

ประสิทธิภาพของวิธีการตรวจสอบภาพถ่ายที่ผ่านการปลอมแปลงแบบคัดลอกและปกปิด An Efficient of Image Detection Method for Copy-Move Forgery

ณัฐพล ชัยทวีธาณันท์^{1*}
Nattapol Chaitawittanun^{1*}

บทคัดย่อ

การปลอมแปลงแบบคัดลอกและปกปิด (Copy-move) เป็นการปลอมแปลงภาพชนิดหนึ่ง การปลอมแปลงลักษณะนี้จะทำการคัดลอกและวางลงที่ส่วนใดส่วนหนึ่งในภาพ ในบทความนี้จะทำการอธิบายการตรวจสอบภาพถ่ายที่ถูกทำการปลอมแปลงแบบ Copy-move ด้วยวิธีการ JPEG Copy-move Detection (JCD) การทำงานของเทคนิคนี้จะเริ่มจากการลดสีของภาพถ่ายลง หลังจากนั้นทำการแบ่งภาพออกเป็นบล็อก และตรวจสอบค่าสีของแต่ละบล็อก หากกลุ่มที่เหมือนด้วยเทคนิคการแบ่งกลุ่มข้อมูล ผลการทดลองแสดงให้เห็นว่าวิธีการ JCD ที่ใช้ตรวจสอบกับภาพ JPEG ให้ผลลัพธ์ที่มีความถูกต้อง 64.36 เปอร์เซ็นต์

คำสำคัญ : การปลอมแปลงภาพถ่าย การตรวจสอบภาพถ่าย คัดลอกและปกปิด

Abstracts

Copy-move forgery is a type of image forgery, in which a part of image is copied and pasted in the same image. This paper describes detecting Copy-move by JPEG Copy-move Detection (JCD) method. Our technique works by first degrading color palette. Then the image is spilt into small $N \times N$ blocks and checks the color of each block. These duplicated blocks are identified using clustering technique. Experimental results have shown the accuracy of JCD method is 64.36 %.

Keywords : Image Forgery, Image Verifiability, Copy-move, JCD

¹ อ. , สาขาวิชาเทคโนโลยีคอมพิวเตอร์อุตสาหกรรม คณะเทคโนโลยีการเกษตร มหาวิทยาลัยราชภัฏเพชรบูรณ์ 67000

* Corresponding author : E-mail: nattapol_ctwtm@hotmail.com Tel. 056-717151 ext. 1444

