

# การตรวจพิสูจน์หาการปลอมแปลงภาพถ่ายดิจิทัลโดยใช้การเปรียบเทียบค่าสีของพิกเซลในภาพ Digital Images Forgery Detection by Comparing Color Value of Image Pixels

รณเวท ศรีพวงวงษ์<sup>1</sup> และ พงษ์พิษณุ ภัคดีณรงค์<sup>2</sup>

คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

E-mail : ronawate.s@outlook.com<sup>1</sup>, ppsn2008@gmail.com<sup>2</sup>

## บทคัดย่อ

ในปัจจุบันภาพถ่ายดิจิทัลมีการใช้กันอย่างแพร่หลายในหลายๆ ด้าน รวมถึงใช้เป็นพยานหลักฐานในการพิจารณาคดี ดังนั้นประเด็นเรื่องความน่าเชื่อถือของภาพถ่ายดิจิทัลจึงเป็นเรื่องที่ต้องให้ความสำคัญอย่างยิ่ง บทความนี้ได้นำเสนอเครื่องมือที่ใช้ตรวจสอบความเป็นต้นฉบับของภาพถ่ายดิจิทัล เพื่อตรวจหาการปลอมแปลงโดยวิธีการคัดลอกและเคลื่อนย้าย โดยใช้การเปรียบเทียบค่าสีของแต่ละพิกเซลในรูปที่อยู่ในระบบเมทริกซ์ โดยใช้เครื่องมือที่พัฒนาขึ้นจากโปรแกรม MATLAB ซึ่งจะมีการใช้ขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดที่แตกต่างกัน โดยจากการทดสอบกับภาพถ่ายดิจิทัลจำนวน 100 ภาพ พบว่าการใช้ขนาดบล็อกพิกเซลเท่ากับ 10 และระดับค่าขีดจำกัดเท่ากับ 5 ให้ผลการตรวจสอบที่ถูกต้องมากที่สุด จำนวน 59 ภาพ

## Abstract

Nowadays digital image has been widely used in many areas, including as the evidence used in the trial. Hence the issue of the reliability of digital image is crucial to provide. This article aims at presenting a tool to

determine the source of digital images which are tampering by means of copying and moving. By comparing the color value of each pixel in the images in its matrix form using the tools developed by MATLAB, which different size of the pixels block and different threshold level were applied. From the exam of 100 images found that using block size of 10 pixels and threshold level 5 yielded the most accurate result of the 59 images.

## 1. บทนำ

ในปัจจุบันเทคโนโลยีด้านการถ่ายภาพโดยการใช้กล้องดิจิทัลได้พัฒนาขึ้นอย่างรวดเร็ว โดยสามารถพบเห็นการใช้ภาพถ่ายดิจิทัลในด้านต่างๆ ในชีวิตประจำวันเป็นจำนวนมาก ในส่วนของงานด้านนิติวิทยาศาสตร์เองนั้น ก็มีความจำเป็นที่จะต้องใช้งานภาพถ่ายดิจิทัลด้วย ไม่ว่าจะเป็นการใช้เพื่อเก็บภาพวัตถุพยานในที่เกิดเหตุ การถ่ายภาพสถานที่เกิดเหตุ หรือการถ่ายภาพผู้ต้องสงสัย ภาพถ่ายดิจิทัลดังกล่าวนี้จะถูกรวบรวมประกอบสำนวนเพื่อใช้เป็นพยานหลักฐานในชั้นศาลด้วย ดังนั้นประเด็นในเรื่องความน่าเชื่อถือจึงเป็นเรื่องที่สำคัญมาก ซึ่งสำหรับภาพถ่ายดิจิทัลแล้วการแก้ไขภาพถ่ายด้วยโปรแกรม

คอมพิวเตอร์สามารถที่จะทำให้ภาพถ่ายนั้นสูญเสียความเป็นต้นฉบับ และทำให้เนื้อหาของภาพดั้งเดิมถูก บิดเบือนหรือคลาดเคลื่อนไปจากความเป็นจริงได้โดยง่าย ด้วยสาเหตุดังที่กล่าวมานี้ ทำให้ในปัจจุบันการนำภาพถ่ายดิจิทัลไปใช้เป็นพยานหลักฐานในการพิจารณาคดีในชั้นศาล เป็นเรื่องที่ยังไม่เป็นที่ยอมรับนัก เนื่องจากในปัจจุบัน การตรวจสอบความเป็นต้นฉบับของภาพถ่ายดิจิทัลนั้น ยังเป็นเรื่องที่ทำได้ยาก ยิ่งจะทำให้หลักฐานภาพถ่ายดิจิทัลที่ได้มานั้น ถูกตั้งข้อสงสัยในด้านความน่าเชื่อถือมากขึ้นเรื่อยๆ

จากปัญหาที่กล่าวมานี้ ทำให้ผู้วิจัยมีความสนใจที่จะพัฒนาเครื่องมือที่ใช้ในการตรวจพิสูจน์หาการปลอมแปลงดังกล่าว โดยมุ่งเน้นไปที่การทำซ้ำหรือตัดส่วนหนึ่งส่วนใดของภาพออกภายในภาพเดียวกัน ซึ่งถือเป็นวิธีการที่แพร่หลายวิธีหนึ่งในปัจจุบัน โดยในการพัฒนาวิธีการตรวจพิสูจน์นั้นจะใช้การเปรียบเทียบค่าสีของแต่ละพิกเซลในรูปที่อยู่ในระบบเมทริกซ์ โดยใช้เครื่องมือที่พัฒนาขึ้นจากโปรแกรม MATLAB ซึ่งจะมีการใช้ขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดที่แตกต่างกันในการตรวจหาการปลอมแปลงจากการคัดลอกและเคลื่อนย้ายในภาพถ่ายดิจิทัลนั้น โดยอาศัยแนวคิดที่ว่าหากมีการคัดลอกและเคลื่อนย้ายวัตถุในภาพเกิดขึ้น ย่อมจะทำให้เกิดการซ้ำกันของการจัดเรียงพิกเซลในภาพถ่ายนั้นๆ หากเราสามารถที่จะพัฒนาเครื่องมือที่จะตรวจหารูปแบบของการซ้ำกันนี้ได้ ก็จะสามารถนำมาประยุกต์ใช้ในการตรวจหาการปลอมแปลงภาพถ่ายดิจิทัลได้ด้วย

## 2. การศึกษาเอกสาร

### 2.1 ภาพดิจิทัล

ภาพดิจิทัล เป็นการแสดงผลภาพในลักษณะของมิติในหน่วยที่เรียกว่าพิกเซล ภาพดิจิทัลสามารถนิยามเป็นฟังก์ชันสองมิติ  $f(x,y)$  โดยที่  $x$  และ  $y$  เป็นพิกัดของภาพ และแอมพลิจูดของ  $f$  ที่พิกัด  $(x,y)$  ใดๆ ภายในภาพคือค่าความเข้มแสงของภาพ (Intensity) ที่ตำแหน่งนั้นๆ และเมื่อ  $x,y$  และแอมพลิจูดของ  $f$  เป็นค่าจำกัด (Finite value) จึงเรียกรูปภาพนี้ว่าเป็นภาพดิจิทัล (Digital Image) และถ้ากำหนดให้ภาพ  $f(x,y)$  มีขนาด  $M$  แถวและ  $N$  คอลัมน์ และพิกัดของจุดกำเนิด (Origin) ของภาพคือที่ตำแหน่ง  $(x,y) = (0,0)$  แล้ว จะสามารถเขียนสมการให้อยู่ในรูปเมทริกซ์ได้ดังสมการที่ 1

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & & \vdots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix} \quad (1)$$

