

# การแทรกกลายน้ำในภาพดิจิทัลสำหรับการป้องกันลิขสิทธิ์ของภาพ

## Digital Image Watermarking for Image Copyright Protection

สมหญิง โภคอุดม<sup>1</sup>

### บทคัดย่อ

การพัฒนาอย่างรวดเร็วของคอมพิวเตอร์และเครือข่ายในการติดต่อสื่อสาร ทำให้การรับส่งข้อมูลดิจิทัลผ่านเครือข่ายอินเทอร์เน็ตสามารถกระทำได้อย่างง่ายดาย แต่ด้วยธรรมชาติของอินเทอร์เน็ตที่เป็นระบบเปิด ข้อมูลข่าวสารที่ส่งผ่านอินเทอร์เน็ตจึงมีโอกาที่จะถูกคัดลอก ดัดแปลงแก้ไข หรือโจรกรรมได้โดยง่าย เมื่อปัญหานี้ทวีความรุนแรงมากขึ้น จึงเป็นเรื่องสำคัญที่จะต้องปกป้องทรัพย์สินทางปัญญาของสื่อดิจิทัล เพื่อรับมือกับปัญหาดังกล่าว การแทรกกลายน้ำในภาพดิจิทัลจึงได้ถูกนำเสนอเพื่อใช้ในการระบุผู้ที่เป็นเจ้าของภาพดิจิทัล หลักการของการแทรกกลายน้ำจะทำการฝังข้อมูลจากเจ้าของภาพลงไปในภาพดิจิทัลต้นฉบับโดยมีกลไกในการตรวจสอบความเป็นเจ้าของภาพที่สอดคล้องกันกับวิธีการฝัง ซึ่งจะต้องดำเนินการในลักษณะที่ข้อมูลที่ใส่เพิ่มเข้าไปในนั้นจะต้องไม่ไปลดคุณภาพด้านการมองเห็นของภาพดิจิทัลและต้องไม่สามารถถูกกำจัดออกไปได้

**คำสำคัญ :** การแทรกกลายน้ำในภาพดิจิทัล, การป้องกันลิขสิทธิ์

### Abstract

With the fast development of computer and communication networks, it has become increasingly easy to distribute and get digital data via internet. Because of its nature, the internet is an open system. Transmitted digital data is easily duplicated, altered, or even stolen. Since this problem has become more serious than before, it is importance to protect the intellectual property of digital media. To tackle the problem, digital image watermarking has been proposed as a means to identify the owner of digital image. The watermarking technique embeds authors' information into the original digital image and provides the corresponding authentication mechanism. This must be performed in such a way that the added information does not cause degradation of the perceptual quality and cannot be removed.

**Keywords :** digital image watermarking, copyright protection

<sup>1</sup>อาจารย์ประจำ สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยอีสเทิร์นเอเซีย

## ความนำ

มนุษย์เราสามารถส่งข่าวสารข้อมูลลับถึงกัน โดยที่บุคคลอื่นไม่สามารถล่วงรู้ได้ว่ามีสารลับซ่อนอยู่ในสื่อที่ถูกนำส่งมาได้ตั้งแต่สมัยกรีกโบราณ ศาสตร์ของการซ่อนข้อมูลเช่นนี้มีชื่อเรียกว่า Steganography โดยในสมัยกรีกโบราณมีบันทึกที่แสดงให้เห็นถึงวิธีการส่งสารเตือนภัยถึงการบุกรุกของศัตรู โดยชาวกรีกจะเขียนข้อความลับเพื่อเตือนภัยบนแผ่นไม้แล้วนำเทียนมาเคลือบข้อความไว้อีกชั้นหนึ่ง ซึ่งเมื่อศัตรูมองเห็นแผ่นไม้ก็ไม่สามารถล่วงรู้ถึงข้อความลับนั้นได้ นอกเสียจากจะมีการลอกเทียนที่เคลือบข้อความนั้นออกไป อีกหนึ่งวิธีที่ปรากฏเป็นหลักฐานคือการใช้หนังสัตว์ของคนที่เขียนข้อความลับ โดยก่อนเขียนข้อความจะทำการโกนผมบนศีรษะออก เมื่อเขียนเสร็จจะปล่อยให้ผมขึ้นเพื่อบดบังข้อความบนหนังศีรษะ จากนั้นจึงจะเดินทางไปหาผู้รับ โดยผู้รับก็จะทำการโกนผมบนหนังศีรษะของผู้นำมาส่งออกเพื่ออ่านข้อความลับ

อีกช่วงหนึ่งที่มีการใช้ Steganography ในการติดต่อสื่อสารมากที่สุด คือ ช่วงสงครามโลกครั้งที่สอง วิธีการที่นำมาใช้ได้แก่ การนำหนังสือพิมพ์รายวันมาใช้เป็นสื่อในการส่งผ่านข้อมูลข่าวสารความลับ โดยผู้รับสารจะต้องทราบวิธีในการแกะข้อความลับจากข่าวในหนังสือพิมพ์ที่ได้มีการตกลงกันไว้ก่อนแล้ว นอกจากนี้ยังมีการใช้น้ำมันมะนาวหรือน้ำมัน เขียนข้อความลับลงบนกระดาษซึ่งข้อความนี้ไม่สามารถมองเห็นได้ จนกว่าจะนำกระดาษนั้นไปอังไฟ เพื่อให้ความร้อนทำให้ข้อความที่เขียนมีสีเข้มขึ้น จนสามารถอ่านได้

มาถึงยุคปัจจุบันที่เทคโนโลยีและช่องทางการติดต่อสื่อสารได้พัฒนาอย่างต่อเนื่อง ข้อมูลข่าวสารได้รับการพัฒนาให้อยู่ในรูปแบบดิจิทัลเพื่อให้สนองตอบต่อ

