ลายน้ำดิจิตอลในรูปภาพและวีดิทัศน์

Digital Watermark in Image and Video

จันทนา ปัญญาวราภรณ์*

Jantana Panyavaraporn*

ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์ มหาวิทยาลัยบูรพา

Department of Electrical Engineering, Faculty of Engineering, Burapha University

บทคัดย่อ

ในปัจจุบันเทคโนโลยีการทำลายน้ำดิจิตอลเป็นหัวข้อที่ได้รับความสนใจมากขึ้น การทำลายน้ำดิจิตอลของรูปภาพ เสียง วีดิทัศน์ และมัลติมีเดีย มีวัตถุประสงค์เพื่อแสดงสิทธิและยืนยันความเป็นเจ้าของ บทความนี้นำเสนอทฤษฎีและพื้นฐานการทำลายน้ำดิจิตอล คุณสมบัติของลายน้ำดิจิตอล เทคนิคการทำลายน้ำดิจิตอล รวมไปถึงวิธีการประเมินผล ในส่วนสุดท้ายนำเสนอการประยุกต์ใช้เทคนิคการทำลายน้ำดิจิตอลรูปภาพและวีดิทัศน์ในโดเมนเชิงพื้นที่และความถี่

คำสำคัญ : ลายน้ำดิจิตอล รูปภาพ วีดิทัศน์ โดเมนเชิงพื้นที่ โดเมนความถี่

Abstract

Nowadays, digital watermark technology is a topic that has been increasing attention all worldwide. The digital watermarking of images, audio, video, and multimedia has been proposed for resolving copyright ownership and authentication. The paper introduced the definition and basic of digital watermarking, qualification of digital watermark, digital watermark techniques, and evaluation criteria. Finally, the application field and possible research direction of digital image and video watermark technology in spatial and frequency domain is pointed out.

Keywords: Digital Watermark, Image, Video, Spatial Domain, Frequency Domain

*Corresponding author.E-mail: Jantanap@eng.buu.ac.th

บทนำ

ระบบเทคโนโลยีเครือข่ายและมัลติมีเดียได้พัฒนาขึ้นอย่างรวดเร็ว ปัจจุบันรูปภาพและวีดิทัศน์เป็นสิ่งที่ปรากฏในโลกออนไลน์ ปัญหาที่พบเห็นก็คือการทำซ้ำ การลอกเลียนแบบ หรือแม้กระทั้งการนำผลงานข้ออื่นไปใช้หาผลประโยชน์โดยไม่ได้รับความเห็นชอบจากเจ้าของผลงาน ปัญหาเหล่านี้ถือเป็นการละเมิดสิทธิทางปัญญา ในหลายองค์กรหรือหน่วยงานได้ให้ความสำคัญกับปัญหาดังกล่าวที่เกิดขึ้น จึงนำมาซึ่งวิธีการป้องกันวิธีหนึ่ง นั่นคือการใช้ตัวบทกฎหมายโดยผู้คิดค้นหรือเจ้าของผลงานทำการจดลิขสิทธิ์เพื่อให้ผลงานได้รับการคุ้มครองจากกฎหมาย แต่อย่างไรก็ตามบางครั้งกฎหมายยังคงมีช่องโหว่หลายประการที่ยังคงไม่สามารถเอาผิดกับผู้กระทำได้ นักวิจัยหลายท่านจึงคิดหาหนทางใหม่ๆ ที่สามารถนำมาใช้งานควบคู่กับตัวบทกฎหมาย นั่นคือการฝังข้อมูลหรือข่าวสารลงในข้อมูลชนิดมัลติมีเดีย เพื่อแสดงสิทธิความเป็นเจ้าของในกรณีที่เกิดเหตุการณ์ฟ้องร้อง วิธีการนี้เรียกว่า “การทำลายน้ำดิจิตอล” โดยที่ลายน้ำดิจิตอลถือเป็นรูปแบบหนึ่งของสเตกาโนกราฟี (Steganography) ซึ่งเป็นการฝัง(หรือซ่อน)ข้อมูลลงบนข้อมูลต้นแบบโดยที่ผู้ใช้ข้อมูลปลายทางจะไม่ทราบ จุดมุ่งหมายหลักของสเตเกโนกราฟี คือการซ่อนข้อมูลข่าวสารไว้ภายในข้อมูลที่ไม่เป็นที่น่าสงสัย และเป็นไปได้ยากในการตรวจหาได้ว่ามีข่าวสารที่เป็นความลับปรากฏซ่อนอยู่ภายใน ซึ่งคล้ายคลึงกับการฝัง(หรือซ่อน)ลายน้ำดิจิตอลในปัจจุบัน (Andersonand & Petiicolus, 1998)

เทคนิคการทำลายน้ำดิจิตอลแตกต่างจากการเข้ารหัสลับทั่วไปตรงที่ ข้อมูลหลังจากการเข้ารหัสลับสามารถดูได้โดยผู้ที่มีกุญแจรหัสเท่านั้น แต่การทำลายน้ำดิจิตอลนั้นใช้หลักการฝัง(หรือซ่อน) สิ่งที่เรียกว่า “สัญญาณลายน้ำ” ลงไปที่ตัวข้อมูลโดยตรง (Podilchuk & Delp, 2001.; Wolfgang *et al.,* 1999) และลายน้ำดิจิตอลที่ดีต้องไม่ทำให้ความคมชัดและความสมบูรณ์ของข้อมูลต้นฉบับลดต่ำลงจนถึงระดับสายตามนุษย์สังเกตเห็นได้ มีความคงทนต่อการโจมตีในลักษณะต่างๆ เช่น การบีบอัดแบบ JPEG การเปลี่ยนแปลงทางเรขาคณิต การประมวลผลสัญญาณ เป็นต้น เมื่อข้อมูลที่มีลายน้ำดิจิตอลฝังอยู่ถูกทำซ้ำหรือคัดลอก ลายน้ำดิจิตอลที่ถูกฝังจะติดไปกับข้อมูลใหม่ด้วย เมื่อตรวจสอบข้อมูลที่ถูกทำซ้ำ ลายน้ำดิจิตอลที่ติดไปกับข้อมูลนั้นจะถูกกู้กลับคืนได้เพื่อใช้แสดงสิทธิความเป็นเจ้าของข้อมูลต้นฉบับ เทคนิคการทำลายน้ำดิจิตอลแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือการทำลายน้ำดิจิตอลในโดเมนเชิงพื้นที่ (Spatial Domain) และการทำลายน้ำดิจิตอลในโดเมนความถี่ (Frequency Domain) (Cheung, 2000) บทความนี้นำเสนอพื้นฐานการทำลายน้ำดิจิตอลในรูปภาพและวีดิทัศน์ โดยพิจารณาการทำลายน้ำดิจิตอลทั้งโดเมนเชิงพื้นที่และความถี่ รวมถึงวิเคราะห์ข้อดีและข้อเสียของแต่ละวิธี

คำจำกัดความและคุณสมบัติของลายน้ำดิจิตอล

การทำลายน้ำดิจิตอลเป็นวิธีที่ใช้ในการแสดงความเป็นเจ้าของต่อข้อมูลชนิดมัลติมีเดีย เช่น รูปภาพ วีดิทัศน์ เป็นต้น โดยทำการฝังสัญญาณลายน้ำที่แสดงถึงเอกลักษณ์ของตนเองไว้ในตัวข้อมูลต้นแบบ สัญญาณลายน้ำที่ฝังเข้าไปนั้นอาจจะมีลักษณะที่มองเห็นได้หรือไม่สามารถมองเห็น ถ้าเปรียบเทียบสัญญาณลายน้ำในทฤษฎีประมวลผลสัญญาณ สัญญาณลายน้ำเสมือนสัญญาณอ่อน (Weak Signal) ในสัญญาณพาห์ (Carrier Signal) และในทฤษฎีการสื่อสารดิจิตอลสัญญาณลายน้ำเปรียบเสมือนสัญญาณที่มีแบนด์วิดธ์แคบ (Narrow-Bandwidth Signal) ในช่องสัญญาณบรอดแบรนด์

ประเภทของลายน้ำดิจิตอลตามลักษณะการมองเห็นได้แบ่งเป็น 2 ชนิด (Peticolas, 1999) ดังนี้

1. ลายน้ำดิจิตอลชนิดที่มองเห็นได้ (Visible Watermark) วัตถุประสงค์ของลายน้ำดิจิตอลชนิดนี้ ก็เพื่อแสดงความเป็นเจ้าของผลงาน ยกตัวอย่างเช่น ตราประทับขององค์กร หรือการติดโลโก้ของสถานีโทรทัศน์ตรงมุมล่างขวาของ

หน้าจอโทรทัศน์ เป็นต้น ทำให้ผู้พบเห็นสามารถรู้ได้โดยทันทีว่าข้อมูลเป็นของผู้ใดหรือหน่วยงานใด นอกจากนี้ยังเป็นการยับยั้งการกระทำที่จะเป็นการละเมิดลิขสิทธิ์ของข้อมูล เนื่องจากการฝังลายน้ำดิจิตอลชนิดนี้ ยากลำบากในการที่จะนำลายน้ำดิจิตอลออกจากตัวรูปภาพหรือสื่อมัลติมีเดีย ก่อนที่จะนำไปเผยแพร่อย่างมิชอบ

