

การพัฒนาโปรแกรมประยุกต์ในการรักษาความปลอดภัยและความเป็นส่วนตัวของผู้ใช้ QR Code ด้วยเทคนิคการอำพรางในภาพเพื่อการสื่อสารที่มีประสิทธิภาพในกองทัพอากาศ

The Application Development in Security and Privacy of QR Code Users Using Steganography Techniques for Efficient Communication in the Royal Air Force

^{1*} ภูมิพัฒน์ ดวงกลาง และ ^{2#} ประสงค์ ประณีตพลกรัง

^{1,2} กองการศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช

^{1*} Phummipat Daungklang and ^{2#} Prasong Praneetpolgrang

^{1,2} Faculty of Academic, Navaminda Kasatriyadhiraj Royal Air Force Academy

*phummipat_d@rtaf.mi.th, #prasong_pr@rtaf.mi.th

บทคัดย่อ

Quick Response Code หรือ QR Code เป็นบาร์โค้ดในรูปแบบเหลี่ยมจัตุรัส 2 มิติที่เป็นผลลัพธ์จากการแปลงข้อความให้อยู่ในรูปแบบภาพที่สามารถเข้าถึงได้ง่าย และรวดเร็วผ่านอุปกรณ์พกพา มีประโยชน์ที่ใช้แทนการส่งข้อมูลที่มีความซับซ้อน และยากต่อการจดจำ ดังนั้น QR Code จึงได้รับความนิยมใช้สำหรับการติดต่อสื่อสาร และแลกเปลี่ยนข้อมูลข่าวสารในปัจจุบัน อย่างไรก็ตาม หากใช้ QR Code อย่างไม่ระมัดระวังอาจเป็นจุดเริ่มต้นของความเสียหายที่ทำให้เกิดความเสียหายต่อหน่วยงานหรือถูกละเมิดความเป็นส่วนตัวได้ ดังนั้น ผู้วิจัยจึงได้พัฒนาระบบการอำพราง QR Code ในภาพ โดยใช้เทคนิคการอำพรางข้อมูลไว้ที่ค่าพิกเซลของภาพแบบบิตนัยสำคัญน้อยที่สุด (Least Significant Bit: LSB) เพื่อเพิ่มประสิทธิภาพในการติดต่อสื่อสารด้วย QR Code ให้มีความปลอดภัย และน่าเชื่อถือ ผลลัพธ์ที่ได้คือภาพหลังการอำพราง QR Code มีความคล้ายคลึงกับภาพต้นฉบับจนยากต่อการแยกแยะด้วยสายตามนุษย์ ซึ่งสามารถใช้ในการติดต่อสื่อสาร และแลกเปลี่ยนข่าวสารได้อย่างปลอดภัยในระบบเครือข่าย

คำสำคัญ: การอำพรางข้อมูล, รหัสคิวอาร์โค้ด, บิตนัยสำคัญน้อยที่สุด

Received : March 29, 2021

Revised : March 14, 2022

Accepted : March 31, 2022

Abstract

A QR Code (Quick Response Code) is a 2D square barcode that is a result from conversion of text into an image format, which can be quickly and easily accessed via mobile devices. They can be used as a substitute for transmitting complex and difficult-to-remember information, so QR codes are popular today for communicating and exchanging information. However, if QR codes are used carelessly, they can cause damage to organization or breach of privacy. Therefore, the researcher has developed a system for concealing the QR Code in an image by using the Least Significant Bit (LSB) pixel value masking technique in order to increase the efficiency of communication with QR Code safely and reliable. The result is that the image after QR code "camouflage" is so similar to original image that it is difficult to be distinguished by human eyes. It can be used for communication and information exchange securely in the network.

Keywords: Steganography, QR Code, Least Significant Bit

1. บทนำ

ในปัจจุบันการสื่อสารข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ตได้รับความนิยมอย่างกว้างขวาง โดยเห็นได้จากโปรแกรมประยุกต์ (Application) ที่มีจำนวนมากขึ้น และมีการพัฒนาแบบก้าวกระโดด รวมถึงแพลตฟอร์มด้านสื่อสังคมออนไลน์ที่มีฟังก์ชันในการอำนวยความสะดวกให้การติดต่อสื่อสารข้อมูลระหว่างผู้ส่ง และผู้รับสารให้เป็นไปอย่างมีประสิทธิภาพ ซึ่งแพลตฟอร์มที่กำลังเป็นที่นิยม ได้แก่ Line WhatsApp Facebook และ Instagram เป็นต้น ในส่วนของข้อมูลที่ใช้ในการติดต่อสื่อสารพบว่า ภาพ (Image) ได้รับความนิยมอย่างมาก เนื่องจากภาพสามารถทำให้ผู้รับสารเข้าใจเนื้อหารายละเอียดของสารได้อย่างรวดเร็ว ซึ่งรูปแบบของภาพที่นิยมใช้สื่อสารกันบนสื่อสังคมออนไลน์ ได้แก่ ภาพถ่าย โพสต์เตอร์ และอินโฟกราฟิกส์ (Infographics) เป็นต้น นอกจากนี้ ข้อมูลที่อยู่ในรูปแบบข้อความ (Text) ยังถูกแปลงให้เป็นภาพที่อยู่ในรูปแบบของรหัสคิวอาร์ (QR Code) ก่อนทำการส่งให้ผู้รับสารอีกด้วย