การใช้งานผ่านเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารสมัยใหม่ ช่องทางหนึ่งที่คนทั่วโลกนิยมใช้เป็นช่องทางการส่งข้อมูลข่าวสารถึงกัน คือ อินเทอร์เน็ต ปัจจุบันเราสามารถใช้อินเทอร์เน็ตส่งข้อมูลข่าวสารถึงกันได้อย่างง่ายดายและรวดเร็วแม้จะอยู่คนละซีกโลก นอกเหนือจากความรวดเร็ว สะดวกสบาย ในการส่งข้อมูลข่าวสารผ่านอินเทอร์เน็ต ในทางกลับกันการที่อินเทอร์เน็ตเป็นระบบเปิดที่มีผู้ใช้งานเป็นจำนวนมาก ข้อมูลข่าวสารที่ส่งและเผยแพร่ผ่านอินเทอร์เน็ตจึงมีโอกาสนในการเข้าถึงโดยบุคคลทั่วไป และถูกคัดลอก ดัดแปลงแก้ไข หรือถูกนำไปใช้โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของได้โดยง่าย หลายๆ หน่วยงานที่เกี่ยวข้องจึงได้พยายามคิดค้นวิธีป้องกันไม่ให้เกิดปัญหาดังกล่าวขึ้น วิธีการหนึ่งก็คือการใช้ตัวบทกฎหมาย แต่ก็สามารถแก้ปัญหาได้ในระดับหนึ่งเท่านั้น เนื่องจากยังมีช่องโหว่สำคัญหลายประการที่เอื้อต่อการกระทำผิดกฎหมายอย่างมาก จึงมีความจำเป็นอย่างยิ่งที่จะต้องพัฒนาวิธีการอื่นๆ เพื่อใช้ในการป้องกันและแก้ไขปัญหา

Digital Image watermarking หรือ การแทรกลายน้ำในภาพดิจิทัล จัดเป็นรูปแบบหนึ่งของ Steganography เพื่อใช้ในการพิสูจน์หรือแสดงความเป็นเจ้าของภาพถ่าย โดยการซ่อนข้อมูลลับที่เรียกว่าสัญญาณลายน้ำเข้าไปในตัวภาพถ่ายดิจิทัลก่อนที่จะทำการเผยแพร่ภาพถ่ายดังกล่าวออกไป ลายน้ำนี้สามารถทำการเปลี่ยนแปลงแก้ไขหรือกู้คืนได้โดยผู้ที่เป็นเจ้าของหรือผู้ที่ได้รับอนุญาตเท่านั้น ภาพ 1 แสดงภาพต้นไม้ที่มีการอำพรางภาพแมวไว้ในภาพ ภาพแมวปรากฏโดยการนำบิตอื่นๆ ของ RGB ออกไปยกเว้น 2 บิตสุดท้ายของแต่ละสี ภาพที่ได้จะเป็นโทนสีเกือบดำ แล้วเพิ่มความสว่าง 85 เท่า จึงจะปรากฏเป็นภาพแมวดังภาพ 2 (เฉลิมศักดิ์ เลิศวงศ์เสถียร, 2547)



ภาพ 1 ภาพต้นไม้ที่มีการอำพรางข้อมูล  
ที่มา. จาก “Steganography ศาสตร์แห่งการซ่อนข้อมูล,”  
2547 โดย เจลิมศักดิ์ เลิศวงศ์เสถียร, ค้นจาก [http://  
th.wikipedia.org](http://th.wikipedia.org).



ภาพ 2 ภาพแมวที่ถูกอำพรางข้อมูล  
ที่มา. จาก “Steganography ศาสตร์แห่งการซ่อนข้อมูล,”  
2547 โดย เจลิมศักดิ์ เลิศวงศ์เสถียร, ค้นจาก [http://  
th.wikipedia.org](http://th.wikipedia.org).

### ประเภทของลายน้ำดิจิทัล

โดยทั่วไปเราสามารถแบ่งประเภทของลายน้ำ  
ดิจิทัลตามการปรากฏของลายน้ำออกเป็น 2 ประเภท คือ

#### 1. ลายน้ำที่เปิดเผย

ลายน้ำที่เปิดเผย (visible watermark) ทำโดย  
การเขียน เติม หรือแทรกตัวข้อมูลลายน้ำที่ต้องการลงไป

ในตัวภาพถ่ายโดยตรง ประโยชน์ที่เห็นได้ชัดของวิธีนี้ก็คือนัก  
บุคคลทั่วไปที่พบเห็นภาพลายน้ำชนิดนี้ จะรู้ได้ทันทีว่า  
ภาพดังกล่าวมีเจ้าของ



ภาพ 3 การแทรกลายน้ำที่เปิดเผยบริเวณมุมบนซ้าย  
ของภาพ  
ที่มา. จาก “เทคนิคการทำภาพลายน้ำ (Watermark)  
แบบง่าย ๆ,” 2009 โดย Jaratsri Chansirimas, ค้นจาก  
[www.ReadyPlanet.com](http://www.ReadyPlanet.com).

การสร้างภาพลายน้ำชนิดนี้สามารถดำเนินการได้  
โดยง่าย ในปัจจุบันมีโปรแกรมหลายโปรแกรมที่มีความ  
สามารถในการทำภาพลายน้ำที่เปิดเผย อาทิ โปรแกรม  
ACDsee โปรแกรม Adobe Photoshop ลายน้ำชนิดนี้  
มีข้อเสียอยู่ตรงที่ลายน้ำที่ใส่เข้าไปจะไปบังภาพ ทำให้  
รายละเอียดบนภาพขาดหายไป โดยเฉพาะเมื่อแทรกลายน้ำ  
ลงไปในพื้นที่สำคัญของภาพ แต่การแทรกลายน้ำ  
ลงไปในส่วนสำคัญของภาพมีข้อดีตรงที่ทำให้ไม่สามารถ  
เคลื่อนย้ายหรือกำจัดลายน้ำออกได้โดยง่าย ในทางกลับกัน  
ถ้าเจ้าของภาพแทรกลายน้ำในส่วนที่ไม่สำคัญ เนื่องจาก  
ไม่ยากให้ลายน้ำไปบังส่วนสำคัญของภาพ เช่น ใส่ใน  
ตำแหน่งมุมภาพบริเวณฉากหลังของภาพ ก็จะทำให้  
การกำจัดลายน้ำออกจากภาพสามารถกระทำได้ง่าย  
ภาพ 3 แสดงการแทรกลายน้ำที่เปิดเผยบริเวณมุมบนซ้าย  
ของภาพ (Chansirimas, 2009)