2. ลายน้ำดิจิตอลชนิดที่ไม่สามารถมองเห็นได้ (Invisible Watermark) การฝังลายน้ำดิจิตอลชนิดนี้จำเป็นต้องใช้กุญแจรหัสลับเป็นส่วนประกอบในการเข้ารหัสสัญญาณ เพื่อป้องกันการเปลี่ยนแปลงแก้ไขจากบุคคลที่ไม่ได้รับอนุญาต โดยผู้ที่เป็นเจ้าของเท่านั้นที่จะรู้กุญแจรหัสลับ ดังนั้นบุคคลอื่นจึงไม่สามารถล่วงรู้ถึงสิ่งที่ฝังอยู่ในข้อมูลได้เลย ถึงแม้ว่าบุคคลนั้นจะรู้กลไกการทำงานของการฝังและถอดสัญญาณลายน้ำออกก็ตาม

ลายน้ำดิจิตอลตามความคงทนในการใช้งานแบ่งได้เป็น 2 ชนิดดังนี้

1. เทคนิคที่มุ่งไปที่ความทนทานของการทำลายน้ำ (Robust Watermarking) สัญญาณลายน้ำที่ถูกใส่ไว้ในตัวข้อมูลจะมีความทนทานต่อการโจมตีแบบต่างๆ เทคนิคประเภทนี้จะมีความเหมาะสมในการใช้งานที่เกี่ยวข้องกับการป้องกันการละเมิดลิขสิทธิ์ของตัวข้อมูลเนื่องจากความยากลำบากในการเปลี่ยนแปลง แก้ไข หรือทำลายสัญญาณลายน้ำ
2. เทคนิคที่มุ่งไปที่ความเปราะบางของการทำลายน้ำ (Fragile Watermarking) สัญญาณลายน้ำที่ถูกใส่ไว้ในตัวข้อมูลจะมีความไวและเสียหายง่ายต่อการเปลี่ยนแปลงของข้อมูลแม้เพียงเล็กน้อย เช่นถ้าข้อมูลที่มีสัญญาณลายน้ำอยู่ภายในถูกเปลี่ยนหรือแก้ไข สัญญาณลายน้ำที่อยู่ภายในก็จะเสียหายจนตรวจสอบไม่ได้ เทคนิคประเภทนี้เหมาะสมที่จะใช้ในการสร้างความน่าเชื่อถือของข้อมูลว่าเป็นของแท้ที่ไม่ได้ผ่านการเปลี่ยนแปลงแก้ไขใดๆ มาก่อน

การออกแบบอัลกอริธึมเพื่อนำมาใช้งานได้อย่างเหมาะสม จึงจำเป็นต้องคำนึงถึงความสัมพันธ์ระหว่างข้อกำหนดที่สำคัญทั้ง 3 ส่วน (Cox & Killian, 1997) นั่นคือ ความโปร่งใส ความคงทน และความปลอดภัย

- *ความโปร่งใส (Transparency)* คุณสมบัตินี้ขึ้นอยู่กับลักษณะการนำไปใช้งาน เช่น ถ้าต้องการลายน้ำดิจิตอลที่ไม่มีผลต่อคุณภาพของข้อมูลต้นแบบก็คือควรเลือกลายน้ำดิจิตอลแบบไม่สามารถมองเห็น เป็นต้น
- *ความคงทน (Robustness)* เมื่อข้อมูลที่มีลายน้ำดิจิตอลถูกโจมตีโดยวิธีการประมวลสัญญาณต่างๆ ทั้งแบบเชิงเส้นและไม่เป็นเชิงเส้น รวมถึงการบีบอัดข้อมูลแบบสูญเสียสัญญาณบางส่วน วิธีการเหล่านี้ต้องไม่ทำให้ข้อมูลลายน้ำดิจิตอลหายไปหรือถูกทำลายไปได้ แม้ในบางกรณีที่ข้อมูลลายน้ำดิจิตอลบางส่วนหายไป ข้อมูลที่คงอยู่ต้องชัดเจนพอที่จะใช้แสดงสิทธิความเป็นเจ้าของได้
- *ความปลอดภัย (Security)* เทคนิคการทำลายน้ำดิจิตอลในรูปภาพต้องมีความปลอดภัย ถึงแม้ว่าจะรู้อัลกอริธึมที่แท้จริงในการฝังหรือการกู้คืนสัญญาณลายน้ำ บุคคลทั่วไปที่ไม่ได้รับอนุญาตก็ไม่สามารถลบสัญญาณลายน้ำทิ้งไปได้ นอกจากเจ้าของผลงานเท่านั้น

รูปแบบการถูกโจมตี

การโจมตีลายน้ำดิจิตอลคือการทำให้ข้อมูลสัญญาณลายน้ำที่ฝังในรูปภาพหรือวีดิทัศน์เกิดความเสียหาย รวมไปถึงกระบวนการประมวลผลสัญญาณที่ทำให้ข้อมูลลายน้ำดิจิตอลจางหรือลบเลือนไป หรือความเสียหายที่เกิดจากการโจมตีของ

ผู้ประสงค์ร้าย ลายน้ำดิจิตอลที่ดีควรมีความทนทานต่อข้อกำหนดความคงทนเบื้องต้น การโจมตีลายน้ำดิจิตอลแบ่งได้หลายแนวทาง ที่นิยมแบ่งกันมี 3 หัวข้อดังนี้ (Kutter & Petitcolas, 1999; Hartumg, 1999)

- **การบีบอัดแบบ JPEG** เป็นการประมวลผลสัญญาณที่ใช้กับภาพดิจิตอลมากที่สุดในปัจจุบัน อัลกอริธึม JPEG เป็นกระบวนการบีบอัดที่ทำการกำจัดส่วนที่ไม่สัมพันธ์ในภาพออกไป ซึ่ง JPEG เป็นตัวทดสอบที่ดีสำหรับการทดสอบความคงทนของลายน้ำดิจิตอล
- **การเปลี่ยนแปลงทางเรขาคณิต** คือการเปลี่ยนลักษณะของภาพโดยไม่มีการสูญเสียในเรื่องของคุณภาพ มีดังนี้
    - การย่อหรือขยายขนาดภาพ (Resizing) มีผลกับอัลกอริธึมที่ฝังสัญญาณลายน้ำในตำแหน่งที่ตายตัว ส่งผลให้ตรวจหาสัญญาณลายน้ำไม่ได้
    - การตัดบางส่วนของภาพ (Cropping) มีผลกับอัลกอริธึมที่กระจายลายน้ำออกไปทั่วทั้งภาพ
    - การเคลื่อนย้ายภาพ (Translation) มีผลต่ออัลกอริธึมที่ฝังสัญญาณลายน้ำลงในตำแหน่งที่ตายตัวและมีการตัดบางส่วนของภาพออกไป
    - การหมุนภาพ (Rotation) เป็นกรณีที่สำคัญที่สุด เช่นในกรณีที่หมุนภาพไป 90 และ 180 องศา เป็นต้น
    - การกลับด้านของภาพ (Flipping) คือเมื่อสลับด้านซ้ายขวาของภาพ มีผลกับอัลกอริธึมที่ฝังสัญญาณลายน้ำลงในตำแหน่งที่ตายตัวเช่นกัน
- **การแก้ไขโดยการประมวลผลสัญญาณ** มีหลายประเภทดังนี้
    - การปรับความสว่างและความแตกต่าง (Brightness and Contrast Enhancement)โดยทั่วไปไม่ทำให้เกิดปัญหาในการตรวจหาสัญญาณลายน้ำ
    - การปรับความคมชัด การทำให้เลือน การกรองแบบเชิงเส้นและแบบไม่เป็นเชิงเส้น (Sharpening, Blurring, Linear and Non Linear Filtering) การทำซ้ำสามารถทำให้สัญญาณลายน้ำเสื่อมลงไปได้
    - การเพิ่มสัญญาณรบกวนแบบคอรีเลทและแบบไม่เป็นคอรีเลท (Addition of Correlated or Uncorrelated noise) เข้าไปในข้อมูลที่มีสัญญาณลายน้ำอยู่ การแปลงอนาลอกเป็นดิจิตอลและดิจิตอลเป็นอนาลอก เช่น การพิมพ์ การสแกน หรือการบันทึกเทป เป็นต้น

ทฤษฎีพื้นฐานของภาพดิจิตอลและวีดิทัศน์

ภาพดิจิตอล

ภาพระดับเทาคือแถวลำดับ (array) 2 มิติของตัวเลข แทนด้วย $I(x,y)$ ใช้ตัวเลขแทนระดับความมืดและความสว่างของพื้นที่ ตัวเลขที่มีค่ามากแสดงว่าพื้นที่มีความสว่างมาก ดังนั้นเลขศูนย์แทนสีดำและเลขมากสุดแทนสีขาว ส่วนตัวเลขที่อยู่ในช่วงกลางแทนความเข้มระดับเทา เรียกตัวเลขกำกับแต่ละพื้นที่เล็กว่า “จุดภาพ” หรือ “พิกเซล (pixel)” ขนาดพื้นที่ทางกายภาพที่แทนด้วยหนึ่งจุดภาพเรียกว่าความละเอียดเชิงพื้นที่หรือความละเอียดเชิงตำแหน่ง (Spatial Resolution) ดังแสดงในสมการที่ 1 เทคนิคการประมวลผลภาพนิยมใช้การแปลงฟูริเยร์แบบไม่ต่อเนื่อง (Discrete Fourier Transform) การแปลงเว็ฟ-เล็ตแบบไม่ต่อเนื่อง (Discrete Wavelet Transform) การแปลงโคโซน์ไม่ต่อเนื่อง (Discrete Cosine Transform) ฯลฯ ทั้งหมดนี้คือความละเอียดในเชิงความถี่ (Frequency Resolution)