จากความนิยมในการใช้ภาพแทนข้อความในการติดต่อสื่อสาร ทำให้ภาพถูกใช้เป็นส่วนในการซ่อนข้อมูลลับหรือข้อมูลส่วนบุคคล ซึ่งกระบวนการซ่อนพรางข้อมูลนี้จะเรียกว่า วิทยาการอำพรางข้อมูล (Steganography) เป็นศาสตร์ที่มุ่งเน้นการทำให้ข้อความไม่สามารถอ่านและเข้าใจได้จากผู้ที่ไม่อยู่ในกลุ่มของผู้รับสาร ทำให้ข้อความสามารถส่งถึงกลุ่มผู้รับสารได้อย่างปลอดภัย และมีความน่าเชื่อถือ

นอกจากความนิยมในการอำพรางข้อมูลในภาพแล้ว การแปลงข้อมูลให้อยู่ในรูปแบบของรหัสคิวอาร์ (QR Code) ก่อนส่งให้กลุ่มผู้รับสารเป็นที่ได้รับความนิยมเช่นกัน ซึ่งในปัจจุบัน QR Code ถือได้ว่าเป็นเครื่องมือที่มีความสำคัญในการใช้สื่อสารข้อมูล โดยประโยชน์ที่เห็นได้ชัดของ QR Code คือ สามารถแปลงข้อมูลหรือหมายเลขที่ซับซ้อนที่จดจำได้ยากให้อยู่ในรูปแบบภาพที่สามารถเข้าถึงผ่านอุปกรณ์พกพาได้อย่างสะดวกและรวดเร็ว จากประโยชน์ของ QR Code ที่ได้กล่าวมาในข้างต้น กองทัพอากาศจึงได้นำ QR Code มาประยุกต์ใช้งานร่วมกับระบบสารสนเทศต่าง ๆ ได้แก่ ด้านกำลังพล ด้านการส่งกำลังบำรุง ด้านการรักษาความปลอดภัยพื้นที่ รวมถึงใช้แทนการส่งลิงค์แบบสำรวจออนไลน์ เป็นต้น อีกทั้งข้าราชการของกองทัพอากาศยังใช้ QR Code ในการทำกิจกรรมต่าง ๆ ในชีวิตประจำวันอีกด้วย ดังนั้นจึงสรุปได้ว่าในโลกยุคปัจจุบัน QR Code ได้เข้าไปมีบทบาทในทุกภาคส่วน

อย่างไรก็ตาม การใช้งาน QR Code ที่ไม่ระมัดระวัง และไม่คำนึงถึงการรักษาความปลอดภัยอาจจะส่งผลเสียต่อหน่วยงานหรือเจ้าของข้อมูลได้ เช่น การถูกละเมิดความเป็นส่วนตัวจากกรณีที่เบอร์หมายเลขโทรศัพท์ตกไปอยู่กับบุคคลที่สาม รวมถึงข้อมูลที่ได้จากการสำรวจ โดยใช้แบบสอบถามออนไลน์ไม่ตรงตามวัตถุประสงค์ที่กำหนดไว้ อันเนื่องมาจากแบบสอบถามถูกส่งไม่ตรงกลุ่มเป้าหมาย ดังนั้น เพื่อเป็นการเพิ่มความปลอดภัย QR Code ก่อนทำการส่งให้ผู้รับสาร ผู้วิจัยจึงมีแนวคิดพัฒนาโปรแกรมประยุกต์สำหรับอำพราง QR Code ในภาพเพื่อเพิ่มประสิทธิภาพให้กับการสื่อสารข้อมูลผ่านระบบเครือข่ายให้มีความปลอดภัย ตลอดจนเป็นต้นแบบการพัฒนาโปรแกรมที่ใช้วิทยาการอำพรางข้อมูลสำหรับใช้งานในกองทัพอากาศต่อไป

2. ขอบเขตงานวิจัย

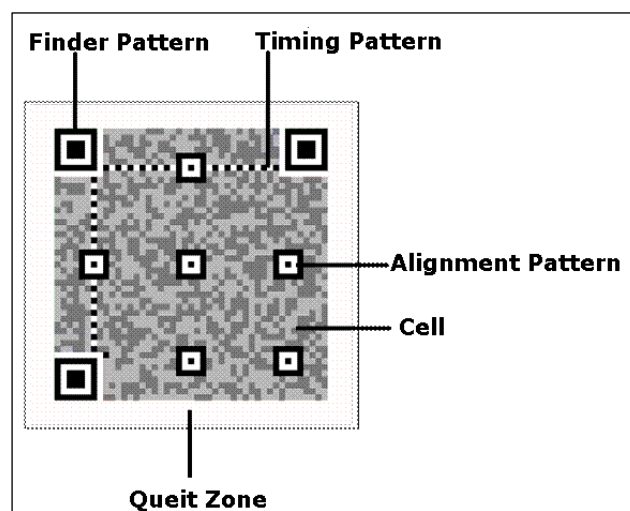
งานวิจัยนี้เป็นการพัฒนาโปรแกรมประยุกต์สำหรับใช้เป็นเครื่องมือในการอำพราง QR Code ในภาพก่อนส่งให้ผู้รับสารผ่านระบบเครือข่าย เพื่อเพิ่มความปลอดภัยในการติดต่อสื่อสาร รวมถึงสามารถรักษาความเป็นส่วนตัวของผู้ใช้ QR Code ซึ่งการพัฒนาโปรแกรมต้นแบบจะใช้เทคนิคการอำพราง QR Code ไว้ที่ค่าพิกเซลของภาพโดยใช้เทคนิค Least Significant Bit (LSB) ใช้ภาษาไพทอนในการพัฒนาโปรแกรม และใช้ไลบรารี OpenCV สำหรับการประมวลผลข้อมูลภาพดิจิทัล รวมถึงใช้โปรแกรมระบบจัดการฐานข้อมูล MySQL สำหรับจัดการบัญชีผู้ใช้งาน

3. แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

3.1 QR Code (Quick Response Code)[1]

เป็นบาร์โค้ดที่อยู่ในรูปแบบสองมิติรูปสี่เหลี่ยมจัตุรัสมีโมดูลข้อมูลตั้งแต่ 21x21 ถึง 177x177 สามารถบรรจุข้อมูลตัวเลขได้ 7,089 ตัวเลข หรือ 4,296 ตัวอักษร ซึ่งข้อมูลที่บรรจุอยู่ใน QR Code จะอยู่ในรูปแบบของค่าไบนารี 0 และ 1 โดย ค่า 0 จะแทนพื้นที่สีขาว และค่า 1 จะแทนพื้นที่สีดำ ในส่วนโครงสร้างภายในของ QR Code (ตามรูปที่ 1) ประกอบด้วย

- 3.1.1 Finder pattern สำหรับการตรวจหาตำแหน่งในการอ่านข้อมูล
- 3.1.2 Timing pattern สำหรับการตรวจตำแหน่งของแต่ละเซลล์
- 3.1.3 Alignment Pattern สำหรับแก้ไขการบิดเบือนของ QR Code
- 3.1.4 Quiet Zone เป็นพื้นที่ขอบ QR Code
- 3.1.5 Data Area หรือ Cell เป็นพื้นที่สำหรับเก็บข้อมูล



รูปที่ 1 ส่วนประกอบของ QR Code

จากประโยชน์ของ QR Code ที่ผู้ใช้งานสามารถแปลงข้อมูลหรือหมายเลขที่มีความซับซ้อนยากต่อการจดจำให้อยู่ในรูปแบบภาพที่สามารถเข้าถึงได้ง่ายผ่านอุปกรณ์พกพา นั้น ทำให้ QR Code ได้รับความนิยมนำมาประยุกต์ใช้กับงานในหลากหลายด้าน ตัวอย่างเช่น การประยุกต์ใช้ QR Code เพื่อส่งเสริมกิจกรรมการเรียนรู้ สำหรับศูนย์รวมรวมสายพันธุ์กล้วยเฉลิมพระเกียรติ จังหวัดกำแพงเพชร ที่ทำให้ผู้มาใช้บริการมีความสะดวกขึ้นในการเข้าถึงข้อมูลของกล้วยไม้สายพันธุ์ต่าง ๆ เช่น ชื่อสายพันธุ์ ความแข็งแรงทนทาน รูปแบบเด่นชัด ชื่อวิทยาศาสตร์ ข้อมูลทั่วไป ลำต้น ใบ ดอกผล และประโยชน์ของกล้วยไม้ชนิดนั้น ๆ เป็นต้น [2] ซึ่งผลลัพธ์จากการสำรวจความพึงพอใจการประยุกต์ใช้งาน QR Code อยู่ในระดับที่สูงมาก นอกจากนี้ QR Code ยังสามารถนำมาใช้กับการบริหารข้อมูลทะเบียนพัสดุ หรือสิ่งของต่าง ๆ ได้ เช่น การประยุกต์ใช้เทคโนโลยี QR Code เพื่อจัดทำทะเบียนพรรณไม้สวนพฤกษศาสตร์โรงเรียน [3] เป็นต้น

3.2 การอำพรางข้อมูล (Steganography)

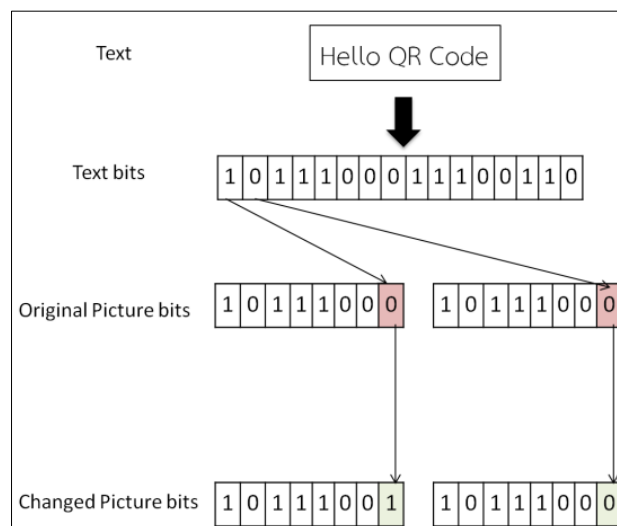
เป็นการสื่อสารข้อมูลที่ใช้เทคนิคการซ่อนพรางข้อมูลชนิดหนึ่งแฝงไปกับข้อมูลอีกชนิดหนึ่งให้ดูเหมือนว่าไม่มีการอำพรางข้อมูลใด ๆ มีวัตถุประสงค์เพื่อไม่ให้บุคคลที่สามสามารถมองเห็น รับรู้ และเข้าใจได้จากสายตาปกติ ซึ่งการอำพรางข้อมูล (Steganography) จะเป็นวิธีที่มุ่งเน้นไม่ให้บุคคลที่สามสามารถรับรู้ได้ถึงการมีอยู่ของข้อมูลลับ

