การวิเคราะห์และปรับปรุงประสิทธิภาพการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ

ANALYSIS AND IMPROVEMENT OF ELEMENTARY CELLULAR AUTOMATA IMAGE ENCRYPTION

มงคล ทองไกรแก้ว
MONGKOL THONGKRAIKAEW

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2558
KMITL-2015-SC-M-050-27

การวิเคราะห์และปรับปรุงประสิทธิภาพการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ

ANALYSIS AND IMPROVEMENT OF ELEMENTARY CELLULAR AUTOMATA IMAGE ENCRYPTION

มงคล ทองไกรแก้ว

MONGKOL THONGKRAIKAEW

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2558

KMITL-2015-SC-M-050-27

ANALYSIS AND IMPROVEMENT OF ELEMENTARY CELLULAR AUTOMATA IMAGE ENCRYPTION

MONGKOL THONGKRAIKAEW

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

FACULTY OF SCIENCE

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2015

KMITL-2015-SC-M-050-27

คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ "การวิเคราะห์และปรับปรุงประสิทธิภาพการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ"(ANALYSIS AND IMPROVEMENT OF ELEMENTARY CELLULAR AUTOMATA IMAGE ENCRYPTION)

ชื่อนักศึกษา นายมงคล ทองไกรแก้ว

รหัสประจำตัว 53650803

ปริญญา วิทยาศาสตรมหาบัณฑิต (สาขาวิชาวิทยาการคอมพิวเตอร์)

ภาควิชา วิทยาการคอมพิวเตอร์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม (ถ้ามี) -

คณะกรรมการสอบวิทยานิพนธ์	ลายมือชื่อ
ผศ.ดร.กรกช ประชุมรักษ์ ประธานกรรมการ	
ดร.วรางคณา กิ้มปาน อาจารย์บัณฑิตประจำ (ในสาขาวิชาที่เกี่ยวข้อง)	
ดร.วนิดา พฤทธิวิทยา ผู้ทรงคุณวุฒิจากภายนอกสถาบันฯ	
ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ อาจารย์ที่ปรึกษาวิทยานิพนธ์	

วัน/ เดือน/ ปี ที่สอบ 15 พฤษภาคม พ.ศ.2558 เวลา 09.00-12.00 น.

สถานที่สอบ ณ ห้อง 301 อาคารปฏิบัติการใหม่ ชั้น 3

คณะวิทยาศาสตร์รับรองแล้ว

(รองศาสตราจารย์ ดร.ดุษณี ธนะยริพัฒน์)
คณบดีคณะวิทยาศาสตร์
วันที่ 14 **เดือน** ก.ค. **พ.ศ.** 58

หัวข้อวิทยานิพนธ์	การวิเคราะห์และปรับปรุงประสิทธิภาพการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ
ชื่อนักศึกษา	มงคล ทองไกรแก้ว
รหัสประจำตัว	53650803
ปริญญา	วิทยาศาสตรมหาบัณฑิต
ภาควิชา	วิทยาการคอมพิวเตอร์
พ.ศ.	2558
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์

บทคัดย่อ

เนื่องจากการเข้ารหัสรูปภาพที่ใช้หลักการของเซลลูลาร์ออโตมาตาแบบพื้นฐาน (Elementary Cellular Automata – ECA) มีปัญหากับภาพที่มีความซ้ำซ้อนของข้อมูลสูง เช่น ภาพที่ประกอบด้วยพิกเซลที่มี โทนสีเดียวกันซึ่งภาพที่ผ่านการเข้ารหัสแล้วของภาพเหล่านี้จะมีการแจกแจงของฮิสโต-แกรมที่ไม่สม่ำเสมอและบางภาพสามารถมองเห็นเค้าโครงของภาพต้นฉบับได้ อีกทั้งวิธีการเดิมสามารถเข้ารหัสได้เฉพาะภาพสีและภาพสีเทาเท่านั้น วิทยานิพนธ์ฉบับนี้จึงทำการปรับปรุงวิธีการเดิมโดยเพิ่มขั้นตอนก่อนนำข้อมูลเพลนเท็กซ์ของแต่ละพิกเซลไปเข้ารหัสเพื่อให้ค่าของพิกเซลก่อนนำไปเข้ารหัสมีการกระจายมากขึ้นและมีการนำวิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทามาปรับปรุงและประยุกต์ใช้เพื่อให้สามารถเข้ารหัสภาพขาวดำได้ ผลการทดลองแสดงให้เห็นว่าวิธีการที่เสนอในวิทยานิพนธ์นี้สามารถเข้ารหัสได้ดีกว่าวิธีการเดิมในทุกลักษณะของภาพและทุกประเภทสีและเมื่อนำไปวัดประสิทธิภาพการเข้ารหัสด้วยพารามิเตอร์มาตรฐาน ได้แก่ ความสม่ำเสมอของฮิสโตแกรมของภาพที่ผ่านการเข้ารหัสแล้ว ความสามารถของคุณสมบัติการแพร่จากค่า Number of Pixel Change Rate (NPCR) และค่า Unified Average Change Intensity (UACI) ความสัมพันธ์ของพิกเซลข้างเคียง (Correlation Coefficient) และค่า Peak Signal-to-Noise Ratio (PSNR) พบว่านอกจากให้ผลที่ดีกว่าวิธีการเข้ารหัสเดิมในทุกคุณสมบัติแล้วค่าที่ได้เข้าใกล้ค่ามาตรฐานทุกค่า

คำสำคัญ : การเข้ารหัสรูปภาพ, เซลลูลาร์ออโตมาตาพื้นฐาน, วิเคราะห์ประสิทธิภาพ

Thesis Title	Analysis and Improvement of Elementary Cellular Automata Image Encryption
Student	Mongkol Thongkraikaew
Student ID	53650803
Degree	Master of Science
Department	Computer Science
Year	2015
Thesis Advisor	Dr. Rungrat Wiangsripanawan

ABSTRACT

The existing Elementary Cellular Automata Image Encryption (ECA) Scheme has problems with the high redundancy images since it results in the non-uniform histograms of all encrypted images and visible contents in some encrypted images. Also, it can be used to encrypt only the color and grayscale images. Hence, this thesis proposes an improved method to ECA by adding the pre-processing step to each plaintext pixel before encryption in order to increase randomness to the pixel. Besides, the method to convert black-and-white to grayscale images is employed and enhanced so that the ECA cannot only be used to encrypt the black-and-white images but also gives satisfied results. The experimental results show that the proposed scheme can be used to encrypt all types of images. It outperforms the existing scheme in all image-security-analysis parameters namely the encrypted image's uniform histogram, the diffusion property via the Number of Pixel Change Rate (NPCR) and the Unified Average Change Intensity (UACI), the Correlation Coefficient and the Peak-Signal-to-Noise Ratio (PSNR). Not only the proposed scheme gives better result than the existing ECA, it also gives near standard values in all parameters.

Keywords : Image Encryption, Elementary Cellular Automata, Analysis

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลงได้ด้วยดีเพราะความช่วยเหลือให้คำแนะนำ ความรู้และความเอาใจใส่จาก ดร. รุ่งรัตน์ เวียงศรีพนาวัลย์ผู้เป็นอาจารย์ที่ปรึกษา ซึ่งท่านได้สละเวลาและให้ความรู้แก่ข้าพเจ้าอย่างเต็มที่ จึงใคร่ขอขอบพระคุณอย่างสูง

ขอขอบคุณ ผศ.ดร.กรกช ประชุมรักษ์ ดร.วรางคณา กิ้มปาน และดร.วนิดา พฤทธิวิทยา คณะกรรมการสอบหัวข้อและโครงร่างวิทยานิพนธ์ ที่กรุณาให้คำแนะนำและข้อชี้แนะจนวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดี

ขอขอบพระคุณบิดา มารดา ที่ได้ให้โอกาสและเป็นแรงสนับสนุนทุกๆด้านแก่ข้าพเจ้าเสมอมา

ขอขอบคุณพี่ๆ เพื่อนๆ น้องๆ ทุกคนที่บริษัทเมโทรซิสเต็มส์คอร์ปอเรชั่น ที่คอยช่วยเหลือเรื่องงานในเวลาที่ข้าพเจ้าลางานเพื่อมาทำวิทยานิพนธ์ และให้กำลังใจข้าพเจ้าจนสำเร็จการศึกษา

ขอขอบคุณเพื่อนๆ พี่ๆ ร่วมรุ่นอันได้แก่ นายจนัสธา ศรีสรวล นางสาวบุญหทัย เครือแก้ว นายอนุสรณ์ เจริญนาน นายณัฐวุฒิ ชัยรัตนทรงพร และเพื่อนพี่น้องทุกคนที่ไม่ได้กล่าวถึงที่ให้คำปรึกษา ช่วยเหลืออำนวยความสะดวกในด้านต่างๆ

ขอขอบคุณสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบังสำหรับทุนสนับสนุนในการประชุมวิชาการต่างๆ และประสบการณ์ดีๆที่ได้จากการเข้าศึกษาในครั้งนี้

สำหรับคุณงามความดีและประโยชน์อันใดที่เกิดขึ้นจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับทุกคนที่กล่าวถึงในวิทยานิพนธ์นี้

มงคล ทองไกรแก้ว

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญตาราง(ต่อ)

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

สารบัญรูป(ต่อ)

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ทุกวันนี้การเติบโตของเครือข่ายคอมพิวเตอร์และการพัฒนาเทคโนโลยีเป็นไปอย่างรวดเร็ว เครือข่ายคอมพิวเตอร์ที่นิยมใช้งานในปัจจุบันคือเครือข่ายอินเทอร์เน็ต ซึ่งเป็นช่องทางติดต่อสื่อสารแบบสาธารณะที่ทุกคนสามารถเข้าถึงข้อมูลได้และเป็นช่องทางการส่งข้อมูลที่ไม่ปลอดภัย ข้อมูลบางอย่างที่ใช้แลกเปลี่ยนกันผ่านอินเทอร์เน็ตอาจเป็นข้อมูลที่ต้องการความปลอดภัยหรือต้องการปกปิดเป็นความลับระหว่างผู้ส่งและผู้รับ เช่น ข้อมูลทางทหารและข้อมูลธุรกรรมทางการเงิน การที่ไม่มีระบบรักษาความปลอดภัยที่ดีพออาจทำให้ข้อมูลสำคัญเหล่านี้รั่วไหลได้

วิธีหนึ่งที่ใช้ในการแก้ปัญหาเรื่องความปลอดภัยในการรับส่งข้อมูลบนเครือข่ายสาธารณะคือการเข้ารหัส (Encryption) มาตรฐานการเข้ารหัสข้อมูลที่ได้รับความนิยมคือ Advanced Encryption Standard (AES) ซึ่งสามารถปกปิดข้อมูลได้อย่างมีประสิทธิภาพ แต่การใช้ AES ในการเข้ารหัสไม่เหมาะกับการเข้ารหัสข้อมูลประเภทรูปภาพ เนื่องจากข้อมูลรูปภาพประกอบด้วยจุดภาพ (Pixel) จำนวนมากทำให้ข้อมูลมีขนาดใหญ่และการที่จุดภาพในบริเวณเดียวกันมักมีค่าความเข้มแสงเดียวกันหรือใกล้เคียงกันทำให้ข้อมูลมีความซ้ำซ้อนสูงและมีความสัมพันธ์ระหว่างพิกเซลข้างเคียงมาก การเข้ารหัสโดยวิธีทั่วไป เช่น AES จึงใช้เวลานานและปกปิดข้อมูลได้ไม่ดีเนื่องจากไม่ได้ถูกออกแบบให้ใช้กับการเข้ารหัสรูปภาพโดยเฉพาะ[1]