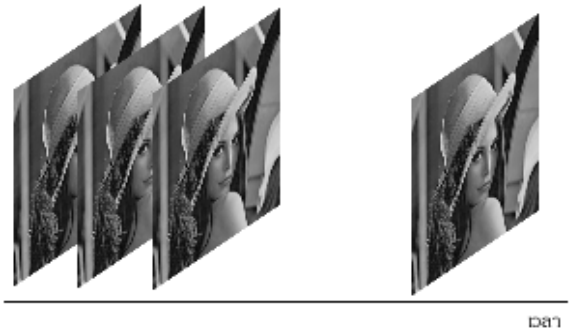
$$I(x,y)=\begin{bmatrix} I(1,1) & I(1,2) & \cdots & I(1,M) \\ I(2,1) & I(2,2) & \cdots & I(2,M) \\ \vdots & \vdots & \cdots & \vdots \\ I(N,1) & I(N,2) & \cdots & I(N,M) \end{bmatrix} \quad (1)$$

ภาพที่สายตามนุษย์มองเห็นเกิดจากหลายภาพซ้อนทับกัน เช่น ภาพสีประกอบด้วยส่วนประกอบของสีแดง เขียว น้ำเงิน ดังแสดงตัวอย่างในภาพที่ 1 หรือภาพถ่ายดาวเทียมที่มี 5 แถบความถี่ซ้อนทับกันโดยแต่ละแถบความถี่จะบอกรายละเอียดที่แตกต่างกันขึ้นอยู่กับคุณสมบัติการนำไปใช้ เป็นต้น

ภาพที่ 1 รูปภาพดิจิตอล

วีดิทัศน์

วีดิทัศน์ (Video) หรือภาพเคลื่อนไหวเป็นชุดของภาพนิ่งที่เรียกว่า “เฟรม (frame)” หลายๆ ภาพต่อกันไปตามเวลา ดังแสดงในภาพที่ 2 เปรียบเทียบได้กับสัญญาณ 3 มิติ เมื่อนับเวลาเป็นมิติที่ 3 หรืออาจจะครอบคลุมถึงสัญญาณ 3 มิติอื่นๆ เช่นภาพ 3 มิติทางการแพทย์เป็นต้น วีดิทัศน์มีความต่อเนื่องทั้งในเชิงพื้นที่และเชิงเวลา วีดิทัศน์ดิจิตอลเป็นการนำเสนอวีดิทัศน์ที่ชักตัวอย่างมาจากฉากธรรมชาติในรูปแบบดิจิตอล แต่ละภาพประกอบไปด้วยค่าตัวอย่างที่ได้มาจากการสุ่มตัวอย่างที่ผ่านการแจงหน่วย ค่าตัวอย่างแต่ละค่าเรียกว่า “จุดภาพ” แต่ละจุดภาพเป็นตัวแทนเซตของค่าตัวเลขที่อธิบายความส่องสว่างหรือค่าสี ซึ่งค่าตัวอย่างประกอบด้วย 2 ส่วน ได้แก่ ส่วนของความส่องสว่าง และส่วนของสัญญาณสี



ภาพที่ 2 ลักษณะของวีดิทัศน์

งานวิจัยที่เกี่ยวข้อง

การทำลายน้ำดิจิตอลในรูปภาพดิจิตอล

นักวิจัยหลายท่านนำเสนอการทำลายน้ำดิจิตอลในรูปภาพหลายชนิด ยกตัวอย่างเช่น ภาพระดับเทา (gray scale image) ภาพสี (color image) ภาพหลายแถบความถี่ (multispectral image) ภาพถ่ายทางการแพทย์ (medical image) เป็น

ต้น ทั้งในโดเมนเชิงพื้นที่และความถี่ (Dharwadkar & Amberker, 2013) ได้นำเสนอการทำลายน้ำดิจิตอลในภาพระดับเทา โดยฝังสัญญาณลายน้ำในคู่ของจุดภาพที่บิตมีความสำคัญน้อยที่สุด (Least Significant Bit: LSB) เทคนิคนี้เป็นการทำลายน้ำดิจิตอลในโดเมนเชิงพื้นที่ ความแตกต่างระหว่างคู่ของจุดภาพถูกนำมาใช้ในการหาความเรียบและหาขอบของรูปภาพ บริเวณพื้นเรียบในรูปภาพจะถูกฝังสัญญาณลายน้ำน้อยกว่าจุดที่เป็นขอบของรูปภาพ ข้อดีคือความผิดเพี้ยนน้อยและปริมาณการฝังสัญญาณลายน้ำสูง เช่นเดียวกับงานวิจัย (Walia & Suneja, 2013) นำเสนอการทำลายน้ำดิจิตอลสำหรับภาพถ่ายทางการแพทย์ในโดเมนเชิงพื้นที่ หลักการทำงานคือใช้กฎของ Weber สัญญาณลายน้ำที่มีความเปราะบางจะถูกฝังในความเข้มของแสงของจุดภาพที่เข้ม ข้อดีคือมีความคงทนต่อการบีบอัดภาพสูง และเหมาะสมกับรูปภาพที่ต้องการส่งผ่านระบบเครือข่าย อย่างไรก็ตามการทำลายน้ำดิจิตอลในโดเมนเชิงพื้นที่ก็ยังคงมีข้อเสีย นั่นคือไม่คงทนต่อการถูกโจมตีเชิงประมวลผลสัญญาณ

จากข้อเสียข้างต้นทำให้นักวิจัยจำนวนมากคิดค้นเทคนิคการทำลายน้ำดิจิตอลในโดเมนความถี่ เช่น การแปลงฟูริเยร์แบบไม่ต่อเนื่อง (Discrete Fourier Transform: DFT) การแปลงเว็ฟเล็ตแบบไม่ต่อเนื่อง (Discrete Wavelet Transform: DWT) การแปลงโคโซน์แบบไม่ต่อเนื่อง (Discrete Cosine Transform: DCT) เป็นต้น ในงานวิจัย (Rangsanseri *et al.,* 2005) นำเสนอการทำลายน้ำดิจิตอลในการแปลงเว็ฟเล็ตแบบไม่ต่อเนื่อง โดยฝังสัญญาณลายน้ำลงในแถบความถี่กลาง นอกจากนั้นมีการประยุกต์เทคนิคการทำลายน้ำในภาพถ่ายเอกสารทางราชการ (Rosiyadi *et al.,* 2012) รูปแบบการทำลายน้ำดิจิตอลโดยใช้การแปลงโคโซน์แบบไม่ต่อเนื่องร่วมกับการหาความแตกต่างของค่าแบบเอกฐาน (Singular Value Decomposition: SVD) วิธีดังกล่าวสามารถปรับปรุงคุณภาพของรูปภาพได้ดีขึ้น และมีความคงทนต่อการถูกโจมตีในลักษณะต่างๆ นอกจากนี้ยังมีงานวิจัยที่รวมการทำลายน้ำดิจิตอลในโดเมนความถี่หลายๆ แบบเข้าด้วยกัน เช่นงานวิจัย (Divecha & Jani, 2013) นำเสนอการฝังสัญญาณลายน้ำในภาพสี โดยใช้การแปลงเว็ฟเล็ตแบบไม่ต่อเนื่องร่วมกับการแปลงโคโซน์แบบไม่ต่อเนื่อง ผลลัพธ์ที่ได้คือสัญญาณลายน้ำมีความคงทนมากขึ้น

มีหลายงานวิจัยที่ทำการฝังสัญญาณลายน้ำทั้งในโดเมนเชิงพื้นที่และอื่นๆ เช่นงานวิจัย (Bouslimi *et al.,* 2012) นำเสนอการฝังสัญญาณลายน้ำทั้งโดเมนเชิงพื้นที่และเอนคริป (Encrypted Domain) เข้าด้วยกัน ทำการวิเคราะห์ผลการทดลองจากภาพถ่ายอัลตร้าซาวด์ วิธีนี้ทำให้รูปภาพที่ได้มีความผิดเพี้ยนน้อยลง และงานวิจัย (Jassim *et al.,* 2013) ทำการฝังสัญญาณลายน้ำในภาพสีที่เกิดจากกล้องถ่ายรูปในโทรศัพท์มือถือ งานวิจัยนี้นำเสนอการทำลายน้ำดิจิตอล 2 ชนิด คือ ลายน้ำที่มีความเปราะบาง (Fragile Watermark) และลายน้ำที่มีความคงทน (Robust Watermark) สัญญาณลายน้ำที่มีความเปราะบางถูกฝังในโดเมนเชิงพื้นที่ของภาพ RGB และสัญญาณลายน้ำที่มีความคงทนจะถูกฝังในโดเมนเว็ฟเล็ตแบบไม่ต่อเนื่อง นอกจากนี้ (Majumder *et al.,* 2013)ได้เสนอการทำลายน้ำดิจิตอลในภาพถ่ายที่ใช้ในการตรวจสอบลักษณะเฉพาะบุคคล (biometric image) เช่น สแกนใบหน้า สแกนตา สแกนลายนิ้วมือ เป็นต้น ในโดเมนเชิงพื้นที่และความถี่ทั้งแบบ DCT และ DWT ทำการวิเคราะห์ผลเมื่อถูกโจมตีในลักษณะต่างๆ และวิเคราะห์ความผิดพลาดจากการรู้จำภาพ และยังมีงานวิจัย (Kunhu *et al.,* 2013) เสนอเทคนิคการทำลายน้ำดิจิตอลในภาพถ่ายดาวเทียม ซึ่งเป็นการฝังสัญญาณลายน้ำทั้งในเชิงพื้นที่และความถี่ ขั้นแรกฝังสัญญาณลายน้ำที่มีความคงทนลงในการแปลงโคโซน์แบบไม่ต่อเนื่อง ขั้นที่สองฝังรหัสยืนยันความเป็นตัวตนในโดเมนเชิงพื้นที่ สังเกตเห็นว่าการฝังสัญญาณลายน้ำทั้งในโดเมนเชิงพื้นที่และความถี่ สามารถป้องกันการสูญเสียข้อมูลจากการโจมตีทั้งในเชิงเรขาคณิตและการโจมตีจากการประมวลผลสัญญาณได้

