

A Digital Watermarking on a witness photo for original verification

การฝังลายน้ำบนภาพพยานวัตถุดิจิทัลเพื่อรับรองความเป็นต้นฉบับ

Received	14 Apr 20
Reviewed	10 May 20
Revised	5 June 20
Accepted	23 Jun 20

Sansanee Hiranchan* Anawat Tinloey and Mahasak Ketchum

ศันสนีย์ หิรัญจันทร์* อนวัช ทินเลย์ และ มหศักดิ์ เกตุฉ่ำ

Department of Information Technology, Faculty of Information Technology, King Mongkut's University of Technology North Bangkok

ภาควิชาสาขาการจัดการเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ กรุงเทพมหานคร

*Corresponding Author, 0847172264 , E-mail: s620702191005@kmutnb.ac.th

*ผู้ติดต่อประสานงาน โทรศัพท์: 0847172264 อีเมล: s620702191005@kmutnb.ac.th

Abstract

A Print invisible digital watermarking unable to see the original image and unchanged a witness photo. A digital watermarking is embedded in the data have a slight sense of orientation and change. It is appropriate to use to create reliable data that is authentic, which has not been modified before. This model proceed with the feature of embedding some watermarking (Fragile Watermarking) applied with embed watermarking on photos or original prints for inspection of 64x64 pixels size of digital image. Infiltrate 256x256 pixel images using digital watermarking inserted into the original image by embedding watermarks.

The result shown the test of embedding watermarking on digital document images to confirm appropriate originality. A Digital Watermarking on a witness photo for original verification found that the features of Fragile Watermarking which are fragile of digital watermarks. The digital watermarking is embedded sensitive data protecting and little change watermarks on photos or digital documentary evidence to confirm the originality and verification. The ability to edit images of digital objects If the image of a digital object was modified or just adapted. The watermarking on the image will be different from the original. Therefore, a model able to check for corrections and modifications from the watermarking embedded in the witness image if the witness image has changed.

Keywords: Digital Watermark, Fake Watermark, Witness Photo

บทคัดย่อ

ประเภทลายน้ำดิจิทัลแบบมองไม่เห็น (Invisible watermark) จะไม่สามารถมองเห็นลายน้ำดิจิทัลในภาพต้นฉบับ และไม่ทำให้ภาพต้นฉบับเกิดการเปลี่ยนแปลงไปจากเดิมหรือเปลี่ยนลักษณะไปจากเดิมน้อยที่สุด ลายน้ำดิจิทัลแบบเปราะบาง (Fragile watermark) ซึ่งเป็นหนึ่งในประเภทของลายน้ำดิจิทัลแบบมองไม่เห็น มีวิธีที่มุ่งเน้นไปที่ความเปราะบางของลายน้ำดิจิทัล โดยลายน้ำดิจิทัลที่ถูกฝังไว้ในข้อมูลจะมีความไวต่อการเสียหายและการเปลี่ยนแปลงแม้เพียงเล็กน้อย วิธีการประเภทนี้มีความเหมาะสมที่จะใช้ในการสร้างความน่าเชื่อถือของข้อมูลว่าเป็นของแท้ที่ไม่ได้ผ่านการเปลี่ยนแปลงแก้ไขใด ๆ มาก่อน ด้วยคุณสมบัติของการฝังลายน้ำแบบเปราะบาง (Fragile Watermarking) ซึ่งมีความเปราะบางของลายน้ำ

ดิจิทัล จึงสามารถนำมาใช้ประยุกต์กับการฝังลายน้ำบนภาพถ่าย หรือภาพพยานวัตถุดิจิทัลเพื่อรับรองความเป็นต้นฉบับ และตรวจสอบการแก้ไขตัดแปลงภาพพยานวัตถุดิจิทัลได้ การทดลองใช้ภาพถ่ายน้ำดิจิทัลขนาด 64x64 พิกเซล แทรกลงในภาพต้นฉบับขนาด 256x256 พิกเซล โดยใช้ลายน้ำดิจิทัลแทรกลงในภาพต้นฉบับด้วยวิธีการฝังลายน้ำแบบเปราะบาง จากนั้นทำการถอดลายน้ำออกจากภาพพยาน

