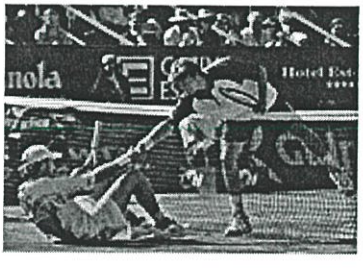
ภาคผนวก ข.
ตัวอย่างรูปภาพที่ใช้ในการทดลอง

ในงานวิจัยนี้ผู้วิจัยได้รวบรวมรูปภาพเพื่อนำมาทำการทดลองตามขั้นตอนการทดลองข้างต้น โดยทำการเลือกรูปภาพดิจิตอลที่มีลักษณะตรงตามเงื่อนไขที่กำหนด คือเป็นภาพที่ได้จากภาพถ่ายของคนสัตว์สิ่งของ ครอบคลุมลักษณะต่างของรูปภาพที่มีความละเอียดน้อยจนถึงมาก และระดับความสว่างแตกต่างกันน้อยจนถึงมาก ดังรูปภาพดังต่อไปนี้

1

2

3



4

5

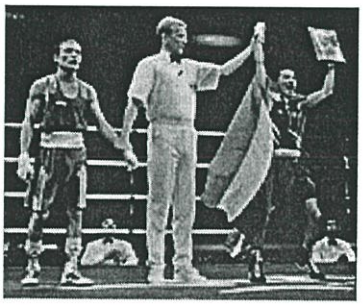
6

รูปที่ ข.1 ตัวอย่างภาพที่นำมาใช้ในการทดลองหมายเลข 1-6

7

8

9



10

11

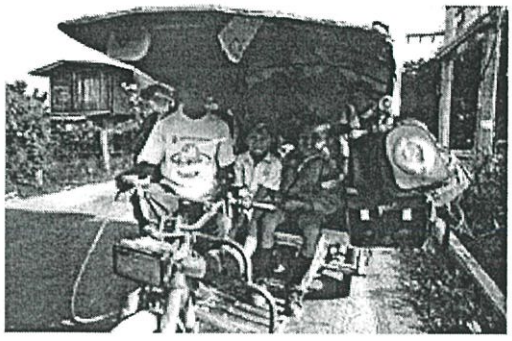
12

13

14

15

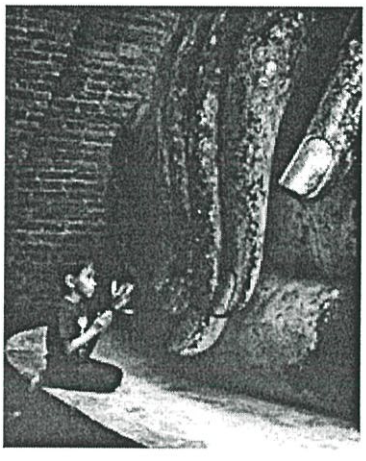
รูปที่ ข.2 ตัวอย่างภาพที่นำมาใช้ในการทดลองหมายเลข 7-15