ค่าแต่ละค่าที่อยู่ในเมทริกซ์จะเรียกว่า พิกเซล (Pixel) โดยภาพหนึ่งๆ จะประกอบไปด้วยจุดภาพหรือพิกเซลมากมาย โดยตำแหน่ง  $(0,0)$  จะอยู่ทางด้านซ้ายมือสุดด้านบนของภาพ การจัดลำดับตำแหน่งของจุดภาพจะเรียงจากซ้ายไปขวาในแต่ละเส้นจุดและจัดลำดับของเส้นจุดจะเรียงจากบนลงล่าง การเก็บค่าของความเข้มแสงของภาพดิจิทัลลงหน่วยความจำในลักษณะเส้นจุด (Raster) นี้จะเรียกภาพบิตแมป (Bitmap) หรือภาพเรสเตอร์ (Raster) แต่รูปที่จัดเก็บในลักษณะนี้จะมีขนาดใหญ่จึงมีการบีบอัดภาพ (Image compression) เพื่อให้ข้อมูลภาพมีขนาดเล็กลง

การสร้างภาพดิจิทัลสามารถสร้างได้จากอุปกรณ์รับภาพเช่น กล้องดิจิทัล หรือ สแกนเนอร์ เป็นต้น ภาพดิจิทัลทั่วไปนั้นมีลักษณะเป็นภาพสี โดยในข้อมูลของภาพมีการเก็บค่าแม่สีของแสง 3 สี คือ R (สีแดง) G (สีเขียว) และ B (สีน้ำเงิน) เป็น 3 รูปแบบ โดยที่แต่ละรูปแบบจะเป็นตัวเก็บค่าความสว่างของสีต่างๆ ไว้ และเมื่อนำภาพมาแสดงที่หน้าจอภาพก็จะเป็นการนำรายละเอียดที่เก็บไว้ในสีต่างๆ มาแสดงพร้อมกันบนจุดๆ เดียว ทำให้เกิดการผสมกันของสี ทำให้เกิดภาพสีที่มีรายละเอียดต่างๆ กันได้ แต่ละจุดของภาพจะมีการจัดเก็บข้อมูลแบบ 8 บิต ดังนั้นภาพสีจะมีการจัดเก็บข้อมูลในแม่สีของแสงแต่ละสีทั้งหมด 3 สี จึงทำให้ต้องใช้การจัดเก็บทั้งหมด 24 บิตต่อหนึ่งจุดของภาพ แบ่งเป็นระดับสีได้ 256 ระดับ โดยที่สีขาวเกิดจากการผสมกันของสี RGB ที่มีค่าความสว่างของสี R เท่ากับ 255 สี G เท่ากับ 255 และสี B เท่ากับ 255 ส่วนสีดำเกิดจากค่าความสว่างของสี R เท่ากับ 0 สี G เท่ากับ 0 และสี B เท่ากับ 0

## 2.2 ระบบเมทริกซ์

เมทริกซ์ (Matrix) คือ กลุ่มของจำนวนที่นำมาเขียนเรียงกันอย่างมีระเบียบภายในเครื่องหมายวงเล็บโดยจำนวนเหล่านี้จะเรียงกันเป็นแถว ซึ่งในแต่ละแถวจะมีจำนวนหลักเท่ากันทุกแถว เรียกจำนวนที่อยู่ในเมทริกซ์ว่า สมาชิกของเมทริกซ์ ซึ่งเราจะระบุตำแหน่งของสมาชิกในเมทริกซ์โดยบอกแถว (Row) และหลัก (Column) ของสมาชิก มักใช้ตัวอักษรภาษาอังกฤษตัวใหญ่แทนเมทริกซ์ และใช้ตัวอักษรภาษาอังกฤษตัวเล็กซึ่งเขียนตัวเลข 2 ตัว

ห้อยต่อไว้ทางด้านขวาแทนสมาชิก (เช่น  $a_{ij}$  คือ สมาชิกของเมทริกซ์ A ที่อยู่ที่แถวที่ i หลักที่ j) ขนาดของเมทริกซ์จะเรียกว่า มิติของเมทริกซ์ โดยเมทริกซ์ที่มี m แถว n หลักจะมีขนาด  $m \times n$  มิติ

$$A = \begin{matrix} \text{หลักที่} & 1 & 2 & \cdots & n & \text{แถวที่} \\ \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} & 1 \\ & 2 \\ & \vdots \\ & m \end{matrix}$$

### 2.2.1 การเท่ากันของเมทริกซ์

กำหนด  $A = [a_{ij}]_{m \times n}$  และ  $B = [b_{ij}]_{p \times q}$  เป็นเมทริกซ์ เมทริกซ์ A และ B จะเท่ากันกันได้ ก็ต่อเมื่อ A และ B ต้องมีมิติเท่ากัน ( $m = p$  และ  $n = q$ ) และสมาชิกที่อยู่ในตำแหน่งเดียวกันต้องมีค่าเท่ากัน ( $a_{ij} = b_{ij}$ )

### 2.2.2 การบวก-ลบเมทริกซ์

กำหนด  $A = [a_{ij}]_{m \times n}$  และ  $B = [b_{ij}]_{m \times n}$  เป็นเมทริกซ์ และให้เมทริกซ์  $C = [c_{ij}]_{m \times n}$  เป็นเมทริกซ์ที่เกิดจากการบวกหรือลบกันของ A กับ B แล้ว  $c_{ij} = a_{ij} \pm b_{ij}$  การบวก-ลบ เมทริกซ์ทำได้โดยนำสมาชิกที่ตำแหน่งเดียวกันมาบวก-ลบกัน ซึ่งเราจะบวก-ลบเมทริกซ์ได้เมื่อเมทริกซ์ที่นำมาบวก-ลบกันมีมิติเท่ากัน

## 2.3 การกำหนดค่าขีดจำกัด

การกำหนดค่าขีดจำกัด (Thresholding) เป็นการปรับปรุงรูปที่มีการเปลี่ยนแปลงค่าระดับความเทาเดิมที่มีค่าต่ำกว่าค่าขีดจำกัดให้เป็นค่าระดับความเทาค่าหนึ่ง และเปลี่ยนแปลงค่าระดับความเทาเดิมที่มีค่าสูงกว่าค่าขีดจำกัดให้เป็นค่าระดับความ

เทาค่าหนึ่ง ซึ่งโดยส่วนมากกำหนดให้เปลี่ยนเป็นค่าระดับความเทาต่ำสุด และสูงสุดในระยะ Gray scale นั้น ทำให้เกิดเป็นรูปที่มีระดับความเทาเพียงแค่ 2 ระดับ (Binary Image) เทคนิคที่ใช้การกำหนดค่าขีดจำกัดนี้ มักถูกใช้ในการแบ่งค่าระดับความเทาของภาพดิจิทัลออกเป็นส่วนๆ เพื่อวัตถุประสงค์บางอย่าง เช่น ใช้ในการจับภาพวัตถุหรือใช้กับรูปที่เป็นตัวอักษรเพียงอย่างเดียว สิ่งสำคัญของการกำหนดค่าขีดจำกัดคือ ต้องกำหนดค่าขีดจำกัดให้เหมาะสมจึงทำให้ภาพถูกแบ่งออกเป็นส่วนๆ ได้ตามต้องการ

## 2.4 งานวิจัยที่เกี่ยวข้อง

จากการปลอมแปลงภาพถ่ายดิจิทัลนั้นสามารถทำได้หลายวิธี ดังนั้นวิธีการตรวจสอบจึงแตกต่างกันไปตามหลักเกณฑ์ที่ใช้ในการตรวจสอบ โดยมีผู้ทำการศึกษาไว้หลายวิธีด้วยกัน เช่น

Neal Krawetz [1] ได้เสนอวิธีการตรวจสอบภาพถ่ายที่มีการแก้ไขตกแต่งจากโปรแกรมคอมพิวเตอร์หลายวิธี คือ การตรวจสอบ Metadata ของภาพถ่ายดิจิทัลว่ามีข้อมูลการแก้ไขระบุไว้หรือไม่ หรือการตรวจ Quantization fingerprint ที่กล้องแต่ละรุ่นนั้นจะมีค่าเฉพาะที่ใช้ในการประมวลผลภาพแตกต่างกัน โดยเปรียบเทียบค่าที่พบในรูปที่ตรวจ กับกล้องดิจิทัลที่ถ่ายนั้นมีค่าตรงกันหรือไม่ และยังเสนอวิธีการตรวจสอบภาพถ่ายขึ้นสูงด้วย Principle component analysis (PCA) และ Error level analysis (ELA) โดยอาศัยสมบัติของภาพในแบบ JPEG ที่มีการบีบอัดของข้อมูลใน