## 2. ลายน้ำที่ไม่เปิดเผย

ลายน้ำที่ไม่เปิดเผย (invisible watermark) สร้างขึ้นโดยการแทรกลายน้ำดิจิทัลลงไปในภาพต้นฉบับ ภายใต้คุณสมบัติที่ต้องคำนึงถึง 2 ประการ คือ

### 1) ความคงทน

ความคงทน (robustness) หมายถึง ลายน้ำที่ใส่เข้าไปต้องยากต่อการถูกกำจัดหรือทำลาย และต้องมีความคงทนต่อการถูกโจมตีหรือถูกดัดแปลงแก้ไข ทั้งนี้รวมไปถึงการบีบอัดข้อมูลเพื่อให้ไฟล์ภาพมีขนาดเล็กลง และถึงแม้ว่าจะถูกกระทำจนส่งผลให้ลายน้ำบางส่วนสูญหายไปแต่ลายน้ำส่วนที่คงอยู่จะต้องมีมากและชัดเจนพอที่จะยืนยันถึงความเป็นเจ้าของที่แน่นอนได้

### 2) ความสามารถด้านการมองเห็น

ความสามารถด้านการมองเห็น (imperceptibility) หมายถึง ลายน้ำที่ใส่เข้าไปต้องไม่ไปลดคุณภาพของภาพที่ถูกแทรกลายน้ำ กล่าวคือ เมื่อนำภาพภายหลังการแทรกลายน้ำมาเปรียบเทียบกับภาพก่อนแทรกลายน้ำ ต้องไม่สามารถสังเกตเห็นความแตกต่างระหว่างกันได้

คุณสมบัติทั้ง 2 ประการต่างมีความสัมพันธ์ผกผันระหว่างกัน กล่าวคือ ยิ่งต้องการแทรกลายน้ำให้มีความคงทนและมีความปลอดภัยมาก ก็จะทำให้คุณภาพด้านการมองเห็นของภาพที่แทรกลายน้ำลดลง ด้วยเหตุนี้จึงมีนักวิจัยจำนวนมากที่พยายามคิดค้นเทคนิคและวิธีการใหม่ๆ ในการแทรกลายน้ำชนิดที่ไม่เปิดเผยจนปรากฏเป็นผลงานวิจัยในที่ประชุมวิชาการและวารสารวิชาการอย่างต่อเนื่อง ภาพ 4 แสดงภาพต้นฉบับก่อนการแทรกลายน้ำ ภาพ 5 แสดงภาพลายน้ำ และภาพ 6 แสดงภาพที่ผ่านการแทรกลายน้ำที่ไม่เปิดเผย (Promcharoen and Rangsanteri, 2010, pp. 1189-1194)

## ประเภทของการแทรกลายน้ำที่ไม่เปิดเผย

เทคนิคและวิธีการแทรกลายน้ำที่ไม่เปิดเผยมีอยู่ด้วยกันหลากหลายวิธี แต่เราสามารถจำแนกออกได้เป็น 2 ประเภทใหญ่ๆ คือ

## 1. การแทรกลายน้ำในโดเมนสเปเชียล

การแทรกลายน้ำในโดเมนสเปเชียล (spatial domain) เป็นการแทรกลายน้ำที่ค่าพิกเซลของภาพถ่ายจะถูกดัดแปลงแก้ไขโดยตรงตามข้อมูลลายน้ำที่ใส่เข้าไป ข้อมูลลายน้ำที่ใส่ด้วยวิธีนี้จะคงทนต่อการโจมตีเชิงเรขาคณิต เช่น การหมุนภาพ การตัดภาพแต่จะไม่คงทนต่อการโจมตีเชิงสัญญาณ เช่น การกรองสัญญาณความถี่สูง การกรองสัญญาณความถี่ต่ำ และไม่คงทนต่อการบีบอัดข้อมูลภาพ ซึ่งถือเป็นจุดบอดที่สำคัญ เนื่องจากเป็น ที่ทราบกันดีว่าการบีบอัดข้อมูลภาพเป็นกระบวนการที่ได้รับความนิยมมากที่สุดในการนำมาใช้เพื่อลดขนาดของข้อมูลภาพที่ต้องการเผยแพร่บนอินเทอร์เน็ต



ภาพ 4 ภาพต้นฉบับก่อนการแทรกลายน้ำ



ภาพ 5 ภาพลายน้ำ



ภาพ 6 ภาพที่ผ่านการแทรกลายน้ำที่ไม่เปิดเผย

## 2. การแทรกลายน้ำในโดเมนความถี่

การแทรกลายน้ำในโดเมนความถี่ (frequency domain) เป็นวิธีการที่ค่าพิกเซลของภาพจะต้องถูกแปลงด้วยสมการการแปลงทางคณิตศาสตร์ เช่น DCT (Discrete Cosine Transform) DWT (Discrete Wavelet Transform) DMT (Discrete Multi-wavelet Transform) ให้เป็นค่าสัมประสิทธิ์ต่างๆ ก่อนที่จะทำการแทรกลายน้ำลงไป โดยภายหลังการแทรกลายน้ำจะต้องทำการแปลงกลับจึงจะได้ภาพที่ผ่านการแทรกลายน้ำออกมา วิธีการนี้ผ่านการพิสูจน์ในงานวิจัยหลายชิ้นว่าให้ลายน้ำที่มีความคงทนต่อการโจมตีเชิงสัญญาณ เช่น การกรองสัญญาณความถี่สูง การกรองสัญญาณความถี่ต่ำ และคงทนต่อการบีบอัดข้อมูลภาพมากกว่าวิธีการแทรกลายน้ำบนโดเมนสเปเชียล (Hartung, 1999, pp. 1079-1107), (Petitcolas, 1999, pp. 1062-1078), (Song and Tan, 2000, pp. 946-950)

