

เทคนิคการซ่อนลายน้ำสำหรับภาพดิจิทัลในโดเมนดีซีที

DCT-DOMAIN WATERMARKING TECHNIQUE
FOR DIGITAL IMAGES



ยุทธพงศ์ ฐิติมัจฉิมา

YUTTHAPONG THITIMAJSHIMA



เลขหม.....
เลขทะเบียน..... 47708
วัน, เดือน, ปี..... 22 ส.ค. 2546

.b.....
.i.....

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาเทคโนโลยีสารสนเทศ

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2546

ISBN 974-324-457-3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

**DCT-DOMAIN WATERMARKING TECHNIQUE
FOR DIGITAL IMAGES**



**A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
SCHOOL OF GRADUATE STUDIES
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG**

2003

ISBN 974-324-457-3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



COPYRIGHT 2003

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

หัวข้อวิทยานิพนธ์	เทคนิคการซ่อนลายน้ำสำหรับภาพดิจิทัลในโดเมนซีที
นักศึกษา	นายยุทธพงศ์ ฐิติวัชฌิมา
รหัสนักศึกษา	43067013
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2546
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ.ดร.นพพร โชติกคำธร
อาจารย์ผู้ควบคุมวิทยานิพนธ์ร่วม	รศ.ดร.ยุทธพงษ์ รั้งสรรค์เสรี

บทคัดย่อ

ในหลายปีที่ผ่านมา การซ่อนลายน้ำดิจิทัลได้ถูกนำมาใช้เพื่อใช้ประโยชน์ในการป้องกันการละเมิดลิขสิทธิ์บนสื่อดิจิทัล เช่น ภาพ เสียง และข้อมูลสื่อผสม ในสภาพแวดล้อมของเครือข่ายซึ่งสามารถกระจายส่งต่อถึงกันอย่างรวดเร็วและ ง่ายตาย เนื่องจากลายน้ำสามารถบ่งบอกถึงความเป็นเจ้าของสื่อเหล่านั้นได้ ในวิทยานิพนธ์นี้เสนอเทคนิคการซ่อนลายน้ำโดยการฝังภาพสัญลักษณ์ลับดิจิทัล 2 มิติแบบไบนารีในภาพดิจิทัลต้นฉบับ ซึ่งเทคนิคนี้การฝังลายน้ำจะกระทำในโดเมนความถี่ของภาพโดยเลือกใช้โดเมนซีทีในการฝังลายน้ำ เทคนิคนี้ไม่จำเป็นต้องใช้ภาพต้นฉบับในการนำภาพสัญลักษณ์ลับกลับมา ผลที่ได้จากการทดลองแสดงให้เห็นว่าเทคนิคการซ่อนลายน้ำแบบนี้มีความคงทนต่อการถูกกระทำในรูปแบบต่าง ๆ เช่น การบีบอัดข้อมูลแบบ JPEG, การกรองความถี่, การใส่สัญญาณรบกวนแบบเกาส์เซียน และการตัดบางส่วนของภาพโดยที่ยังคงนำภาพสัญลักษณ์ลับกลับคืนมาได้

Thesis Title	DCT-domain watermarking technique for digital images
Student	Mr. Yutthapong Thitimajshima
Student ID.	43067013
Degree	Master of Science
Programme	Information Technology
Year	2003
Thesis Advisor	Asst.Prof.Dr. Nopporn Chotikakamthorn
Co. Thesis Advisor	Assoc. Prof. Dr. Yutthapong Rangsanseri

ABSTRACT

In recent years, digital watermarking has been introduced as a means of effectively protecting copyrights on the digitized media such as image, audio and multimedia data in a networked environment, since it makes possible to identify the owner of a document.. In this thesis, we present a watermarking technique for hiding a confidential two-dimension binary watermark into a digital image. Our technique is applied to the frequency domain of the image. The DCT domain is chosen for watermarking. Additionally, this technique does not require original image to recover the embedded signature. Experimental results show that the proposed watermarking technique is robust to various kinds of attacks against JPEG compression, filtering, noises and cropping.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องจากได้รับความอนุเคราะห์ และความช่วยเหลือ ให้ความรู้ คำแนะนำ แนวทางในการวิจัย และแนวทางการแก้ไขปัญหาต่างๆ เป็นอย่างดีจาก รศ.ดร.ยุทธพงษ์ รังสรรค์เสรี อาจารย์ผู้ควบคุมวิทยานิพนธ์ร่วม และผศ.ดร.นพพร โชติกคำธร อาจารย์ผู้ควบคุมวิทยานิพนธ์

ขอขอบพระคุณท่านกรรมการสอบทุกท่านที่ได้สละเวลาอันมีค่าในการตรวจสอบวิทยานิพนธ์ในครั้งนี้ และช่วยแก้ไขวิทยานิพนธ์ฉบับนี้ให้สมบูรณ์ยิ่งขึ้น

ขอขอบคุณคุณแม่ และครอบครัวที่คอยดูแลเอาใจใส่ ให้ความช่วยเหลือ และเป็นกำลังใจที่ดีมาโดยตลอด

ขอขอบคุณ อาทิว ฟันฐู พี่ประพนธ์ บุ่ม เบ็ด น้อย กอร์ฟ พี่เอ็บเบ็ด ที่ให้ความช่วยเหลือด้านต่างๆ และเป็นกำลังใจตลอดมา

คุณค่าและประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอบมอบแต่ผู้มีพระคุณทุกท่าน



ยุทธพงษ์ รังสรรค์เสรี

สารบัญ

	หน้า
บทคัดย่อภาษาไทย.....	I
บทคัดย่อภาษาอังกฤษ.....	II
กิตติกรรมประกาศ.....	III
สารบัญ.....	IV
สารบัญรูป.....	VI
สารบัญตาราง.....	IX
บทที่ 1 บทนำ.....	1
1.1 ที่มาของงานวิจัย.....	1
1.2 วัตถุประสงค์ของงานวิจัย.....	2
1.3 ขอบเขตของงานวิจัย.....	3
1.4 เนื้อหาของวิทยานิพนธ์.....	3
บทที่ 2 เทคโนโลยีการซ่อนลายน้ำ.....	5
2.1 ภาพดิจิทัล.....	5
2.2 ประวัติและความเป็นมาของการซ่อนลายน้ำ.....	6
2.3 เทคโนโลยีการซ่อนลายน้ำดิจิทัล.....	10
2.4 คุณสมบัติที่ต้องการของการซ่อนลายน้ำ.....	17
2.5 ข้อกำหนดของความคงทน.....	18
2.6 เทคโนโลยีสำหรับการป้องกันการละเมิดลิขสิทธิ์.....	21
2.7 การประยุกต์ใช้เทคนิคการซ่อนลายน้ำ.....	24
บทที่ 3 เทคนิคการซ่อนลายน้ำในโดเมนความถี่สำหรับภาพดิจิทัล.....	28
3.1 การสร้างสัญญาณลายน้ำดิจิทัล.....	28
3.2 กระบวนการซ่อนลายน้ำด้วยเทคนิคการแปลงฟูริเยร์.....	29
3.3 กระบวนการซ่อนลายน้ำด้วยเทคนิคดีสครีต โคซายน์ทรานส์ฟอร์ม.....	34
3.4 การวัดประสิทธิภาพของอัลกอริทึม.....	39

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

	หน้า
บทที่ 4 ผลการทดลอง.....	43
4.1 ผลการทดลองเมื่อใช้เทคนิคการแปลงฟูริเยร์.....	43
4.2 ผลการทดลองเมื่อใช้เทคนิคดิสครีต โคซายน์ทรานส์ฟอร์ม.....	50
4.3 การทดสอบความคงทนของลายน้ำ.....	57
บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ.....	78
5.1 สรุปผลการวิจัย.....	78
5.2 ปัญหาที่พบและข้อเสนอแนะ.....	81
เอกสารอ้างอิง.....	83
ภาคผนวก.....	85
- ภาคผนวก ก. ผลงานวิจัยที่ได้รับการตีพิมพ์.....	86
ประวัติผู้เขียน.....	91

สารบัญรูป

รูปที่	หน้า
2.1	การสร้างภาพดิจิทัลจากคอมพิวเตอร์และการจับภาพจากโลกความจริง.....6
2.2	การนำข้อมูลดิจิทัลไปขายเพื่อผลทางการค้า.....8
2.3	การคัดแปลงหรือลักลอบแทรกสัญญาณ.....8
2.4	การบิดเบือนของสัญญาณ.....9
2.5	ประเภทของเทคนิคการซ่อนลายน้ำภาพดิจิทัล.....13
2.6	(ก) การใส่ลายน้ำดิจิทัลลงไปในบริเวณมุมขวาล่างของรูปภาพ (ข) การใส่ลายน้ำดิจิทัลไปในบริเวณกลางรูปภาพ.....14
2.7	กระบวนการฝังลายน้ำ.....15
2.8	การเผยแพร่ข้อมูลที่มีการฝังลายน้ำ.....15
2.9	กระบวนการตรวจหาลายน้ำกลับคืน.....16
2.10	การประยุกต์ใช้เทคนิคการทำลายน้ำ.....25
3.1	กระบวนการฝังลายน้ำดิจิทัลด้วยเทคนิคการแปลงฟูรีเยร์.....31
3.2	กระบวนการตรวจหาลายน้ำจากการฝังลายน้ำด้วยเทคนิคการแปลงฟูรีเยร์.....33
3.3	การเรียงลำดับของสัมประสิทธิ์ DCT ใหม่ในรูปแบบของซิกแซกสแกน.....35
3.4	กระบวนการฝังลายน้ำดิจิทัลด้วยเทคนิคดิสครีตโคไซน์ทรานส์ฟอร์ม.....37
3.5	กระบวนการตรวจหาลายน้ำจากการฝังลายน้ำด้วยเทคนิคดิสครีตโคไซน์ทรานส์ฟอร์ม.....39
4.1	(ก) ภาพต้นฉบับ Lena ขนาด 512x512 พิกเซล ภาพสัญญาณกลับขนาด 128x128 พิกเซล และภาพสัญญาณกลับขนาด 512x512 พิกเซลที่ได้จากการปรับขนาด (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้ว ภาพลายน้ำที่นำกลับคืน และภาพลายน้ำที่นำกลับคืน และทำการปรับขนาด เมื่อกำหนดให้ α เท่ากับ 5500.....44
4.2	(ก) ภาพต้นฉบับ Airplane ขนาด 512x512 พิกเซล ภาพสัญญาณกลับขนาด 128x128 พิกเซล และภาพสัญญาณกลับขนาด 512x512 พิกเซลที่ได้จากการปรับขนาด (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้ว ภาพลายน้ำที่นำกลับคืน และภาพลายน้ำที่นำกลับคืน และทำการปรับขนาด เมื่อกำหนดให้ α เท่ากับ 5500.....45
4.3	(ก) ภาพต้นฉบับ Lena และภาพสัญญาณกลับขนาด ขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.2 (ค) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.3 (ง) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.5...46

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญรูป (ต่อ)

รูปที่	หน้า
4.4 (ก) ภาพต้นฉบับ Boat และภาพสัญลักษณ์ลับขนาด ขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.2 (ค) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.3 (ง) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.5	48
4.5 (ก) ภาพต้นฉบับขนาด 512x512 พิกเซล โทนสีเทา 8 บิต และภาพสัญลักษณ์ลับ ขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 30	51
4.6 (ก) ภาพต้นฉบับขนาด 512x512 พิกเซล โทนสีเทา 8 บิต และภาพสัญลักษณ์ลับขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 30	52
4.7 ภาพต้นฉบับขนาด 512x512 พิกเซล โทนสีเทา 8 บิต จำนวน 6 ภาพ	53
4.8 ภาพสัญลักษณ์ลับขนาด 128x128 พิกเซล	54
4.9 ภาพต้นฉบับที่ฝังลายน้ำแล้วและภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน	55
4.10 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากการนำลายน้ำกลับคืน	57
4.11 ภาพลายน้ำที่ผ่านการบีบอัดข้อมูลแบบ JPEG โดยคุณภาพของภาพเท่ากับ 50% และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน	58
4.12 ภาพลายน้ำที่ผ่านการบีบอัดข้อมูลแบบ JPEG โดยคุณภาพของภาพเท่ากับ 20% และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน	61
4.13 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจาก ผ่านการบีบอัดข้อมูลแบบ JPEG	63
4.14 กราฟเปรียบเทียบค่า NC เฉลี่ยของทุกภาพที่ตรวจสอบได้จากภาพลายน้ำที่นำ กลับคืนหลังจากผ่านการบีบอัดข้อมูลแบบ JPEG	64
4.15 ภาพลายน้ำที่ผ่านการกรองความถี่แบบ 3x3 averaging filter และภาพสัญลักษณ์ลับ ที่ได้จากการนำลายน้ำกลับคืน	64
4.16 ภาพลายน้ำที่ผ่านการกรองความถี่แบบ 3x3 Median Filter และภาพสัญลักษณ์ลับ ที่ได้จากการนำลายน้ำกลับคืน	57

สารบัญรูป (ต่อ)

รูปที่	หน้า
4.17 (ก) กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืน หลังจากผ่านการกรองความถี่แบบ 3x3 averaging filter (ข) กราฟเปรียบเทียบ ค่า NC ของภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืนหลังจากผ่าน การกรองความถี่แบบ 3x3 median filter.....	69
4.18 ภาพลายน้ำที่ผ่านการใส่สัญญาณรบกวนเกาซ์เซียน และภาพสัญลักษณ์ลับที่ได้ จากการนำลายน้ำกลับคืน.....	70
4.19 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจาก ผ่านการใส่สัญญาณรบกวนเกาซ์เซียน.....	72
4.20 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจาก ทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10%.....	73
4.21 กราฟเปรียบเทียบค่า NC เฉลี่ยของทุกภาพที่ตรวจสอบได้จากภาพลายน้ำที่ นำกลับคืนหลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10%.....	74
4.22 ภาพลายน้ำที่ผ่านการตัดบางส่วนของภาพ โดยมีพื้นที่ของภาพเหลือเพียง 25% และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน.....	74
4.23 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากผ่าน การตัดบางส่วนของภาพ โดยมีพื้นที่ของภาพเหลือเพียง 25%.....	77
5.1 อธิบายลักษณะของการรวมกันของพลังงานระหว่างเทคนิคคีสคริต โทชานน์ ทรานส์ฟอร์มและคีสคริตฟูรีเยร์ทรานส์ฟอร์ม.....	80

สารบัญตาราง

ตารางที่	หน้า
4.1 ค่า NC ของภาพถ่ายน้ำที่ได้หลังจากทำการบีบอัดข้อมูลแบบ JPEG ด้วย quality factors ที่แตกต่างกัน.....	58
4.2 ค่า NC ของภาพถ่ายน้ำที่ได้หลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10%.....	73
5.1 ตารางเปรียบเทียบผลการทดลองที่ได้จากการคำนวณการช่อนลายน้ำทั้ง 2 วิธี.....	79



บทที่ 1

บทนำ

1.1 ที่มาของงานวิจัย

สื่อผสมแบบดิจิทัลเป็นเทคโนโลยีที่รวมเอาสื่อข้อมูลดิจิทัลหลากหลายรูปแบบเข้ามาไว้ด้วยกันเพื่อที่จะนำไปใช้งานกับโปรแกรมคอมพิวเตอร์ ทำให้การสื่อสารและใช้งานคอมพิวเตอร์มีความน่าสนใจมากยิ่งขึ้น ดังนั้นจึงเกิดการขยายตัวของกลุ่มผู้ใช้งานคอมพิวเตอร์ และธุรกิจบนระบบเครือข่าย ซึ่งในปัจจุบันกลุ่มผู้ใช้งานเทคโนโลยีดังกล่าวจะครอบคลุมตั้งแต่ระดับองค์กร ธุรกิจที่อาจจะใช้ในการแสดงผลของงานที่ทำหรือออกแบบ เช่น โฆษณา ไปจนถึงระดับครัวเรือน ที่เน้นการใช้งานในด้านความบันเทิงเป็นหลัก

ในปัจจุบันสื่อผสมแบบดิจิทัลเช่น วิดีโอ รูปภาพ และเสียง ได้ถูกนำมาใช้อย่างกว้างขวาง สามารถกระจายส่งถึงกันได้อย่างรวดเร็วและง่ายดายขึ้นตามการพัฒนาและเติบโตของระบบเครือข่ายคอมพิวเตอร์ โดยเฉพาะการใช้งานเครือข่าย World Wide Web ที่ใช้กันอย่างกว้างขวาง และถ้าหากข้อมูลนั้นๆ ถูกคัดลอกและเผยแพร่ต่อไปโดยมิได้รับอนุญาตจากเจ้าของข้อมูลเสียก่อน ก็จะทำให้เจ้าของข้อมูลที่แท้จริงเสียผลประโยชน์ที่พึงจะได้รับ ซึ่งจะมีผลกระทบต่อระบบเศรษฐกิจ และการทำธุรกรรมบนอินเทอร์เน็ตที่มีการพัฒนากันอย่างกว้างขวางในปัจจุบัน ดังนั้นเพื่อยับยั้งการละเมิดสิทธิของเจ้าของข้อมูลโดยมิชอบธรรม จึงจำเป็นที่จะต้องมีการคุ้มครองการใช้งานของข้อมูลที่เกี่ยวข้องกับสิทธิทางปัญญา โดยมิให้ผู้ที่ไม่ได้เป็นเจ้าของข้อมูลนั้นๆ นำข้อมูลไปใช้โดยมิได้รับอนุญาต ซึ่งก็คือการจดลิขสิทธิ์ที่จะเป็นหลักฐานในการยืนยันถึงความเป็นเจ้าของต่องานหนึ่งๆ

ลิขสิทธิ์ถือเป็นทรัพย์สินทางปัญญาประเภทหนึ่ง ที่กฎหมายให้ความคุ้มครองโดยให้เจ้าของผลงานถือสิทธิแต่เพียงผู้เดียวที่จะกระทำการใดๆ เกี่ยวกับงานสร้างสรรค์ที่ตนเองได้กระทำขึ้น งานสร้างสรรค์ที่ได้รับการคุ้มครองตามพระราชบัญญัติลิขสิทธิ์ ต้องเป็นงานในสาขาวรรณกรรม นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ รวมถึงงานอื่นๆ ในแผนกวรรณคดี วิทยาศาสตร์ หรือแผนกศิลปะ งานเหล่านี้ถือเป็นผลงานที่เกิดจากการใช้สติปัญญา ความรู้ความสามารถ และความวิริยะอุตสาหะ ในการสร้างสรรค์งานให้เกิดขึ้น ซึ่งถือเป็นทรัพย์สินทางปัญญาที่มีคุณค่าทางเศรษฐกิจ

เนื่องจากหลายหน่วยงานได้เล็งเห็นถึงความสำคัญของปัญหาที่เกิดขึ้นจากการล่วงละเมิดลิขสิทธิ์ทางปัญญาในสื่อประเภทต่างๆ และเล็งเห็นถึงความพยายามและความทุ่มเทเป็นอย่างมากในการสร้างสรรค์ผลงานในแต่ละชิ้นขึ้นมา จึงไม่เป็นการยุติธรรมที่บุคคลใดบุคคลหนึ่งที่จะเห็นแก่ประโยชน์ส่วนตัวลักลอบนำทรัพย์สินทางปัญญาเหล่านี้ไปใช้หรือนำไปเพื่อทำประโยชน์ทาง

เอกสารนี้เป็นเอกสารสงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ทางการค้า

ไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การค้าโดยไม่ได้รับอนุญาตจากผู้ที่เป็นเจ้าของผลงาน แม้ว่าในปัจจุบันจะมีกฎหมายปกป้องลิขสิทธิ์ทางปัญญาออกมาบังคับใช้อย่างชัดเจน แต่บางครั้งตัวบทกฎหมายที่มีอยู่ก็ไม่สามารถดำเนินการกับผู้กระทำผิดเหล่านั้นได้ง่าย เพราะรูปแบบของคดีที่จะมีการจับกุมและดำเนินคดีได้นั้นต้องมีเจ้าของลิขสิทธิ์แจ้งจับหรือเจ้าทุกข์เข้าร้องเรียนต่อเจ้าหน้าที่ แต่ในทางเป็นจริงนั้นเป็นไปได้ยากที่เจ้าของลิขสิทธิ์จะดูแลได้ทั่วถึง จึงเป็นการดีกว่าถ้าหากสามารถคิดค้นพัฒนาวิธีป้องกันการละเมิดลิขสิทธิ์ในตัวผลิตภัณฑ์ได้โดยตรง

อย่างไรก็ตามถึงแม้ว่าจะมีกลไกในการป้องกันการละเมิดลิขสิทธิ์หลากหลายวิธี เช่น การเข้ารหัส การลงทะเบียน หรือการใส่เลขทะเบียน ก็ยังไม่สามารถยับยั้งปัญหาดังกล่าวได้ ยกตัวอย่างในกรณีของการเข้ารหัสลับตัวข้อมูล ข้อมูลที่ผ่านการถอดรหัสแล้วจะสามารถถูกคัดลอกหรือทำซ้ำได้โดยที่เราไม่สามารถที่จะติดตามหาผู้ที่กระทำความผิดดังกล่าวมาลงโทษได้ ดังนั้นเพื่อที่จะยับยั้งหรือติดตามร่องรอยของการละเมิดลิขสิทธิ์ จึงได้มีแนวความคิดที่จะซ่อนสัญลักษณ์ลับเข้าไปในสื่อแบบดิจิทัลเพื่อใช้ในการตรวจสอบและแสดงว่าใครเป็นเจ้าของสื่อต่างๆจริง วิธีการในการซ่อนสัญลักษณ์ลับเข้าไปในสื่อเรียกว่า ลายน้ำดิจิทัล (Digital Watermarking) เพื่อยับยั้งการกระทำที่จะเป็นการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาของข้อมูลมัลติมีเดีย โดยวิธีการนี้จะแตกต่างจากวิธีการเข้ารหัสลับทั่วไปที่ข้อมูลภายหลังจากการเข้ารหัสจะสามารถดูได้โดยผู้ที่มีกุญแจรหัสเท่านั้น แต่วิธีดังกล่าวนี้จะใช้หลักการในการซ่อนสิ่งที่เรียกว่าสัญญาณลายน้ำ (Watermark Signal) ลงไปในข้อมูลมัลติมีเดีย โดยจะไม่ทำให้คุณภาพของข้อมูลนั้นๆ ลดต่ำจนเกินไป

1.2 วัตถุประสงค์ของงานวิจัย

วิทยานิพนธ์ฉบับนี้มีวัตถุประสงค์เพื่อประเมินการใช้งานของการซ่อนลายน้ำในภาพดิจิทัลเพื่อป้องกันการคัดลอก นำไปประยุกต์ใช้ในการเผยแพร่ข้อมูลดิจิทัล และเป็นการสร้างแนวทางใหม่สำหรับการทำงานที่มีประสิทธิภาพ และเป็นทางเลือกหนึ่งที่จะสามารถป้องกันการละเมิดลิขสิทธิ์ จากความเสี่ยงต่อการถูกละเมิดลิขสิทธิ์ได้ง่ายของภาพดิจิทัล โดยนำเสนอเทคนิคการซ่อนลายน้ำที่ทำงานในโดเมนความถี่สำหรับภาพดิจิทัล โดยมีการหาระดับของลายน้ำที่ฝังลงในภาพดิจิทัลให้เหมาะสม เพื่อให้มีความคงทนต่อเทคนิคการประมวลผลภาพและการลดทอนทางเรขาคณิตได้มากขึ้น รวมถึงการตรวจหาลายน้ำโดยไม่ต้องใช้ภาพต้นแบบ ซึ่งแตกต่างจากงานวิจัยก่อนหน้านี้ที่การตรวจหาลายน้ำดิจิทัลในภาพดิจิทัลมักต้องใช้ภาพต้นฉบับมาเปรียบเทียบกับภาพที่ต้องการตรวจหาลายน้ำ [1,2] ซึ่งเป็นการไม่สะดวกที่ต้องมีภาพต้นฉบับไว้เสมอในการตรวจหาลายน้ำ รวมถึงการเปรียบเทียบภาพที่มีลายน้ำและภาพต้นฉบับ ลายน้ำที่ได้และลายน้ำต้นฉบับซึ่งได้นำเสนออัลกอริทึมที่มีความคงทน มีมาตรฐานในการวัดค่าที่สามารถเป็นจุดเริ่มต้นที่ดีในการป้องกันข้อมูลภาพดิจิทัลกับปัญหาที่เกิดขึ้นในปัจจุบัน

1.3 ขอบเขตของงานวิจัย

ในงานวิจัยนี้เสนอวิธีการซ่อนลายน้ำภาพดิจิทัล โดยใช้การฝังภาพสัญญาณลับ 2 มิติ แบบไบนารีในภาพดิจิทัลต้นฉบับแบบโทนสีเทาด้วยเทคนิคการแปลงฟูริเยร์ (Fourier Transform) และเทคนิคโคไซน์ทรานส์ฟอร์ม (Discrete Cosine Transform) ลายน้ำจะถูกฝังลงในโดเมนความถี่ของภาพดิจิทัลต้นฉบับ โดยเทคนิคนี้ไม่จำเป็นต้องใช้ภาพต้นฉบับในการตรวจหาภาพสัญญาณลับกลับคืน ซึ่งทำให้กระบวนการในการถอดรหัสทำได้ง่ายและสะดวก ผลที่ได้จากการทดลองยังแสดงให้เห็นว่าเทคนิคการซ่อนลายน้ำแบบนี้มี ความคงทนต่อการประมวลผลสัญญาณภาพในรูปแบบต่างๆ โดยสามารถทดสอบประสิทธิภาพของลายน้ำภาพดิจิทัลด้วยวิธีการต่างๆ เช่น การบีบอัดข้อมูลภาพ การกรองภาพ และการตัดบางส่วนของภาพ เป็นต้น

1.4 เนื้อหาของวิทยานิพนธ์

ในวิทยานิพนธ์นี้ได้เสนอวิธีการซ่อนลายน้ำในภาพดิจิทัล โดยเนื้อหาต่อไปนี้ของวิทยานิพนธ์ฉบับนี้มีการจัดเรียงข้อมูลที่เน้นหลักการสำคัญดังต่อไปนี้ คือ

บทที่ 1 บทนำ

กล่าวถึง ที่มาของงานวิจัย วัตถุประสงค์ของงานวิจัย ขอบเขตของงานวิจัย และเนื้อหาต่างๆ ของวิทยานิพนธ์ฉบับนี้

บทที่ 2 เทคโนโลยีการฝังลายน้ำ

เบื้องต้นจะกล่าวถึงความหมายของภาพดิจิทัลเพื่อให้ทราบถึงที่มาและประเภทของภาพดิจิทัล ซึ่งทำให้เกิดแนวคิดของการซ่อนลายน้ำ ประวัติความเป็นมาของเทคโนโลยีการซ่อนลายน้ำภาพดิจิทัล การแบ่งประเภทของเทคนิคการซ่อนลายน้ำที่ได้มีการนำเสนอออกมา รูปแบบมาตรฐานของกระบวนการฝังลายน้ำ การเผยแพร่ของสื่อที่มีลายน้ำ รวมถึงการตรวจหาลายน้ำกลับคืน กล่าวถึงคุณสมบัติของการซ่อนลายน้ำภาพดิจิทัลที่ต้องการเพื่อให้กระบวนการซ่อนลายน้ำสามารถใช้งานได้อย่างมีประสิทธิภาพ เทคโนโลยีสำหรับการป้องกันการละเมิดลิขสิทธิ์กับสื่อต่างๆ ข้อกำหนดของความคงทนในการซ่อนลายน้ำภาพดิจิทัลและการประยุกต์ใช้ลายน้ำดิจิทัลกับงานประเภทต่างๆ

บทที่ 3 เทคนิคการซ่อนลายน้ำในโดเมนความถี่สำหรับภาพดิจิทัล

กล่าวถึง วิธีการในการสร้างสัญญาณลายน้ำ การซ่อนลายน้ำดิจิทัลสำหรับภาพโทนสีเทาในโดเมนความถี่ซึ่งกล่าวถึง 2 วิธีคือ กระบวนการซ่อนลายน้ำด้วยเทคนิคการแปลงฟูริเยร์ โดยจะแบ่งออกเป็น 2 ส่วน ประกอบด้วยการฝังลายน้ำลงในภาพดิจิทัลและการตรวจหาลายน้ำดิจิทัลกลับคืน และกระบวนการซ่อนลายน้ำด้วยเทคนิคโคไซน์ทรานส์ฟอร์ม โดยแบ่งเป็น 2 ส่วนเช่นเดียวกัน ประกอบด้วยการฝังลายน้ำลงในภาพดิจิทัลและการตรวจหาลายน้ำดิจิทัลกลับ

คืน สุกทำยเป็นการวัดประสิทธิภาพของอัลกอริทึมเป็นการคำนวณค่าความผิดพลาด และการคำนวณค่าเปรียบเทียบภาพลายน้ำที่ทำการฝังและที่ตรวจหาได้ เพื่อพิสูจน์ความสำเร็จของประสิทธิภาพอัลกอริทึมที่ดี

บทที่ 4 ผลการทดลอง

กล่าวถึง การซ่อนลายน้ำกับภาพดิจิทัลด้วยอัลกอริทึมที่นำเสนอ การตรวจหาลายน้ำ รวมถึงการทดสอบความคงทนของลายน้ำที่ผ่านเทคนิคในการประมวลผลสัญญาณภาพแบบต่างๆ และความผิดพลาดเชิงเรขาคณิต รวมถึงการคำนวณหาค่าความผิดพลาดและค่าเปรียบเทียบของภาพลายน้ำและภาพต้นฉบับต่างๆ ที่ได้ใช้ในการทดลอง

บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ

สรุปผลการทดสอบของการซ่อนลายน้ำและการตรวจหาลายน้ำแบบใหม่ที่ไม่จำเป็นต้องใช้ภาพต้นแบบตามอัลกอริทึมที่ได้นำเสนอ ที่ฝังลงบนภาพโทนสีเทาที่ผ่านการทดสอบด้วยเทคนิคต่างๆ พร้อมทั้งเสนอแนะแนวทางการวิจัยที่สามารถพัฒนาต่อไปได้ เพื่อให้นำไปใช้งานในงานจริงได้หลากหลายมากขึ้น สามารถนำไปใช้ในการพัฒนาอัลกอริทึมอื่นๆ เพื่อให้มีประสิทธิภาพมากยิ่งขึ้น

บทที่ 2

เทคโนโลยีการซ่อนลายน้ำ

การซ่อนลายน้ำ จัดเป็นงานทางด้านการประมวลผลสัญญาณภาพ (Image Processing) ซึ่งได้มีผู้ศึกษาเกี่ยวกับการซ่อนลายน้ำในรูปแบบต่างๆ เป็นจำนวนมาก เนื่องจากข้อดีหลายๆ อย่างของสื่อดิจิทัลเมื่อเทียบกับสื่ออื่นๆ ทำให้ความนิยมในการใช้สื่อดิจิทัลได้กระจายไปอย่างกว้างขวาง โดยข้อมูลดิจิทัลสามารถที่จะทำสำเนาขึ้นมาใหม่ให้เหมือนกับต้นฉบับได้ง่าย ซึ่งทำให้เกิดการละเมิดลิขสิทธิ์ได้ง่าย แนวทางการแก้ไขปัญหานี้ เราสามารถนำการฝังลายน้ำดิจิทัลซึ่งเป็นเทคโนโลยีใหม่ที่น่าหลักการในการวิจัยหลายๆ แขนงมาใช้ อย่างเช่น สเตเกโนกราฟี คริปโตกราฟี ทฤษฎีการสื่อสารและการประมวลผลสัญญาณ ในบทนี้จะนำเสนอเทคโนโลยีใหม่ที่ใช้ในการป้องกันลิขสิทธิ์ของสื่อดิจิทัล โดยพิจารณาในส่วนของวงจรประยุกต์ใช้ที่เป็นไปได้ ความต้องการในด้านต่างๆ ของการซ่อนลายน้ำ ส่วนประกอบที่สำคัญในการซ่อนลายน้ำประกอบด้วยภาพดิจิทัล ทฤษฎีในการฝังลายน้ำและนำลายน้ำกลับคืน โดยจะกล่าวแยกออกเป็นประเภทต่างๆ ตามเทคนิคการฝังลายน้ำกับภาพดิจิทัล ซึ่งมีดังต่อไปนี้

2.1 ภาพดิจิทัล

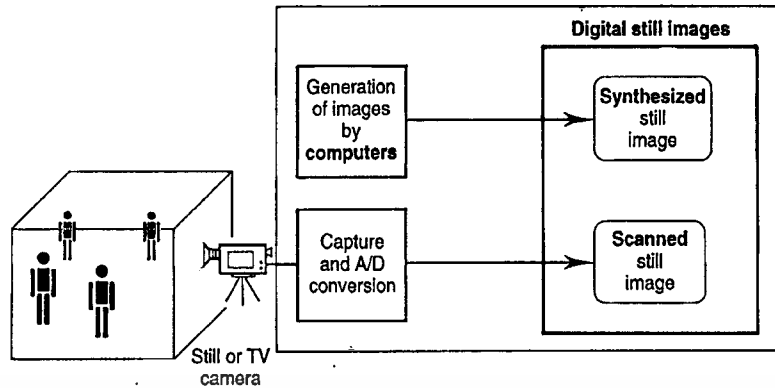
ภาพดิจิทัล มีที่มาได้จากการจับภาพจากโลกของความเป็นจริงหรือสร้างด้วยเครื่องคอมพิวเตอร์ ภาพดิจิทัลที่ได้จากโลกของความเป็นจริงสามารถทำได้หลายแนวทาง ซึ่งแต่ละแนวทางจะได้อุปกรณ์ที่มีความแตกต่างกันออกไปดังนี้

1. การสแกนจากภาพพิมพ์
2. ไฟล์ภาพจาก CD-ROM ที่มาจากห้องปฏิบัติการด้านภาพถ่ายโดยเฉพาะ
3. การจับภาพจากกล้องถ่ายภาพวิดีโอ
4. การจับภาพจากกล้องถ่ายภาพนิ่ง
5. การดึงภาพจากกล้องถ่ายภาพวิดีโอแบบอนาล็อก

ภาพดิจิทัลทุกภาพที่ได้จากการสแกนสิ่งพิมพ์ต่างๆ เรียกว่า ภาพนิ่ง ภาพอาจสร้างจากคอมพิวเตอร์ที่ไม่ได้จับภาพจากโลกความเป็นจริงหรือที่เรียกว่า การสังเคราะห์ภาพ เทคนิคการสังเคราะห์ภาพ มีดังนี้

1. วิธีการสร้างภาพบนคอมพิวเตอร์ด้วยโปรแกรมการวาดภาพ
2. การจับภาพบิตแมพที่จอแสดงผลคอมพิวเตอร์หรือเรียกเทคนิคนี้ว่า Screen capture
3. การแปลงกราฟฟิคบนเครื่องคอมพิวเตอร์เป็นภาพบิตแมพ
4. การสร้างภาพใดๆ จากโปรแกรม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.1 การสร้างภาพดิจิทัลจากคอมพิวเตอร์และการจับภาพจากโลกความเป็นจริง

ภาพสามารถเปลี่ยนแปลงได้โดยการใช้โปรแกรมแก้ไขภาพ โปรแกรมแก้ไขภาพจะเหมือนกับโปรแกรมแก้ไขกราฟฟิก โดยไม่ทำให้ความหมายของเนื้อหาเปลี่ยนไป นั่นคือโปรแกรมแก้ไขภาพจะทำการแก้ไขเอกสารแต่ไม่ใช่เปลี่ยนแปลงเอกสารใหม่ ส่วนใหญ่โปรแกรมแก้ไขภาพจะมีตัวเลือกให้เลือกมากมาย โดยเฉพาะในงานด้านภาพถ่ายที่มีการแก้ไขตั้งแต่แบบง่ายจนถึงแบบที่มีความซับซ้อน รวมทั้งการสร้างองค์ประกอบของภาพจากภาพหลายๆ ภาพร่วมกัน การสร้างภาพซ้อน การเปลี่ยนสี การทำบางส่วนของภาพให้มีความผิดเพี้ยนหรือการดัดภาพ

ภาพคอมพิวเตอร์จะอ้างถึงบิตแมพ (Bitmap) บิตแมพอย่างง่ายคือเมตริกซ์ขนาด 2 มิติ ข้อมูลภาพแต่ละค่าเรียกว่าพิกเซล (Pixel) เป็นหน่วยของข้อมูลภาพที่มีขนาดเล็กที่สุด แต่ละพิกเซลมีค่าตัวเลขค่าหนึ่งเรียกว่าขนาดแอมพลิจูด (Amplitude) จำนวนของบิตที่เข้ารหัสในแต่ละพิกเซลเรียกว่า Amplitude depth หรือ Pixel depth เช่น ชนิดของ Pixel depth ได้แก่ 1 (สำหรับภาพขาวดำ) 2 4 8 12 16 หรือ 24 บิต ค่าตัวเลขจะให้ค่าจุดขาวหรือดำในภาพหลายระดับความเทาหรือภาพสี

2.2 ประวัติและความเป็นมาของการซ่อนลายนำ

เทคนิคการซ่อนลายนำมีหลักการพื้นฐานอยู่บนหลายๆ สาขาการวิจัย เช่น สเตเกโนกราฟี คริปโตกราฟี ทฤษฎีการสื่อสาร และการประมวลผลสัญญาณ