จากงานประชุมวิชาการระดับชาติ มหาวิทยาลัยทักษิณ ครั้งที่ 22 ปี 2555

บทนำ

การถ่ายภาพเป็นกิจกรรมที่ได้รับความนิยมและสามารถทำได้ทุกที่ซึ่งทำให้กิจกรรมประเภทนี้มีผู้สนใจเพิ่มมากขึ้น ทั้งนี้เนื่องจากกล้องดิจิทัลซึ่งใช้เป็นอุปกรณ์หลักสำหรับการบันทึกภาพในปัจจุบันได้มีการพัฒนาขีดความสามารถให้เทียบเท่าหรือดีกว่ากล้องแบบเดิมที่ใช้ฟิล์ม โดยกล้องดิจิทัลนั้นมีราคาถูกและมีความสะดวกในการใช้งาน ซึ่งสามารถบันทึกภาพลงหน่วยความจำและแสดงผลพร้อมหลังการถ่ายภาพได้ทันที [1] ทำให้ภาพดิจิทัลดังกล่าวถูกนำไปใช้งานอย่างแพร่หลายในสื่อชนิดต่างๆ ได้แก่ หนังสือพิมพ์ นิตยสาร หรือบนเครือข่ายอินเทอร์เน็ต รวมถึงยังมีการนำภาพจากกล้องดิจิทัลไปใช้ประกอบเป็นหลักฐานในการพิจารณาคดี [2] ภาพถ่ายที่บุคคลทั่วไปได้มีการบันทึกไว้นั้นบางส่วนอาจจะมีการบันทึกเหตุการณ์สำคัญต่างๆ ซึ่งภาพที่บันทึกได้เหล่านั้นถูกนำมาใช้ประโยชน์เพื่อเป็นเครื่องมือยืนยันและสามารถใช้เป็นหลักฐานสำคัญในการกำหนดบทลงโทษกับบุคคลในรูปมีส่วนเกี่ยวข้องกับเหตุการณ์นั้นๆ หรือเพื่อยืนยันความบริสุทธิ์จากกรณีที่มีผู้อื่นฟ้องร้อง ซึ่งในประเด็นของการนำภาพไปใช้เป็นหลักฐานในการพิจารณาคดีนั้น ในปัจจุบันอาจเกิดข้อกังขาว่าภาพที่นำมาใช้งานเป็นภาพที่ผ่านการปลอมแปลงมาหรือไม่ [3] การคัดแปลง ปลอมแปลง หรือตัดต่อภาพถ่ายดิจิทัลกำลังกลายเป็นวัฒนธรรมอันตรายที่แพร่ระบาดในโลกอินเทอร์เน็ตอย่างน่ากลัว คนดัง ดารา นักการเมือง หรือแม้แต่ชาวบ้านสามารถเป็นเหยื่อของการตัดต่อภาพถ่ายดิจิทัลได้ทั้งสิ้น [4] การปลอมแปลงภาพอาจมีวัตถุประสงค์เพื่อก่อให้เกิดการเข้าใจผิด เพื่อกำไรใส่ร้ายป้ายสีผู้อื่น หรือเพื่อบิดเบือนความจริง โดยส่งผลให้เกิดการเสื่อมเสียต่อชื่อเสียง และความน่าเชื่อถือของผู้ที่มีส่วนเกี่ยวข้อง ตลอดจนอาจก่อให้เกิดเป็นคดีความขึ้นได้

ในบทความนี้นำเสนอวิธีการตรวจสอบการปลอมแปลงแบบ Copy-move ส่วนที่ 2 จะเป็นการอธิบายลักษณะของการปลอมแปลงภาพ ส่วนที่ 3 จะทำการเสนอเทคนิคการตรวจสอบด้วยวิธีการ JPEG Copy-move Detection ส่วนที่ 4 เป็นการแสดงผลที่ได้จากการตรวจสอบ และส่วนสุดท้ายเป็นการสรุปผลการวิจัย

ลักษณะการปลอมแปลงภาพ

ประเภทของการปลอมแปลงภาพที่พบมากในปัจจุบันมี 2 ประเภทได้แก่ การคัดลอกและปกปิด (Copy-move) และการผสมผสานภาพเพื่อให้เกิดความหมายใหม่ (Image Splicing) ลักษณะการปลอมแปลงด้วยวิธี Copy-move เกิดจากการคัดลอกส่วนใดส่วนหนึ่งในภาพมาวางทับยังตำแหน่งที่ต้องการจะปกปิด ส่วนใหญ่การปลอมแปลงลักษณะนี้จะกระทำกับวัตถุ บุคคล และจุดสังเกตที่สำคัญ เพื่อไม่ให้ปรากฏภายในภาพดังภาพที่ 1



(a)



(b)

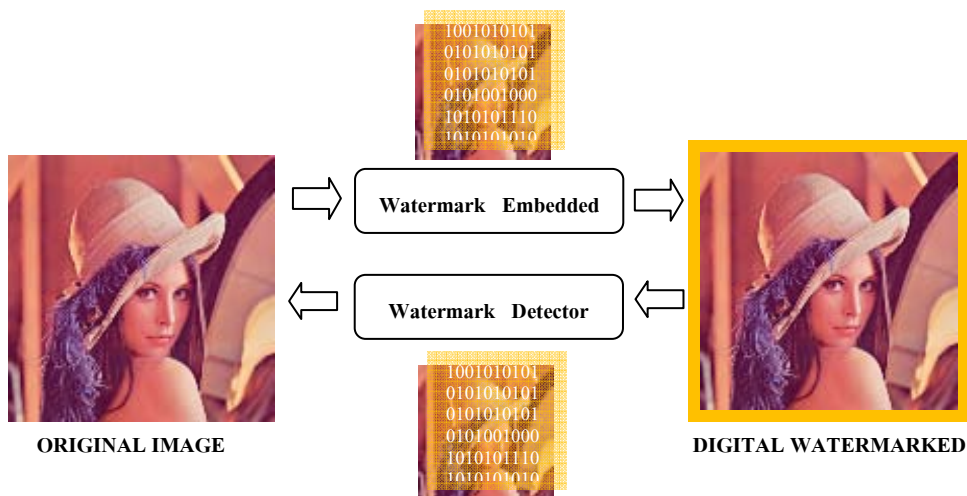
ภาพที่ 1 ลักษณะการปลอมแปลง Copy-move (a) ภาพต้นฉบับ (b) ภาพที่ถูกปลอมแปลงด้วยการนำต้นไม้ปิดบังถังขยะ

