

# การอำพรางข้อมูลด้วย Steganography บน QRCode

## Steganography hiding data within QRCode

ปรีญาทิพย์ แดงมี และ วรพล ลีลาเกียรติสกุล

คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหาสารคาม

Email : {preyatip@gmail.com, woraphon@mut.ac.th}

### Abstract

Nowadays, QRCode is popular and being used in businesses especially on products. Somehow, to make QRCode more functional, we propose the new technique to embed secret data on QRcode in order to communicate secretly between sender and receiver such as commercial transaction and etc. So, all embedded data must be concealed and must not increase too much burden to system process. This proposed technique is based on Steganography method. It was experimented by using RGB Channel and 3 x 3 RGB Channel. For the experimental results, we found that using the 3 x 3 RGB Channel presented more efficiency than RGB Channel.

**Keywords:** QRCode, Steganography, RGB, Barcode 2D, two-dimensional barcode

### บทคัดย่อ

ปัจจุบัน QRCode เป็นที่นิยมและถูกนำไปใช้งานในทางธุรกิจต่างๆ โดยเฉพาะบนสินค้าต่างๆ อย่างไรก็ตามในการที่จะทำ QRCode สามารถทำงานได้หลากหลายมากขึ้น เราจึงได้นำเสนอเทคนิคใหม่ในการฝังข้อมูลความลับลงบน QRCode เพื่อที่ ทำให้สามารถติดต่อสื่อสารข้อมูลความลับโดยใช้ QRCode ได้ เช่น การทำ Transaction ทางการค้า เป็นต้น ดังนั้นข้อมูลที่จะฝังจะต้องถูกปกปิด และกระบวนการทำงานต้องไม่สร้างภาระให้กับระบบมากเกินไป เทคนิคนี้ทำงานบนหลักการวิทยาการอำพรางข้อมูล (Steganography) และได้ทำการทดสอบโดยการฝังข้อมูลลงไปยัง RGB Channel และ 3x3 RGB Channel จากผลการทดลองพบว่าการใช้ 3x3 RGB Channel ให้ประสิทธิภาพที่ดีกว่า RGB Channel

**คำสำคัญ :** บาร์โค้ด, Steganography, การอำพรางข้อมูล, RGB, บาร์โค้ดสองมิติ

### 1. บทนำ

บาร์โค้ดสองมิติถูกพัฒนามาจากบาร์โค้ดหนึ่งมิติเพื่อสร้างประสิทธิภาพให้สูงขึ้นทั้งการสแกนข้อมูลได้ 360 องศา การมีความจุข้อมูลที่สูงขึ้นและความไวในการอ่านข้อมูลและการแก้ไขข้อผิดพลาดของข้อมูลซึ่ง QRCode ได้รับความนิยมอย่างมากในกลุ่มของบาร์โค้ดสองมิติ [1] QRCode ได้ถูกพัฒนาโดยบริษัท Nippon Denso ประเทศญี่ปุ่นในปี 1994 ได้ถูกสร้างในรูปแบบของเมตริกซ์ ซึ่งมีทำให้สามารถจุข้อมูลได้มากขึ้น รองรับความหนาแน่นของข้อมูลได้มากขึ้นและมีความแม่นยำสูง QRCode ประกอบไปด้วยการเข้ารหัส (coding region) และการทำงานของกราฟหลายส่วนซึ่งข้อมูลจะถูกอยู่ในรูปแบบของบาร์โค้ดสองมิติประกอบด้วยโมดูลสีดำจะถูกเก็บค่าที่ไบนารี 1 และโมดูลสีขาวจะถูกเก็บค่าที่ไบนารี 0 โครงสร้างของ QRCode ประกอบไปด้วยที่ติดตั้งส่วนของการค้นหา (Finder pattern) ที่สามมุมของภาพบาร์โค้ด ขนาดและความราบเรียบในส่วนของสัญลักษณ์ (symbol) ถูกกำหนดพร้อมกับการแก้ไขข้อผิดพลาด 4 ระดับซึ่งบาร์โค้ดนี้สามารถรองรับข้อมูลได้หลากหลายรูปแบบอีกด้วย

อย่างไรก็ตาม แอปพลิเคชันสำหรับการสร้างหรืออ่านข้อมูลของ QRCode ยังเหมาะสมสำหรับการใช้งานในลักษณะทั่วไปที่มีการฝังข้อมูลและอ่านข้อมูลได้ทุกที่ไม่จำกัดแหล่งที่มาหรือผู้รับ จึงเหมาะสำหรับการใช้งานส่งข้อมูลทั่วไปที่สามารถเปิดเผยได้และในขณะเดียวกัน เมื่อผู้ใช้งานจำเป็นต้องส่งข้อมูลที่ต้องการความปลอดภัยและเจาะจงผู้รับ โดยที่ต้องการส่งไปในช่องทางเดียวกัน อาทิเช่น รหัสผ่านสมาชิก เลขบัญชี รหัสยืนยันตัวตน เป็นต้น โดยจำเป็นต้องคำนึงถึงการจัดหาอุปกรณ์เพิ่ม เวลา ต้นทุนและความปลอดภัย จึงเป็นที่เรื่องยากในการควบคุมให้ได้ตามความต้องการ ผู้ทัววิจัยจึงได้ทำการศึกษาหาวิธีการสร้างความปลอดภัยให้กับข้อมูลในส่วนที่เป็นความลับโดยอาศัยการอำพรางข้อมูลไปกับบาร์โค้ดเดิมที่ต้องการส่งอยู่แล้วซึ่งจะทำให้ไม่ต้องเพิ่มอุปกรณ์การส่งข้อมูลลับ สามารถลดเวลาในการส่งได้เพราะส่งไปพร้อมบาร์โค้ด