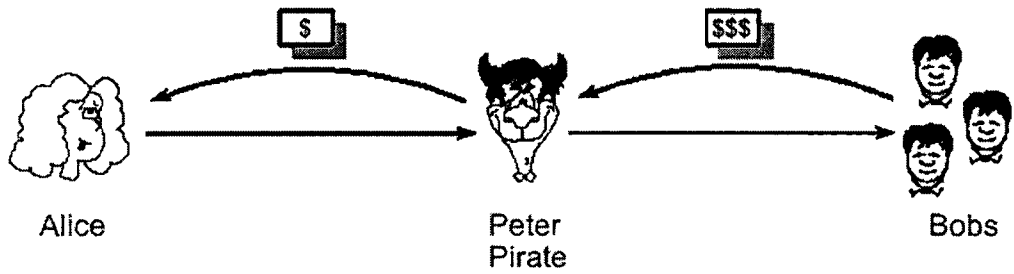
สเตเกโนกราฟี เป็นศาสตร์ของการซ่อนข้อมูลข่าวสารในการสื่อสารซึ่งยังคงมีอยู่ในการสื่อสารปัจจุบัน ซึ่งต่างจากคริปโตกราฟีที่ตั้งใจทำให้ข่าวสารนี้ไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถอ่านออกได้ จุดหมายของสเตเกโนกราฟีคือการซ่อนข้อมูลข่าวสารไว้ภายในข้อมูลที่ไม่เป็นที่น่าสงสัยซึ่งทำให้เป็นไปได้ยากที่จะตรวจหาได้ว่ามีข่าวสารที่เป็นความลับปรากฏซ่อนอยู่ภายในซึ่งคล้ายคลึงกับการซ่อนลายนำดิจิทัลในปัจจุบัน [3] โดยหนึ่งในเอกสารแรกๆ ที่บรรยายเกี่ยวกับเทคนิคสเตเกโนกราฟี คือพงศาวดารของ Herodotus เรื่องมืออยู่ว่า Demeratus ต้องการที่จะเตือน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Sparta ว่า Xerxes มุ่งหมายที่จะบุกรุกดินแดนของกรีก โดยส่งข่าวสารด้วยวิธีเคลือบแว็กซ์ไว้ที่บางส่วนของแผ่นปapyrusที่ใช้สำหรับเขียนหนังสือ แล้วขูดแว็กซ์ออกจากแผ่นปapyrusและเขียนข่าวสารไว้บนไม้ จากนั้นก็ปิดทับด้วยแผ่นปapyrusที่เคลือบด้วยแว็กซ์ จึงนำผ่านทหารยามไปได้โดยง่าย อีกเรื่องหนึ่ง มีผู้ตีข่าวเปอร์เซียชื่อว่า Histiaeus ทำการโกนผมทาสของเขาออกและสักข่าวสารไว้บนหัวของทาสผู้นั้น หลังจากที่เส้นผมของทาสผู้นั้นยาวขึ้นปกปิดข้อความเหล่านั้น Histiaeus ก็ส่งทาสผู้นั้นไปยังเป้าหมายของเขาโดยสั่งให้โกนหัวทาสผู้นั้นด้วย

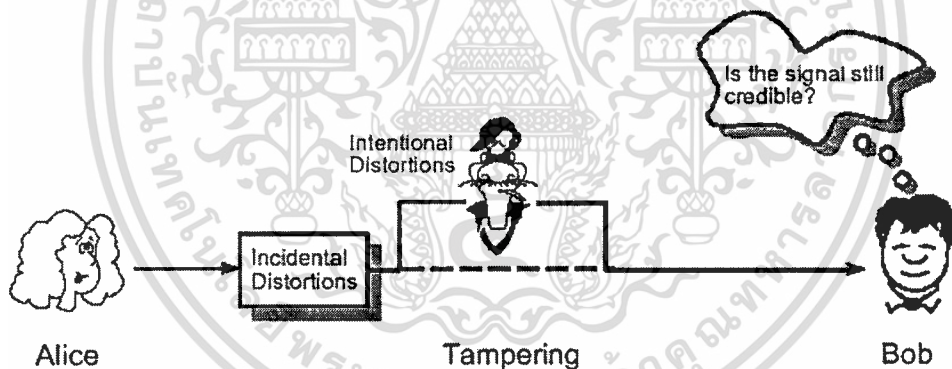
สำหรับเทคนิคอีกแบบหนึ่งคือคริปโตกราฟี คือการที่ผู้ส่งสามารถบิดเบือนข้อมูลในการส่ง เพื่อป้องกันการขโมยข้อมูลจากนักเจาะระบบ ส่วนผู้รับก็ต้องมีความสามารถในการแปลงข้อมูลที่บิดเบือนนั้นให้กลับเป็นข้อมูลเดิมที่ผู้ส่งต้องการส่งมาให้ได้ [4] Caesar Cipher เป็น Symmetric Key Algorithm แบบง่าย ๆ อย่างหนึ่ง ที่มีความเก่าแก่มาก เป็นวิธีที่ Julius Caesar เป็นผู้คิดขึ้น หลักการของ Caesar Cipher สำหรับอักษรภาษาอังกฤษ คือการแทนที่อักษรแต่ละตัวใน Plaintext ด้วยอักษรตัวที่ k ถัดไป เช่น ถ้า $k=4$ อักษร a จะถูกแทนที่ด้วยอักษร d และอักษร b จะถูกแทนที่ด้วยอักษร e ซึ่งค่า k ดังกล่าวจะถูกเรียกว่ากุญแจลับ หลังจากที่เข้ารหัสแล้วข้อความก็จะอ่านไม่รู้เรื่อง แต่มันก็ไม่ยากนักที่จะขโมยข้อมูล ถ้าเรารู้ว่าข้อความถูกเข้ารหัสด้วยวิธี Caesar Cipher เนื่องจากความเป็นไปได้มีเพียงแค่ 25 key เท่านั้น จึงได้คิดค้น Monoalphabetic Cipher เป็นวิธีการเข้ารหัสที่ถูกพัฒนามาจาก Caesar Cipher โดยมีหลักการ คือการแทนที่อักษรด้วยอักษรอีกตัวหนึ่ง แต่จะไม่แทนที่กันอย่างมีรูปแบบเหมือนกับ Caesar Cipher ที่แทนด้วยอักษรที่อยู่ห่างออกไป k ตัวสำหรับทุกอักษร ซึ่งวิธีนี้อักษรตัวหนึ่งสามารถถูกแทนที่ด้วยอักษรใดก็ได้ อักษรแต่ละตัวจะมีอักษรที่ใช้แทนที่ที่ไม่ซ้ำกัน ดังนั้นวิธีนี้จึงมีประสิทธิภาพมากกว่า Caesar Cipher และมีความเป็นไปได้ในการจับคู่อักษรได้ถึง $25!$ หรือ 10^{26} ถ้านักเจาะระบบต้องการจะขโมยข้อมูลก็ต้องใช้เวลา นานมากในการค้นหาคู่อักษร แต่จากการวิเคราะห์ภาษาแล้ว จะมีอักษรบางตัวที่ปรากฏบ่อยมาก เช่น 13% เป็น e และ 9% เป็น t และยังมีชุดอักษรที่เกิดขึ้นบ่อย ๆ เช่น in, it, the, on ทำให้การขโมยข้อมูลทำได้ง่ายขึ้น และถ้านักเจาะระบบรู้ว่าคำบางคำจะต้องเกิดขึ้นอย่างแน่นอน ก็จะทำให้การถอดรหัสง่ายขึ้นอีก

ตัวอย่างเหตุการณ์เบื้องต้น 3 แบบ [5] ในการใช้ระบบรักษาความปลอดภัยแบบเก่า โดยได้ทำการศึกษาแต่ละแบบอย่างย่อๆ ทีละแบบ และตรวจสอบความบกพร่องของเทคนิคที่ใช้อยู่ ในการปกป้องข้อมูลมัลติมีเดีย เริ่มต้นด้วยการศึกษาปัญหาการละเมิดลิขสิทธิ์ซึ่งก็คือการทำซ้ำโดยไม่ได้รับอนุญาต หรือการนำข้อมูลดิจิทัลไปขายเพื่อผลทางการค้า ความง่ายในการคัดลอกข้อมูลศักยภาพในการคัดลอกได้เหมือนจริงรวมทั้งการใช้สื่อดิจิทัลในการสร้างข้อมูลและเผยแพร่ข้อมูลอย่างแพร่หลายทำให้การละเมิดลิขสิทธิ์ เป็นปัญหาสำคัญในระบบความปลอดภัยของข้อมูล



รูปที่ 2.2 การนำข้อมูลดิจิทัลไปขายเพื่อผลทางการค้า

รูปที่ 2.3 แสดงการขายข้อมูลมัลติมีเดียของ Alice ให้แก่ Peter ถึงแม้จะสามารถป้องกันข้อมูลได้ในระหว่างการส่งไปยัง Peter โดยการใช้กระบวนการเข้ารหัสข้อมูลที่ติดตั้งไว้แต่ก็ไม่สามารถปกป้องข้อมูลจากการละเมิดลิขสิทธิ์ได้เมื่อ Peter ทำการถอดรหัสข้อมูลนั้น กล่าวคือยังมีกลไกใดที่จะป้องกันไม่ให้ Peter ทำการคัดลอกและขายข้อมูลของ Alice ให้แก่ผู้อื่น ดังนั้นจึงจำเป็นต้องมีระบบรักษาความปลอดภัยเพิ่มเติมเพื่อปกป้องทรัพย์สินทางปัญญา

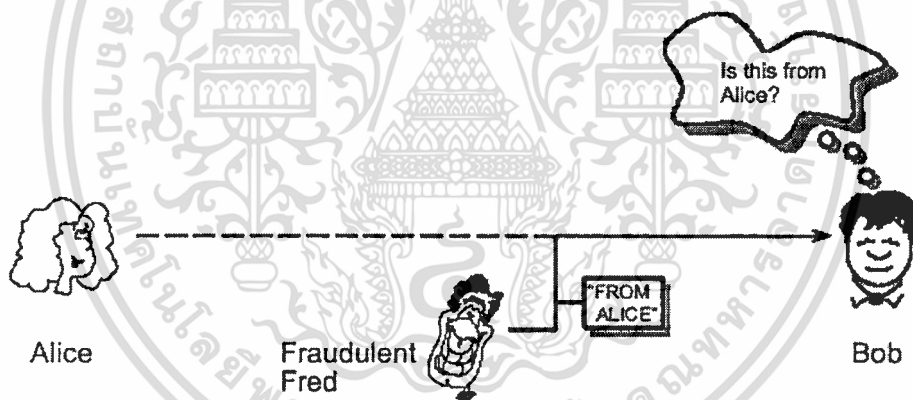


รูปที่ 2.3 การดัดแปลงหรือลักลอบแทรกสัญญาณ

วิธีการตรวจสอบความเป็นเจ้าของแบบดั้งเดิมก็ไม่เหมาะสำหรับการปกป้องข้อมูลมัลติมีเดียจากการดัดแปลงหรือลักลอบแทรกสัญญาณที่มีอยู่ด้วยวิธีการใดๆ ก็ตาม ในรูป 2.4 แสดงให้เห็นภาพเหตุการณ์ที่อาจเกิดขึ้นได้ Alice ส่งข้อมูลให้แก่ Bob แต่ว่าก่อนที่จะถึงมือ Bob สัญญาณถูกบิดเบือนโดยบังเอิญอันเนื่องมาจากการทำให้ผิดเพี้ยนไปเช่น การบีบอัดข้อมูล การสุ่มบิต ผิดพลาด หรือการสูญหายของแพ็กเกจ นอกจากนี้ข้อมูลยังอาจถูกแก้ไขให้นำเสนอผิดพลาดได้โดย Tom ซึ่งสามารถแก้ไขข้อมูลได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในการตรวจสอบความเป็นเจ้าของแบบเดิมที่ได้นำเสนอออกมา การส่งผ่านข้อมูลแบบนี้ใช้วิธีการแบบทางเดียวโดยการสร้างลำดับบิตที่เรียกกันว่าลายเซ็นดิจิทัล ลายเซ็นดิจิทัลจะถูกส่งไปยัง Bob พร้อมกับสัญญา เมื่อถึงผู้รับ Bob สามารถส่งต่อสัญญาที่เค้าได้รับด้วยวิธีเดิมเช่นกัน และยังเปรียบเทียบบิตที่ได้รับกับลายเซ็นดิจิทัลหากสัญญาทั้งสองตรงกันแสดงว่าถูกต้องเชื่อถือได้ แต่หากไม่ตรงกันก็แสดงว่ามีการบิดเบือนของสัญญาเกิดขึ้น แม้ว่าวิธีการยืนยันความถูกต้องจะมีประสิทธิภาพสำหรับข้อมูลบางชนิดแต่ก็ไม่เหมาะที่จะใช้กับข้อมูลมัลติมีเดียเพราะวิธีการดังกล่าวไม่สามารถแยกแยะความแตกต่างระหว่างการบิดเบือนของสัญญาหรือเปลี่ยนแปลงของสัญญาที่เกิดขึ้น โดยบังเอิญโดยที่ไม่สามารถหลีกเลี่ยงได้กับสัญญาที่บิดเบือนทำให้เกิดความเข้าใจผิด ในทั้ง 2 สถานการณ์นี้การนำเสนอรูปแบบของข้อมูลดิจิทัลจะถูกตัดแปลงแก้ไขแต่ก่อนหน้าสัญญาที่ถูกส่งมายังคงน่าเชื่อถือ ความสามารถในการที่จะแยกแยะการบิดเบือนหรือเปลี่ยนแปลงของสัญญาเพื่อนำมาช่วยในการตัดสินใจที่ขึ้นกับแอปพลิเคชันเหมือนกับที่ทุกคนย่อมต้องการให้เนื้อหาหรือผลของแอปพลิเคชันถูกต้องน่าเชื่อถือ



รูปที่ 2.4 การบิดเบือนของสัญญา

รูปที่ 2.5 แสดงกระบวนการที่ Fred ส่งข้อมูลหา Bob โดย Fred ต้องการทำให้ข้อมูลดูเหมือนถูกส่งมาจาก Alice เราอาจส่งข้อมูลแสดงความเป็นเจ้าของในรูปแบบของข้อมูลที่มีการเข้ารหัสอีกส่วนหนึ่งมาด้วยเพื่อรับรองว่าเป็นผู้ส่งที่มีสิทธิ์ถูกต้อง อย่างไรก็ตามข้อมูลมัลติมีเดียมักจะผ่านการแปลงรูปแบบและเปลี่ยนแปลงสื่อขณะกำลังส่ง การเปลี่ยนแปลงดังกล่าวอาจทำให้สูญเสียข้อมูลที่ยืนยันได้ซึ่งทำให้ Bob ไม่สามารถระบุตัวผู้ส่งที่มีสิทธิ์ถูกต้องได้ในเหตุการณ์เช่นนี้ จำเป็นอย่างยิ่งที่จะต้องมียุทธวิธีใหม่สำหรับการรับรองสัญญา

ในการแก้ไขจุดบกพร่องของระบบรักษาความปลอดภัยแบบเดิมที่ได้กล่าวมานี้ นักวิจัยหลายท่านได้เสนอการใช้เทคโนโลยีลายน้ำดิจิทัล ลายน้ำดิจิทัลสามารถใช้ได้ดีสำหรับ ภาพ เสียง และวีดีโอ เพราะความปลอดภัยจะถูกกำหนดมาพร้อมกับทรัพย์สินทางปัญญานั้นๆ แล้วเนื้อหาที่แท้จริงจะได้รับการป้องกัน โดยวิธีนี้ข้อมูลเกี่ยวกับความปลอดภัยจะเดินทางไปกับสัญญาณด้วยแม้ว่ารูปแบบของสัญญาณจะมีการเปลี่ยนแปลงไปเพื่อให้สามารถดึงลายน้ำออกมาได้อย่างปลอดภัย

2.3 เทคโนโลยีการซ่อนลายน้ำดิจิทัล

ลายน้ำดิจิทัลจะใช้เพื่อแสดงความเป็นเจ้าของสื่อต่างๆ การซ่อนลายน้ำกับข้อมูลภาพดิจิทัล ประกอบด้วยข้อมูลภาพกับลายน้ำดิจิทัล โดยที่ลายน้ำคือข้อมูลสำคัญ (Key Information) หรือรหัสส่วนตัวที่ฝังลงไปบนภาพ และต้องไม่เห็นความแตกต่างระหว่างภาพต้นฉบับกับภาพที่มีลายน้ำ ลายน้ำดิจิทัลเป็นการฝังข้อมูลอย่างถาวร แสดงว่ามันจะยังคงอยู่ในข้อมูลดั้งเดิมแม้จะถูกกระทำในรูปแบบต่างๆ ที่ทำให้เกิดการผิดเพี้ยนก็ตาม สำหรับการซ่อนลายน้ำดิจิทัลของภาพกระบวนการซ่อนลายน้ำเพื่อให้ได้ภาพที่ต้องการควรมีคุณสมบัติคือ [1] ลายน้ำดิจิทัลที่ฝังในข้อมูลภาพต้องไม่ปรากฏให้สามารถมองเห็นได้ การถอดหรือตรวจหาลายน้ำของผู้ที่ไม่ได้รับสิทธิต้องไม่สามารถกระทำได้แม้จะทราบแบบแผนพื้นฐานที่ใช้ในการซ่อนลายน้ำก็ตาม และลายน้ำต้องมีความคงทนต่อกระบวนการประมวลผลสัญญาณต่างๆ รวมถึงการลดทอนทางเรขาคณิต โดยสามารถทดสอบประสิทธิภาพของลายน้ำภาพดิจิทัลด้วยวิธีการต่างๆ เช่น การบีบอัดข้อมูลภาพ, การกรองภาพ, การถูกสัญญาณรบกวน, การตัดบางส่วนของภาพ เป็นต้น

ในกรณีที่มีการละเมิดลิขสิทธิ์เกิดขึ้น ลายน้ำดิจิทัลที่อยู่ภายในรูปภาพจะสามารถนำมาใช้ในการอ้างสิทธิ์เพื่อฟ้องร้องต่อการกระทำดังกล่าว อีกทั้งยังอาจนำมาใช้ในการหาตัวบุคคลที่กระทำการละเมิดลิขสิทธิ์ตัวข้อมูลได้อีกด้วย โดยในการใช้งานนั้นจะมีการใส่สัญญาณลายน้ำที่มีลักษณะเฉพาะที่แสดงถึงสิทธิความเป็นเจ้าของในตัวข้อมูลเสียก่อน จึงจะเผยแพร่ข้อมูลนั้นๆ ให้กับลูกค้า โดยในลายน้ำจะเป็นรหัสเฉพาะของสินค้าชิ้นนั้นๆ เพื่อที่ว่าเมื่อมีการละเมิดลิขสิทธิ์เกิดขึ้นเราจะสามารถสืบหาร่องรอยหลักฐานได้ว่าการกระทำผิดนั้นเริ่มต้นขึ้นจากบุคคลใด เนื่องจากลายน้ำและลูกค้าที่ได้รับข้อมูลนั้นจะถูกบันทึกเอาไว้ในระบบฐานข้อมูล เมื่อมีหลักฐานเช่นนี้แล้วการที่จะฟ้องร้องเพื่อเอาผิดบุคคลดังกล่าวย่อมสามารถกระทำได้ง่าย

การซ่อนลายน้ำในภาพดิจิทัลอาจนำไปประยุกต์ใช้งานได้ในธุรกิจสิ่งพิมพ์ เพราะหากการทำลายน้ำดิจิทัลมีความทนทานต่อการแปลงสัญญาณจากระบบดิจิทัลเป็นแอนะล็อก (Digital to Analog) และจากระบบแอนะล็อกเป็นดิจิทัล (Analog to Digital) แล้ว การที่จะพิมพ์หน้าปกหนังสือโดยใช้ภาพที่มีลายน้ำดิจิทัลอยู่ก็จะเป็นไปได้ เพื่อป้องกันการคัดลอกภาพนั้นไปใช้อย่างผิดกฎหมาย หรืออาจจะนำมาใช้ในการทำธุรกรรมบนอินเทอร์เน็ต (E-Commerce) เพื่อที่ป้องกันมิให้รูปภาพที่มีการเผยแพร่หรือจำหน่ายถูกคัดลอกและนำไปใช้อย่างผิดกฎหมาย เพราะบุคคลที่จะเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆ ทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ทำการคัดลอกก็ย่อมที่จะกลัวการถูกติดตามและฟ้องร้องอันเนื่องมาจากลายน้ำที่ซ่อนอยู่ในตัวรูปภาพ นอกจากนี้การใช้ภาพที่ไม่ทราบที่มาที่ไปก็จะมีกรรมวัตรระวังมากขึ้นด้วย เพราะหากเจ้าของภาพนั้นมาพบและพิสูจน์โดยใช้ลายน้ำดิจิทัลที่ซ่อนอยู่ในภาพถึงความเป็นเจ้าของได้ ก็จะสามารถฟ้องร้องต่อบุคคลที่นำภาพดังกล่าวมาใช้งานได้

ในส่วนการซ่อนลายน้ำดิจิทัลในสัญญาณเสียง จะสามารถนำมาประยุกต์ใช้ได้ ในธุรกิจที่เกี่ยวข้องกับดนตรี โดยหากทำการใส่สัญญาณลายน้ำลงในข้อมูลเพลงที่อยู่ในรูปแบบ MPEG-I Layer 3 ก็จะสามารถที่จะยับยั้งปัญหาในการคัดลอกและเผยแพร่บทเพลงอย่างผิดกฎหมายได้ในระดับหนึ่ง อีกทั้งยังเป็นการส่งเสริมการทำธุรกรรมทางอินเทอร์เน็ตให้มีความปลอดภัยมากขึ้นอีกด้วย นอกจากนี้การซ่อนลายน้ำดิจิทัลในข้อมูลวิดีโอ อาจพิจารณาเหมือนกับการนำรูปภาพหลายรูปมาเรียงต่อกัน จะช่วยป้องกันการละเมิดลิขสิทธิ์ได้ในหลายๆ ทาง ยกตัวอย่างเช่น ในธุรกิจภาพยนตร์ การซ่อนลายน้ำดิจิทัลจะช่วยลดปัญหาการละเมิดลิขสิทธิ์โดยการคัดลอกตัวข้อมูลลงในแผ่นซีดีหรือดีวีดี เพื่อจัดจำหน่ายอย่างผิดกฎหมาย เพราะหากมีตัวอย่างของข้อมูลที่มีสัญญาณลายน้ำอยู่ เราก็จะสามารถตามจับผู้กระทำความผิดมาลงโทษได้ ยิ่งไปกว่านั้นการส่งผ่านข้อมูลวิดีโอผ่านทางระบบเครือข่ายยังได้รับการป้องกันได้อีกด้วย ตัวอย่างการใช้งานระบบวิดีโอผ่านเครือข่าย เช่น video-on-demand และ pay-per-view

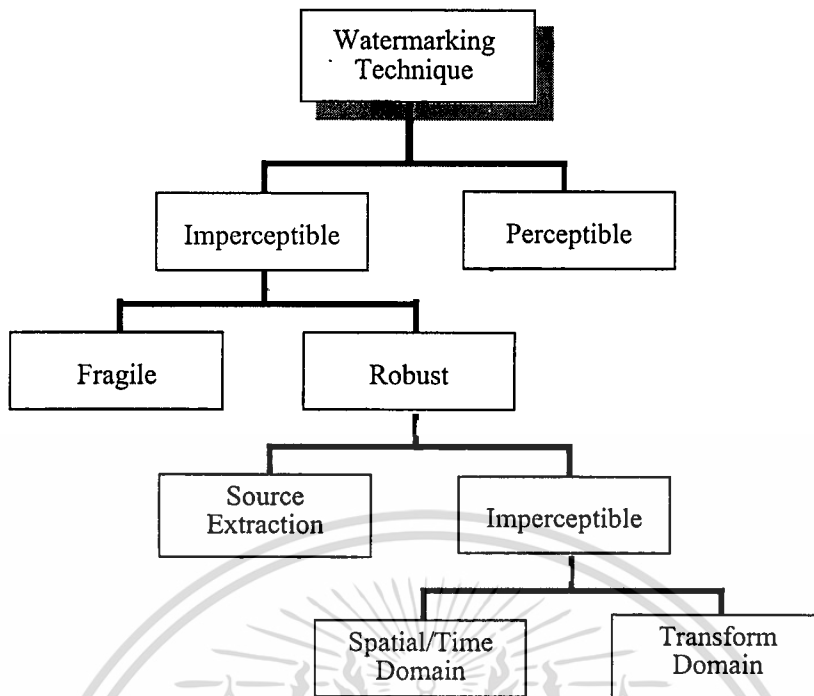
ในกรณีของการเข้ารหัสข้อมูลเพื่อป้องกันบุคคลอื่นที่ไม่มีกุญแจรหัสลับเข้ามาใช้งานข้อมูลนั้น เมื่อใดก็ตามที่ข้อมูลได้ถูกถอดรหัสออกมา ความปลอดภัยของข้อมูลนั้นก็ลดลง เนื่องจากข้อมูลสามารถถูกคัดลอกภายหลังขั้นตอนที่ผ่านการถอดรหัสแล้ว ซึ่งจะไม่สามารถป้องกันปัญหาการละเมิดลิขสิทธิ์ของข้อมูลนั้น ได้เลย ดังนั้นเราอาจนำเทคนิคการซ่อนลายน้ำดิจิทัลมาประยุกต์ใช้งานร่วมกับเทคนิคการเข้ารหัสลับเพื่อให้ข้อมูลมีความปลอดภัยเพิ่มมากขึ้นกว่าเดิม [6] เมื่อใดก็ตามที่ข้อมูลถูกถอดรหัสออกมาแล้ว ตัวข้อมูลยังคงถูกป้องกันเอาไว้อีกชั้นหนึ่งจากการซ่อนลายน้ำดิจิทัล ดังนั้นหลังจากขั้นตอนการถอดรหัสถ้ามีการละเมิดลิขสิทธิ์ของตัวข้อมูลเกิดขึ้น เราจะสามารถหาตัวบุคคลที่กระทำความผิดนั้นได้ เพราะข้อมูลที่ถูกคัดลอกไป จะยังคงมีลายน้ำดิจิทัลติดอยู่ด้วยเช่นเดียวกับข้อมูลต้นฉบับที่ถูกคัดลอก เพราะฉะนั้นเมื่อใดก็ตามที่มีการตรวจพบข้อมูลที่ถูกละเมิดลิขสิทธิ์ลายน้ำภายในข้อมูลดังกล่าวจะถูกใช้เพื่อตามรอยย้อนกลับไปหาว่าข้อมูลที่ถูกคัดลอกนั้น เป็นข้อมูลที่ถูกเผยแพร่ให้กับลูกค้าคนไหน แนวความคิดเช่นนี้ได้ถูกนำมาประยุกต์ใช้ในการซ่อนลายน้ำดิจิทัลของข้อมูลมัลติมีเดียปัจจุบัน

ปัจจุบันมีนักวิจัยหลายกลุ่มทั่วโลกให้ความสนใจในการพัฒนาเทคโนโลยีทางการซ่อนลายน้ำดิจิทัล ทำให้เป็นที่เชื่อกันว่าเทคโนโลยีดังกล่าวจะถูกนำมาใช้อย่างกว้างขวางในอนาคตอันใกล้ รวมไปถึงเทคโนโลยีอื่นๆ ที่ใช้ในการป้องกันการละเมิดลิขสิทธิ์จะได้รับการพัฒนาอย่างต่อเนื่องต่อไป อย่างไรก็ตามจะเห็นได้ว่าเมื่อมีการป้องกันก็ย่อมจะมีผู้หาช่องทางในการทำลาย

อยู่เรื่อยไป แต่ปัญหานี้จะไม่เกิดขึ้นเลยถ้าทุกคนมีจิตสำนึกที่ดี เห็นความสำคัญเห็นคุณค่าของทรัพย์สินทางปัญญา รวมถึงการร่วมมือกันไม่สนับสนุนสินค้าหรือผลิตภัณฑ์ที่ทำขึ้นอย่างผิดกฎหมาย [3]

การสื่อสารในวงกว้างของข้อมูลสื่อผสมทำให้มีความจำเป็นอย่างยิ่งในการปกป้องข้อมูลสื่อผสมจากการลอกเลียนแบบและนำไปใช้อย่างผิดกฎหมาย ความก้าวหน้าทางเทคโนโลยีที่ช่วยอำนวยความสะดวกในการคัดลอกและทำธุรกรรมอิเล็กทรอนิกส์ ก็เป็นอีกปัจจัยหนึ่งที่ทำให้การขโมยและการละเมิดทรัพย์สินทางปัญญาเป็นไปได้โดยง่าย ระบบรักษาความปลอดภัยที่มีอยู่สำหรับการทำธุรกิจด้านข้อมูล จะช่วยรักษาความปลอดภัยให้กับการช่องทางการสื่อสารระหว่างสองฝ่าย เทคนิคเหล่านี้นำเอาเครื่องมือรักษาความปลอดภัยที่ติดตั้งไว้มาควบคุมการเรียกใช้ข้อมูล การเข้ารหัส และการตรวจสอบข้อมูลภายใต้ข้อตกลง อย่างไรก็ตามเมื่อมีการซื้อขายข้อมูลแบบดิจิทัล ปัญหาเกี่ยวกับของแท้และความเป็นเจ้าของก็มักจะตามมาแต่นี้ไม่ใช่ปัญหาสำคัญสำหรับระบบอานาล็อก เพราะในระบบอานาล็อกนั้นการคัดลอกข้อมูลลงในฟิล์ม เทป และ VHS วีดีโอ จะมีคุณภาพไม่ดีเท่าต้นฉบับ ซึ่งข้อจำกัดเกี่ยวกับคุณภาพของเนื้อหาตัวเองสามารถช่วยป้องกันการเผยแพร่และเสนอขายข้อมูลที่ผิดกฎหมายได้ ในทางตรงกันข้าม ข้อมูลดิจิทัลสามารถคัดลอกและเก็บไว้ได้อย่างสะดวกสบาย ซึ่งทำให้บั่นทอนกับลิขสิทธิ์และการใช้ข้อมูลสามารถทำได้ยากลำบาก ยิ่งไปกว่านั้น ขณะนี้ยังไม่มีกลไกใดๆ ที่สามารถตรวจหาการลอกเลียนแบบและการคัดแปลงเนื้อหาอย่างผิดกฎหมายได้เลย ปัญหาใหม่ๆ เกี่ยวกับความปลอดภัยของข้อมูลสื่อผสมเหล่านี้ไม่สามารถแก้ไขได้ด้วยระบบรักษาความปลอดภัยแบบกระจายอย่างเดิมได้

การทำภาพพิมพ์ลายน้ำดิจิทัลเป็นวิธีเสมือนกับวิธีการที่มีฝีมือในยุคสมัยก่อนใช้ในการแสดงความเป็นเจ้าของต่อรูปภาพ โดยพวกเขาจะใส่สัญลักษณ์ที่แสดงถึงเอกลักษณ์ของตนเองไว้ในตัวรูปภาพ โดยสัญลักษณ์ที่ใส่เข้าไปนั้นอาจจะมีลักษณะที่มองเห็นได้หรือไม่ก็ได้ก็ได้นั้นแนวคิดของการทำภาพพิมพ์ลายน้ำดิจิทัลจึงเป็นการใส่สัญลักษณ์ที่มีลักษณะเฉพาะเข้าไปในตัวข้อมูลมัลติมีเดีย ซึ่งสัญญาณดังกล่าวจะแสดงถึงความเป็นเจ้าของต่อข้อมูลนั้นๆ จากหลักการดังกล่าวเราอาจแบ่งประเภทของภาพลายน้ำดิจิทัลออกเป็น 2 ชนิดได้ คือ ภาพลายน้ำดิจิทัลชนิดที่มองเห็นได้ (Perceptible) และภาพลายน้ำดิจิทัลชนิดที่ไม่สามารถมองเห็นได้ (Imperceptible) รูปที่ 2.5 แสดงการแบ่งประเภทของเทคนิคการซ่อนลายน้ำภาพดิจิทัล โดยวิทยานิพนธ์ฉบับนี้จะกล่าวถึงเทคนิคการซ่อนลายน้ำที่ไม่สามารถมองเห็นได้



รูปที่ 2.5 ประเภทของเทคนิคการซ่อนลายน้ำภาพดิจิทัล

เทคนิคการซ่อนลายน้ำที่สามารถมองเป็นได้เป็นแบบที่เห็นการเปลี่ยนแปลงในสัญญาณต้นฉบับได้อย่างชัดเจนเมื่อลายน้ำถูกฝังเข้าไป แต่จะไม่ทำให้สัญญาณต้นฉบับผิดเพี้ยนไปมาก แม้เทคนิคการซ่อนลายน้ำที่สามารถมองเห็นได้จะไม่เป็นที่นิยมเท่ากับการซ่อนลายน้ำที่ไม่สามารถมองเห็นได้ แต่ก็มี การนำมาใช้อย่างประสบความสำเร็จเช่นกันในภาพดิจิทัล โดยการฝังสัญลักษณ์ของเจ้าของสื่อที่มองทะลุได้ลงไปทำให้เห็นลายน้ำและยังเห็นลายละเอียดของภาพดิจิทัลได้อย่างชัดเจน

การใส่ลายน้ำดิจิทัลชนิดที่มองเห็นได้นั้นจะทำได้โดยการเขียน เติม หรือแทรกตัว ข้อมูลที่ต้องการลงไปในตัวรูปภาพโดยตรง ซึ่งประโยชน์ของการทำภาพพิมพ์ลายน้ำดิจิทัลชนิดที่มองเห็นได้ก็คือ เป็นการแสดงสิทธิ์ความเป็นเจ้าของในตัวข้อมูลมัลติมีเดียต่างๆ บุคคลทั่วไปที่พบเห็นจะสามารถรู้ได้โดยทันทีว่าภาพนั้นๆ เป็นของผู้ใด นอกจากนี้ยังเป็นการยับยั้งการกระทำที่จะเป็นการละเมิดลิขสิทธิ์ของข้อมูลนั้นๆ เช่น ความยากลำบากในการที่จะนำลายน้ำออกจากตัวรูปภาพก่อนที่จะนำไปเผยแพร่อย่างมิชอบ รูปที่ 2.6 ได้แสดงตัวอย่างของรูปภาพที่มีลายน้ำดิจิทัลชนิดที่มองเห็นได้อยู่



(ก)



(ข)

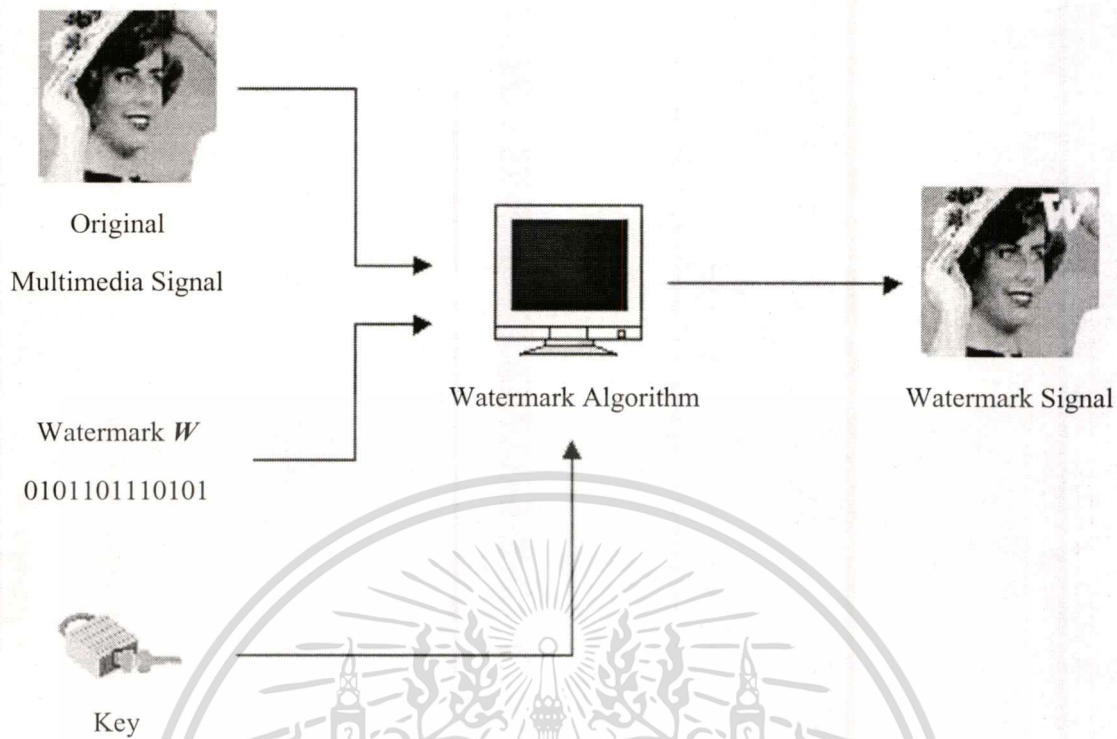
รูปที่ 2.6 (ก) การใส่ลายน้ําดิจิตอลลงไปในบริเวณมุมขวาล่างของรูปภาพ (ข) การใส่ลายน้ําดิจิตอล
ไปในบริเวณกลางรูปภาพ

อย่างไรก็ตามวิธีการนี้มีข้อด้อยอย่างหนึ่งก็คือ ข้อมูลมัลติมีเดียจะมีคุณภาพลดลงเป็น
อย่างมาก เนื่องจากตัวลายน้ําจะไปบดบังรายละเอียดของรูปภาพที่ใส่ แต่ถึงอย่างไรการทำภาพพิมพ์
ลายน้ําดิจิตอลในรูปแบบนี้ยังคงเป็นที่นิยมใช้ในการแสดงสิทธิความเป็นเจ้าของ เพราะสามารถ
ดำเนินการได้ง่ายและไม่ซับซ้อน และในบางครั้งความพยายามที่จะกำจัดลายน้ําทิ้งที่อยู่ในรูปภาพนั้นๆ
ออก อาจส่งผลกระทบต่อไปถึงคุณภาพของรูปซึ่งอาจจะเสียหาย และมีคุณภาพต่ำลง เช่นในรูปที่ 2.6
(ก) เป็นการใส่ภาพลายน้ําดิจิตอลชนิดที่มองเห็นได้ลงไป ในบริเวณมุมขวาล่างของรูปภาพ ซึ่งการ
ใส่ในบริเวณนี้จะไม่กระทบต่อรายละเอียดที่สำคัญของรูปภาพมากนัก แต่ในขณะเดียวกันตัวลายน้ํา
ดิจิตอลจะถูกกำจัดออกไปได้โดยง่ายโดยไม่กระทบต่อส่วนสำคัญของรูป ส่วนในรูปที่ 2.6 (ข) ลายน้ํา
จะถูกใส่ลงไป ในบริเวณกลางรูปภาพ ซึ่งเป็นบริเวณที่มีความสำคัญของรูปภาพ ทำให้ตัวลายน้ํา
ดิจิตอลมีความยากลำบากในการเอาออกโดยที่ไม่กระทบถึงคุณภาพของรูป ในขณะที่คุณภาพ
ของรูปนั้นก็ลดลงไปมากเช่นกัน ในปัจจุบันมีโปรแกรมใช้งานหลายชนิดที่มีความสามารถในการ
การทำภาพลายน้ําดังกล่าวได้ ยกตัวอย่างเช่น โปรแกรม Adobe Photoshop