จากผลการทดสอบการฝังลายน้ำบนภาพพยานวัตถุดิจิทัลเพื่อรับรองความเป็นต้นฉบับ พบว่า ด้วยคุณสมบัติของการฝังลายน้ำแบบเปราะบาง (Fragile Watermarking) ซึ่งมีความเปราะบางของลายน้ำดิจิทัล โดยลายน้ำดิจิทัลที่ถูกฝังไว้ในข้อมูลจะมีความไวต่อการเสียหาย และการเปลี่ยนแปลง แม้เพียงเล็กน้อย สามารถนำมาใช้ประยุกต์กับการฝังลายน้ำบนภาพถ่าย หรือภาพพยานวัตถุดิจิทัลเพื่อรับรองความเป็นต้นฉบับและตรวจสอบ การแก้ไขตัดแปลงภาพพยานวัตถุดิจิทัลได้ โดยหากภาพพยานวัตถุดิจิทัล ถูกแก้ไข ตัดแปลงหรือถูกโจมตีเพียงเล็กน้อย ลายน้ำบนภาพก็จะผิดเพี้ยน ไปจากต้นฉบับ ดังนั้น หากภาพพยานวัตถุดิจิทัลมีการเปลี่ยนแปลง เพียงเล็กน้อย ลายน้ำที่ถูกถอดออกมาจะมีสภาพเสียหายไม่เหมือนลายน้ำต้นฉบับ จึงสามารถตรวจสอบการแก้ไขตัดแปลงจากลายน้ำที่ฝังอยู่ในภาพพยานวัตถุได้

คำสำคัญ: ลายน้ำดิจิทัล การปลอมแปลงภาพถ่ายน้ำ ภาพพยานวัตถุดิจิทัล

1. บทนำ

ในการเก็บรวบรวม และจัดส่งพยานวัตถุจากสถานที่เกิดเหตุถือเป็นสิ่งที่สำคัญที่สุดในขั้นสืบสวนและสอบสวน หรือในชั้นศาลก็ตาม การเก็บพยานวัตถุต้องกระทำถูกต้องตามกฎหมาย จึงถือเป็นพยานที่ยอมรับได้ และวิธีการเก็บพยานวัตถุจะต้องเป็นวิธีที่เหมาะสม [1] โดยผู้เก็บต้องมีการถ่ายภาพพยานวัตถุที่ตรวจพบไว้ พยานวัตถุทุกชิ้นจะต้องทำการถ่ายภาพไว้ก่อนทำการเก็บ และควรถ่ายภาพทั้งในระยะไกลและใกล้ การถ่ายในระยะใกล้เพื่อยืนยันตำแหน่งที่พบ และแสดงความสัมพันธ์ของพยานวัตถุนั้นกับสภาพโดยรอบ ส่วนการถ่ายโอนในระยะใกล้ เพื่อให้เห็นพยานวัตถุจริงที่จะทำการเก็บ ซึ่งในการถ่ายภาพระยะใกล้ควรมีมาตรวัดระยะกำกับทุกครั้ง เพื่อจะได้ทราบขนาดที่แน่นอนของวัตถุนั้น ๆ จากภาพถ่ายได้ ซึ่งผู้เก็บจะต้องเลือกวิธีการเก็บที่ไม่ทำให้สิ่งเหล่านี้เสียไป การเก็บที่ผิดวิธีหรือไม่เหมาะสมสามารถทำให้ก่อข้อโต้แย้งในชั้นศาลได้ ดังนั้น ภาพถ่ายในสถานที่เกิดเหตุรวมถึงภาพพยานวัตถุจึงมีความสำคัญมาก ต้องสามารถทำการตรวจสอบภาพพยานวัตถุ เพื่อรับรองความเป็นต้นฉบับ และการพิสูจน์ความเป็นเจ้าของลิขสิทธิ์ หรือผู้ถ่ายภาพ โดยต้องสามารถตรวจสอบการตัดแปลงได้ [2]

2. วัสดุ อุปกรณ์ และวิธีการวิจัย

2.1 ขอบเขตการวิจัย

2.1.1.ภาพต้นฉบับที่ใช้ในการแทรกลายน้ำดิจิทัลเป็นไฟล์รูปภาพ ชนิดโทนสีเทา (Gray Scale) สกุล .bmp

2.1.2.ลายน้ำดิจิทัลที่ใช้เป็นสัญลักษณ์หน่วยงานเป็นไฟล์รูปภาพ ชนิดขาวดำ (Binary Image) สกุล .bmp

2.1.3.การแทรกและถอดลายน้ำดิจิทัลกระทำในโดเมนความถี่ (Frequency Domain) โดยใช้วิธีการแปลงเวฟเลต (Wavelet Transform)

2.1.4.รหัสลับ (Key) ที่ใช้แสดงความเป็นเจ้าของมี 2 รหัส คือ รหัสลับที่ใช้ในการสร้างตารางเทียบค่า (Look-up Table :LUT) และการเลือกแบนด์ (Band) ของภาพที่ผ่านการแปลงเวฟเลตเพื่อใช้แทรกและถอดลายน้ำดิจิทัล

2.1.5.ขั้นตอนการแทรกและถอดลายน้ำดิจิทัลบนภาพพยานวัตถุดิจิทัลนี้ ใช้โปรแกรม MATLAB

2.2 การแทรกลายน้ำดิจิทัล [2]