การปลอมแปลงแบบ Image splicing เกิดจากการนำส่วนใดส่วนหนึ่งจากภาพอื่นที่ไม่ใช่ภาพต้นแบบนำมาวางในภาพต้นฉบับเป็นการจงใจทำเพื่อต้องการสร้างภาพขึ้นมาใหม่และเปลี่ยนแปลงเนื้อหาของภาพต้นฉบับเดิม ซึ่งการปลอมแปลงลักษณะนี้จะต้องใช้ภาพตั้งแต่ 2 ภาพขึ้นไป [5] ตัวอย่างลักษณะการปลอมแปลงแสดงได้ดังภาพที่ 2



ภาพที่ 2 ลักษณะการปลอมแปลงแบบ Image splicing

วิธีการตรวจสอบภาพที่ใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการตรวจสอบแบ่งออกเป็น 2 ประเภทหลัก คือ แบบแอคทีฟ (Active) และแบบพาสซีฟ (Passive) [6] โดยกระบวนการตรวจสอบแบบแอคทีฟที่นั้นมีแนวคิดในการซ่อนข้อมูลลับบางอย่างไว้ภายในภาพก่อนที่จะนำไปใช้งานเพื่อสามารถทำการตรวจสอบได้ในภายหลังว่ามีภาพถ่ายดังกล่าวนั้นมีการถูกปลอมแปลงมาหรือไม่ ซึ่งวิธีการแบบแอคทีฟที่ได้รับความนิยมมีชื่อเรียกว่า การทำลายน้ำดิจิทัล (Digital Watermark) ดังภาพที่ 3 การซ่อนข้อมูลลงไปภายในภาพก่อนการนำไปใช้งานเพื่อที่จะสามารถตรวจสอบประวัติของภาพนั้นได้ในภายหลัง [7] แต่เทคนิคนี้ยังมีข้อจำกัดอยู่บางประการ เช่น ต้องใช้ผู้ที่มีความรู้เพื่อทำการฝังข้อมูลลับเข้าไปยังภาพก่อนที่จะนำภาพดังกล่าวไปใช้งาน ด้วยเหตุนี้วิธีการดังกล่าวจึงไม่เหมาะสมกับการนำมาใช้ในการตรวจสอบการปลอมแปลงของภาพที่เกิดจากการกระทำของบุคคลหลายกลุ่ม

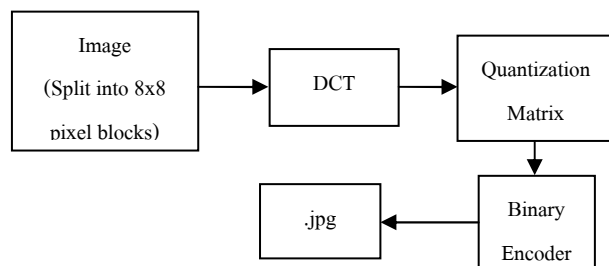


ภาพที่ 3 กระบวนการของการทำลายน้ำดิจิทัล

จากงานประชุมวิชาการระดับชาติ มหาวิทยาลัยทักษิณ ครั้งที่ 22 ปี 2555

ในขณะที่วิธีการแบบแพสซีฟไม่จำเป็นต้องมีขั้นตอนของการฝังข้อมูลลงในภาพถ่ายก่อน จึงเป็นวิธีที่เหมาะสมในการตรวจสอบรูปภาพได้ดีกว่า เนื่องจากโดยส่วนใหญ่แล้วภาพที่มีการนำมาปลอมแปลงจะไม่มีข้อมูลฝังลงในภาพก่อน แต่อย่างไรก็ตามการนำวิธีการแบบแพสซีฟมาใช้เพื่อตรวจสอบการปลอมแปลงของภาพนั้นผู้ที่ทำการตรวจสอบควรจะทราบจำแนกประเภทของการปลอมแปลงภาพอย่างคร่าว ๆ ได้ ว่าภาพดังกล่าวนั้นถูกปลอมแปลงมาจากวิธีการใด เพื่อให้สามารถเลือกใช้วิธีการตรวจสอบการปลอมแปลงของภาพดังกล่าวได้อย่างเหมาะสม