การทำลายน้ำดิจิตอลในวีดิทัศน์

การทำลายน้ำดิจิตอลในวีดิทัศน์นิยมทำในโดเมนความถี่ งานวิจัย (Jantana, 2011) นำเสนอการทำลายน้ำดิจิตอลโดยใช้การแปลงเว็ฟเล็ตแบบไม่ต่อเนื่องลงในแถบความถี่กลาง เนื่องจากวีดิทัศน์ชนิด QCIF มีขนาด 196*144 จุดภาพต่อเฟรม เมื่อกู้คืนสัญญาณลายน้ำจะมีสัญญาณรบกวนแทรกเข้าเนื่องจากการกู้คืนสัญญาณลายน้ำไม่จำเป็นต้องใช้ข้อมูลต้นฉบับ และงานวิจัย (Chen *et al.,* 2011) นำเสนอการทำลายน้ำดิจิตอลในมาตรฐานตัวเข้ารหัสวีดิทัศน์ H.264 โดยฝังสัญญาณลายน้ำในบล็อกที่มีพลังงานต่ำและสูงใน I เฟรมเท่านั้นเพื่อป้องกันการถูกโจมตีแบบตัวกรองผ่านต่ำและตัวกรองผ่านสูง และงานวิจัย (Verma, *et al.,* 2013) นำเสนอการทำลายน้ำดิจิตอลในวีดิทัศน์เช่นเดียวกัน แต่ต่างจากวิธีข้างต้นคือการใช้แบบจำลองสี YCbCr ในโดเมนเว็ฟเล็ต ผลการทดสอบแสดงให้เห็นว่าสามารถทนต่อการถูกโจมตีในลักษณะต่างๆ ได้ นอกจากนั้นงานวิจัย (Chimanna & Khot, 2013) นำเสนอการทำลายน้ำดิจิตอลโดยแปลงเว็ฟเล็ตแบบไม่ต่อเนื่องร่วมกับการวิเคราะห์หาองค์ประกอบหลัก (Principal Component Analysis: PCA) ผลที่ได้จากวิธีดังกล่าวคือมีความคงทนต่อการโจมตี เช่น สัญญาณรบกวนแบบเกาเซียน สัญญาณรบกวนแบบเม็ดขาวและดำ การกรองความถี่กลาง การหมุนและการตัด เป็นต้น

จากงานวิจัยที่เกี่ยวข้อง สามารถสรุปผลดังตารางที่ 1 โดยแบ่งตามชนิดและเทคนิคการทำลายน้ำดิจิตอล สังเกตเห็นว่าในปัจจุบันภาพดิจิตอลนิยมฝังลายน้ำดิจิตอลทั้งในโดเมนเชิงพื้นที่และโดเมนความถี่หรือโดเมนอื่นๆ ซึ่งการทำลายน้ำดิจิตอลโดยใช้อย่างน้อย 2 เทคนิค ทำให้ภาพดิจิตอลเมื่อถูกโจมตีไม่ว่าลักษณะใดก็ตามสามารถกู้คืนสัญญาณลายน้ำได้ สำหรับการเข้ารหัสวีดิทัศน์นิยมใช้การแปลงในโดเมนความถี่ เนื่องจากมาตรฐานการเข้ารหัสวีดิทัศน์มีการแปลงในโดเมนความถี่อยู่แล้ว จึงง่ายต่อการทำลายน้ำดิจิตอลในโดเมนความถี่

ตารางที่ 1 สรุปงานวิจัยที่เกี่ยวข้อง

	โดเมนเชิงพื้นที่	**โดเมนความถี่**	**โดเมนเชิงพื้นที่ และโดเมนอื่น ๆ**
ภาพดิจิตอล			
ภาพระดับเทา	(Dharwadkar & Amberker, 2013)	-	-
ภาพสี	-	(Divecha & Jani, 2013)	(Jassim *et al.,* 2013)
ภาพหลายแถบความถี่	-	(Rangsanseri *et al.,* 2005)	(Kunhu *et al.,* 2013)
ภาพถ่ายทางการแพทย์	(Walia & Suneja, 2013)	-	(Bouslimi *et al.,* 2012)
ภาพถ่ายที่ใช้ในการตรวจสอบลักษณะเฉพาะบุคคล	-	-	(Majumder *et al.,* 2013)
ภาพถ่ายเอกสารทางราชการ	-	(Rosiyadi *et al.,* 2012)	-
วีดิทัศน์	-	(Jantana, 2011) (Chen *et al.,* 2011) (Verma, *et al.,* 2013) (Chimanna & Khot, 2013)	-

ขั้นตอนการฝังและตรวจสอบลายน้ำดิจิตอล

การทำลายน้ำดิจิตอลประกอบด้วย 2 ขั้นตอนหลัก คือ การฝังลายน้ำ (Watermark Embedding) และการตรวจสอบลายน้ำ (Watermark Extracting) หรือเรียกว่าการกู้คืนสัญญาณลายน้ำ (Watermark Retrieval) ก็ได้ โดยข้อมูลที่ผ่านกระบวนการฝังสัญญาณลายน้ำจะถูกใส่ไปพร้อมกุญแจลับที่ใช้ในการเข้ารหัส เพื่อเป็นการยืนยันว่าเจ้าของกุญแจลับเท่านั้นที่สามารถแก้ไขข้อมูลและตรวจสอบลายน้ำได้ ดังแสดงในภาพที่ 3 สัญญาณลายน้ำ $M(x,y)$ มีหลายชนิด ยกตัวอย่างเช่น ไบนารี $\{-1,+1\}$ หรือ $\{-1,0,+1\}$ หรือสัญญาณแบบสุ่ม เป็นต้น การฝังสัญญาณลายน้ำแบบเชิงเส้นเป็นดังสมการที่ 2

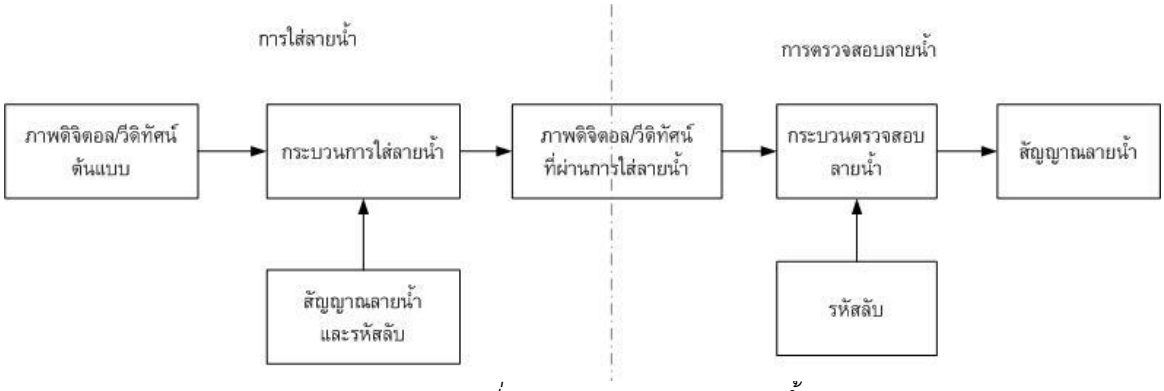
$$W(x,y)=I(x,y)+\alpha M(x,y) \qquad (2)$$