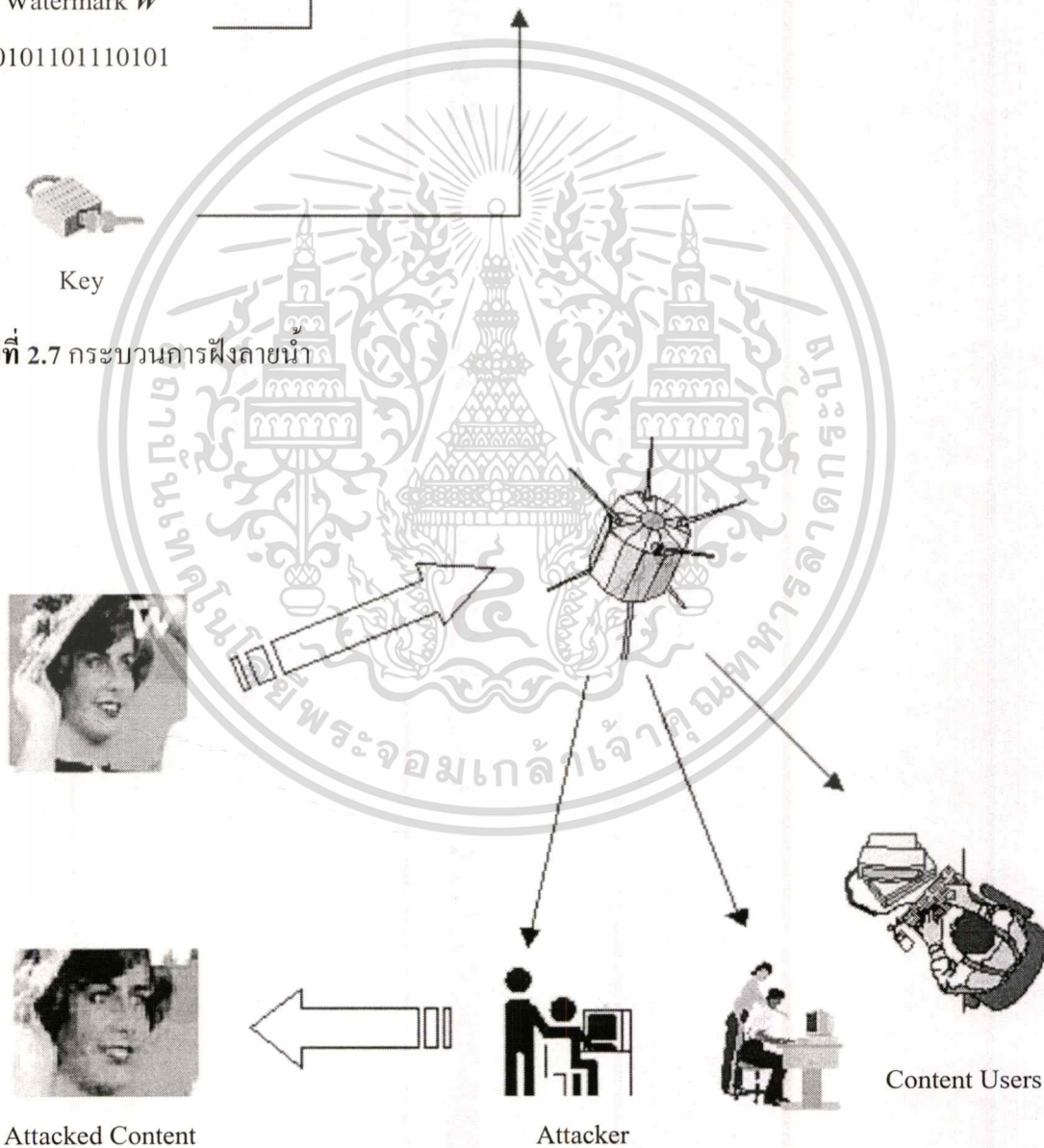
วิธีหนึ่งที่สามารถจัดการกับปัญหานี้ได้คือการฝังรหัสที่ไม่สามารถมองด้วยตาเปล่าได้ลง
ในภาพต้นฉบับเพื่อแสดงความเป็นเจ้าของ เราเรียกเทคนิคนี้ว่า การซ่อนลายน้ําดิจิตอล ซึ่งลายน้ํา
ดิจิตอลอาจจะประกอบไปด้วยรหัสลิขสิทธิ์ รหัสที่ใช้แสดงความเป็นเจ้าของ หรือรหัสที่ใช้ในการ
แปลสัญญาณ รหัสลายน้ําเหล่านี้จะไม่สามารถตรวจสอบได้หากไม่ได้ใช้เครื่องมือตรวจสอบ
โดยเฉพาะ รหัสทั่วไปที่มักจะถูกฝังลายน้ําคือ ภาพ เสียง และวีดิโอดิจิตอล

รูปที่ 2.7 แสดงกระบวนการทั่วไปของกระบวนการฝังลายน้ํา ภาพลายน้ําซึ่งมักจะเป็น
ข้อมูลแบบไบนารีจะถูกฝังลงในภาพต้นฉบับด้วยกุญแจลับ ข้อมูลที่ฝังลงไปโดยปกติจะทำให้เกิด
การเปลี่ยนแปลงของสัญญาณเล็กน้อย โดยกุญแจลับและลายน้ําจะเป็นตัวกำหนดในการสร้าง
สัญญาณลายน้ํา ในขั้นตอนการฝังลายน้ําแบบนี้จะมีการฝังลายน้ําในสัญญาณต้นแบบซึ่งไม่มีการ
แสดงภาพลายน้ําออกมาให้เห็น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 2.7 กระบวนการฝังลายน้ำ

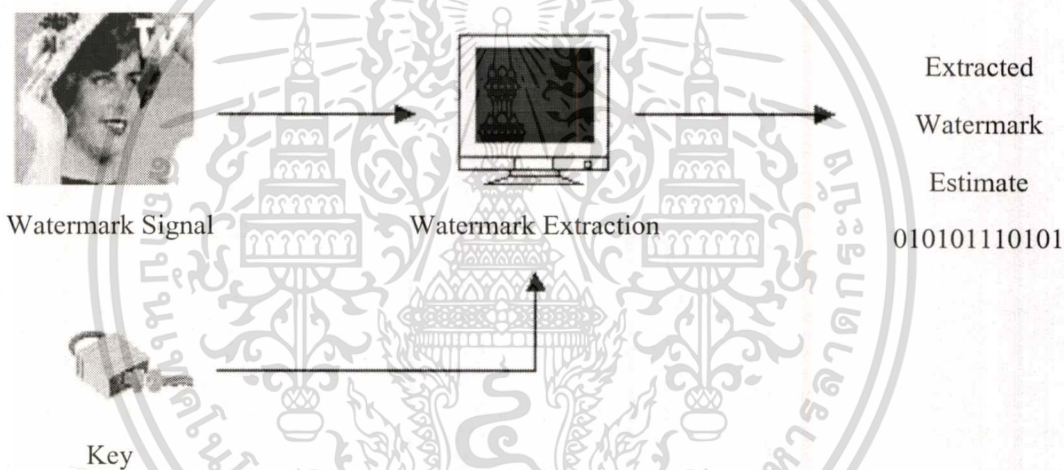


รูปที่ 2.8 การเผยแพร่ข้อมูลที่มีการฝังลายน้ำ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อทำการฝังลายน้ำไปแล้วก็จะสามารถนำข้อมูลนี้ไปเผยแพร่ในระบบเปิดได้ ดังรูปที่ 2.8 เมื่อข้อมูลได้ถูกเผยแพร่สู่ผู้ใช้งานอื่นๆในระบบแล้วนั้นข้อมูลอาจผ่านผู้ไม่ประสงค์ดีที่มีจุดมุ่งหมายในการลบลายน้ำที่ฝังอยู่ในข้อมูลออก เพื่อนำข้อมูลนั้นไปขายหรือเผยแพร่ต่อไปโดยไม่ได้รับอนุญาต

เมื่อได้ภาพที่ส่งสัยในความเป็นเจ้าของ สามารถตรวจสอบได้ด้วยการใช้กุญแจลับในการตรวจสอบ ดังรูปที่ 2.9 ขั้นตอนนี้เรียกว่าการตรวจหาลายน้ำกลับคืน ซึ่งในบางกระบวนการของการตรวจสอบจำเป็นต้องใช้ภาพต้นแบบในการตรวจหาลายน้ำด้วย สิ่งที่ทำหายในการออกแบบคือการซ่อนลายน้ำที่สามารถทำหน้าที่ได้ตามที่กำหนดไว้อย่างสมบูรณ์ สำหรับการลอกเลียนแบบภาพลายน้ำต้องสามารถเรียกคืนได้ใหม่ถึงแม้ว่าสัญญาณที่ถูกฝังลายน้ำนั้นจะผ่านการบิดเบือนข้อมูลมาก่อนก็ตาม ซึ่งความปลอดภัยของการซ่อนลายน้ำจะมาจากความลับของกุญแจลับ ถ้าหากไม่สามารถเข้าถึงข้อมูลได้ก็จะไม่สามารถดึงลายน้ำออกมาได้



รูปที่ 2.9 กระบวนการตรวจหาลายน้ำกลับคืน

ประเภทของเทคนิคการซ่อนลายน้ำแบบไม่สามารถมองเห็นได้ ยังสามารถแบ่งได้อีก 2 ประเภทคือ ลายน้ำที่ไม่คงทน (Fragile) [7] และลายน้ำที่มีความคงทน (Robust) [8] ซึ่งลายน้ำที่ไม่คงทนจะถูกฝังลงในสัญญาณต้นฉบับและทำให้การเปลี่ยนแปลงอันไม่พึงประสงค์ใดๆ ต่อภาพที่มีการฝังลายน้ำจะส่งผลต่อลายน้ำที่ดึงออกมาและเป็นข้อมูลสำหรับการจับผิดต่อไป ในทางตรงกันข้ามการซ่อนลายน้ำที่มีความคงทน ลายน้ำจะถูกฝังลงในสัญญาณต้นฉบับ แบบให้ยากต่อการลบมันจะถูกออกแบบให้ทนต่อการแก้ไข หรือการบิดเบือนในรูปแบบต่าง ๆ โดยเราให้ความหมายของการบิดเบือนว่าเป็นการตัดแปลงใด ๆ ก็ตามที่เกิดขึ้นกับสัญญาณภาพที่มีการฝังลายน้ำและส่งผลต่อความน่าเชื่อถือของลายน้ำที่นำกลับคืนมา

ประเภทของซอคลายน้ำแบบมีความคงทนเราสามารถแบ่งรูปแบบการทำงานได้ 2 ประเภทคือ ต้องใช้ภาพต้นฉบับ (Source Extraction) [1,2] และไม่ต้องใช้ภาพต้นฉบับ (Destination Extraction) [8,9,10,11,12] ในแบบที่ต้องใช้ภาพต้นฉบับกำหนดว่าต้องใช้สัญญาณต้นฉบับในการตรวจหาลายน้ำกลับคืน และวิธีนี้จะมีลักษณะพิเศษคือมีความคงทนต่อการบิดเบือนสัญญาณ แต่ความคงทนนี้ก็มักจะถูกพร่องเมื่อใช้งานจริง เนื่องจากสัญญาณต้นฉบับเป็นสิ่งจำเป็นสำหรับการนำลายน้ำกลับคืนและมีความสำคัญกับการถูกคัดลอกต้นฉบับที่ไม่มีลายน้ำ อย่างไรก็ตามวิธีนี้มีประโยชน์มากเมื่อต้องการความคงทน แตกต่างกับแบบที่ไม่ต้องใช้ภาพต้นฉบับที่ต้องการเพียงกุญแจลับสำหรับการนำลายน้ำกลับคืน วิธีนี้แบ่งได้อีก 2 กลุ่มคือ เทคนิคที่กระทำในโดเมนสเปเชียล (Spatial Domain) [13,14] และเทคนิคที่กระทำในโดเมนความถี่ (Frequency Domain) [8,9,10,11,12] โดยเทคนิคที่กระทำในโดเมนสเปเชียล ลายน้ำจะถูกฝังในโดเมนสเปเชียลของภาพต้นฉบับ ขณะที่เทคนิคที่กระทำในโดเมนความถี่ ลายน้ำจะถูกฝังในโดเมนความถี่ของภาพที่ได้จากการทำงานของ คอสไครต์โคไซน์ทรานส์ฟอร์ม (Discrete Cosine Transform) [10,11] ฟูรีเยร์ทรานส์ฟอร์ม (Fourier Transform) [9] หรือ เวฟเล็ตทรานส์ฟอร์ม (Wavelet Transform) [12] กับภาพต้นฉบับ

โดยทั่วไปการเข้ารหัสและตรวจสอบความเป็นเจ้าของจะใช้มาตรฐานระบบการเข้ารหัส แต่ลายน้ำดิจิทัลจะแตกต่างตรงที่ไม่ป้องกันการละเมิด โดยการควบคุมการใช้ข้อมูล แต่จะทำการแสดงหลักฐานการละเมิดหลังจากเกิดเหตุการณ์นั้นขึ้นแล้ว

ปัจจุบันนี้เรากำลังอยู่ในช่วงประเมินผลของเทคโนโลยีซึ่งนักวิจัยกำลังพัฒนาหลักเกณฑ์ทั่วไปสำหรับการซอคลายน้ำที่มีประสิทธิภาพ ปรับปรุงความน่าเชื่อถือ และความเที่ยงตรงภายใต้การคำนวณที่ซับซ้อน และปรับให้เหมาะสมกับความต้องการของธุรกิจข้อมูลสื่อผสมที่เปลี่ยนแปลงตลอดเวลา อย่างไรก็ตามการซอคลายน้ำดิจิทัลยังคงอยู่ในช่วงพัฒนาแม้จะเริ่มมีบริการเพื่อการค้าแล้วก็ตาม ซึ่งในอดีตยังต้องใช้เวลา 10 – 20 ปี กว่าระบบการเข้ารหัสข้อมูลจะถูกนำมาใช้โดยทั่วไป

2.4 คุณสมบัติที่ต้องการของการซอคลายน้ำ

ในการซอคลายน้ำ ลายน้ำที่มีประสิทธิภาพเพื่อให้สามารถทำงานตามจุดมุ่งหมายได้ ควรมีคุณสมบัติดังต่อไปนี้ [1]

2.4.1 ไม่ปรากฏให้เห็น (Invisible)

ลายน้ำดิจิทัลที่ฝังในข้อมูลภาพต้องไม่ปรากฏให้สามารถมองเห็นได้ เนื่องจากไม่ต้องการให้ผู้ใช้งานโดยทั่วไปสังเกตเห็นลายน้ำที่ได้ทำการซ่อนไว้ แม้ว่าจะงานประยุกต์บางอย่างจะเอกลักษณะเป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่นอนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต้องการลายน้ำที่มองเห็นได้ก็ตามแต่ลายน้ำที่จะทำการศึกษาต่อไปนี้จะมุ่งที่ไม่สามารถมองเห็นลายน้ำที่ซ่อนได้

2.4.2 ความปลอดภัย (Security)

การถอดหรือตรวจหาลายน้ำของผู้ที่ไม่ได้รับสิทธิต้องไม่สามารถกระทำได้แม้จะทราบแบบแผนพื้นฐานที่ใช้ในการซ่อนลายน้ำก็ตาม เนื่องจากผู้ที่ไม่ได้รับสิทธิจะไม่รู้ตำแหน่งและกระบวนการในการตรวจหาลายน้ำกลับคืน

2.4.3 การง่ายในการตรวจหาลายน้ำกลับคืน (Easily Extracted)

การตรวจหาลายน้ำกลับคืนออกจากภาพที่ได้ทำการฝังลายน้ำจากผู้ที่ได้รับอนุญาต ต้องสามารถทำได้ง่าย และลายน้ำที่ได้ต้องมีความเที่ยงตรงและสะดวกในการตรวจสอบความเป็นเจ้าของของผู้ที่เป็นเจ้าของหรือผู้ที่ได้รับสิทธิ

2.4.4 ความคงทน (Robustness)

ลายน้ำที่ถูกบกรุกจากการกระทำต่าง ๆ ทั้งการกระทำที่ตั้งใจและไม่ตั้งใจต้องไม่ทำให้คุณภาพของภาพและลายน้ำลดลงกว่าจุดที่ยอมรับได้ การใช้สัญญาณดิจิทัลในรูปของเพลง ภาพและวิดีโอ โดยทั่วไปมักจะเกิดความเพี้ยนของสัญญาณหลายชนิด เช่น การบีบอัดแบบมีการสูญเสีย ในกรณีของภาพ เช่น การกรอง การเปลี่ยนขนาด การปรับปรุงความคมชัด การตัดบางส่วน การหมุนภาพ และอื่นๆ สำหรับการทำให้ลายน้ำให้เกิดประโยชน์นั้น ลายน้ำควรจะสามารถตรวจหาได้แม้ว่าหลังจากเกิดการเพี้ยนทางสัญญาณเหล่านี้ ความคงทนที่จะต่อต้านการเพี้ยนของสัญญาณเหล่านี้ขึ้นอยู่กับลักษณะของอัลกอริทึมในการบีบอัดข้อมูลแบบมีการสูญเสีย ซึ่งทำงานโดยตัดข้อมูลที่ไม่ว่าสำคัญบางส่วนที่ไม่มีผลกระทบต่อคุณภาพของภาพ เสียง หรือวิดีโอหลังผ่านการบีบอัดออก ดังนั้นการซ่อนลายน้ำไว้ในส่วนของข้อมูลที่ไม่ว่าสำคัญดูเหมือนว่าจะไม่สามารถคงอยู่ได้ในการบีบอัดข้อมูล ในกรณีของการทำลายน้ำภาพ ความคงทนต่อการเปลี่ยนแปลงทางเรขาคณิต เช่น การเปลี่ยนขนาด การหมุน และการตัดบางส่วนของภาพยังคงเป็นประเด็นสำคัญอยู่ ซึ่งก่อนที่จะนำการทำลายน้ำมาใช้ในการป้องกันลิขสิทธิ์ได้อย่างสมบูรณ์จำเป็นจะต้องแก้ปัญหาเหล่านี้ได้เสียก่อน

2.5 ข้อกำหนดของความคงทน

เครื่องมือในการทำลายน้ำต้องสามารถฝังข้อมูลที่ไม่ว่าสามารถลบออกได้ โดยการแก้ไขภาพโดยบังเอิญหรือโดยตั้งใจกระทำ และการปลอมลายน้ำ เครื่องมือหลายๆ ตัวที่มีอยู่อย่างแพร่หลายสำหรับการประมวลผลสัญญาณภาพดิจิทัล มุ่งไปที่การปรับปรุงหรือแก้ไขภาพ เทคนิคการ

ประมวลผลที่มีอยู่สามารถแยกออกได้เป็นสองประเภท คือ การแก้ไขโดยการประมวลผลสัญญาณและความเพี้ยนแบบเรขาคณิต ซึ่งมีรายละเอียดของการประมวลผลสัญญาณหรือความผิดเพี้ยนต่างๆ ที่อาจจะเกิดขึ้นกับข้อมูลได้

2.5.1 การแก้ไขโดยการประมวลผลสัญญาณ

การปรับความสว่างและคอนทราสต์ (Brightness and Contrast Enhancement) โดยทั่วไปแล้วไม่ทำให้เกิดปัญหาในการตรวจหาลายน้ำ ในทางตรงกันข้าม การทำปรับปรุงแบบนี้มักจะทำการตรวจหา ซึ่งทำเพื่อให้ได้ผลลัพธ์ที่ดีขึ้น

การปรับความคมชัด การทำให้เลือน การกรองแบบเชิงเส้นและแบบไม่เป็นเชิงเส้น (Sharpening, Blurring, Linear and Non Linear Filtering) ถ้าทำแบบนี้มากๆ สามารถทำให้ลายน้ำเสื่อมลงไปได้ แต่ในกรณีนี้ สิ่งที่ทำให้มีการลดคุณภาพของภาพไปอย่างมาก คือตัวกรองภาพที่เรียกว่า Despeckle ซึ่งมีกระบวนการแบบปรับเปลี่ยนได้ โดยลดรายละเอียดของภาพแบบสุ่มเล็กน้อยต่างกันไปโดยยังคงรายละเอียดของภาพไว้

การเพิ่มสัญญาณรบกวนแบบคอรีเลตและแบบไม่เป็นคอรีเลต (Addition of Correlated or Uncorrelated Noise) เข้าไปในเนื้อหาที่มีลายน้ำอยู่

การแปลงแอนะล็อกเป็นดิจิทัลและดิจิทัลเป็นแอนะล็อก (Digital-Analog (D/A) and Analog-Digital (A/D) Conversions) เช่น การพิมพ์และการสแกน หรือการบันทึกเทป

การบีบอัดแบบ JPEG ที่มีการสูญเสีย (Lossy JPEG Compression) กล่าวได้ว่าเป็นการประมวลผลสัญญาณที่ใช้กับภาพมากที่สุด จึงเป็นตัวทดสอบที่ดีสำหรับการทดสอบความคงทนของลายน้ำ

2.5.2 การเปลี่ยนแปลงทางเรขาคณิต

การเปลี่ยนแปลงทางเรขาคณิต (Geometric Manipulations) มุ่งไปที่การเปลี่ยนลักษณะของภาพโดยไม่มีการสูญเสียในเรื่องของคุณภาพ มีดังนี้

การย่อหรือขยายขนาดภาพ (Resizing) ขนาดของภาพถูกเปลี่ยนไปเมื่อเทียบกับต้นแบบซึ่งจะมีผลกับอัลกอริทึมที่ฝังลายน้ำในตำแหน่งที่ตายตัวซึ่งจะไม่สามารถตรวจหาลายน้ำได้

การตัดบางส่วนของภาพ (Cropping) เป็นการตัดบางส่วนของภาพออกไป ซึ่งทำให้มีผลกับอัลกอริทึมที่กระจายลายน้ำออกไปทั่วทั้งภาพ

การเคลื่อนย้ายภาพ (Translation) จะมีผลอย่างมากถ้าหากพิจารณาพร้อมกับการตัดบางส่วนของภาพออกไป ถ้าหากส่วนย่อยของภาพถูกแยกออกจากภาพต้นแบบ ซึ่งทำให้เราไม่สามารถรู้ได้ว่าเกิดจากการตัดบางส่วนของภาพนี้ออกจากตำแหน่งใดจากภาพต้นแบบ ในกรณีที่ไม่มีภาพต้นแบบในการเปรียบเทียบหากมีการเคลื่อนย้ายส่วนย่อยของภาพที่ถูกตัดออกไปไว้ยังตำแหน่งอื่น การเคลื่อนย้ายภาพนี้จะมีผลต่ออัลกอริทึมที่ฝังลายน้ำลงในตำแหน่งที่ตายตัว

การหมุนภาพ (Rotation) เป็นกรณีที่สำคัญที่สุดหากพิจารณาในกรณีที่หมุนภาพไป 90 และ 180 องศา ซึ่งเหมือนกับปัญหาที่พบในการย่อหรือขยายขนาดของภาพ

การกลับด้านของภาพ (Flip) คือเมื่อสลับด้านซ้ายขวาของภาพ จะมีผลกับอัลกอริทึมที่ฝังลายน้ำลงในตำแหน่งที่ตายตัว

2.5.3 แทมเปอร์ริงและคอลลูชัน

มีข้อตกลงกันอย่างแพร่หลายว่า อัลกอริทึมของการทำลายน้ำควรจะยอมให้มีการฝังรหัสหลายๆ รหัสลงในข้อมูลเดียวกันได้ โดยที่ลายน้ำก่อนหน้าไม่ควรถูกทำให้คุณภาพลดลงไปเนื่องจากการฝังรหัสใหม่ลงไป สิ่งนี้เป็นลักษณะพิเศษสุดท้ายที่สำคัญสำหรับความคงทนต่อการทำลายน้ำปลอมขึ้นมา โดยเฉพาะอย่างยิ่งอัลกอริทึมต้องทนทานต่อการทำแทมเปอร์ เช่น การพยายามเปลี่ยนลายน้ำ และการทำคอลลูชัน เช่น บุคคลหลายๆ คนร่วมกันพยายามทำลายลายน้ำ การทำแทมเปอร์อาจมีจุดมุ่งหมายไปที่การลบลายน้ำ โดยใช้การประมวลผลสัญญาณหรือการทำทางด้านเรขาคณิต หรือทำการแก้ไขลายน้ำ ซึ่งเป็นเรื่องง่ายถ้าหากทำการฝังรหัสที่สามารถอ่านได้แบบเปิดเผย ส่วนคอลลูชันมุ่งไปที่การลบลายน้ำเป็นหลักและสามารถทำได้ง่าย ซึ่งยังไม่ปรากฏว่ามีวิธีใดสามารถจัดการกับการลบลายน้ำด้วยวิธีนี้ได้

โดยทั่วไปแล้ว ดูเหมือนว่าการทำให้การตรวจหาหรือการอ่านลายน้ำจากภาพควรจะชัดเจน ดังนั้นจึงเป็นสิ่งสำคัญที่ยอมให้ฝ่ายจัดซื้อสามารถตรวจหาและอ่านลายน้ำได้ แต่ควรป้องกันฝ่ายจัดซื้อไม่ให้ลบลายน้ำออกไปโดยการทำการประมวลผลบางอย่างกับภาพโดยบังเอิญ

2.6 เทคโนโลยีสำหรับการป้องกันการละเมิดลิขสิทธิ์ [15]

2.6.1 การป้องกันการละเมิดลิขสิทธิ์ในดีวีดี (Digital Video Disc Copy Protection)

ดิจิตอลดีวีดีโอดีสค์ หรือดีวีดีเป็นสื่อชนิดหนึ่งที่ใช้เก็บข้อมูลดิจิตอลซึ่งมีความจุที่สูงมาก และกำลังจะเข้ามาแทนที่แผ่นซีดีซึ่งมีความจุน้อยกว่า การคัดลอกข้อมูลจากแผ่นดีวีดีนั้นสามารถทำได้อย่างง่ายดายโดยใช้เครื่องบันทึกวีดีโอเทป (VCR: Video Cassette Recorder) ต่อเข้ากับเครื่องเล่นดีวีดี (DVD Display) และทำการบันทึกสัญญาณที่ส่งออกมาทางด้านเอาต์พุท ทำให้ได้มีแผ่นวีดีโอเดือนเป็นจำนวนมากในเวลาอันรวดเร็ว ด้วยเหตุนี้จึงทำให้ผู้ผลิตดีวีดีถูกแย่งส่วนแบ่งทางการตลาดโดยมีแผ่นวีดีโอเดือนเหล่านี้ บริษัทมาโครวิชซึ่งเป็นบริษัทหนึ่งที่ได้พัฒนาเทคโนโลยีต่างๆ ในด้านความปลอดภัยในการสื่อสารข้อมูลให้กับโรงถ่ายภาพยนตร์และผู้ผลิตเครื่องรับส่งโทรทัศน์ ได้สังเกตเห็นถึงความสำคัญของปัญหาเหล่านี้ จึงได้ริเริ่มคิดค้นเทคโนโลยีเพื่อแก้ปัญหาดังกล่าว โดยใช้กระบวนการบางอย่าง เพื่อใช้ในการป้องกันการคัดลอกข้อมูล

กระบวนการที่ได้คิดค้นขึ้น จะถูกกระทำในขั้นตอนของการเขียนข้อมูลลงบนแผ่นดีวีดี โดยจะทำการกำหนดข้อมูลกลุ่มหนึ่งที่มีขนาดมากกว่าหนึ่งบิตให้เป็นบิตที่ใช้ในการควบคุมปริมาณการทำซ้ำ (Copy Protection Control Bits) โดยบิตเหล่านี้จะถูกเซตให้เป็น '1' ทั้งหมด เมื่อแผ่นดีวีดีถูกอ่านผ่านเครื่องเล่นดีวีดี บิตควบคุมเหล่านี้ก็จะถูกส่งผ่านชิพที่ทำหน้าที่เป็นตัวแปลงสัญญาณจากดิจิตอลเป็นอนาล็อก (Digital-to-Analog Converter) ที่อยู่บนแผงวงจรภายในเครื่องเล่นดีวีดี และถูกส่งออกไปพร้อมกับสัญญาณภาพออกทางจอโทรทัศน์ โดยบิตควบคุมเหล่านี้จะไม่ไปรบกวนการมองเห็นของสัญญาณภาพปกติที่ส่งออกไป แต่จะมีผลเมื่อมีการทำคัดลอกโดยใช้เครื่องบันทึกวีดีโอเทป ซึ่งจะทำให้สัญญาณภาพที่ถูกบันทึกมีความผิดเพี้ยนไปจากเดิม

นอกจากบริษัทมาโครวิชแล้ว ที่ห้องวิจัยของไอบีเอ็ม ณ กรุงโตเกียว ก็ได้เสนอเทคโนโลยีที่ช่วยป้องกันการละเมิดลิขสิทธิ์ในดีวีดีเช่นกัน เทคโนโลยีที่ไอบีเอ็มเสนอเป็นการทำภาพพิมพ์ลายน้ำดิจิตอล (Digital Watermarking) หรือการใส่ลายน้ำดิจิตอลลงในแผ่นดีวีดี ซึ่งภายหลังสามารถที่จะทำการตรวจสอบตัวลายน้ำที่ถูกใส่เอาไว้ในแผ่นดีวีดีนั้นได้ ลายน้ำดิจิตอลที่ถูกใส่อยู่ในดีวีดีนั้นจะอยู่ในส่วนของข้อมูลที่ไม่สามารถมองเห็นได้ โดยผู้ที่เป็นเจ้าของลิขสิทธิ์จะเป็นผู้กำหนดว่าจะใส่ข้อมูลใดเข้าไป ข้อมูลนี้จะถูกเรียกว่า “ข้อความสำหรับควบคุมการทำซ้ำ” (CCI: Copy Control Information) เช่น “Never Copy” “Copy Once” หรือ “Copy Free” เป็นต้น ซึ่งข้อมูลเหล่านี้จะมีผลทำให้อุปกรณ์บันทึกหรือเครื่องเล่นดีวีดีหยุดการทำงานโดยอัตโนมัติ เมื่อมีการกระทำที่ไม่เป็นไปตามข้อความสำหรับการควบคุมนั้น เช่นกรณีที่เครื่องเล่นดีวีดี ตรวจพบข้อความ “Never Copy” เมื่อมีการทำคัดลอกเกิดขึ้นตัวเครื่องจะหยุดการบันทึกทันที หรือในกรณีที่ตรวจพบข้อความ “Copy Once” เมื่อมีการคัดลอกทำเกิดขึ้น ก่อนที่ตัวเครื่องจะทำการบันทึกมันก็จะทำการแก้ไขสถานะของข้อมูลไปเป็น “Never Copy” ทำให้ครั้งต่อไปไม่สามารถทำการคัดลอกได้อีก

2.6.2 การป้องกันการละเมิดลิขสิทธิ์ในวีดีโอเทป (Videocassette Copy Protection)

เทคโนโลยีที่ใช้ในการป้องกันการคัดลอกที่ผิดกฎหมายในวีดีโอเทป มีหลักการก็คือ การเพิ่มสัญญาณอิเล็กทรอนิกส์เข้าไปในสัญญาณวีดีโอในขั้นตอนของการผลิต ซึ่งสัญญาณพัลส์นี้จะไม่มีผลใดๆ ต่อตัวเทป ที่ผ่านกระบวนการผลิตอย่างถูกต้อง แต่สัญญาณนี้จะมีผลเมื่อมีการทำซ้ำโดยใช้เครื่องบันทึกวีดีโอเทป โดยจะไปปรับกวนระบบการบันทึกภายในเครื่อง (VCR 's Automatic Gain Control) ทำให้คุณภาพของภาพที่ถูกบันทึกเสียหาย เช่นสัญญาณภาพมีลักษณะมืดหรือมีสัญญาณรบกวน สีของภาพขาดหายไป สัญญาณภาพขาดหายไปเป็นบางเฟรมหรือไม่มีสัญญาณภาพเลย เป็นต้น

2.6.3 การป้องกันการละเมิดลิขสิทธิ์ในซอฟต์แวร์ (Computer Software Protection)

ปัจจุบันจะเห็นได้ว่ามีซอฟต์แวร์เถื่อนผลิตและวางจำหน่ายอยู่อย่างเกลื่อนตลาด ทำให้ผู้ที่เป็นเจ้าของลิขสิทธิ์ในซอฟต์แวร์เหล่านั้นต้องสูญเสียผลประโยชน์อย่างมาก เนื่องจากผู้ใช้ส่วนใหญ่ต่างก็หันไปใช้ซอฟต์แวร์เถื่อนเหล่านี้ โดยไม่คำนึงถึงคุณค่าและความสำคัญของทรัพย์สินทางปัญญาที่เกิดจากการใช้ความคิดและความพยายามทุ่มเทเป็นอย่างมากของเจ้าของผลงาน จึงได้มีการคิดค้นเทคโนโลยีที่จะป้องกันการละเมิดลิขสิทธิ์ในซอฟต์แวร์ต่างๆ ขึ้นมา

โดยทั่วไปปัญหาของการใช้ซอฟต์แวร์โดยผิดกฎหมายสามารถแบ่งออกเป็น 4 ลักษณะ ดังนี้

1. Softlifting เป็นลักษณะการใช้ซอฟต์แวร์แบบ Single Licensed Copy คือการนำซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องไปใช้กับคอมพิวเตอร์หลายๆเครื่อง หรือเป็นการใช้ซอฟต์แวร์ร่วมกันหลายๆ คน
2. Renting เป็นการคัดลอกซอฟต์แวร์ประเภทให้เช่าหรือใช้ได้ชั่วคราวมาใช้ส่วนตัว
3. Software Counterfeiting เป็นการคัดลอกซอฟต์แวร์ที่มีลิขสิทธิ์ แล้วนำมาจัดจำหน่ายในรูปแบบที่ดูเหมือนถูกกฎหมาย
4. Downloading เป็นการใช้ซอฟต์แวร์ของผู้ใช้ที่ไม่มีสิทธิ์ถูกต้อง โดยใช้วิธีการดาวน์โหลดซอฟต์แวร์มาใช้ผ่านทางอินเทอร์เน็ต

SafeDisk และ SafeCast คือสองโปรแกรมหลักที่บริษัทมาโครวิชั่นได้คิดค้นขึ้นเพื่อแก้ปัญหาการละเมิดลิขสิทธิ์ในการใช้ซอฟต์แวร์ ซึ่งกำลังเป็นปัญหาอยู่ในปัจจุบัน ซึ่งอาจยังไม่เป็นที่รู้จักแพร่หลายนักในประเทศไทย

1. SafeDisc เป็นโปรแกรมตัวแรกที่มาโครวิชั่นผลิตขึ้น โดยมีชื่อทางการค้าว่า SafeDisc ตัวโปรแกรมถูกใช้เพื่อช่วยให้ผู้ผลิตซอฟต์แวร์สามารถป้องกันการคัดลอกข้อมูลที่ถูกเก็บในแผ่นซีดีรอม หรือป้องกันการใช้งานของตัวซอฟต์แวร์โดยไม่ได้รับอนุญาตได้ นอกจากนี้ SafeDisc ยังสามารถป้องกันการคัดลอกโดยการดาวน์โหลดผ่านทางเครือข่ายอินเทอร์เน็ตได้อีกด้วย ตัวเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โปรแกรมได้รับการออกแบบให้สามารถป้องกันการคัดลอกข้อมูลลงในตัวฮาร์ดดิสก์ของคอมพิวเตอร์ หรือบันทึกลงในแผ่นซีดี โดยหลักการอย่างง่าย ๆ SafeDisc จะใช้แผ่นซีดีรอมที่เก็บตัวซอฟต์แวร์เป็นเสมือนกุญแจรหัสในการเข้าไปใช้ซอฟต์แวร์ นั่นคือซอฟต์แวร์จะทำงานได้ก็ต่อเมื่อมีซีดีรอมแผ่นจริงอยู่ในไดรว์เท่านั้น

เทคโนโลยีของ SafeDisc จะประกอบด้วยส่วนที่สำคัญ 3 ประการด้วยกัน คือ

- ลายเซ็นดิจิทัล (Digital Signature)
- การเข้ารหัสข้อมูล (Encrypted Wrapper Protection)
- การป้องกันการเข้าถึงตัวข้อมูล (Anti-Hacking Software)

ในขั้นตอนการผลิต ข้อมูลทั้งหมดของซอฟต์แวร์จะถูกนำมาเข้ารหัส จากนั้น SafeDisc จะสร้างลายเซ็นดิจิทัลที่มีค่าเฉพาะสำหรับซอฟต์แวร์แต่ละตัว เมื่อผู้ใช้เปิดแผ่นซีดีรอมขึ้นมา ตัวโปรแกรมก็จะทำการตรวจสอบลายเซ็นดิจิทัลจากข้อมูลในแผ่นซีดีรอมนั้นเพื่อยืนยันว่าซอฟต์แวร์ที่กำลังใช้งานอยู่เป็นของแท้ จากนั้นจึงยอมให้ซอฟต์แวร์ดังกล่าวถอดรหัส (Decryption) จึงจะสามารถใช้ซอฟต์แวร์ได้ตามปกติ แต่ถ้าโปรแกรมตรวจสอบไม่พบลายเซ็นดิจิทัลดังกล่าวก็จะไม่สามารถใช้งานซอฟต์แวร์นั้นได้

2. SafeCast โปรแกรมนี้ได้รับการออกแบบขึ้นมาเพื่อช่วยนักพัฒนาโปรแกรมในการป้องกันการใช้ซอฟต์แวร์ที่ยังไม่วางจำหน่ายเผยแพร่ หรือซอฟต์แวร์ที่อยู่ในขั้นของการทดลองใช้งาน มิให้มีการทำซ้ำหรือใช้งานโดยไม่ได้รับอนุญาต นั่นคือทำให้สามารถควบคุมการแพร่กระจายของซอฟต์แวร์ให้อยู่ในขอบเขตที่ต้องการได้ ในขณะที่ SafeDisc ใช้สำหรับการป้องกันการใช้ซอฟต์แวร์ที่ออกวางจำหน่ายแล้ว ซึ่งจุดนี้เองที่เป็นจุดแตกต่างระหว่าง SafeCast และ SafeDisc การทำงานของ SafeCast สามารถสรุปได้คือ ผู้ที่เป็นเจ้าของซอฟต์แวร์สามารถเข้ารหัสตัวข้อมูลที่ต้องการก่อนที่จะเผยแพร่ซอฟต์แวร์ดังกล่าวไปยังผู้ใช้โดยตรง หลังจากนั้นผู้ที่ต้องการใช้ซอฟต์แวร์จะต้องติดต่อกับผู้ที่เป็นเจ้าของโดยตรง หรือผ่านทางเครือข่ายอินเทอร์เน็ต เพื่อขอรับกุญแจรหัสที่ใช้ในการถอดรหัสข้อมูลจึงจะสามารถใช้งานซอฟต์แวร์นั้นได้