การตรวจสอบว่าคุณภาพของภาพถ่ายนั้นมีความคลาดเคลื่อนไปจากที่ควรจะเป็นหรือไม่

ในขณะที่ Jan Lukáš และคณะ [2] ได้เสนอวิธีการตรวจสอบภาพถ่ายดิจิทัล โดยอาศัยรูปแบบของ Noise ที่เป็นลักษณะเฉพาะตัวของกล้องดิจิทัลในการตรวจหาบริเวณที่มีการปลอมแปลงในภาพ ที่พบรูปแบบของ Noise ได้น้อยกว่าบริเวณที่ไม่มีการปลอมแปลง

วิธีการแก้ไขปลอมแปลงภาพถ่ายดิจิทัลที่ทำได้ง่ายและเป็นที่ยอมรับวิธีหนึ่งก็คือ การคัดลอกและเคลื่อนย้าย ดังนั้นจึงมีผู้ศึกษาวิธีการตรวจสอบภาพถ่ายที่ผ่านการปลอมแปลงในลักษณะนี้ไว้หลายวิธีด้วยกัน เช่น

Alin C Popescu และคณะ [3] ใช้วิธีการแบ่งภาพออกเป็นบล็อกตามขนาดที่กำหนดแล้วเปรียบเทียบ noise และค่าการบีบอัดข้อมูลโดยใช้ PCA เพื่อหาบริเวณที่เหมือนกันในภาพ

Jessica Fridrich และคณะ [4] และ Yanjun Cao และคณะ [5] เลือกใช้วิธี Robust match โดยใช้ค่าสัมประสิทธิ์ DCT ในการตรวจหาบริเวณที่มีการคัดลอกและเคลื่อนย้ายในภาพซึ่งใช้เวลาในการตรวจสอบค่อนข้างนาน ขณะที่ Preeti Yadav [6] เลือกใช้วิธี Discrete Wavelet Transform (DWT) ในการตรวจหาบริเวณที่มีค่าการบีบอัดข้อมูลเหมือนกัน

ในบทความนี้จะแบ่งภาพออกเป็นบล็อกเช่นเดียวกัน จากนั้นจะตรวจสอบภาพถ่ายดิจิทัลโดยการเปรียบเทียบค่าสีในแต่ละพิกเซลของภาพเพื่อตรวจหาบริเวณที่มีการปลอมแปลง โดยเลือกใช้

ขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดที่ให้ผล  
ถูกต้องแม่นยำมากที่สุด

### 3. วิธีการดำเนินงานวิจัย

#### 3.1 ศึกษาปัญหาและความต้องการของระบบ

การศึกษาค้นคว้าและความต้องการของการ  
พัฒนาเครื่องมือตรวจพิสูจน์หาการปลอมแปลง  
ภาพถ่ายดิจิทัลโดยใช้การเปรียบเทียบค่าสีของ  
พิกเซลในภาพ เป็นการศึกษาถึงความเป็นไปได้ใน  
การพัฒนาโปรแกรมที่สามารถที่จะระบุส่วนใดส่วน  
หนึ่งของภาพถ่ายดิจิทัลที่ผ่านการปลอมแปลงจาก  
วิธีการคัดลอกและเคลื่อนย้าย โดยใช้การ  
เปรียบเทียบค่าสีของแต่ละพิกเซลได้หรือไม่ จาก  
การศึกษาค้นคว้าเบื้องต้น พบว่ามีความเป็นไปได้ใน  
การพัฒนาเครื่องมือตรวจสอบขึ้น โดยอาศัย  
คุณสมบัติพื้นฐานของภาพถ่ายดิจิทัลมาช่วยในการ  
ตรวจสอบหาบริเวณใดๆ ของรูปที่มีพิกเซลที่  
เหมือนกันอันเกิดจากการปลอมแปลงโดยวิธีการ  
คัดลอกและเคลื่อนย้าย และแสดงผลให้เห็นเป็นภาพ  
แบบ Binary Image (ขาว-ดำ) โดยที่ภาพถ่ายดิจิทัล  
ที่นำมาตรวจสอบนั้นทางผู้วิจัยได้จัดทำขึ้นเอง  
เพื่อที่จะสามารถตรวจสอบได้อย่างถูกต้องแม่นยำว่า  
เครื่องมือที่พัฒนาขึ้นสามารถตรวจสอบพบบริเวณที่  
มีการปลอมแปลงได้อย่างถูกต้องหรือไม่ ในส่วนของ  
โปรแกรมที่ใช้ในการพัฒนาเครื่องมือสำหรับตรวจหา  
การปลอมแปลงภาพถ่ายดิจิทัลที่ผู้วิจัยใช้นั้น มี  
รายการดังต่อไปนี้

- เครื่องคอมพิวเตอร์ความเร็ว 2 x 2.3 GHz
- หน่วยความจำหลัก (RAM) ความจุ 32 GB
- หน่วยเก็บข้อมูลที่มีพื้นที่ 680 MB

- ระบบปฏิบัติการ Windows 7
- โปรแกรม MATLAB R2009a

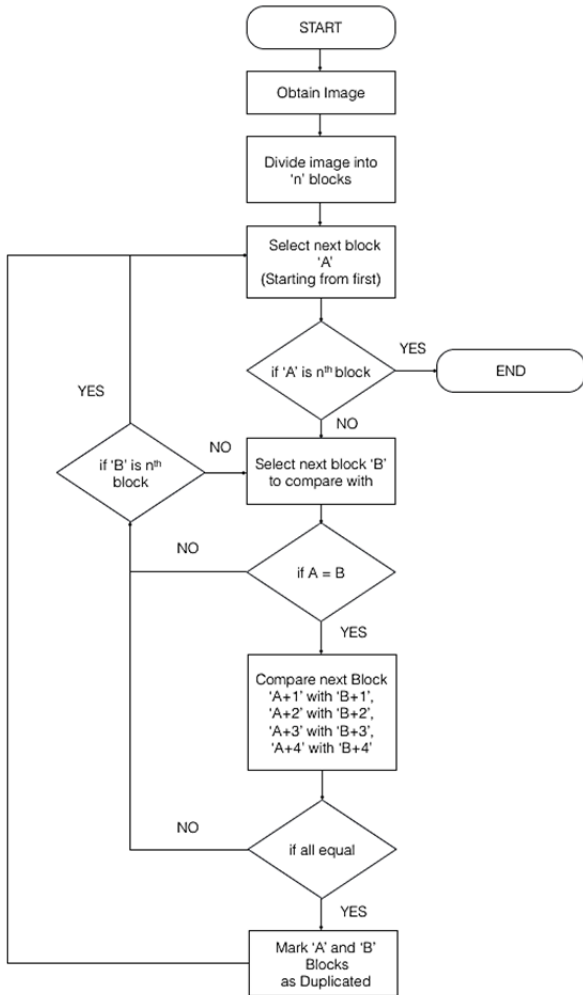
#### 3.2 แนวคิดและการออกแบบ

ในการพัฒนาเครื่องมือตรวจพิสูจน์หาการ  
ปลอมแปลงภาพถ่ายดิจิทัล โดยใช้การเปรียบเทียบ  
ค่าสีของพิกเซลในภาพ มีขั้นตอนการทำงานดังนี้