ลดต้นทุนและสร้างความปลอดภัยให้ข้อมูลโดยข้อมูลไม่ที่สังเกต เนื่องจากบาร์โค้ดยังคงสภาพเดิมไม่เปลี่ยนแปลงและผู้ที่สแกน บาร์โค้ดทั่วไปก็ไม่สามารถอ่านข้อมูลลับเห็นได้นอกจากข้อมูลปกติ ซึ่งเป็นที่ทราบกันดีว่าการอำพรางข้อมูล Steganography นั้นคือการอำพรางข้อมูลชนิดหนึ่งที่เหมาะสมสำหรับเก็บข้อมูลลงในภาพได้อย่างมีประสิทธิภาพโดยที่ภาพนั้นยังคงสภาพเดิมโดยไม่เป็นที่สังเกตว่ามี การฝังข้อมูลลงไปและไม่สามารถอ่านข้อมูลลับได้หากไม่มี ภูเขาในการอ่านทำให้ข้อมูลลับมีความปลอดภัยมากขึ้น เราจึงมีความสนใจที่จะนำการวิทยาการอำพรางข้อมูล (Steganography) มาใช้ในการซ่อนข้อมูลลับลงใน QRCode ซึ่งสามารถช่วยทั้ง ทางด้านความปลอดภัย พื้นที่การเก็บข้อมูล ระยะเวลาในการส่ง ข้อมูลรวมถึงต้นทุนในการจัดหาอุปกรณ์ และเนื่องจากการอำพราง ข้อมูล Steganography จะต้องอาศัยภาพที่มีอยู่แล้วโดยใช้การอำ พรางไม่ให้เห็นการเปลี่ยนแปลงนั้น จึงจำเป็นต้องคงสภาพเดิม บาร์โค้ดทั้ง ขนาด รูปลักษณะและข้อมูลปกติที่สามารถสแกนได้ โดยทั่วไปการอำพรางข้อมูล Steganography สำหรับการอำพราง ข้อมูลลับให้ดูเหมือนสภาพเดิม จึงไม่สามารถขยายพื้นที่หรือ เปลี่ยนแปลงภาพใดๆตามที่มีได้ เนื่องจากจะทำให้กระทบกับข้อมูล ปกติ ผู้ท้าววิจัยจึงได้ทำการศึกษาหาวิธีที่จะสามารถเพิ่มการฝังข้อมูล ลับลงไปให้ได้มากขึ้นเพื่อรองรับข้อมูลลับที่ต้องการปริมาณความจุ ที่สูงขึ้นในพื้นที่ที่มีอย่างจำกัด

ในงานวิจัยนี้จะประกอบไปด้วยส่วนต่างๆดังนี้ ส่วนที่ 2 อธิบาย เกี่ยวกับพื้นฐานและงานวิจัยที่เกี่ยวข้อง, ส่วนที่ 3 อธิบายเกี่ยวกับ เทคนิคที่นำเสนอสำหรับการฝังข้อมูลด้วยวิทยาการอำพรางข้อมูล (Steganography) ลงบน QRCode, ส่วนที่ 4 แสดงผลการทดลองของ การใช้ Steganography ในการอำพรางข้อมูลโดยทำการแยกข้อมูล ผ่านช่องทาง RGB ของภาพแบ่งออกเป็น Channel คือแบบ RGB Channel และแบบ 3x3 RGB Channel และส่วนที่ 5 กล่าวถึงบทสรุปผลการทดลองที่ได้ของงานวิจัยนี้

## 2. พื้นฐานและงานวิจัยที่เกี่ยวข้อง

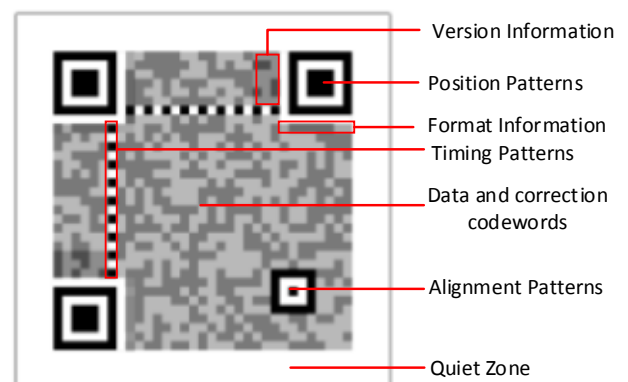
### 2.1. พื้นฐาน

2.1.1. QRCode [2] เป็นบาร์โค้ดสองมิติแบบเมตริกซ์ที่ถูก พัฒนาขึ้นโดยบริษัท Nippon Denso ประเทศญี่ปุ่นในปี ค.ศ. 1994 มี สร้างไว้ตั้งแต่เวอร์ชัน 1 ถึงเวอร์ชัน 40 และมีการตรวจสอบความ ถูกต้องแบ่งเป็น L, M, Q, H ลักษณะของบาร์โค้ดเป็นรูปสี่เหลี่ยมจัตุรัส มีโมดูลข้อมูล 21x21 ถึง 177x177 โมดูล สามารถบรรจุข้อมูล ได้มากที่สุด 7,089 ตัวเลข หรือ 4,296 ตัวอักษร ข้อมูลเลขฐานสอง 2,953 ไบต์ และตัวอักษรญี่ปุ่น 1,817 ตัวอักษร