นอกจากนี้ SafeCast ยังสามารถทำงานในแบบ “Try and Die” คือ ข้อมูลที่เข้ารหัสไว้จะมีการกำหนดวันสิ้นสุดการใช้งานไว้ เมื่อครบกำหนดผู้ใช้ก็จะไม่สามารถใช้ซอฟต์แวร์นั้นได้อีกต่อไป หรือในลักษณะการทำงานที่คล้ายคลึงกันคือ การทำงานแบบ “Try Before You Buy” ซึ่งจะถูกใช้เมื่อต้องการให้บุคคลทั่วไปทดลองใช้ซอฟต์แวร์นั้น แต่จะถูกควบคุมการทำงานบางอย่าง นั่นก็คือไม่สามารถใช้งานโปรแกรมได้เต็มความสามารถ แต่เมื่อผู้ใช้ตัดสินใจซื้อ ก็จะได้รับซอฟต์แวร์ที่มีการทำงานสมบูรณ์ไป

2.6.4 การป้องกันการละเมิดลิขสิทธิ์ในเพลง (Music Copyright Protection)

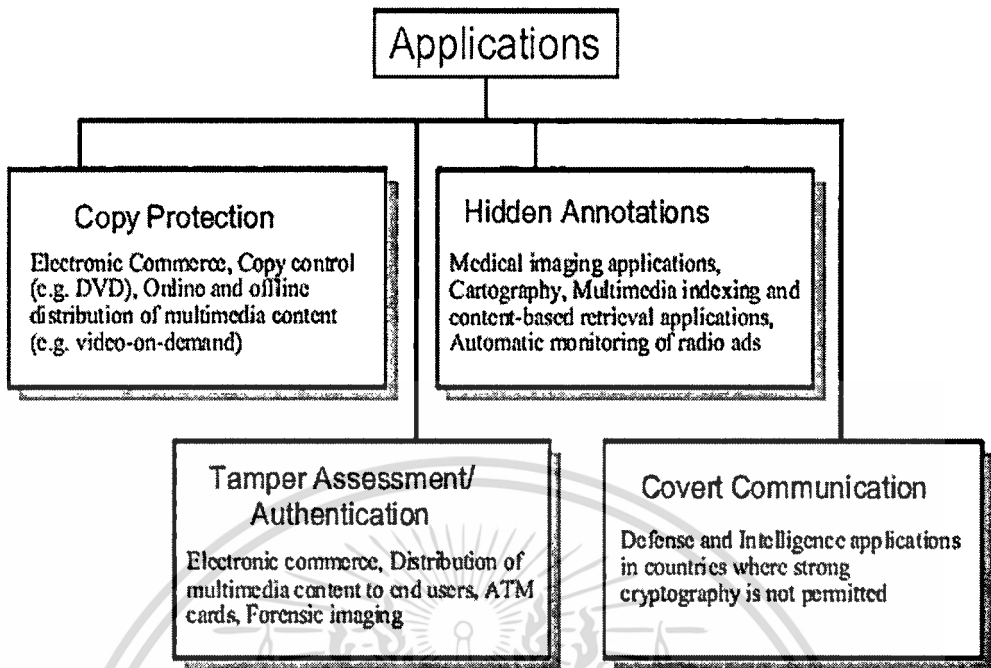
เสียงเพลงที่อยู่ในรูปสัญญาณดิจิทัล นับเป็นสื่ออย่างหนึ่งที่ทำให้เกิดปัญหาการละเมิดลิขสิทธิ์อย่างกว้างขวาง ในต่างประเทศจึงได้มีการรวมตัวกันของบริษัทต่างๆที่มีความเกี่ยวข้องในอุตสาหกรรมเพลงเพื่อทำการวิจัยและพัฒนาเทคโนโลยีเพื่อใช้ในการแก้ปัญหาดังกล่าว โดยใช้ชื่อกลุ่มวิจัยนี้ว่า SDMI (Secure Digital Music Initiative) สิ่งในกลุ่ม SDMI คาดหวังก็คือการทำให้เครื่องเล่นหรือเครื่องบันทึกเสียงเพลงในอนาคต มีความสามารถในการยับยั้งขัดขวางการคัดลอกที่ผิดกฎหมายได้โดยอาศัยเทคโนโลยีต่างๆในการป้องกัน เทคโนโลยีหนึ่งที่จะกล่าวถึงในที่นี้ก็คือ เทคโนโลยีการทำภาพพิมพ์ลายน้ำดิจิทัลนั่นเอง โดยตัวลายน้ำดิจิทัลนี้ก็จะเป็ยสัญญาณเฉพาะที่สร้างขึ้นเพื่อจะซ่อนอยู่ในสัญญาณเสียง ภาพ หรือวิดีโอ ซึ่งสัญญาณที่ถูกใส่นี้สามารถบ่งบอกถึงข้อมูลที่เกี่ยวข้องกับลิขสิทธิ์ หรือข้อกำหนดในการใช้ข้อมูลได้ ปัจจุบันจึงได้มีการนำเทคโนโลยีดังกล่าวไปประยุกต์ใช้ในหลายๆ ด้าน กลุ่ม SDMI ก็เช่นกันที่ได้นำเทคโนโลยีนี้มาประยุกต์ใช้ในระบบการป้องกันการละเมิดลิขสิทธิ์ในเพลง โดยออกแบบตัวอุปกรณ์เครื่องเล่นหรือบันทึกให้มีความสามารถในการตรวจสอบข้อมูลลายน้ำดิจิทัลก่อนที่จะทำงานตามปกติ ตัวอย่างการใช้งานของระบบที่ SDMI คิดค้นก็คือ ผู้ใช้สามารถที่จะหาซื้อแผ่นซีดีที่มีการป้องกันไว้ได้ตามร้านทั่วไป และสามารถเปิดแผ่นซีดีนั้น ได้ด้วยเครื่องเล่นซีดีที่เป็นที่ยอมรับของ SDMI (SDMI-Compliant CD Player) แต่เมื่อไรก็ตามที่มีการคัดลอกเพลงจากซีดีแผ่นนี้ แล้วนำไปแปลงเป็นไฟล์ MP3 เพื่อนำไปเผยแพร่ทางอินเทอร์เน็ต จะมีผลทำให้ผู้ที่ดาวน์โหลดไฟล์ MP3 นี้ไปไม่สามารถที่จะเปิดฟังได้ในเครื่องเล่นที่ได้รับการรับรองโดย SDMI เป็นต้น

2.7 การประยุกต์ใช้เทคนิคการซ่อนลายน้ำ

การประยุกต์ใช้ลายน้ำดิจิทัลสามารถแบ่งออกได้เป็น 4 กลุ่มหลักๆ คือ [8]

1. การป้องกันการคัดลอก (Copy Protection)
2. การซ่อนคำอธิบายประกอบ (Hidden Annotations)
3. การพิสูจน์ความถูกต้อง (Tamper Assessment / Authenticity)
4. ความปลอดภัยโดยไม่พบในการสื่อสาร (Covert Communications)

ความนิยมในการใช้เทคโนโลยีนี้กับมัลติมีเดียจะเห็นได้จากความต้องการให้มีรูปแบบมาตรฐานสำหรับกระบวนการสร้างลายน้ำเพื่อสื่อมัลติมีเดียหลักๆ เช่น Digital Versatile Disk (DVD), MP3, MPEG-4, JPEG2000 และอื่นๆ



รูปที่ 2.10 การประยุกต์ใช้เทคนิคการทำลายน้ำ

2.7.1 การป้องกันการคัดลอก

ในงานประยุกต์นี้ ข้อมูลที่อยู่ในกระบวนการทำลายน้ำจะเกี่ยวกับผู้สร้าง ผู้เผยแพร่ ผู้ซื้อ หรือเงื่อนไขในลิขสิทธิ์ระหว่างพวกเขาสามารถที่จะฝังลงไปในส่วนของข้อมูลมัลติมีเดียได้ เมื่อได้ทำการฝังข้อมูลลงไปแล้ว เราสามารถตรวจหากรรมสิทธิ์ได้ในภายหลังว่าได้มาอย่างถูกต้องหรือไม่ สมมุติว่าเจ้าของข้อมูลได้จัดหาภาพให้แก่ลูกค้าไปเพื่อตีพิมพ์ โดยได้รับค่าธรรมเนียมสำหรับการใช้ภาพนั้นๆ แต่อย่างไรก็ตาม ผู้ที่นำภาพไปพิมพ์มีโอกาสที่จะละเลยไม่จ่ายค่าธรรมเนียมนี้ได้ เพื่อยับยั้งการละเมิดลิขสิทธิ์นี้ เจ้าของสามารถที่จะฝังลายน้ำซึ่งเป็นข้อมูลที่สามารแสดงถึงความเป็นเจ้าของของผู้ที่ได้รับสิทธิ์ในการตีพิมพ์ได้ ในกรณีแรกลายน้ำใช้สำหรับยืนยันความเป็นเจ้าของได้ (Ownership Assertion) ซึ่งเจ้าของสามารถควบคุมและตรวจสอบข้อมูลที่ถูกตีพิมพ์ที่น่าสงสัยได้ โดยตรวจหาลายน้ำที่แสดงความเป็นเจ้าของที่ถูกฝังไว้ได้ ถ้าปรากฏว่ามีลายน้ำปรากฏอยู่อย่างชัดเจนก็สามารถที่จะใช้เป็นหลักฐานในการแสดงความเป็นเจ้าของได้ ในกรณีที่สอง ลายน้ำใช้สำหรับการพิมพ์ลายนิ้วมือ (Fingerprinting) เพื่อป้องกันผู้ที่ไม่ได้รับอนุญาตทำสำเนาและทำการแจกจ่ายภาพ โดยเจ้าของสามารถฝังข้อมูลที่ระบุถึงผู้ที่ได้รับอนุญาตให้ตีพิมพ์ภาพนั้นๆ ได้ ถ้าหากมีการตรวจพบการทำสำเนาภาพโดยไม่ได้รับอนุญาตซึ่งเจ้าของสามารถระบุผู้รับต้นแบบและทำการยกเลิกการทำธุรกิจกับผู้นั้นได้ ในบางเหตุการณ์สำหรับการป้องกันลิขสิทธิ์อาจจะใช้ลายน้ำที่สามารถมองเห็นได้หรือไม่สามารถมองเห็นได้ก็ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.7.2 การซ่อนคำอธิบายประกอบ

การทำลายน้ำดิจิทัล สามารถใช้ในการซ่อนฉลากข้อความและหมายเหตุไว้ในข้อมูลมัลติมีเดีย โดยใช้ในการติดฉลากข้อความ (Content Labeling) การทำดรรชนีและติดตามข้อมูลมัลติมีเดีย ใช้ในการควบคุม ใช้ในงานที่ต้องการควบคุมระดับในการเข้าถึงข้อมูล หรือในแผนที่และภาพถ่ายทางการแพทย์ ในการทำฉลาก รหัสที่ฝังเข้าไปประกอบด้วยคำอธิบายของข้อมูลที่เกี่ยวข้องกับข้อความภายใน เช่น ภาพถ่ายสามารถที่จะใส่รายละเอียดเกี่ยวกับวัน เวลา สถานที่ในภาพได้โดยอัตโนมัติเมื่อทำการถ่ายภาพ ไลยน้ำสามารถใช้ในการป้องกันข้อมูลดิจิทัลวิดีโอในระบบปิดได้ โดยใช้ฮาร์ดแวร์พิเศษสำหรับทำสำเนาและดูรายละเอียด ซึ่งจะมีรหัสที่แสดงถึงจำนวนครั้งที่อนุญาตให้ทำสำเนา ดังนั้นทุกครั้งเมื่อมีการทำสำเนาฮาร์ดแวร์ตัวนี้จะทำการเปลี่ยนแปลงรหัสและเมื่อจำนวนเท่ากับศูนย์ระบบจะไม่สามารถดูข้อมูลได้อีก เช่น DVD (Digital Video Disc) ในงานประยุกต์ใหม่ๆ จะสามารถกำหนดระดับในการเข้าถึงข้อมูลมัลติมีเดียได้หลายระดับ โดยใช้การทำลายน้ำ การควบคุมรายละเอียดของภาพ ถ้าผู้ใช้มีระดับในการเข้าถึงสูงรายละเอียดของภาพก็จะปรากฏออกมา แต่ถ้าผู้ใช้มีระดับในการเข้าถึงต่ำก็จะไม่สามารถเห็นรายละเอียดของภาพได้ อีกกรณีหนึ่งสำหรับข้อมูลเพิ่มเติม อย่างในการแสดงระบบแทร็กหลายภาษา (Multilingual Tracks) สามารถฝังลงในไฟล์วิดีโอได้ในการแพร่ภาพ ในงานเกี่ยวกับทางการแพทย์ ระบบการทำลายน้ำสามารถฝังการบันทึกของผู้ป่วยลงในภาพเอ็กซเรย์ได้ เพื่อเพิ่มความรวดเร็วในการดูบันทึก และป้องกันความผิดพลาดที่ไม่ตรงกันระหว่างของบันทึกคนไข้และภาพ

2.7.3 การพิสูจน์ความถูกต้อง

ในบางงานประยุกต์ อย่างเช่นพาณิชย์อิเล็กทรอนิกส์เกี่ยวกับข้อมูลมัลติมีเดีย ภาพถ่ายทางการแพทย์ ภาพข่าว ซึ่งมีความสำคัญมากถ้าหากมีการปรับเปลี่ยนหรือแต่งเติมรายละเอียดข้อมูลลงไปให้แตกต่างจากต้นฉบับ โดยการแก้ไขนี้มีผลไปในทางลบแล้วถูกเผยแพร่ออกไปจะเกิดผลเสียหายอย่างมาก ซึ่งป้องกันได้โดยใช้อัลกอริทึมของลายเซ็นดิจิทัลและคริปโตกราฟี แต่อย่างไรก็ตามการใช้เทคนิคการทำลายน้ำสามารถตรวจสอบความถูกต้องได้ง่าย โดยเหตุที่ผู้ที่มีสิทธิ์รับรองถูกฝังข้อมูลโดยตรงลงในเนื้อหา ไลยน้ำถูกแยกจากวัตถุที่อาจเกิดความเสียหายได้ ถ้าตรงกับรหัสที่ฝังเอาไว้ ดังนั้นข้อมูลนั้นตั้งสันนิษฐานได้ว่าไม่เกิดความเสียหายมาก่อนและระบุถึงผู้สร้างได้ด้วยรหัสนี้ ถ้าไลยน้ำไม่ตรงกับรหัสที่ฝังไว้แสดงว่าเกิดความผิดปกติขึ้นในข้อมูล ดังนั้นไลยน้ำแบบนี้ถูกเรียกว่า *fragile* โดยในกรณีที่รหัสถูกแก้ไขได้ง่ายโดยการแก้ไขเนื้อหา ซึ่งแตกต่างจากงานประยุกต์ก่อนนี้ซึ่งไลยน้ำจำเป็นต้องมีความคงทนสูง

2.8.4 ความปลอดภัยโดยไม่ปรากฏในการสื่อสาร

ลายน้ำดิจิทัลถูกใช้ในวงกว้างเหมือนกับการซ่อนแขนเนลของการสื่อสาร ซึ่งซ่อนข้อมูลจำนวนมากไว้ในข้อมูลเสียง ภาพ และวิดีโอ งานประยุกต์เหล่านี้ถูกใช้ในทางทหารและบริการข่าวสารโดยใช้เทคนิคของคริปโตกราฟีและสเตเกโนกราฟี



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

เทคนิคการซ่อนลายน้ำในโดเมนความถี่สำหรับภาพดิจิทัล

ในการศึกษาวิจัยวิทยานิพนธ์นี้ได้เสนอวิธีการซ่อนลายน้ำภาพดิจิทัล โดยใช้การฝังภาพสัญลักษณ์ลับ 2 มิติแบบไบนารีในภาพดิจิทัลต้นฉบับแบบโทนสีเทาด้วยเทคนิคการแปลงฟูริเยร์ (Fourier Transform) และเทคนิคโคไซน์ครีตโคซายน์ทรานส์ฟอร์ม (Discrete Cosine Transform) ลายน้ำจะถูกฝังลงในโดเมนความถี่ของภาพดิจิทัลต้นฉบับ กระบวนการในการฝังลายน้ำและตรวจหาลายน้ำที่ฝังไว้ทั้ง 2 วิธีการดังกล่าวจะได้กล่าวต่อไปในเนื้อหาของบทนี้ รวมถึงการตรวจสอบความผิดพลาดและรวมถึงการเปรียบเทียบลายน้ำของภาพสัญลักษณ์ลับที่ทำการฝังไว้ เพื่อให้การวิจัยมีความน่าเชื่อถือและสามารถวัดและเปรียบเทียบเพื่อพัฒนาต่อไปได้

3.1 การสร้างสัญญาณลายน้ำดิจิทัล

กระบวนการสร้างสัญญาณลายน้ำดิจิทัล (Digital Watermark) ที่นำเสนออันดับแรกประกอบด้วย ภาพสัญลักษณ์ลับแบบไบนารี (s) ที่ทำการแปลงบริเวณพิกเซลที่เป็นข้อมูลภาพให้มีค่าเป็น 1 และพิกเซลที่เป็นพื้นหลัง (Background) ให้มีค่าเป็น -1

$$S = \{s_i, 1 \leq i \leq M\}, \quad s_i \in \{-1, 1\} \quad (3.1)$$

ลำดับของ s_i จะถูกขยายด้วยแฟกเตอร์ของแอมพลิจูดที่ปรับได้ ($\alpha \geq 0$) เป็นค่าคงที่ที่กำหนดจากความคงทนของสัญลักษณ์ที่ใช้ ค่าของ α จะถูกเลือกเพื่อให้ได้ค่าที่ดีที่สุดระหว่างความคงทนกับการไม่ปรากฏให้เห็น ในการเลือกค่าของ α ทำให้มีผลต่อประสิทธิภาพของระบบสองด้าน คือมีผลกระทบต่อการทำให้สังเกตเห็นได้ เมื่อ α มีค่าสูงจะทำให้ลายน้ำปรากฏเด่นชัดมากขึ้นหมายถึงทำให้สังเกตเห็นได้มากขึ้น แต่ก็ทำให้ระบบมีความคงทนมากขึ้นด้วย ในทางตรงกันข้ามหาก α มีค่าน้อยจะทำให้ลายน้ำไม่ปรากฏให้เห็นเด่นชัดมากหมายถึงทำให้สังเกตเห็นได้ยากขึ้น แต่ก็ทำให้ระบบมีความคงทนน้อยลงด้วย นำค่าที่ได้ไปมอดูเลตด้วยลำดับสัญญาณรบกวนแบบสุ่ม (Pseudo-Random Sequence : p) ซึ่งสร้างขึ้นโดยใช้ค่า Seed เป็นกุญแจลับในการสร้างสัญญาณรบกวนแบบสุ่มนี้ขึ้นมา โดยการเพิ่มลำดับแบบสุ่มลงไปในการฝังลายน้ำ และการตรวจหาลายน้ำ จะต้องทำการสร้างลำดับสัญญาณรบกวนแบบสุ่มขึ้นมาใหม่โดยใช้ค่า Seed ที่ถูกต้องโดยไม่ต้องใช้ภาพต้นแบบ โดยแต่ละจำนวนมีค่าเป็น 1 และ -1 ดังนั้นลำดับที่ใช้นั้นจึงไม่ควรง่ายเกินไปเพื่อให้การจะคาดเดาทำได้ยากและเป็นการรักษาความปลอดภัยจากผู้ที่ไม่ได้รับสิทธิ์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$P = \{p_i, 1 \leq i \leq M\}, \quad p_i \in \{-1, 1\} \quad (3.2)$$

3.2 กระบวนการซ่อนลายนำด้วยเทคนิคการแปลงฟูรีเยร์ (Fourier Transform) [13]

กระบวนการซ่อนลายนำดิจิทัลโดยปกติจะแบ่งออกเป็น 2 ส่วน ประกอบด้วย การฝังลายนำลงในภาพดิจิทัลและการตรวจหาลายนำดิจิทัลกลับคืน

3.2.1 การฝังลายนำด้วยเทคนิคการแปลงฟูรีเยร์

ในการฝังลายนำในโดเมนความถี่กับภาพดิจิทัลต้นฉบับจะใช้วิธีการ FFT (Fast Fourier Transform) แบบ 2 มิติในการแปลงข้อมูลภาพต้นฉบับสู่โดเมนความถี่ การแปลงระหว่างสัญญาณในเชิงความถี่และเชิงเวลาอยู่หลายแบบซึ่งทุกแบบก็มีวัตถุประสงค์เดียวกันคือต้องการแปลงระหว่างสัญญาณในเชิงเวลากับสัญญาณในเชิงความถี่ (สเปกตรัม) จุดที่แตกต่างกันของการแปลงแต่ละแบบก็คือ คุณลักษณะของสัญญาณที่จะแปลงเท่านั้น ซึ่งเมื่อกล่าวถึงการแปลง FFT โดยหลักการแล้วขอให้นึกถึงว่ามันคือ การแปลง DFT (Discrete Fourier Transform) นั่นเอง การแปลง DFT มีทั้งสัญญาณในเชิงเวลา และในเชิงความถี่เป็นแบบไม่ต่อเนื่อง จุดนี้เป็นจุดที่สำคัญมากเพราะมันบ่งบอกว่าจะสามารถกระทำการแปลงโดยใช้การคำนวณ (การคูณ และบวก) ทางดิจิทัลได้ ซึ่งสามารถประยุกต์ได้สะดวกมากในคอมพิวเตอร์ หรือในฮาร์ดแวร์โดยตรงได้ ต่างกับการแปลงแบบอื่นที่มีสัญญาณแบบต่อเนื่องเกี่ยวข้องด้วยซึ่งทำให้การแปลงต้องใช้วิธีอินทิเกรตซึ่งยุ่งยากกว่ามาก เนื่องจากการแปลง DFT มีประโยชน์ในการใช้งานมาก จึงได้มีความพยายามคิดค้นหาวิธีที่จะคำนวณ DFT ให้เร็วขึ้น และมีประสิทธิภาพขึ้นกว่าปกติ การแปลง FFT ก็คือชื่อที่ใช้เรียก “วิธีการคำนวณ DFT อย่างรวดเร็ว” กว่าความคิดปกตินั่นเอง

การคำนวณ DFT โดยตรงจากนิยาม ถ้าสัญญาณมีความยาวเท่ากับ N จะต้องใช้ในการคำนวณถึงประมาณ N^2 CMACs (CMAC คือ Complex Multiplication and Accumulation, เป็นหน่วยวัดการคำนวณ ซึ่ง 1 CMAC เท่ากับการกระทำทางคณิตศาสตร์ที่ประกอบด้วย การคูณเลขเชิงซ้อน 2 จำนวน เสร็จแล้วนำเอาผลลัพธ์ที่ได้ไปบวกสมทบเข้ากับเลขเชิงซ้อนอีกจำนวนหนึ่ง) ซึ่งมีความสูงค่ามาก โดยเฉพาะเมื่อ N มีค่าสูงๆ การใช้ FFT จะช่วยลดจำนวน CMAC ที่ต้องใช้ลงได้มาก โดยการแปลงภาพโทนสีเทาขนาด $M \times N$ มีสมการในการแปลงดังนี้

สมการ Forward FFT

$$F(p, q) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m, n) e^{-j(2\pi/M)pm} e^{-j(2\pi/N)qn} \quad (3.3)$$

เมื่อ

$$p = 0, 1, \dots, M-1 \text{ และ } q = 0, 1, \dots, N-1$$

$F(p, q)$ คือค่าสัมประสิทธิ์ FFT

$f(m, n)$ คือค่าระดับสีในพิกเซล

เมื่อแปลงภาพต้นฉบับไปสู่โดเมนความถี่จะได้ค่าสัมประสิทธิ์เป็นจำนวนเชิงซ้อน (Complex Number) โดยให้สัมประสิทธิ์จริงและจินตภาพของความถี่ A แทนด้วย A_r และ A_i ตามลำดับ แมกนิจูดและเฟสของความถี่ A แทนด้วย $F(A)$ และ $P(A)$ ลำดับของลายน้ำจะฝังในแมกนิจูด $F(A)$ โดยมีรูปแบบการคำนวณดังสมการนี้

$$v'_i = v_i + \alpha \cdot p_i \cdot s_i \quad (3.4)$$

เมื่อ v_i เป็นลำดับของพิกเซลหรือแมกนิจูด

แฟคเตอร์ของแอมพลิจูด α เป็นค่าคงที่ที่โดยพิจารณาจากความคงทนของสัญลักษณ์ที่ใช้ ค่าของ α จะถูกเลือกเพื่อให้ได้ค่าที่ดีที่สุดในระหว่างความทนทานกับการมองไม่เห็น

หลังจากนั้นจะแปลง FFT กลับด้วย (3.5) เพื่อให้ได้ภาพที่ฝังลายน้ำ กระบวนการฝังลายน้ำดังที่กล่าวแสดงได้ดังรูปที่ 3.1

$$f(m, n) = \frac{1}{MN} \sum_{p=0}^{M-1} \sum_{q=0}^{N-1} F(p, q) e^{j(2\pi/M)pm} e^{j(2\pi/N)qn} \quad (3.5)$$

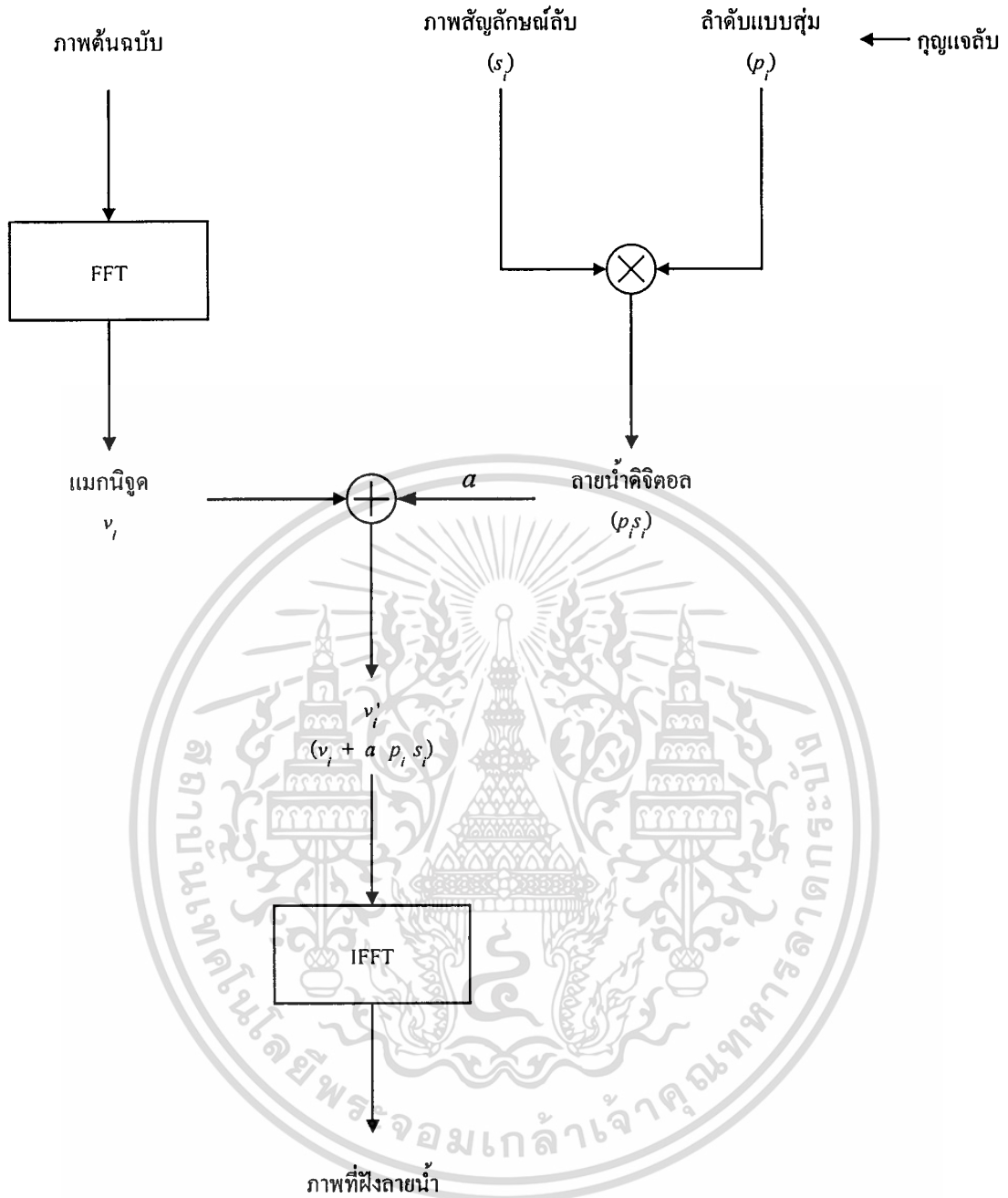
เมื่อ

$$m = 0, 1, \dots, M-1 \text{ และ } n = 0, 1, \dots, N-1$$

$F(p, q)$ คือค่าสัมประสิทธิ์ FFT

$f(m, n)$ คือค่าระดับสีในพิกเซล

เนื่องจากธรรมชาติของสัญญาณรบกวนแบบสุ่มมักมีสัญญาณรบกวน ดังนั้นสัญญาณลายน้ำซึ่งใช้สัญญาณรบกวนแบบสุ่มจะมีลักษณะเหมือนสัญญาณรบกวนเช่นกัน ด้วยเหตุนี้จึงทำให้ยากต่อการตรวจพบ ระบุตำแหน่ง และเปลี่ยนแปลงแก้ไข



รูปที่ 3.1 กระบวนการฝังลายน้ำดิจิทัลด้วยเทคนิคการแปลงฟูริเยร์

3.2.2 การตรวจหาลายน้ำจากการฝังลายน้ำด้วยเทคนิคการแปลงฟูริเยร์

ภาพที่ถูกฝังลายน้ำอาจพิจารณาได้ว่าเป็นภาพต้นฉบับที่ถูกรบกวนโดยสัญญาณแบบสุ่ม การคาดเดาภาพต้นฉบับจึงสามารถทำได้โดยใช้เทคนิคของการกำจัดสัญญาณรบกวน (Noise Reduction) โดยในวิทยานิพนธ์นี้เลือกตัวกรองสัญญาณแบบเฉลี่ยข้อมูล (Average Filtering) หรือที่ใช้ในการทำภาพให้เลือน (Smoothing) ในการกำจัดสัญญาณรบกวน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การ Smoothing ทำได้ง่าย โดยการคอนโวลูชัน (Convolution) ภาพกับมาสก์ (Mask) ขนาดเล็ก ๆ โดยมีหลักการทำงานดังนี้

$$f_f(i,j) = \frac{1}{k^2} \sum_{m=1}^k \sum_{n=1}^k f_{raw}(m,n) \quad (3.6)$$

โดยที่ $f_f(i,j)$ คือ จุดภาพตำแหน่งที่ i,j ที่ประมวลผลได้จากการกำจัดสัญญาณรบกวน
 $f_{raw}(m,n)$ คือจุดภาพเริ่มต้นที่นำเข้ามาประมวลผลโดยรวมจุดภาพ i,j
 k^2 คือ ขนาดของจุดจำนวนของจุดภาพรอบข้างของจุดภาพ i,j ที่นำมาเฉลี่ยข้อมูล

กรณีที่มาสก์มีขนาด 3×3 จะได้ว่า

$$f_f(i,j) = \frac{1}{9} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \times f_{raw}(m,n) \quad (3.7)$$

กรณีที่มาสก์มีขนาด 5×5 จะได้ว่า

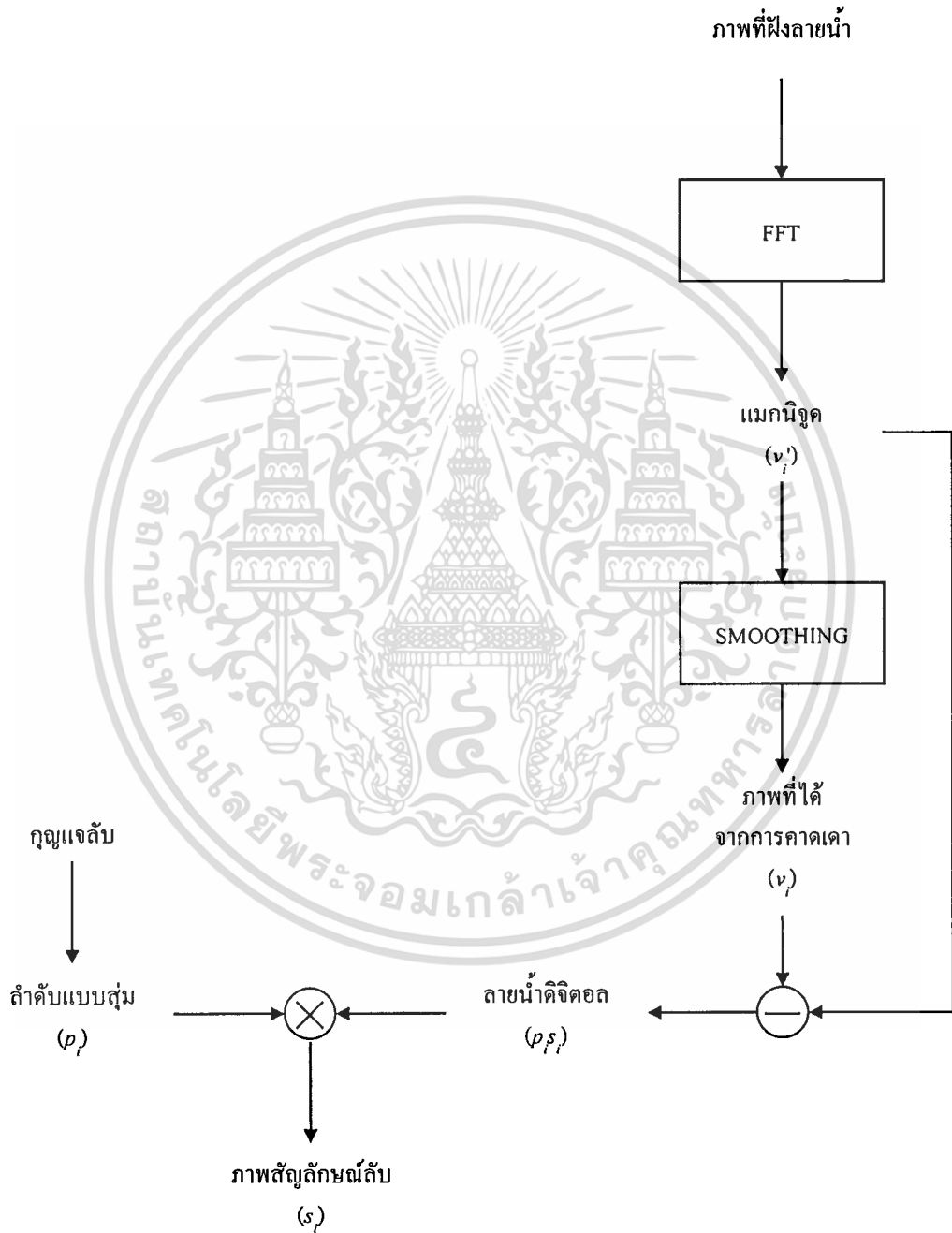
$$f_f(i,j) = \frac{1}{25} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \times f_{raw}(m,n) \quad (3.8)$$

นั่นคือเป็นการทำตัวกรองแบบเฉลี่ยข้อมูลที่มีมาสก์ขนาดต่าง ๆ มาทำคอนโวลูชันกับภาพที่ต้องการกำจัดสัญญาณรบกวนนั่นเอง

ซึ่งในวิทยานิพนธ์ฉบับนี้เลือกมาสก์ขนาด 5×5 ซึ่งสัมประสิทธิ์ทุกตัวมีค่าเท่ากันเท่ากับ $1/25$ การคาดเดาภาพต้นฉบับ v , จึงคำนวณได้ด้วยสูตรง่าย ๆ ดังนี้

$$v_i = \frac{1}{c \times c} \sum_{i=1}^{c \times c} v'_i \quad (3.9)$$

เมื่อ c เป็นขนาดของ Convolution Mask



รูปที่ 3.2 กระบวนการตรวจหาลายน้ำจากการฝงลายน้ำด้วยเทคนิคการแปลงฟูริเยร์

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เมื่อได้ค่าที่ทำการคาดเดาแล้ว นำมาหาค่าผลต่าง (δ) ของแมกนิจูดระหว่างค่าที่ทำการคาดเดาได้กับค่าของภาพที่มีลายน้ำ ค่าผลต่างที่ได้ก็คือค่าของบิตลายน้ำที่ฝังไว้ ($\alpha \cdot p_i \cdot s_i$) หลังจากนั้นสามารถทำการคำนวณหาค่า $p_i \cdot s_i$ ได้โดยการพิจารณาจากเครื่องหมายของค่าผลต่าง (δ) ที่หาได้ สุดท้ายสัญลักษณ์ดิจิตอลที่ถูกฝังไว้ (s_i) สามารถนำกลับคืนได้ด้วยการคูณกับลำดับสัญญาณรบกวนแบบสุ่ม (p_i) ซึ่งสร้างจากกฏเกณฑ์ที่ผู้ฝังลายน้ำทราบนั่นเอง โดยกระบวนการการตรวจหาลายน้ำดังกล่าวแสดงได้ดังรูปที่ 3.2

ถ้ารหัสลำดับแบบสุ่มถูกสร้างผิดจากครั้งแรก หรือไม่สัมพันธ์ (Synchronization) กับลำดับสุ่มแบบเดิมถูกนำมาใช้ ภาพที่แปลงกลับได้จะใช้ไม่ได้และบิต s_i ที่ได้กลับคืนจะเป็นบิตแบบสุ่ม (Random bit)

3.3 กระบวนการซ่อนลายน้ำด้วยเทคนิคโคไซน์ทรานส์ฟอร์ม (Discrete Cosine Transform)