ในขณะที่วิทยาการเข้ารหัสลับ (Cryptography) จะเน้นการทำให้ข้อมูลไม่สามารถอ่านและเข้าใจได้ โดยทั่วไปแล้วการอำพรางข้อมูลจะต้องมีการเตรียมการ และออกแบบข้อมูลลับให้อยู่ในรูปแบบที่มีความเหมาะสมต่อการนำไปอำพรางบนสื่อสัญญาณต่าง ๆ เช่น การอำพรางข้อความในภาพจะต้องทำการแปลงข้อความให้อยู่ในรูปแบบรหัส ASCII หรือ Byte เพื่อให้เหมาะสมพร้อมที่จะนำเข้าไปเผยแพร่ร่วมกับแต่ละค่าพิกเซลของภาพ

ปัจจุบันการอำพรางข้อมูลในภาพได้รับความนิยมอย่างแพร่หลาย เนื่องจากภาพเป็นเครื่องมือที่ใช้ในการติดต่อสื่อสารที่มีประสิทธิภาพ สามารถทำให้ผู้รับสารรับรู้และเข้าใจในเนื้อหาของสารได้ง่ายและรวดเร็ว โดยการอำพรางข้อมูลในภาพแบ่งได้หลัก ๆ ดังนี้ การอำพรางข้อมูลเชิงโดเมนพื้นที่ ซึ่งจะซ่อนข้อมูลไว้ที่ค่าพิกเซล (Pixel) ของภาพ และการอำพรางข้อมูลไว้ที่โดเมนความถี่ที่ได้จากการแปลงโคไซน์ไม่ต่อเนื่อง (Discrete Cosine Transform : DCT) นอกจากนี้ยังมีการอำพรางข้อมูลภาพแบบผสมร่วมกันระหว่างเชิงโดเมนพื้นที่ และความถี่อีกด้วย สำหรับงานวิจัยนี้ ผู้วิจัยจะใช้การอำพรางข้อมูลไว้ที่ค่าพิกเซลของภาพ โดยพิจารณาการอำพรางข้อมูลไว้ที่บิตนัยสำคัญน้อยที่สุด (Least Significant Bit : LSB) เนื่องจากสามารถเข้าใจได้ง่าย และสามารถใช้ได้กับข้อมูลภาพทุกประเภท อย่างไรก็ตาม การอำพรางข้อมูลในภาพลักษณะนี้อาจจะสามารถทำให้เห็นถึงความบิดเบือนข้อมูลหลังจากที่มีการอำพรางแล้วได้ง่ายกว่า เมื่อเปรียบเทียบกับวิธีการอำพรางข้อมูลในรูปแบบเชิงโดเมนความถี่

การอำพรางข้อมูลในภาพแบบบิตนัยสำคัญน้อยที่สุด Least Significant Bit (LSB) [1] มีหลักการคือจะอำพรางข้อความไว้ที่บิตที่มีนัยสำคัญน้อยที่สุด เนื่องจากจะทำให้มีการเปลี่ยนแปลงเฉดสีในภาพน้อยที่สุด และยากที่จะสังเกตเห็นด้วยสายตาของมนุษย์ สำหรับกระบวนการอำพรางข้อมูลแบบ Least Significant Bit มีขั้นตอน (ตามรูปที่ 2) ดังนี้

- 3.2.1 แปลงข้อมูลที่ต้องการจะอำพรางให้อยู่ในรูปแบบ ASCII Byte
- 3.2.2 แปลงข้อมูลจากรูปแบบ ASCII Byte เป็นบิต
- 3.2.3 แปลงข้อมูลภาพที่ต้องการที่จะใช้เป็นสื่อให้อยู่ในรูปแบบบิต
- 3.2.4 นำแต่ละบิตของข้อมูลไปแทนที่บิตสุดท้ายของแต่ละค่าพิกเซลในภาพจนครบทุกบิตของข้อมูล



รูปที่ 2 การอำพรางข้อความโดยใช้วิธีการ LSB

จากวัตถุประสงค์ของการอำพรางข้อมูลที่มุ่งเน้นไม่ให้นักลับที่สามสามารถรับรู้ได้ถึงการมีอยู่ของข้อมูลลับ จึงทำให้มีการประยุกต์ใช้เทคนิคการอำพรางข้อมูลร่วมกับงานด้านการรักษาความปลอดภัยข้อมูล โดยมีงานวิจัยที่เกี่ยวข้องกับเทคนิคการอำพรางข้อมูลในหลากหลายรูปแบบ ได้แก่ การฝังข้อมูลลับเกี่ยวกับการทำ Transaction ทางการค้าไปบน QR Code เพื่อสร้างทางเลือกให้กับผู้ใช้งาน QR Code สามารถติดต่อสื่อสารข้อมูลลับผ่านการใช้ QR Code โดยไม่เพิ่มภาระให้กับ

ระบบมากเกินไป [1] นอกจากนี้ พบว่ามีการพัฒนาโปรแกรมประยุกต์สำหรับใช้อำพรางข้อมูลที่มีการเข้ารหัสแล้วนำไปทำการอำพรางลงบนภาพ เพื่อเพิ่มความปลอดภัยของข้อมูลลับให้มากยิ่งขึ้น โดยผลลัพธ์ที่ได้จากงานวิจัยดังกล่าวจะทำให้ยากที่จะรับรู้ได้ว่ามีข้อมูลลับ รวมถึงหากรับรู้ก็ยากต่อการถอดรหัสข้อมูลลับ เพื่อทำความเข้าใจ [4]

4. การดำเนินการวิจัย

จากความนิยมในการใช้ QR Code ในการแปลงข้อมูลที่ซับซ้อนให้เป็นภาพสำหรับใช้ติดต่อสื่อสารผ่านช่องทางที่มีการรักษาความปลอดภัย ดังนั้น ผู้วิจัยจึงพัฒนาโปรแกรมประยุกต์สำหรับอำพรางข้อมูล QR Code ในภาพ โดยการพัฒนาที่ใช้แนวทางของวงจรการพัฒนาระบบ (System Development Life Cycle : SDLC) [5] ประกอบด้วย ดังนี้