วิธีการเข้ารหัสรูปภาพโดยเฉพาะมีอยู่หลายวิธี เซลลูลาร์ออโตมาตาเป็นวิธีหนึ่งที่สามารถนำมาประยุกต์ใช้ในการเข้ารหัส โดย Chen และ Lai [1-2] ได้นำเซลลูลาร์ออโตมาตาแบบ 2 มิติมาใช้ในการสร้างตัวเลขสุ่มเทียมเพื่อใช้ในการเข้ารหัสและ Jun [3] ได้เป็นผู้ริเริ่มในการนำคุณสมบัติของการเปลี่ยนสถานะของเซลลูลาร์ออโตมาตาแบบพื้นฐานมาประยุกต์ใช้กับการเข้ารหัสรูปภาพ ซึ่งวนิดา [4] ได้ปรับปรุงงานวิจัยของ Jun โดยเพิ่มประสิทธิภาพการปกปิดข้อมูลด้วยการเพิ่มขั้นตอนการสลับบิตและเพิ่มจำนวนกุญแจ (Key) ที่ใช้ในการเข้ารหัส แต่การศึกษางานวิจัยของวนิดาพบว่าวิธีการที่ใช้ในการเข้ารหัสไม่สามารถปกปิดข้อมูลรูปภาพบางลักษณะหรือบางคีย์และเมื่อนำพารามิเตอร์มาตรฐาน เช่น NPCR UACI และ Correlation Coefficient มาวัดประสิทธิภาพการเข้ารหัสรูปภาพพบว่าให้ค่าที่ไม่ใกล้เคียงกับค่ามาตรฐาน อีกทั้งงานวิจัยวนิดาไม่มีการนำเสนอวิธีการเข้ารหัสภาพขาวดำโดยใช้เซลลูลาร์ออโตมาตาแบบพื้นฐาน ดังนั้นงานวิจัยนี้จึงมีวัตถุประสงค์ในการปรับปรุง

วิธีการและประสิทธิภาพในการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานให้สามารถปกปิดข้อมูลในทุกคีย์และทุกลักษณะของภาพและเมื่อตรวจสอบด้วยพารามิเตอร์ในการวัดประสิทธิภาพสามารถให้ค่าใกล้เคียงกับค่ามาตรฐาน อีกทั้งสามารถเข้ารหัสภาพได้ทุกประเภทสี

1.2 จุดมุ่งหมายและวัตถุประสงค์ของการศึกษา

งานวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนาขั้นตอนวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาพื้นฐานให้สามารถปกปิดข้อมูลรูปภาพได้ทุกลักษณะและทุกประเภทสี (ภาพสี ภาพสีเทา ภาพขาวดำ) อีกทั้งมีการนำพารามิเตอร์ที่นิยมใช้ในการวัดประสิทธิภาพการเข้ารหัสรูปภาพมาใช้ในการทดสอบเพื่อเปรียบเทียบกับงานวิจัยเดิมโดยต้องมีประสิทธิภาพดีกว่างานวิจัยเดิมและค่าที่ได้ต้องใกล้เคียงกับค่ามาตรฐาน

1.3 สมมติฐานของการศึกษา

การนำภาพในฐานข้อมูล USC-SIPI [6] ทุกภาพมาทดสอบเข้ารหัสด้วยวิธีการเดิมพบว่าภาพที่ผ่านการเข้ารหัสแล้วของภาพที่มีลักษณะเป็นโทนสีเดียวกันจะคงเค้าโครงของภาพต้นฉบับซึ่งสามารถมองเห็นได้ด้วยตาเปล่าหรือให้ค่าฮิสโตแกรมที่ไม่สม่ำเสมอ งานวิจัยนี้จึงปรับปรุงอัลกอริทึมให้มีการแจกแจงพิกเซลมากขึ้นเพื่อเพิ่มความสามารถในการปกปิดข้อมูลและเพิ่มขั้นตอนการเปลี่ยนภาพขาวดำเป็นภาพสีเทาเพื่อให้สามารถเข้ารหัสภาพขาวดำซึ่งงานวิจัยเดิมไม่สามารถเข้ารหัสได้

1.4 ขอบเขตการศึกษา

ขอบเขตของงานวิจัยมีรายละเอียดดังต่อไปนี้

1. ภาพสีเทาที่ใช้ในการเข้ารหัสต้องมีค่าความเข้มแสงที่มีค่าความลึกของบิต (Bit Depth) เท่ากับ 8 หรือค่าความเข้มแสงของแต่ละจุดภาพต้องมีค่าอยู่ระหว่าง 0 ถึง 255
2. ภาพสีที่ใช้ในการเข้ารหัสต้องเป็นภาพในระบบ RGB และมีค่าความเข้มแสงของแต่ละสีที่มีค่าความลึกของบิตเท่ากับ 8 หรือค่าความเข้มแสงของแต่ละจุดภาพต้องมีค่าอยู่ระหว่าง 0 ถึง 255
3. เครื่องมือที่ใช้ในการประมวลผลภาพและพัฒนาโปรแกรมการเข้ารหัสและถอดรหัสคือโปรแกรม Matlab version. 7.14.0 (R2012a)
4. รูปภาพที่ใช้ในการทดลองมาจากฐานข้อมูลของ USC-SIPI [6] มีทั้งหมด 44 รูปและรูปภาพขาวดำมีจำนวนทั้งหมด 16 รูป ซึ่งได้มาจากการนำภาพสีในฐานข้อมูลทำการแปลงเป็นภาพขาวดำ

1.5 ขั้นตอนการศึกษาและดำเนินงานวิจัย

ขั้นตอนการศึกษาและดำเนินงานวิจัยมีดังต่อไปนี้

1. ศึกษาวิธีการประมวลผลภาพเบื้องต้นและศึกษาทฤษฎีเบื้องต้นเกี่ยวกับเซลลูลาร์ออโต-มาตา และการเข้ารหัสข้อมูล
2. ศึกษางานวิจัยที่เกี่ยวข้องกับการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานและหาปัญหาของงานวิจัยเพื่อจะนำมาปรับปรุง
3. ตั้งสมมติฐานจากปัญหาเพื่อปรับปรุงวิธีการเข้ารหัสให้มีประสิทธิภาพเพิ่มมากขึ้นและเพิ่มความปลอดภัยของข้อมูลจากการโจมตี
4. นำเสนอวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานที่ได้ปรับปรุงแล้ว
5. พัฒนาโปรแกรมตามที่ได้นำเสนอ
6. วิเคราะห์ผลการทดลอง
7. สรุปและอภิปรายผลการทดลอง
8. เขียนวิทยานิพนธ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่ได้รับจากการศึกษาและปรับปรุงขั้นตอนวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานมีดังต่อไปนี้

1. ได้อัลกอริทึมในการเข้ารหัสที่สามารถเข้ารหัสและถอดรหัสภาพได้ทุกประเภทสี
2. สามารถนำไปใช้เป็นแนวทางในการพัฒนาขั้นตอนการเข้ารหัสไฟล์วีดีโอหรือภาพเคลื่อนไหว
3. สามารถนำไปใช้เป็นแนวทางในการพัฒนาขั้นตอนการเข้ารหัสรูปภาพด้วยวิธีอื่น

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ทฤษฎีและงานวิจัยที่เกี่ยวข้องในงานวิจัยนี้ประกอบด้วย ความรู้พื้นฐานเกี่ยวกับการประมวลผลภาพ (Image Processing) ความรู้เบื้องต้นเกี่ยวกับการเข้ารหัส (Cryptography) การใช้เซลลูลาร์ออโต-มาตาพื้นฐานในการเข้ารหัสรูปภาพ การเปลี่ยนภาพขาวดำเป็นภาพสีเทา พารามิเตอร์ที่ใช้ในการวัดประสิทธิภาพการเข้ารหัสรูปภาพ และงานวิจัยที่เกี่ยวข้องกับการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตา

2.1 การประมวลผลภาพดิจิตอล

2.1.1 ภาพดิจิตอล (Digital Image)

ภาพดิจิตอลเป็นฟังก์ชันสองมิติ โดยที่ $f(x,y)$ คือ ค่าความเข้มแสง ซึ่ง x และ y คือพิกัดของภาพ[1] ในแกนนอน (x) และแกนตั้ง (y) โดยค่าความเข้มแสงทั้งหมดเป็นจำนวนเต็มบวกและเป็นจำนวนจำกัด (Finite Number) ค่า $f(x,y)$ ถูกจัดเก็บอยู่ในรูปแบบของแถวลำดับ (Array) 2 มิติ แต่ละตำแหน่งของแถวลำดับจะเรียกว่า “จุดภาพ (Pixel)” [4]

2.1.2 ความลึกของบิต (Bit Depth)

ค่าความลึกของบิต คือ จำนวนบิตที่ใช้ในการเก็บค่าความเข้มแสงของแต่ละจุดภาพ ซึ่งบอกถึงจำนวนของค่าความเข้มแสงทั้งหมดที่เป็นไปได้ ค่าความลึกของบิตเท่ากับ 8 หมายความว่าในหนึ่งจุดภาพใช้บิตในการเก็บค่าความเข้มแสงจำนวน 8 บิต ค่าความเข้มแสงทั้งหมดมีค่าเท่ากับ 2^8 หรือเท่ากับ 256 ค่า โดยมีค่าอยู่ระหว่าง 0 – 255

2.1.3 ประเภทของสีภาพ

ประเภทของสีภาพจะขึ้นอยู่กับระบบการจัดเก็บข้อมูลรูปภาพและค่าความลึกของบิต ซึ่งประเภทของสีภาพมีการนิยามไว้หลายรูปแบบ แต่ที่นิยมใช้มี 3 รูปแบบด้วยกัน คือ ภาพขาวดำ (Binary Image) ภาพสีเทา (Grayscale Image หรือ Gray-Level Image) และภาพสี (Color Image)

1. ภาพขาวดำ (Black and White หรือ Binary Image)

ภาพขาวดำมีความลึกของบิตเท่ากับ 1 ดังนั้นค่าความเข้มของแสงมี 2 ค่าเท่านั้น คือ 0 และ 1 ซึ่ง 0 แทนจุดภาพสีดำ และ 1 แทนจุดภาพสีขาว [5] ระบบการจัดเก็บข้อมูลใช้แถวลำดับเพียงชุดเดียวในการเก็บข้อมูลความเข้มแสงจึงมี 1 มิติ ตัวอย่างของภาพขาวดำและการเก็บข้อมูลความเข้มแสงแสดงดังรูปที่ 2.1

(a) ตัวอย่างภาพขาวดำ

$f(1,1) = 1$	$f(1,2) = 0$	$f(1,3) = 1$

(b) ตัวอย่างการเก็บข้อมูลความเข้มแสง

รูปที่ 2.1 ตัวอย่างภาพขาวดำและตัวอย่างการเก็บข้อมูลความเข้มแสง

2. ภาพสีเทา (Grayscale image)