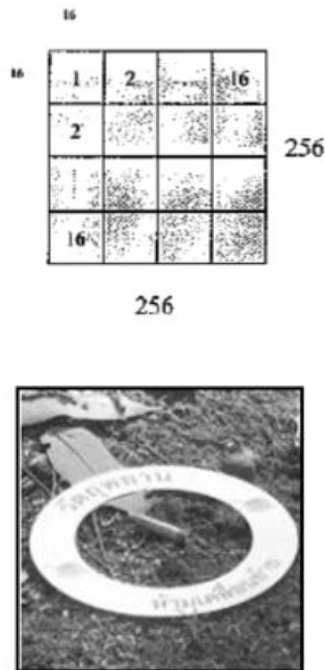
2.2.1 แบ่งบริเวณภาพต้นฉบับ

กำหนดให้ X แทนภาพต้นฉบับซึ่งเป็นภาพระดับโทนเทา (Gray Level Image) ขนาด $N_1 \times N_2$ จุดภาพภาพต้นฉบับสามารถแทนด้วย สมการ

$$x = \{x(i, j); 0 \leq i < N_1 \ 0 \leq j < N_2\} \quad (1)$$

เมื่อ $x(i, j) \in \{0, \dots, 2^L - 1\}$ คือ ความเข้มของจุดภาพที่ตำแหน่ง (i, j) และ L คือ จำนวนหน่วยความจำซึ่งมีหน่วยเป็น Bit ที่ใช้ในแต่ละจุดภาพ

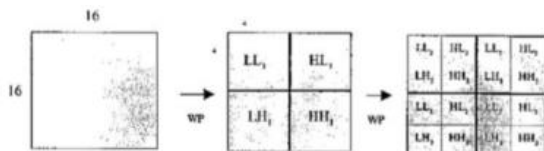
จากนั้นทำการแบ่งภาพต้นฉบับออกเป็นช่อง (Block) ขนาด 16×16 พิกเซล (Pixel) จำนวนบริเวณทั้งหมดที่ได้มีความสัมพันธ์กับภาพ ต้นฉบับคือ $N_1/16 \times N_2/16$ บริเวณ เช่น ถ้า $N_1 = N_2 = 256$ พิกเซล จะทำให้ได้จำนวนบริเวณในภาพต้นฉบับเป็น 16×16 พิกเซล



รูปที่ 1 แบ่งภาพต้นฉบับออกเป็นบริเวณขนาด 16 x 16 พิกเซล (Pixel)

2.2.2 แปลงโดเมนของภาพ

ภาพต้นฉบับขนาด 16 x 16 พิกเซล ถูกแปลงจากโดเมนปกติให้อยู่ในโดเมนความถี่ด้วยวิธีการแปลงเวฟเลตแพกเกตส์ โดยค่าระดับในการแปลงนั้นจะต้องให้ขนาดแต่ละบริเวณที่ได้จากการแปลงเวฟเลตแพกเกตส์ของรูปภาพต้นฉบับมีขนาดเท่ากับรูปภาพลายน้ำดิจิทัล เช่น ลายน้ำดิจิทัลซึ่งถูกแบ่งให้มีขนาด 4 x 4 พิกเซล ภาพต้นฉบับถูกแบ่งให้มีขนาด 16 x 16 พิกเซล ดังนั้น ระดับการแปลงภาพต้นฉบับโดยใช้การแปลงเวฟเลตแพกเกตส์แบบฮาร์ (Haar Wavelet) จะมีค่าระดับเป็น 2 ซึ่งการแปลงเวฟเลตที่ระดับนี้ จะทำให้บริเวณภาพต้นฉบับที่จะเลือกแทรกลายน้ำมีขนาดเดียวกับขนาดของลายน้ำดิจิทัล คือ 4 x 4 พิกเซล [1]



รูปที่ 2 แปลงเวฟเลตแพกเกตส์ระดับที่ 1 และ 2 ของภาพต้นฉบับ

2.2.3 เลือกบริเวณที่จะแทรกลายน้ำ

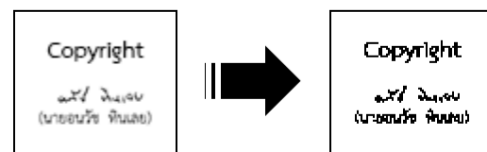
ทำการเลือกบริเวณของภาพต้นฉบับที่จะแทรกลายน้ำดิจิทัลลงไป ซึ่งการเลือกบริเวณนี้ถือเป็นรหัสลับอย่างหนึ่งของการสร้างความปลอดภัยในกระบวนการแทรกลายน้ำ เนื่องจากจะต้องใช้รหัสลับนี้ในกระบวนการถอดลายน้ำ [2]