เมื่อ $I(x,y)$ คือข้อมูลต้นฉบับ

α คือพารามิเตอร์ที่ควบคุมระดับสัญญาณลายน้ำ

$M(x,y)$ คือ สัญญาณลายน้ำ

$W(x,y)$ คือ ข้อมูลต้นแบบที่ถูกฝังสัญญาณลายน้ำลงไปแล้ว



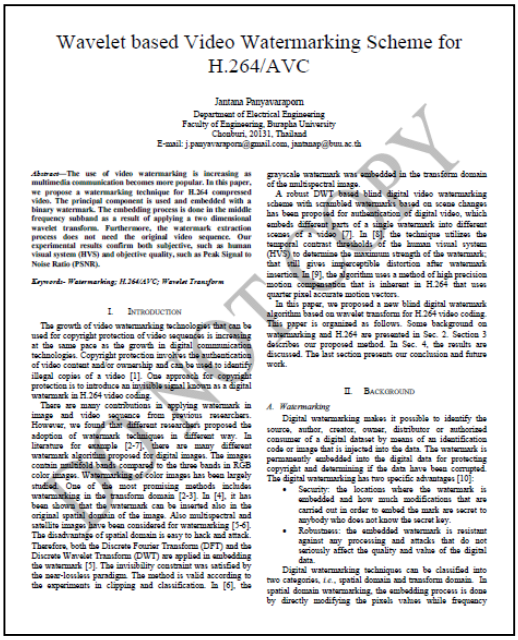
ภาพที่ 3 การฝังและตรวจสอบลายน้ำ

<u>การฝังสัญญาณลายน้ำในโดเมนเชิงพื้นที่</u>

ลายน้ำดิจิตอลชนิดที่มองเห็นได้ (Visible Watermark)

ขั้นตอนการฝังสัญญาณลายน้ำในรูปภาพหรือวีดิทัศน์ (พิจารณาวีดิทัศน์เพียง 1 เฟรมเท่านั้น) ดังแสดงในภาพที่ 3 หลักการคือ ฝังสัญญาณลายน้ำลงในตำแหน่ง (x,y) ที่ต้องการตามสมการที่ 2 ยกตัวอย่างเช่น ภาพที่ 4(ก) การฝังสัญญาณลายน้ำด้วยการติดโลโก้ในรูปถ่ายส่วนตัว และภาพที่ 4(ข) การฝังสัญญาณลายน้ำในเอกสาร สังเกตว่าสัญญาณลายน้ำลักษณะนี้โดยส่วนใหญ่เป็นสัญญาณลายน้ำแบบมองเห็นได้ ด้วยเหตุผลที่ว่าการฝังสัญญาณลายน้ำในโดเมนเชิงพื้นที่ ทำให้ข้อมูลต้นแบบเกิดการสูญเสียหรืออาจกล่าวอีกนัยหนึ่งได้ว่าข้อมูลมีความเปลี่ยนแปลงอย่างเห็นได้ชัด

4(ก)



Wavelet based Video Watermarking Scheme for H.264/AVC

Jantana Panyavaraporn
Department of Electrical Engineering
Faculty of Engineering, Burapha University
Chonburi, 20131, Thailand
E-mail: j.panyavaraporn@gmail.com, jantanap@buu.ac.th

Abstract—The use of video watermarking is increasing as multimedia communication becomes more popular. In this paper, we propose a watermarking technique for H.264 compressed video. The principal component is used and embedded with a binary watermark. The embedding process is done in the middle frequency subband as a result of applying a two dimensional wavelet transform. Furthermore, the watermark extraction process does not need the original video sequence. Our experimental results confirm both subjective, such as human visual system (HVS) and objective quality, such as Peak Signal to Noise Ratio (PSNR).

Keywords- Watermarking; H.264/AVC; Wavelet Transform

I. INTRODUCTION

The growth of video watermarking technologies that can be used for copyright protection of video sequences is increasing at the same pace as the growth in digital communication technologies. Copyright protection involves the authentication of video content and/or ownership and can be used to identify illegal copies of a video [1]. One approach for copyright protection is to introduce an invisible signal known as a digital watermark in H.264 video coding.

There are many contributions in applying watermark in image and video sequence from previous researchers. However, we found that different researchers proposed the adoption of watermark techniques in different way. In literature for example [2-7], there are many different watermark algorithm proposed for digital images. The images contain pixel-field bands compared to the three bands in RGB color images. Watermarking of color images has been largely studied. One of the most promising methods includes watermarking in the transform domain [2-3]. In [4], it has been shown that the watermark can be inserted also in the original spatial domain of the image. Also multispectral and satellite images have been considered for watermarking [5-6]. The disadvantage of spatial domain is easy to hack and attack. Therefore, both the Discrete Fourier Transform (DFT) and the Discrete Wavelet Transform (DWT) are applied in embedding the watermark [7]. The invisibility constraint was satisfied by the near-lossless paradigm. The method is valid according to the experiments in clipping and classification. In [6], the grayscale watermark was embedded in the transform domain of the multispectral image.

A robust DWT based blind digital video watermarking scheme with scrambled watermarks based on scene changes has been proposed for authentication of digital video, which embeds different parts of a single watermark into different scenes of a video [7]. In [8], the technique utilizes the temporal contrast thresholds of the human visual system (HVS) to determine the maximum strength of the watermark; that still gives imperceptible distortion after watermark insertion. In [9], the algorithm uses a method of high precision motion compensation that is inherent in H.264 that uses quarter pixel accurate motion vectors.

In this paper, we proposed a new blind digital watermark algorithm based on wavelet transform for H.264 video coding. This paper is organized as follows. Some background on watermarking and H.264 are presented in Sec. 2. Section 3 describes our proposed method. In Sec. 4, the results are discussed. The last section presents our conclusion and future work.

II. BACKGROUND

A. Watermarking

Digital watermarking makes it possible to identify the source, author, creator, owner, distributor or authorised consumer of a digital dataset by means of an identification code or image that is injected into the data. The watermark is permanently embedded into the digital data for protecting copyright and determining if the data have been corrupted. The digital watermarking has two specific advantages [10]:

- Security: the locations where the watermark is embedded and how much modifications that are carried out in order to embed the mark are secret to anybody who does not know the secret key.
- Robustness: the embedded watermark is resistant against any processing and attacks that do not seriously affect the quality and value of the digital data.

Digital watermarking techniques can be classified into two categories, *i.e.*, spatial domain and transform domain. In spatial domain watermarking, the embedding process is done by directly modifying the pixels values while frequency

4(ข)

ภาพที่ 4 ตัวอย่างการฝังสัญญาณลายน้ำชนิดที่มองเห็นได้ในโดเมนเชิงพื้นที่

ลายน้ำดิจิตอลชนิดที่ไม่สามารถมองเห็น (Invisible Watermark)

ยกตัวอย่างเช่น การฝังสัญญาณลายน้ำในบิตมีความสำคัญน้อยที่สุด (Least Significant Bit: LSB) ในภาพระดับเทา 8 บิต (0-255) โดยทำการฝังสัญญาณลายน้ำในตำแหน่งบิตที่ 8 สัญญาณลายน้ำที่ใช้เป็นภาพไบนารี หรือเรียกอีกชื่อว่าภาพขาวดำ ซึ่งขนาดของรูปภาพต้นแบบและสัญญาณลายน้ำต้องเท่ากัน ขั้นตอนการฝังสัญญาณลายน้ำมีดังนี้

1. แปลงค่าแต่ละจุดภาพในรูปภาพต้นแบบจาก เลขฐานสิบ เป็น เลขฐานสอง
2. เปรียบเทียบบิตสุดท้ายหรือตำแหน่งสุดท้ายของเลขฐานสองจากข้อ 1 กับภาพไบนารี แบ่งเป็น 4 กรณีดังนี้

บิตสุดท้ายของรูปภาพต้นแบบ	*ภาพไบนารีหรือลายน้ำดิจิตอล*	*รูปภาพที่ถูกฝังสัญญาณลายน้ำ*
0	0	ไม่เปลี่ยนแปลงค่า
0	1	เพิ่ม 1
1	0	ลด 1
1	1	ไม่เปลี่ยนแปลงค่า

สังเกตว่าตำแหน่งใดมีสัญญาณลายน้ำฝังอยู่ ค่าในบิตสุดท้ายจะเป็น 1 เสมอ การฝังสัญญาณลายน้ำวิธีนี้ไม่ทำให้รูปภาพเปลี่ยนแปลงไป เนื่องจากมีการเพิ่มหรือลดเพียงแค่ $-1, 0, +1$ เฉพาะบิตสุดท้ายเท่านั้นดังแสดงภาพที่ 5(ค)

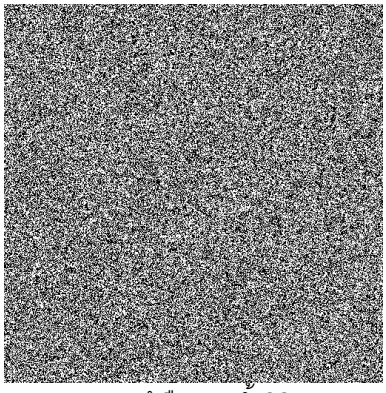

(ก) รูปภาพต้นแบบ (ข) ภาพไบนารีหรือลายน้ำดิจิตอล (ค) รูปภาพที่ถูกฝังสัญญาณลายน้ำ

ภาพที่ 5 ตัวอย่างการฝังสัญญาณลายน้ำชนิดที่ไม่สามารถมองเห็นในโดเมนเชิงพื้นที่

สำหรับการตรวจสอบหรือกู้คืนสัญญาณลายน้ำดิจิตอล มีหลักดังนี้

บิตสุดท้ายของรูปภาพที่ถูกฝังสัญญาณลายน้ำ	สัญญาณลายน้ำที่ตรวจสอบได้
0	0
1	1

สัญญาณลายน้ำที่กู้คืนได้เหมือนกับสัญญาณลายน้ำก่อนฝังในรูปภาพต้นแบบ แต่ถ้าในรูปภาพมีสัญญาณรบกวนชนิดเกาส์เซียน (ภาพที่ 6(ก)) การใช้วิธีนี้ไม่สามารถกู้คืนสัญญาณลายน้ำได้ ดังแสดงในภาพที่ 6(ข) ข้อเสียของการฝังลายน้ำในเชิงพื้นที่ คือไม่ทนต่อการถูกโจมตีเชิงสัญญาณ เช่น สัญญาณรบกวน การกรองสัญญาณ ฯลฯ แต่ข้อดีของการฝังลายน้ำในเชิงพื้นที่ คือทนทานต่อการโจมตีเชิงเรขาคณิต (ภาพที่ 6(ค-ง)) เช่น การหมุนภาพ การตัดภาพ เป็นต้น