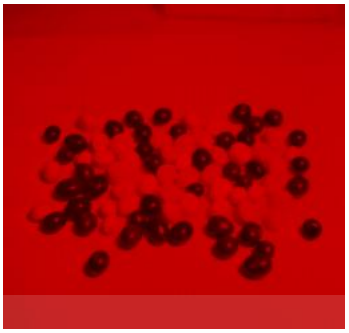
ภาพสีเทามีความลึกของบิตเท่ากับ 2 ขึ้นไป แต่ค่าความลึกของบิตที่นิยมใช้กันมากที่สุดคือ 8 บิต ดังนั้นค่าความเข้มแสงมีทั้งหมด 256 ค่า คือตั้งแต่ 0 ถึง 255 การจัดเก็บข้อมูลใช้ระบบเดียวกับภาพขาวดำคือ 1 มิติ รูปที่ 2.2 แสดงตัวอย่างของภาพสีเทา

รูปที่ 2.2 ตัวอย่างภาพสีเทา

3. ภาพสี (Color Image)

ภาพสีมีลักษณะคล้ายกับภาพสีเทาคือมีความลึกของบิตเท่ากัน แตกต่างกันในส่วนระบบการจัดเก็บค่าความเข้มแสง ระบบที่ใช้งานกับภาพสีเรียกว่าระบบ RGB ซึ่งใช้แถวลำดับ 3 ชุด หรือลำดับแถว 3 มิติในการเก็บความเข้มแสง โดยชุดแรกเก็บค่าความแสงสีแดง (Red) ชุดสองเก็บค่าความเข้มแสงสีเขียว (Green) และชุดสุดท้ายเก็บค่าความเข้มแสงสีน้ำเงิน (Blue) และเมื่อนำแต่ละสีในตำแหน่งเดียวกันของแต่ละชุดมาผสมกันจะได้สีของตำแหน่งภาพในตำแหน่งนั้นดังตัวอย่างในรูปที่ 2.3

(a) ภาพ Jelly bean



(b) ค่าความเข้มแสงสีแดง

(c) ค่าความเข้มแสงสีเขียว

(d) ค่าความเข้มแสงสีน้ำเงิน

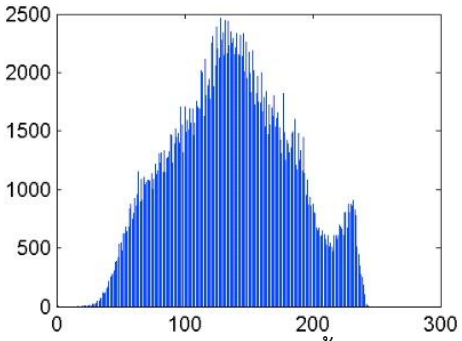
รูปที่ 2.3 ภาพ Jelly bean

2.1.4 ฮิสโตแกรม (Histogram)

ฮิสโตแกรมเป็นกราฟของฟังก์ชัน $f(x)$ ที่แสดงจำนวนจุดภาพทั้งหมดของรูปภาพในแต่ละความเข้มแสง เมื่อ x คือค่าความเข้มแสงและ $f(x)$ คือจำนวนจุดภาพทั้งหมดในภาพที่มีค่าความเข้มแสงเท่ากับ x

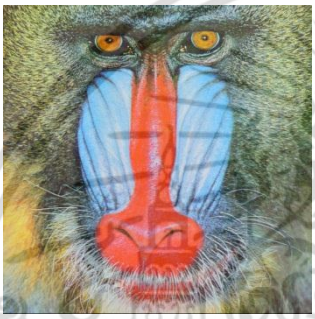
ฮิสโตแกรมของภาพสีเทาจะมีกราฟเพียงกราฟเดียวเนื่องจากมีการเก็บค่าความเข้มแสงเพียงชุดเดียวดังตัวอย่างในรูปที่ 2.4 แต่กรณีที่ภาพเป็นภาพสีจะมี 3 กราฟเนื่องจากมีการเก็บค่าความเข้มแสง 3 ชุด คือ สีแดง สีเขียว และสีน้ำเงิน ดังตัวอย่างในรูปที่ 2.5 และในส่วนของภาพขาวดำจะไม่นิยมนำมาแสดงเป็นกราฟฮิสโตแกรมเนื่องจากมีค่าความเข้มแสงจำนวนสองค่านั้นคือ 0 และ 1 เท่านั้น

(a) ภาพ Elaine

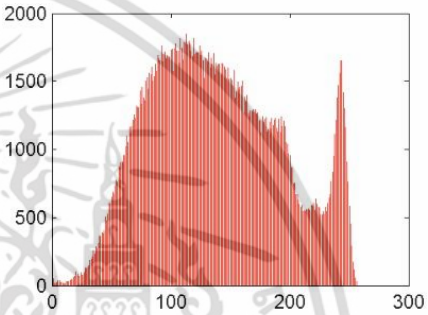


(b) ฮิสโตแกรมสีน้ำเงิน

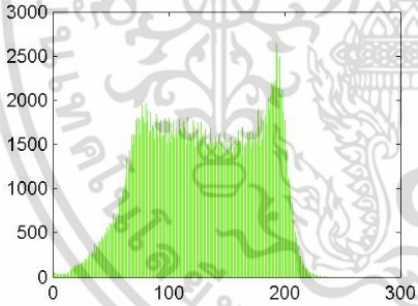
รูปที่ 2.4 ภาพสีเทา Elaine และ ฮิสโตแกรม



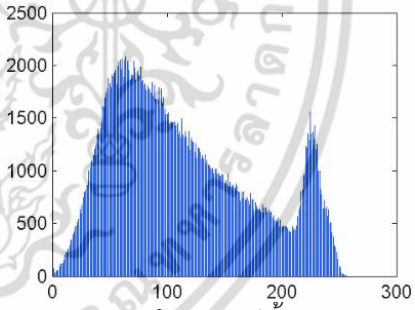
(a) ภาพ Baboon



(b) ฮิสโตแกรมสีแดง



(c) ฮิสโตแกรมสีเขียว

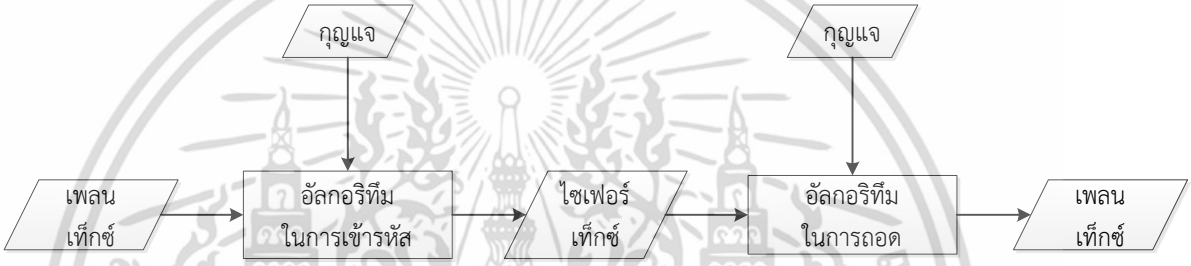


(d) ฮิสโตแกรมสีน้ำเงิน

รูปที่ 2.5 ภาพสี Baboon และ ฮิสโตแกรม (RGB)

2.2 ทฤษฎีการเข้ารหัสข้อมูลเบื้องต้น

การเข้ารหัสข้อมูลโดยพื้นฐานจะมีการนำกระบวนการทางคณิตศาสตร์มาใช้ในการเปลี่ยนแปลงข้อมูลต้นฉบับก่อนทำการส่งข้อมูลหรือจัดเก็บข้อมูล [7-8] โดยการนำข้อมูลอิเล็กทรอนิกส์ต้นฉบับที่เรียกว่าเพลนเท็กซ์ (Plain text) และกุญแจ (Key)ไปผ่านกระบวนการทางคณิตศาสตร์หรืออัลกอริทึมในการเข้ารหัส (Encryption Algorithm) ซึ่งข้อมูลต้นฉบับเมื่อผ่านการเข้ารหัสข้อมูลแล้วจะไม่สามารถอ่านหรือเข้าใจข้อมูลนั้นได้และเรียกข้อมูลชุดนั้นว่า ไซเฟอร์เท็กซ์ (Cipher text) เมื่อผู้รับได้รับไซเฟอร์เท็กซ์ ผู้รับจะต้องทราบกุญแจที่ถูกต้องและนำกุญแจนั้นไปผ่านขั้นตอนการถอดรหัส (Decryption Algorithm) จึงจะได้ข้อมูลเพลนเท็กซ์ที่ต้องการ รูปที่ 2.6 แสดงการเข้ารหัสและถอดรหัสพื้นฐาน

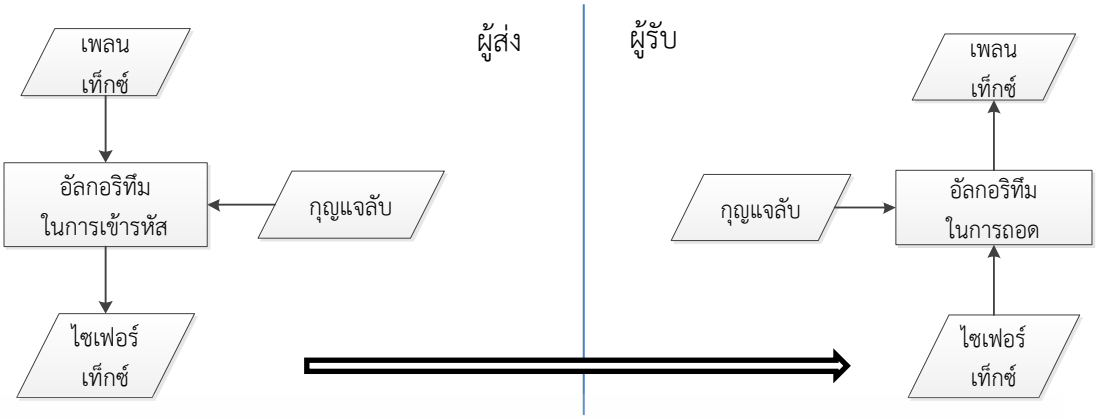


รูปที่ 2.6 การเข้ารหัสและถอดรหัสพื้นฐาน

กลไกในการเข้ารหัสสามารถแบ่งตามวิธีใช้กุญแจออกเป็น 2 แบบ คือ การเข้ารหัสด้วยกุญแจแบบสมมาตร (Symmetric-Key) และการเข้ารหัสด้วยกุญแจอสมมาตร (Asymmetric-Key) [9]

2.2.1 การเข้ารหัสด้วยกุญแจแบบสมมาตร

การเข้ารหัสด้วยกุญแจแบบสมมาตรผู้ส่งและผู้ส่งจะใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัสและเรียกกุญแจนี้ว่ากุญแจลับ (Secret Key) ซึ่งผู้ส่งและผู้รับข้อมูลต้องหาช่องทางที่ปลอดภัยในการแลกเปลี่ยนกุญแจลับก่อน ตัวอย่างของอัลกอริทึมในการเข้ารหัสแบบสมมาตรคือ DES และ AES[1] รูปที่ 2.7 แสดงการเข้ารหัสและถอดรหัสด้วยกุญแจแบบสมมาตร