ไฟล์ภาพดิจิทัลที่ใช้งานอยู่ในปัจจุบันมีรูปแบบของการบีบอัดข้อมูล 2 แบบ คือการบีบอัดข้อมูลแบบมีการสูญเสีย (Lossy data compression) ซึ่งเกิดการสูญเสียข้อมูลเป็นบางส่วนในกระบวนการบีบอัดข้อมูล เมื่อทำการขยายขนาดของข้อมูลให้มีขนาดเท่าเดิมแล้วยังคงเหลือข้อมูลบางส่วนที่ยังไม่สูญเสียไป และการบีบอัดข้อมูลแบบไม่มีการสูญเสีย (Lossless data compression) ข้อมูลของภาพหลังการบีบอัดลักษณะนี้เมื่อนำมาขยายยังคงมีขนาดเท่าเดิมไม่เกิดการสูญเสียรายละเอียดของภาพแต่อย่างใด ภาพถ่ายจากกล้องดิจิทัลนั้นจะใช้การบีบอัดข้อมูลแบบมีการสูญเสียซึ่งข้อมูลบางส่วนที่ไม่มีความสำคัญจะเกิดการสูญเสียไปในระหว่างการบีบอัดข้อมูลและเมื่อขยายขนาดของข้อมูลออกมาแล้วข้อมูลที่มีความสำคัญก็จะยังคงอยู่ครบถ้วน ทำให้ฟังก์ชันการแปลงโคไซน์แบบไม่ต่อเนื่อง (Discrete Cosine Transform) กลายเป็นมาตรฐานของรูปแบบการบีบอัดข้อมูลหลาย ๆ แบบของข้อมูลภาพนิ่ง เช่น Joint Photographic Experts Group (JPEG) ตามภาพที่ 4