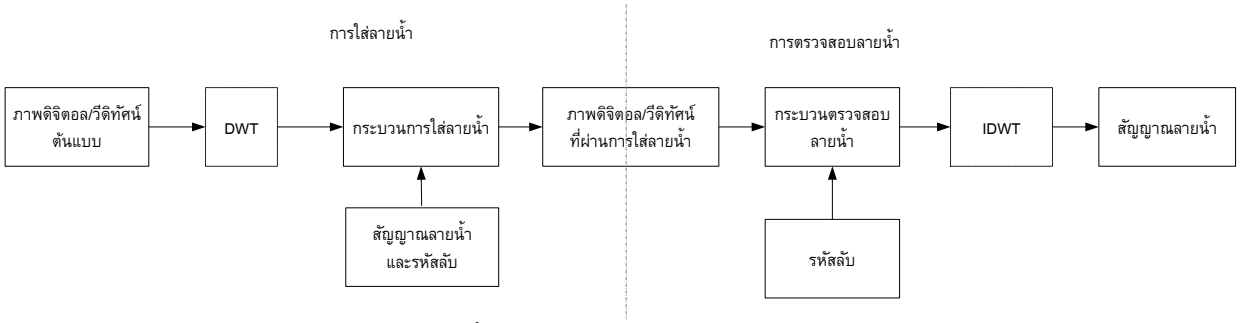
(ก) สัญญาณรบกวนชนิดเกาส์เซียน (ข) กู้คืนลายน้ำดิจิตอล

(ค) หมุน 15 องศา (ง) กู้คืนลายน้ำดิจิตอล

ภาพที่ 6 การกู้คืนลายน้ำดิจิตอลเมื่อถูกโจมตี

<u>การฝังสัญญาณลายน้ำในโดเมนความถี่</u>

การฝังสัญญาณลายน้ำในโดเมนความถี่ส่วนใหญ่เป็นลายน้ำดิจิตอลชนิดที่ไม่สามารถมองเห็นได้ (Invisible Watermark) จากกระบวนการฝังและตรวจสอบสัญญาณลายน้ำในภาพที่ 3 ทำการเพิ่มขั้นตอนการแปลงข้อมูลต้นแบบ (รูปภาพ/วีดิทัศน์) ให้อยู่ในโดเมนความถี่ เช่น การแปลงโคไซน์แบบไม่ต่อเนื่อง (Discrete Cosine Transform: DCT) การแปลงเวฟเล็ตแบบไม่ต่อเนื่อง (Discrete Wavelet Transform: DWT) หรือ การแปลงฟูริเยร์แบบไม่ต่อเนื่อ(Discrete Fourier Transform: DFT) เป็นต้น และในส่วนก่อนตรวจสอบลายน้ำทำการเพิ่มขั้นตอนการแปลงกลับ เช่น ในกรณีที่แปลงข้อมูลโดยใช้ DWT ต้องทำการแปลงกลับโดยใช้ IDWT (Inverse Discrete Wavelet Transform) ดังแสดงในภาพที่ 7 ในหัวข้อถัดไปแสดงตัวอย่างขั้นตอนการฝังสัญญาณลายน้ำและการตรวจสอบสัญญาณลายน้ำในโดเมนเวฟเล็ต



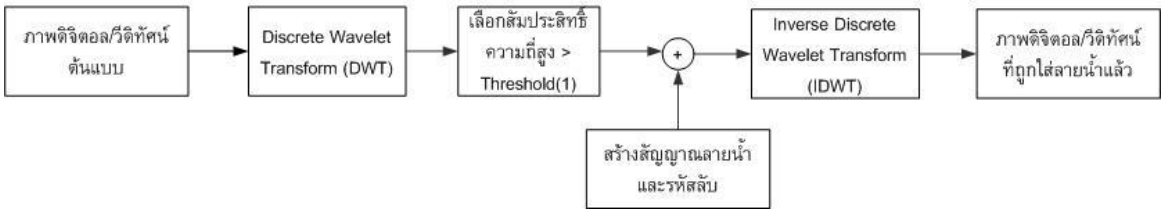
ภาพที่ 7 การฝังและตรวจสอบลายน้ำในโดเมนความถี่โดยใช้การแปลงเวฟเล็ตแบบไม่ต่อเนื่อง (DWT)

ตัวอย่างการฝังสัญญาณลายน้ำในโดเมนเวฟเล็ต เมื่อสัญญาณลายน้ำเป็นตัวเลขแบบสุ่ม
(จันทนา ปัญญาวราภรณ์, 2554)

<u>ขั้นตอนการฝังสัญญาณลายน้ำ</u>

การฝังลายน้ำด้วยเทคนิคการกำหนดค่าเทรโชลด์แบบคงที่ดังแสดงในภาพที่ 8 โดยนำข้อมูลต้นแบบมาทำการแปลง DWT สามารถจำแนกออกมาเป็นแถบความถี่ย่อย LL_n, LH_n, HL_n, HH_n $(n = 1, 2,\ldots, N)$ ซึ่งสามารถแยกองค์ประกอบได้ถึง N ระดับ จากนั้นเลือกใช้สัมประสิทธิ์ในส่วนของแถบความถี่สูง LH_n, HL_n, HH_n สัญญาณลายน้ำจะถูกรวมกับสัมประสิทธิ์ส่วนนี้

เท่านั้น กำหนดค่าเทรโชลด์ (T1) ที่น้อยกว่าค่าสัมประสิทธิ์ความถี่สูง จากนั้นรวมสัญญาณลายน้ำและรหัสลับตามสมการที่ 2 ขั้นตอนสุดท้ายจึงทำการแปลงข้อมูลกลับด้วย IDWT ผลลัพธ์ที่ได้คือ ภาพที่ถูกฝังด้วยสัญญาณลายน้ำแบบมองไม่เห็นดังแสดงในภาพที่ 9(ข)



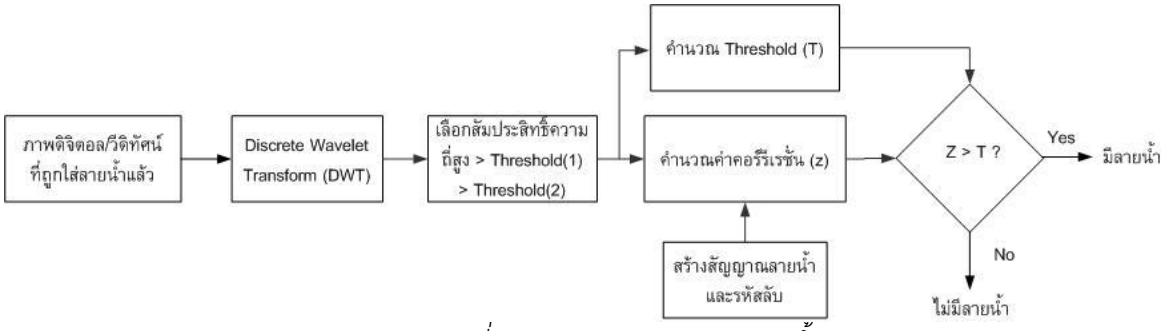
ภาพที่ 8 การฝังลายน้ำดิจิตอลด้วยเทคนิคการกำหนดค่าเทรโชลด์แบบคงที่

(ก) (ข)

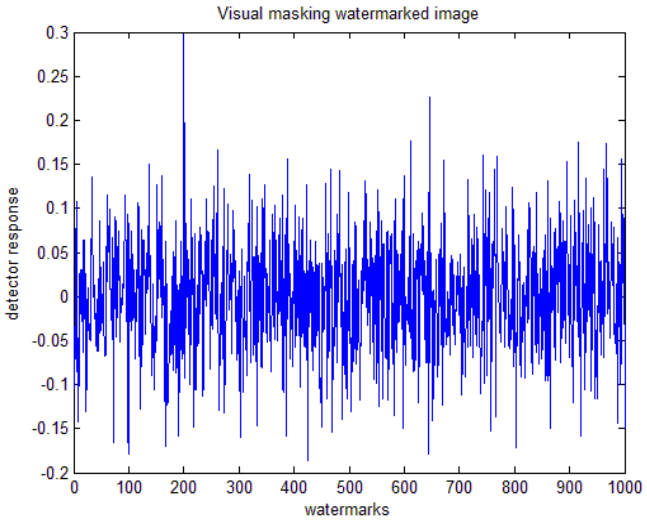
ภาพที่ 9 Akiyo (ก) ภาพต้นแบบ (ข) ภาพที่ถูกฝังสัญญาณลายน้ำ (จันทนา ปัญญาวราภรณ์, 2554)