รูปที่ 2.7 การเข้ารหัสและถอดรหัสด้วยกุญแจแบบสมมาตร

การเข้ารหัสด้วยกุญแจสมมาตรสามารถแบ่งออกเป็น 2 ประเภท คือ สตรีมไซเฟอร์ (Stream Cipher) และบล็อกไซเฟอร์ (Block Cipher)

1. สตรีมไซเฟอร์ (Stream Cipher)

สตรีมไซเฟอร์เป็นการเข้ารหัสทีละหน่วย เช่น บิต ไบต์ ซึ่งเหมาะกับข้อมูลที่มีลักษณะเป็นสตรีม (stream content) เพลนเท็กซ์ $P = p_1p_2p_3 \cdots p_n$ กุญแจ $K = k_1k_2k_3 \cdots k_n$และไซเฟอร์เท็กซ์ $C = c_1c_2c_3 \cdots c_n$ จะถูกมองเป็นสตรีม สมการของการเข้ารหัสแบบสตรีมไซเฟอร์ [9] เป็นดังต่อไปนี้

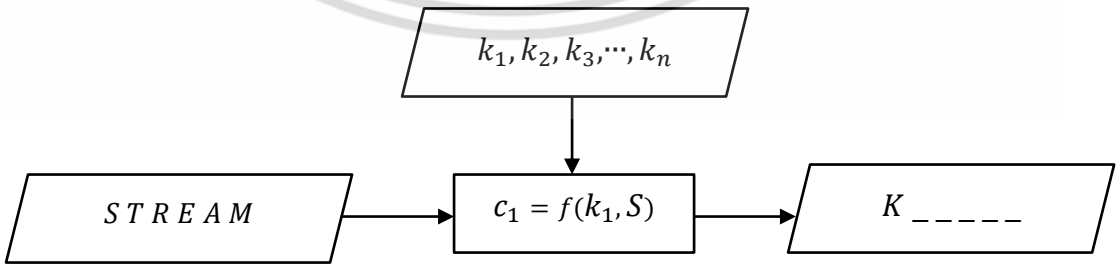
$$c_i = f(k_i, p_i) \tag{2.1}$$

เมื่อ c_i คือ ค่าสตรีมของไซเฟอร์เท็กซ์ในตำแหน่ง i

f คือ ค่าฟังก์ชันในการเข้ารหัส

k_i คือ ค่าสตรีมของกุญแจในตำแหน่ง i

p_i คือ ค่าสตรีมของเพลนเท็กซ์ในตำแหน่ง i



รูปที่ 2.8 ตัวอย่างการเข้ารหัสด้วยกุญแจสมมาตรแบบสตรีมไซเฟอร์

2. บล็อกไซเฟอร์ (Block Cipher)

บล็อกไซเฟอร์เป็นวิธีการเข้ารหัสที่มีการแบ่งเพลนเท็กซ์เป็นบล็อกที่มีขนาดเท่ากัน แล้วทำการเข้ารหัสทีละบล็อกโดยใช้กุญแจเดียวกันในการเข้ารหัสแต่ละกลุ่ม ถ้าข้อมูลในบล็อกสุดท้ายไม่เต็ม จะมีการเติมให้เต็ม (Padding) ก่อนนำไปเข้ารหัส สมการของการเข้ารหัสแบบบล็อกไซเฟอร์[9] เป็นดังต่อไปนี้

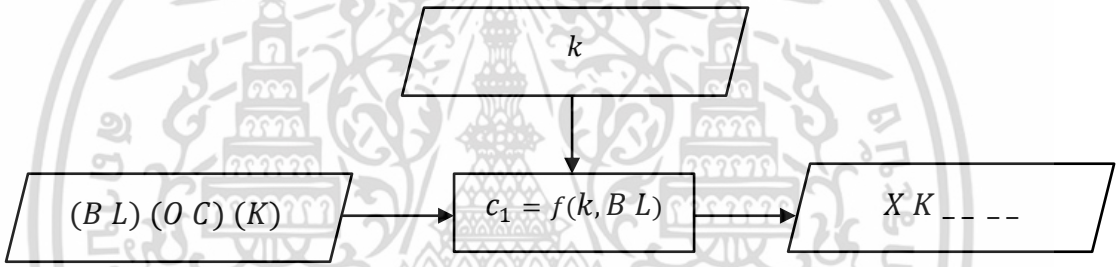
$$c_i = f(k, p_i) \tag{2.2}$$

เมื่อ c_i คือ ค่าของบล็อกไซเฟอร์เท็กซ์ในตำแหน่ง i

f คือ ค่าฟังก์ชันในการเข้ารหัส

k คือ กุญแจลับ

p_i คือ ค่าของบล็อกเพลนเท็กซ์ในตำแหน่ง i



*หมายเหตุ บล็อกมีขนาด *2* ตัวอักษร

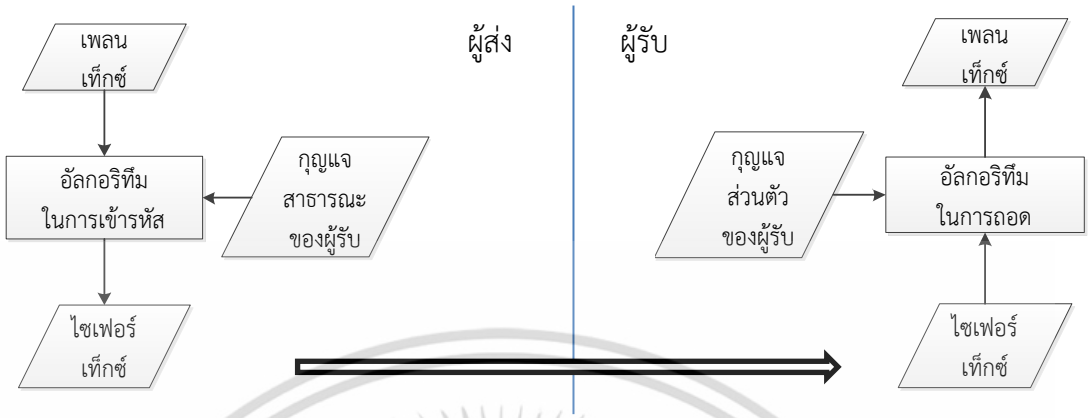
รูปที่ 2.9 ตัวอย่างการเข้ารหัสด้วยกุญแจสมมาตรแบบบล็อกไซเฟอร์

ข้อเสียของการเข้ารหัสแบบสมมาตรคือ 1.ช่องทางที่ใช้ในการแลกเปลี่ยนกุญแจลับระหว่างผู้รับและผู้ส่งต้องเป็นช่องทางที่ปลอดภัยมาก 2.หากมีการส่งข้อมูลให้ผู้รับหลายคนและไม่ต้องการให้ผู้รับทราบข้อมูลของผู้รับคนอื่น ผู้ส่งต้องสร้างกุญแจลับตามจำนวนผู้รับซึ่งถ้าผู้รับมีจำนวนมากจะทำให้เกิดปัญหาในการจัดการกุญแจ [8]

2.2.2 การเข้ารหัสด้วยกุญแจแบบอสมมาตร

การเข้ารหัสด้วยกุญแจแบบอสมมาตรประกอบด้วยกุญแจ 2 กุญแจ คือ กุญแจที่ใช้สำหรับเข้ารหัสเพลนเท็กซ์เรียกว่ากุญแจสาธารณะ (Public Key) และกุญแจที่ใช้สำหรับการถอดรหัสไซเฟอร์เท็กซ์เรียกว่ากุญแจส่วนตัว (Private Key) การเข้ารหัสแบบนี้แม้ผู้โจมตีทราบกุญแจสาธารณะจะไม่สามารถใช้กุญแจสาธารณะในการถอดรหัสหรือใช้กุญแจสาธารณะในการหาค่ากุญแจส่วนตัวได้ ในการส่งข้อมูล ผู้ส่งจะนำเพลนเท็กซ์มาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับที่ได้ประกาศไว้ก่อนหน้า เมื่อผู้รับได้รับข้อมูลจะนำไซเฟอร์เท็กซ์ที่ได้รับและกุญแจส่วนตัวของตนเองไปผ่านขั้นตอนการถอดรหัสเพื่อให้ได้เพลนเท็กซ์ที่ผู้ส่งต้องการส่งมาให้ ในการถอดรหัสมีเพียงผู้รับเท่านั้นที่สามารถ

ถอดรหัสได้เนื่องจากเป็นผู้เดียวที่มีกุญแจส่วนตัว [8] รูปที่ 2.10 แสดงการเข้ารหัสและถอดรหัสรูปภาพด้วยกุญแจแบบอสมมาตร ตัวอย่างอัลกอริทึมที่ใช้การเข้ารหัสแบบอสมมาตรเช่น RSA



รูปที่ 2.10 การเข้ารหัสและถอดรหัสด้วยกุญแจแบบอสมมาตร

2.2.3 การเข้ารหัสรูปภาพ

วิธีการเข้ารหัสข้อมูลตัวอักษรแบบสมมาตรที่นิยมในปัจจุบัน เช่น AES ฟ[1] ซึ่งเป็นอัลกอริทึมที่มีความซับซ้อนและมีความปลอดภัยในการเข้ารหัสข้อมูลมากนั้นไม่เหมาะกับการเข้ารหัสข้อมูลประเภทรูปภาพ เนื่องจากข้อมูลประเภทรูปภาพมีขนาดใหญ่และมีความซ้ำซ้อนสูงกว่าข้อมูลประเภทตัวอักษรมากจึงใช้เวลาในการเข้ารหัสนานทำให้จำเป็นต้องมีวิธีการเข้ารหัสรูปภาพโดยเฉพาะ วิธีการเข้ารหัสที่ออกแบบให้ใช้กับข้อมูลรูปภาพโดยเฉพาะมีหลายวิธี แบ่งตามลักษณะของอัลกอริทึมในการเข้ารหัสได้ดังนี้ [30]

1. การเปลี่ยนแปลงลำดับ (Permutation)

การเปลี่ยนแปลงลำดับเป็นอัลกอริทึมการเข้ารหัสที่เก่าแก่ที่สุด โดยการสุ่มสลับตำแหน่งในแต่ละพิกเซลเพื่อลดความสัมพันธ์ระหว่างพิกเซลข้างเคียง สามารถสลับตำแหน่งพิกเซลเพียง 1 พิกเซล หรือสลับตำแหน่งเป็นแถวได้

2. การสุ่มค่า (Random)

เป็นการสุ่มตัวเลขด้วยตัวสร้างเลขสุ่มเทียม เพื่อนำมา Xor (Exclusive-OR) หรือ Modulation กับข้อมูลรูปภาพต้นฉบับ ซึ่งการสร้างเลขสุ่มเทียมที่ดีสามารถช่วยเพิ่มความปลอดภัยของภาพที่ผ่านการเข้ารหัสทำให้ถูกโจมตีได้ยากยิ่งขึ้น

3. การแพร่และความสับสน (Diffusion and Confusion)