1. การสร้างภาพถ่ายดิจิทัลสำหรับ  
ตรวจสอบเครื่องมือตรวจพิสูจน์หาการปลอมแปลงที่  
พัฒนาขึ้นจำนวน 100 ภาพ โดยผู้วิจัยจัดทำขึ้นมา  
ใหม่ทั้งหมดเพื่อให้สามารถระบุแหล่งที่มา และระบุ  
จุดที่มีการปลอมแปลงได้อย่างถูกต้อง ภาพทั้งหมด  
ถ่ายจากกล้องดิจิทัล โดยเป็นภาพใน Format JPEG  
ขนาด 1800 x 1200 พิกเซล หรือขนาดประมาณ 2  
ล้านพิกเซล ซึ่งเป็นความละเอียดมาตรฐานที่ใช้กัน  
อย่างแพร่หลาย โดยเลือกรูปที่มีความหลากหลายทั้ง  
ในแง่องค์ประกอบของภาพและสีสันทัน จากนั้นนำ  
ภาพถ่ายดิจิทัลทั้ง 100 ภาพมาทำการปลอมแปลง  
ด้วยโปรแกรม Photoshop CS6 ด้วยวิธีคัดลอกและ  
เคลื่อนย้ายภายในภาพเดียวกัน

2. การวิเคราะห์และการออกแบบเครื่องมือ  
ตรวจพิสูจน์หาการปลอมแปลงภาพถ่ายดิจิทัลโดย  
ใช้การเปรียบเทียบค่าสีของพิกเซลในภาพ โดยอาศัย  
หลักการแบ่งภาพออกเป็นส่วนของบล็อกพิกเซลตาม  
ขนาดที่กำหนด แล้วทำการเปรียบเทียบบล็อกนั้นๆ  
เทียบกับบล็อกถัดไป โดยอาศัยค่าสี RGB ของแต่ละ  
พิกเซลในบล็อก ที่อยู่ในรูปแบบของเมทริกซ์มา  
เปรียบเทียบกันว่าในแต่ละบล็อกมีความแตกต่างกัน  
น้อยกว่าหรือมากกว่าค่าระดับขีดจำกัดที่กำหนดไว้  
โดยหากมีค่าความแตกต่างของแต่ละพิกเซลน้อยกว่า

ค่าระดับขีดจำกัดที่กำหนดไว้ ให้แสดงผลว่าทั้งสองบล็อกนั้นเป็นบล็อกที่ผ่านการปลอมแปลง แต่หากว่ามีค่าความแตกต่างมากกว่าค่าที่กำหนดไว้ ให้เลือกบล็อกถัดไปเพื่อตรวจสอบต่อไป



รูปที่ 1 ฝั่งงานระบบของการพัฒนาเครื่องมือตรวจสอบหาการปลอมแปลงภาพถ่ายดิจิทัลจากวิธีคัดลอกและเคลื่อนย้าย โดยใช้การเปรียบเทียบค่าสีของพิกเซลในภาพ

และเพื่อลดความผิดพลาดจากการตรวจสอบให้น้อยลง ผู้วิจัยได้กำหนดให้เมื่อตรวจพบบล็อกที่มีความแตกต่างกันน้อยกว่าค่าระดับขีดจำกัดที่กำหนดไว้แล้ว ให้ทำการตรวจสอบบล็อกถัดไปทางขวาที่ติดกันอีก 4 บล็อก โดยอาศัยคุณสมบัติของ

ภาพดิจิทัลแบบ Raster Image ที่พิกเซลที่อยู่ใกล้เคียงกันมักจะมีค่าสีที่ใกล้เคียงกัน โดยถ้าผลออกมาว่ายังคงมีความแตกต่างกันน้อยกว่าค่าระดับขีดจำกัดที่กำหนดไว้ทั้ง 4 บล็อกตามลำดับ จึงจะสรุปว่าบล็อกแรกที่ทำกรตรวจสอบนั้นเป็นบล็อกที่ผ่านการปลอมแปลง จากนั้นทำซ้ำตามกระบวนการทั้งหมดนี้ไปเรื่อยๆ จนถึงบล็อกพิกเซลสุดท้าย จากนั้นจึงแสดงภาพผลการตรวจ โดยแสดงส่วนที่ตรวจพบการปลอมแปลงในภาพด้วยสีดำ โดยในงานวิจัยนี้มีการใช้ขนาดของบล็อกที่แตกต่างกันในการตรวจสอบ เพื่อศึกษาว่าขนาดบล็อกพิกเซล และค่าระดับขีดจำกัดที่เหมาะสมในการตรวจสอบเท่าใดที่สามารถให้ผลการตรวจพิสูจน์ที่ถูกต้องแม่นยำมากที่สุดภายในเวลาที่เหมาะสมโดยมีขั้นตอนและวิธีการในภาพรวมดังนี้

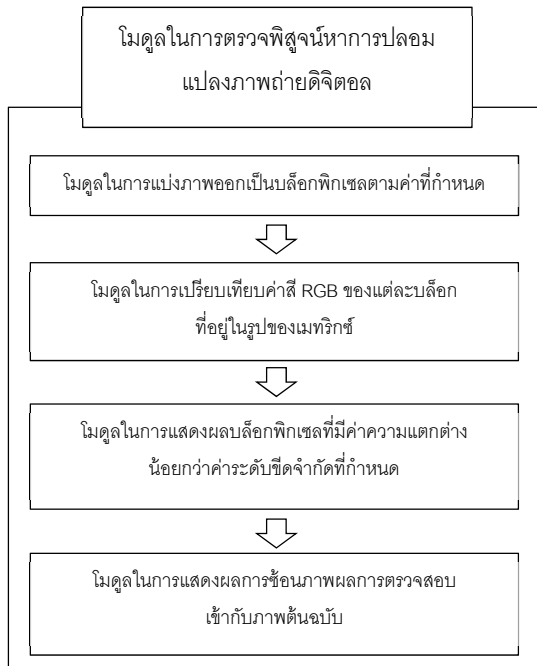
### 3.3 การพัฒนาเครื่องมือ

การพัฒนาเครื่องมือตรวจสอบพิสูจน์หาการปลอมแปลงภาพถ่ายดิจิทัล โดยใช้การเปรียบเทียบค่าสีของพิกเซลในภาพ สามารถแบ่งการทำงานออกเป็นโมดูลที่ทำงานต่อเนื่องกันได้ 3 โมดูล ดังนี้

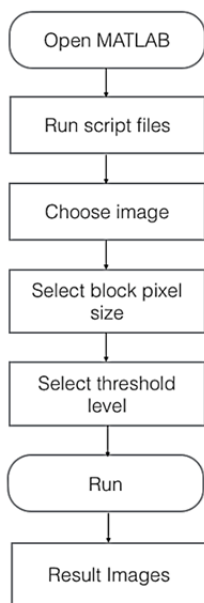
### 3.4 การทดสอบเครื่องมือ

ทดสอบการทำงานของเครื่องมือโดยใช้ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดที่แตกต่างกันดังนี้

- ขนาดบล็อกพิกเซล 20 ที่ค่าระดับขีดจำกัดที่ 10
- ขนาดบล็อกพิกเซล 20 ที่ค่าระดับขีดจำกัดที่ 5
- ขนาดบล็อกพิกเซล 20 ที่ค่าระดับขีดจำกัดที่ 1
- ขนาดบล็อกพิกเซล 10 ที่ค่าระดับขีดจำกัดที่ 10
- ขนาดบล็อกพิกเซล 10 ที่ค่าระดับขีดจำกัดที่ 5
- ขนาดบล็อกพิกเซล 10 ที่ค่าระดับขีดจำกัดที่ 1



รูปที่ 2 โมดูลต่างๆ ของเครื่องมือตรวจพิสูจน์หาการปลอมแปลงภาพถ่ายดิจิทัล



รูปที่ 3 ภาพแสดงขั้นตอนในการใช้งานเครื่องมือตรวจพิสูจน์หาการปลอมแปลงภาพถ่ายดิจิทัล

โดยในการทดสอบเครื่องมือนั้นเริ่มจากเปิดโปรแกรม MATLAB เรียกไฟล์เครื่องมือที่เขียนไว้ขึ้นมาจากนั้นเลือกภาพถ่ายดิจิทัลที่ต้องการตรวจสอบ เลือก

ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดที่ต้องการ แล้วจึงรันโปรแกรม ดังแสดงในรูปที่ 3