ภายในโครงสร้างจะประกอบไปด้วย [3] รูปแบบการค้นหาของ QRCode อยู่ที่มุมทั้งสามของบาร์โค้ดคือมุมซ้ายบน มุมซ้ายล่าง และ มุมขวบน (Position Patterns) และรูปแบบการทำงาน (Alignment Patterns) สำหรับการทำให้อ่านได้รวดเร็ว การแสดงเวอร์ชันของ บาร์โค้ด (Version Information) รูปแบบของ QRCode (Format Information) ระบุพิกัดของสัญลักษณ์ในบาร์โค้ดเพื่อถอดรหัส (Timing Patterns) ส่วนที่ข้อมูลถูกเข้ารหัสและตรวจสอบ ข้อผิดพลาด (Data and Correction codewords) และส่วนที่ใช้เก็บ ข้อมูลของระดับการตรวจสอบข้อผิดพลาด (Format information)

ในส่วนของโครงสร้างของ QRCode นั้นจะประกอบไปด้วย สีขาวและสีดำบนพื้นผิวของภาพโดยสีดำจะถูกใช้กับค่าไบนารี 1 และ สีขาวจะถูกใช้กับค่าไบนารี 0 เป็นบาร์โค้ดสองมิติในรูปแบบ เมตริกซ์ที่สามารถอ่านข้อมูลความได้ทุกทิศทางโดยรูปที่ 1 ที่ได้ทำ การแสดงโครงสร้างของ QRCode มีฟังก์ชันสำหรับแก้ไข ข้อผิดพลาด (Correction codewords) [3] ในการอ่านข้อมูลบนภาพ บาร์โค้ดแบ่งได้ 4 ระดับดังนี้

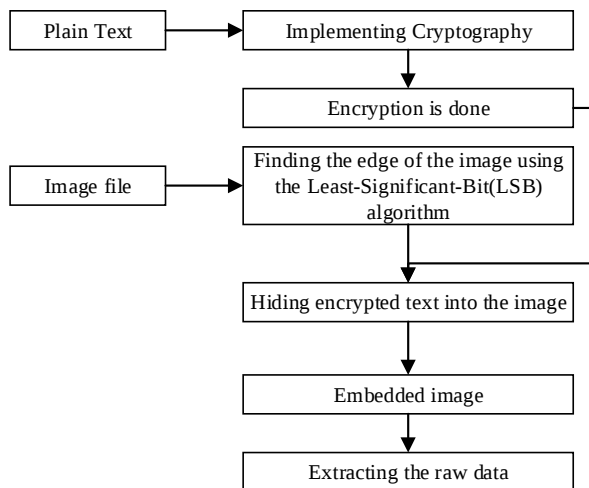
- level L : 7% ของรหัสที่สามารถทำให้กลับมาสมบูรณ์ได้
- level M : 15% ของรหัสที่สามารถทำให้กลับมาสมบูรณ์ได้
- level Q : 25% ของรหัสที่สามารถทำให้กลับมาสมบูรณ์ได้
- level H : 30% ของรหัสที่สามารถทำให้กลับมาสมบูรณ์ได้



รูปที่ 1. แสดงโครงสร้างของ QRCode [3]

#### 2.1.2. การอำพรางข้อมูล (Steganography) [4]

คือการอำพรางข้อมูลให้อยู่ในลักษณะเดิมโดยที่ไม่เป็นที่สังเกต และการฝังข้อมูลลงในพื้นที่ที่มีอยู่อย่างจำกัดเนื่องจากการทำงาน ของการอำพรางข้อมูลของ Steganography จะต้องอาศัยภาพที่มีอยู่ แล้วในการอำพรางข้อมูล ซึ่งกระบวนการอำพรางข้อมูลสามารถ อธิบายขั้นตอนได้ดังรูปที่ 2



รูปที่ 2. แสดงโครงสร้างของการอำพรางข้อมูลด้วย Steganography [4]

จากรูปที่ 2 เป็นการอธิบายขั้นตอนการทำงานของการทำงานของการอำพรางข้อมูล โดยจะทำการฝังข้อมูลลงไปบนรูปภาพและข้อความ (Plain Text) ที่ถูกป้อนลงไปจะถูกซ่อนลงไปในภาพโดยผ่านวิทยาการการเข้ารหัสลับ (Implementing Cryptography) ในการเข้ารหัสข้อมูลไว้ (Encryption is done) ซึ่งจะมีคีย์ (Key) การในเปิดข้อมูลที่ทราบเฉพาะผู้ส่งและผู้รับข้อมูลลับเท่านั้นที่รู้ เพื่อใช้สำหรับการตรวจสอบสิทธิ์การเข้าถึงข้อมูล จากนั้นผู้ส่งจะทำการเลือกภาพ (Image file) ที่ต้องการให้ข้อมูลลับฝังลงไป โดยการทำพรางข้อมูลจะทำการเลือกฝังบิตที่มีค่าน้อยสำคัญต่ำสุด (Least Significant Bit : LSB) สำหรับใช้ทำการเข้ารหัส (Hiding encrypted text into the image) ลงในภาพถือว่าเสร็จสิ้นกระบวนการอำพรางข้อมูลทำให้เราได้ภาพที่ถูกอำพรางข้อมูลไว้ (Embedded image)