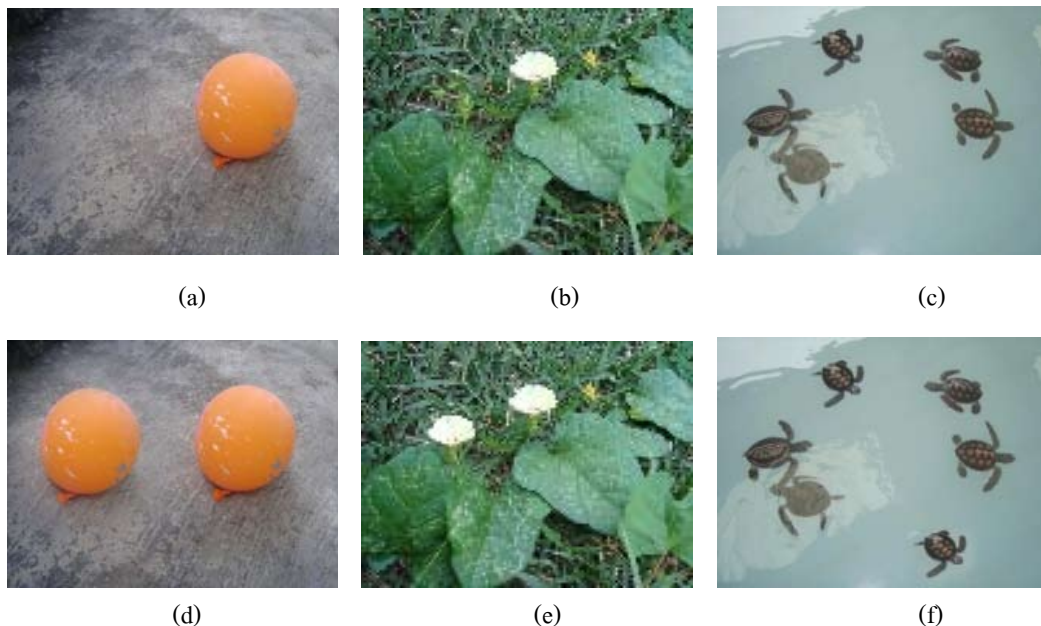


ภาพที่ 4 กระบวนการบีบอัดไฟล์ JPEG

ภาพประเภท JPEG เป็นไฟล์ภาพที่มีขนาดเล็กและคุณภาพของภาพถ่ายจัดอยู่ในระดับที่ดีจึงเป็นที่นิยมใช้งานบนอินเทอร์เน็ตและการถ่ายภาพในกล้องดิจิทัลทั่วไปอย่างแพร่หลาย การตรวจสอบภาพไฟล์ที่มีนามสกุล JPEG ที่ผ่านการปลอมแปลงในลักษณะ Copy-move จึงเป็นประเด็นที่น่าสนใจ เนื้อหาในส่วนถัดไปจะเป็นการนำเสนอเทคนิคที่ใช้ตรวจสอบภาพถ่าย JPEG

วิธีการวิจัย

การเตรียมข้อมูลเพื่อการตรวจสอบการตรวจสอบประสิทธิภาพของศึกษารุ่นนี้ผู้วิจัยได้ทำการทดสอบกับไฟล์ภาพนามสกุล JPEG จำนวน 20 ภาพ มีความละเอียดภาพที่ 512 x 384 และถูกการปลอมแปลงภาพแบบ Copy-move ด้วยโปรแกรม Adobe Photoshop CS4 ตัวอย่างภาพที่ถูกปลอมแปลง แสดงได้ดังภาพที่ 5



ภาพที่ 5 (a - c) ภาพต้นฉบับ (d - f) ภาพที่ปลอมแปลงด้วยเทคนิค Copy-move

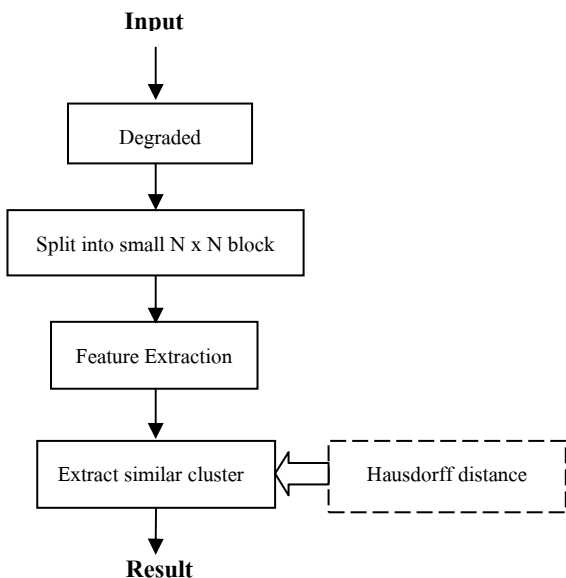
การตรวจสอบด้วยวิธีการ JCD

การตรวจสอบไฟล์ภาพที่ถูกปลอมแปลงมีนักวิจัยจำนวนมากไม่น้อยมุ่งเน้นพัฒนาการตรวจสอบ Fridrich *et al.* [8] ได้พัฒนาเทคนิคการตรวจสอบที่ทำการแบ่งภาพออกเป็นบล็อกซ้อนทับกัน (Overlapping) และใช้การแปลงโคไซน์แบบไม่ต่อเนื่อง (Discrete Cosine Transform : DCT) ดึงลักษณะเด่นของภาพออกมา หลังจากนั้นทำการเปรียบเทียบความคล้ายคลึงของบล็อก ซึ่งสอดคล้องกับวิธีการของ Popescu and Farid [9] ที่พัฒนาวิธีการโดยใช้ การวิเคราะห์องค์ประกอบหลัก (Principal Component Analysis : PCA) ส่งผลให้มีมิติของบล็อกที่ใช้ในการแสดงผลถูกลดจำนวนลง Farid and Bravo [10] เสนอความคิดเห็นเกี่ยวกับการใช้ระบบเกี่ยวกับการมองเห็นของมนุษย์ในการตรวจสอบการปลอมแปลง เช่น เงามของสิ่งของ การสะท้อนของวัตถุ และลักษณะการบิดเบือนของวัตถุ การตรวจสอบที่ถูกพัฒนาขึ้นจากนักวิจัยส่วนใหญ่จะพัฒนาในส่วนของการหาคุณลักษณะพิเศษด้วยเทคนิคที่แตกต่างกัน เช่น DCT PCA และ DWT วิธีการตรวจสอบไฟล์ภาพ JPEG จะมีขั้นตอนแรกคือ การแบ่งภาพออกเป็นบล็อกย่อยๆ และทำการหาคุณลักษณะพิเศษที่แตกต่างกันออกไป หลังจากนั้นจะทำการตรวจสอบคุณลักษณะพิเศษที่เหมือนกันด้วยการจำแนกแบบ Lexicographically