2.2.4 ปรับค่าสัมประสิทธิ์

ทำการปรับค่าสัมประสิทธิ์ในบริเวณภาพต้นฉบับที่เลือกให้เป็นค่าตัวเลขจำนวนเต็ม

2.2.5 แบ่งบริเวณภาพลายน้ำดิจิทัล

ก่อนแบ่งบริเวณภาพลายน้ำดิจิทัล ต้องทำการเปลี่ยนภาพ สัญลักษณ์ ที่ต้องการใช้ให้เป็นภาพขาวดำ (Binary image) โดยใช้โปรแกรม MATLAB [6]



รูปที่ 3 แปลงภาพลายน้ำที่จะใช้เป็นภาพขาวดำ (Binary image)

กำหนดให้ W แทนลายน้ำดิจิทัลซึ่งเป็นภาพสองระดับขนาด $M_1 \times M_2$ จุดภาพ ซึ่งมีขนาดเป็นหนึ่งในสี่ ของภาพต้นฉบับ สามารถแทนด้วยสมการ

$$W = \{W(i,j); 0 \leq i < M_1, 0 \leq j < M_2\} \quad (2)$$

เมื่อ $W(i,j) \in \{0,1\}$ สำหรับทุก ๆ i,j ที่ซึ่ง $0 \leq i < M_1, 0 \leq j < M_2$

การแบ่งพื้นที่ภาพลายน้ำดิจิทัลจะทำการแบ่งในลักษณะเดียวกัน โดยขนาดแต่ละบริเวณบนภาพลายน้ำนั้น มีความสัมพันธ์กับภาพต้นฉบับ และภาพลายน้ำ คือ $[M_1 \times \frac{16}{N_1}] \times [M_2 \times \frac{16}{N_2}]$ ซึ่งในที่นี้จะได้อะบบภาพลายน้ำที่มีขนาด 4x4 พิกเซล

2.2.6 แทรกลายน้ำดิจิทัล

การแทรกลายน้ำดิจิทัลบนภาพต้นฉบับจะกระทำผ่านตาราง เทียบค่าไบนารี ซึ่งมีรหัสลับที่ใช้ในการสร้างตารางเทียบค่าไบนารี บนารี ซึ่งมีรหัสลับที่ใช้ในการสร้างตารางเทียบค่าไบนารี ซึ่งมีรหัสลับที่ใช้ในการสร้างตารางเทียบค่าไบนารี โดยรหัสลับที่ใช้สร้างตารางนี้จะต้องเป็นรหัสเดียวกันทั้งตอนแทรกและถอดลายน้ำดิจิทัลดิจิทัล จึงจะได้ลายน้ำดิจิทัลกลับคืนมา ตารางเทียบค่าไบนารี คือ ตารางค่าที่เป็นไปได้ทั้งหมดของสัมประสิทธิ์จากการแปลงเป็น

โดเมนความถี่ เทียบกับค่าไบนารีที่ได้จากการสุ่มวิธีการแทรกบิตลายน้ำดิจิทัลลงในสัมประสิทธิ์ภาพต้นฉบับ ณ ตำแหน่งใด ๆ หากค่าบิตลายน้ำดิจิทัลนั้นมีค่าเท่ากับค่าไบนารี ณ ตำแหน่งสัมประสิทธิ์ค่าเดียวกัน ไม่ต้องทำการเปลี่ยนค่าสัมประสิทธิ์นั้น ๆ ให้ใช้ค่าสัมประสิทธิ์เดิม แต่หากบิตลายน้ำที่แทรกมีค่าไม่ตรงกับค่าไบนารี ณ ตำแหน่งนั้น ให้หาค่าสัมประสิทธิ์ใหม่ข้างเคียงที่มีค่าไบนารีตรงกับค่าบิตลายน้ำนั้น แล้วเปลี่ยนค่าสัมประสิทธิ์เดิมเป็นค่าสัมประสิทธิ์ใหม่แทนที่ เช่น การแทรกบิตลายน้ำ ค่า 1 ลงในสัมประสิทธิ์ของภาพต้นฉบับ สัมประสิทธิ์ของภาพต้นฉบับจะไม่ถูกเปลี่ยนแปลง ถ้าค่าไบนารี ณ ตำแหน่งสัมประสิทธิ์เดียวกันในตารางเทียบค่าไบนารี มีค่าเป็น 1 เหมือนกัน แต่ถ้าค่าไบนารี ณ ตำแหน่งสัมประสิทธิ์นั้น ในตารางเทียบค่า ดังกล่าว มีค่าเป็น 0 สัมประสิทธิ์ของภาพต้นฉบับจะถูกเปลี่ยนเป็นค่าสัมประสิทธิ์ข้างเคียงที่มีค่าไบนารีเป็น 1 แทน การแทรกบิตลายน้ำค่า 0 ก็ใช้วิธีเดียวกัน

$$x'_1 = \begin{cases} x_i & \text{ถ้า } LUT(x_i) = w_i \\ x_i + \delta & \text{ถ้า } LUT(x_i) \neq w_i \text{ และ} \\ & \delta = \min\{d = x'_1 - x_1 : LUT(x'_1) = w_1\} \end{cases} \quad (3)$$