16

17

18

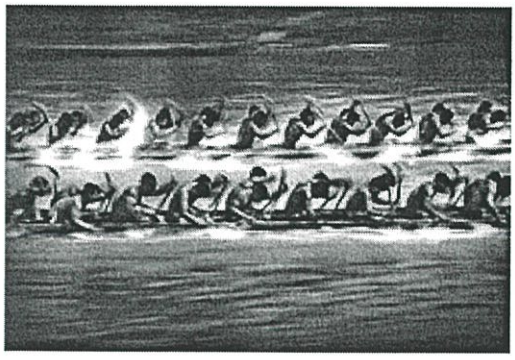


19

20

21

รูปที่ ข.3 ตัวอย่างภาพที่นำมาใช้ในการทดลองหมายเลข 16-21



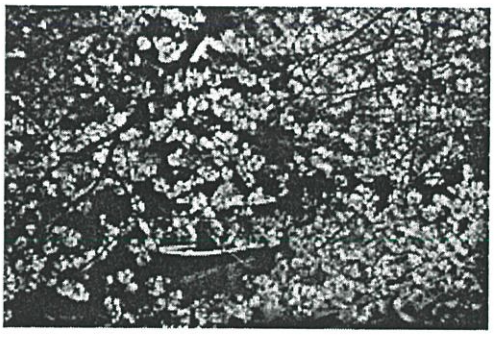
22

23

24

25

26



27

รูปที่ ข.4 ตัวอย่างภาพที่นำมาใช้ในการทดลองหมายเลข 22-27

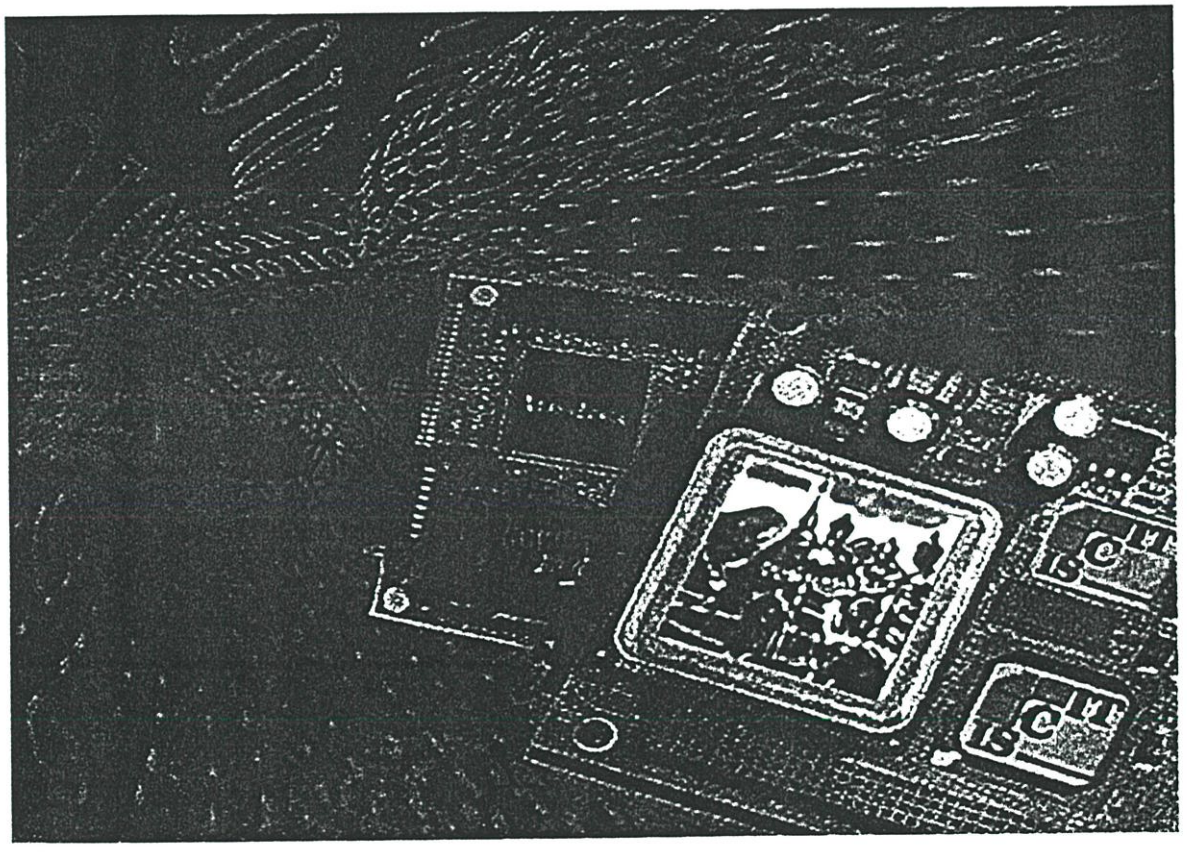
ภาคผนวก ค.
บทความและผลงานวิจัยที่ได้รับการตีพิมพ์

1. Wasin Sangiamkun and Nopporn Chotikakamthorn. "PARTIAL IMAGE AUTHENTICATION BY DIGITAL WATERMARKING" 2001 International Symposium on Communication and Information Technology (ISCIT 2001 Proceedings). pp.349-352

PROCEEDINGS

2001 International Symposium on Communications and Information Technology

ISCIT 2001



The Merging Decade of
Communication Systems and Information Technology

November 14 - 16, 2001

Chiang Mai Orchid Hotel, Chiang Mai, Thailand

ISCIT 2001 EIC JICA IEEE Thailand Section

PARTIAL IMAGE AUTHENTICATION BY DIGITAL WATERMARKING

Wasin Sangiamkun and Nopporn Chotikakamthorn

Faculty of Information Technology
King Mongkut's Institue of Technology Ladkrabang
Address Chalongkrung Rd. Lardkrabang Bangkok 10520
Phone:+66-1-476-2007
Email: s9067032@kmitl.ac.th

ABSTRACT

In this paper, The problem of image authentication by means of digital watermarking is considered. A new image verification scheme based on the test of relative similarity between neighbouring blocks of image is proposed. The method differs from other work which uses similar measure in the way and image signature being tighly tied with each part of the image to be verified. In addition, due to limited bandwidth available. Our proposed scheme can deal with this bandwidth authentication region tradeoff, by allowing for variable size regions of authentication. Experimental result are included.