ในส่วนของผู้วิจัยได้ทำการพัฒนาระบบการตรวจสอบโดยใช้การจำแนกคุณลักษณะพิเศษด้วยวิธีการแบ่งกลุ่มข้อมูล มีขั้นตอนหลักดังนี้

- ขั้นตอนที่ 1 ลดจำนวนสีของภาพ
- ขั้นตอนที่ 2 แยกภาพออกเป็นบล็อกขนาด $N \times N$
- ขั้นตอนที่ 3 ตรวจสอบค่าสีของแต่ละบล็อกและทำการจัดกลุ่ม
- ขั้นตอนที่ 4 หากกลุ่มที่เหมือนกันด้วยวิธี Hausdorff distance

จากงานประชุมวิชาการระดับชาติ มหาวิทยาลัยทักษิณ ครั้งที่ 22 ปี 2555



ภาพที่ 6 ขั้นตอนกระบวนการตรวจสอบการปลอมแปลงภาพ

ขั้นตอนแรกของการตรวจสอบจะทำการเบลอภาพเพื่อจัดรายละเอียดของภาพและลดจำนวนสี หลังจากนั้นจะแบ่งภาพออกเป็นบล็อกพิกเซลย่อยๆ ขนาด $N \times N$ ซึ่งจะคล้ายคลึงกับวิธีการของ Fridrich [8] และทำการตรวจสอบค่าสีของแต่ละบล็อกเพื่อเข้าสู่ขั้นตอนการแบ่งกลุ่มและทำการตรวจสอบความคล้ายคลึงของกลุ่มข้อมูลที่ได้ ด้วยการวัดระยะห่างของกลุ่มข้อมูลด้วยเทคนิค Hausdorff Distance และขั้นตอนสุดท้ายจะแสดงแถบสีแดงบริเวณที่ตรวจสอบพบความเหมือนกันภายในภาพ

ผลการวิจัยและอภิปรายผล

ผลการตรวจสอบด้วยวิธี JCD

จากการตรวจสอบภาพถ่ายที่มีการปลอมแปลงลักษณะ Copy-move ด้วยวิธีการ JCD ของไฟล์ภาพแบบ JPEG สามารถแสดงตัวอย่างผลการทดสอบได้ดังภาพที่ 7



(a)



(b)



(c)



(d)



(e)



(f)

ภาพที่ 7 (a), (c), (e) ภาพที่ผ่านการปลอมแปลงแบบ Copy-move (b), (d), (f) ผลจากการตรวจสอบด้วยวิธีการ JCD

ผลลัพธ์ของการตรวจสอบภาพที่เกิดจากปลอมแปลงแบบ Copy-move ในภาพที่ 7 ภาพ (a) (c) และ (e) ที่ได้ทำการคัดลอกจุดสำคัญภายในภาพและนำมาวางยังตำแหน่งอื่น ผลจากการทดสอบสามารถแสดงตำแหน่งที่ตรวจสอบได้ดังภาพ (b) (d) และ (f) ซึ่งแสดงความเหมือนกันของบริเวณที่ถูกคัดลอก และตำแหน่งที่เคลื่อนย้ายไปปกปิดด้วยการทำเครื่องหมายสีแดงยังบริเวณที่ตรวจพบ ประสิทธิภาพของการตรวจสอบภาพด้วยวิธีการ JCD ที่นำมาทดลองทั้งหมดแสดง ดังตารางที่ 1