กระบวนการซ่อนลายน้ำดิจิตอลโดยปกติจะแบ่งออกเป็น 2 ส่วน ประกอบด้วย การฝังลายน้ำลงในภาพดิจิตอล และการตรวจหาลายน้ำดิจิตอลกลับคืน

3.3.1 การฝังลายน้ำด้วยเทคนิคโคไซน์ทรานส์ฟอร์ม

ในขั้นตอนแรกจะนำภาพต้นฉบับที่จะทำการฝังลายน้ำทำการแปลง DCT 2 มิติ ภาพโทนาสึเทจขนาด $N \times N$ โดยมีสมการในการแปลงดังนี้
สมการ Forward DCT

$$C(u, v) = \frac{1}{\sqrt{2N}} \alpha(u) \alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \left[\frac{(2x+1)v\pi}{2N} \right] \cos \left[\frac{(2y+1)u\pi}{2N} \right] \quad (3.10)$$

เมื่อ

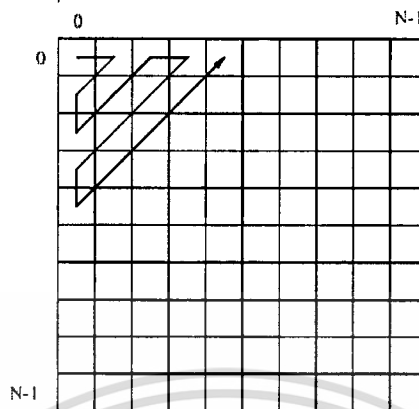
$C(u, v)$ คือค่าสัมประสิทธิ์ DCT

$f(x, y)$ คือค่าระดับสีในพิกเซล

$\alpha(i) = 1/\sqrt{2}$ เมื่อ $i = 0$ และ $\alpha(i) = 1$ เมื่อ $i > 0$

หลังจากผ่านการแปลง DCT แล้ว ค่าสัมประสิทธิ์ DCT จะถูกนำมาจัดเป็นลำดับ 1 มิติ โดยเรียงลำดับจากความถี่ต่ำไปยังความถี่สูงด้วยรูปแบบซิกแซกสแกน เช่นเดียวกับอัลกอริธึมการ

บีบอัดข้อมูลของ JPEG ดังแสดงในรูปที่ 3.3 สิ่งที่แตกต่างกันจากอัลกอริทึมที่ผ่านมาคือเป็นไปได้ยากในการถอดรหัสถ้าไม่มีภาพต้นฉบับอยู่ด้วย



รูปที่ 3.3 การเรียงลำดับของสัมประสิทธิ์ DCT ใหม่ในรูปแบบของซิกแซกสแกน

ในการฝังลายน้ำ เพื่อให้ได้ค่าที่ดีที่สุดระหว่างการไม่ปรากฏให้เห็นและความคงทน ค่าสัมประสิทธิ์ตั้งแต่ลำดับแรกถึงลำดับที่ L จะถูกข้ามไป โดยเหตุที่ระดับพลังงานของลายน้ำที่สูงจะทำให้สามารถตรวจหาได้ง่าย ลายน้ำที่ถูกสังเกตเห็นได้มีผลมาจากตำแหน่งของลายน้ำที่อยู่ในสเปกตรัมของ DCT ด้วยเหตุผลนี้ ทำให้ได้ช่วงที่เหมาะสมระหว่างการที่ไม่สามารถมองเห็นลายน้ำได้ ซึ่งหมายถึงการแทรกรหัสลงในองค์ประกอบความถี่สูงหรือความถี่กลางของภาพจะมีความคงทนต่อการเสียหายของภาพ และทำให้ง่ายในการตรวจหาลายน้ำกว่าลายน้ำถูกฝังอยู่ในสเปกตรัมความถี่ต่ำ จากการทดลองพบว่าเมื่อให้ $\alpha = 30$ และข้ามสัมประสิทธิ์ DCT ค่าแรกไปประมาณ $L = 50,000$ ค่า คือทำการฝังลายน้ำลงไปที่ยังสัมประสิทธิ์ตำแหน่งที่ 50,001 ไปจนถึง $50,001 + M$ ซึ่งทำให้ได้ช่วงที่เหมาะสมระหว่างการที่ไม่สามารถมองเห็นลายน้ำได้และความคงทนต่อการเสียหายของภาพ ที่จริงแล้วค่า α ที่สูงขึ้นจำเป็นต้องแทรกลายน้ำในความถี่ที่สูงขึ้น ทำให้ความคงทนต่อเทคนิคการประมวลผลภาพจะลดลงซึ่งเทคนิคแบบนี้จะไปเปลี่ยนแปลงองค์ประกอบที่ความถี่สูงของภาพ เช่น การกรองความถี่ต่ำ การบีบอัดภาพ ในอีกทางหนึ่งค่า α ไม่สามารถทำให้ต่ำลงมากเกินไปได้เพราะจะทำให้สูญเสียความคงทนของลายน้ำไป และ L ต้องไม่ควรต่ำกว่า 50,000 เพราะจะทำให้สามารถสังเกตเห็นลายน้ำได้มากขึ้นและค่า M เท่ากับจำนวนพิกเซลของภาพสัญลักษณ์ที่จะทำการฝัง ซึ่งทำให้ได้ช่วงและตำแหน่งที่เหมาะสม การกำหนดค่าที่แน่นอนให้กับ α และ L ทำให้เรามุ่งประเด็นไปที่ค่า PSNR ของภาพที่ถูกฝังลายน้ำแล้ว สำหรับค่า L และ M ได้ข้อสรุปสำหรับการทำลายน้ำด้วยวิธีนี้โดยคิดเป็นเปอร์เซ็นต์เมื่อเทียบกับขนาดของภาพ เพื่อความสะดวกในการทำลายน้ำกับภาพในขนาดอื่นๆ โดยเปอร์เซ็นต์คิดจากจำนวนลำดับทั้งหมดของภาพขนาด $N \times N$ จึงได้ $L = 20\%$ และ $M = 6.25\%$ ดังนั้นค่าสัมประสิทธิ์ตั้งแต่ลำดับที่ $L+1$ ถึง $L+M$ ในลำดับซิกแซก

สแกน จะถูกเลือกขึ้นมาเพื่อสร้างเวกเตอร์ $T = \{t_i, 1 \leq i \leq M\}$ และลายน้ำจะถูกฝังในเวกเตอร์ T เพื่อให้ได้เวกเตอร์ใหม่ $T' = \{t'_i, 1 \leq i \leq M\}$ เป็นเวกเตอร์ที่ผ่านการฝังลายน้ำแล้ว โดยมีรูปแบบการคำนวณดัง สมการนี้

$$t'_i = t_i + \alpha \cdot p_i \cdot s_i, \quad i = 1, 2, \dots, M \quad (3.11)$$

เวกเตอร์ T' จะถูกแทรกกลับลงไปในซิกแนกสแกนอีกครั้ง และทำการแปลง DCT กลับ เพื่อให้ได้ภาพที่ฝังลายน้ำ ดังแสดงขั้นตอนการฝังลายน้ำในรูปที่ 3.4

สมการ Inverse DCT

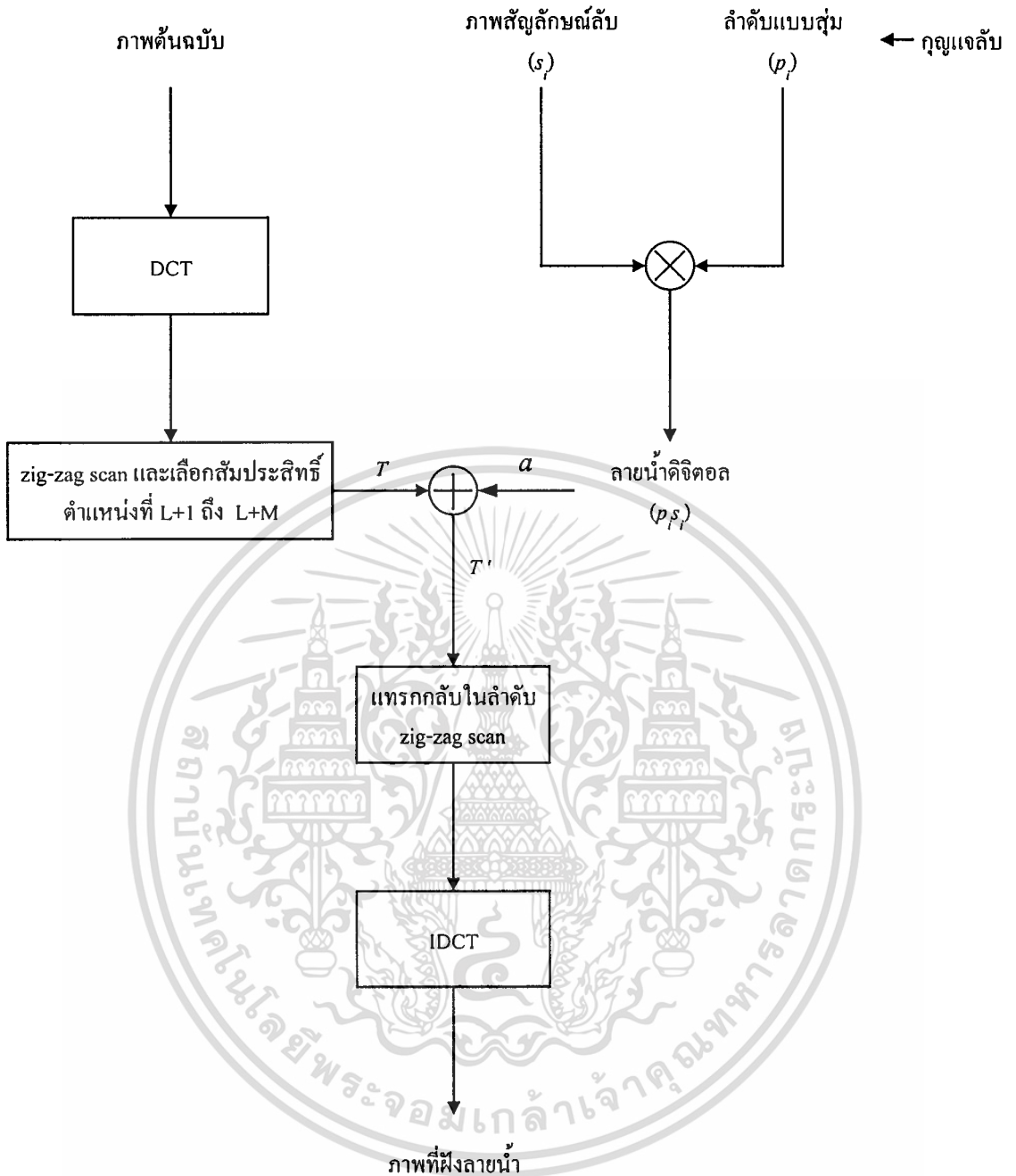
$$f(x, y) = \frac{1}{\sqrt{2N}} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u) \alpha(v) C(u, v) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2y+1)v\pi}{2N} \right] \quad (3.12)$$

เมื่อ

$C(u, v)$ คือค่าสัมประสิทธิ์ DCT

$f(x, y)$ คือค่าระดับสีในพิกเซล

$\alpha(i) = 1/\sqrt{2}$ เมื่อ $i = 0$ และ $\alpha(i) = 1$ เมื่อ $i > 0$



รูปที่ 3.4 กระบวนการฝังลายน้ำดิจิทัลด้วยเทคนิคคิตรีต โคซายน์ทรานส์ฟอร์ม

เพื่อระบุนรายละเอียดของอัลกอริทึมในการทำลายน้ำให้สมบูรณ์ ดังนั้นพารามิเตอร์บางตัว ถูกกำหนดให้มีค่าคงที่ โดยเฉพาะความยาว M ของรหัสและตำแหน่งที่ทำการฝังลงในสเปกตรัม ความถี่ต้องมีค่าแน่นอน นอกจากนี้ ค่าของ α ต้องถูกกำหนดไว้ด้วย โดยเป็นตัวกำหนดค่าพลังงานของรหัสที่ฝังลงไป โดยทั้งหมดนี้เราตั้งสมมุติฐานในการทำงานบนภาพโทนสีเทาขนาด 512×512

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.2 การตรวจหาลายน้ำจากการฝังลายน้ำด้วยเทคนิคดิสครีตโคซายน์ทรานส์ฟอร์ม

รูปที่ 3.5 แสดงขั้นตอนการตรวจหาลายน้ำ ซึ่งผู้ที่ได้รับอนุญาตสามารถนำข้อมูลที่ซ่อนไว้กลับมาได้โดยง่าย แม้ว่าจะไม่มีภาพต้นฉบับแต่ก็สามารถนำกลับมาได้ด้วยการคาดเดาภาพต้นฉบับ โดยภาพที่ถูกฝังลายน้ำอาจพิจารณาได้ว่าเป็นภาพต้นฉบับที่ถูกรบกวนโดยสัญญาณแบบสุ่ม การคาดเดาภาพต้นฉบับจริงจึงทำได้โดยใช้เทคนิคของการกำจัดสัญญาณรบกวน (Noise Reduction) โดยในวิทยานิพนธ์นี้เลือกตัวกรองสัญญาณแบบเฉลี่ยข้อมูล (Average Filtering) หรือที่ใช้ในการทำภาพให้เลื่อน (Smoothing) ดังที่ได้กล่าวไว้ใน การตรวจหาลายน้ำจากการฝังลายน้ำด้วยเทคนิคการแปลงฟูริเยร์

การ Smoothing ทำได้ง่าย โดยการคอนโวลูชัน (Convolution) ภาพกับมาสก์ (Mask) ขนาดเล็กๆ เช่น 5×5 ซึ่งสัมประสิทธิ์ทุกตัวมีค่าเท่ากันเท่ากับ $1/25$ ดังนั้นภาพที่ได้จากการคาดเดาจะได้รับการ Smoothing ภาพที่ฝังลายน้ำซึ่งคำนวณได้ดังนี้

$$i'_k = \frac{1}{c \times c} \sum_{k=1}^{c \times c} i_k^* \quad (3.13)$$

เมื่อ c เป็นขนาดของ Convolution Mask

นำภาพที่ฝังลายน้ำมาทำการแปลง DCT หลังจากนั้นทำสัมประสิทธิ์ DCT ที่ได้ทำการ Smoothing เพื่อให้ได้สัมประสิทธิ์ DCT ที่ได้จากการคาดเดาและเลือกค่าสัมประสิทธิ์ตั้งแต่ลำดับที่ $L+1$ ถึง $L+M$ ในลำดับซิกแซกสแกน ขึ้นมาเพื่อสร้างเวกเตอร์ T' และ T^* ตามลำดับ

ค่าผลต่าง (δ) ระหว่าง ค่าของภาพที่ฝังลายน้ำกับค่าของภาพที่ได้จากการคาดเดาก็คือ ค่าของบิตที่ฝังไว้นั่นเอง อธิบายได้ด้วยสูตรดังนี้

$$\delta_i = t_i^* - t'_i = \alpha \cdot p_i \cdot s_i \quad (3.14)$$

หลังจากนั้นสามารถทำการคำนวณหาค่าบิตลายน้ำที่ฝังไว้ ได้โดยการพิจารณาจากเครื่องหมายของค่าผลต่าง (δ) ที่ทำได้ ซึ่งอธิบายด้วยสูตรได้ดังนี้

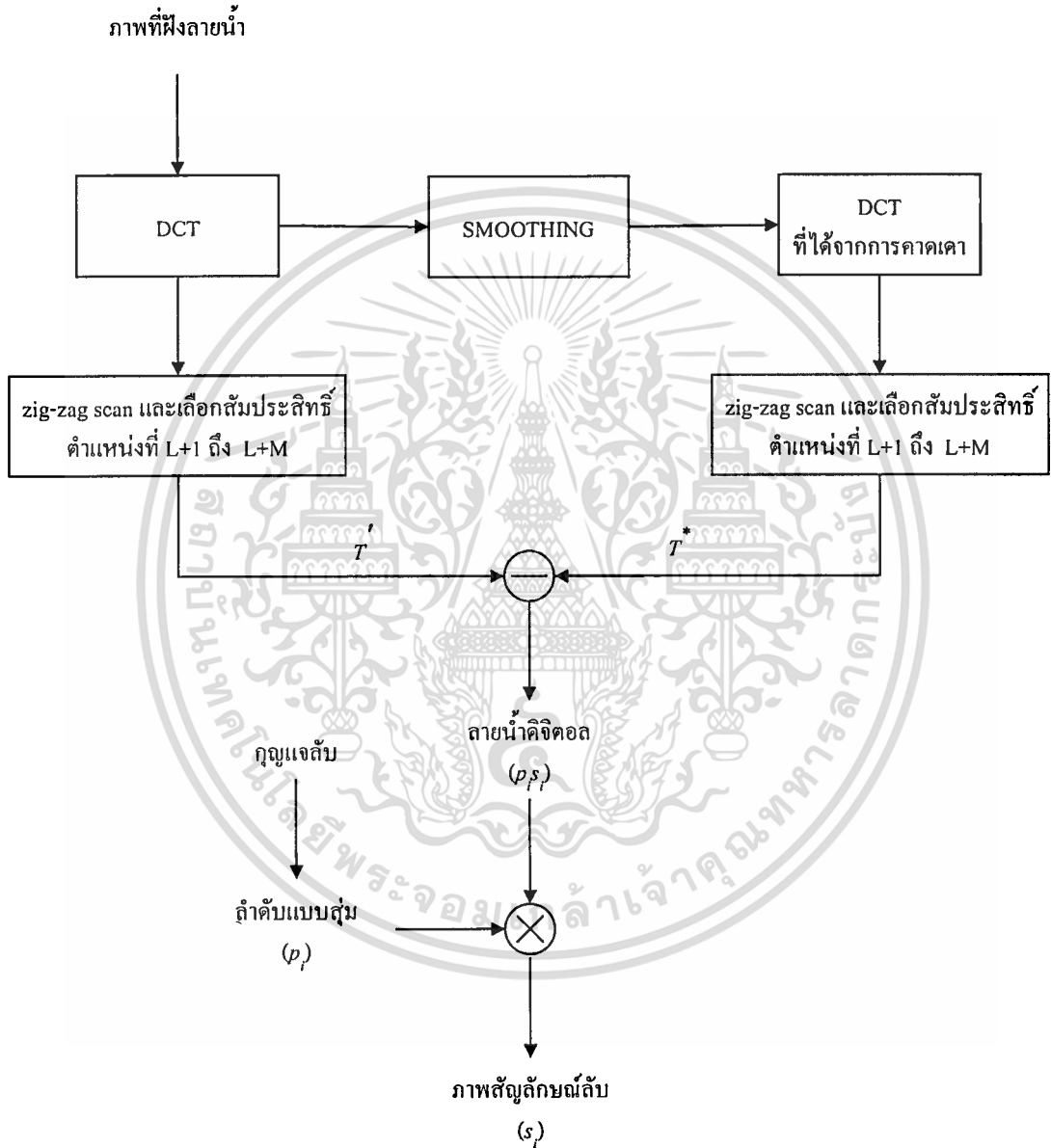
$$\text{sgn}(\delta_i) = p_i \cdot s_i \quad (3.15)$$

ลำดับบิตของสัญลักษณ์ดิจิทัลที่ถูกฝังไว้สามารถนำกลับคืนได้ด้วยการคูณกับลำดับแบบสุ่ม p_i ซึ่งสร้างจากกุญแจลับที่ผู้ฝังลายน้ำทราบนั่นเอง แต่หากว่าลำดับแบบสุ่มที่ใช้ผิดหรือไม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สอดคล้องกับลำดับแบบสุ่มที่ใช้ฝึกลายน้ำ มันก็จะไม่สามารถใช้งานได้และบิตที่น่ากลับคืนมาก็จะเป็นบิตแบบสุ่ม

สุดท้ายนำลำดับบิตของสัญลักษณ์ดิจิทัลที่ได้มาจัดเรียงในรูปแบบ 2 มิติดั้งเดิม ก็จะได้ภาพสัญลักษณ์ลับดิจิทัล



รูปที่ 3.5 กระบวนการตรวจหาลายน้ำจากการฝึกลายน้ำด้วยเทคนิคดิสครีต โคซายน์ทรานส์ฟอร์ม

3.4 การวัดประสิทธิภาพของอัลกอริทึม

ความสำเร็จของประสิทธิภาพอัลกอริทึมที่ดี สามารถประเมินได้จากใช้เครื่องมือวัดคุณภาพ แต่เนื่องจากปัญหาที่เกิดขึ้นคือประสิทธิภาพมักเกี่ยวข้องกับด้านการรับรู้ ดังนั้นการจะวัดเป็นเอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จำนวนตัวเลขจึงอาจมีการคลาดเคลื่อนได้บ้าง แต่ในที่นี้เราจะนำเสนอวิธีการวัดที่เป็นที่นิยมที่สุดทั้งหมดเพื่อเน้นถึงประสิทธิภาพของอัลกอริทึมที่ดี

3.4.1 การวัดโดยใช้สายตา

การวัดคุณภาพโดยใช้สายตาของผู้ที่ไม่เกี่ยวข้องทำการตัดสินคุณภาพของภาพภายหลังการทำลายน้ำเป็นวิธีการพื้นฐานแต่ให้ผลที่น่าเชื่อถือมาก ในฐานะที่เป็นผู้ใช้ธรรมดาและยังใช้สายตาของผู้เชี่ยวชาญที่มีความสามารถในการสังเกตความบกพร่องเล็กน้อยที่ผู้ใช้ทั่วไปอาจมองข้าม ในการตัดสินใจอาจใช้กฎเกณฑ์ต่างๆ เช่น การตัดสินใจจากภาพทดสอบแล้วให้ระดับคะแนนเมื่อผู้ทดสอบได้มองภาพทดสอบแล้วระบุระดับคุณภาพตามที่ได้ระบุไว้ โดยอาจมีชุดภาพมาตรฐานที่มีระดับคะแนนระบุไว้อ้างอิงด้วยก็ได้ ระดับคุณภาพสามารถแสดงได้ทั้งระดับความถูกต้องและระดับความผิดพลาด หรือการตัดสินจากชุดภาพทดสอบแล้วเรียงลำดับคุณภาพของภาพ ซึ่งผู้ใช้จะเรียงลำดับภาพทดสอบตามคุณภาพของภาพที่เห็นผู้ทดสอบจะตัดสินใจในลักษณะเปรียบเทียบว่าดีกว่าหรือแยกว่า

3.4.2 Peak Signal-to-Noise Ratio (PSNR)

ในการหาค่าความผิดพลาดเชิงเลข นิยมใช้ค่าความผิดพลาดกำลังสองเฉลี่ย (Mean Square Error, MSE) ถ้ามีค่าน้อยแสดงว่าภาพที่ได้กลับคืนมามีความผิดเพี้ยนจากภาพต้นแบบน้อย สามารถหาค่าความผิดพลาดกำลังสองเฉลี่ยของข้อมูลภาพขนาด $M \times N$ ได้ดังนี้

$$MSE = \frac{1}{M \times N} \sum_{x=1}^M \sum_{y=1}^N [f(x,y) - \bar{f}(x,y)]^2 \quad (3.16)$$

โดยที่ M คือ จำนวนพิกเซลตามความกว้างของภาพ

N คือ จำนวนพิกเซลตามความสูงของภาพ

$f(x,y)$ คือ ค่าของพิกเซลที่ตำแหน่ง (x,y) ของภาพต้นแบบ

$\bar{f}(x,y)$ คือ ค่าของพิกเซลที่ตำแหน่ง (x,y) ของภาพที่สร้างกลับคืนมาใหม่

เพื่อให้ได้เครื่องมือวัดที่สามารถวัดที่เป็นตัวเลขที่ชัดเจนขึ้น เราเลือกใช้อัตราส่วนของสัญญาณต่อสัญญาณรบกวนสูงสุด (Peak Signal-to-Noise Ratio, PSNR) ในการวัดสัญญาณรบกวนที่ถูกฝังลงในภาพต้นฉบับเนื่องจากการซ่อนลายน้ำภาพดิจิทัล ซึ่งถึงแม้ว่าเครื่องมืออันนี้จะไม่เที่ยงตรงนักแต่ก็เป็นวิธีหนึ่งที่ใช้กันอย่างแพร่หลายในการวัด การไม่ปรากฏให้เห็นและประสิทธิภาพของอัลกอริทึมการฝังลายน้ำ ค่า PSNR หาได้จาก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

$$PSNR = 10 \log \frac{Peak^2}{MSE} \quad (dB) \quad (3.17)$$

โดยที่ Peak คือค่าสูงสุดของขอบเขตข้อมูล สำหรับภาพที่มีพิกเซลแทนด้วยขนาดข้อมูล n บิต จะมีจำนวนระดับความเทา (Gray Scale) เท่ากับ 2^n จะได้ว่า

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE} \quad (dB) \quad (3.18)$$

ดังนั้นภาพขนาด 8 บิต หรือมีจำนวนระดับความเทาเท่ากับ 256 ระดับ จะได้ว่า

$$PSNR = 10 \log \frac{255^2}{MSE} \quad (dB) \quad (3.19)$$

3.6.3 Normalize Correlation (NC)

นอกจากการคำนวณหาค่า PSNR ในการวัดค่าความผิดพลาดของภาพที่ฝั่งลายน้ำแล้ว การเปรียบเทียบลายน้ำที่ตรวจหาได้กลับลายน้ำที่ทำการฝังยังสามารถทำการเปรียบเทียบได้ โดยหลังจากที่นำลายน้ำกลับคืนได้แล้ว ผู้ใช้สามารถเปรียบเทียบผลกับลายน้ำที่อ้างอิง การวัดสามารถนิยามได้ดังนี้

$$Normalize \ Correlation \ (NC) = \frac{\sum_{i=1}^M s_i s'_i}{\sum_{i=1}^M s_i^2} \quad (3.20)$$

เมื่อ s_i คือ ภาพสัญลักษณ์ดิจิตอลต้นฉบับ และ s'_i คือ ภาพสัญลักษณ์ดิจิตอลที่ได้จากการนำลายน้ำกลับคืน

ค่า NC ที่ได้แสดงถึงความเหมือนของภาพสัญลักษณ์ที่ได้ทำการฝังกับภาพที่ตรวจหา กลับมาได้โดยค่าที่ได้หากจะมีค่าใกล้เคียง 1 แสดงว่าลายน้ำที่ได้มีความเหมือนกันมาก สามารถระบุได้ว่าเป็นภาพที่ได้ทำการฝังลายน้ำของเจ้าของลิขสิทธิ์จริงๆ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดังนั้นในการฝึกลายน้ำเมื่อภาพที่ได้ฝึกลายน้ำแล้ว เมื่อทำการตรวจหาลายน้ำกลับคืนไม่
ว่าภาพที่ได้ทำการฝึกลายน้ำจะผ่านการบิดเบือนอย่างไรก็ตาม ค่า NC ที่คำนวณได้ควรจะมีค่าใกล้
เคียง 1 มากที่สุดเพื่อที่จะมั่นใจได้ว่าภาพที่ทำการตรวจหาลายน้ำอยู่นั้นเป็นภาพของผู้ตรวจลายน้ำ
จริง ๆ



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

ผลการทดลอง

ในบทนี้จะเป็นการเสนอผลการทดลองที่ได้ผ่านกระบวนการซ่อนลายน้ำภาพดิจิทัลตามอัลกอริทึมที่ได้นำเสนอไว้ในบทที่ 3 ที่ผ่านมาทั้งเทคนิคการแปลงฟูริเยร์และเทคนิคคิสตรีตโคซายน์ทรานส์ฟอร์ม ในเบื้องต้นหลังจากภาพดิจิทัลต้นฉบับได้ผ่านกระบวนการซ่อนลายน้ำแล้ว การเปรียบเทียบกันระหว่างภาพทั้งสองดังกล่าวด้วยการมองตาเปล่า หลังจากนั้นจะได้ทำการคำนวณค่า PSNR ของภาพที่ผ่านการฝังลายน้ำแล้ว รวมถึงภาพสัญลักษณ์ลับที่ได้ทำการฝังในภาพต้นฉบับและทำการตรวจหาค้นกลับมาได้นอกจากการเปรียบเทียบด้วยตาเปล่าแล้ว จะได้มีการคำนวณค่า NC ในการเปรียบเทียบกับภาพสัญลักษณ์ลับต้นฉบับด้วยเพื่อใช้ในการอ้างอิงถึงการยอมรับภาพนั้นๆ ของผู้เป็นเจ้าของลิขสิทธิ์ภาพ หลังจากนั้นจะเป็นการทดลองนำภาพที่ได้ฝังลายน้ำแล้วไปผ่านกระบวนการวัดความคงทนของภาพ โดยการนำภาพไปผ่านเทคนิคการประมวลผลสัญญาณ และความผิดเพี้ยนทางเรขาคณิตต่างๆ เพื่อยืนยันว่าอัลกอริทึมที่นำเสนอมีความคงทนต่อการรบกวนต่างๆ โดยลายน้ำจะยังคงอยู่กับภาพและสามารถตรวจหาค้นกลับมาได้

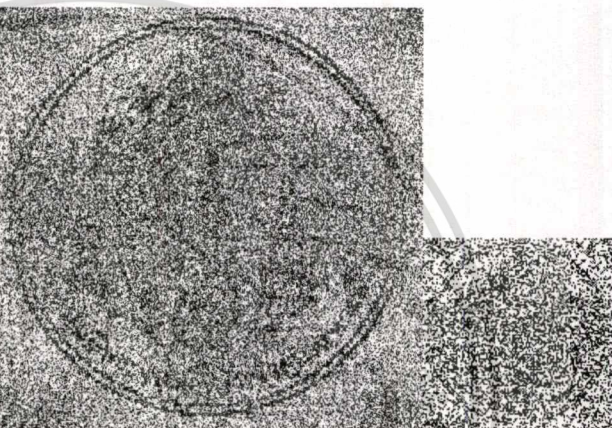
4.1 ผลการทดลองเมื่อใช้เทคนิคการแปลงฟูริเยร์

จากการทดลองเราได้นำภาพ Lena ขนาด 512x512 พิกเซล โทนสีเทา 8 บิต เป็นภาพต้นฉบับ และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญลักษณ์ลับที่จะฝังในภาพต้นฉบับ โดยเป็นภาพแบบไบนารีขนาดเท่ากับขนาดของภาพต้นฉบับ ซึ่งได้จากการปรับขนาดจากภาพ 128 พิกเซลเพื่อให้สามารถใช้ทดลองด้วยเทคนิคการแปลงฟูริเยร์ได้และสามารถเปรียบเทียบคุณภาพกับเทคนิคคิสตรีตโคซายน์ทรานส์ฟอร์ม แสดงดังรูปที่ 4.1 (ก) เมื่อทำการฝังลายน้ำด้วยเทคนิคการแปลงฟูริเยร์ตามที่ได้นำเสนอไปในบทก่อนหน้านี้ โดยกำหนดตัวแปรต่างๆ ให้มีค่าดังต่อไปนี้

กฎเกณฑ์มีค่าเป็น 500 และขนาดของ convolution C มีค่าเป็น 5 และแอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 5500 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.1 (ข)



(ก)



(ข)

รูปที่ 4.1 (ก) ภาพต้นฉบับ Lena ขนาด 512x512 พิกเซล ภาพสัญลักษณ์ลิบขนาด 128x128 พิกเซล และภาพสัญลักษณ์ลิบขนาด 512x512 พิกเซลที่ได้จากการปรับขนาด (ข) ภาพดิจิทัลที่ฟังลายน้ำแล้ว ภาพลายน้ำที่นำกลับคืน และภาพลายน้ำที่นำกลับคืนและทำการปรับขนาดเมื่อกำหนดให้ α เท่ากับ 5500

ค่า NC ของภาพสัญลักษณ์ดิจิทัลที่ได้จากการนำลายน้ำกลับคืนเมื่อเปรียบเทียบกับภาพสัญลักษณ์ดิจิทัลต้นฉบับจะเท่ากับ 0.5843 สำหรับภาพขนาด 512 พิกเซลและเท่ากับ 0.5851 สำหรับภาพขนาด 128 พิกเซลเมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 5500

ค่า PSNR ของภาพดิจิทัลที่ได้ทำการซ่อนลายน้ำจะเท่ากับ 30.3529 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 5500

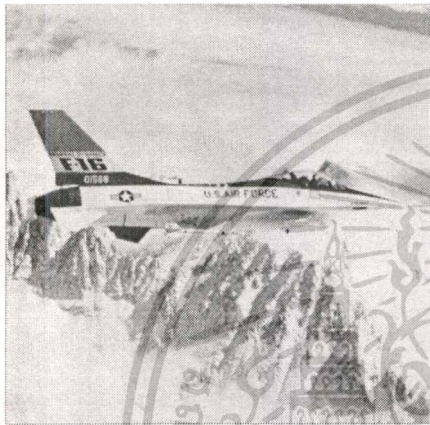
ได้ทดลองทำการซ่อนลายน้ำโดยใช้ภาพ Airplane เป็นภาพต้นฉบับและทำการใส่ลายน้ำด้วยอัลกอริทึมที่นำเสนอ โดยใช้ค่าตัวแปรเหมือนที่ใช้กับการทำภาพ Airplane และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญลักษณ์ลิบที่จะ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

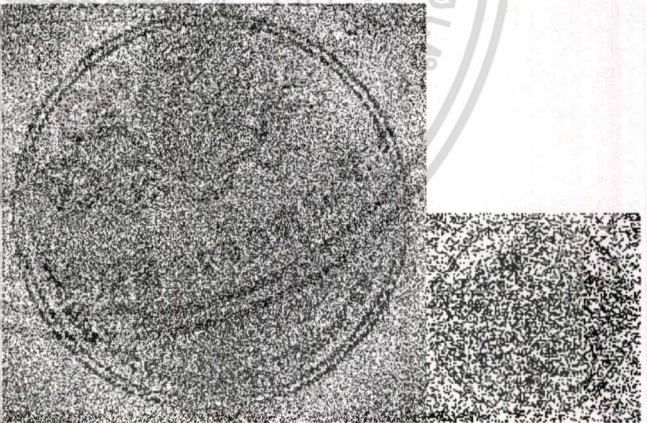
ฝั่งในภาพต้นฉบับเช่นกัน ดังแสดงในรูปที่ 4.2 (ก) เมื่อให้แอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 5500 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.2 (ข)

ค่า NC ของภาพสัญลักษณ์ดิจิทัลที่ได้จากการนำลายน้ำกลับคืนเมื่อเปรียบเทียบกับภาพสัญลักษณ์ดิจิทัลต้นฉบับจะเท่ากับ 0.5518 สำหรับภาพขนาด 512 พิกเซลและเท่ากับ 0.5541 สำหรับภาพขนาด 128 พิกเซลเมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 5500

ค่า PSNR ของภาพดิจิทัลที่ได้ทำการซ่อนลายน้ำจะเท่ากับ 30.3529 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 5500



(ก)



(ข)

รูปที่ 4.2 (ก) ภาพต้นฉบับ Airplane ขนาด 512x512 พิกเซล ภาพสัญลักษณ์ต้นฉบับขนาด 128x128 พิกเซล และภาพสัญลักษณ์ต้นฉบับขนาด 512x512 พิกเซลที่ได้จากการปรับขนาด (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้ว ภาพลายน้ำที่นำกลับคืน และภาพลายน้ำที่นำกลับคืนและทำการปรับขนาด เมื่อกำหนดให้ α เท่ากับ 5500

การปรับแต่งอัลกอริทึมให้มีประสิทธิภาพมากขึ้น

จากการทดลองปรับแต่งอัลกอริทึมเทคนิคการแปลงฟูริเยร์พบว่าสามารถเพิ่มประสิทธิภาพอัลกอริทึมให้ดีขึ้นได้ โดยการฝังลายน้ำในแมกนิจูด $F(A)$ ใช้รูปแบบการคำนวณดังสมการนี้

$$v'_i = v_i + \alpha \cdot v_i \cdot p_i \cdot s_i \quad (4.1)$$

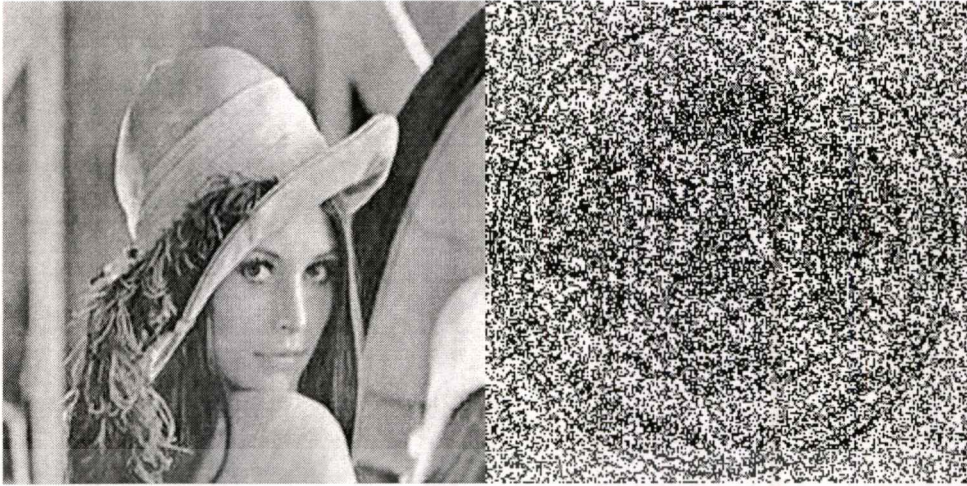
จากการทดลองเราได้นำภาพ Lena ขนาด 512x512 พิกเซล โทนสีเทา 8 บิต เป็นภาพต้นฉบับ และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญลักษณ์ลับที่จะฝังในภาพต้นฉบับ โดยเป็นภาพแบบไบนารีขนาดเท่ากับขนาดของภาพต้นฉบับ ซึ่งได้จากการปรับขนาดจากภาพ 128 พิกเซล แสดงดังรูปที่ 4.3 (ก) โดยกำหนดตัวแปรต่าง ๆ ให้มีค่าดังต่อไปนี้

กุญแจลับมีค่าเป็น 500 และขนาดของ convolution C มีค่าเป็น 5 และแอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 0.2 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.3 (ข) เมื่อแอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 0.3 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.3 (ค) และเมื่อแอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 0.5 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.3 (ง) ตามลำดับ