### 3.5 การประเมินผลการวิจัย

การประเมินผลการทำงานของเครื่องมือจากผลการตรวจสอบที่ได้ในรูปแบบของภาพ Binary Image ที่ระบุตำแหน่งที่มีการปลอมแปลง โดยผู้วิจัยจะนำผลของรูปที่ได้มาเทียบกับตำแหน่งที่มีการปลอมแปลงในแต่ละรูปที่ผู้วิจัยได้จัดทำไว้ ว่าผลที่ได้แสดงบริเวณที่มีการปลอมแปลงอย่างชัดเจนหรือไม่ โดยตรวจสอบผลในด้านต่างๆ ดังนี้

- จำนวนภาพผลการตรวจสอบแสดงบริเวณที่มีการปลอมแปลงอย่างถูกต้องชัดเจน (Positive)
- จำนวนภาพผลการตรวจสอบแสดงบริเวณที่มีการปลอมแปลงมากกว่าความเป็นจริง (False Positive)
- จำนวนภาพผลการตรวจสอบแสดงบริเวณที่มีการปลอมแปลงน้อยกว่าความเป็นจริง (False Negative)
- ระยะเวลาในการตรวจสอบของภาพแต่ละภาพ

จากนั้นจึงวิเคราะห์ผลการทดสอบ โดยพิจารณาถึงผลของลักษณะของภาพถ่าย และตัวแปรต่างๆ ที่มีต่อความแม่นยำของผลการตรวจสอบ และระยะเวลาที่ใช้ในการตรวจสอบ

## 4. ผลการวิจัย

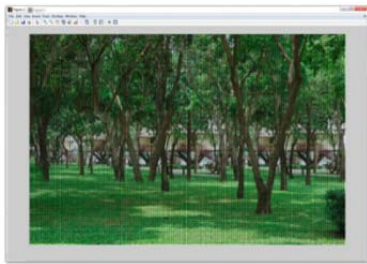
### 4.1 การแสดงผลการตรวจพิสูจน์

ผลที่ได้จากการตรวจพิสูจน์ภาพถ่ายดิจิทัล ด้วยชุดคำสั่งของเครื่องมือตรวจพิสูจน์หาการปลอม

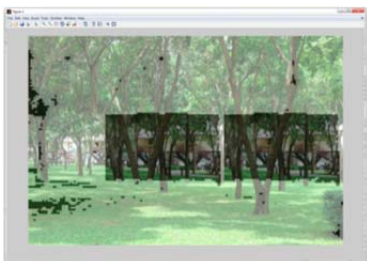
แปลงภาพถ่ายดิจิทัลโดยใช้การเปรียบเทียบค่าสีของพิกเซลในภาพ จะแสดงผลออกมาเป็นภาพ 3 ภาพด้วยกันคือ

รูปที่ 1 แสดงรูปที่แบ่งเป็นบล็อกตามขนาดของบล็อกพิกเซลที่กำหนดไว้ (ก)

รูปที่ 2 แสดงภาพผลการตรวจสอบโดยการเปรียบเทียบค่าสีของแต่ละบล็อกที่แบ่งไว้กับบล็อกถัดไป โดยแสดงเป็นพื้นที่สีดำซ้อนอยู่บนส่วนที่ตรวจพบการปลอมแปลง ซึ่งเป็นบริเวณที่มีความแตกต่างของค่าสีน้อยกว่าค่าระดับขีดจำกัดที่กำหนดไว้ (ข)



(ก)



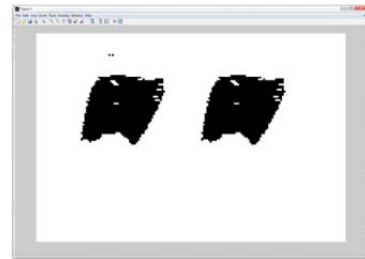
(ข)



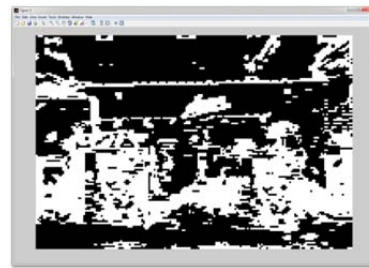
(ค)

รูปที่ 4 ภาพแสดงผลการตรวจพิสูจน์ภาพถ่ายดิจิทัล ที่ได้จากการตรวจพิสูจน์ด้วยเครื่องมือที่พัฒนาขึ้น

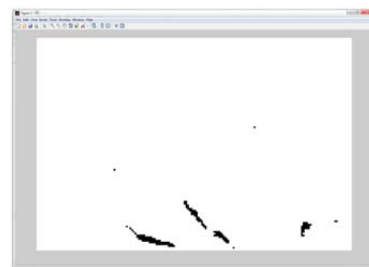
รูปที่ 3 แสดงภาพเฉพาะส่วนที่เครื่องมือตรวจพบว่าการปลอมแปลง โดยแสดงเป็นภาพแบบ Binary Image แสดงพื้นที่สีดำในบริเวณที่ตรวจพบว่าการปลอมแปลงและพื้นที่สีขาวในส่วนที่ตรวจไม่พบการปลอมแปลง เพื่อความชัดเจน(ค)



(ก)



(ข)



(ค)

รูปที่ 5 ภาพแสดงผลการตรวจพิสูจน์ที่แสดงบริเวณที่มีการปลอมแปลงอย่างถูกต้อง (Positive) (ก), แสดงบริเวณที่มีการปลอมแปลงมากกว่าความเป็นจริง (False Positive) (ข) และแสดงบริเวณที่มีการปลอมแปลงน้อยกว่าความเป็นจริง (False Negative) (ค)

การบันทึกผลการตรวจพิสูจน์ที่ได้จากเครื่องมือที่พัฒนาขึ้น จะบันทึกผล 2 ส่วนด้วยกันคือ

1. ผลความถูกต้องในการตรวจพิสูจน์ ซึ่งสามารถแบ่งได้เป็น 3 กลุ่มด้วยกัน คือ



- รูปที่แสดงบริเวณที่มีการปลอมแปลงอย่างถูกต้องชัดเจน (Positive) (ก)
- รูปที่แสดงผลการปลอมแปลงมากกว่าความเป็นจริง (False Positive) (ข)
- รูปที่แสดงผลการปลอมแปลงน้อยกว่าความเป็นจริง (False Negative) (ค)

2. ระยะเวลาในการการตรวจพิสูจน์ โดยบันทึกระยะเวลาในการตรวจพิสูจน์ นับตั้งแต่เริ่มเปิดใช้งานชุดคำสั่ง จนถึงเวลาที่แสดงผลการตรวจสอบครบทั้งสามภาพ โดยบันทึกหน่วยของเวลาเป็นนาที

## 4.2 ผลการตรวจพิสูจน์

### 4.2.1 ความถูกต้องแม่นยำของการตรวจพิสูจน์

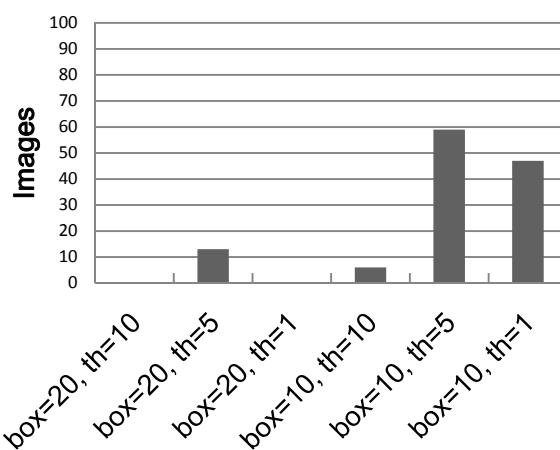
ผลการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่มีการใช้ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดแตกต่างกันได้ดังนี้

ตารางที่ 1 แสดงผลการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่มีการใช้ขนาด บล็อกพิกเซลและค่าระดับขีดจำกัดแตกต่างกัน

box / th	Positive	False Positive	False Negative
box=20, th=10	0	97	3
box=20, th=5	13	49	38
box=20, th=1	0	0	100
box=10, th=10	6	91	3
box=10, th=5	59	34	7
box=10, th=1	47	4	49