รูปที่ 4 การแทรกผ่านตารางเทียบค่าไบนารี

ตัวอย่าง [5]การแทรกบิตตัวอย่างการแทรกบิตลายน้ำ โดยทำการแทรกบิตลายน้ำ ณ ตำแหน่งแถวที่ 1 คอลัมน์ที่ 1 ซึ่งมีค่าเท่ากับ 1 ลงในสัมประสิทธิ์ของภาพต้นฉบับ ณ ตำแหน่งที่ตรงกันซึ่งมีค่าเท่ากับ -4 แต่ค่าไบนารีซึ่งตรงกับค่า ณ ตำแหน่ง -4 ของตารางเทียบค่ามีค่าเป็น 0 จึงต้องตระเวนทั้งสองด้านซ้ายขวาของตาราง เพื่อหาค่าไบนารีที่เป็น 1 ซึ่งในที่นี้ตำแหน่งที่ใกล้เคียงที่สุดตรงกับค่าตำแหน่ง -2 ของตารางจึงแทนที่สัมประสิทธิ์ค่า -4 ของภาพต้นฉบับดังกล่าวด้วยค่าใหม่คือ -2 กรณีแทรกบิตลายน้ำค่า 1 ตัวถัดมาลงในสัมประสิทธิ์ภาพต้นฉบับซึ่งมีค่าเป็น 0 และค่าไบนารี ณ ตำแหน่งดังกล่าวในตารางเทียบค่ามีค่าเป็น 1 เหมือนกัน ให้คงสัมประสิทธิ์ค่า 0 เดิมไว้ไม่ต้องเปลี่ยนแปลง กรณีการแทรกบิตลายน้ำค่า 0 ก็ทำเช่นเดียวกันโดยทำการแทรกบิตลายน้ำ ณ ตำแหน่งแถวที่ 1 คอลัมน์ที่ 1 ซึ่งมีค่าเท่ากับ 1 ลงในสัมประสิทธิ์ของภาพต้นฉบับ ณ ตำแหน่งที่ตรงกันซึ่งมีค่าเท่ากับ -4 แต่ค่าไบนารีซึ่งตรงกับค่า ณ ตำแหน่ง -4 ของตารางเทียบค่ามีค่าเป็น 0 จึงต้องตระเวนทั้งสองด้านซ้ายขวาของตารางเพื่อหา

ค่าไบนารีที่เป็น 1 ซึ่งในที่นี้ตำแหน่งที่ใกล้เคียงที่สุดตรงกับค่าตำแหน่ง -2 ของตาราง จึงแทนที่สัมประสิทธิ์ค่า -4 ของภาพต้นฉบับดังกล่าวด้วยค่าใหม่คือ -2 กรณีแทรกบิตลายน้ำค่า 1 ตัวถัดมาลงในสัมประสิทธิ์ภาพต้นฉบับซึ่งมีค่าเป็น 0 และค่าไบนารี ณ ตำแหน่งดังกล่าวในตารางเทียบค่ามีค่าเป็น 1 เหมือนกัน ให้คงสัมประสิทธิ์ค่า 0 เดิมไว้ไม่ต้องเปลี่ยนแปลงกรณีการแทรกบิตลายน้ำค่า 0 ก็ทำเช่นเดียวกัน

x	x'	x''
1	1	1
1	0	0
1	1	0
0	0	1
1	0	0
1	1	0
0	0	1
0	0	1

x	x'	x''
-4	0	7
1	-2	4
-7	1	8
6	0	-1
-2	0	7
0	-3	4
-7	0	8
4	1	-3

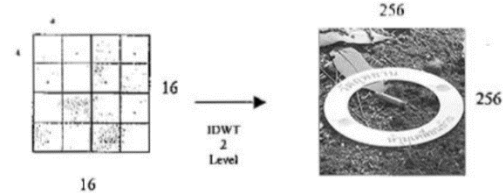
x	x'	x''
-2	0	7
0	-3	4
-7	0	8
4	1	-3

x	x'	x''
-2	0	7
0	-3	4
-7	0	8
4	1	-3

รูปที่ 5 การแทรกบิตลายน้ำลงในสัมประสิทธิ์

2.2.7. แปลงภาพกลับสู่โดเมนปกติ

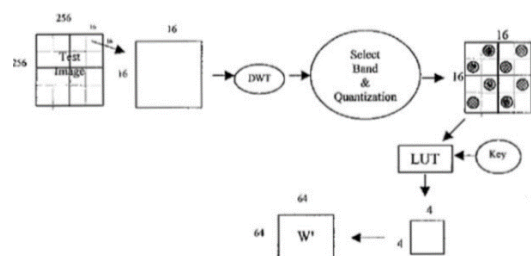
ทำการแปลงกลับเวฟเลต (Inverse Discrete Wavelet Transform) ทำจนครบทุกบริเวณของภาพ จากนั้นนำบริเวณทั้งหมดรวมกลับคืนจะได้ภาพที่มีลายน้ำแฝงอยู่