หลักการของการแพร่และความสับสนถูกนำไปเป็นหลักการหนึ่งในการออกแบบการเข้ารหัสในรูปแบบบล็อกไซเฟอร์เช่น DES และ AES ในการเข้ารหัสรูปภาพมีการนำหลักการนี้มาใช้เช่นเดียวกันโดยเทคนิคที่นิยมใช้เพื่อสร้างการแพร่และความสับสนคือ Chaotic Map [30] ซึ่งช่วยในการควบคุมลำดับในการเข้ารหัสให้เกิดความวุ่นวายมากขึ้น

2.3 เซลลูลาร์ออโตมาตา

เซลลูลาร์ออโตมาตา[1-4] เป็นแบบจำลองทางคณิตศาสตร์ที่ใช้อธิบายถึงระบบต่างๆ ในธรรมชาติ ถูกนำเสนอครั้งแรกโดย J.von Neumann และ Ulam โดยมีชื่อว่า เซลลูลาร์สเปซ (Cellular space) เพื่อใช้ในการสร้างแบบจำลองทางชีววิทยา หลังจากนั้นได้ถูกนำไปใช้กับงานหลากหลายรูปแบบ[10] โดยจะแตกต่างไปตามการใช้งาน แต่มีลักษณะสำคัญที่เหมือนกันคือมีการแยกองค์ประกอบออกเป็นส่วน และเกี่ยวข้องกับเวลาที่เปลี่ยนแปลงแบบไม่ต่อเนื่อง (Discrete) โดยจะเรียกแต่ละส่วนว่าเซลล์ (Cell) ซึ่งมีลักษณะเหมือนแถวลำดับโดยปกติสามารถขยายได้ไม่จำกัด แต่ละเซลล์มีสถานะ (State) ของตนเองและจะเปลี่ยนแปลงไปเมื่อเวลาเปลี่ยนจาก t เป็น $t+1$ สถานะใหม่ของเซลล์จะถูกกำหนดโดยสถานะในช่วงเวลา t ของเซลล์ที่อยู่ใกล้เคียงเรียกว่าสถานะย่านข้างเคียง (Neighborhood) แต่ละเซลล์จะมีฟังก์ชันที่ใช้กำหนดค่าสถานะใหม่ตามสถานะย่านข้างเคียงเรียกว่า กฎ (Rule) สามารถเขียนเป็นสมการได้ดังสมการที่ 2.3

$$s_i^{t+1} = f_i(s_{neighborhood}^t) \tag{2.3}$$

เมื่อ s_i^{t+1} คือ สถานะของเซลล์ i ที่เวลา $t+1$

f_i คือ กฎของเซลล์ที่ i

$s_{neighborhood}^t$ คือ สถานะย่านข้างเคียงของเซลล์ i ที่เวลา t

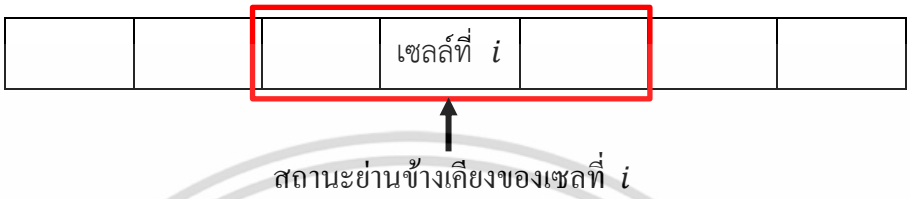
$t=0$	1	0	0	1	1	0	1
$t=1$	1	0	1	0	1	1	0

รูปที่ 2.11 ตัวอย่างเซลลูลาร์ออโตมาตาที่เวลา $t=0$ และ $t=1$

รูปที่ 2.11 แสดงตัวอย่างของเซลลูลาร์ออโตมาตา ช่องสี่เหลี่ยมแต่ละช่องคือเซลล์ โดยแต่ละเซลล์จะมีค่าสถานะของตัวเองคือเซตของตัวเลข {0,1} เมื่อเวลาที่ 0 เปลี่ยนเป็นเวลาที่ 1 ค่าสถานะของแต่ละเซลล์จะมีการเปลี่ยนแปลงตามกฎที่ได้กำหนด การที่ค่าสถานะของสองเซลล์ที่มีค่าสถานะย่านข้างเคียงเหมือนกันแต่เมื่อเวลาเปลี่ยนค่าสถานะที่เปลี่ยนมีค่าไม่เท่ากันเกิดจากทั้งสองเซลล์มีกฎที่แตกต่างกัน

2.3.1 เซลลูลาร์ออโตมาตาแบบพื้นฐาน

เซลลูลาร์ออโตมาตาแบบพื้นฐานเป็นเซลลูลาร์ออโตมาตาที่มีรูปแบบอย่างง่าย แถวลำดับเป็นแบบ 1 มิติ เซตของสถานะจะมีแค่ 2 ค่าเท่านั้น คือ {0,1} หรือใช้สีขาวแทนค่า 0 และสีดำแทนค่า 1 สถานะย่านข้างเคียงของเซลล์ประกอบด้วย 3 คือ เซลล์ที่อยู่ด้านซ้ายของเซลล์ เซลล์ที่อยู่ด้านขวาของเซลล์ และตัวเซลล์นั้นเอง ดังตัวอย่างในรูปที่ 2.12



รูปที่ 2.12 สถานะย่านข้างเคียงของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

การที่เซลล์ย่านข้างเคียงมีทั้งหมด 3 ค่า และกฎที่ใช้กำหนดให้กับแต่ละเซลล์จะใช้กฎเดียวกันทั้งหมดจึงสามารถเขียนให้อยู่ในรูปของสมการได้ดังนี้

$$s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) \tag{2.4}$$

เมื่อ s_i^{t+1} คือ สถานะของเซลล์ i ที่เวลา $t+1$

f คือ กฎของเซลล์

$s_{i-1}^t, s_i^t, s_{i+1}^t$ คือ สถานะย่านข้างเคียงของเซลล์ i ที่เวลา t

เนื่องจากสถานะย่านข้างเคียงมี 3 เซลล์ และแต่ละเซลล์มีสถานะที่เป็นไปได้ 2 ค่า ดังนั้นแต่ละกฎจะมีค่าสถานะของย่านข้างเคียงที่เป็นไปได้ทั้งหมดเท่ากับ 2^3 หรือ 8 รูปแบบ อีกทั้งแต่ละรูปแบบสามารถกำหนดค่าสถานะใหม่ได้อีก 2 ค่า ดังนั้นจำนวนกฎทั้งหมดที่เป็นไปได้ของเซลลูลาร์ออโตมาตาพื้นฐานคือ 2^8 หรือ 256 กฎ ดังตัวอย่างในตารางที่ 2.1

ตารางที่ 2.1 สถานะย่านข้างเคียงที่เป็นไปได้ทั้งหมด

สถานะย่านข้างเคียงทั้งหมด		
s_{i-1}^{t}	s_{i}^{t}	s_{i+1}^{t}
1	1	1
1	1	0
1	0	1
1	0	0
0	1	1
0	1	0
0	0	1
0	0	0

ตารางที่ 2.2 ตัวอย่างกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

สถานะย่านข้างเคียง	111	110	101	100	011	010	001	000
สถานะใหม่ของกฎ 2	0	0	0	0	0	0	1	0
สถานะใหม่ของกฎ 150	1	0	0	1	0	1	1	0
สถานะใหม่ของกฎ 255	1	1	1	1	1	1	1	1

จากตัวอย่างกฎของเซลลูลาร์ออโตมาตาในตารางที่ 2.2 หากนำสถานะย่านข้างเคียงหลังจากแปลงเป็นเลขฐาน 10 แล้วมาเป็นเลขชี้กำลังของเลขฐาน 2 แล้วนำค่าที่ได้ไปคูณกับค่าสถานะใหม่ของค่าสถานะย่านข้างเคียงนั้นซึ่งมีค่าเป็น (0 หรือ 1) จากนั้นนำค่าที่คำนวณได้ในทุกย่านข้างเคียงมาบวกกันจะได้เป็นเลขฐาน 10 ที่เป็นชื่อเรียกของกฎนั้นซึ่งตังตัวอย่างในตารางที่ 2.3

ตารางที่ 2.3 การแปลงกฎ 150 ของเซลลูลาร์ออโตมาตาแบบพื้นฐานเป็นเลขฐาน 10

สถานะย่านข้างเคียง (ฐาน 2)	สถานะย่านข้างเคียง (ฐาน 10)	เลขชี้กำลังของเลขฐาน 2	ตัวอย่างสถานะใหม่ของกฎ 150	
1 1 1	7	$2^7=128$	1	128×1 = 128
1 1 0	6	$2^6=64$	0	64×0 = 0
1 0 1	5	$2^5=32$	0	32×0 = 0
1 0 0	4	$2^4=16$	1	16×1 = 16
0 1 1	3	$2^3=8$	0	8×0 = 0
0 1 0	2	$2^2=4$	1	4×1 = 4
0 0 1	1	$2^1=2$	1	2×1 = 2
0 0 0	0	$2^0=1$	0	1×0 = 0
	ผลรวมของแต่ละย่านข้างเคียงหรือชื่อของกฎ			**150**

ในทางกลับกันหากทราบชื่อกฎเป็นเลขฐาน 10 สามารถหาความสัมพันธ์ระหว่างสถานะใหม่ของแต่ละเซลล์โดยเปลี่ยนหมายเลขกฎให้อยู่ในรูปของเลขฐาน 2 และนำค่าที่ได้มาประจำตำแหน่งของแต่ละเลขชี้กำลังรวมทั้งค่าสถานะย่านข้างเคียงทั้ง 8 รูปแบบ ตารางที่ 2.4 แสดงตัวอย่างวิธีการหาค่าสถานะใหม่ของกฎ 150

ตารางที่ 2.4 การแปลงเลขฐาน 10 เป็นกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

$150_{10} = 10010110_2$				
ค่าประจำตำแหน่ง	เลขฐาน 2 ของ 150	เลขชี้กำลัง(ฐาน 10)	เลขชี้กำลัง (ฐาน 2) หรือรูปแบบสถานะย่านข้างเคียง	สถานะใหม่
2^7=128	1	7	1 1 1	1
2^6=64	0	6	1 1 0	0
2^5=32	0	5	1 0 1	0
2^4=16	1	4	1 0 0	1
2^3=8	0	3	0 1 1	0
2^2=4	1	2	0 1 0	1
2^1=2	1	1	0 0 1	1
2^0=1	0	0	0 0 0	0

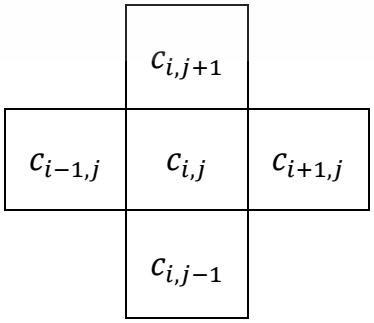
2.3.2 เซลลูลาร์ออโตมาตาแบบ 2 มิติ

เซลลูลาร์ออโตมาตาแบบ 2 มิติส่วนใหญ่จะกำหนดเซตของสถานะเช่นเดียวกับเซลลูลาร์ออโตมาตาแบบพื้นฐานคือ {0,1} ในส่วนของย่านข้างเคียงของเซลลูลาร์ออโตมาตาแบบ 2 มิติที่นิยมใช้มี 2 รูปแบบ คือ ย่านข้างเคียงของวอนนิวแมน (Von Neumann neighborhoods) และ ย่านข้างเคียงของมัวร์ (Moore neighborhoods) ซึ่งสามารถอธิบายได้ดังนี้