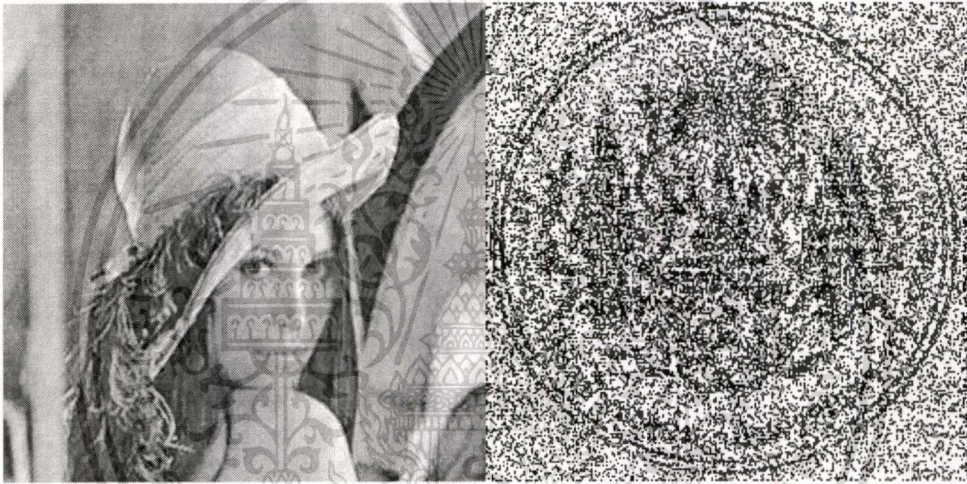


(ก)

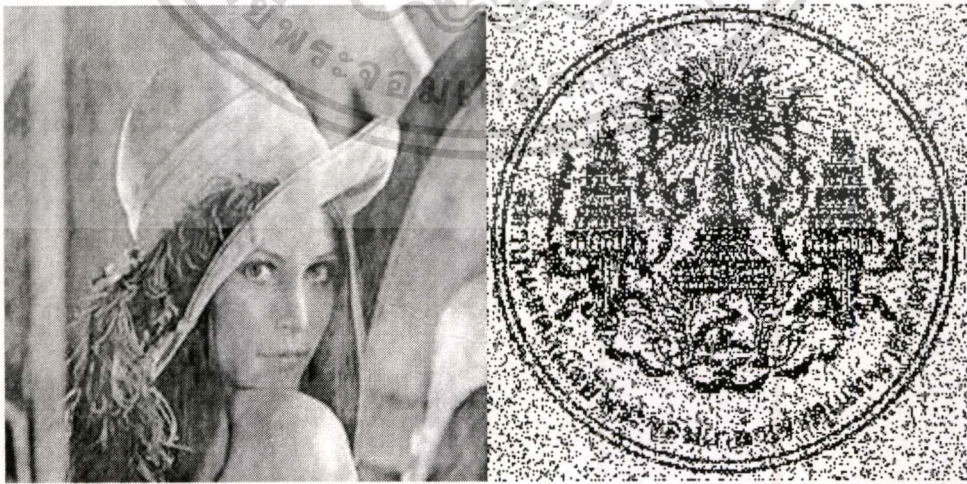
รูปที่ 4.3 (ก) ภาพต้นฉบับ Lena และภาพสัญลักษณ์ลับขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.2 (ค) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.3 (ง) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.5



(ข)



(ค)



(ง)

รูปที่ 4.3 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค่า NC ของภาพสัญลักษณ์ดิจิทัลที่ได้จากการนำลายน้ำกลับคืนเมื่อเปรียบเทียบกับภาพสัญลักษณ์ดิจิทัลต้นฉบับจะเท่ากับ 0.6428 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.2 เท่ากับ 0.7116 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.3 และเท่ากับ 0.8288 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.5

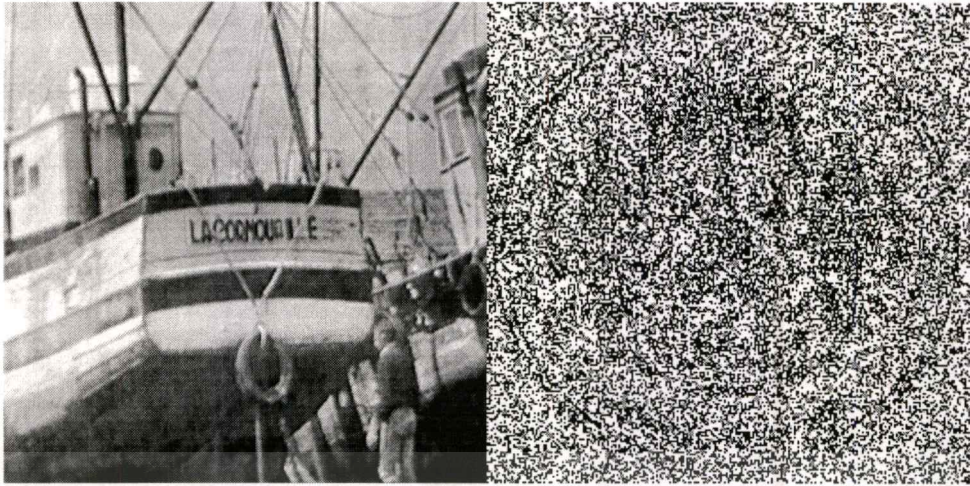
ค่า PSNR ของภาพดิจิทัลที่ได้ทำการซ่อนลายน้ำจะเท่ากับ 30.8419 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.2 เท่ากับ 29.3355 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.3 และเท่ากับ 23.7553 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.5

ได้ทดลองทำการซ่อนลายน้ำโดยใช้ภาพ Boat เป็นภาพต้นฉบับและทำการใส่ลายน้ำด้วยอัลกอริทึมที่นำเสนอ โดยใช้ค่าตัวแปรเหมือนที่ใช้กับการทำภาพ Lena และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญลักษณ์ลับที่จะฝังในภาพต้นฉบับเช่นกัน ดังแสดงในรูปที่ 4.4 (ก) เมื่อให้แอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 0.2 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.4 (ข) เมื่อแอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 0.3 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.4 (ค) และเมื่อแอมพลิจูดแฟกเตอร์ (α) มีค่าเป็น 0.5 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.4 (ง) ตามลำดับ

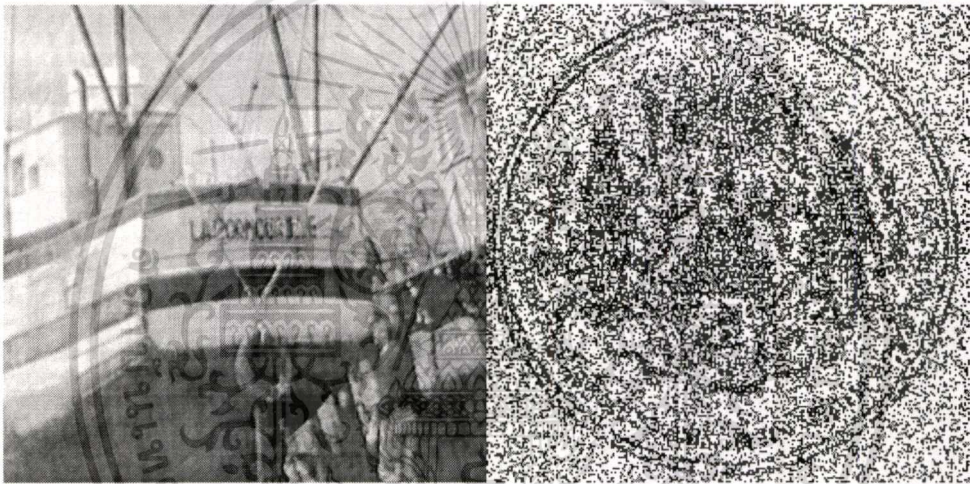


(ก)

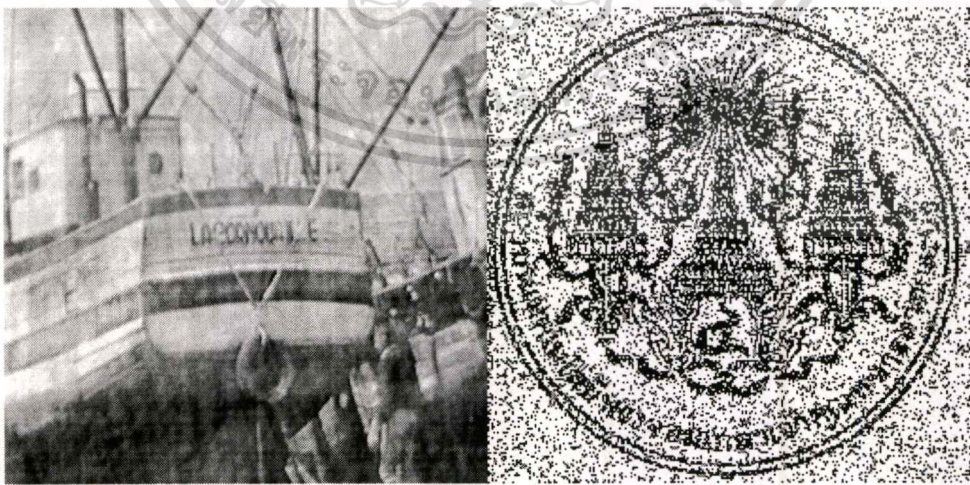
รูปที่ 4.4 (ก) ภาพต้นฉบับ Boat และภาพสัญลักษณ์ลับขนาด ขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.2 (ค) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.3 (ง) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 0.5



(บ)



(ค)



(ง)

รูปที่ 4.4 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ค่า NC ของภาพสัญญาณดิจิทัลที่ได้จากการนำลายน้ำกลับคืนเมื่อเปรียบเทียบกับภาพสัญญาณดิจิทัลต้นฉบับจะเท่ากับ 0.6376 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.2 เท่ากับ 0.7062 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.3 และเท่ากับ 0.8219 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.5

ค่า PSNR ของภาพดิจิทัลที่ได้จากการซ่อนลายน้ำจะเท่ากับ 27.6393 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.2 เท่ากับ 23.9756 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.3 และเท่ากับ 21.0815 dB เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 0.5

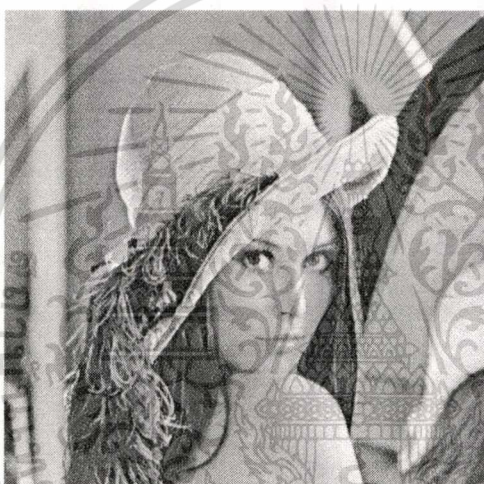
4.2 ผลการทดลองเมื่อใช้เทคนิคคีสคริตโคชาน์ทรานส์ฟอร์ม

จากการทดลองเราได้นำภาพ Lena ขนาด 512x512 พิกเซล โทนสีเทา 8 บิตเป็นภาพต้นฉบับ และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญญาณลับที่จะฝังในภาพต้นฉบับ ซึ่งเป็นภาพแบบไบนารี มีขนาด 128x128 พิกเซล แสดงดังรูปที่ 4.5 (ก)

เมื่อทำการฝังลายน้ำด้วยเทคนิคคีสคริตโคชาน์ทรานส์ฟอร์มตามที่ได้นำเสนอไป โดยกำหนดตัวแปรต่างๆ ให้มีค่าดังต่อไปนี้ กุญแจลับมีค่าเป็น 500, ขนาดของ convolution c มีค่าเป็น 5, แอมพลิจูดแฟกเตอร์ α มีค่าเป็น 30, $L = 20\%$ (52,429) และ $M = 128 \times 128$ (16,384) ผลการทดลองดังแสดงในรูปที่ 4.5 (ข)



(ก)



(ข)

รูปที่ 4.5 (ก) ภาพต้นฉบับขนาด 512x512 พิกเซล โทนสีเทา 8 บิต และภาพสัญญาณรบกวนขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฟุ้งลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 30

ค่า NC ของภาพสัญญาณรบกวนดิจิทัลที่ได้จากการนำลายน้ำกลับคืนเมื่อเปรียบเทียบกับภาพสัญญาณรบกวนต้นฉบับจะเท่ากับ 0.9890 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 30

ค่า PSNR ของภาพดิจิทัลที่ได้ทำการซ่อนลายน้ำจะเท่ากับ 30.4534 เมื่อแอมพลิจูดแฟกเตอร์ α มีค่าเป็น 30

ได้ทดลองทำการซ่อนลายน้ำโดยใช้ภาพ Boat เป็นภาพต้นฉบับและทำการใส่ลายน้ำด้วยอัลกอริทึมที่นำเสนอ โดยใช้ค่าตัวแปรเหมือนที่ใช้กับการทำภาพ Lena และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญญาณรบกวนที่จะฝังในภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ต้นฉบับเช่นกัน ดังแสดงในรูปที่ 4.6 (ก) เมื่อให้แอมพลิจูดเฟกเตอร์ (α) มีค่าเป็น 30 จะได้ผลลัพธ์ออกมาดังแสดงในรูปที่ 4.6 (ข)

ค่า NC ของภาพสัญลักษณ์ดิจิทัลที่ได้จากการนำลายน้ำกลับคืนเมื่อเปรียบเทียบกับภาพสัญลักษณ์ดิจิทัลต้นฉบับจะเท่ากับ 0.9902 เมื่อแอมพลิจูดเฟกเตอร์ α มีค่าเป็น 30

ค่า PSNR ของภาพดิจิทัลที่ได้ทำการซ่อนลายน้ำจะเท่ากับ 30.4534 เมื่อแอมพลิจูดเฟกเตอร์ α มีค่าเป็น 30



(ข)

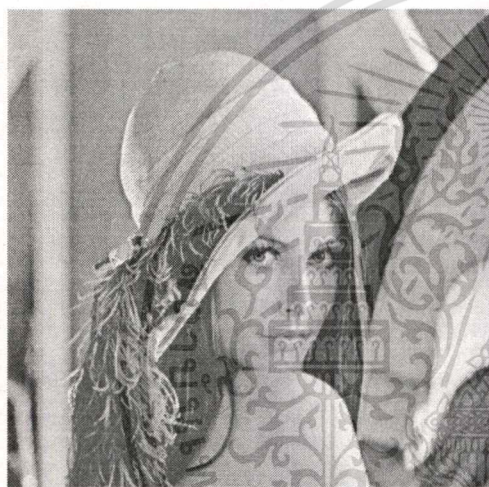
รูปที่ 4.6 (ก) ภาพต้นฉบับขนาด 512x512 พิกเซล โทนสีเทา 8 บิต และภาพสัญลักษณ์ต้นฉบับขนาด 512x512 พิกเซล (ข) ภาพดิจิทัลที่ฝังลายน้ำแล้วและภาพลายน้ำที่นำกลับคืน เมื่อกำหนดให้ α เท่ากับ 30

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

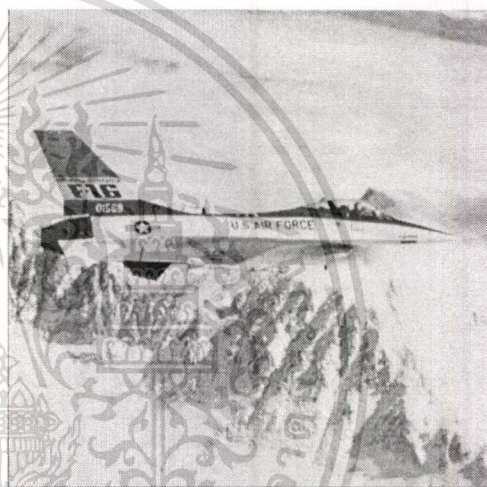
การปรับแต่งอัลกอริทึมให้มีประสิทธิภาพมากขึ้น

จากการทดลองปรับแต่งอัลกอริทึมเทคนิคดีสครีต โทซายน์ทรานส์ฟอร์มพบว่าสามารถเพิ่มประสิทธิภาพอัลกอริทึมให้ดีขึ้นได้ โดยการทำการ SMOOTHING ภาพที่ฝังลายน้ำ ให้ได้ภาพที่ได้จากการคาดเดา ก่อนที่จะนำภาพทั้งสองผ่านกระบวนการ DCT แล้วจึงดำเนินการขั้นตอนต่อไปดังเดิม

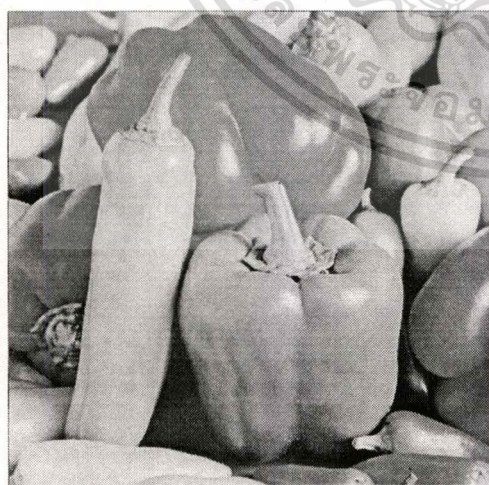
จากการทดลองเราได้นำภาพขนาด 512x512 พิกเซล โทนสีเทา 8 บิตจำนวน 6 ภาพเป็นภาพต้นฉบับดังแสดงในรูปที่ 4.7 และใช้ตราสัญลักษณ์ของสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังเป็นภาพสัญลักษณ์ลับที่จะฝังในภาพต้นฉบับ ซึ่งเป็นภาพแบบไบนารี มีขนาด 128x128 พิกเซล แสดงดังรูปที่ 4.8



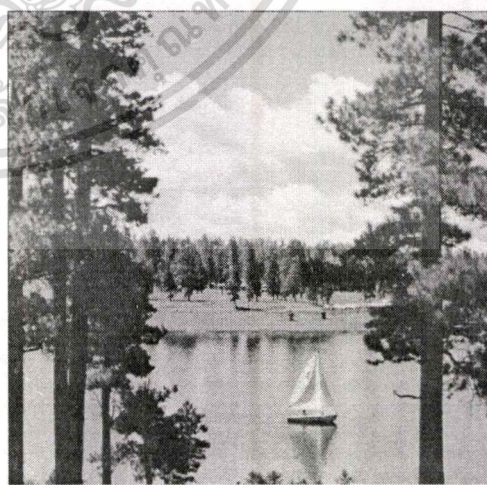
(ก) Lena



(ข) Airplane



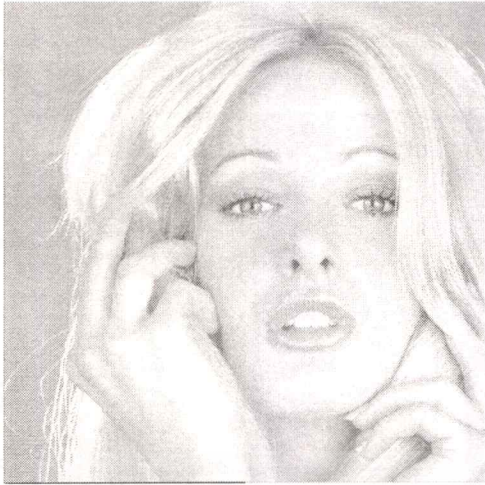
(ค) Peppers



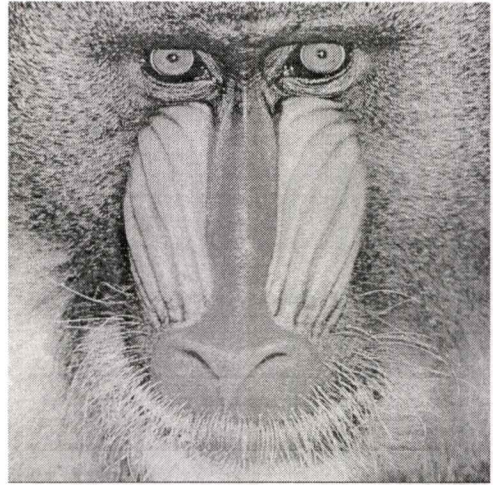
(ง) Sailboat

รูปที่ 4.7 ภาพต้นฉบับขนาด 512x512 พิกเซล โทนสีเทา 8 บิต จำนวน 6 ภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(จ) Tiffany



(ฉ) Baboon

รูปที่ 4.7 (ต่อ)

รูปที่ 4.8 ภาพลัทธิลักษณะลิบขนาด 128x128 พิกเซล

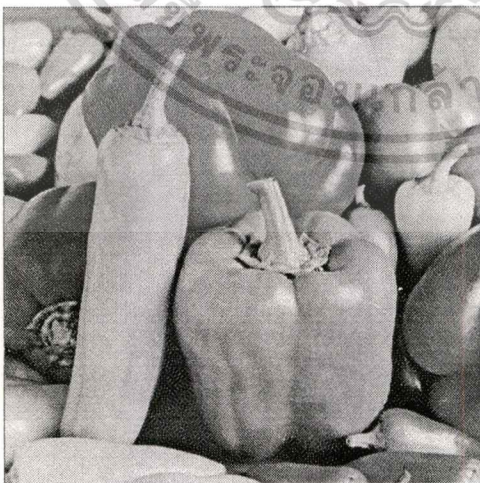
เมื่อทำการฝังลายน้ำด้วยเทคนิคดีสครีต โศขายนัทรานส์ฟอร์มตามที่ได้นำเสนอไป โดยกำหนดตัวแปรต่างๆ ให้มีค่าดังต่อไปนี้ ภูญแจลับมีค่าเป็น 500, ขนาดของ convolution c มีค่าเป็น 5, แอมพลิจูดแฟกเตอร์ α มีค่าเป็น 30, $L = 20\%$ (52,429) และ $M = 128 \times 128$ (16,384) ผลการทดลองดังแสดงในรูปที่ 4.9



(ก) PSNR = 30.4534 dB และ NC = 0.9979



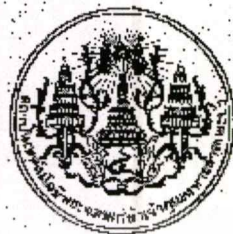
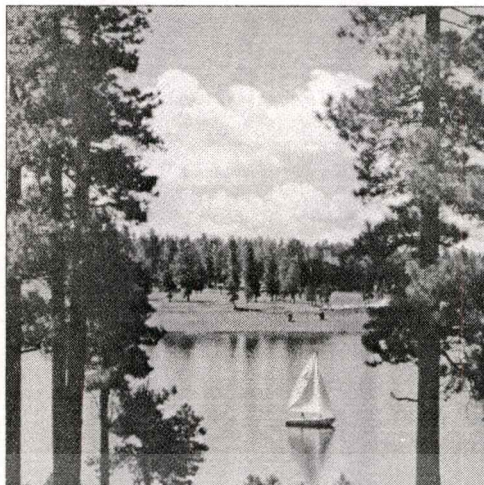
(ข) PSNR = 30.1665 dB และ NC = 0.9953



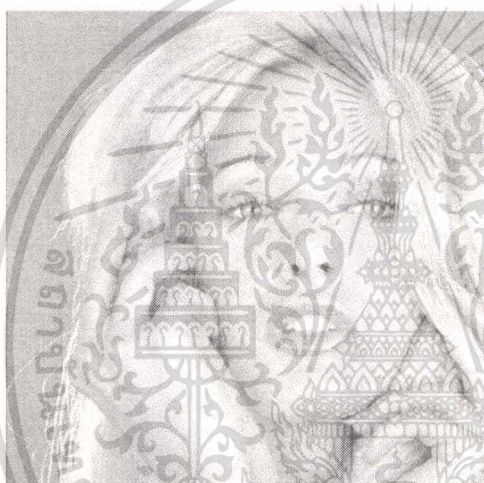
(ค) PSNR = 30.4537 dB และ NC = 0.9968

รูปที่ 4.9 ภาพต้นฉบับที่ฟังลายน้ำแล้วและภาพสัญญาณกลับที่ได้จากการนำลายน้ำกลับคืน

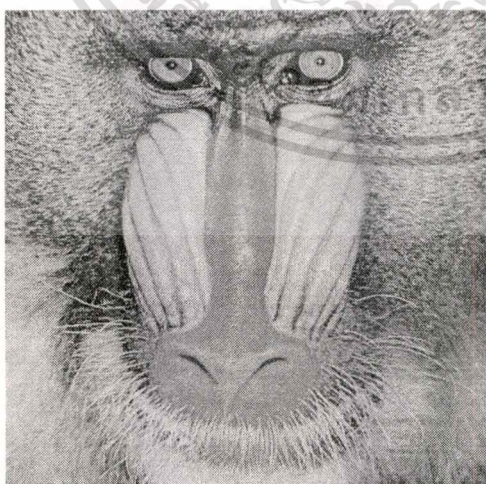
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ง) PSNR = 30.4534 dB และ NC = 0.9898



(จ) PSNR = 30.4541 dB และ NC = 0.9951

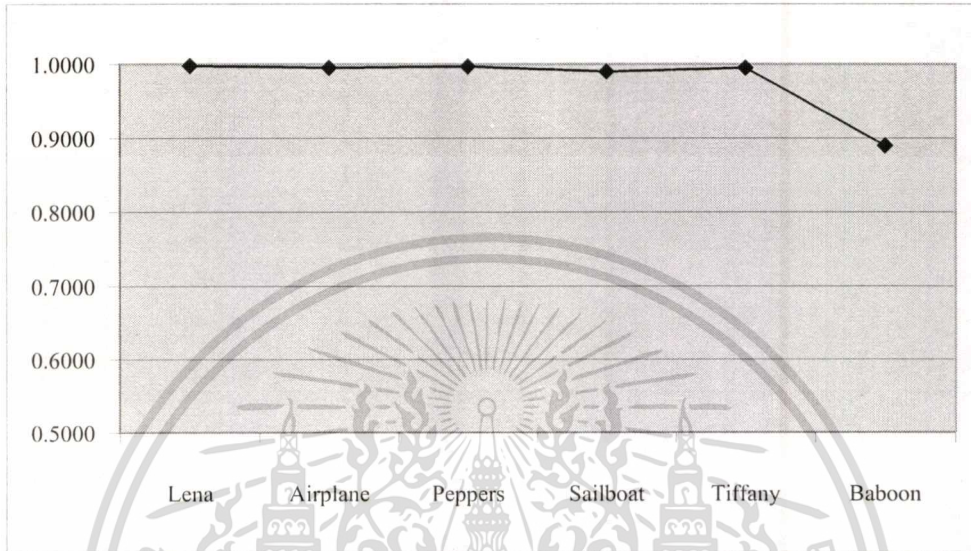


(ฉ) PSNR = 30.4536 dB และ NC = 0.8900

รูปที่ 4.9 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนจากการซ่อนลายน้ำกับภาพดิจิทัลต้นฉบับทั้ง 6 ภาพได้ง่าย จึงแสดงกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้ดังแสดงในรูปที่ 4.10



รูปที่ 4.10 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากการนำลายน้ำกลับคืน

4.3 การทดสอบความคงทนของลายน้ำ

เพื่อทดสอบความคงทนของอัลกอริทึมที่ได้นำเสนอว่าภาพที่ได้ฝังลายน้ำสามารถผ่านเทคนิคการประมวลผลสัญญาณ และความผิดเพี้ยนทางเรขาคณิต โดยลายน้ำจะยังสามารถตรวจหาได้ ซึ่งได้ทำการทดสอบกับเทคนิคดังต่อไปนี้

4.3.1 การทดสอบความคงทนของลายน้ำต่อเทคนิคการประมวลผลสัญญาณภาพ

ทำการทดสอบด้วยการบีบอัดข้อมูลแบบ JPEG การกรองความถี่ (Filtering) และการใส่สัญญาณรบกวนเกาส์เซียน ต่อภาพที่ได้ผ่านกระบวนการในการฝังลายน้ำแล้ว

4.3.1.1 การบีบอัดข้อมูลแบบ JPEG

เป็นการทดลองนำภาพดิจิทัลที่มีลายน้ำทำการบีบอัดข้อมูลแบบ JPEG ซึ่งเป็นวิธีการบีบอัดที่มีการสูญเสีย (Lossy Compression) ในโดเมนความถี่ โดยในการทดลองจะกำหนด Quality Factor เท่ากับ 10% ถึง 70% ค่า NC ของภาพที่ตรวจสอบได้หลังจากทำการบีบอัดข้อมูลแสดงในตารางที่ 4.1

ตารางที่ 4.1 ค่า NC ของภาพลายน้ำที่ได้หลังจากทำการบีบอัดข้อมูลแบบ JPEG ด้วย quality factors ที่แตกต่างกัน

Quality factor	70%	60%	50%	40%	30%	20%	10%
Lena	0.9955	0.9890	0.9873	0.9656	0.9473	0.8506	0.5980
Airplane	0.9932	0.9858	0.9811	0.9623	0.9426	0.8390	0.6172
Peppers	0.9953	0.9904	0.9898	0.9712	0.9539	0.8519	0.5944
Sailboat	0.9877	0.9751	0.9698	0.9586	0.9346	0.8445	0.6431
Tiffany	0.9926	0.9896	0.9845	0.9674	0.9492	0.8464	0.5963
Baboon	0.8844	0.8713	0.8606	0.8553	0.8322	0.7706	0.6410

ภาพลายน้ำที่นำกลับคืนหลังจากการบีบอัดข้อมูลแบบ JPEG ด้วย Quality Factor เท่ากับ 50% และ 20% ในการทดลองกับภาพทั้ง 6 ภาพแสดงในรูปที่ 4.11 และรูปที่ 4.12 ตามลำดับ

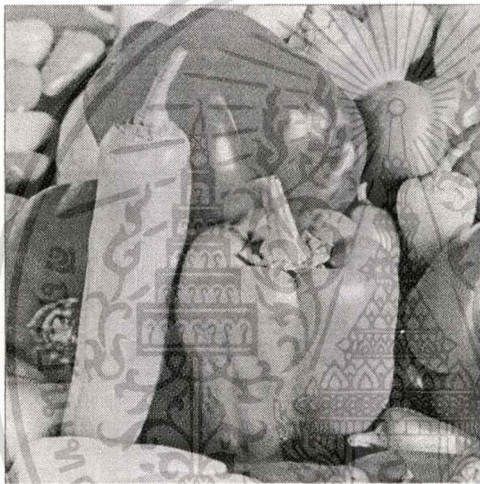


(ก) PSNR = 29.0145 dB และ NC = 0.9873

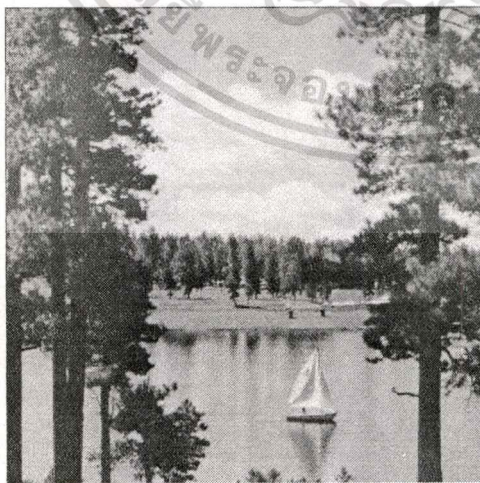
รูปที่ 4.11 ภาพลายน้ำที่ผ่านการบีบอัดข้อมูลแบบ JPEG โดยคุณภาพของภาพเท่ากับ 50% และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน



(ข) PSNR = 28.9437 dB และ NC = 0.9811



(ค) PSNR = 29.2267 dB และ NC = 0.9898



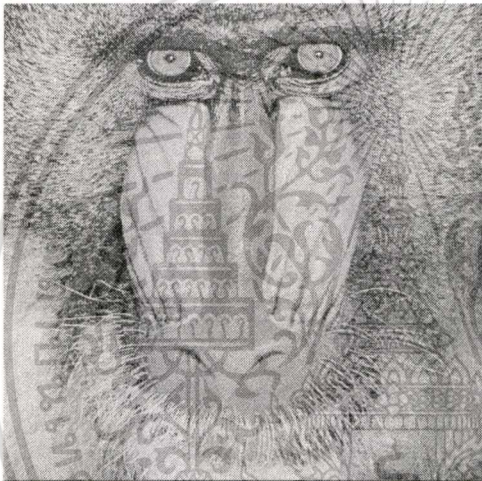
(ง) PSNR = 28.7164 dB และ NC = 0.9698

รูปที่ 4.11 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



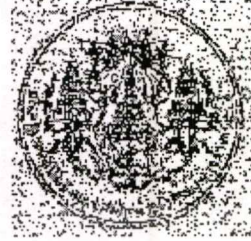
(จ) PSNR = 28.9766 dB และ NC = 0.9845



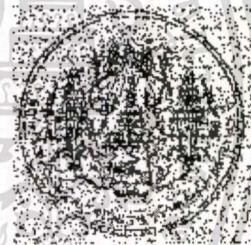
(ฉ) PSNR = 26.6620 dB และ NC = 0.8606

รูปที่ 4.11 (ต่อ)

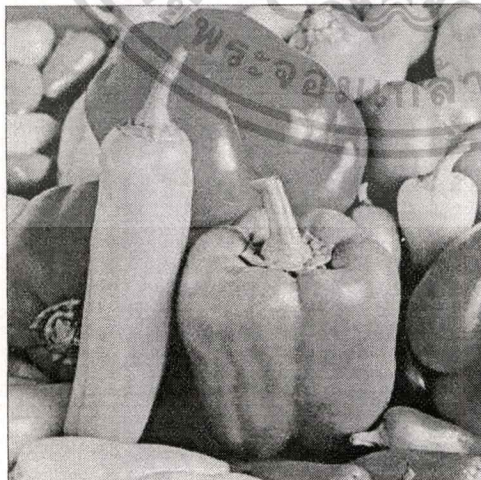
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ก) PSNR = 28.9766 dB และ NC = 0.8506

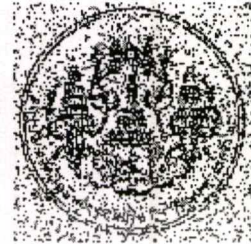
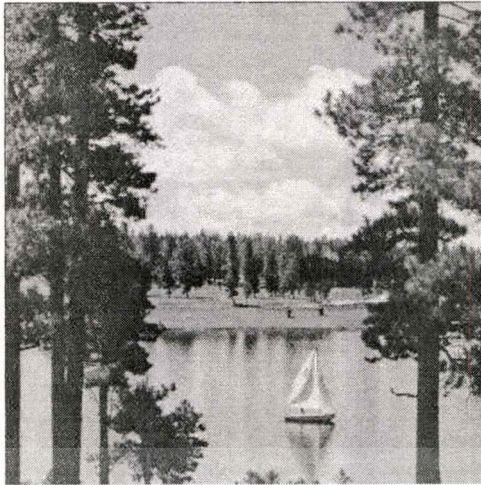


(ข) PSNR = 29.1921 dB และ NC = 0.8390

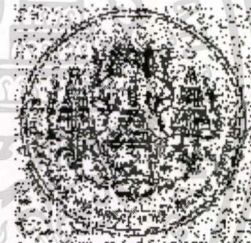


(ค) PSNR = 29.6101 dB และ NC = 0.8519

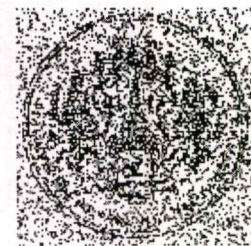
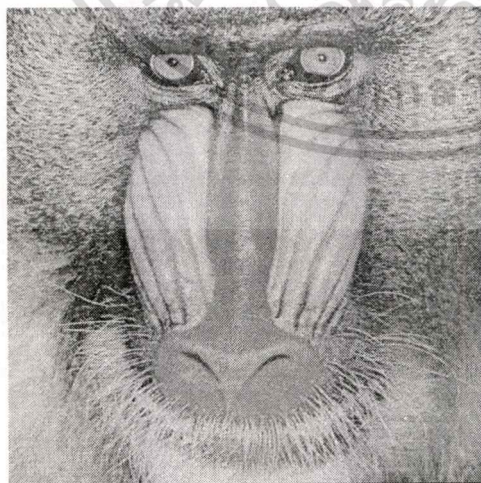
รูปที่ 4.12 ภาพลายน้ำที่ผ่านการบีบอัดข้อมูลแบบ JPEG โดยคุณภาพของภาพเท่ากับ 20% และภาพ
 สัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน
 เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
 ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ง) PSNR = 28.4507 dB และ NC = 0.8445



(จ) PSNR = 29.3533 dB และ NC = 0.8464

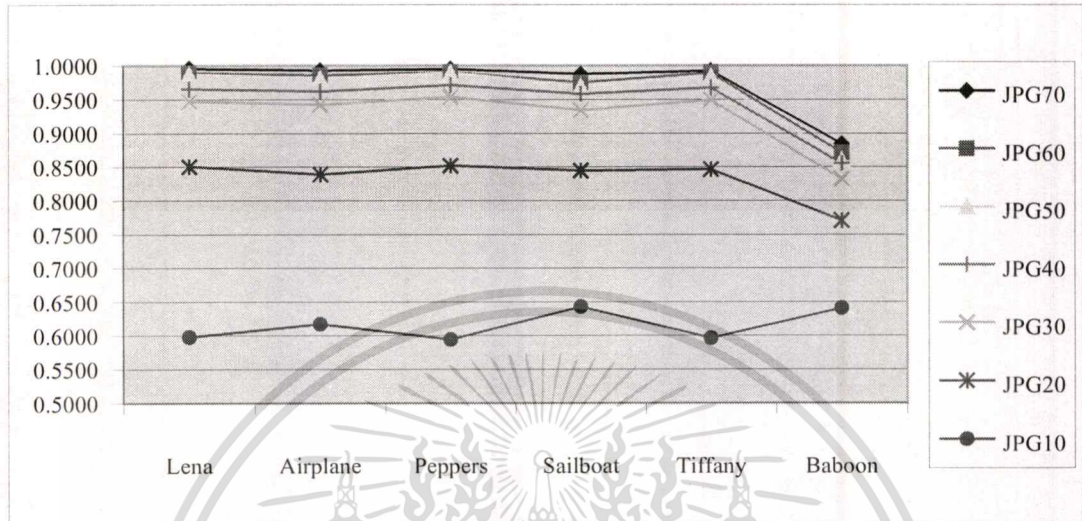


(ฉ) PSNR = 25.0807 dB และ NC = 0.7706

รูปที่ 4.12 (ต่อ)