สำหรับการสกัดข้อมูล (Extracting the raw data) ผู้รับจะต้องการแสดงสิทธิ์ให้ตรงกับที่ผู้ส่งได้ทำการกำหนดไว้ ข้อมูล (Cypher Text) จึงจะทำการแปลงกลับมาเป็นข้อมูลเดิมดังต้นฉบับ

## 2.2. งานวิจัยที่เกี่ยวข้อง

A.Daneshkhah [8] นำเสนอการเปลี่ยนบิตของข้อความสำหรับฝังใน ค่าน้อยสำคัญต่ำสุด (LSB) เพิ่มใน bit plane ลำดับที่สองและลำดับที่สี่ของข้อมูลสำหรับการจัดการการฝัง 1 จุดต่อ 1 bit plane พบว่าสามารถรองรับความจุได้

M.Jayachandran [9] ใช้การอำพรางข้อมูล (Steganography) กับภาพ SAR (Synthetic Aperture Rader) สำหรับส่งข้อมูลลับไว้ในภาพเพื่อลดเวลาในการส่งข้อมูลการเข้ารหัสและการถอดรหัส โดย LZW พบว่าสามารถทำได้ทั้งสองข้อมูล

R. Sartid [10] นำเสนอการฝังข้อมูลลับลงไปใน QRCode ด้วยลายน้ำ (Watermarking) โดยการแบ่งโคไซน์ไม่ต่อเนื่อง (discrete cosine transform – DCT) ใช้ค่าความถี่จากภาพ JPEG ขนาด 8\*8

G.Karthigai Seivi and team [1] นำเสนอการฝังข้อมูลด้วยการใช้ LSB ในการทำการอำพรางข้อมูลในภาพซึ่งพบว่าสามารถทำได้อย่างมีประสิทธิภาพขึ้นอยู่กับการวิเคราะห์เชิงสถิติ

Graham Finlayson, Steven Hordley [11] นำเสนอการจับคู่ของเจดสีที่มีความชัดเจนหลักเคียงบริเวณส่วนที่มีจุดตัดชัดเจนซึ่งช่วยทำให้ค่าที่ได้ออกมามีความคงที่

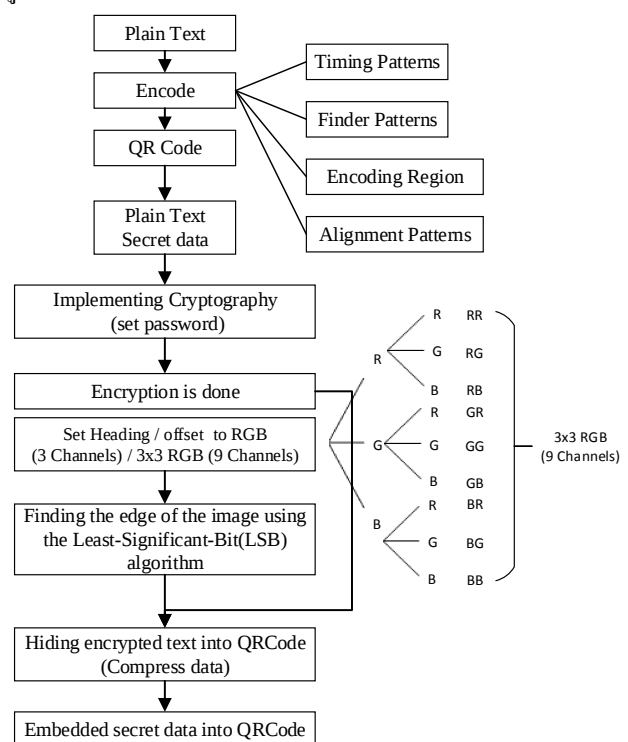
Xiuli Lv, Hongyu Bian, Yufei Yang [12] นำเสนอการใช้ขั้นตอนวิธีการของภาพสีทั้งที่จริงและสังเคราะห์ขึ้นเองในการสร้างลายน้ำฝังลงไปในช่วงสีโทนสว่างของค่าช่วงของสี YCbCr

Gabriela Mogos [16] ทำการวิจัยช่องทางควอนตัมสำหรับซ่อนข้อมูลด้วยพื้นฐานของสี RGB คือ แดง เขียว และน้ำเงิน ในการสร้างมิติโดยการแยก RGB

## 3. เทคนิคที่น่าสนใจ

### 3.1. การอำพรางข้อมูลบนภาพ QRCode

ในการอำพรางข้อมูลลับบน QRCode สามารถทำการอธิบายได้ดังรูปที่ 3



รูปที่ 3. แสดงกระบวนการของการอำพรางข้อมูลบน QRCode

จากรูปที่ 3 เป็นการแสดงขั้นตอนการทำงานระหว่าง QRCode ที่มีการฝังข้อมูลปกติและมีการฝังข้อมูลลับลงไปโดยมีลำดับขั้นตอนการทำงานดังนี้

1. สร้าง QRCode [1]