ย่านข้างเคียงของวอนนิวแมนมีจำนวนเซลล์ข้างเคียงทั้งหมด 5 เซลล์ ดังรูปที่ 2.13 สถานะย่านข้างเคียงของเซลล์ในตำแหน่งแถวที่ i และหลักที่ j สามารถเขียนเป็นสมการได้ดังนี้

$$\text{Von Neumann neighborhood } (c_{i,j}) = \{c_{i,j}, c_{i-1,j}, c_{i+1,j}, c_{i,j-1}, c_{i,j+1}\} \quad (2.5)$$

เมื่อ $c_{i,j}$ คือ เซลล์ในตำแหน่งแถวที่ i และหลักที่ j



รูปที่ 2.13 ย่านข้างเคียงของวอนนิวแมน

ย่านข้างเคียงของมัวร์ มีจำนวนเซลล์ข้างเคียงทั้งหมด 9 เซลล์ ดังรูปที่ 2.14 ดังนั้น สถานะย่านข้างเคียงของเซลล์ในตำแหน่งแถวที่ i และหลักที่ j เขียนเป็นสมการได้ดังนี้

$$\text{Moore neighborhood } (c_{i,j}) = \{c_{i,j}, c_{i-1,j}, c_{i+1,j}, c_{i,j-1}, c_{i,j+1}, c_{i-1,j-1}, c_{i-1,j+1}, c_{i+1,j-1}, c_{i+1,j+1}\} \quad (2.6)$$

เมื่อ $c_{i,j}$ คือ เซลล์ในตำแหน่งแถวที่ i และหลักที่ j

$c_{i-1,j+1}$	$c_{i,j+1}$	$c_{i+1,j+1}$
$c_{i-1,j}$	$c_{i,j}$	$c_{i+1,j}$
$c_{i-1,j-1}$	$c_{i,j-1}$	$c_{i+1,j-1}$

รูปที่ 2.14 ย่านข้างเคียงของมัวร์

กฎของเซลลูลาร์ออโตมาตาแบบ 2 มิติ มีหลายรูปแบบ เช่น แบบเป็นฟังก์ชันของสถานะของย่านข้างเคียงเหมือนกับเซลลูลาร์ออโตมาตาแบบพื้นฐาน หรือแบบโทเทิลลิสติก (Totalistic rule) ที่เป็นฟังก์ชันของผลรวมของสถานะย่านข้างเคียงทั้งหมด เป็นต้น [3]

2.4 งานวิจัยที่เกี่ยวข้องกับการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตา

จากการศึกษางานวิจัยที่นำเซลลูลาร์ออโตมาตามาใช้ในการเข้ารหัสรูปภาพพบว่าส่วนมากเป็นวิธีการเข้ารหัสด้วยกุญแจแบบสมมาตร [3] แต่ละงานวิจัยมีการนำเซลลูลาร์ออโตมาตาไปใช้งานในวัตถุประสงค์ที่แตกต่างกันซึ่งสามารถแบ่งออกได้ 2 กลุ่มดังนี้

2.4.1 งานวิจัยที่นำเซลลูลาร์ออโตมาตาใช้เป็นขั้นตอนการเข้ารหัส

ในกลุ่มนี้เป็นงานวิจัยที่นำเซลลูลาร์ออโตมาตามาประยุกต์ใช้เพื่อเป็นส่วนหนึ่งของฟังก์ชันที่ใช้ในการเข้ารหัสซึ่งจะใช้เพลนเท็กซ์เป็นสถานะเริ่มต้นของเซลลูลาร์ออโตมาตา แล้วใช้การเปลี่ยนสถานะของเซลลูลาร์ออโตมาตาเป็นฟังก์ชันในการเข้ารหัส

สำหรับตัวอย่างของงานวิจัยในกลุ่มนี้ ได้แก่ งานวิจัยของ Puhua [11] เป็นงานวิจัยที่เข้ารหัสด้วยกุญแจแบบอสมมาตรซึ่งแต่ละเซลล์มีกฎที่แตกต่างกันเรียกว่าเซลลูลาร์ออโตมาตาแบบไม่ยูนิฟอร์ม (Non-Uniform) ฟังก์ชันที่ใช้ในการเข้ารหัสคือกฎของเซลลูลาร์ออโตมาตาที่เป็นแบบเชิงเส้นบางส่วน(Partially linear function) โดยกุญแจสาธารณะเป็นฟังก์ชันไม่เชิงเส้น (Non-linear

function) แต่กุญแจส่วนตัวที่ใช้ในการถอดรหัสเป็นแบบเชิงเส้นจึงทำให้วิธีนี้สามารถถอดรหัสได้อย่างรวดเร็ว

งานวิจัยของ Maryam และคณะ [12-13] ได้ใช้เซลลูลาร์ออโตมาตาแบบ 2 มิติแบบไม่ยูนิฟอร์ม โดยที่กฎของเซลลูลาร์ออโตมาตาใช้สถานะย่านข้างเคียงมากกว่า 1 ช่วงเวลา และใช้ Chaos Mapping ในการเลือกกฎของแต่ละเซลล์

2.4.2 งานวิจัยที่นำเซลลูลาร์ออโตมาตาสร้างกุญแจ

งานวิจัยในกลุ่มนี้เป็นการนำเซลลูลาร์ออโตมาตามาใช้เป็นตัวสร้างเลขสุ่มเทียม (Pseudo random number generator) เพื่อสร้างคีย์ลับในการเข้ารหัสข้อมูล ตัวอย่างงานวิจัยในกลุ่มนี้ ได้แก่ งานวิจัยของ Rong และคณะ [15-16] ใช้เซลลูลาร์ออโตมาตา 2 มิติแบบยูนิฟอร์ม (Uniform) คือ ใช้กฎเดียวกันทั้งหมดในทุกเซลล์และใช้ฟังก์ชันในการเข้ารหัสที่มีความซับซ้อน

2.5 การใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ

2.5.1 งานวิจัยของ Jun

Jun [3] เป็นผู้ริเริ่มนำเซลลูลาร์ออโตมาตาพื้นฐานมาใช้ในการเข้ารหัสรูปภาพ โดยนำเงื่อนไขแบบคาบ (Periodic boundary) มาประยุกต์ใช้ในการสร้างแอทแทรคแตอร์เพื่อใช้ในขั้นตอนการเข้ารหัสและการสร้างกุญแจ

2.5.1.1 แอทแทรคเตอร์ (Attractor)

ในงานวิจัยของ Jun ได้กำหนดเงื่อนไขเพิ่มเติมให้กับเซลลูลาร์ออโตมาตาพื้นฐานดังนี้

1. จำนวนเซลล์ของเซลลูลาร์ออโตมาตาเป็นแบบจำกัด คือ มีจำนวนเพียง 8 เซลล์เท่านั้นดังรูปที่ 2.15

เซลล์ที่	1	2	3	4	5	6	7	8

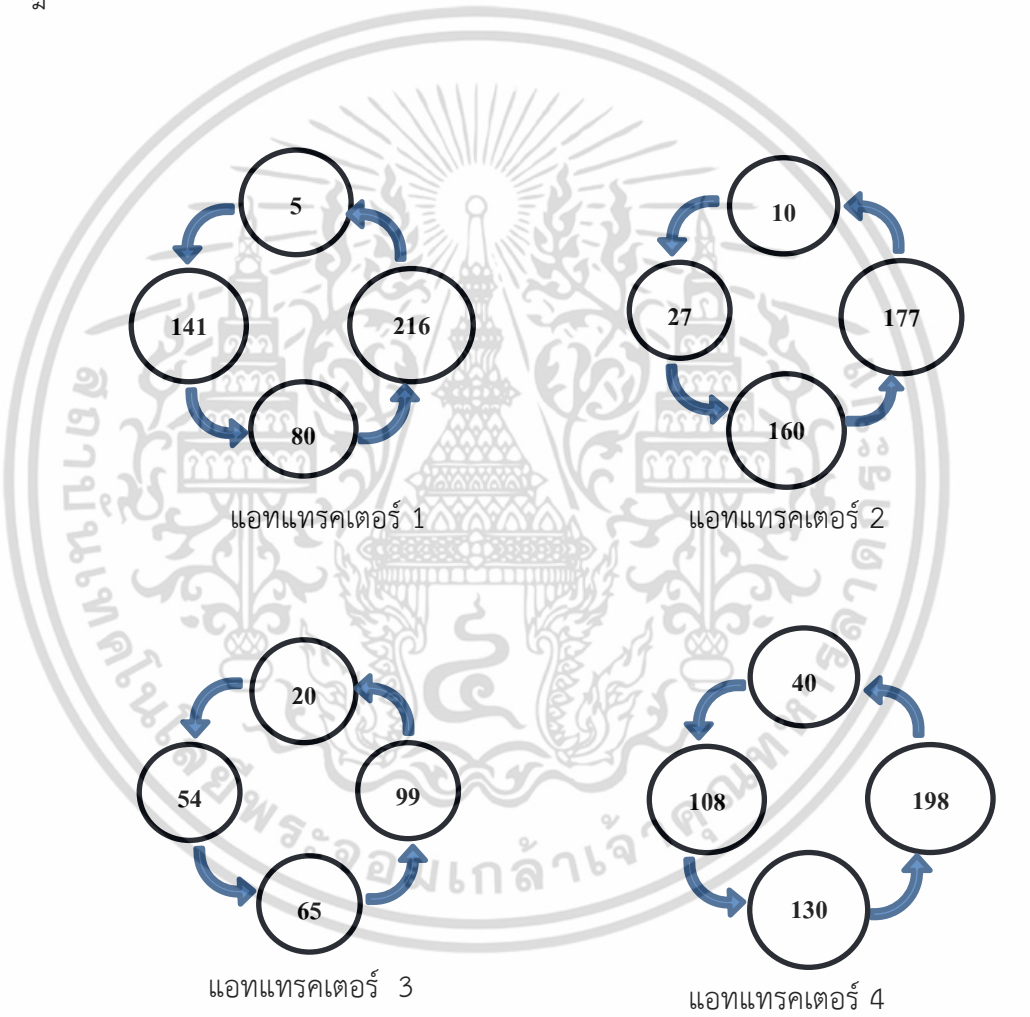
รูปที่ 2.15 จำนวนเซลล์ของเซลลูลาร์ออโตมาตาพื้นฐาน

2. ขอบเขตของเซลลูลาร์ออโตมาตาเป็นแบบคาบ (Periodic Boundary) คือเมื่อสุดเขตที่เซลล์ที่ 8 ให้วนกลับไปเริ่มใหม่ที่เซลล์ที่ 1 ในทางกลับกันถ้าสุดขอบที่เซลล์ที่ 1 ให้วนกลับไปเริ่มต้นที่เซลล์ที่ 8 ดังรูปที่ 2.16