4.1 กำหนดปัญหา

ปัจจุบันกองทัพอากาศยึดถือแนวทางการพัฒนาระบบงานบนพื้นฐานการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO) [6] ที่มุ่งเน้นการติดต่อสื่อสาร และแลกเปลี่ยนข้อมูลข่าวสารระหว่างหน่วยงานผ่านเครือข่าย ทำให้ในปัจจุบันข้าราชการส่วนใหญ่มีทักษะและขีดความสามารถในการปฏิบัติงาน ติดต่อสื่อสาร และแลกเปลี่ยนข้อมูลกันผ่านระบบเครือข่ายโดยใช้โปรแกรมประยุกต์ หรือแพลตฟอร์มสื่อสารออนไลน์ที่กองทัพอากาศอนุมัติให้ใช้งาน และหนึ่งในเทคโนโลยีที่ได้รับความนิยมใช้ในการแลกเปลี่ยนข้อมูลข่าวสารระหว่างกันคือ QR Code ซึ่งการใช้ QR Code อย่างไม่มีมัลแวร์อาจทำให้ผู้ที่ไม่ประสงค์ดีสามารถเข้าถึงข้อมูล และอาจส่งผลกระทบต่อหน่วยงาน เจ้าของข้อมูล รวมถึงตัวผู้ส่ง QR Code ดังนั้น QR Code จำเป็นต้องมีการรักษาความปลอดภัยก่อนการส่งให้ผู้รับสาร

4.2 การวิเคราะห์

จากปัญหาที่ QR Code จำเป็นต้องได้รับการรักษาความปลอดภัยก่อนส่งให้ผู้รับสาร ผู้วิจัยจึงได้วิเคราะห์ความต้องการ และมีแนวทางการรักษาความปลอดภัย QR Code ดังนี้

4.2.1 QR Code จะต้องผ่านกระบวนการอำพรางในภาพก่อนส่งให้ผู้รับสาร

4.2.2 ข้อมูลผู้ส่งและผู้รับสารจะต้องถูกอำพรางในภาพด้วยเพื่อใช้กำหนดและยืนยันกลุ่มของผู้รับสารให้ชัดเจน

4.2.3 ผู้ใช้งานจะต้องทำการลงทะเบียนก่อนการใช้งานระบบอำพรางข้อมูล

4.3 การออกแบบ

จากข้อมูลที่ได้ในขั้นตอนการวิเคราะห์ระบบ ผู้วิจัยจึงได้ออกแบบระบบอำพราง QR Code ในภาพ (รูปที่ 3) มีรายละเอียดดังนี้

4.3.1 ระบบอำพราง QR Code จะประกอบด้วย ส่วนฐานข้อมูลผู้ใช้งานที่ใช้จัดเก็บบัญชีผู้ใช้งาน ซึ่งบริหารจัดการบัญชีผู้ใช้งานผ่านโปรแกรม Web User Manager และอำพราง QR Code ในภาพด้วยโปรแกรม QR Steganography Client โปรแกรมทั้งสองส่วนจะทำงานร่วมกันโดยผู้ใช้งานจะต้องมีข้อมูลในระบบฐานข้อมูลของโปรแกรม Web User Manager ถึงจะสามารถเข้าใช้งานโปรแกรม QR Steganography Client ได้

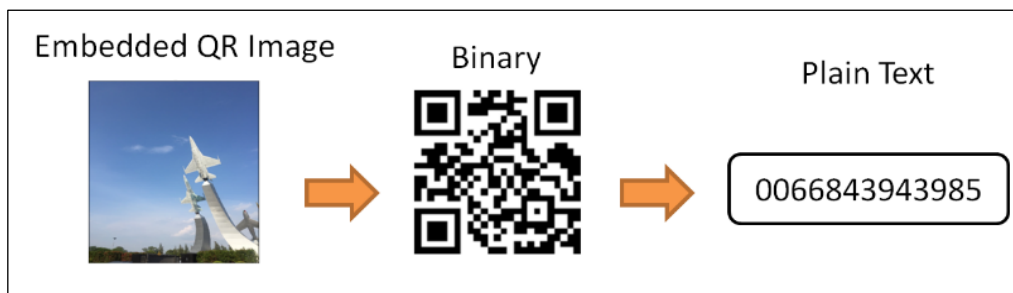
4.3.2 ผู้ใช้งานจะเริ่มต้นการใช้งานโดยการลงทะเบียนผ่านโปรแกรม Web User Manager

4.3.3 หลังจากการลงทะเบียนผู้ใช้งานจะทำการดาวน์โหลดโปรแกรม QR Steganography Client เพื่อใช้ในการอำพราง QR Code ในภาพ ซึ่งการใช้งานในแต่ละครั้ง ระบบจะทำการตรวจสอบสิทธิ์ และสถานะผู้ใช้งานในฐานข้อมูลบัญชีผู้ใช้งาน รวมถึงระบบจะเก็บประวัติการใช้งานของผู้ใช้งานแต่ละคนอีกด้วย


```
def make_secrete_qrcode_image(base_image,qr_image):
    rows,cols = qr_image.shape
    for row in range(rows):
        for col in range(cols):
            if qr_image[row,col] > 0 :
                base_image[row,col,0] = base_image[row,col,0]+1
    return base_image
```