โดยการป้อนข้อมูลปกติลงไปซึ่งจะเป็นข้อมูลส่วนที่ผู้ส่งอนุญาตให้ผู้รับสามารถสแกนเห็นได้ โดยสามารถอ่านข้อมูลได้ด้วยแอปพลิเคชันหรือระบบที่ใช้สำหรับอ่าน QRCode ซึ่งในการสร้าง QRCode ในส่วนนี้จะถูกเป็นภาพต้นฉบับเพื่อให้เราใช้ในการฝังข้อมูลลงไปไปในขั้นตอนต่อไป ซึ่งจะมีกระบวนการในการฝังข้อมูล สร้างส่วนของการค้นหา (Timing Patterns, Finder Patterns) ป้องกันการผิดพลาดของข้อมูลและขยายขนาดตามผู้ส่งเลือก และความหนาแน่นของบิต (Alignment Patterns) ที่แสดงนั้นจะขึ้นอยู่กับข้อมูลของผู้ส่งใส่ลงไปนั่นเอง

2. เริ่มกระบวนการอำพรางข้อมูลด้วยการป้อนข้อมูลลับ (Secret data) ลงไปและกำหนดรหัสผ่าน (Set password) ซึ่งผู้ส่งจะเป็นผู้ที่กำหนดคีย์สำหรับการเข้าถึงข้อมูลลับที่ถูกอำพรางไว้ โดยค่าที่ผู้ใช้งานได้กำหนดนั้นจะถูกเก็บเป็น offset ของ Header และจะมีขนาด stride ที่มากที่สุดสำหรับการสร้าง RNG (Random Number Generation)

3. หลังจากได้มีการกำหนดรหัสผ่านแล้ว การเข้ารหัสจะเริ่มทำงานโดย QRCode จะถูกแบ่งการทำงานเป็น 3 ส่วน คือ

3.1. ส่วนหัว (Header) จะถูกกำหนดค่าในบิตลงในพิกเซลเพื่อใช้สำหรับการควบคุมข้อมูล อันได้แก่

- Active channel โดยปกติช่องทางที่ถูกเปิดใช้งาน คือ RGB channel (3 channels) [14] ซึ่งเราต้องการทำการทดลองโดยการขยายช่องทางให้สามารถรองรับได้มากขึ้นโดยการกำหนด RGB channel ให้ทำการสร้าง Channel Mixer เป็น 3x3 RGB ซึ่งจะได้ออกเป็น 9 channels อันได้แก่ RR, RG, RB, GR, GG, GB, BR, BG, BB สำหรับกำหนด header

3.2. กำหนด Channel parameter ที่จะทำการกำหนด offset เป็น 0 คือพิกเซลที่มีค่าน้อยสำคัญต่ำที่สุด (LSB : least significant bits) เพื่อเป็นช่องสำหรับการเข้ารหัสซึ่งคือพิกเซลแรก

สำหรับการทดสอบได้กำหนด Channel ตาม RGB กล่าวคือ RGB Channel จะมีทั้งหมด 3 Channels และสำหรับการทดสอบแบบ 3x3 RGB Channel จะมีทั้งหมด 9 Channels เพื่อทดสอบค่าว่าสามารถรองรับการฝังข้อมูลบน Channel ดังกล่าวได้หรือไม่และมีประสิทธิภาพเพียงใด

- กำหนดความยาวส่วนหัว (Header Length) ให้มีขนาด 1 ไบต์ (ซึ่งไม่รวมกับ 3 บิตของ Channel parameter ที่ได้จากการทดสอบแบบ RGB Channel และ 9 ของ Channel parameter ที่ได้จากการทดสอบแบบ 3x3 RGB Channel)

- กำหนด Message PARAMS สำหรับควบคุมบิตที่จะส่งผลกระทบต่อข้อความที่จะทำการเข้ารหัส

- กำหนดขนาดข้อมูลที่จะส่ง (PAYLOAD Size)
- ป้อนข้อมูลลับ (Message Data)
- กำหนดรูปแบบการเก็บข้อมูลเข้ารหัสดังนี้

ENCRYPT(COMPRESS(FILENAME + MESSAGE) )

3.3. บีบอัดข้อมูลนำเข้า (Compress data) สามารถกำหนดได้ดังนี้

mixed bzcompress ( string \$source [, int \$blocksize = 4 [, int \$workfactor = 0 ] ] )

- blocksize : สำหรับระบุ blocksize ที่ใช้ระหว่างการบีบอัดและควรใช้ตัวเลขระหว่าง 1 ถึง 9 ซึ่ง 9 คือค่าการบีบอัดที่ดีที่สุดและใช้ทรัพยากรมากสุดเช่นกัน

- Workfactor : ใช้สำหรับควบคุมขั้นตอนการทำงานของบีบอัดเมื่อได้รับข้อมูลมา โดยกำหนดให้มีค่าระหว่าง 0 ถึง 250 (0 ในกรณีพิเศษ)

- การเข้ารหัสสามารถกำหนดได้ดังนี้

string mcrypt\_encrypt (string \$cipher, string \$key, string \$data, string \$mode [, string \$iv ] )

- cipher : หนึ่งในค่าคงที่ของ MCRYPT\_ciphername หรือชื่อของกระบวนการทำงานกำหนดเป็น string.