8	1	2	3	4	5	6	7	8	1

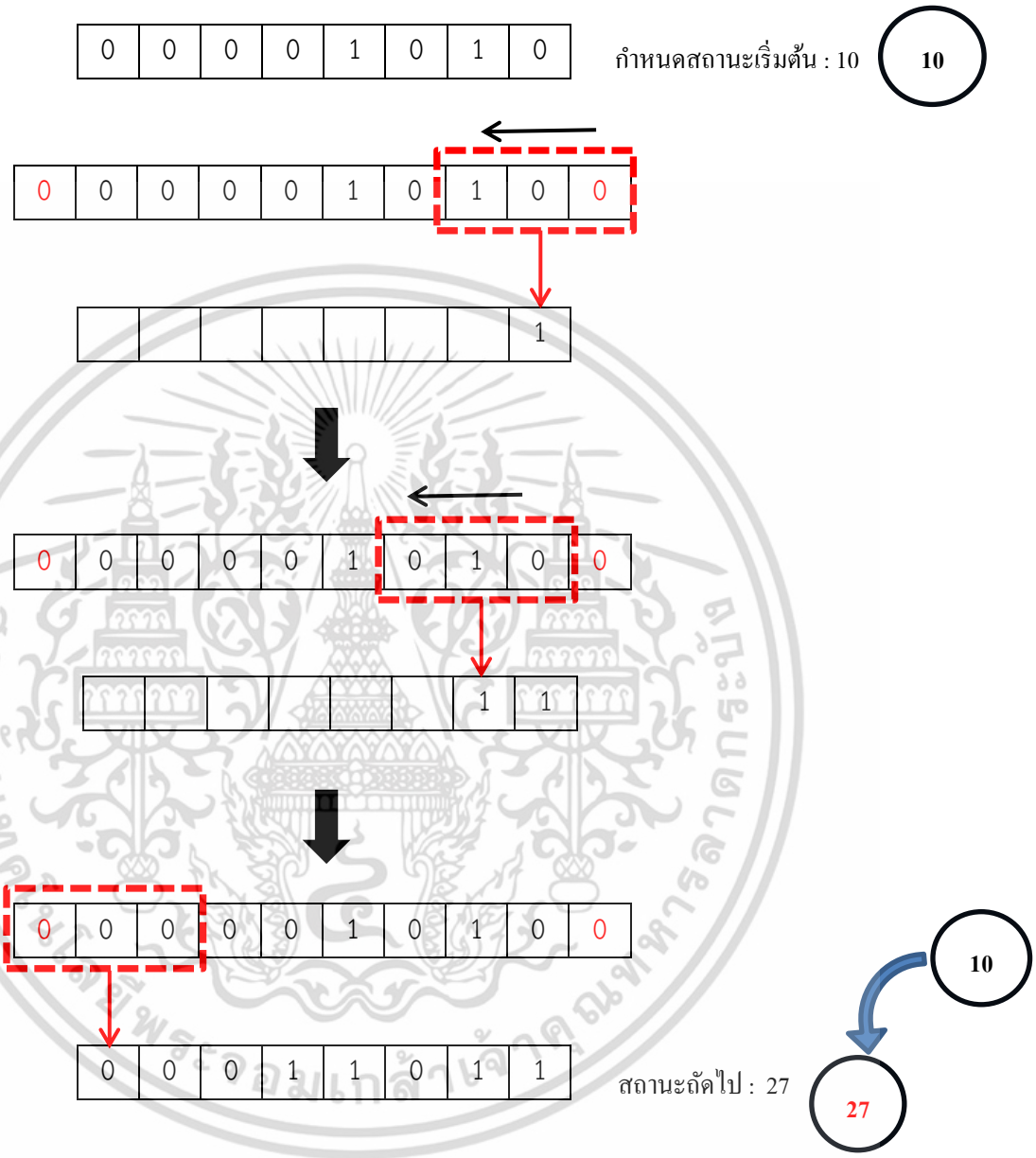
รูปที่ 2.16 รูปแบบของขอบเขตเซลลูลาร์ออโตมาที่เป็นแบบคาบ

จากทั้ง 2 เงื่อนไขที่กล่าวมาข้างต้นเมื่อนำมากำหนดสถานะเริ่มต้นให้แต่ละเซลล์ตามคุณสมบัติเซลลูลาร์ออโตมาตาแบบพื้นฐาน (สถานะของแต่ละเซลล์มีค่าอยู่ในเซต {0,1}) มีบางกฎที่เมื่อเขียนออกมาเป็นแผนภาพการเปลี่ยนสถานะจะได้กราฟที่มีลักษณะเป็นวงกลม (Cycle) คือทุกสถานะในแต่ละเซลล์จะเปลี่ยนกลับมาเป็นค่าเดิม เรียกกราฟลักษณะนี้ว่าแอทแทรคเตอร์[3] ซึ่งพบว่าจากจำนวน 256 กฎ มี 128 กฎที่มีแอทแทรคเตอร์และจำนวนแอทแทรคเตอร์ในแต่ละกฎจะไม่เท่ากันรูปที่ 2.17 แสดงแอทแทรคเตอร์ทั้งหมดของกฎ 22 ซึ่งวิธีการหาแอทแทรคเตอร์จะกล่าวถึงในหัวข้อที่ 2.5.2 และรูปที่ 2.18 แสดงตัวอย่างการคำนวณหาสถานะถัดไปของแอทแทรคเตอร์ที่ 2 ของกฎ 22



รูปที่ 2.17 แผนภาพการเปลี่ยนสถานะของกฎ 22

สถานะย่านข้างเคียง	111	110	101	100	011	010	001	000
สถานะใหม่ของกฎ 22	0	0	0	1	0	1	1	0



รูปที่ 2.18 ตัวอย่างขั้นตอนการสร้างแอทแทรคเตอร์ที่ 2 ของกฎ 22

คุณสมบัติของแอทแทรคเตอร์สามารถนำมาเขียนเป็นสมการได้ดังนี้

$$state(1) \oplus state(2) \oplus \ldots \oplus state(k) = 0 \quad (2.7)$$

เมื่อ $state(i)$ คือ ค่าของสถานะที่ i ของแอทแทรคเตอร์

k คือ สถานะทั้งหมดของแอทแทรคเตอร์

จากคุณสมบัติในสมการที่ 2.7 หากนำค่าคงที่ใดๆ มาทำการ Xor จะได้ค่าคงที่นั้น

$$n \oplus state(1) \oplus state(2) \oplus \ldots \oplus state(k) = n \oplus 0 = n \quad (2.8)$$

เมื่อ n คือ ค่าคงที่ใดๆ

Jun นำคุณสมบัติในสมการที่ 2.8 มาประยุกต์ใช้กับการเข้ารหัส โดยนำค่าที่ต้องการเข้ารหัสไป Xor กับสถานะของแอทแทรคเตอร์บางส่วนเพื่อให้ได้ไซเฟอร์เท็กซ์และในการถอดรหัสให้นำค่าไซเฟอร์เท็กซ์ไป Xor กับสถานะที่เหลือของแอทแทรคเตอร์เพื่อจะได้ค่าข้อมูลต้นฉบับ (เพลนเท็กซ์) กลับมา

$$plain \oplus state(1) \oplus state(2) \oplus \ldots \oplus state(t) = cipher \quad (2.9)$$

$$cipher \oplus state(t+1) \oplus state(t+2) \oplus \ldots \oplus state(k) = plain \quad (2.10)$$

เมื่อ $plain$ คือ ค่าต้นฉบับหรือค่าที่ต้องการเข้ารหัส

$cipher$ คือ ค่าที่ผ่านการเข้ารหัส

t คือ จำนวนสถานะบางส่วนจากสถานะทั้งหมดของแอทแทรคเตอร์

k คือ จำนวนสถานะทั้งหมดของแอทแทรคเตอร์

2.5.1.2 กุญแจที่ใช้ในการเข้ารหัส

ในงานวิจัยของ Jun กุญแจลับที่ใช้สำหรับเข้ารหัสและถอดรหัสประกอบด้วย 3 ส่วนคือ

1. rule หมายถึงกฎของเซลลูลาร์ออโตมาตาที่ใช้ในการคำนวณหาแอทแทรคเตอร์
2. stateone หมายถึงสถานะเริ่มต้นที่ใช้ในการสร้างแอทแทรคเตอร์และเป็นสถานะเริ่มต้นในการเข้ารหัส
3. seed หมายถึงค่าที่กำหนดให้กับตัวเลขสุ่มเทียมเพื่อสุ่มจำนวนสถานะที่ใช้การเข้ารหัส

2.5.2 งานวิจัยของวนิดา

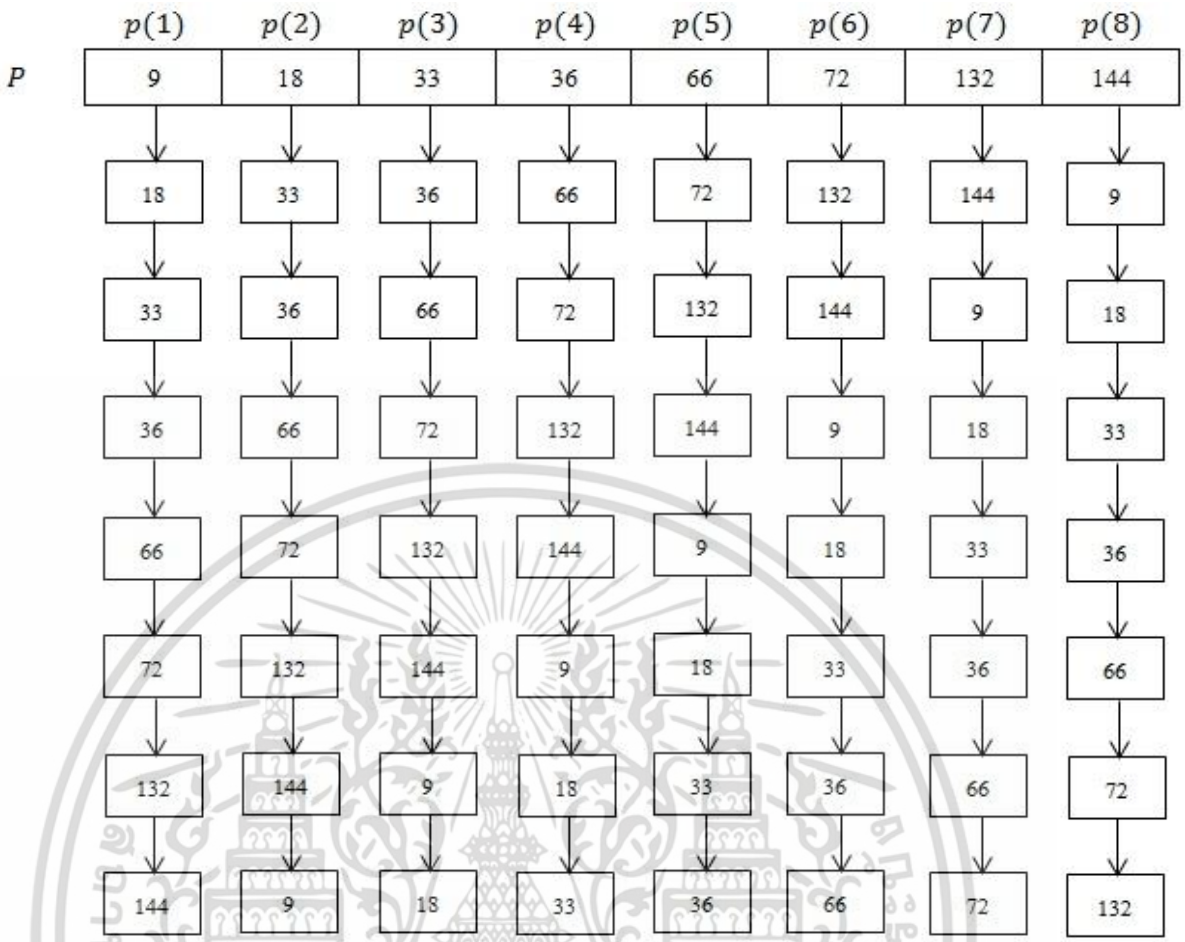
งานวิจัยของ Jun มีข้อเสียคือจำนวนคีย์ที่ใช้ในการเข้ารหัสมีไม่มากและสามารถปกปิดข้อมูลรูปภาพได้เพียงบางภาพเท่านั้น วนิดา[4] ทำการปรับปรุงกระบวนการสร้างคีย์ที่ใช้ในการเข้ารหัสเพื่อเพิ่มจำนวนของคีย์และปรับปรุงวิธีการเข้ารหัสเพื่อเพิ่มความสามารถในการปกปิดข้อมูล จากคีย์เดิมที่ใช้คือ (rule,stateone,seed) ปรับเปลี่ยนเป็น (rule,seedstate,seedtime) ซึ่ง rule คงความหมายเดิมคือกฎที่ใช้คำนวณหาแอทแทรคเตอร์ seedstate หมายถึงค่าที่ใช้กำหนดให้กับตัวสร้างเลขสุ่มเทียมเพื่อเลือกสถานะเริ่มต้นของแอทแทรคเตอร์ในแต่ละจุดภาพ และ seedtime หมายถึงค่าที่ใช้กำหนดให้กับตัวสร้างเลขสุ่มเทียมเพื่อหาจำนวนสถานะที่ใช้ในการเข้ารหัสในแต่ละจุดภาพ