## ขั้นตอนการทำภาพลายน้ำที่ไม่เปิดเผย

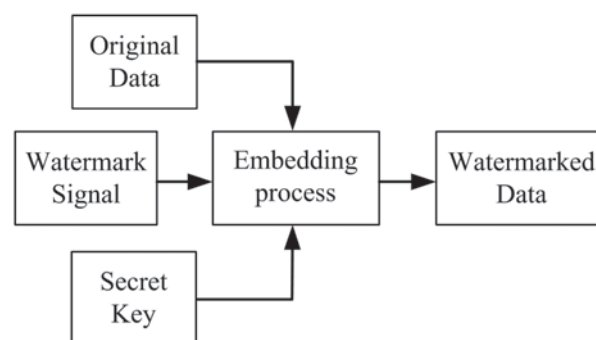
การทำภาพลายน้ำที่ไม่เปิดเผยไม่ว่าจะเป็นวิธีที่ทำบนโดเมนสเปเชียลหรือบนโดเมนความถี่ล้วนประกอบ

ไปด้วยขั้นตอนต่างๆ ไป ที่เหมือนกัน 2 ขั้นตอน คือ การแทรกลายน้ำ (watermark embedding) และการกู้คืนลายน้ำ (watermark detection)

### 1. การแทรกลายน้ำ

การแทรกลายน้ำ (watermark embedding) ข้อมูลภาพจะผ่านกระบวนการใส่สัญญาณลายน้ำ โดยอาจมีการเข้ารหัสสัญญาณลายน้ำที่ใส่เข้าไปซึ่งจะมีกุญแจลับ (secret key) ที่ใช้ในการเข้ารหัส โดยมีเพียงผู้ที่ถือกุญแจลับนี้เท่านั้นที่สามารถเปลี่ยนแปลงแก้ไขสัญญาณลายน้ำดังกล่าวได้ (Cox, Kilian, Leighton, and Shamoon, 1997, pp. 1673-1687)

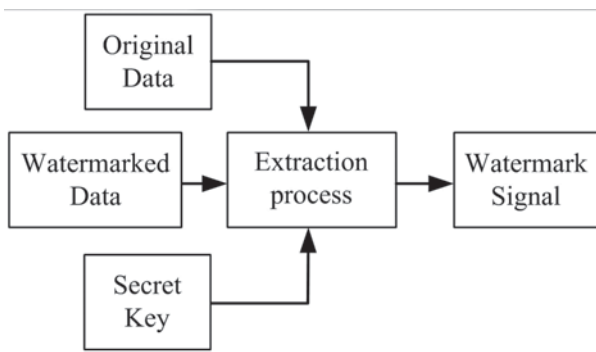
ข้อมูลเข้าของขั้นตอนการแทรกลายน้ำดิจิทัลประกอบไปด้วย ข้อมูลหรือภาพต้นฉบับ (original data) สัญญาณลายน้ำ (watermark signal) และรหัสลับ (secret Key) ส่วนข้อมูลออกที่ได้ คือ ข้อมูลหรือภาพดิจิทัลที่ผ่านการแทรกลายน้ำ (watermarked data) กระบวนการแทรกลายน้ำ แสดงดังภาพ 7



ภาพ 7 กระบวนการแทรกลายน้ำ

### 2. การกู้คืนลายน้ำ

การกู้คืนลายน้ำ (watermark extraction) สามารถจำแนกออกเป็น 2 วิธี คือ วิธีที่ต้องใช้ภาพต้นฉบับในการกู้คืนลายน้ำ (blind method) และวิธีที่ไม่ต้องใช้ข้อมูลภาพต้นฉบับในการกู้คืนลายน้ำ (non-blind method) (Lee, and Jung, 2001, pp. 272-277)



ภาพ 8 กระบวนการกู้คืนลายน้ำที่ใช้ภาพต้นฉบับในการกู้คืน

ข้อมูลเข้าของขั้นตอนการกู้คืนลายน้ำประกอบไปด้วย ภาพดิจิทัลที่ผ่านการแทรกลายน้ำ (watermarked data) ข้อมูลหรือภาพต้นฉบับ (original data) และรหัสลับ (secret key) ส่วนข้อมูลออกที่ได้ คือ สัญญาณลายน้ำ (watermark signal) ภาพ 8 แสดงกระบวนการกู้คืนลายน้ำที่ต้องใช้ภาพต้นฉบับในการกู้คืนลายน้ำ

### การวัดคุณภาพด้านการมองเห็น

การวัดคุณภาพด้านการมองเห็นของภาพที่ผ่านการแทรกลายน้ำ เป็นการตรวจสอบความเหมือนกันระหว่างภาพดิจิทัลต้นฉบับและภาพที่ถูกแทรกลายน้ำ โดยมีวิธีการวัดหรือดัชนีที่นิยมใช้วัดคุณภาพด้านการมองเห็นของภาพที่ผ่านการแทรกลายน้ำ ดังนี้

#### 1. การวัดด้วยสายตา

การวัดคุณภาพด้านการมองเห็นของภาพที่ผ่านการแทรกลายน้ำ โดยใช้สายตาของผู้ที่ไม่เกี่ยวข้องมาทำการตัดสินคุณภาพของภาพภายหลังจากการแทรกลายน้ำจัดเป็นวิธีการพื้นฐานแต่ให้ผลที่น่าเชื่อถือ นอกจากการใช้สายตาของผู้ใช้ธรรมดาเป็นผู้วัดแล้วยังอาจใช้สายตาของผู้เชี่ยวชาญที่มีความสามารถในการสังเกตข้อบกพร่องเล็กๆ น้อยๆ ที่บุคคลทั่วไปอาจมองข้าม วิธีการวัดอาจใช้เกณฑ์ต่างๆ เช่น ให้ผู้ทดสอบมองภาพแล้วระบุระดับคุณภาพ โดยอาจมีชุดภาพมาตรฐานที่มีระดับคะแนนระบุไว้เพื่ออ้างอิง ระดับคุณภาพสามารถแสดงได้ทั้งระดับความเหมือนและระดับความแตกต่าง