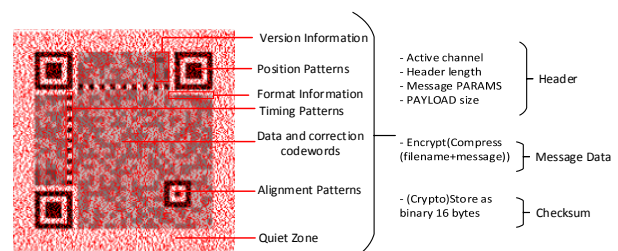
- Key : สำหรับข้อมูลที่เข้ารหัสแล้ว

- Message Data : ข้อมูลนั้นจะถูกนำมาถอดรหัสด้วยค่า cypher และ mode

- Mode : ค่าคงที่ของ MCRYPT\_MODE\_modename

3.4. Checksum : ถูกเชื่อมเข้ากับข้อความโดยใช้ MD5 Checksum สำหรับการตรวจสอบครั้งสุดท้าย 16 ไบต์ของ bitstream โดยมีการเก็บเป็นไบนารีและรวมเข้ากับขนาดฟิลด์ของ PAYLOAD ในส่วนของ header

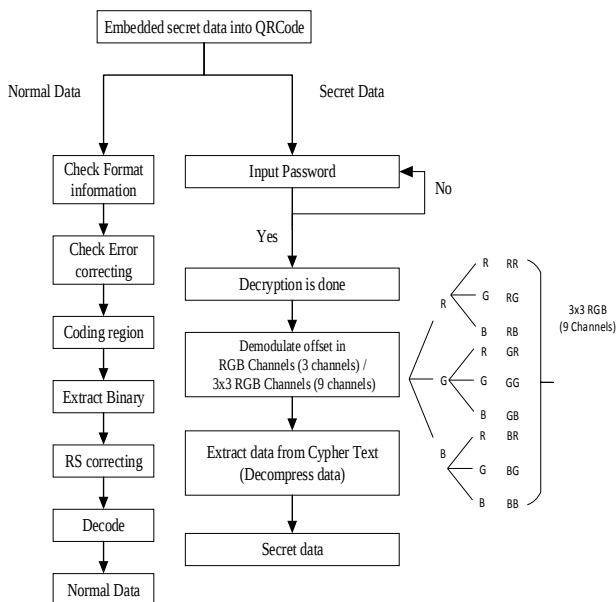
เมื่อแสดงในลักษณะภาพรวมของ QRCode ที่มีการฝังข้อมูลลงไปในรูปแบบการอำพรางข้อมูลจะถูกแยกค่า RGB ของภาพเพื่อสร้าง Channel โดยเก็บค่า Active channel, Header length, Message PARAMS ไว้ในส่วนของ Header และเก็บค่า Encrypt ซึ่งประกอบไปด้วย Filename และ Message ไว้ในส่วน Message Data และเก็บค่าไบนารี 16 ไบต์ไว้ในส่วนของการ Checksum ดังรูปที่ 4



รูปที่ 4. แสดงส่วนประกอบของ QRCode และ โครงสร้างภาพรวม  
เมื่อมีการอำพรางข้อมูล

### 3.2. การสกัดข้อมูล

ผู้ใช้งานทั่วไปสามารถใช้อ่านข้อมูล QRCode ที่เป็นข้อมูลปกติ และ ผู้รับสามารถสกัดข้อมูลได้ทั้งข้อมูลบนบาร์โค้ดและข้อมูลลับที่ถูกอำพรางขึ้นอยู่กับการอ่านข้อมูลประเภทใด ซึ่งหากผู้ใช้งานต้องการเปิดข้อมูลปกติที่อยู่บน QRCode สามารถใช้แอปพลิเคชันทั่วไปในการเปิดได้ โดยที่ข้อมูลจะไม่กระทบกับข้อมูลลับ ในทางกลับกัน หากผู้ใช้งานต้องการสกัดข้อมูลลับผู้ใช้งานจะต้องใส่รหัสผ่านซึ่งเป็นคีย์ในการเปิดให้ตรงกับที่ผู้ส่งได้กำหนดไว้ จึงจะสามารถเปิดข้อมูลลับได้ โดยกระบวนการสกัดข้อมูลสามารถแสดงกระบวนการทำงานได้ดังรูปที่ 5



รูปที่ 5. กระบวนการทำงานของการสกัดข้อมูล

จากภาพจะเห็นว่าเมื่อได้ QRCode ที่ถูกทำการฝังข้อมูลทั้งสองชนิดมาแล้ว ผู้รับสามารถเลือกได้ว่าต้องการดูข้อมูลชนิดใด ซึ่งแต่ละส่วนสามารถอธิบายได้ดังนี้

#### 1. ในส่วนของ QRCode [5] (Normal Data)

- อ่านค่ารูปแบบและเวอร์ชันของ QRCode
- สกัดข้อมูลพร้อมการแก้ไขข้อผิดพลาด (Error correcting)
- จัดการกับข้อมูลในส่วนของการ coding region ด้วยการใช้อยู่ XOR operator ในจุดที่ถูกกำหนดไว้.

- สกัดค่าไบนารี 0 และ 1 จากเมตริกซ์ข้อมูลที่ได้จากข้อมูลที่ถูกกำหนดไว้

- รับข้อมูลและตรวจสอบความถูกต้องของ code stream.