รูปที่ 5 อัลกอริทึมปรับค่าบิตสุดท้ายของภาพสำหรับซ่อน QR Code

สำหรับกระบวนการกู้คืน QR Code จะเป็นกระบวนการย้อนกลับของกระบวนการอำพราง (รูปที่ 6) โดยจะพิจารณาค่า Pixel ในภาพผลลัพธ์ที่ได้จากการอำพรางข้อมูล (The Embedded QR Image) ว่าเป็นเลขคู่หรือเลขคี่เพื่อนำมาสร้างเป็น QR Code (รูปที่ 7) ซึ่งในกรณีที่ค่า Pixel เป็นเลขคู่จะกำหนดให้ค่า Pixel ของภาพ QR Code เป็น 0 ในขณะที่ค่า Pixel เป็นเลขคี่จะกำหนดให้ค่า Pixel ของภาพ QR Code เป็น 1 โดยผลลัพธ์ที่ได้คือภาพ QR Code ที่อยู่ในรูปแบบไบนารีที่สามารถแปลงเป็นข้อความให้ผู้รับสารสามารถเข้าใจได้



รูปที่ 6 กระบวนการกู้คืน QR Code

```
def qrcode_decode(the_secret_image,rows,cols):
    result = np.zeros([rows,cols])
    pixels = np.array(the_secret_image)
    for row in range(rows):
        for col in range(cols):
            if pixels[row,col,0] % 2 != 0 :
                result[row,col] = 1
    return result
```

รูปที่ 7 อัลกอริทึมสร้าง QR Code

4.5 การติดตั้งระบบ

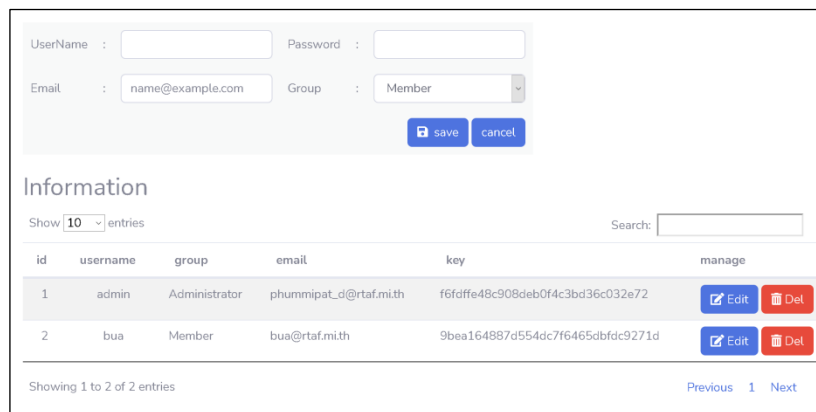
ระบบอำพราง QR Code ในภาพจะติดตั้งให้ผู้ใช้งานสามารถเข้าถึงระบบผ่านเครือข่ายของกองทัพอากาศ ซึ่งระบบจะติดตั้งบนระบบปฏิบัติการ Window Server 2012 และใช้ IIS เป็น Web Server โดยผู้ใช้งานสามารถลงทะเบียนและดาวน์โหลดโปรแกรมไปใช้งาน และเมื่อทำการอำพรางข้อมูลผ่านระบบแล้ว ผู้ใช้งานสามารถนำภาพที่ได้ส่งต่อให้กับผู้รับสารได้โดยที่บุคคลที่สามไม่สามารถรับรู้ว่ามีข้อมูลลับในภาพนั้น ๆ

5. ผลการวิจัย

การวิจัยนี้เป็นการพัฒนาระบบอำพราง QR Code ในภาพ มีวัตถุประสงค์เพื่อการรักษาความปลอดภัย QR Code ทำให้การติดต่อสื่อสารโดยใช้ QR Code มีความน่าเชื่อถือ รวมถึงสามารถอำพรางข้อมูลลับที่บุคคลที่สามไม่สามารถรับรู้หรือเข้าใจได้ โดยระบบจะประกอบด้วย ดังนี้

5.1 ส่วนบริหารจัดการบัญชีผู้ใช้งาน

ซึ่งทำหน้าที่ในการรับลงทะเบียน แก้ไขและลบบัญชีผู้ใช้งาน (ตามรูปที่ 8)



The screenshot displays a web-based user management interface. At the top, there is a form with fields for 'UserName', 'Password', 'Email' (pre-filled with 'name@example.com'), and 'Group' (a dropdown menu set to 'Member'). Below these fields are 'save' and 'cancel' buttons. Underneath the form is a section titled 'Information' containing a 'Show 10 entries' dropdown, a search bar, and a table of users. The table has columns for 'id', 'username', 'group', 'email', 'key', and 'manage'. It lists two users: 'admin' (Administrator) and 'bua' (Member). Each user entry has 'Edit' and 'Del' buttons in the 'manage' column. At the bottom, it shows 'Showing 1 to 2 of 2 entries' and navigation links for 'Previous', '1', and 'Next'.

id	username	group	email	key	manage
1	admin	Administrator	phummipat_d@rtaf.mi.th	f6fdffe48c908deb0f4c3bd36c032e72	Edit Del
2	bua	Member	bua@rtaf.mi.th	9bea164887d554dc7f6465dbfdc9271d	Edit Del