อีกวิธีหนึ่งคือการใช้ผู้ทดสอบเรียงลำดับคุณภาพของภาพ โดยให้เรียงลำดับภาพทดสอบตามคุณภาพของภาพที่เห็น ผู้ทดสอบจะตัดสินใจในลักษณะเปรียบเทียบว่าดีกว่าหรือแย่กว่า

#### 2. การวัดด้วยค่า PSNR

ค่า PSNR (Peak Signal-to-Noise Ratio) เป็นค่ามาตรฐานที่นักวิจัยนิยมนำมาใช้วัดคุณภาพด้านการมองเห็นของภาพมากที่สุด ค่า PSNR ที่มีค่ามากจะแสดงถึงคุณภาพของภาพที่แทรกลายน้ำว่ามีความเหมือนกับภาพต้นฉบับมาก โดยทั่วไปแล้วค่า PSNR ที่ยอมรับได้สำหรับการนำภาพไปใช้ออยู่ที่ 30 dB ขึ้นไป (Chen, Chang, and Hwang, 1998, p. 1485-1488) ซึ่งค่า PSNR สามารถคำนวณได้ดังนี้

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

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

โดยที่

$M$  คือ จำนวนพิกเซลตามความกว้างของภาพ

$N$  คือ จำนวนพิกเซลตามความสูงของภาพ

$f(x, y)$  คือ ค่าพิกเซลที่ตำแหน่ง  $W_{ij}$  ของภาพต้นฉบับ

$\bar{f}(x, y)$  คือ ค่าพิกเซลที่ตำแหน่ง  $W_{ij}$  ของภาพที่ผ่านการแทรกลายน้ำ

Peak คือ ค่าสูงสุดของขอบเขตค่าพิกเซลของภาพ

สำหรับภาพที่มีขนาด  $n$  บิต ที่มีจำนวนระดับสีเทา (Gray Scale) เท่ากับ  $2^n$  ระดับ จะได้ว่า

$$PSNR = 10 \log \frac{(2^n - 1)^2}{MSE} \quad (dB) \quad (3)$$

ดังนั้นภาพขนาด 8 บิต จะได้ว่า

$$PSNR = 10 \log \frac{255^2}{MSE} \quad (dB) \quad (4)$$

### 3. การวัดด้วยค่า UQI

UQI (Universal Quality Index) เป็นดัชนีที่ใช้วัดคุณภาพการมองเห็นของภาพที่นำเสนอในปี 2002 (Wang and Bovik, 2002, pp. 81-84) โดย Wang และ Bovik ได้แสดงให้เห็นว่ามีหลายกรณีที่ PSNR ไม่สามารถแยกแยะความแตกต่างระหว่าง 2 ภาพได้ แต่ UQI สามารถทำได้

สมการของ UQI เป็นดังสมการที่ (5) และ (6) สมการที่ (6) จะประกอบไปด้วย 3 เทอม โดยเทอมแรกแสดงการสูญเสียความสัมพันธ์ระหว่างค่าพิกเซลของภาพทั้ง 2 ภาพ (loss of correlation) เทอมที่สองแสดงการบิดเบือนของแสงเงา (luminance distortion) และเทอมสุดท้ายแสดงการบิดเบือนความแตกต่างระหว่างความสว่างและความมืด (contrast distortion) ทั้งนี้ค่า UQI ที่คำนวณได้จะมีค่าอยู่ในช่วง  $[1, -1]$  โดยค่าที่ดีที่สุดคือ 1

$$UQI = \frac{1}{M} \sum_{j=1}^M Q_j \quad (5)$$

$$Q = \frac{\sigma_{xy}}{\sigma_x \sigma_y} \cdot \frac{2\bar{x}\bar{y}}{(\bar{x})^2 + (\bar{y})^2} \cdot \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2} \quad (6)$$

เมื่อ

$y = \{y_i | i=1, 2, \dots, 64\}$  เป็นค่าพิกเซลในกรอบขนาด  $8 \times 8$  ของภาพต้นฉบับ

$y = \{y_i | i=1, 2, \dots, 64\}$  เป็นค่าพิกเซลในกรอบขนาด  $8 \times 8$  ของภาพที่แทรกกลายน้ำ

$M$  คือ จำนวนครั้งของการเลื่อนกรอบขนาด  $8 \times 8$  โดยเลื่อนครั้งละ 1 พิกเซล จากด้านขวาไปซ้ายและจากบนลงล่างจนครบทั้งภาพ

### การโจมตีกลายน้ำ

การโจมตีกลายน้ำ คือ การทำให้ข้อมูลลายน้ำซึ่งถูกฝังในภาพเกิดความเสียหาย โดยอาจเป็นการกระทำโดยตั้งใจหรือไม่ได้ตั้งใจ รวมไปถึงการประมวลผลสัญญาณภาพซึ่งทำให้ข้อมูลลายน้ำสูญหายไปบางส่วน การโจมตีลายน้ำที่พบเห็นได้บ่อย มีอยู่ด้วยกัน 3 รูปแบบใหญ่ๆ ดังนี้

#### 1. การบีบอัดแบบ JPEG

อัลกอริทึม JPEG จะทำการกำจัดส่วนที่มองเห็นได้ที่ไม่สัมพันธ์ในภาพเพื่อลดขนาดของไฟล์ภาพให้เล็กลง จัดเป็นอัลกอริทึมการบีบอัดที่นิยมใช้กับภาพมากที่สุด นิยมนำมาใช้ในการส่งข้อมูลภาพบนอินเทอร์เน็ต การโจมตีนี้จึงเป็นตัวอย่างทดสอบที่ดีในการทดสอบความคงทนของลายน้ำ ลายน้ำควรจะยืดหยุ่นกับระดับการบีบอัดซึ่งระดับการบีบอัดจะถูกควบคุมโดยแฟกเตอร์คุณภาพ เช่น 100, 90, 80, 70, ..., 10% ยิ่งแฟกเตอร์คุณภาพน้อยขนาดของไฟล์ภาพก็จะน้อยลงตามไป ส่งผลให้ลายน้ำมีโอกาสถูกทำลายมากขึ้น ภาพ 9 แสดงภาพที่ได้จากการโจมตีภาพที่ผ่านการแทรกกลายน้ำลงในภาพ 6 ด้วยการบีบอัดข้อมูลตามมาตรฐาน JPEG ที่แฟกเตอร์คุณภาพ 50% และภาพ 10 แสดงลายน้ำที่กู้คืนจากภาพดังกล่าว (Promcharoen, and Rangsanteri, 2010, p. 1189-1194)