ขั้นตอนการตรวจสอบสัญญาณลายน้ำ

การตรวจหาสัญญาณลายน้ำมีขั้นตอนดังแสดงในภาพที่ 10 ขั้นแรกนำภาพที่ฝังสัญญาณลายน้ำมาแยกองค์ประกอบภาพระดับ *n* โดยแยกองค์ประกอบถึงระดับเดียวกันกับขั้นตอนการฝังสัญญาณลายน้ำ เลือกใช้สัมประสิทธิ์ในส่วนของแถบความถี่สูง LH_n, HL_n, HH_n และกำหนดค่าเทรโชลด์เป็น T2 ค่าเทรโชลด์ที่ได้จะทำการแยกสัมประสิทธิ์ส่วนที่มีสัญญาณลายน้ำออกมาเพื่อนำมาหาค่าคอร์รีเรชันระหว่างสัญญาณลายน้ำที่ผิดเพี้ยนไปกับสัญญาณลายน้ำต้นฉบับ ได้กำหนดให้ค่า $T2 \geq T1$ เนื่องจากไม่ควรคอรีเรทสัญญาณลายน้ำต้นฉบับกับสัมประสิทธิ์ส่วนเกินที่สัญญาณลายน้ำไม่ได้รวมเข้าไป และเพื่อความคงทนเพราะค่าสัมประสิทธิ์บางค่าจากภาพต้นแบบอาจมีค่าต่ำกว่า T1 หรือมากกว่า T1 ภายหลังจากถูกโจมตีทำให้ข้อมูลผิดเพี้ยนไป ค่าเทรโชลด์ของการตรวจหาสัญญาณลายน้ำและค่าคอร์รีเลชันระหว่างสัญญาณลายน้ำกับค่าสัมประสิทธิ์ของ $W(x,y)$ เป็นตัวบอกว่าภาพที่นำมาทดสอบมีลายน้ำอยู่หรือไม่ ผลการทดลองจากภาพที่ 11 เป็นกราฟที่ได้จากการตรวจสอบสัญญาณลายน้ำ โดยตั้งค่าเทรโชลด์ไว้ที่ 30 จะสังเกตเห็นว่าที่ตำแหน่ง 200 เส้นกราฟจะขึ้นสูงผิดปกติ ซึ่งจุดนี้เป็นจุดที่ฝังรหัสลับเข้าไปในขั้นตอนการฝังสัญญาณลายน้ำ ผลการทดลองนี้แสดงให้เห็นว่าวิธีนี้สามารถตรวจหาสัญญาณลายน้ำได้อย่างแม่นยำ



ภาพที่ 10 การตรวจหาสัญญาณลายน้ำ



ภาพที่ 11 ผลการทดสอบสัญญาณลายน้ำ (จันทนา ปัญญาวราภรณ์, 2554)

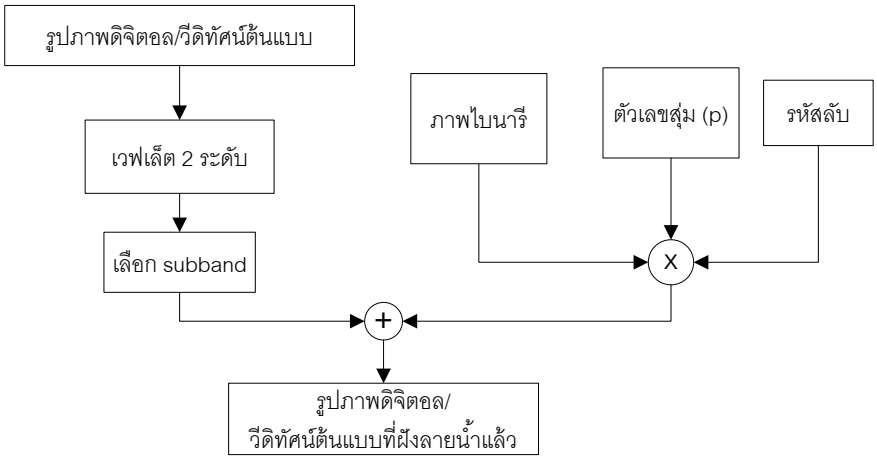
ตัวอย่างการฝังลายน้ำในโดเมนเวฟเล็ต เมื่อสัญญาณลายน้ำเป็นภาพไบนารี *(Panyavaraporn, 2011)*

ขั้นตอนการฝังสัญญาณลายน้ำ

ขั้นตอนการฝังสัญญาณลายน้ำแสดงในภาพที่ 12 โดยนำข้อมูลภาพ/วีดิทัศน์ต้นแบบมาทำการแปลงเวฟเล็ตแบบไม่ต่อเนื่อง (DWT) 2 ระดับ จากนั้นเลือกใช้สัมประสิทธิ์ในส่วนของแถบความถี่สูง LH_2 HL_2 และ HH_2 สัญญาณลายน้ำที่สังเกตเห็นได้มีผลมาจากตำแหน่งของสัญญาณลายน้ำที่ใส่ในแต่ละแถบความถี่ของการแปลงเวฟเล็ต ด้วยเหตุผลนี้จึงเลือกแทรกสัญญาณลายน้ำลงในองค์ประกอบความถี่สูงของภาพทำให้มีความคงทนต่อการเสียหายของสัญญาณลายน้ำ

ลายน้ำดิจิตอลที่ใช้เป็นภาพไบนารี (S_i) (ดังแสดงในภาพที่ 13(ค)) ทำการแปลงภาพไบนารี โดย ข้อมูล(ฉากหน้า)ให้มีค่าเป็น 1 และพื้นหลังให้มีค่าเป็น -1 ตัวเลขแบบสุ่ม (P_i) สร้างขึ้นมาโดยใช้ค่า Seed เป็นกุญแจลับ ในการสร้างตัวเลขแบบสุ่มนี้ขึ้นมา โดยการเพิ่มลำดับแบบสุ่มลงไปในรูปภาพดิจิตอล/วีดิทัศน์ที่ต้องการฝังสัญญาณลายน้ำ และการตรวจหาสัญญาณลายน้ำจะต้องทำการสร้างลำดับตัวเลขแบบสุ่มขึ้นมาใหม่โดยใช้ค่า Seed เดิม โดยค่าของตัวเลขแบบสุ่มคือ 1 และ -1 ดังนั้นลำดับที่ใช้นั้นจึงไม่ควรง่ายเกินไปเพื่อให้การคาดเดาทำได้ยากและเป็นการรักษาความปลอดภัยจากผู้ที่ไม่ได้รับสิทธิ์

จากนั้นรวมลำดับสัญญาณลายน้ำ เข้ากับสัมประสิทธิ์ในแถบความถี่ที่เลือก ดังในสมการที่ 2 สัญญาณลายน้ำจะไม่ถูกรวมเข้าทุกตำแหน่ง ขั้นตอนสุดท้ายจึงทำการแปลงข้อมูลกลับ ดังแสดงตัวอย่างรูปภาพต้นแบบและภาพที่ถูกฝังด้วยสัญญาณลายน้ำดังแสดงในภาพที่ 13 (ก)-(ข)



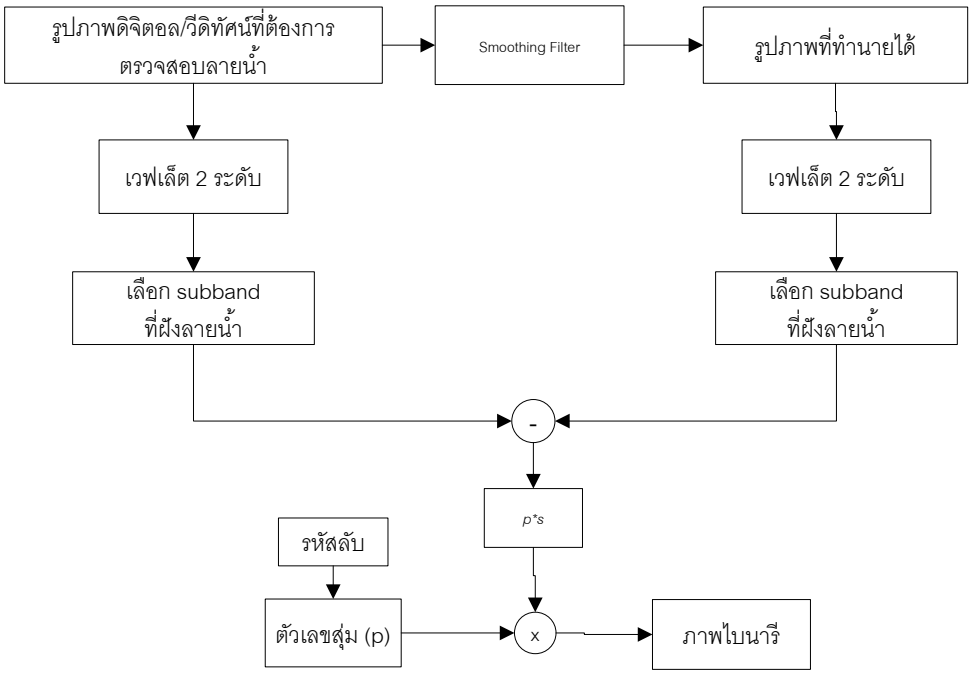
ภาพที่ 12 ขั้นตอนการฝังสัญญาณลายน้ำ

(ก) (ข) (ค) (ง)