จากผลการตรวจพิสูจน์ที่ได้จะเห็นได้ว่าเครื่องมือที่พัฒนาขึ้น สามารถที่จะใช้ตรวจสอบภาพถ่ายดิจิทัลที่ผ่านการปลอมแปลงด้วยวิธีคัดลอกและเคลื่อนย้ายได้ โดยที่ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดที่ใช้มีผลโดยตรงกับระดับความถูกต้องแม่นยำของผลการตรวจสอบ

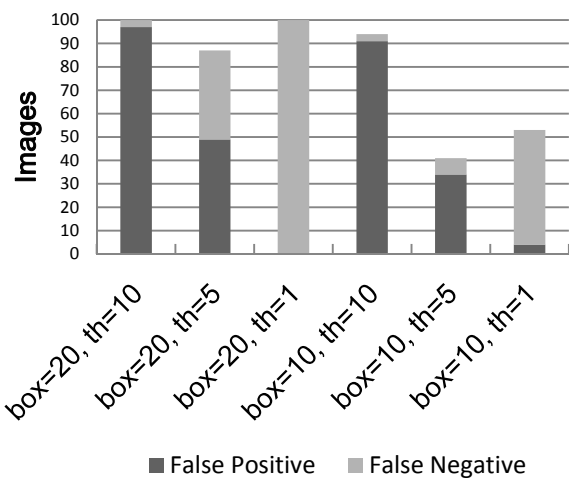
โดยจะเห็นได้ว่าผลการตรวจพิสูจน์ที่ใช้ขนาดบล็อกพิกเซลเท่ากับ 20 x 20 พิกเซลนั้นได้ผลการตรวจสอบที่ถูกต้อง (Positive) น้อยมาก และเมื่อเปลี่ยนแปลงขนาดบล็อกพิกเซลให้เล็กลงเป็น 10 x 10 พิกเซล ซึ่งจะทำให้ผลการตรวจพิสูจน์ละเอียดขึ้นพบว่าได้ผลการตรวจสอบที่ถูกต้อง (Positive) เพิ่มขึ้นจากเดิม และเมื่อนำมาแยกพิจารณาในแต่ละค่าขีดจำกัดที่เลือกใช้นั้นจะพบว่า ที่ค่าระดับขีดจำกัดเท่ากับ 5 ได้ผลการตรวจสอบที่ถูกต้อง (Positive) มากที่สุดรองลงมาคือที่ค่าระดับขีดจำกัดเท่ากับ 1 และ 10 ตามลำดับ ดังแสดงความสัมพันธ์ในรูปที่ 6



รูปที่ 6 แผนภูมิแสดงจำนวนผลการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่ได้ผลเป็น Positive ที่ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดต่างๆ

ในส่วนของการตรวจพิสูจน์ให้ผลที่ไม่ตรงกับความเป็นจริงนั้นพบว่าผลการตรวจพิสูจน์ที่ใช้ขนาดบล็อกพิกเซลเท่ากับ 20 x 20 พิกเซล ได้ผลการตรวจพิสูจน์ที่มีความผิดพลาดทั้งที่แสดงบริเวณที่มีการปลอมแปลงมากกว่า (False Positive) และน้อยกว่าความเป็นจริง (False Negative) ค่อนข้างมาก ในขณะที่เมื่อเปลี่ยนขนาดบล็อกพิกเซลให้เล็กลงเป็น

10 x 10 พิกเซล พบว่าให้ผลการตรวจพิสูจน์ที่ผิดพลาดน้อยลง และเมื่อนำมาแยกพิจารณาในแต่ละค่าขีดจำกัดที่เลือกใช้นั้นจะพบว่า ค่าขีดจำกัดเท่ากับ 10 มีแนวโน้มจะแสดงบริเวณที่มีการปลอมแปลงมากกว่าความเป็นจริง (False Positive) และที่ค่าขีดจำกัดเท่ากับ 1 มีแนวโน้มจะแสดงบริเวณที่มีการปลอมแปลงน้อยกว่าความเป็นจริง (False Negative) ค่อนข้างมาก ดังแสดงความสัมพันธ์ในรูปที่ 7



รูปที่ 7 แผนภูมิแสดงจำนวนผลการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่ได้ผลเป็น Negative ที่ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดต่างๆ

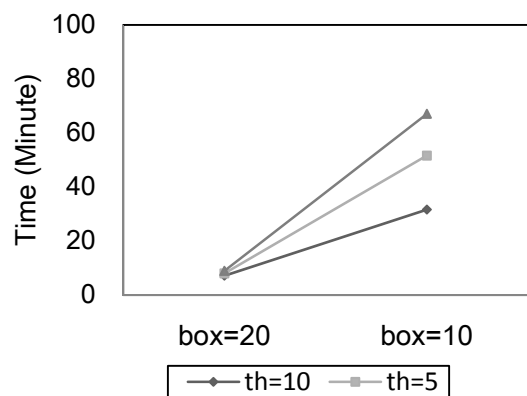
#### 4.2.2 ระยะเวลาในการตรวจพิสูจน์

การตรวจพิสูจน์ภาพถ่ายดิจิทัลโดยใช้ขนาดของบล็อกพิกเซล และค่าระดับขีดจำกัดที่แตกต่างกัน จะใช้เวลาในการตรวจพิสูจน์โดยเฉลี่ย ดังแสดงในตารางที่ 2

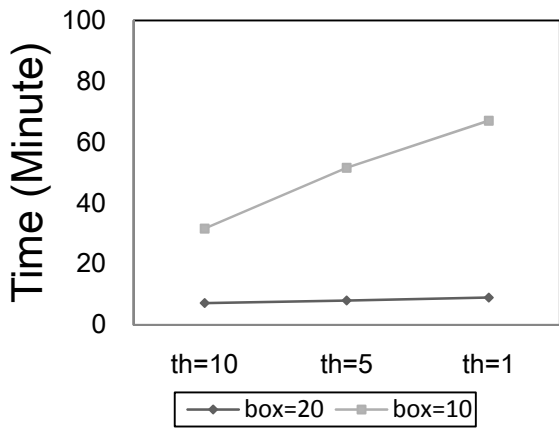
ตารางที่ 2 แสดงระยะเวลาเฉลี่ยที่ใช้ในการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่มีการใช้ขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดแตกต่างกัน

threshold	Time (Minute)	
	box=20	box=10
th=10	7.17	31.64
th=5	8.01	51.63
th=1	8.97	67.08

จะเห็นได้ว่าขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดที่เลือกใช้ มีผลโดยตรงต่อระยะเวลาที่ใช้ในการตรวจสอบ เมื่อขนาดของบล็อกพิกเซลมีขนาดเล็กลง ก็มีแนวโน้มที่จะทำให้ระยะเวลาในการตรวจพิสูจน์นานขึ้นด้วย เช่นเดียวกันกับค่าระดับขีดจำกัดที่เลือกใช้ เมื่อใช้ค่าระดับขีดจำกัดที่มีค่าน้อย ก็ยิ่งส่งผลให้ระยะเวลาในการตรวจพิสูจน์มากขึ้น ดังแสดงความสัมพันธ์ในรูปที่ 8 และ 9



รูปที่ 8 ภาพกราฟเปรียบเทียบความสัมพันธ์ระหว่างเวลาเฉลี่ยที่ใช้ในการตรวจพิสูจน์ (นาที) กับขนาดบล็อกพิกเซล ที่ค่าระดับขีดจำกัด 10, 5 และ 1 ตามลำดับ



รูปที่ 9 ภาพแสดงการเปรียบเทียบความสัมพันธ์ระหว่างเวลาเฉลี่ยที่ใช้ในการตรวจพิสูจน์ (นาที) กับค่าระดับขีดจำกัดที่ขนาดบล็อกพิกเซล 20 x 20 พิกเซล และขนาดบล็อกพิกเซล 10 x 10 พิกเซล