#### 2. การโจมตีเชิงเรขาคณิต

การโจมตีเชิงเรขาคณิต เป็นการโจมตีภาพที่มุ่งไปที่การเปลี่ยนลักษณะของภาพ ได้แก่

##### 1) การลด/เพิ่มขนาดของภาพ (resizing)

การลด/เพิ่มขนาดภาพ เป็นการลดหรือเพิ่มจำนวนพิกเซล ซึ่งส่งผลกระทบต่ออัลกอริทึมการแทรกกลายน้ำในตำแหน่งที่ตายตัว ทำให้ตำแหน่งที่เคอร์เนลไวด์คลาดเคลื่อนจนไม่สามารถตรวจหาลายน้ำได้



ภาพ 9 ภาพที่ผ่านการแทรกกลายน้ำลงในภาพ 6 ที่ถูก  
โคมตีด้วยการบีบอัดข้อมูลตามมาตรฐาน JPEG ที่แฟกเตอร์  
คุณภาพ 50%



ภาพ 10 ลายน้ำที่กู้คืนจากภาพ 9

## 2) การตัดบางส่วนของภาพ (cropping)

การตัดบางส่วนของภาพ จะส่งผลโดยตรงกับ  
อัลกอริทึมการแทรกกลายน้ำที่มีการกระจายลายน้ำใส่ลงไป  
ทั่วทั้งภาพ การตัดบางส่วนของภาพออกไปจะทำให้ลายน้ำ  
บางส่วนขาดหายไปด้วย

## 3) การเคลื่อนย้ายภาพ (translation)

ถ้าหากมีการเคลื่อนย้ายบางส่วนของภาพไปไว้  
ยังตำแหน่งอื่น การใช้อัลกอริทึมการแทรกกลายน้ำลง  
ในตำแหน่งที่ตายตัวเมื่อถูกโคมตีจะส่งผลให้ลายน้ำที่  
ตรวจหามาได้วางสลับตำแหน่ง

## 4) การหมุนภาพ (rotation)

การหมุนภาพส่งผลกระทบต่อการแทรกกลายน้ำ  
คล้ายกับการบิด/เพิ่มขนาดของภาพ

## 5) การกลับด้านของภาพ (flipping)

การสลับด้านซ้ายขวาของภาพ จะมีผลกระทบกับ

อัลกอริทึมที่แทรกกลายน้ำลงในตำแหน่งที่ตายตัว เช่นเดียว  
กับการเคลื่อนย้ายภาพ

## 3. การโคมตีเชิงสัญญาณ

การโคมตีเชิงสัญญาณมีหลายประเภท ได้แก่

1) การปรับความสว่างและความแตกต่างระหว่าง  
ความสว่างและความมืดของภาพ (brightness and  
contrast enhancement)

โดยทั่วไปแล้วการประมวลผลสัญญาณประเภทนี้  
ไม่ส่งผลกระทบต่อมากต่อการตรวจหาลายน้ำ ในทางตรง  
กลับกันมักนิยมนำมาใช้ก่อนการตรวจหาลายน้ำเพื่อให้  
ภาพที่ต้องการตรวจหาลายน้ำมีความสว่างและความ  
แตกต่างระหว่างความสว่างและความมืดของภาพใกล้เคียง  
กับภาพต้นฉบับ เพื่อให้ได้ผลลัพธ์ในการตรวจหาลายน้ำ  
ที่ดีกว่า

2) การปรับความคมชัด การทำให้เลือน การกรอง  
แบบเชิงเส้นและแบบไม่เป็นเชิงเส้น (sharpening,  
blurring, linear and non linear filtering)

การประมวลผลประเภทนี้ เมื่อกระทำแล้วจะไป  
ลดคุณภาพด้านการมองเห็นของภาพไปอย่างมาก และเมื่อ  
กระทำซ้ำๆ อาจส่งผลให้ลายน้ำที่ใส่มีค่าเปลี่ยนแปลงไป  
ทำให้ลายน้ำที่กู้คืนมามีความผิดพลาด

3) การเพิ่มสัญญาณรบกวนแบบคอรีเลทและ  
แบบไม่เป็นคอรีเลท (addition of correlated or  
uncorrelated noise)

เป็นการเพิ่มสัญญาณรบกวนเข้าไปในภาพซึ่ง  
ส่งผลต่อลายน้ำและภาพคล้ายคลึงกับที่ส่งผลต่อการ  
ปรับความคมชัด การทำให้เลือน การกรองแบบเชิงเส้น  
และแบบไม่เป็นเชิงเส้น

4) การแปลงสัญญาณจากอนาลอกเป็นดิจิทัลและ  
จากดิจิทัลเป็นอนาลอก เช่น การพิมพ์ภาพ การสแกนภาพ  
เป็นการแปลงสัญญาณระหว่างดิจิทัลและอนาล็อก ซึ่งแม้  
จะทำการแปลงกลับค่าพิกเซลของภาพก็จะต้องผิดเพี้ยนไป  
และส่งผลกระทบไปถึงลายน้ำที่ซ่อนอยู่ในภาพ