1. INTRODUCTION

Digital watermarking is a way of embedding digital signal into a 'host' data in such a way that human perceptual property of the host data isn't significantly altered. This technique is widely used for copyright protection, authentication, tamper detection depend on the implementation and the requirement. The propose method is focus on digital image, the most proliferate media being copyright violated and easily forged.

Main problem in this research topic is the binary definition of digital security technique is too strict and not well adapted to digital image. In real world, image pixel values can be changed by many of manipulation such as brightness/contrast, format conversion, compression, etc. But the actual semantic meaning isn't modified.

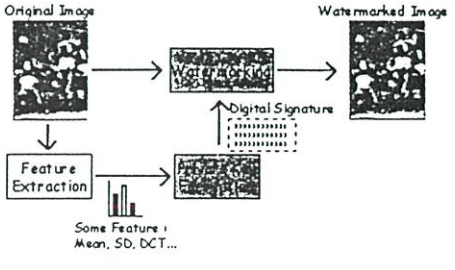
Most methods currently proposed to provide image authentication are based on a fragile or semifragile watermark. The basic idea is to insert a watermark that is easily destroyed or altered as a result of image manipulation. By extracting the damaged watermark, it is possible to detect data manipulation. The major drawbacks of these approaches is that it is difficult to distinguish between malicious and common manipulation. And it is easily for malicious party to remove it from host data before manipulation. By adding back the watermark into the modified host data, alteration can not be detected.

There is a alternative approach[1][2][4], A watermark is used as a means for embedding digital signature which is generated from image features. The modified version of standard digital signature scheme is applied for signature generation and verification process. The main advantage of those methods is that they allow for a more robust and precise detection the tampered region. Our method is different from one cited in some ways. For example, the use of relative similarity between features corresponding to adjacent blocks of image for signature construction and verification are detailed here. In addition, the proposed method allows for a detection resolution to be varied across the image.

This paper is organized as follows; an image authentication scheme based on relative block similarity measure is first described in Sect.2 In Sect.3, a spread-spectrum based data embedding scheme[3] developed for image authentication is detailed. In subsequent section, some experimental results are given. Discussions and concluding remarks are provide in Sect.5.

2. PROPOSED SCHEME

In this paper, we consider the problem of grayscale image authentication. Here, an image is regarded as authentic if its appearance is visually the same as the original created image. Inevitably, the definition is subject to individual judgement. However, given the purpose of image under interest, as well as their context, it should be quite clear what one means by saying that two images are identical or different. In this paper, we are only interested in fact or information an image convey to us, not its esthetic aspect.



(a) Digital Signature Watermarking

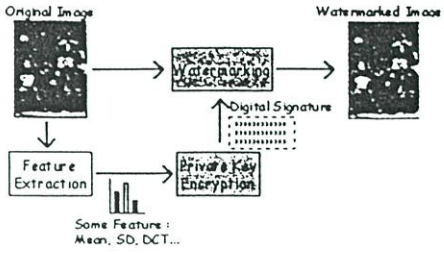


Figure 1
Proposed image watermark scheme

Figure 1 shows the basic idea of our method. First, we extract features from the original image, encrypt and then hide them using a robust and invisible watermark technique. Then, in order to check whether and image has been altered, we simply compare its feature with those of the original image recovered from the watermark.

2.1 Feature Extraction

The choice of image features used will directly affect the type of image alterations that we wish to be able to detect. Additionally, those features will depend on the type of image under consideration. The features are typically selected so that invariant properties are maintained under weak image alterations (lossy compression), noise (watermark) and broken for malicious manipulations.

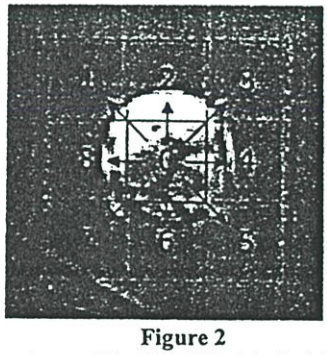


Figure 2
Image Blocking (20x20 pixels).