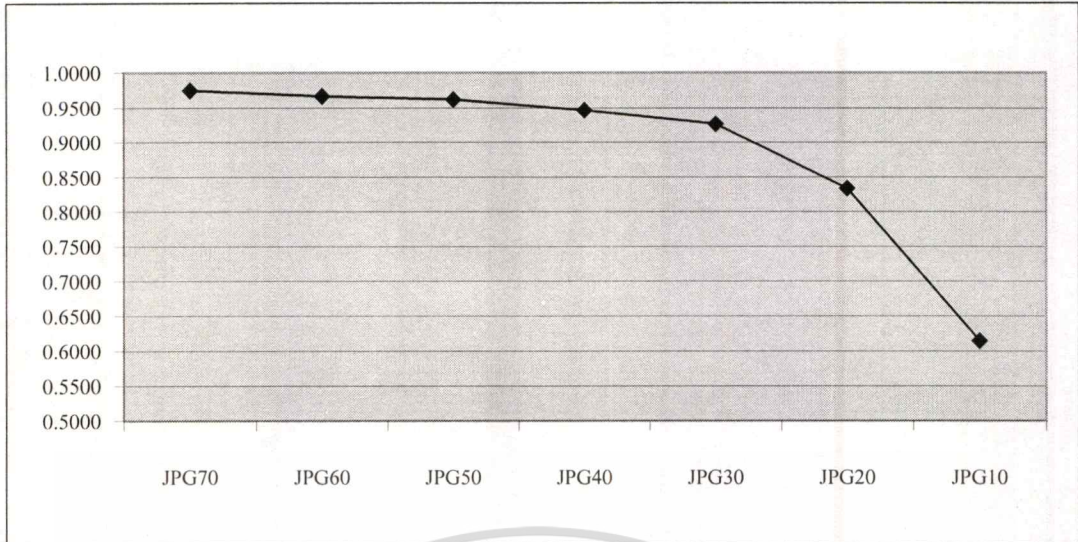
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนหลังจากบีบอัดข้อมูลแบบ JPEG ด้วย Quality Factor ที่แตกต่างกันได้ง่าย จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้ดังแสดงในรูปที่ 4.13



รูปที่ 4.13 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากผ่านการบีบอัดข้อมูลแบบ JPEG

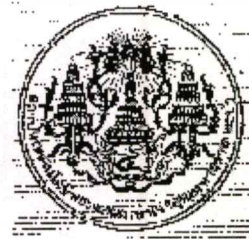
เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนหลังจากบีบอัดข้อมูลแบบ JPEG ด้วย Quality Factor ที่แตกต่างกันได้ง่าย จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้โดยทำการเฉลี่ยจากค่าที่ได้จากทุกภาพในแต่ละ Quality Factor ได้กราฟดังแสดงในรูปที่ 4.14



รูปที่ 4.14 กราฟเปรียบเทียบค่า NC เฉลี่ยของทุกภาพที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากผ่านการบีบอัดข้อมูลแบบ JPEG

4.3.1.2 การกรองความถี่

โดยปกติการกรองความถี่ใช้สำหรับการทำภาพให้เลือนและสำหรับการลดทอนสัญญาณรบกวน โดยทดลองนำภาพที่ฝังลายน้ำมาผ่านการกรองความถี่ 2 แบบที่นิยมใช้คือ averaging filter และ median filter ด้วย mask ขนาด 3x3 กับภาพที่ได้ทำการฝังลายน้ำแล้ว ดังแสดงในรูปที่ 4.15 และ 4.16 ตามลำดับ และเพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนหลังจากผ่านการกรองความถี่ทั้ง 2 แบบได้ง่าย จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้ดังแสดงในรูปที่ 4.17



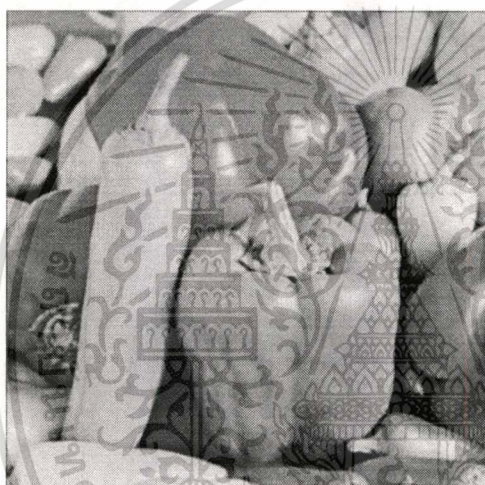
(ก) PSNR = 31.1608 dB และ NC = 0.9522

รูปที่ 4.15 ภาพลายน้ำที่ผ่านการกรองความถี่แบบ 3x3 averaging filter และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน

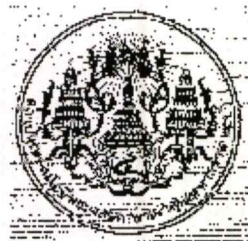
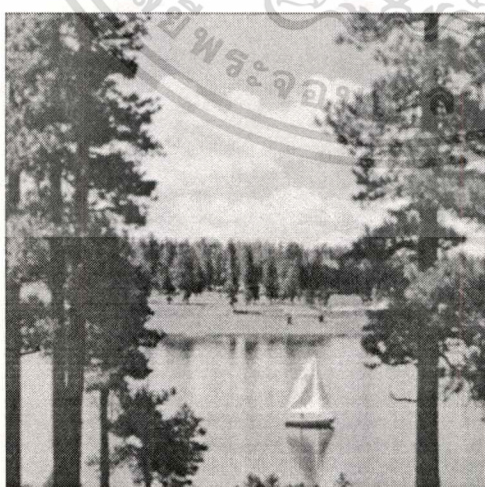
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ข) PSNR = 30.7382 dB และ NC = 0.9490



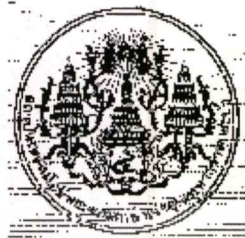
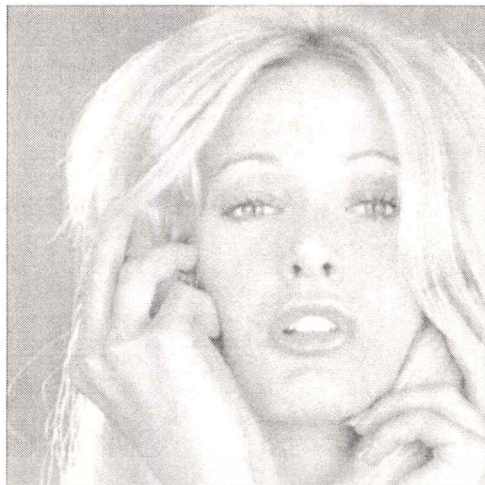
(ค) PSNR = 31.7945 dB และ NC = 0.9473



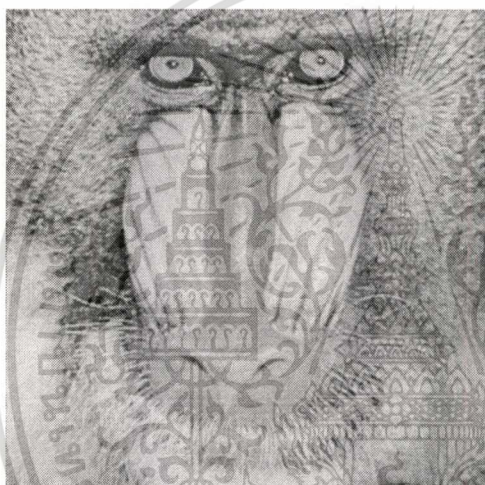
(ง) PSNR = 30.0139 dB และ NC = 0.9378

รูปที่ 4.15 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(จ) PSNR = 30.5501 dB และ NC = 0.9541



(ฉ) PSNR = 24.3970 dB และ NC = 0.8489

รูปที่ 4.15 (ต่อ)

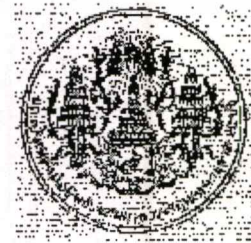
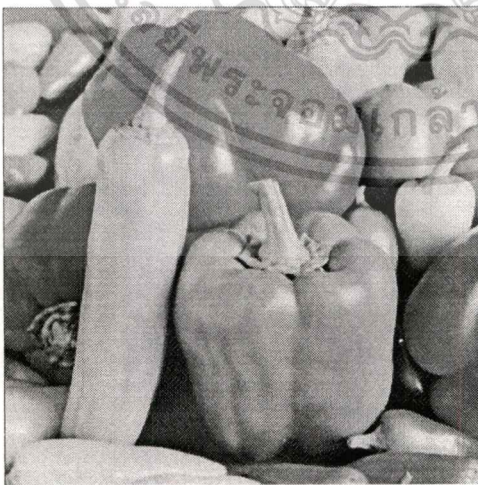
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ก) PSNR = 32.8581 dB และ NC = 0.9254



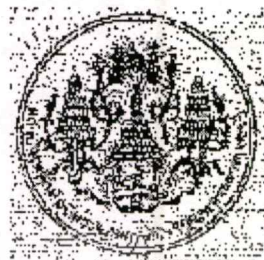
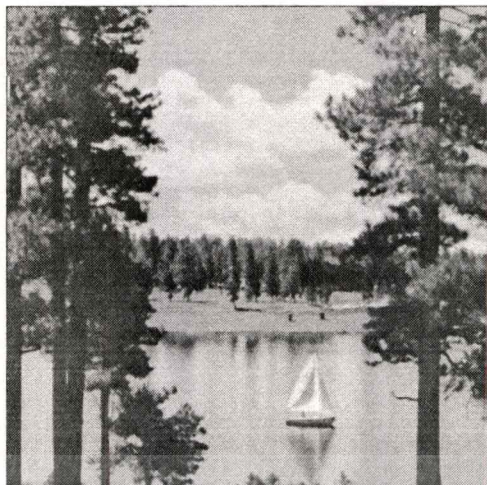
(ข) PSNR = 32.7090 dB และ NC = 0.9065



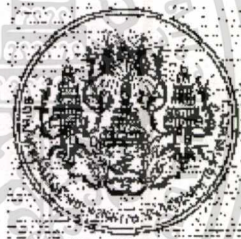
(ค) PSNR = 33.5347 dB และ NC = 0.9091

รูปที่ 4.16 ภาพลายน้ำที่ผ่านการกรองความถี่แบบ 3x3 Median Filter และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน

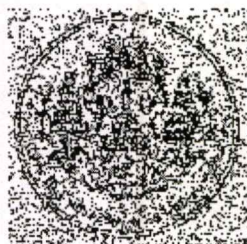
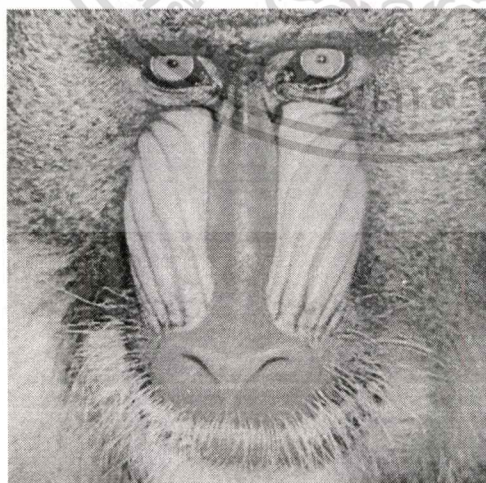
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ง) PSNR = 30.6888 dB และ NC = 0.8863



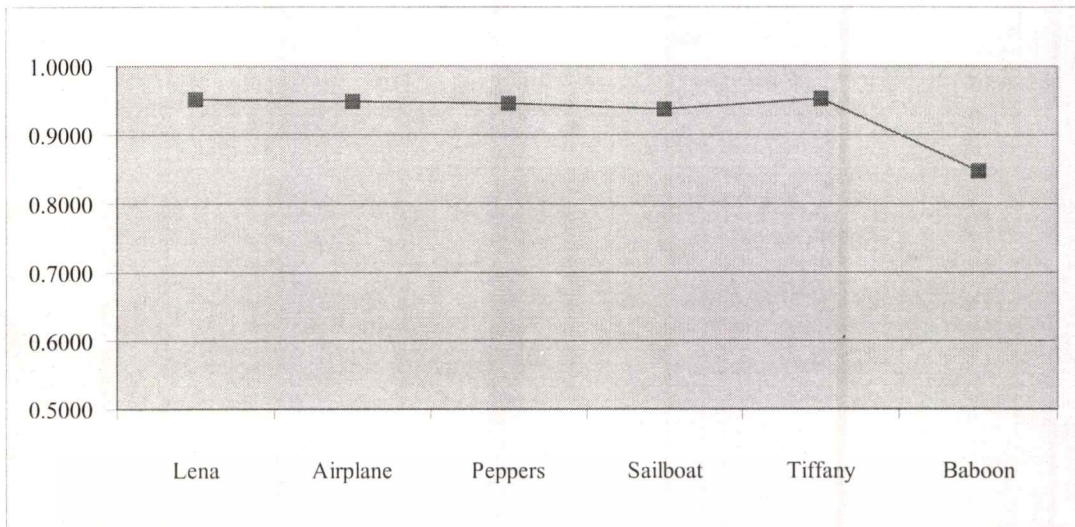
(จ) PSNR = 33.2791 dB และ NC = 0.9339



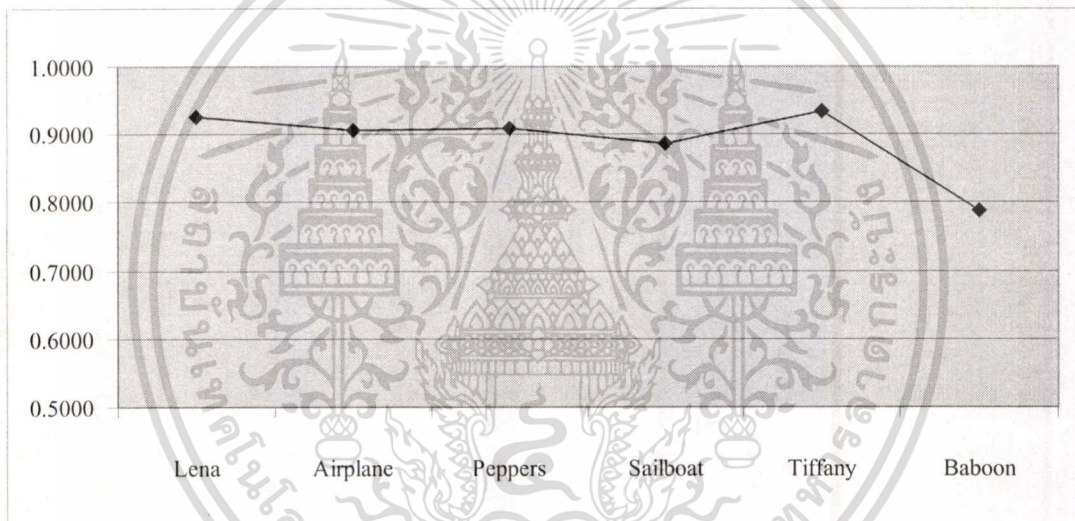
(ฉ) PSNR = 24.7701 dB และ NC = 0.7884

รูปที่ 4.16 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่าจะกรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ก)

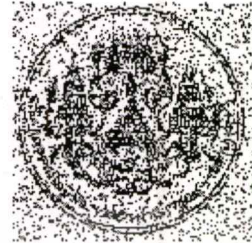


(ข)

รูปที่ 4.17 (ก) กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากผ่านการกรองความถี่แบบ 3x3 averaging filter (ข) กราฟเปรียบเทียบค่า NC ของภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืนหลังจากผ่านการกรองความถี่แบบ 3x3 median filter

4.3.1.3 การใส่สัญญาณรบกวนแบบเกาส์เซียน

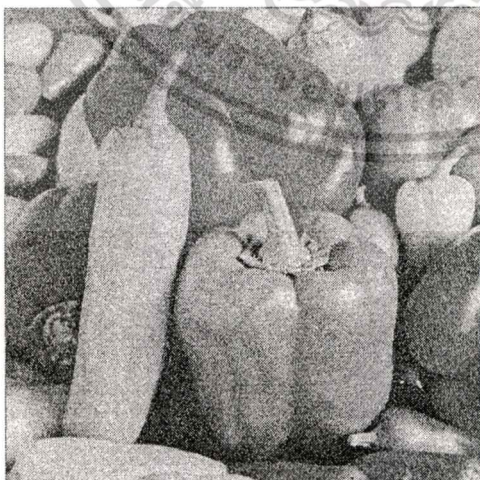
เพื่อทดสอบความคงทนของลายน้ำจากความเสียหายรูปแบบอื่น ๆ ทดลองใส่สัญญาณรบกวนแบบเกาส์เซียน ซึ่งผลที่ได้หลังจากทดสอบกับภาพลายน้ำแสดงดังรูปที่ 4.18



(ก) PSNR = 17.9262 dB และ NC = 0.8181



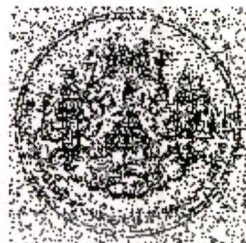
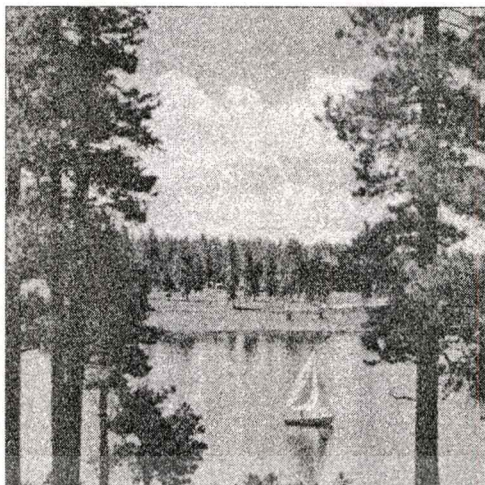
(ข) PSNR = 18.0645 dB และ NC = 0.8256



(ค) PSNR = 18.4517 dB และ NC = 0.8186

รูปที่ 4.18 ภาพลายน้ำที่ผ่านการใส่สัญญาณรบกวนเกาส์เซียน และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน

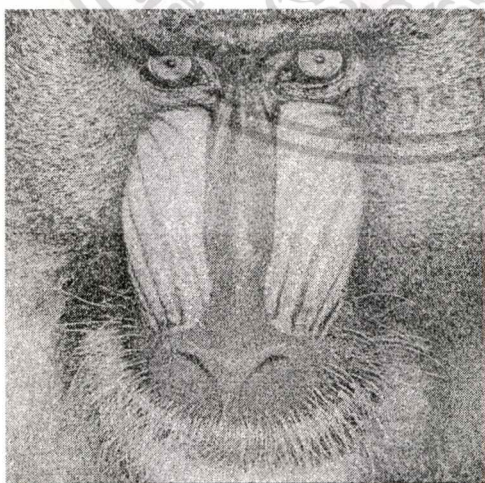
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



(ง) PSNR = 18.0426 dB และ NC = 0.8130



(จ) PSNR = 18.3139 dB และ NC = 0.8273

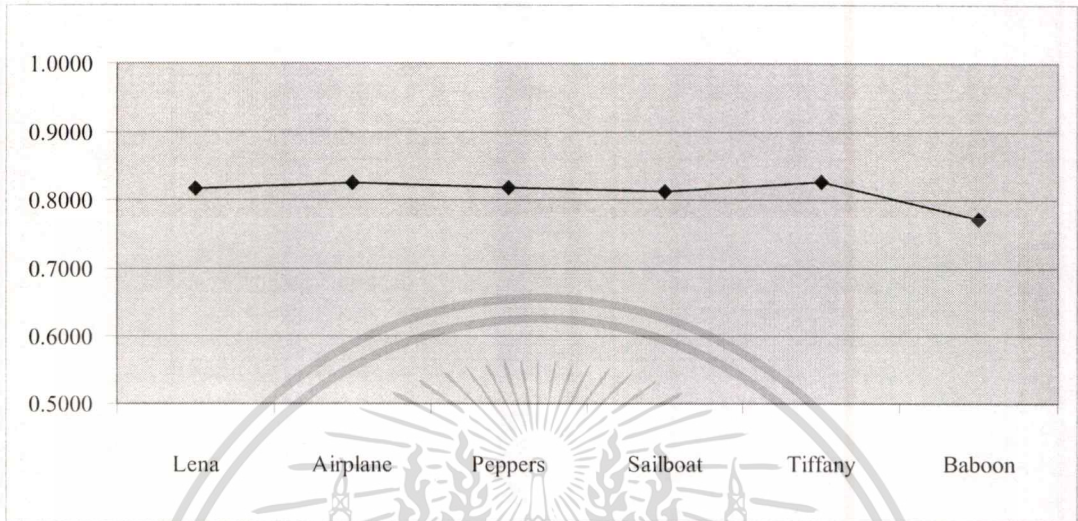


(ฉ) PSNR = 17.9448 dB และ NC = 0.7727

รูปที่ 4.18 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนจากภาพลายน้ำที่ผ่านการใส่สัญญาณรบกวนเกาซ์เซียน จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้ดังแสดงในรูปที่ 4.19



รูปที่ 4.19 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากผ่านการใส่สัญญาณรบกวนเกาซ์เซียน

4.3.2 การทดสอบความคงทนของลายน้ำต่อความผิดเพี้ยนทางเรขาคณิต

ทำการทดสอบด้วยการตัดบางส่วนของภาพ จากภาพที่ได้ทำการฝังลายน้ำแล้ว

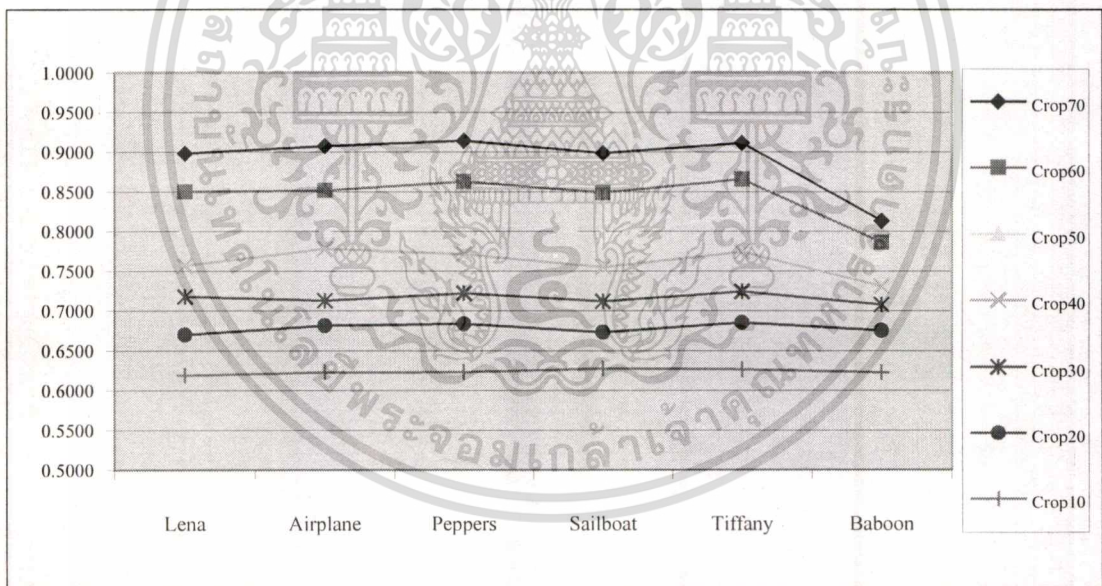
4.3.2.1 การตัดบางส่วนของภาพ

เป็นการทดลองนำภาพดิจิทัลที่มีลายน้ำทำการตัดบางส่วนของภาพ โดยในการทดลองจะทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10% ซึ่งเป็นผลให้จำนวนลายน้ำที่ฝังอยู่ในภาพก็ลดลงตามไปด้วย ค่า NC ของภาพที่ตรวจสอบได้หลังจากทำการตัดบางส่วนของภาพแสดงในตารางที่ 4.2

ตารางที่ 4.2 ค่า NC ของภาพลายน้ำที่ได้หลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10%

พื้นที่ภาพ	70%	60%	50%	40%	30%	20%	10%
Lena	0.8984	0.8500	0.8020	0.7570	0.7177	0.6701	0.6189
Airplane	0.9078	0.8517	0.8026	0.7780	0.7126	0.6813	0.6229
Peppers	0.9146	0.8630	0.8141	0.7712	0.7221	0.6835	0.6233
Sailboat	0.8987	0.8489	0.7950	0.7550	0.7117	0.6730	0.6280
Tiffany	0.9116	0.8659	0.8211	0.7742	0.7242	0.6851	0.6267
Baboon	0.8135	0.7863	0.7659	0.7308	0.7075	0.6752	0.6229

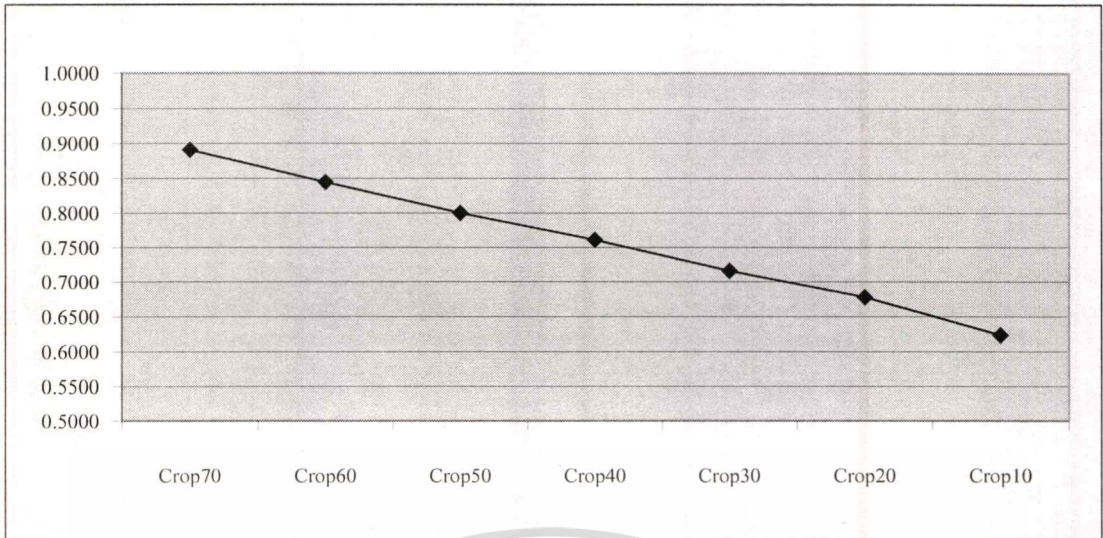
เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้หลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10% ได้ง่าย จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้ดังแสดงในรูปที่ 4.20



รูปที่ 4.20 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10%

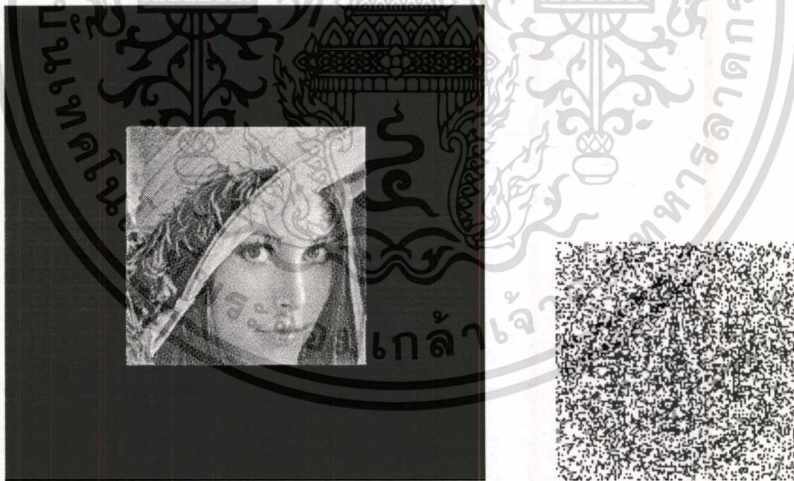
เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนหลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10% ได้ง่าย จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้โดยทำการเฉลี่ยจากค่าที่ได้จากทุกภาพในแต่ละภาพได้กราฟดังแสดงในรูปที่ 4.21

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้าไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



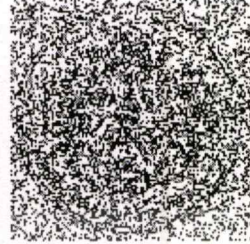
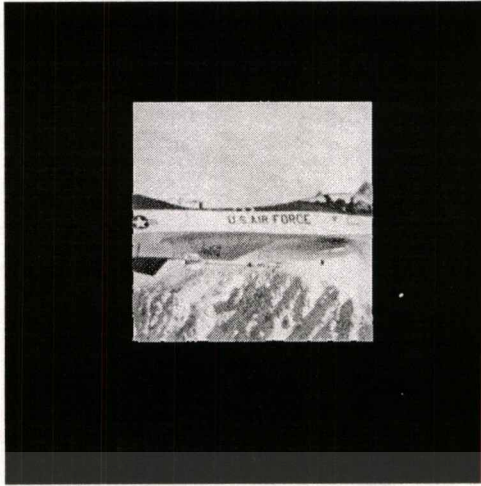
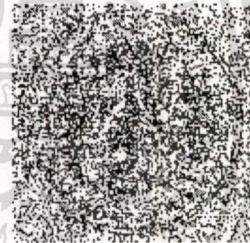
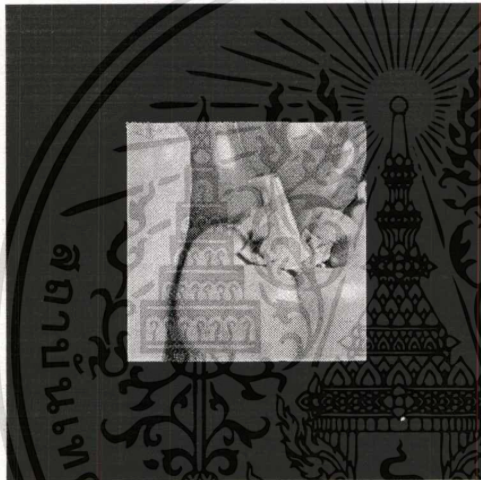
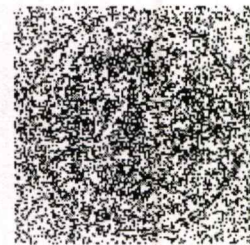
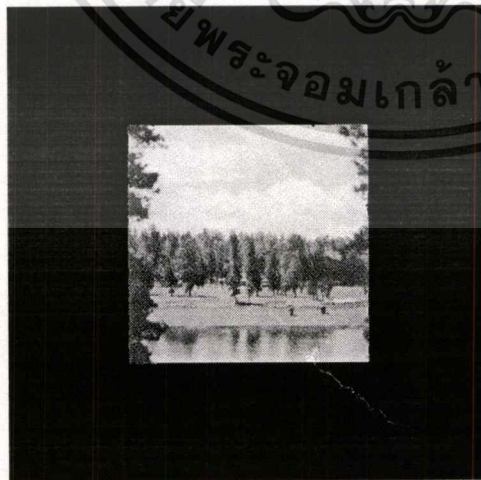
รูปที่ 4.21 กราฟเปรียบเทียบค่า NC เฉลี่ยของทุกภาพที่ตรวจสอบได้จากภาพลายน้ำที่นำกลับคืนหลังจากทำการตัดบางส่วนของภาพให้เหลือพื้นที่ของภาพเท่ากับ 70% ถึง 10%

รูปที่ 4.22 เป็นตัวอย่างการทดลองนำภาพดิจิทัลที่มีลายน้ำทำการตัดบางส่วนของภาพด้านละ 128 พิกเซล จนเหลือพื้นที่ภาพเพียง 25% จากพื้นที่ของภาพเดิม และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน



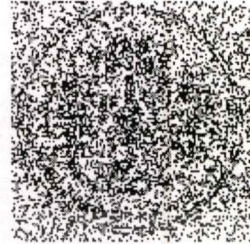
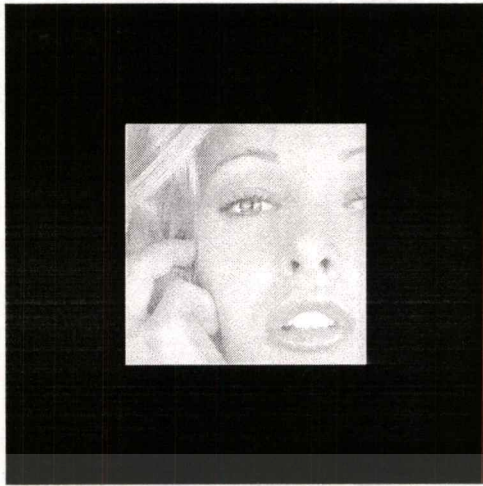
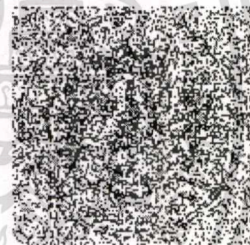
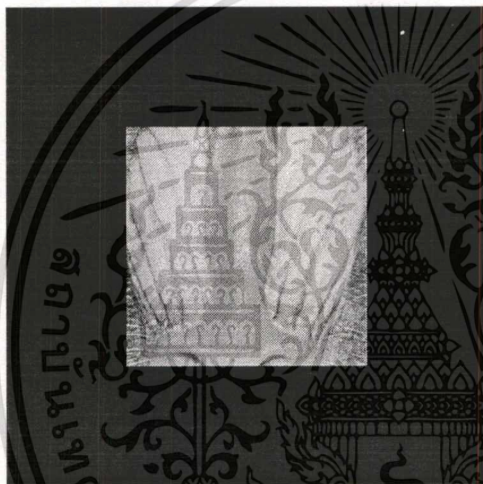
(ก) $NC = 0.6913$

รูปที่ 4.22 ภาพลายน้ำที่ผ่านการตัดบางส่วนของภาพโดยมีพื้นที่ของภาพเหลือเพียง 25% และภาพสัญลักษณ์ลับที่ได้จากการนำลายน้ำกลับคืน

(ข) $NC = 0.6866$ (ค) $NC = 0.7011$ (ง) $NC = 0.6930$

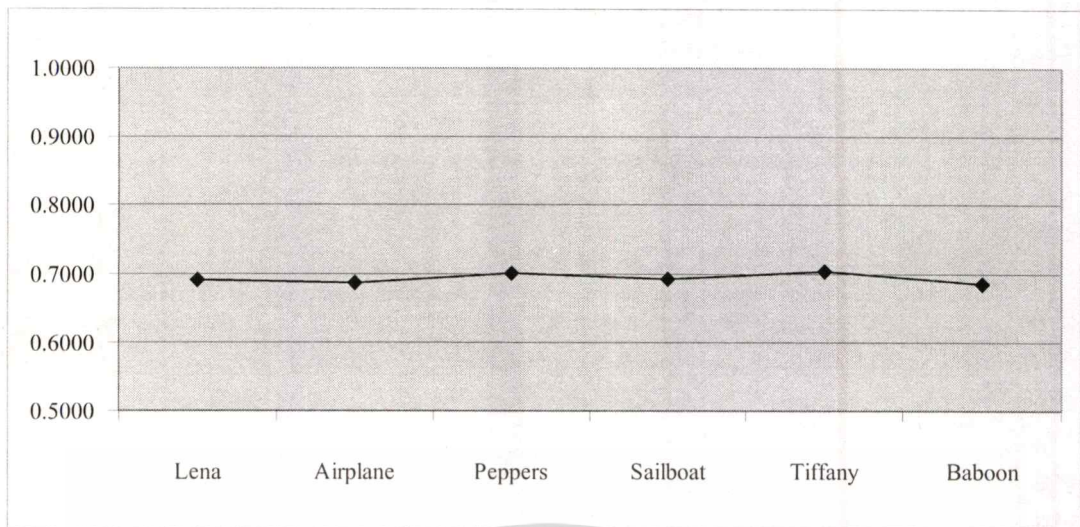
รูปที่ 4.22 (ต่อ)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

(จ) $NC = 0.7034$ (ข) $NC = 0.6851$

รูปที่ 4.22 (ต่อ)

เพื่อให้สามารถเปรียบเทียบผลการทดลองที่ได้จากการนำลายน้ำกลับคืนจากภาพลายน้ำที่ผ่านการตัดบางส่วนของภาพ โดยมีพื้นที่ของภาพเหลือเพียง 25% จึงได้แสดงเป็นกราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้ดังแสดงในรูปที่ 4.23



รูปที่ 4.23 กราฟเปรียบเทียบค่า NC ที่ตรวจสอบได้จากภาพถ่ายน้ำที่นำกลับคืนหลังจากผ่านการตัดบางส่วนของภาพ โดยมีพื้นที่ของภาพเหลือเพียง 25%