## การวัดคุณภาพด้านความคงทนของลายน้ำ

การวัดคุณภาพด้านความคงทนของลายน้ำที่คุ้นมาภายหลังจากการถูกโจมตีด้วยรูปแบบต่างๆ จะวัดจากค่า Normalized Cross Correlation: NC โดยค่า NC ที่คำนวณได้จะมีค่าอยู่ในช่วง [0, 1] และค่าที่แสดงถึงคุณภาพความคงทนของลายน้ำมากที่สุดคือ 1 การคำนวณค่า NC แสดงดังสมการที่ (7)

$$NC = \frac{\left( \sum_{i=1}^{M_W} \sum_{j=1}^{N_W} [W_{(i,j)} \cdot W'_{(i,j)}] \right)}{\left( \sum_{i=1}^{M_W} \sum_{j=1}^{N_W} [W_{(i,j)}]^2 \right)} \quad (7)$$

เมื่อ

$W_{ij}$  คือ ค่าพิกเซลที่ตำแหน่ง (i, j) ของลายน้ำต้นฉบับ

$W'_{ij}$  คือ ค่าพิกเซลที่ตำแหน่ง (i, j) ของลายน้ำที่คุ้นมาได้

$N_W$  คือ จำนวนพิกเซลตามความกว้างของลายน้ำ

$M_W$  คือ จำนวนพิกเซลตามความสูงของลายน้ำ

## การใช้งานลายน้ำดิจิทัล

ตัวอย่างของการใช้งานลายน้ำดิจิทัล

1. การแทรกลายน้ำที่เปิดเผยเพื่อแสดงความเป็นเจ้าของผลงาน
2. การแทรกลายน้ำที่ไม่เปิดเผยเพื่อใช้เป็นหลักฐานในการพิสูจน์ความเป็นเจ้าของผลงาน
3. การใช้ลายน้ำในการระบุบุคคลที่ได้รับสิทธิ์ถูกต้อง เพื่อใช้ตรวจหาผู้ที่เผยแพร่งานโดยไม่ได้รับอนุญาต
4. การติดตามการใช้ผลงาน การปรับปรุงผลงาน หรือการคัดลอกผลงาน
5. การแทรกลายน้ำในลายมือชื่อ เพื่อใช้ตรวจสอบลายมือชื่อปลอม
6. การใช้ลายน้ำเพื่อบอกให้อุปกรณ์บันทึกสัญญาณทราบว่าไม่สามารถบันทึกหรือทำการคัดลอกได้

## งานวิจัยด้านการแทรกลายน้ำดิจิทัล

ปัจจุบันมีนักวิจัยทั่วโลกให้ความสนใจในการพัฒนาวิธีการเทคโนโลยีทางด้านการทำภาพพิมพ์ลายน้ำดิจิทัล ปรากฏเป็นผลงานวิจัยจำนวนมากที่ตีพิมพ์เผยแพร่ในวารสารวิชาการและการประชุมวิชาการ ในที่นี้ขอยกตัวอย่างมาพอสังเขป

1. Cox และคณะ (Cox, Kilian, Leighton and Shamoon, 1997, p. 1673-1687) ได้นำเสนอเทคนิคของการแทรกลายน้ำดิจิทัลแบบการกระจายแถบความถี่ (Spread Spectrum Communication) ลงในค่าสัมประสิทธิ์ของโดเมนความถี่ที่ได้จากการแปลงแบบดิสครีต (Discrete Cosine Transform : DCT) จากการวิจัยพวกเขาพบว่าลายน้ำจะมีความคงทนถ้าทำการแทรกลายน้ำลงในค่าสัมประสิทธิ์ส่วนที่เป็นความถี่ต่ำ

2. Dugad และคณะ (Dugad, Ratakonda, , and Ahuja, 1998, p. 419-423) นำเสนอเทคนิคการทำลายน้ำแบบกระจายแถบความถี่โดยอาศัยการแปลงเวฟเลต (Discrete Wavelet Transform : DWT) ที่แทรกลายน้ำเข้ากับค่าสัมประสิทธิ์ที่มีค่าสูงในสับแบนด์ความถี่สูงเพื่อรักษาคุณภาพด้านการมองเห็นของภาพที่ผ่านการแทรกลายน้ำ แต่เทคนิคดังกล่าวก็ไม่คงทนต่อการที่ภาพจะถูกดัดแปลงแก้ไข

3. Huang และ Wu (Huang, and Wu, 2000, p. 516-523) ได้นำเสนอวิธีการแทรกลายน้ำในภาพดิจิทัลที่อาศัยหลักการแปลงแบบดิสครีตโคไซน์ (Discrete Cosine Transform--DCT) ร่วมกับกระบวนการทางพันธุศาสตร์ (genetic algorithm-- GA) พวกเขาทำการแทรกลายน้ำเข้ากับค่าสัมประสิทธิ์ DCT ส่วนที่เป็นความถี่กลาง และนำ GA มาค้นหาค่าตำแหน่งที่เหมาะสมในการแทรกลายน้ำจนได้ภาพภายหลังการแทรกลายน้ำที่มีคุณภาพ

4. Shieh และคณะ (Shieh, Huang, Wang, and Pan, 2004, pp. 555-565) ได้นำเสนอเทคนิคในการแทรกลายน้ำที่ใช้ GA มาช่วยในการค้นหาค่าตำแหน่ง

ที่เหมาะสมที่สุดในการแทรกกลายน้ำเข้ากับค่าสัมประสิทธิ์ของบล็อก DCT ขนาด 8x8 พิกเซล ซึ่งช่วยเพิ่มประสิทธิภาพทั้งในด้านความคงทนของลายน้ำและด้านคุณภาพการมองเห็นของภาพภายหลังการแทรกกลายน้ำได้ในคราวเดียวกัน

5. Areef และ Heniedy (Areef, and Heniedy, 2005, p. 607-617) ได้นำเทคนิคของ Shieh และคณะมาใช้ร่วมกับการแปลงแบบเวฟเลต (Discrete Wavelet Transform : DWT) โดยการนำ GA มาช่วยในการค้นหาค่าที่เหมาะสมที่สุดในการแทรกกลายน้ำเข้ากับค่าสัมประสิทธิ์เวฟเลต โดยทดสอบความคงทนของลายน้ำด้วยการบีบอัดภาพตามมาตรฐาน JPEG