- ใช้ RS correcting ทำการตรวจสอบความถูกต้อง โดยจะทำการเลือกและกำหนดให้ block ที่ตอบสนองกับเวอร์ชันและระดับของการแก้ไขและการตรวจพบข้อผิดพลาด

- ข้อมูลที่ถูกถอดจะถูกคำนวณตัวอักษรและทำการแสดงผลเป็น Normal Data

#### 2. ในส่วนของ การสกัดข้อมูลลับ (Secret Data)

- โหลด QRCode ที่ถูกอำพรางข้อมูลเรียบร้อยแล้ว

- ใส่รหัสผ่านที่ผู้ใช้งานต้นทางได้กำหนดไว้

- ทำการ Demodulate offset เก็บใน RGB Channel และ 3x3 RGB channel

- คลายข้อมูลที่ถูกบีบ (Decompress data)

โดยกำหนดให้ bzdecompress ( string \$source [, int \$small = 0 ] )

- Small : ทางเลือกสำหรับขั้นตอนวิธีการคลายข้อมูลจะถูกใช้ในกรณีที่ความจำถูกใช้น้อย

- การถอดรหัส cypher text ด้วย header จาก Carrier ที่นำมากำหนดดังนี้

`string mcrypt_decrypt ( string $cipher , string $key , string $data , string $mode [, string $iv ] )`

- cipher : หนึ่งในค่าคงที่ของ MCRYPT\_ciphernam, หรือชื่อของกระบวนการทำงานกำหนดเป็น string

- Key : สำหรับข้อมูลที่เข้ารหัสแล้ว

- Data : ข้อมูลนั้นจะถูกนำมาถอดรหัสด้วยค่า cypher และ mode

- Mode : หนึ่งในค่าคงที่ของ MCRYPT\_MODE\_modename

- Iv : ถูกใช้ในการเริ่มต้นใน CBC, CFB, OFB modes และในบางกระบวนการของโหมด STREAM.

### 4. การทดลองและผลการทดลอง

ผู้วิจัยได้ทำการทดสอบการทำงานของระบบโดยการเขียนโปรแกรมภาษา PHP และกำหนดให้ QRCode ที่ทำการทดสอบการฝังข้อมูลลงบน QRCode ที่มีการ Encode ข้อมูลอยู่แล้วโดยไม่กระทบกับข้อมูลปกติด้วยการฝังข้อมูลลับลงไปบน RGB Channel และ 3x3 RGB Channel เพื่อการแบ่งพื้นที่สำหรับการฝังข้อมูลลับและความเสมือนภาพในการรักษาภาพเดิมของบาร์โค้ดดังการทดสอบในตารางที่ 1

ตารางที่ 1. แสดงภาพ QRCode หลังจากถูกอำพรางข้อมูลบน RGB Channel และ 3x3 RGB Channel

| Effect | RGB Channel | 3x3 RGB Channel |
|--------|-------------|-----------------|
|--------|-------------|-----------------|

| pixels |                                                                                   |                                                                                   |
|--------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| No     |  |  |
| Yes    |  |  |

จากการแสดงผลในตารางที่ 1 จะเห็นได้ว่าภาพแฉกบนที่ไม่ถูกกำหนดให้แสดงสีของพื้นที่ของการแบ่ง Channel ทั้งสองแบบไม่มีความแตกต่างกันเมื่อมองด้วยตาเปล่า แต่เมื่อถูกกำหนดให้แสดงสี (Effect pixel) Channel ที่ถูกกำหนดพบว่า RGB Channel และ 3x3 RGB Channel มีการแสดงสี (Effect pixel) แตกต่างกัน

เมื่อทำการทดสอบความไวและการฝังและสกัดข้อมูล ผู้วิจัยได้ทำการทดสอบให้มีขนาดคงที่โดยเลือกแก้ไขข้อผิดพลาดที่ใช้สำหรับทดสอบคือ ระดับ M และบาร์โค้ดมีขนาด 4 และป้อนข้อมูลทั่วไปคือ a-z (26 ตัวอักษร) โดยทำการทดสอบการอำพรางข้อมูลลับบน Channel ของภาพ 2 แบบคือ RGB Channel และ 3x3 RGB Channel โดยทำการป้อนข้อมูลลับโดยเพิ่มจำนวนตัวอักษรตามลำดับเพื่อทดสอบประสิทธิภาพของการซ่อนข้อมูลลับ ซึ่งสามารถแสดงผลของทั้งสอง Channel ได้ดังตารางที่ 2

ตารางที่ 2. แสดงผลเวลาที่ใช้ในการประมวลผลและการทดสอบฝังข้อมูลและสกัดข้อมูลบน RGB Channel และ 3x3 RGB Channel

| จำนวน (Byte) | เวลาของรอบการประมวลผล (วินาที) |         | RGB       |            | 3x3 RGB   |            |
|--------------|--------------------------------|---------|-----------|------------|-----------|------------|
|              | RGB                            | 3x3 RGB | ฝังข้อมูล | สกัดข้อมูล | ฝังข้อมูล | สกัดข้อมูล |
| 400          | 0.01099                        | 0.01200 | ผ่าน      | ผ่าน       | ผ่าน      | ผ่าน       |
| 800          | 0.00999                        | 0.01300 | ผ่าน      | ผ่าน       | ผ่าน      | ผ่าน       |
| 1,600        | 0.00800                        | 0.00700 | ผ่าน      | ผ่าน       | ผ่าน      | ผ่าน       |
| 2,400        | 0.00900                        | 0.01200 | ไม่ผ่าน   | ไม่ผ่าน    | ผ่าน      | ผ่าน       |
| 3,200        | 0.00600                        | 0.00600 | ไม่ผ่าน   | ไม่ผ่าน    | ผ่าน      | ผ่าน       |
| 4,000        | 0.01300                        | 0.00800 | ไม่ผ่าน   | ไม่ผ่าน    | ผ่าน      | ผ่าน       |
| 4,800        | 0.01100                        | 0.01199 | ไม่ผ่าน   | ไม่ผ่าน    | ผ่าน      | ผ่าน       |
| 5,600        | 0.00700                        | 0.01200 | ไม่ผ่าน   | ไม่ผ่าน    | ไม่ผ่าน   | ไม่ผ่าน    |