ตารางที่ 1 ค่า TPR และ Accuracy Rate ของวิธีการตรวจสอบ JCD

ชนิดไฟล์ภาพ	JCD	
	TPR	Accuracy Rate (%)
JPEG	0.9589	64.36

จากงานประชุมวิชาการระดับชาติ มหาวิทยาลัยทักษิณ ครั้งที่ 22 ปี 2555

ภาพถ่ายที่ถูกนำมาตรวจสอบด้วยวิธีการ JCD ผลการทดลองแสดงให้เห็นประสิทธิภาพในการตรวจสอบภาพที่มีการปลอมแปลงแบบ Copy-move ของไฟล์ภาพแบบ JPEG พบว่า สามารถแสดงตำแหน่งที่มีการปลอมแปลงได้อย่างถูกต้องให้ค่า True Positive Rate (TPR) เท่ากับ 0.9589 และค่าความแม่นยำในการตรวจสอบที่ 64.36 เปอร์เซ็นต์

สรุปผลการวิจัย

บทความนี้ได้นำเสนอวิธีการตรวจสอบการปลอมแปลงภาพแบบ Copy-move ด้วยวิธีการ JCD กับไฟล์ภาพชนิด JPEG จากผลการทดลองพบว่า ในการตรวจสอบภาพที่มีการปลอมแปลงนั้นควรจะมีการจำแนกประเภทของไฟล์ภาพและลักษณะของการปลอมแปลงภาพก่อน เพื่อจะได้ใช้วิธีการที่เหมาะสมสำหรับการตรวจสอบการปลอมแปลงประเภทนั้นๆ ภาพที่มีรายละเอียดคล้ายคลึงกันอย่างมาก เช่น น้ำทะเล ท้องฟ้า เป็นต้น ทำให้การค้นหาวีธีนี้ใช้ไม่ได้ผลจึงควรที่จะมีเทคนิคประเภทอื่นเข้าร่วมในการตรวจสอบเพิ่มเติมด้วย ประสิทธิภาพของการตรวจสอบตำแหน่งที่มีการปลอมแปลงให้ความถูกต้องในการค้นหาที่ 64.36 เปอร์เซ็นต์

เอกสารอ้างอิง

- [1] Weiqi, L., Zhenhua, Q., Feng, P., and Jiwu, H. (2007). "A survey of passivetechonology for digital image forensics, Springer Science . **Frontiers of computer science in China.**, vol. 1, no. 2, pp. 166-179.
- [2] Johnson, M.K. (2007). **Light and optical tools for image forensics.** Ph.D. Thesis, Dartmouth College, Computer Science Deptl., Germany.
- [3] Brugioni, D.A. (1999). Photo fakery : the history and techniques of photographic deception and manipulation. **Virginia Brassey's publishers.**
- [4] Lint, Z., Wang, R., Tang, X., and Shum, H.Y. (2005). "Detecting Doctored images using camera response normality and consistency, in Proc. **Computer Vision and Pattern Recognition.**, vol. 1, no. 43-48.
- [5] Hsu, Y.F., and S.F. Chang, (2006). "Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency", IEEE International Conference. **Multimedia and Expo 2006**, pp. 549-552, July 9-12.
- [6] Mahdian, B., and Saic, S. (2010), "A bibliography on blind methods for identifying image forgery", ELSEVIER. **Signal Processing: Image Communication.**, vol. 25, Issue 6, pp. 389-399.
- [7] Cox, I., Miller, M., and Bloom, J. (2001). Digital Watermarking : Principles & Practice. Morgan Kaufmann.
- [8] Fridrich, J., Soukal, D., and Lukas, J. (2003). "Detection of Copy-Move Forgery in Digital Images", in Proc. **Digital Forensic Research Workshop**, Cleveland, OH, Aug.
- [9] Popescuand, A., and Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images". **IEEE Trans. Signal Processing**, vol. 53, no.10, pp. 3948-3959.
- [10] Farid, H., and Bravo, M. (2010). "Image forensic analyses that elude the human visual system", **SPIE Symposiumon Electronic Imaging**, San Jose.