6. Wei และคณะ (Wei, Dai, and Li, 2006, p. 2365-2368) ได้ปรับปรุงสมการในการใส่และกู้คืนลายน้ำของ Shieh และคณะ ให้สั้นกระชับขึ้น และนำเสนอสมการในการกำหนดพารามิเตอร์ของ GA อันได้แก่ค่าความน่าจะเป็นในการครอสโอเวอร์และค่าความน่าจะเป็นในการมิวเตชันให้สามารถเปลี่ยนแปลงค่าไปตามจำนวนรอบในการประมวลผลของ GA และสรุปให้เห็นว่าวิธีการที่ปรับปรุงขึ้นนี้ให้ผลลัพธ์ที่ดีกว่าทั้งในด้านความคงทนของลายน้ำและด้านคุณภาพการมองเห็นของภาพภายหลังการแทรกกลายน้ำ

7. Xiang และ Jianjun (Xiang, and Jianjun,

2009, pp. 2221-2224) นำเสนอวิธีการแทรกกลายน้ำ โดยใช้การแปลงแบบเวฟเลตในการฝังลายน้ำลงบนภาพถ่ายทางภูมิศาสตร์ (DEM Images) ที่ไม่ต้องใช้ภาพต้นฉบับในการกู้คืนลายน้ำ โดยใช้อัลกอริทึมของอาณานิคมมด (Ant Colony Algorithm--ACA) ในการหาค่าพลังงานในการฝังลายน้ำ

## บทสรุป

การแทรกกลายน้ำในภาพดิจิทัล (digital image watermarking) ถือเป็นเทคนิคหนึ่งของ วิทยาการอำพรางข้อมูล (steganography) ซึ่งนับว่าเป็นเทคนิคที่มีความสำคัญต่อการนำไปใช้ในการป้องกันการละเมิดลิขสิทธิ์ของภาพดิจิทัล ซึ่งถือเป็นปัญหาใหญ่ที่เกิดขึ้นในสังคมออนไลน์ปัจจุบัน ก่อนหน้านี้นี้การทำภาพพิมพ์ลายน้ำดิจิทัลไม่ค่อยได้รับความสนใจจากนักวิจัยมากนัก จนกระทั่งมีการให้ความสำคัญกับเรื่องของลิขสิทธิ์ในสื่อดิจิทัลมากขึ้น เทคนิคนี้จึงได้รับความนิยมเพิ่มขึ้นอย่างรวดเร็ว แต่ถึงแม้ว่าจะมีงานวิจัยเพื่อป้องกันการละเมิดลิขสิทธิ์ด้านมัลติมีเดียออกมามากเพียงไร นักวิจัยก็ยังคงต้องพัฒนาเทคนิควิธีการใหม่ๆ เพื่อให้ทันต่อผู้ที่จ้องทำลายวิธีการที่ได้คิดค้นขึ้น แต่ปัญหาเหล่านี้จะไม่เกิดขึ้นเลยถ้าทุกคนในสังคมมีจิตสำนึกที่ดีและเคารพต่อสิทธิในความเป็นเจ้าของผลงาน

---

## เอกสารอ้างอิง

- เฉลิมศักดิ์ เลิศวงศ์เสถียร. (2547). *Steganography ศาสตร์แห่งการซ่อนข้อมูล*. ค้นจาก <http://th.wikipedia.org>
- Areef, T. E., & Heniedy, H. S. (2005). Optimal transform domain watermarking embedding via genetic algorithms. *IEEE*, 607-617.
- Chansirimas, J. (2009). *เทคนิคการทำภาพลายน้ำ (Watermark) แบบง่าย ๆ*. Retrieved from [http:// www. ReadyPlanet.com](http://www.ReadyPlanet.com)
- Chen, T. S., Chang, C.C., & Hwang, M. S. (1998). A Virtual Image Cryptosystem Based upon Vector Quantization. *IEEE Transactions on Image Processing*, 7(10), 1485-1488.

- Cox, I. J., Kilian, Leighton, J. F. T., & Shamoon, T. (1997). Secure Spread Spectrum Watermarking for Multimedia. *IEEE Transactions on Image Processing*, 6(12), 1673-1687.
- Dugad, R., Ratakonda, K., & Ahuja, N. (1998). A new wavelet-based scheme for watermarking images. *Proceeding of the IEEE International Conference on Image Processing (ICIP 1998)*, 2, 419-423.
- Hartung, F., & Kutter, M. (1999). Multimedia Watermarking Techniques. *Proceeding of the IEEE*, 87(7), 1079-1107.
- Huang, C. H., & Wu, J. L. (2000). A watermark optimization technique based on genetic algorithms. *Proceeding of SPIE-Visual Communications Image Processing*, 3971, 516-523.
- Lee, S. J., & Jung, S. H. (2001). A survey of watermarking techniques applied to multimedia. *The International Symposium on Industrial Electronics (ISIE2001)*, 1, 272-277.
- Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding-A survey. *Proceeding of the IEEE*, 87(7), 1062-1078.
- Promcharoen, S., & Rangsanteri, Y. (2010). Ant Colony System Watermarking Based on DCT Domain Technique. *Proceeding of the 3rd Technology and Innovation for Sustainable Development International Conference (TISD2010)*, 1189-1194.
- Shieh, C.-S., Huang, H. C., Wang, F. H., & Pan, J. S. (2004). Genetic watermarking based on transform domain techniques. *Pattern Recognition*, 37(3), 555-565.
- Song, Y. J., & Tan, T. N. (2000). Comparison of Four Different Digital Watermarking Techniques. *Proceeding of the 5<sup>th</sup> International Conference on Signal Processing (ICSP2000)*, 2, 946-950.
- Wang, Z., & Bovik, A. C. (2002). A universal image quality index. *The IEEE Signal Processing Letters*, 9(3), 81-84.
- Wei, Z., Dai, J., & Li, J. (2006). Genetic watermarking based on DCT domain techniques. *Proceeding of IEEE CCECE/CCGEI*, 2365-2368.
- Xiang, H. & Jianjun, L. (2009). A digital watermarking algorithm for DEM image based on stationary wavelet transform. *Proceeding of the International Conference on Information Assurance and Security*, 2221-2224.