จากตารางที่ 2 แสดงผลการทดสอบพบว่า รอบการประมวลผลของ 3x3 RGB Channel มีค่าเฉลี่ยความนานกว่ารอบการประมวลผลของ RGB Channel ประมาณ 9.33% แต่ RGB Channel สามารถเก็บข้อมูลลับได้สูงสุด 1,600 Bytes ในขณะที่ 3x3 RGB Channel เก็บข้อมูลลับได้สูงสุด 4,800 Bytes กล่าวคือ 3x3 RGB Channel มีความจุข้อมูลได้สูงกว่า แต่ในขณะเดียวกัน RGB Channel ก็มีความเร็วในการประมวลผลที่เร็วกว่าเช่นกัน

## 5. บทสรุป

สำหรับงานวิจัยนี้ เราได้นำเสนอวิธีการฝังข้อมูลและสกัดข้อมูลลับบน QRCode ด้วยวิทยาการอำพรางข้อมูล Steganography เพื่อสร้างทางเลือกให้แก่ผู้ใช้งานในการส่งข้อมูลให้มีความปลอดภัยสูงขึ้น อีกทั้งยังได้พื้นที่และระยะเวลาในการขนส่งที่ดีขึ้น โดยไม่ทำให้ข้อมูลต้นฉบับเสียหายอีกด้วย แต่ในขณะเดียวกัน การอำพรางข้อมูลจำเป็นต้องอาศัยภาพเดิมที่จะให้ทำการฝังข้อมูลลับลงไปดังเช่น QRCode ซึ่งเราไม่สามารถกำหนดขนาดภาพต้นฉบับให้มีปริมาณเพียงพอในการใส่ข้อมูลลับลงไปได้ เราจึงทำการทดสอบกับ Channel ที่ใช้ในการฝังข้อมูลลับลงไปคือ RGB Channel ของภาพ และทำการขยาย Channel ออกในลักษณะ Channel Mixer จึงได้ 3x3 RGB Channel ขึ้นมาและทำการทดสอบฝังข้อมูลลับลงไปขนาด QRCode ที่เหมือนกัน ซึ่งพบว่า 3x3 RGB Channel ใช้เวลาในการประมวลผลมากกว่า RGB Channel ประมาณ 9.33% แต่ในขณะเดียวกัน 3x3 RGB Channel ก็ยังสามารถรองรับความจุของข้อมูลลับได้มากกว่าถึงประมาณ 3 เท่า

## เอกสารอ้างอิง

- [1] Yue Liu, Mingjun Liu, "Automatic Recognition Algorithm of Quick Response Code Based on Embedded System", In IEEE Transaction in 2006.
- [2] Phaisarn and Wichian, "QR-Code Generator", IEEE Transaction in 2010.
- [3] Yu-Hsuan Chang, Chung-Hua Chu and Ming-Syan Chen, "A General Scheme for Extracting QRCode from a non-uniform background in Camera Phones and Applications", IEEE Transaction in 2007.
- [4] G.Karthigai Seivi, Leon Mariadhasan, K. L. Shunmuganathan, "Steganography Using Edge Adaptive Image", IEEE Transaction in 2012.
- [5] RouA-Lin, FengYuan, GengYing, "QRCode image detection using run-length coding", In IEEE Transactions in 2011.
- [6] S.Dumitrescu, X.Wu, and Z.Wang, "Detection of LSB Steganography via Sample Pair Analysis", IEEE transactions on signal processing,
- [7] Andrew D. Ker, "Steganalysis of LSB Matching in Gray scale Images", IEEE signal processing letters, vol. 12, no. 6, pp. 441-444, Jun. 2005.
- [8] Ali Daneshkhah, Hassan Aghaeinia and Seyed Hamed Seyed, "A More Secure Steganography Method in

- Spatial Domain", Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.
- [9] M.Jayachandran<sup>1</sup> and J.Manikandan<sup>2</sup>, " SAR Image Compression using Steganography", In IEEE Transactions in 2010.
- [10] R. Sartid , V. Suppat,"QRCode Using Invisible Watermarking in Frequency Domain", In IEEE Transactions in 2011.
- [11] Graham Finlayson, Steven Hordley," A Theory of Selection for Gamut Mapping Colour Constancy".
- [12]Xiuli Lv , Hongyu Bian , Yufei Yang , "Color Image Watermarking Using Support Vector", IEEE Transaction in 2009.
- [13] M.Shrikalaa, P.Mathivanan , J.S.Leena Jasmine," Conversion of Stegano Images into a 3D Stereo Image using RANSAC." , In IEEE Transactions in 2013.
- [14] Alvis Sokolovs, Iija Galkin, Oskars Krievs and Juhan Laugis,"Simulation Methods for 3x3 Converter", In IEEE Transaction in 2006.
- [15] Takuya Imaide, Toshiro Kinugasa, "A Multimedia Color Camera Providing Multi-Format Digital Images" , In IEEE Transactions in 1993.
- [16] Gabriela Mogos, "A quantum way to data hiding" International Journal of Multimedia and Ubiquitous Engineering in 2009.