To achieve these requirements. We first select the significant region or interested object to be protected in image. Then divide it into non-overlapping blocks (Figure 2). For each block, calculate the mean of pixel luminance. Instead of constructing the image's signature directly, we propose to use a feature set obtained by comparing block mean luminance of center block with these of eight adjacent blocks (Eq. 1). The relation between each pair of comparison is quantized to one of represented by 16 different levels. (Eq.2).

$$\tilde{f}_{0,i} = \frac{f_0 - f_i}{\max(\text{luminance})} \qquad (1)$$

$$encode(\tilde{f}_{o,i}) = \begin{cases} 0 & \tilde{f}_{o,i} \le -0.32 \\ 1 & \tilde{f}_{o,i} \le -0.24 \\ 2 & \tilde{f}_{o,i} \le -0.16 \\ \cdot & \\ \cdot & \\ 13 & \tilde{f}_{o,i} \le 0.24 \\ 14 & \tilde{f}_{o,i} \le 0.32 \\ 15 & \tilde{f}_{o,i} > 0.32 \end{cases} \qquad (2)$$

2.2 Watermarking Technique

In this section, we describe method to embed the feature obtained from previous topic. We combine the 36 bits feature with watermark header (block-size, block-coordinate), as shows in figure 3. We can adjust the block-size and position of feature relative with the watermark. So the final feature will be 48 bits string. It will be encrypted by Private-Key encryption such as RSA. Then this signature is embedded into original image. A bit of signature is spreaded by pseudo noise modulation. This technique make the signature more robust against image manipulation. The large spreading code has more robustness but the limitation of host size or image resolution is the trade off. We find the smallest spreading code size in our experiments and found that the appropriate size is 140x140 or 160x160 pixel. (Eq.3). The watermark appearance look like weakened noise in protected image (Figure 4).

101001010 . . . 01001 1000 0001 0001
(a) (b) (c) (d)

Figure 3
Feature Structure
(a) Relative Block Feature (36 bits)
(b) Feature Block Size (4 bits)
(c) Vertical coordinate of feature (4 bits)
(d) Horizontal coordinate of feature (4 bits)

Define :
I' : Matrix M x N represent Watermarked Image
I : Matrix M x N represent Original Image
P_{ij} : Pseudo Noise | P ∈ {1,-1}, Mean(P) ≈ 0
S : Scaling Factor
D_i : Signature | D ∈ {1,-1}
W : Matrix m x n represent Watermark

$$W = D_i * P_{i,j} * S$$
$$I' = I + W \qquad (3)$$

Note the here * denotes an element-wise matrix product.

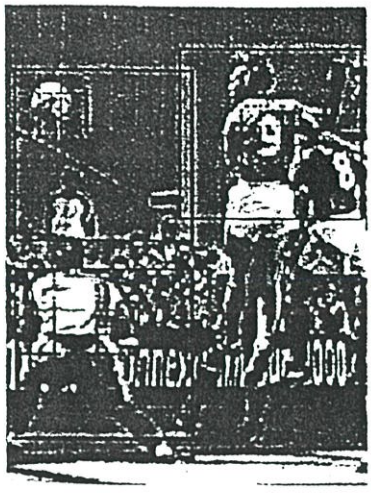


Figure 4
Protected image that contain 3 watermark (show by 3 rectangle.

Figure 4 shows an example of watermark image. Solid line and dot line show the positions of watermarks and features in the image. Three regions of image is protected, the ball, the player on the left, and the one on the right. The feature position is identified in signature. The ball and on-the-right player watermark is top-left feature. The on-the-right player is center feature.

2.3 Watermark Detection

In verification process, The viewer uses pseudo-noise sequence that is same as the one used duries watermarking process. While sliding through all regions of image, calculate the correlation between pseudo-noise and image pixels. The region that containing watermark will response with high value of correlation. (Figure 5)

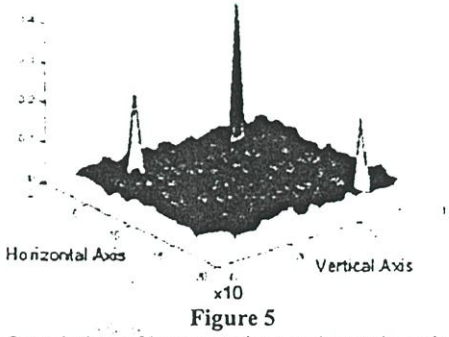
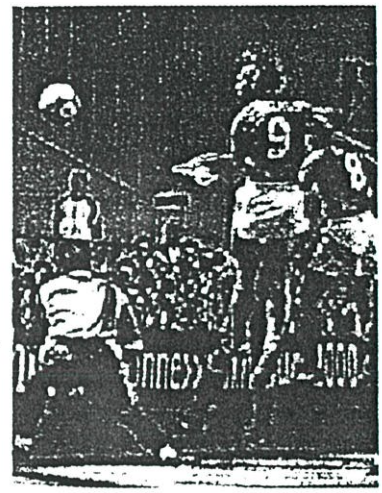


Figure 5
Correlation of image regions and pseudo-noise

Then, the signature will be recovered by noise re-modulation. Then it will be decrypted by public key and this decrypted feature will be compared by the feature extracted from verified image.