รูปที่ 6 การรวมกลับภาพลายน้ำ

2.3 การถอดลายน้ำดิจิทัล

ใช้กระบวนการเดียวกับการแทรกลายน้ำดิจิทัล สามารถถอดได้โดยตรงจากภาพลายน้ำ โดยไม่ต้องใช้ภาพต้นฉบับ



รูปที่ 7 ขั้นตอนการถอดลายน้ำดิจิทัล

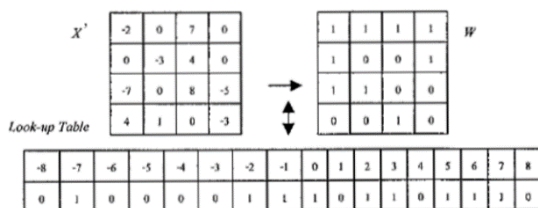
การถอดลายน้ำดิจิทัล สามารถอธิบายลำดับได้ดังนี้

- 1) แบ่งบริเวณภาพลายน้ำ เริ่มจากนำภาพลายน้ำที่ต้องการทดสอบหาลายน้ำดิจิทัล มาทำการแบ่งพื้นที่ออกเป็นบริเวณ 16×16 พิกเซล
- 2) แปลงโดเมนของภาพลายน้ำ ทำการแปลงโดเมนของภาพลายน้ำจากโดเมนปกติเป็นโดเมนความถี่ด้วยวิธีการแปลงเวฟเลตแพกเกตส์ 2 ระดับ
- 3) เลือกบริเวณที่ใช้แทรกลายน้ำให้สอดคล้องที่ตรงกันในการเลือกบริเวณของภาพที่มีลายน้ำดิจิทัลแทรกอยู่
- 4) ปรับปรุงสัมประสิทธิ์ ทำการปรับปรุงค่าสัมประสิทธิ์ในบริเวณนั้น ๆ ให้มีค่าเป็นเลขจำนวนเต็ม
- 5) ถอดลายน้ำดิจิทัล สร้างตารางเทียบค่าไบนารีจากรหัสลับที่ใช้ในขั้นตอนการแทรกลายน้ำ ซึ่งจะเป็นตารางเดียวกันทั้งกระบวนการแทรกและถอดลายน้ำ จากนั้นทำการถอดบิตลายน้ำ จากตารางเทียบค่าซึ่งเป็นค่าบิตไบนารี ณ ตำแหน่งที่สัมประสิทธิ์ในตารางเทียบค่ามีค่าตรงกับค่าสัมประสิทธิ์ในบริเวณที่เลือกแทรกลายน้ำ การถอดลายน้ำแสดงดังสมการ

$$w'_i = LUT(x'_i) \quad (4)$$

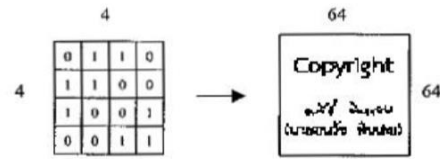
เมื่อ x'_i เป็นค่าสัมประสิทธิ์ของภาพทดสอบ
 w'_i เป็นลายน้ำดิจิทัลที่ถอดออกมาได้

ตัวอย่างการถอดบิตลายน้ำจากสัมประสิทธิ์ภาพทดสอบ ตัวแรกแถวที่ 1 คอลัมน์ที่ 1 มีค่าเท่ากับ -2 ตารางเทียบค่า ณ ตำแหน่งค่า -2 มีค่าไบนารีเป็น 1 ดังนั้น บิตลายน้ำที่ถอดได้จึงมีค่าเป็น 1 การถอดบิตตัวถัดไปก็เช่นเดียวกัน จะเห็นได้ว่าสามารถถอดลายน้ำ ได้โดยตรงจากตารางเทียบค่าไบนารี โดยไม่ต้องอาศัยภาพต้นฉบับ



รูปที่ 8 การถอดบิตลายน้ำออกจากสัมประสิทธิ์

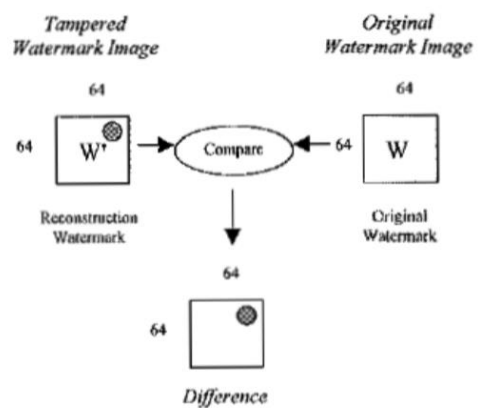
เมื่อทำการถอดบิตลายน้ำตามขั้นตอนจนครบทุกบริเวณแล้ว จึงนำบิตลายน้ำที่ได้ในแต่ละบริเวณกลับมา รวมกัน ก็จะได้ลายน้ำดิจิทัลที่ถอดออกมาจากภาพทดสอบคืนมา