ภาพที่ 13 Akiyo (ก) ภาพต้นแบบ (ข) ภาพที่ถูกฝังสัญญาณลายน้ำ (ค) ภาพไบนารี (ง) ภาพไบนารีหลังการตรวจสอบ (Panyavaraporn, 2011)

<u>ขั้นตอนการตรวจสอบสัญญาณลายน้ำ</u>

การตรวจสอบสัญญาณลายน้ำ (ดังแสดงในภาพที่ 14) ไม่จำเป็นต้องใช้รูปภาพดิจิตอลหรือวีดิทัศน์ต้นแบบในการตรวจสอบ หลักการคือทำนายค่าจริงของจุดภาพโดยใช้วิธีคอนโวลูชัน (Convolution) กับค่าสัมประสิทธิ์ $W(x,y)$ โดยใช้ตัวกรองขนาด 3x3 จุดภาพในการตรวจสอบสัญญาณลายน้ำ จำเป็นต้องรู้ลำดับตัวเลขแบบสุ่มเดิม (P) ที่เลือกใช้ในการฝังสัญญาณลายน้ำ ถ้าใส่ค่าผิดภาพที่ถูกฝังสัญญาณลายน้ำที่แปลงกลับมาจะใช้ไม่ได้เช่นกัน



ภาพที่ 14 ขั้นตอนการตรวจสอบสัญญาณลายน้ำ

การวัดประสิทธิภาพของลายน้ำดิจิตอล

เครื่องมือพื้นฐานที่ใช้เปรียบเทียบคุณภาพของข้อมูลต้นแบบและข้อมูลที่ผ่านการฝังลายน้ำแล้วคือ PSNR (Peak Signal to Noise Ratio) สามารถคำนวณได้จากสมการที่ 3

$$PSNR = 10\log\frac{\left(2^{b} - 1\right)}{MSE} \tag{3}$$

เมื่อ *b* คือจำนวนของบิตที่ถูกใช้ในแต่ละจุดภาพ และ *MSE* (Mean Square Error) คำนวณจากสมการที่ 4

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(O(i,j) - \mathrm{R}(i,j)\right)^{2} \tag{4}$$

$M \times N$ คือขนาดของข้อมูล $O(i,j)$คือค่าจุดภาพต้นแบบ และ $\mathrm{R}(i,j)$คือภาพที่ผ่านการฝังลายน้ำ

เครื่องมืออีกชนิดที่ใช้ในการวัดความเหมือนระหว่างภาพลายน้ำดิจิตอลต้นแบบ(S_i)และภาพลายน้ำดิจิตอลที่ได้จากการกู้คืนหรือจากขั้นตอนการตรวจสอบ(S_i') คือ normalized correlation (*NC*) สามารถคำนวณได้จากสมการที่ 5

$$NC = \frac{\sum S_i S_i'}{\sum S_i^{2}} \tag{5}$$

การวัดคุณภาพของลายน้ำดิจิตอลที่สำคัญอีกประเภทหนึ่งคือการวัดโดยใช้ความรู้สึกจากการมองของมนุษย์ หรือเรียกว่า Human Visual System

สรุป

สัญญาณลายน้ำที่ฝังในโดเมนเชิงพื้นที่จะเกิดการสูญหายเมื่อผ่านการโจมตีเชิงสัญญาณ เช่นการกรองสัญญาณ แต่การฝังสัญญาณลายน้ำลักษณะดังกล่าวมีข้อดีคือจะทนทานต่อการโจมตีเชิงเรขาคณิต เช่น การหมุนภาพ การตัดภาพ เป็นต้น ในทางตรงกันข้ามสัญญาณลายน้ำที่ถูกฝังในโดเมนความถี่จะทนทานต่อการกรองสัญญาณความถี่ต่ำ การกรองสัญญาณความถี่สูง และการบีบอัด เป็นต้น ดังนั้นควรเลือกลายน้ำดิจิตอลตามจุดประสงค์ในการใช้งาน ยกตัวอย่างเช่น ในงานที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์ควรใช้สัญญาณลายน้ำที่ทนทานต่อการถูกโจมตี (Robust Watermarking) ส่วนงานประเภทที่ต้องการความน่าเชื่อถือของข้อมูลควรใช้สัญญาณลายน้ำที่เปราะบาง (Fragile Watermarking) เพื่อเป็นการยืนยันว่าข้อมูลเป็นของแท้ไม่ได้ผ่านการเปลี่ยนแปลงและแก้ไข

เอกสารอ้างอิง

จันทนา ปัญญาวราภรณ์. (2554). เทคนิคการใส่ลายน้ำในเวฟเล็ตโดเมนด้วยเทคนิคการกำหนดค่าเทรโชลด์แบบคงที่สำหรับวีดิทัศน์. ในการประชุมวิชาการทางวิศวกรรมไฟฟ้าครั้งที่ 34. (หน้า 1009 -1012).

Andersonand, R. J., Petiicolus, F. (1998). On the limits of steganography. In *IEEE Journal on Selected Areas in Communication*, *16* , 474-481.

Bouslimi, D., Coatrieux, G., Cozic, M. and Roux, C. (2012). A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images. **In** *IEEE Transactions on Information Technology in Biomedicine.* V.16, No.5, pp. 891-899.

Chen, W.-M., Lai, C.-J., Wang, H.-C., Chao, H.-C. and Lo, C.-H. (2011). H.264 video watermarking with secret image sharing . In *IET Image Processing.* V.5, No.4, pp. 349-354.

Cheung, W. N. (2000). Digital image watermarking in spatial and transform domains. In *Proc. TENCON*. (pp. 374-378).

Chimanna, M.A. and Khot, S.R. (2013). Robustness of video watermarking against various attacks using Wavelet Transform techniques and Principle Component Analysis. In *Proc. of International Conference on Information Communication and Embedded Systems.* (pp. 613-618).

Cox, J. and Killian, J. (1997). Secure Spread Spectrum Watermarking or Multimedia. In *IEEE Trans. Image Proc.* V.6, No.12, pp.1673-1687.

Dharwadkar, N.V. and Amberker, B.B. (2013). An adaptive gray-scale image watermarking scheme using smooth and edge areas of an image. In *Proceeding of Intelligent Systems and Signal Processing.* (pp. 66-71).

Divecha, N. and Jani, N.N. (2003). Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images. In *Proceeding of Intelligent Systems and Signal Processing*. (pp. 204-208).

Hartumg, F. (1999). Spread Spectrum Watermarking: Malicious Attacks and Counter Attacks. In *Proceeding of SPI3657: Security and Watermarking of Multimedia contents*. (pp. 25-27).

Jassim, T., Abd-Alhameed, R. and Al-Ahmad, H. (2013). New Robust and Fragile Watermarking Scheme for Colour Images Captured by Mobile Phone Cameras . In *Proceeding of Computer Modelling and Simulation*. (pp. 465-469)

Kunhu, Alavi and Al-Ahmad, Hussain, (2013). Multi watermarking algorithm based on DCT and hash functions for color satellite images. In *Proceeding of Innovations in Information Technology*. (pp. 21-27).

Kutter, M., Petitcolas, and F. A. (1999). A Fair Benchmark for Image Watermarking Systems. In *Proceeding of Electronic Imaging*: *Security and Watermarking of Multimedia Contents.* V.3657. pp. 226-239.

Majumder, S., Devi, K.J. and Sarkar, S.K. (2013). Singular value decomposition and wavelet-based iris biometric watermarking. . In *IET Biometrics.* V.2, No.1, pp. 21-27.

Panyavaraporn, J. (2011). Wavelet based Video Watermarking Scheme for H.264/AVC. In *Proc. Intelligent Signal Processing and Communication System*. (pp. 1-5).

Peticolas, F. A. (1999). Information Hiding – A Survey. In *Proceeding of the IEEE*, Special issue on Protection of Multimedia Contents. V.89, No.4, pp. 1062-1078.

Podilchuk, C. I., Delp, E.J. (2001). Digital watermarking algorithms and applications. In *Proc. IEEE Signal Processing Magazine*. (pp. 33-46).

Rangsanseri, Y., Panyavaraporn, J., Thitimajshima, P. (2005). PCA/Wavelet Based Watermarking of Multispectral Images. In *Proc 2005 International Symposium on Remote Sensing*.

Rosiyadi, D., Shi-Jinn Horng., Pingzhi Fan, Xian Wang, Khan, M.K. and Yi Pan. (2012). Copyright Protection for E-Government Document Images. In *IEEE Multimedia*. V.19, No.3, pp. 62-73.

Verma, A.K., Singhal, M. and Patvardhan, C. (2013). Robust temporal video watermarking using YCbCr color space in Wavelet domain. In *Proc IEEE 3rd International Advance Computing Conference*. (pp.1195-1200).

Walia, E. and Suneja, A. (2013). Fragile and blind watermarking technique based on Weber's law for medical image authentication. In *IET Computer Vision.* V.7, No.1, pp. 9-19.

Wolfgang, R. B., Podilchuk, C.I., & Delp., E.J. (1999). Perceptual watermarks for digital images and video. In *Proc. IEEE*. (pp. 1108-1126).