### 5. สรุปผลการวิจัย

จากการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่ผ่านการปลอมแปลงด้วยเครื่องมือตรวจพิสูจน์การปลอมแปลง โดยใช้การเปรียบเทียบค่าสีของแต่ละพิกเซลในรูปที่อยู่ในระบบเมทริกซ์ โดยใช้เครื่องมือที่พัฒนาขึ้นจากโปรแกรม MATLAB ซึ่งจะมีการใช้ขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดที่แตกต่างกัน จากการทดสอบกับภาพถ่ายดิจิทัลจำนวน 100 ภาพ พบว่าการใช้ขนาดบล็อกพิกเซลเท่ากับ 10 และระดับค่าขีดจำกัดเท่ากับ 5 ให้ผลการตรวจสอบที่ถูกต้องมากที่สุดจำนวน 59 ภาพ

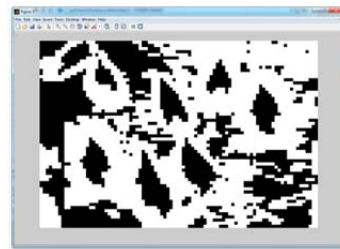
#### 5.1 อภิปรายผล

จากผลการตรวจพิสูจน์จะเห็นได้ว่าการกำหนดขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดที่เหมาะสมมีผลต่อความถูกต้องและระยะเวลาในการตรวจสอบ ซึ่งในการวิจัยนี้การใช้ขนาดบล็อกพิกเซล 10 x 10 พิกเซล และค่าระดับขีดจำกัดเท่ากับ 5 ให้ผลการตรวจที่ถูกต้อง โดยแสดงส่วนที่มีการปลอม

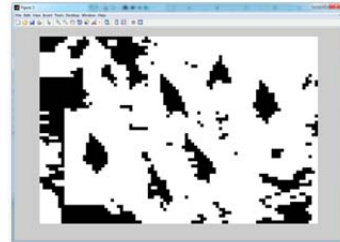
แปลงอย่างชัดเจนประมาณร้อยละ 60 แต่อย่างไรก็ตามในการตรวจพิสูจน์ยังมีหลายปัจจัยที่มีผลต่อการตรวจดังนี้

#### 1. การกำหนดขนาดบล็อกพิกเซลและค่าขีดจำกัด

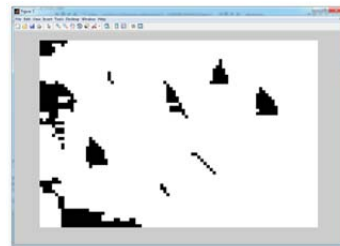
การกำหนดขนาดบล็อกพิกเซลและค่าขีดจำกัดมีผลสำคัญต่ออัตราความถูกต้องในการตรวจพิสูจน์ถ้าเลือกใช้บล็อกขนาดใหญ่เกินไป หรือกำหนดค่าระดับขีดจำกัดมากเกินไปก็อาจได้ผลเป็น False Positive ได้



(ก)



(ข)



(ค)

รูปที่ 10 ภาพแสดงผลการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่ใช้ขนาดบล็อกพิกเซล 20 x 20 และค่าระดับขีดจำกัดแตกต่างกันคือ (ก) th=10, (ข) th=5 และ (ค) th=1 ตามลำดับ

## 2. ระยะเวลาที่ใช้ในการตรวจพิสูจน์

ขนาดของบล็อกพิกเซลและค่าขีดจำกัดที่เลือกใช้มีผลโดยตรงกับระยะเวลาในการตรวจพิสูจน์ โดยยิ่งใช้ขนาดบล็อกพิกเซลที่เล็กและค่าขีดจำกัดที่น้อย ก็จะทำให้เวลาที่ใช้ในการตรวจพิสูจน์เพิ่มมากขึ้นด้วยเป็นทวีคูณ และยิ่งอาจส่งผลให้ผลการตรวจพิสูจน์ที่ได้มีโอกาสเป็น False Negative มากอีกด้วย

## 3. ลักษณะของภาพถ่ายที่ใช้ในการตรวจพิสูจน์

ลักษณะของภาพถ่ายที่นำมาตรวจพิสูจน์เอง ก็มีผลต่อความถูกต้องแม่นยำในการตรวจพิสูจน์เช่นกัน โดยจากการวิจัยพบว่ารูปที่ส่วนของรูปที่มีสีสันใกล้เคียงกันเป็นพื้นที่ขนาดใหญ่ เช่น ท้องฟ้า ทะเล กำแพง ที่มีความแตกต่างกันของสีน้อยหรือไม่มีเลย มักจะทำให้ผลการตรวจพิสูจน์ผิดพลาด โดยผลการตรวจพิสูจน์มักแสดงบริเวณที่ตรวจพบการปลอมแปลงมากกว่าความเป็นจริง (False Positive) เนื่องจากมีค่าสีที่ใกล้เคียงกัน ในขณะที่เดียวกันรูปที่มีรายละเอียดของภาพค่อนข้างมาก หรือมีส่วนต่างของสีสันในภาพมาก ก็มีแนวโน้มที่ผลการตรวจพิสูจน์จะแสดงบริเวณที่ตรวจพบการปลอมแปลงน้อยกว่าความเป็นจริง (False Negative) เนื่องจากมีค่าสีในพื้นที่นั้นๆ ของภาพแตกต่างกันมากเกินกว่าค่าที่กำหนด

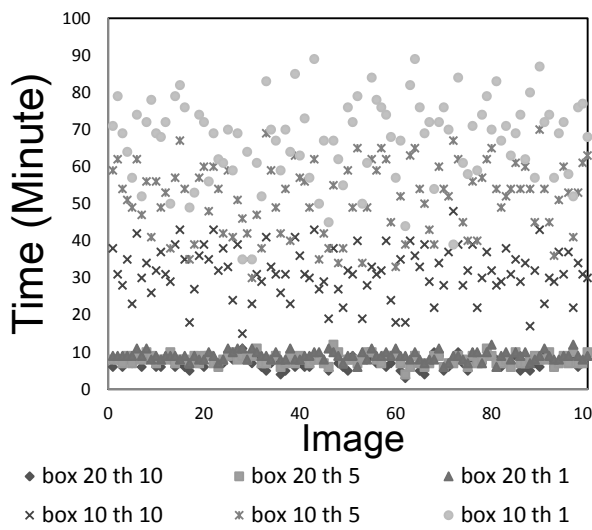
## 4. บริเวณที่มีการปลอมแปลงในภาพ

ตำแหน่งที่มีการปลอมแปลงในภาพก็มีผลต่อผลการตรวจพิสูจน์ เนื่องจากในการตรวจพิสูจน์นั้นใช้การแบ่งภาพออกเป็นบล็อกพิกเซลที่ขนาดต่างๆ กัน แล้วใช้การเปรียบเทียบค่าสีกับบล็อกถัดไปเพื่อระบุตำแหน่งที่มีการปลอมแปลง ทำให้มีโอกาสที่ตำแหน่ง

ของส่วนที่เป็นต้นฉบับ กับส่วนที่มีการคัดลอกไปจะไม่ตรงกันเมื่อแบ่งภาพด้วยบล็อกพิกเซล หรือตำแหน่งที่มีการปลอมแปลงด้วยวิธีการคัดลอกและเคลื่อนย้ายมีขนาดเล็กกว่าขนาดของบล็อกพิกเซลที่ใช้ ก็อาจทำให้ผลการตรวจพิสูจน์ออกมาคลาดเคลื่อนได้ ซึ่งในกรณีนี้สามารถลดความผิดพลาดของผลการตรวจพิสูจน์ได้โดยการเลือกกำหนดขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดให้ละเอียดขึ้น แต่หากกำหนดขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดน้อยมากเกินไปอาจทำให้ใช้เวลาในการตรวจพิสูจน์มากเกินไป และยิ่งอาจทำให้ได้ผลการตรวจพิสูจน์แสดงบริเวณที่ตรวจพบการปลอมแปลงน้อยกว่าความเป็นจริง (False Negative) เพิ่มขึ้นอีกด้วย