รูปที่ 9 การรวมกลับลายน้ำดิจิทัล

2.4 การทดสอบโจมตีและระบุตำแหน่งการปลอมแปลงภาพลายน้ำ

นำภาพทดสอบที่มีลายน้ำดิจิทัลแฝงอยู่มาทำการทดสอบ โจมตีในลักษณะต่าง ๆ แล้วทำการถอดลายน้ำ จากนั้นเปรียบเทียบลายน้ำดิจิทัลที่ถอดมาได้จากภาพที่ผ่านการโจมตีกับลายน้ำดิจิทัลต้นฉบับ สังเกตลักษณะการปลอมแปลงที่เกิดขึ้นบนลายน้ำดิจิทัล และตำแหน่งการปลอมแปลงดังกล่าว



รูปที่ 10 ขั้นตอนการทดสอบโจมตีและระบุตำแหน่งการปลอมแปลง

การทดสอบโจมตีที่ใช้ในงานวิจัยนี้ ประกอบด้วย

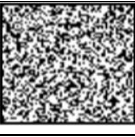
- 1) การแก้ไขปลอมแปลงรูปภาพโดยเจตนา เพื่อบิดเบือนความหมายของภาพ โดยทำการเพิ่มและลบรายละเอียดข้อมูลบนเอกสาร ภาพในลักษณะต่าง ๆ จากบริเวณพื้นที่ขนาดเล็กไปถึงพื้นที่ขนาดใหญ่
- 2) การตัดภาพออกเป็นบางส่วน เป็นการตัดภาพที่มีลายน้ำแฝงในลักษณะต่าง ๆ
- 3) การหมุนภาพ ทำการหมุนภาพเป็นมุม 9 องศา

3. ผลการวิจัย

การทดลองใช้ภาพลายน้ำดิจิทัลขนาด 64×64 พิกเซล แทรกลงในภาพต้นฉบับขนาด 256×256 พิกเซล โดยใช้ลายน้ำดิจิทัลแทรกลงในภาพต้นฉบับด้วยวิธีการฝังลายน้ำแบบ

เปราะบาง จากนั้นทำการถอดลายน้ำออกจากภาพวัตถุพยาน พบว่า ภาพลายน้ำดิจิทัลขนาด 64x64 พิกเซล ยังมีลักษณะคงเดิม จากนั้น ทดสอบการโจมตีภาพลายน้ำในรูปแบบ ต่าง ๆ พบว่า ภาพลายน้ำที่มีการแก้ไข ดัดแปลง เมื่อถอดลายน้ำออกมาแล้ว ภาพลายน้ำดิจิทัลขนาด 64x64 จุดภาพที่ถอดได้จะเสียหายและผิดเพี้ยนไปจากเดิม ดังตารางที่ 1 ดังนั้นจึงสามารถนำการฝังลายน้ำแบบเปราะบาง มาใช้ฝังลายน้ำในภาพต้นฉบับเพื่อเก็บรักษาภาพดิจิทัลต้นฉบับ โดยสามารถยืนยันความแท้ต้นฉบับ และพิสูจน์การแก้ไขดัดแปลงกับภาพพยานวัตถุดิจิทัลได้

ตารางที่ 1 เปรียบเทียบการโจมตีภาพลายน้ำในรูปแบบต่าง ๆ

การทดลอง	ภาพวัตถุพยานที่ฝังลายน้ำ	ลายน้ำที่ถอดได้
ภาพวัตถุพยานที่ฝังลายน้ำแบบดั้งเดิม		
กรณีทดลองเปลี่ยนแปลงภาพฝังลายน้ำ		
เพิ่มข้อความในภาพต้นฉบับ		
ตัดบางส่วนของภาพที่ฝังลายน้ำออก		
เปลี่ยนองศาของภาพที่ฝังลายน้ำออก		

จากตารางที่ 1 พบว่า การถอดลายน้ำจากภาพลายน้ำที่ฝังลายน้ำลงในภาพถ่ายพยานวัตถุดิจิทัลด้วยวิธีการฝังลายน้ำดิจิทัล แบบเปราะบาง (Fragile watermark) ปรากฏผลการทดลองตามตารางดังนี้

1. ภาพลายน้ำต้นฉบับที่ได้ทำการฝังลายน้ำไปในภาพถ่ายพยานวัตถุดิจิทัลโดยใช้วิธีการฝังลายน้ำดิจิทัลแบบเปราะบาง (Fragile watermark) จะไม่สามารถมองเห็นลายน้ำที่ถูกฝังลงไปในภาพลายน้ำได้ แต่สามารถถอดลายน้ำออกมาจากภาพลายน้ำได้อย่างสมบูรณ์