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

วิทยานิพนธ์ฉบับนี้เสนอวิธีการซ่อนลายน้ำภาพดิจิทัล โดยใช้การฝังภาพสัญญาณลับ 2 มิติแบบไปนารีในภาพดิจิทัลต้นฉบับแบบโทนสีเทาด้วยเทคนิคการแปลงฟูรีเยร์ (Fourier Transform) และเทคนิคคอสคริตโคไซน์ทรานส์ฟอร์ม (Discrete Cosine Transform) ลายน้ำจะถูกฝังลงในโดเมนความถี่ของภาพดิจิทัลต้นฉบับ ซึ่งถูกขยายด้วยแฟคเตอร์ของแอมพลิจูดที่ปรับได้ (α) เป็นค่าคงที่ที่กำหนดจากความคงทนของสัญญาณลับที่ใช้ ค่าของ α จะถูกเลือกเพื่อให้ได้ค่าที่ดีที่สุดระหว่างความคงทนกับการไม่ปรากฏให้เห็น ในการเลือกค่าของ α ทำให้มีผลต่อประสิทธิภาพของระบบสองด้าน คือมีผลกระทบต่อการทำให้สังเกตเห็นได้ เมื่อ α มีค่าสูงจะทำให้ลายน้ำปรากฏเด่นชัดมากขึ้นหมายถึงทำให้สังเกตเห็นได้มากขึ้น แต่ก็ทำให้ระบบมีความคงทนมากขึ้นด้วย ในทางตรงกันข้ามหาก α มีค่าน้อยจะทำให้ลายน้ำไม่ปรากฏให้เห็นเด่นชัดมากหมายถึงทำให้สังเกตเห็นได้ยากขึ้น แต่ก็ทำให้ระบบมีความคงทนน้อยลงด้วย โดยเทคนิคนี้ไม่จำเป็นต้องใช้ภาพต้นฉบับในการนำภาพสัญญาณลับกลับคืน ซึ่งทำให้กระบวนการในการถอดรหัสทำได้ง่ายและสะดวก ผลที่ได้จากการทดลองยังแสดงให้เห็นว่าเทคนิคการซ่อนลายน้ำแบบนี้มีความคงทนต่อการประมวลผลสัญญาณภาพในรูปแบบต่าง ๆ โดยสามารถทดสอบประสิทธิภาพของลายน้ำภาพดิจิทัลด้วยวิธีการต่างๆ เช่น การบีบอัดข้อมูลภาพ การใส่สัญญาณรบกวนแบบเกาส์เซียน การกรองภาพ และรวมถึงความผิดเพี้ยนทางเรขาคณิตโดยการตัดบางส่วนของภาพออกซึ่งทำให้ภาพขาดรายละเอียดของข้อมูลลายน้ำที่ฝังลงไป ในภาพตั้งแต่เหลือพื้นที่ภาพ 70% และลดลงจนเหลือเพียง 10% ของภาพเดิม ซึ่งผลการทดลองที่ได้ยังคงสามารถทำการตรวจหาลายน้ำจากภาพได้อย่างดี ซึ่งผลที่ได้มีการตรวจสอบและสามารถคำนวณค่าได้เป็นตัวเลขไม่ว่าจะเป็นการวัดค่าความผิดพลาด PSNR ของภาพที่ได้ทำการใส่ลายน้ำ รวมถึงการเปรียบเทียบภาพลายน้ำต้นฉบับกับภาพลายน้ำที่ทำการตรวจหาได้เป็นค่า NC ซึ่งเป็นข้อมูลในการตัดสินใจยอมรับภาพที่ได้ตรวจหาว่าเป็นภาพที่เป็นเจ้าของลิขสิทธิ์จริงๆ

เมื่อเปรียบเทียบผลการทดลองระหว่างการซ่อนลายน้ำภาพดิจิทัลด้วยเทคนิคการแปลงฟูรีเยร์ (Fourier Transform) และเทคนิคคอสคริตโคไซน์ทรานส์ฟอร์ม (Discrete Cosine Transform) ทำให้พบว่าด้วยคุณสมบัติต่างๆของเทคนิคคอสคริตโคไซน์ทรานส์ฟอร์ม ทำให้การซ่อนลายน้ำภาพดิจิทัลด้วยเทคนิคคอสคริตโคไซน์ทรานส์ฟอร์ม ดีกว่าการซ่อนลายน้ำด้วยเทคนิคการแปลงฟูรีเยร์ ดังแสดงได้ในตาราง 5.1 ตารางเปรียบเทียบผลการทดลอง

ตารางที่ 5.1 ตารางเปรียบเทียบผลการทดลองที่ได้จากการคำนวณการซ่อนลายน้ำทั้ง 2 วิธี

	FFT	FFT หลังปรับแต่ง	DCT	DCT หลังปรับแต่ง
PSNR	30.3529	30.8419	30.4534	30.4534
NC	0.5843	0.6428	0.9890	0.9902

จากตารางค่า NC ที่แสดงทำให้ทราบว่า การซ่อนลายน้ำภาพดิจิทัลด้วยเทคนิคดิสครีตโคไซน์ทรานส์ฟอร์ม (DCT) มีประสิทธิภาพมากกว่าการซ่อนลายน้ำภาพดิจิทัลด้วยเทคนิคการแปลงฟูริเยร์ (FFT) เปรียบเทียบได้จาก ค่า NC ที่วัดได้จากลายน้ำที่นำกลับคืน เมื่อกระบวนการฝังลายน้ำและค่า PSNR ที่เหมือนกันระหว่าง 2 กระบวนการ พบว่าค่า NC ที่ได้จากการซ่อนลายน้ำภาพดิจิทัลด้วยเทคนิคดิสครีตโคไซน์ทรานส์ฟอร์มมีค่ามากกว่าการซ่อนลายน้ำภาพดิจิทัลด้วยเทคนิคการแปลงฟูริเยร์อย่างเห็นได้ชัด ทั้งนี้สามารถอธิบายได้ว่า [14] DFT เป็นวิธีการทรานส์ฟอร์มวิธีหนึ่งที่ประกอบไปด้วยฟังก์ชันพื้นฐาน ได้แก่ อัลกอริทึมการคำนวณที่มีประสิทธิภาพและการรวมกันของพลังงานที่ดีสำหรับรูปทั่วไป Fast Fourier Transforms (FFT) อัลกอริทึมสามารถใช้ในการคำนวณ DFT และ inverse DFT ได้เป็นอย่างดี บวกกับการที่รูปทั่วไป ส่วนประกอบที่สำคัญของพลังงานของสัญญาณคือต้องมุ่งไปที่บริเวณที่มีความถี่ต่ำ ซึ่ง DFT มีความสำคัญมากในการประมวลผลสัญญาณดิจิทัล ด้วยเหตุนี้เองเมื่อเริ่มแรกของการพัฒนาเทคนิคการทรานส์ฟอร์มภาพที่ได้พัฒนาขึ้นในช่วงปลายปี 1960 DFT จึงเป็นเทคนิคแรกๆ ที่ได้รับความสนใจ

มันมีความเป็นไปได้ที่จะสามารถปรับปรุงคุณสมบัติการรวมกันของพลังงานของ DFT ให้ดีขึ้น โดยที่ไม่ต้องคำนึงถึงคุณสมบัติอื่น The discrete cosine transform (DCT) เป็นวิธีที่สามารถทำได้ DCT มีความสามารถใกล้เคียงกับ DFT มาก แต่เป็นวิธีการทรานส์ฟอร์มที่ได้รับความนิยมมากกว่าเทคนิคการทรานส์ฟอร์มภาพแบบอื่นๆ ความสัมพันธ์ระหว่าง DCT และ DFT รวมถึงข้อดีในด้านการรวมกันของพลังงานที่ดีที่ DCT มีเหนือกว่า DFT อธิบายได้ดังนี้

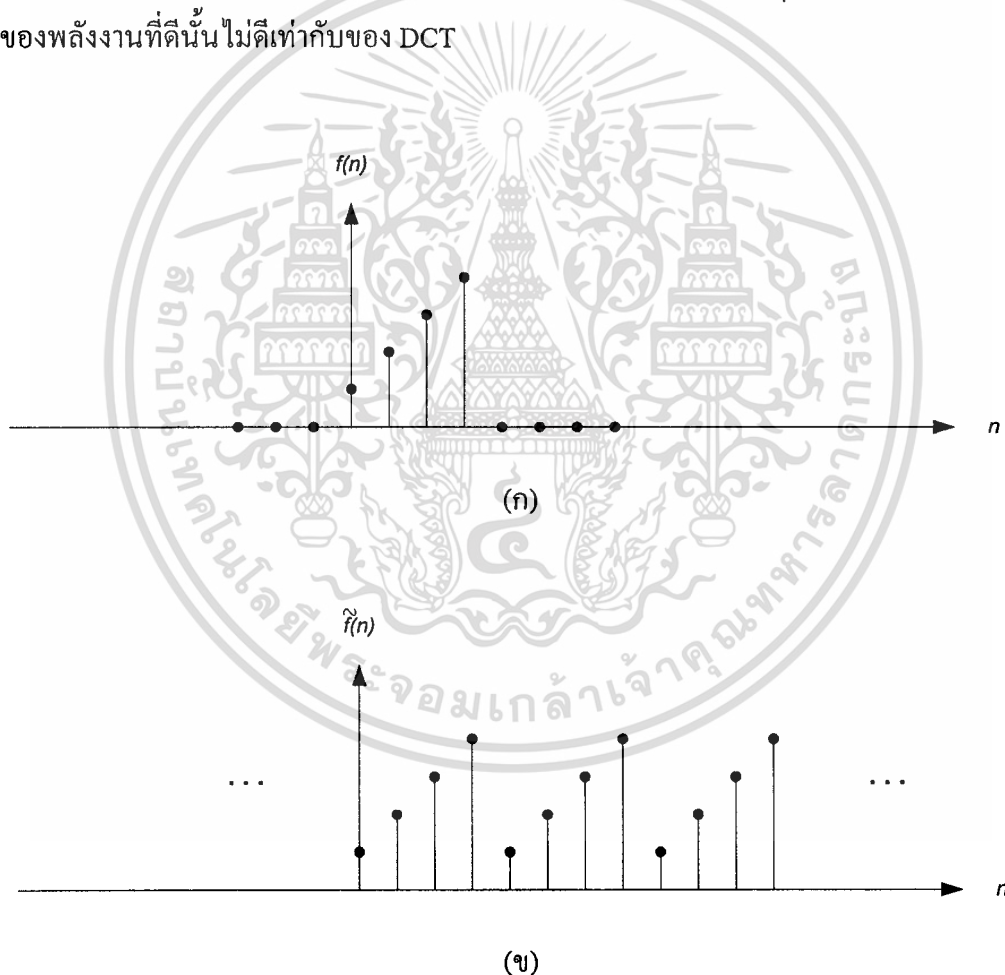
พิจารณาลำดับ N -point 1-D ซึ่งแสดงในรูป 5.1(ก) ในตัวอย่างนี้ $N=4$ DFT $F(k)$ ประกอบด้วยค่าสัมประสิทธิ์ DFS $\tilde{F}(k)$ โดย $0 \leq k \leq N-1$ สัมประสิทธิ์ DFS $\tilde{F}(k)$ ได้มาจาก periodic sequence $\tilde{f}(n)$ ดังแสดงในรูป 5.1(ข)

จากรูป 5.1(ข) $\tilde{f}(n)$ มีความเด่นชัดของความไม่ต่อเนื่องที่ไม่เป็นไปตามธรรมชาติ ซึ่งเกิดขึ้นมาจากการรวมกันของจุดเริ่มต้นกับสิ้นสุดลงของ $f(n)$ ความไม่ต่อเนื่องผลักดันพลังงานสู่ความถี่สูงและลดประสิทธิภาพด้านการรวมกันของพลังงานที่ดีของ DFT เพื่อที่จำกำจัดความไม่ต่อเนื่องที่ไม่เป็นไปตามธรรมชาติ เราสร้าง $2N$ -point sequence $g(n)$ จาก $f(n)$ ดังแสดงในรูป 5.1 (ค) ลำดับ $g(n)$ จะสมมาตรกัน N point แรกของ $g(n)$ เหมือนกันกับของ $f(n)$ ถ้าเราคำนวณ

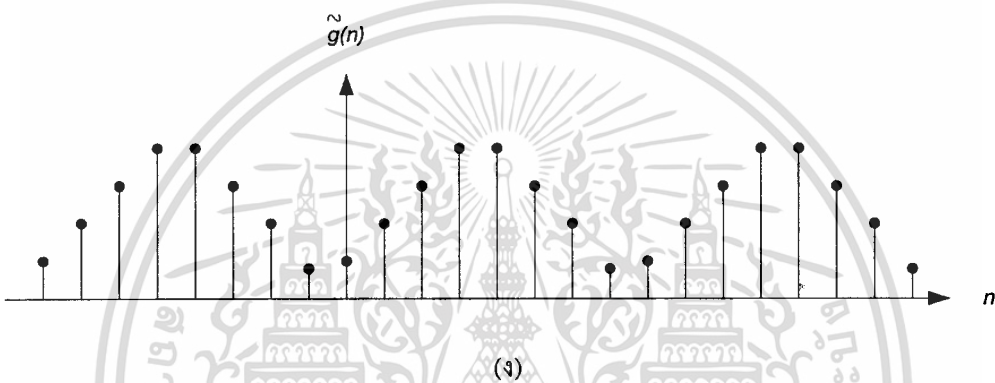
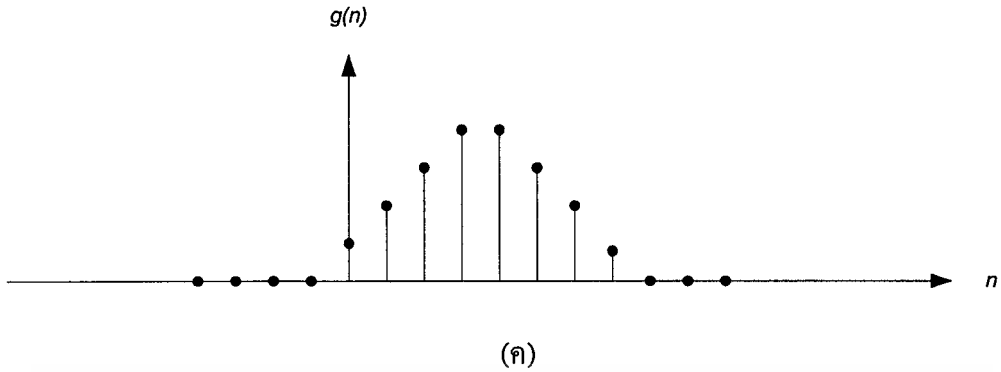
$2N$ -point DFT ของ $g(n)$ จะได้ว่า DFT $G(k)$ เหมือนกันกับสัมประสิทธิ์ DFS $G(k)$ ซึ่งได้มาจาก periodic sequence $\tilde{g}(n)$ ดังแสดงในรูป 5.1(ง)

DCT ถูกนิยามในนามของ $G(k)$ จะเห็นได้ชัดว่าลำดับ $\tilde{g}(n)$ ไม่มีความไม่ต่อเนื่องที่ไม่เป็นธรรมชาติ และประสิทธิภาพด้านการรวมกันของพลังงานที่ดีของ DCT ดีขึ้นถึงแม้ว่าขนาดของ DFT นั้นเพิ่มขึ้นเป็น 2 เท่าแต่ความต้องการด้านการคำนวณก็ยังคงเหมือนกันกับ N -point DFT อันเป็นผลมาจากการสมมาตรกันของ $g(n)$

วิธีการทรานส์ฟอร์มของการประมวลผลภาพนอกจากใช้ DFT และ DCT แล้วยังมีวิธีอื่นอีกเช่น Haar, Hadamard, discrete sine และ slant แต่เมื่อพิจารณาจากคุณสมบัติด้านการรวมกันของพลังงานที่ดีและความต้องการด้านการคำนวณ เข้าด้วยกันแล้ว DCT จึงถือว่าเป็นวิธีที่ดีที่สุด การทรานส์ฟอร์ม แบบ Haar และ Hadamard ใช้การคำนวณน้อยกว่า DCT แต่คุณสมบัติด้านการรวมกันของพลังงานที่ด้อยกว่า DCT



รูปที่ 5.1 อธิบายลักษณะของการรวมกันของพลังงานระหว่างเทคนิคดิสครีต โคไซน์ทรานส์ฟอร์ม และดิสครีตฟูริเยร์ทรานส์ฟอร์ม



รูปที่ 5.1 (ต่อ)

5.2 ปัญหาที่พบและข้อเสนอแนะ

1. ในการวิจัยการซ่อนลายน้ำด้วยเทคนิคการแปลงฟูรีเยร์ได้พบว่า กระบวนการในการแปลงดังกล่าวมีข้อจำกัดคือเมื่อแปลงภาพต้นฉบับไปสู่โดเมนความถี่จะได้ค่าสัมประสิทธิ์เป็นจำนวนเชิงซ้อน ซึ่งค่าที่ได้ประกอบด้วยค่าแมกนิจูดและเฟสของพิกเซล แต่เพื่อให้ลายน้ำที่ทำการซ่อนมีประสิทธิภาพที่ดี มีความคงทนลายน้ำจะฝังในแมกนิจูดของพิกเซล ดังนั้นกระบวนการก่อนการฝังลายน้ำจึงต้องมีการแยกค่าของพิกเซลและทำการฝังก่อนที่จะนำค่าเฟสของพิกเซลมารวมอีกครั้งหนึ่งค่าที่ได้จึงมีการผิดเพี้ยนไป ทำให้ภาพที่ได้จากการฝังลายน้ำเมื่อมองด้วยตาเปล่าพบว่าภาพมีการผิดเพี้ยนไปมากพอสมควร

2. ในการวิจัยการซ่อนลายน้ำด้วยเทคนิคการแปลงฟูรีเยร์พบว่า ความคงทนของการซ่อนลายน้ำด้วยวิธีนี้ไม่ดัดนัก ดังนั้นในการฝังลายน้ำจึงต้องทำการฝังลายน้ำจำนวนมากจึงทำให้การตรวจหาลายน้ำกลับคืนจะมีคุณภาพที่สามารถมองด้วยตาเปล่าได้อย่างแม่นยำ ในการฝังลายน้ำจำนวนมากมีผลโดยตรงกับภาพทำให้ภาพคุณภาพด้อยลงไป

3. ค่าตัวแปรต่างๆที่กำหนดขึ้นเป็นค่าที่ผู้จัดทำได้ทำการทดลองและเลือกกำหนดขึ้นซึ่งอาจจะไม่ใช่ค่าที่ดีที่สุดสำหรับภาพใดภาพหนึ่ง แต่เป็นค่าที่เลือกเพื่อให้กระบวนการที่เสนอในงาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น เมื่อนำไปใช้ประโยชน์ด้านการค้า

ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

วิจัยนี้จะสามารถประยุกต์ใช้กับภาพโทนสีเทาได้ในระดับผลการทดลองที่ใกล้เคียงกันของหลายๆ ภาพ ทั้งนี้มีปัจจัยอีกหลายอย่างที่ทำให้ภาพแต่ละภาพเมื่อประยุกต์ใช้อัลกอริทึมที่นำเสนอแล้ว ได้ผลการทดลองที่แตกต่างกันไปบ้าง เช่น ลักษณะของภาพต้นฉบับ ลักษณะของภาพสัญลักษณ์ลับที่ใช้ เป็นต้น

4. ในวิทยานิพนธ์ฉบับนี้มุ่งเน้นที่การนำเสนอเทคนิคการซ่อนลายน้ำในภาพดิจิทัลโทนสีเทา ซึ่งอาจจะสามารถนำกระบวนการที่นำเสนอไปประยุกต์ในการวิจัยการซ่อนลายน้ำในภาพดิจิทัลแบบอื่นๆ ต่อไปได้

5. ในวิทยานิพนธ์ฉบับนี้เสนอเทคนิคการซ่อนลายน้ำภาพดิจิทัลในโดเมนความถี่ โดยมีการเสนอเทคนิคโดยใช้การแปลงข้อมูลภาพสู่โดเมนความถี่ 2 แบบด้วยกันคือ เทคนิคการแปลงฟูริเยร์ และเทคนิคดิสครีตโคไซน์ทรานส์ฟอร์ม ซึ่งกระบวนการที่นำเสนออาจสามารถใช้วิธีการแปลงภาพไปสู่โดเมนความถี่ด้วยเวฟเล็ตที่เป็นที่นิยมใช้กันอย่างกว้างขวางได้อีกวิธีหนึ่ง



เอกสารอ้างอิง

- [1] I.J. Cox, J. Kilian, F.T. Leighton and T. Shamoan, "Secure Spread Spectrum Water-marking for Multimedia.", IEEE Trans. Image Proc., vol. 6, no. 12, 1997, pp. 1673-1687.
- [2] C. T. Hsu and J. L. Wu, "Hidden digital watermark in images.", IEEE Trans. Image Processing, vol. 8, 1999, pp. 58-68.
- [3] R.J. Anderson and F. Petitcolas. "On the Limits of Stenography.", IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, May 1998, pp. 474-481.
- [4] J. F. Kurose and K. W. Ross. **Computer Networking**. Addison Wesley Longman. 2000.
- [5] Deepa Kundur. "Multiresolution Digital Watermarking: Algorithms and Implications for Multimedia Signals.", A thesis of Doctor of Philosophy Graduate Department of Electrical and Computer Engineering, University of Toronto. 1999.
- [6] F. A. P. Peticolas, R. J. Anderson and M. G. Kuhn, "Information Hiding-A Survey.", Proceedings of the IEEE, Special issue on protection of multimedia contents, vol. 89, no. 7, July 1999, pp. 1062-1078.
- [7] F. Mintzer, G. Braudaway and A. Bell. "Opportunities for watermarking Standards.", Communications of the ACM, vol. 41, no. 7, July 1998, pp. 56-64.
- [8] S.D. Lin and C.F. Chen, "A Robust DCT-Based Watermarking for Copyright Protection.", IEEE Trans. Consumer Electronics, vol. 46, No. 3, June 2000.
- [9] P. Thitimajshima, Y. Thitimajshima and Y. Rangsanseri, "Hiding Confidential Signature into Digital Images via Frequency Domain.", IEEE Region 10 Inter. Conf. on Electrical and Electronic Technology, pp. 246-249, August 2001.
- [10] ยุทธพงศ์ จิตติมัจฉิมา และ ยุทธพงษ์ รั้งสรณ์เสรี "การซ่อนลายน้ำภาพดิจิทัลเพื่อป้องกันลิขสิทธิ์โดยใช้ดีสคริตโคซายน์ทรานส์ฟอร์ม," การประชุมวิชาการครั้งที่ 40, 2545, หน้า 11-18.
- [11] Y. Thitimajshima, N. Chotikakamthorn, Y. Rangsanseri and P. Thitimajshima, "A Robust DCT-Based Watermarking of Still Images with 2D Binary Digital Watermarks.", 2001 International Symposium on Communications and Information Technology, pp. 341-344, 2001.

- [12] P. Rakpratanporn, P. Thitimajshima, Y. Rangsaneri, "Wavelet-based Watermarking for Digital Images,". 2000 Asia-Pacific Symposium on Broadcasting and Communications, pp. 95-100, 2000.
- [13] W. Bender, D. Gruhl, N. Moromoto and A. Lu, "Techniques for Data Hiding.," IBM Sys. J., vol. 35, No. 3, pp.313-336, 1996.
- [14] N. Nikolaidis and I. Pitas, "Robust Image Watermarking in the Spatial Domain.," Signal Processing, vol. 66, pp. 385-403, 1998.
- [15] ปัทมาภรณ์ ทิพากร และ ชำรงรัตน์ อมรรักษ์ยา, "Development of Digital Watermarking Techniques for Copyright Protection.," [Online]. Available : <http://www.cpe.eng.kmutt.ac.th/~mcl/water.htm>. 2002.
- [16] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "Robust watermarking of still images for copyright protection.," In Proc. 13th Inter. Conf. Digital Signal Processing, vol. 2, pp. 499-502, 1997.
- [17] A. Piva, M. Barni, F. Bartolini and V. Cappellini, "DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image.," Image Processing, vol. 1, pp. 520-523, 1997.
- [18] X. Niu, Z Ming and S. Sun, "Digital watermarking of still images with gray-level digital watermarks.," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp.137-145, February 2000.
- [19] F. Hartung and M. Kutter, "Multimedia watermarking techniques.," Proceedings of the IEEE, vol. 87, pp. 1079 –1107, July 1999.



ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก ก.

ผลงานที่ได้รับการตีพิมพ์

1. P. Thitimajshima, Y.Thitimajshima and Y. Rangsanseri, “**Hiding Confidential Signature into Digital Images via Frequency Domain.**”, IEEE Region 10 Inter. Conf. on Electrical and Electronic Technology, pp. 246-249, August 2001.
2. Y. Thitimajshima, N. Chotikakamthorn, Y. Rangsanseri and P. Thitimajshima, “**A Robust DCT-Based Watermarking of Still Images with 2D Binary Digital Watermarks.**”, 2001 International Symposium on Communications and Information Technology, pp. 341-344, 2001.
3. ยุทธพงศ์ ฐิติมีชฌิมา และ ยุทธพงษ์ รังสรรค์เสรี “**การซ่อนลายน้ำภาพดิจิทัลเพื่อป้องกันลิขสิทธิ์โดยใช้ดีสครีตโคไซน์ทรานส์ฟอร์ม,**” การประชุมวิชาการครั้งที่ 40 มหาวิทยาลัยเกษตรศาสตร์, 2545, หน้า 11-18.



A ROBUST DCT-BASED WATERMARKING OF STILL IMAGES WITH 2D BINARY DIGITAL WATERMARKS

*Yutthapong Thitimajshima
Nopporn Chotikakamthorn*

Faculty of Information Technology
King Mongkut's Institute of Technology
Ladkrabang
Bangkok 10520, Thailand
Fax: +66-2-326-9086
Email: {s3067013, kcnoppor}@kmitl.ac.th

*Yuttapong Rangsanseri
Punya Thitimajshima*

Department of Telecommunications Engineering
Faculty of Engineering, King Mongkut's
Institute of Technology Ladkrabang
Bangkok 10520, Thailand
Fax: +66-2-326-9086
Email: {kryuttha, ktpunya}@kmitl.ac.th

ABSTRACT

In this paper, we describe a watermarking technique for hiding a confidential two-dimension binary watermark into a still image. Our technique is applied to the frequency domain of the image obtained by two-dimension DCT. The watermark is embedded into the low frequency and stored according to a zigzag format. Additionally, this technique does not require original image to recover the embedded signature. Experimental results show that the proposed watermarking technique is robust to various kinds of attacks.

1. INTRODUCTION

The growth of networked multimedia systems has caused problems that images, music and movies can be copied from the internet easily. Digital watermarking represents a viable solution to the problem of copyright violation. One approach is to add an invisible image to an image that can be used to provide solid proof of ownership. Digital watermarking techniques have been developed to meet the needs of these growing concerns. Digital watermarking is the imperceptible marking of multimedia data to brand ownership.

In order to be effective, an imperceptible watermark should meet the following requirements [1]:

Unobtrusive: The watermark should be perceptually invisible, or its presence should not interfere with the work being protected.

Robust: The watermark must be difficult to remove for an attacker trying to counterfeit the copyright of the data.

Readily extractable: The data owner or an independent control authority should easily extract it.

Unambiguous: Retrieval of the watermark should unambiguously identify the owner.

During the past few years, many watermarking techniques have been developed. These techniques can be classified either based on spatial domain [2,3] or frequency domain [1,4] (e.g. DCT, wavelet transforms). The spatial domain

watermarking would be robust against noises and JPEG compression as the transform domain methods. Many schemes have found that the transform domain approach has some advantages because most the signal processing operations can be well characterized in the frequency domain, and several good perceptual models are developed in the frequency domain. The technique proposed in this paper is also based on frequency domain.

In this paper, we propose a technique in frequency domain approach based on two-dimension DCT that does not require original image to recover the embedded signature. This paper is organized as follows. In section 2, we proposed the algorithm for embed and extract a watermark. The experimental results and we compare the characteristics of the robustness to the various kinds of attacks such as filtering and JPEG compression are shown in section 3. Finally, the conclusion is given in section 4.

2. THE PROPOSED ALGORITHM

In our method, the watermark is supposed to be a two-dimension binary digital signature such as a binary image. In general, the size of the watermark should be much smaller than the size of the original gray-level image. The watermarking process consists of two main steps: watermark embedding and watermark extracting, to be described as follows.

2.1 Watermark Embedding

Figure 1 shows a block diagram of the watermark embedding process. First, the binary signature image is scanned from left to right and from top to bottom, to produce a bit sequence of watermark S . The data pixels are valued as 1 and the background pixels are valued as -1:

$$S = \{s_i, 1 \leq i \leq M\}, \quad s_i \in \{-1, 1\} \quad (1)$$

The pseudo-random sequence P which each number can take a value either 1 or -1 is

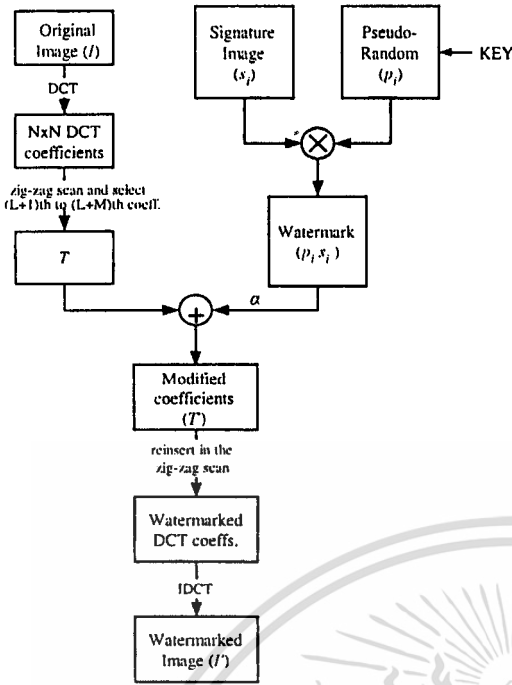


Fig. 1: Watermark embedding process.

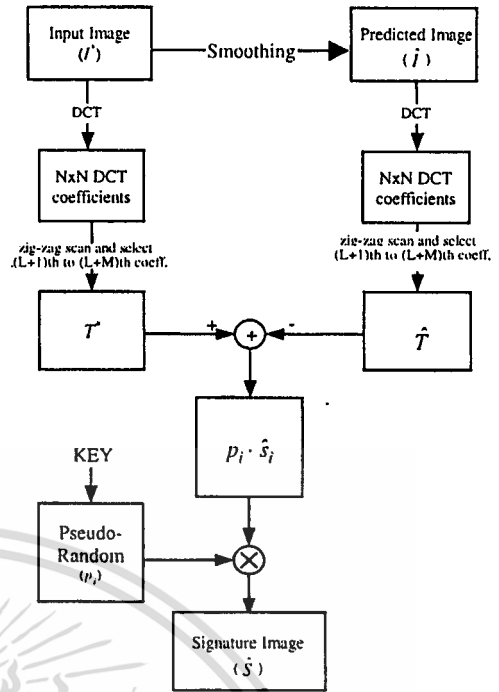


Fig. 2: Watermark extracting process.

equiprobably generated with a secret key for embedding and extracting of the watermark.

$$P = \{p_i, 1 \leq i \leq M\}, \quad p_i \in \{-1, 1\} \quad (2)$$

The two-dimension DCT of an $N \times N$ image I is computed. The DCT coefficients are reordered into a zig-zag scan, such as in the JPEG compression algorithm. In order to obtain the perceptual invisibility without loss of robustness, the lowest L coefficients are skipped. Then, a watermark is embedded in the last M numbers. The $(L+1)$ th to $(L+M)$ th DCT coefficients are selected to generate a vector $T = \{t_i, 1 \leq i \leq M\}$.

The watermark is embedded into the vector T , to obtain a new vector $T' = \{t'_i, 1 \leq i \leq M\}$, according to the following rule:

$$t'_i = t_i + \alpha \cdot p_i \cdot s_i, \quad i=1, 2, \dots, M \quad (3)$$

where α denotes a magnitude factor which is a constant determining the signature strength. The value is selected to offer the best trade-off between robustness and unobtrusiveness.

The vector T' is then reinserted in the zig-zag scan and the inverse DCT is then performed to obtain the watermarked image I' .

2.2 Watermark Extracting

Figure 2 shows the block diagram of the watermark extracting process. The watermark extracting can be performed without knowledge of the original image. Instead, a prediction of the original value of the pixels is needed. The watermarked image may be considered to be the original image that is perturbed by the pseudo-random noise. Thus, a prediction of the original value of the pixels is to use noise-elimination technique. In this paper we used a smoothing technique.

The predicted image \hat{I} can be obtained by smoothing the input image I' with a spatial convolution mask. In this paper we use a 5×5 mask and all elements are equal to $1/25$. The prediction of the original value can be defined as:

$$\hat{i}_k = \frac{1}{c \times c} \sum_k^{c \times c} i_k^* \quad (4)$$

where c is the size of the convolution mask.

The watermarked image and the predicted image are DCT transformed independently. The $(L+1)$ th to $(L+M)$ th DCT coefficients, reordered in to a zig-zag scan, are selected to generate a vector T^* and \hat{T} respectively.

From (3), the estimate of the watermark \hat{S} is indicated by the difference between T^* and \hat{T} . The equation can be represented as:

$$\delta_i = t_i^* - \hat{t}_i = \alpha \cdot p_i \cdot \hat{s}_i \quad (5)$$

Therefore, the sign of the difference between the predicted and the actual value is the value of the embedded bit:

$$\text{sgn}(\delta_i) = p_i \cdot \hat{s}_i \quad (6)$$

The watermark can then be estimated by multiplying pseudo-random number to the embedded bit. If a wrong pseudo-random sequence is used, the scheme does not work. Finally, the watermark sequence is rearranged as two-dimension array to reproduce the signature image.

After extracting the embedded signature, a similarity measurement between the original signature S and the extracted signature \hat{S} can be evaluated by using the correlation value:

$$\text{CorrelationValue}(CV) = \frac{\sum_{i=1}^M S_i \hat{S}_i}{\sum_{i=1}^M S_i^2} \quad (7)$$

3. EXPERIMENTAL RESULTS

Figure 3 shows the original "Lena" 256-gray level image of size 512×512 and the signature image is the logo of King Mongkut's Institute of technology Ladkrabang (KMUTL) which is a binary image of size 128×128.

Figure 4 shows the watermarked image and the extracted watermark image with the following parameters: the amplitude factor is 30, the key is 500, $L = 20\%$ (52,429), $M = 128 \times 128$ (16,384), and the size of convolution mask is 5.



Fig. 3: The original image and the signature image.

The distortion due to watermark embedding is measured by the Peak Signal to Noise Ratio (PSNR). The PSNR of the resulted image is equal to 30.4534 dB. The CV values of the extracted signature image that compared with referenced signature image is equal to 0.9979.

To test and verify the robustness of our algorithm, many image-processing operations such as filtering and JPEG compression, were applied to the watermarked image in Figure 4 and the results of the extracting process are provided as follows.

3.1 Filtering

Smoothing filters are usually used for blurring and for noise reduction. The watermarks extracted after attacks by applying two popular filter types including neighborhood averaging filter and median filter, with a mask of size 3×3, are illustrated in Figure 5 and 6 respectively.

3.2 JPEG compression

Attack by JPEG compression is tested by varying the quality factor from 10% to 70%. The results of watermark extraction measured by the correlation value are provided in Table 1. Also, the watermarked images and the extracted watermarks where quality factor equals to 60% and 30% are shown in Figure 7 and 8 respectively.

Table 1: The CV values after JPEG compression with different quality factors.

Quality	70	50	20	10
CV	0.9955	0.9873	0.8506	0.5980

The results described above show that the proposed watermarking technique is robust to various kinds of attacks such as filtering and JPEG compression.



Fig. 4: Watermarked and extracted watermark images.

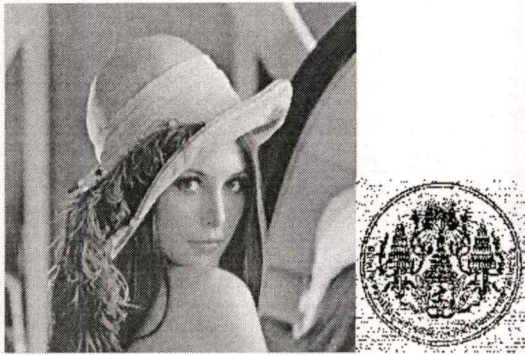


Fig. 5: Attack by 3x3 median filter.
(PSNR=33.4635 dB, CV=0.9254)

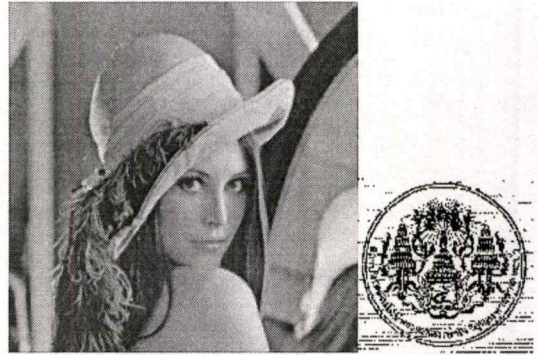


Fig. 6: Attack by 3x3 neighborhood averaging filter.
(PSNR=31.7948 dB, CV=0.9522)



Fig. 7: Attack by JPEG compression with 60%
quality factor. (PSNR=29.2579 dB, CV=0.9890)

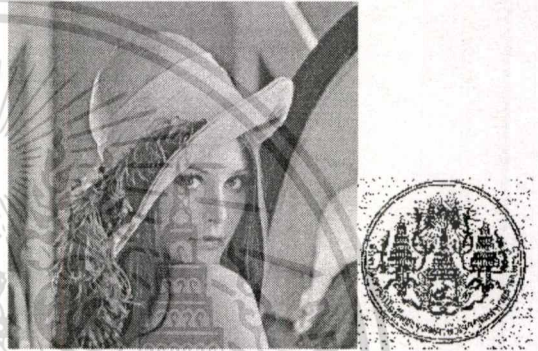


Fig. 8: Attack by JPEG compression with 30%
quality factor. (PSNR=29.1139 dB, CV=0.9473)

4. CONCLUSION

In this paper, we have presented a watermarking scheme for embedding a two-dimension binary watermark into a gray-level image. Our technique is applied to the frequency domain of the image resulted from two-dimension DCT. The watermark is embedded with a secret key into the low frequency and stored according to a zigzag format. The extraction of the watermark can be performed without knowledge of the original image, but the correct secret key is needed. Finally, since the transform domain algorithm to encode the watermark information is used, the information is robust enough against JPEG compression and ordinary image processing.

REFERENCES

- [1] I.J. Cox, J. Kilian, F.T. Leighton and T. Shanon: "Secure Spread Spectrum Watermarking for Multimedia," IEEE Trans. Image Proc., Vol. 6, No. 12, pp. 1673-1687, 1997.
- [2] W. Bender, D. Gruhl, N. Morimoto and A. Lu: "Techniques for Data Hiding," IBM Sys. J., Vol. 35, No. 3, pp.313-336, 1996.
- [3] N. Nikolaidis and I. Pitas: "Robust Image Watermarking in the Spatial Domain," Signal Processing, Vol. 66, pp. 385-403, 1998.
- [4] S.D. Lin and C.F. Chen: "A Robust DCT-Based Watermarking for Copyright Protection," IEEE Trans. Consumer Electronics, Vol. 46, No. 3, August 2000.

ประวัติผู้เขียน

นายยุทธพงศ์ จิตมัชฌิมา เกิดเมื่อวันที่ 16 กรกฎาคม 2522 ที่จังหวัดสงขลา สำเร็จการศึกษาระดับปริญญาตรี สาขาเทคโนโลยีการจัดการ จากสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปีการศึกษา 2543

ปี พ.ศ. 2544 - 2545 ทำงานในตำแหน่ง IS PROBLEM MANAGEMENT ANALYST บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)

ปี พ.ศ. 2546 - ปัจจุบัน ทำงานในตำแหน่ง PROGRAMMER ANALYST บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)



เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ตัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้