3. EXPERIMENT RESULT

Figure 6 shows our results using the previously described technique. In this example, the original image has been protected using the block mean luminance. We have removed the ball by cut and paste, Figure 6(b). Figure 6(c) show the regions that have been identified by our proposed method.

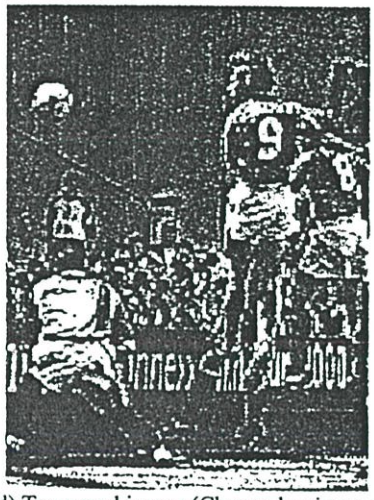


(a) Watermarked Image

(b) Tampered image (Remove Ball)

Figure 6
The Inzaghi Image (400x300 256 grayscale)

(c) Detection of altered region (#1).



(d) Tampered image (Change luminance)

(e) Detection of altered region (#2)

Figure 6 (con't)

4. CONCLUDING REMARKS

In this paper, the image authentication method based on relative similarity of neighboring block features has been proposed. Details on the construction of a signature representing the image have been provided. The proposed scheme has the advantages of being able to identify a modified portion of the image. Specially, it is suitable for the image that contains many objects. The significant region will be protected with the secure and robust watermarking. The method allows for more flexibility in trading between image quality degradation, security and tolerance level, and the data embedding capacity. Experimental results have been provided to demonstrate the performance of the proposed works.

Acknowledgement

This work was partly supported by Japan International Cooperation Agency (JICA)

REFERENCES

[1] Zhu, B., Swanson, M., Tewfik, A. "Transparent Robust Authentication and Distortion Measurement Technique for Images." Proc. IEEE Signal Processing Workshop. (1996) 45-48.

[2] Marc Schneider and Shih-Fu Chang. "A Robust Content Based Digital Signature for Image Authentication." IEEE-TIP. Vol.3, pp.227-230. 1996.

[3] Ingemar J. Cox. et.al. "Secure Spread Spectrum Watermarking for Multimedia." IEEE-TIP. Vol.6, No.12, pp.1673-1687, December 1997.

[4] Jiri Fridrich. "Image Watermarking for Tamper Detection." IEEE-ICIP. Vol.2, pp.404-408. 1998.

[5] Won-Gyum Kim, Jong C. Lee and Won D. Lee. "An Image Watermarking Scheme with Hidden Signatures." IEEE-ICIP. Vol.2, pp.206-210. 1999.

[6] Christian Rey and Jean-Luc Dugelay. "Blind Detection of Malicious Alterations on Still Images Using Robust Watermarks." The Institution of Electrical Engineers., Savoy Place, London WC2R 0BL, UK. 2000.

ประวัติผู้เขียน

ชื่อผู้เขียน	นายวศิน เสงี่ยมกุล
วัน/เดือน/ปี เกิด	24 ธันวาคม พ.ศ. 2516
วุฒิการศึกษาระดับปริญญาตรี	วิทยาศาสตรบัณฑิต (วท.บ.) สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ปีการศึกษา 2539
ประสบการณ์ในการทำงาน	นักวิชาการคอมพิวเตอร์ ฝ่ายระบบและโปรแกรม สำนักวิจัยและบริการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหาร ลาดกระบัง (สจล.) ปี พ.ศ. 2540 - 2544
	โปรแกรมเมอร์ ฝ่ายระบบสารสนเทศ บริษัท เนชั่นแนลไทย จำกัด 101 หมู่ 2 ถ.เทพารักษ์ ต.บางเสาธง กิ่งอำเภอบางเสาธง สมุทรปราการ 10540 ปี พ.ศ. 2544 - ปัจจุบัน