2. การเพิ่มข้อความ “Edit” ลงไปในภาพลายน้ำเมื่อถอดลายน้ำออกมา ปรากฏว่าลายน้ำที่ได้จะมีความผิดเพี้ยนไปจากลายน้ำเดิม

3. การตัดข้อความบางส่วนในภาพลายน้ำโดยตัดคำว่า “ห้าม” ในข้อความ “ห้ามเคลื่อนย้าย” เมื่อถอดลายน้ำออกมา ปรากฏว่าลายน้ำที่ได้จะมีความผิดเพี้ยนไปจากลายน้ำเดิม

4. การหมุนภาพลายน้ำ 9 องศา เมื่อถอดลายน้ำออกมา ปรากฏว่า ลายน้ำที่ได้จะมีความผิดเพี้ยนไปจากลายน้ำเดิม

4. อภิปรายผลและสรุป

ด้วยคุณสมบัติของการฝังลายน้ำแบบเปราะบาง (Fragile Watermarking) ซึ่งมีความเปราะบางของลายน้ำดิจิทัล โดยลายน้ำดิจิทัลที่ถูกฝังไว้ในข้อมูลจะมีความไวต่อการเสียหาย และการเปลี่ยนแปลง แม้เพียงเล็กน้อยสามารถนำมาใช้ประยุกต์กับการฝังลายน้ำบนภาพถ่ายหรือภาพพยานวัตถุดิจิทัลเพื่อรับรองความแท้ต้นฉบับและตรวจสอบ การแก้ไขดัดแปลงภาพพยานวัตถุดิจิทัลได้ โดยหากภาพพยานวัตถุดิจิทัล ถูกแก้ไข ดัดแปลงหรือถูกโจมตีเพียงเล็กน้อย ลายน้ำบนภาพก็จะผิดเพี้ยน ไปจากต้นฉบับ ดังนั้น หากภาพพยานวัตถุดิจิทัลมีการเปลี่ยนแปลง เพียงเล็กน้อย ลายน้ำที่ถูกถอดออกมาก็จะมีสภาพเสียหายไม่เหมือนลายน้ำต้นฉบับ จึงสามารถตรวจสอบการแก้ไขดัดแปลงจากลายน้ำที่ฝังอยู่ในภาพพยานวัตถุได้

5. องค์ความรู้ใหม่ที่ได้จากการวิจัย

กระบวนการตรวจสอบการแก้ไขหรือดัดแปลงลายน้ำบนภาพดิจิทัล และการสืบค้นหาความถูกต้องของภาพดิจิทัลต้นฉบับด้วยเทคนิคการฝังลายน้ำแบบเปราะบาง (Fragile Watermarking)

6. เอกสารอ้างอิง

- 1] ส. ส. วราภรณ์ พรหมวิกร. ความน่าเชื่อถือของพยานหลักฐานทางนิติวิทยาศาสตร์: ปัญหา สาเหตุ และแนวทางการพัฒนาสำหรับประเทศไทย. วารสารเทคโนโลยีภาคใต้ ปีที่ 12 ฉบับที่ 2; 2019.
- 2] ว. พ. อารังรัตน์ อมรรักษ์. ภาพพิมพ์ลายน้ำดิจิทัล: วิธีการป้องกันการละเมิดลิขสิทธิ์ทางปัญญาสำหรับรูปภาพ. วารสารวิชาการพระจอมเกล้าพระนครเหนือ ปีที่ 13 ฉบับที่ 2; 2546.

- [3] ด. อมรรักษา. การทำภาพพิมพ์ลายน้ำดิจิทัล (Digital Watermarking). วารสารสำนักหอสมุด มหาวิทยาลัยเชียงใหม่ ปีที่ 9; 2545.
- [4] น. หนูหอม. การฝังลายน้ำอเนกประสงค์บนรูปภาพดิจิทัล เพื่อตรวจสอบรับรองความเป็นต้นฉบับ และพิสูจน์ความเป็นเจ้าของ; 2553.
- [5] น. ตริพลกุล. การทำลายน้ำดิจิทัลบนเอกสารราชการ; 2553.
- [6] ด. โพธิ์โสโนทัย. การใช้งานโปรแกรม MATLAB สำหรับวิเคราะห์ทางสถิติ. สถาบันเทคโนโลยีเจ้าคุณทหารลาดกระบัง; 2557.
- [7] ส. ผลสมบูรณ์. ลายน้ำดิจิทัลสำหรับรูปภาพที่คืนสภาพได้จากการหมุน การปรับขนาดและการเคลื่อนที่ โดยใช้ฟังก์ชันเอ็กซ์โพเนนเชียลเชิงซ้อน. จุฬาลงกรณ์มหาวิทยาลัย; 2547.