รูปที่ 8 ส่วนบริหารจัดการบัญชีผู้ใช้งาน

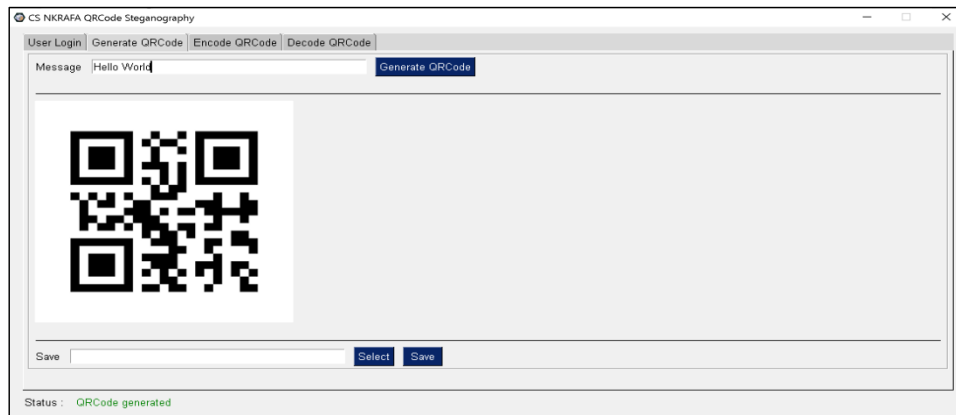
5.2 ส่วนโปรแกรมอำพราง QR Code (QR Steganography Client)

ทำหน้าที่ประมวลผลภาพสำหรับอำพราง QR Code ในภาพ โดยการทำงานจะประกอบด้วย 3 เมนูหลัก ดังนี้

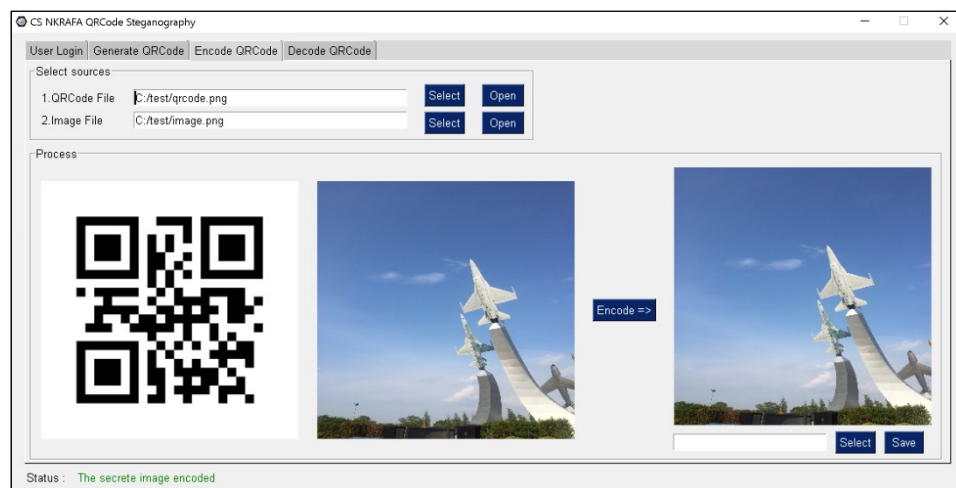
5.2.1 Generate QR Code จะทำหน้าที่ในการสร้าง QR Code (ตามรูปที่ 9)

5.2.2 Encode QR Code จะทำการประมวลผลการอำพราง QR Code ร่วมกับภาพ (ตามรูปที่ 10)

5.2.3 Decode QR Code เป็นส่วนที่จะใช้กู้คืน QR Code ที่ได้อำพรางไว้ในภาพ (ตามรูปที่ 11)



รูปที่ 9 ส่วนสร้าง QR Code



รูปที่ 10 ส่วนประมวลผลการอำพราง QR Code



รูปที่ 11 ส่วนประมวลผลการกู้คืน QR Code

6. สรุปผลการวิจัย

จากการประมวลผลอำพราง QR Code ในภาพด้วยโปรแกรม QR Steganography Client โดยใช้เทคนิค LSB พบว่า ภาพต้นฉบับก่อนการอำพราง QR Code ตามรูปที่ 12(ก) และภาพผลลัพธ์หลังอำพราง QR Code ตามรูปที่ 12 (ข) มีความคล้ายคลึงกันจนยากต่อการแยกแยะด้วยสายตาคิดว่าภาพใดมีการซ่อนพราง QR Code ในประเด็นขนาดของภาพที่ใช้เป็นสื่อสำหรับอำพราง QR Code นั้น สรุปได้ว่าภาพจะต้องมีขนาด หรือ Dimension ที่ใหญ่กว่า QR Code



รูปที่ 12 (ก) ภาพต้นฉบับ



รูปที่ 12 (ข) ภาพหลังการอำพรางข้อมูล

7. ข้อเสนอแนะ

ในปัจจุบัน QR Code มีความสำคัญต่อการติดต่อสื่อสารและแลกเปลี่ยนข้อมูลข่าวสาร โดยจะสังเกตได้จากผู้ใช้งานนิยมส่ง QR Code แทนการส่งข้อมูลที่มีความซับซ้อน และยากต่อการจดจำ อย่างไรก็ตามด้วยความสะดวกของการใช้ QR Code อาจทำให้ผู้ใช้งานใช้ QR Code อย่างไม่ระมัดระวังจนส่งผลให้เกิดความเสียหายต่อหน่วยงานหรือถูกละเมิดความเป็นส่วนตัว ดังนั้น ผู้วิจัยจึงได้พัฒนาระบบการอำพราง QR Code ในภาพ โดยใช้เทคนิคการอำพรางข้อมูลไว้ที่ค่าพิกเซลของภาพแบบ LSB เพื่อเพิ่มประสิทธิภาพในการติดต่อสื่อสารด้วย QR Code ให้มีความปลอดภัยและน่าเชื่อถือ โดยระบบสามารถอำพราง QR Code ในภาพที่ให้ภาพผลลัพธ์หลังการอำพราง QR Code มีความคล้ายคลึงกับภาพต้นฉบับจนยากต่อการแยกแยะด้วยสายตามนุษย์