## 5. ระยะเวลาการตรวจพิสูจน์

ในงานวิจัยนี้ถึงแม้ว่าจะใช้รูปที่นำมาตรวจพิสูจน์ที่มีขนาดเท่ากันคือขนาด 1800 x 1200 พิกเซล และกำหนดขนาดบล็อกพิกเซลและค่าระดับขีดจำกัดที่เท่ากัน แต่พบว่าระยะเวลาที่ใช้ในการตรวจพิสูจน์ในแต่ละภาพใช้เวลาไม่เท่ากัน ที่เป็นเช่นนี้เนื่องจากว่าในขั้นตอนการออกแบบเครื่องมือนี้ ผู้วิจัยได้กำหนดให้เมื่อตรวจพบบล็อกที่มีความแตกต่างกันน้อยกว่าค่าระดับขีดจำกัดที่กำหนดไว้แล้ว ให้ทำการตรวจสอบบล็อกถัดไปทางขวาที่ติดกันอีก 4 บล็อก เพื่อลดความผิดพลาดจากการตรวจสอบ ทำให้กระบวนการเปรียบเทียบบล็อกพิกเซลถัดไปอีก 4 บล็อกเมื่อพบคู่บล็อกที่เหมือนกันเกิดขึ้นไม่เท่ากันในแต่ละภาพ ทำให้เวลาที่ใช้ในการตรวจพิสูจน์นั้นแตกต่างกันไป ดังแสดงในรูปที่ 11



รูปที่ 11 แผนภูมิแสดงเวลาที่ใช้ในการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่แตกต่างกันในแต่ละภาพ

## 6. การแปรผลข้อมูล

ผลการตรวจพิสูจน์ที่ได้จากเครื่องมืออยู่ในรูปของภาพขาว-ดำ (Binary Image) โดยส่วนที่เป็นสีดำแสดงถึงส่วนที่เครื่องมือตรวจพบบริเวณที่มีการปลอมแปลงในภาพ เนื่องจากผลที่ได้เป็นรูปที่ต้องอาศัยการแปลผลของผู้ทำการตรวจพิสูจน์ จึงทำให้

อาจมีความคลาดเคลื่อนในการตัดสินใจได้ ดังนั้นทักษะการใช้เครื่องมือ และประสบการณ์ของผู้ตรวจพิสูจน์ จึงเป็นสิ่งสำคัญ

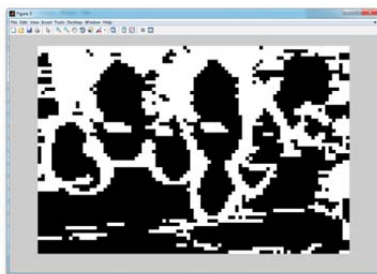
ดังรูปที่ 12 จะเห็นได้ว่า ผลที่ได้จากการใช้ขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดในการตรวจพิสูจน์ที่  $box=20$  และ  $th=10$  และ  $th=5$  แม้จะยังไม่สามารถระบุส่วนที่มีการปลอมแปลงในภาพได้อย่างชัดเจน แต่ก็ทำให้เห็นถึงบริเวณที่อาจจะมีการปลอมแปลงได้ และเมื่อปรับขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดไปจนถึง  $box=10$  และ  $th=1$  ก็จะทำให้ได้ผลลัพธ์ที่แสดงบริเวณที่มีการปลอมแปลงได้อย่างชัดเจน ซึ่งการเลือกใช้ขนาดของบล็อกพิกเซลและค่าระดับขีดจำกัดนี้จำเป็นต้องอาศัยการทดลองซ้ำ และทักษะในการสังเกตภาพของผู้ตรวจพิสูจน์ด้วย



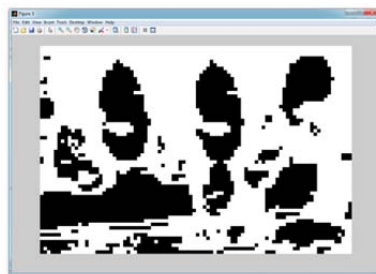
Original Image



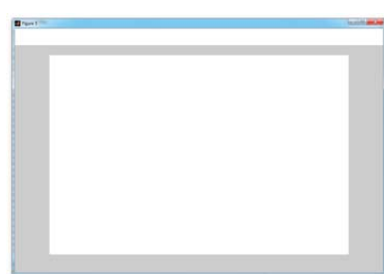
Forgery Image



box=20, th=10



box=20, th=5



box=20, th=1



รูปที่ 12 ภาพแสดงผลการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่มีการใช้ขนาดบล็อกพิกเซลและค่าระดับสีที่จำกัดแตกต่างกัน

#### 5.4 ข้อเสนอแนะ

ถึงแม้ว่าเครื่องมือในการตรวจพิสูจน์ภาพถ่ายดิจิทัลที่ผู้วิจัยได้พัฒนาขึ้นในครั้งนี้ จะสามารถใช้ตรวจพิสูจน์หาบริเวณที่มีการปลอมแปลงในภาพถ่ายดิจิทัลได้ตามวัตถุประสงค์ แต่อย่างไรก็ตามเครื่องมือนี้ยังมีข้อบกพร่องอีกหลายประการที่ควรนำไปพัฒนาในงานวิจัยครั้งต่อไป ดังนี้

- ควรพัฒนาส่วนติดต่อผู้ใช้ (Graphic User Interface) เพื่อให้สามารถใช้งานได้สะดวกขึ้น

- เครื่องมือตรวจสอบได้เฉพาะภาพถ่ายดิจิทัลที่ผ่านการปลอมแปลงด้วยวิธีคัดลอกและเคลื่อนย้ายเพียงอย่างเดียว ไม่สามารถตรวจพิสูจน์ภาพถ่ายดิจิทัลที่ผ่านการแก้ไขปลอมแปลงด้วยวิธีการอื่นๆ ได้ ซึ่งในการตรวจสอบจำเป็นที่จะต้องใช้อย่างน้อยวิธีร่วมกัน

- การตรวจพิสูจน์ยังต่ออาศัยทักษะและประสบการณ์ของผู้ทำการตรวจในการระบุส่วนที่มีการปลอมแปลง จึงอาจเกิดความคลาดเคลื่อนจากผู้ใช้งานได้

- ผลการตรวจพิสูจน์ไม่สามารถที่จะระบุได้ว่าบริเวณที่พบการปลอมแปลงนั้น ส่วนใดเป็นต้นฉบับ และส่วนใดที่เป็นส่วนที่คัดลอกมา ผู้ทำการตรวจพิสูจน์ต้องอาศัยความเชี่ยวชาญในการตัดสินใจ

- ผลการตรวจพิสูจน์ที่ได้นั้นหากว่าพบส่วนที่ผ่านการปลอมแปลงได้อย่างชัดเจน จะสรุปได้ว่าการปลอมแปลงด้วยวิธีคัดลอกและเคลื่อนย้ายในภาพ แต่หากว่าตรวจไม่พบบริเวณที่มีการปลอมแปลง จะไม่สามารถตัดสินได้ว่าภาพถ่ายนั้นไม่มีปลอมแปลง เนื่องจากภาพถ่ายดิจิทัลนั้นอาจผ่านการปลอมแปลงด้วยวิธีการอื่นก็เป็นได้

#### เอกสารอ้างอิง

[1] N.Krawetz "A Picture's worth digital image analysis and forensics" Black hat briefing, USA 2007

[2] J.Lukáš, J.Fridrich, and M.Goljan "Detecting Digital Image Forgeries Using Sensor Pattern Noise" Department of Electrical and Computer Engineering, SUNY Binghamton 2006

[3] A.Popescu and H.Farid "Exposing Digital Forgeries by Detecting Duplicated Image Regions" Department of Computer Science, Dartmouth College 2004

[4] J.Fridrich, D.Soukal, and J.Lukáš "Detection of Copy-Move Forgery in Digital Images"

Department of Electrical and Computer Engineering, SUNY Binghamton 2009

[5] Y.Cao, T.Gao, L.Fan, Q.Yang "A robust detection algorithm for copy-move forgery in digital images" College of Information Technical Science, Nankai University 2011

[6] P.Yadav "Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform" Department of Computer Science and Engineering, CSVTU 2012