สำหรับการวิจัยในอนาคตเพื่อเป็นการยกระดับมาตรการให้การรักษาความปลอดภัยและความเป็นส่วนตัวของผู้ใช้ QR Code ได้เพิ่มมากขึ้นนั้น ผู้วิจัยขอเสนอให้ทำการทดลองเข้ารหัสข้อความหรือข้อมูลก่อนการแปลงเป็น QR Code [7] รวมถึงทดลองประยุกต์การอำพรางข้อมูลไว้ที่ค่าอื่น ๆ ที่ไม่ใช่ค่าพิกเซลของภาพ หรือประยุกต์ใช้การอำพราง QR Code ไว้ที่การแปลงโคไซน์ไม่ต่อเนื่อง (DCT) ของภาพ เป็นต้น

8. เอกสารอ้างอิง

- [1] ปรีญาทิพย์ แดงมี และ วรพล ลีลาเกียรติสกุล. (2015). การอำพรางข้อมูลลับด้วย Steganography บน QRCode. JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY, 5(1) : 35-41.

- [2] ขวัญจุฑา คำบรรลือ, วิวัฒน์ มีสุวรรณ และ พิษณุภา ขวงสร้อย. (2560). การประยุกต์ใช้เทคโนโลยีคิวอาร์โค้ดเพื่อส่งเสริมกิจกรรมการเรียนรู้สำหรับศูนย์รวมสายพันธุ์กล้วย เณลิมพระเกียรติ จังหวัดกำแพงเพชร. วารสารศึกษาศาสตร์ มหาวิทยาลัยนเรศวร, 19(1) : 184-193.
- [3] กิตติพงษ์ จันทรถาวร และ ชุตินาถ วาฤทธิ. (2563). การประยุกต์ใช้เทคโนโลยีรหัสคิวอาร์เพื่อจัดทำทะเบียนพรรณไม้สวนพฤกษศาสตร์โรงเรียน. วารสารวิชาการนวัตกรรมการจัดการเทคโนโลยี มหาวิทยาลัยราชภัฏมหาสารคาม, 7(1) : 8-19.
- [4] มนธล พรหมวิเชียร และ เกียรติศักดิ์ โยชนะง. (2010). โปรแกรมประยุกต์การอำพรางข้อมูลลงภาพโดยใช้วิธีการสลับบิตร่วมกับการเข้ารหัสข้อมูลโดยใช้มาตรฐานการเข้ารหัสลับขั้นสูง. THE 6 th NATIONAL CONFERENCE ON COMPUTING AND INFORMATION TECHNOLOGY(692-679). Bangkok, Thailand.
- [5] ปรีชา พินทุศรี, จูติรัตน์ จันทรคารา, ยุทธเดช ช้อยแสง, ธนิกา กอสันประเสริฐ และ ดวงนภา บัวสันต์. (2562). การพัฒนาโปรแกรมสารสนเทศเพื่อการบริหารจัดการด้านทะเบียนทรัพย์สินของมหาวิทยาลัยเอกชนแห่งหนึ่งในจังหวัดนครปฐม. วารสารมหาวิทยาลัยคริสเตียน, 25(2): 79-91.
- [6] ยุทธศาสตร์กองทัพอากาศ 20 ปี (พ.ศ.2561 - 2580) (ฉบับปรับปรุง พ.ศ.2563).
- [7] Simalaotao, P. (2018). The Prototype Development of Traceability System of LSB Steganography in Image Files with Base64 and MD5 Encoding. Journal of Thai Interdisciplinary Research, 14(1):29-34.
- [8] Al-Sadoon, B., Mathkour, H., and Assassa, G. (2007). On the Development of Steganographic Tools, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia.
- [9] Bandyopadhyay, S. K., Bhattacharyya, D., Ganguly, D., Mukherjee, S., and Das, P. (2008). A Tutorial Review on Steganography, University of Calcutta, Computer Science and Engineering Department, Heritage Institute of Technology, Anandapur, Kolkata.
- [10] Dobsicek, M. (2003). Modern Steganography, Department of Computer Science and Engineering, Faculty of Electrical Engineering, Czech Technical University in Prague, Karlovo náměstí, Czech Republic.
- [11] Fridrich, J., Goljan, M., Du, R. (2001). Reliable Detection of LSB Steganography in Color and Grayscale Images, Air Force Research Laboratory, the Air Force Office of Scientific Research (AFOSR).
- [12] Hunt, K. (2005). A Java Framework for Experimentation with Steganography, The University of Wisconsin - La SIGCSE '05, St. Louis, Missouri, USA.
- [13] Johnson, N. F., and Jajodia, S. (1998). Steganalysis of Images Created using Current Steganography Software, Workshop on Information Hiding Proceedings(273-289). Portland, Oregon, USA.
- [14] Abbas, C., Joan, C., Kevin, C. and Paul, M. K. (2009), Digital Image Steganography: Survey and Analysis of Current Methods, School of Computing and Intelligent Systems, Faculty of Computing and Engineering University of Ulster at Magee, Londonderry, Northern Ireland, United Kingdom.
- [15] LENTI, J., (2000). Steganographic Methods, Department of Control Engineering and Information Technology, Budapest University of Technology and Economics, Budapest, Hungary.
- [16] Lin, E. T. and Delp, E. J. (2000). A Review of Data Hiding in Digital Images (VIPER), School of Electrical and Computer Engineering, Purdue University, Indiana.