2.5.2.1 การเตรียมข้อมูลสำหรับการเข้ารหัสและถอดรหัส

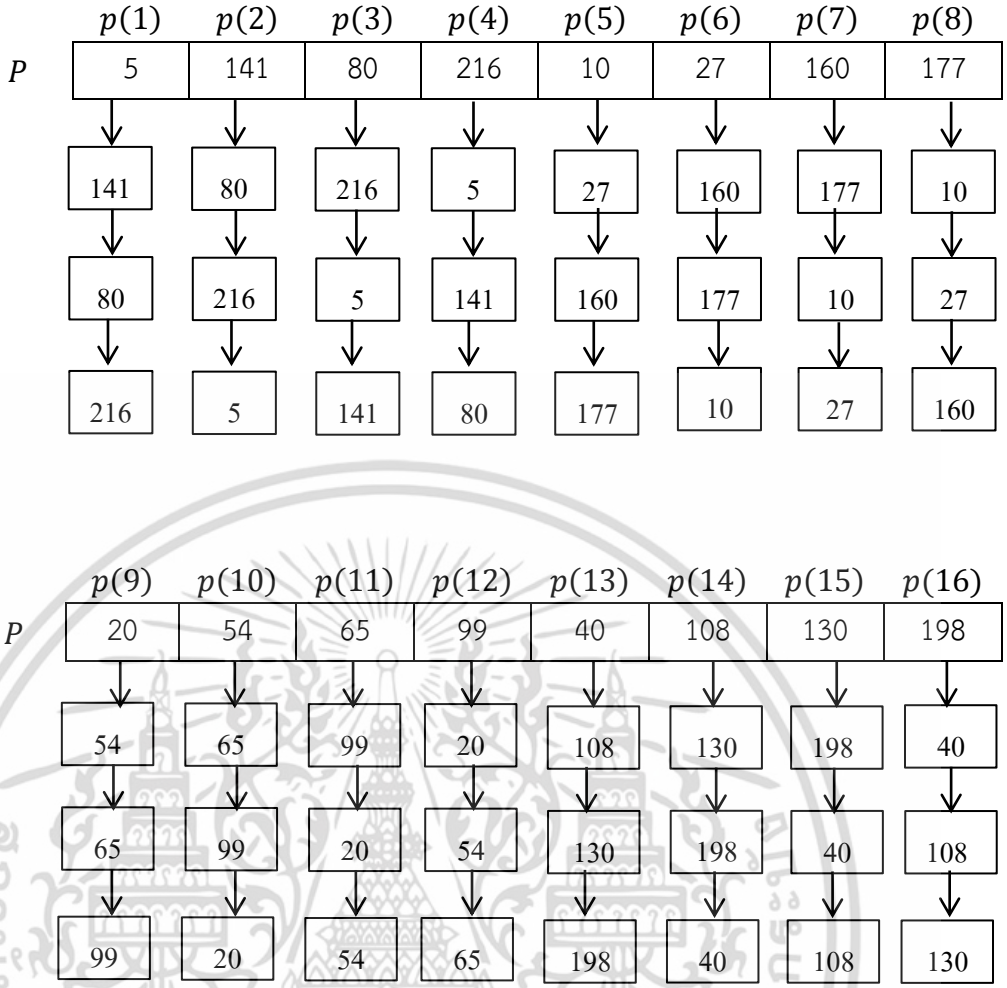
วนิดาได้ทำการเพิ่มขั้นตอนในการเตรียมข้อมูลก่อนทำการเข้ารหัสและถอดรหัสดังนี้

1. การหาแอทแทรคเตอร์ทั้งหมด

วนิดาหาแอทแทรคเตอร์ของแต่ละกฎโดยนำทุกค่าตั้งแต่ 0-255 หรือ 00000000_2 - 11111111_2 มาเป็นสถานะเริ่มต้นในการสร้างแผนภาพการเปลี่ยนสถานะ (ซึ่งมีเพียงบางค่าเท่านั้นที่มีคุณสมบัติเป็นแอทแทรคเตอร์ได้) และนำค่าสถานะเริ่มต้นที่มีคุณสมบัติเป็นแอทแทรคเตอร์ไปเก็บไว้ในแถวลำดับ P ซึ่งแต่ละช่องของแถวลำดับจะเก็บแผนภาพของแอทแทรคเตอร์เป็นโครงสร้างข้อมูลแบบลิงค์ลิสต์ (Linked - List) โดยมีสถานะเริ่มต้นเป็นสมาชิกในแถวลำดับซึ่งจะชี้ไปยังสถานะถัดไปของตนเองจนครบทุกสถานะของแอทแทรคเตอร์ รูปที่ 2.19 แสดงตัวอย่างโครงสร้างที่ใช้ในการเก็บแอทแทรคเตอร์ของกฎ 2 ที่มีเพียงแอทแทรคเตอร์เดียวโดยในรูปเป็นโครงสร้างของกฎ 2 ซึ่งมี 1 แอทแทรคเตอร์ 8 สถานะ ดังนั้นจะได้แถวลำดับจำนวน 8 ช่อง รูปที่ 2.20 แสดงโครงสร้างที่ใช้ในการเก็บแอทแทรคเตอร์ของกฎที่มีมากกว่า 1 แอทแทรคเตอร์โดยในรูปเป็นโครงสร้างของกฎ 22 ซึ่งมี 4 แอทแทรคเตอร์และแต่ละแอทแทรคเตอร์มี 4 สถานะ ดังนั้นจะได้แถวลำดับ P จำนวน 16 (4×4) ช่อง วิธีนี้ช่วยให้สามารถเข้ารหัสได้เร็วขึ้นแต่ต้องใช้พื้นที่ในการเก็บข้อมูลเพิ่มขึ้นเช่นกัน



รูปที่ 2.19 ตัวอย่างโครงสร้างพิเศษที่ใช้ในการเก็บค่าแอทแทรคเตอร์ของกฎ 2 [4]



รูปที่ 2.20 ตัวอย่างโครงสร้างพิเศษที่ใช้ในการเก็บค่าแอทแทรคเตอร์ของกฎ 22

2. การหาสถานะเริ่มต้นของแต่ละจุดภาพ

การหาสถานะเริ่มต้นของแต่ละจุดภาพเริ่มต้นจากการนำค่า seedstate ที่ได้จากกุญแจ มากำหนดค่าเริ่มต้นให้กับตัวสร้างเลขสุ่มเทียม โดยกำหนดให้สร้างตัวเลขเป็นจำนวนเท่ากับจำนวนจุดภาพทั้งหมดของภาพที่ใช้ในการเข้ารหัส สมมติภาพที่ต้องการเข้ารหัสมีขนาด $r \times c$ ดังนั้นต้องทำการสุ่มตัวเลขทั้งหมดจำนวน $r \times c$ และเก็บไว้ในแถวลำดับ S

เมื่อได้ข้อมูลที่กล่าวมาข้างต้นแล้วขั้นตอนต่อไปเป็นการหาแอทแทรคเตอร์ของแต่ละจุดภาพเพื่อใช้สำหรับการเข้ารหัสโดยสมการในการหาสถานะแอทแทรคเตอร์เริ่มต้นมีดังนี้

$$start(r,c) = p((s(r,c)\ mod\ q) + 1) \tag{2.11}$$

เมื่อ $start(r,c)$ คือ ค่าสถานะเริ่มต้นในแอทแทรคเตอร์ของจุดภาพตำแหน่งแถวที่ r หลักที่ c

$s(r,c)$ คือ ค่าในแถวลำดับ S ตำแหน่งแถวที่ r หลักที่ c

$p(i)$ คือ ค่าสถานะในแถวลำดับ P ที่ตำแหน่ง i

q คือ จำนวนสถานะทั้งหมดในแถวลำดับ P

i คือ ค่าตำแหน่งในแถวลำดับ P

$P =$

5	141	80	216	10	27	160	177

$q = 8$

S

6	8
20	4

$$start(r,c) = p((s(r,c)\ mod\ q) + 1)$$

$$start(1,1) = p\big((s(1,1)\ mod\ 8) + 1\big) = p\big((6\ mod\ 8) + 1\big) = p(7) = 160$$
$$start(1,2) = p\big((s(1,2)\ mod\ 8) + 1\big) = p\big((8\ mod\ 8) + 1\big) = p(1) = 5$$
$$start(2,1) = p\big((s(2,1)\ mod\ 8) + 1\big) = p\big((20\ mod\ 8) + 1\big) = p(5) = 10$$
$$start(2,2) = p\big((s(2,2)\ mod\ 8) + 1\big) = p\big((4\ mod\ 8) + 1\big) = p(5) = 10$$

รูปที่ 2.21 ตัวอย่างการคำนวณหาสถานะเริ่มต้น

3. การหาจำนวนสถานะในการเข้ารหัส

การหาจำนวนสถานะที่ใช้ในการเข้ารหัสมีวิธีการใกล้เคียงกับการหาสถานะเริ่มต้น โดยเริ่มจากการนำค่า seedtime ที่ได้จากกุญแจมากำหนดค่าเริ่มต้นให้กับตัวสร้างเลขสุ่มเทียม จากนั้นสุ่มค่าให้เท่ากับจำนวนจุดภาพของภาพที่จะเข้ารหัสและเก็บไว้ในแถวลำดับ T แต่ก่อนที่จะเก็บค่าลงไปในแถวลำดับ T ต้องแน่ใจก่อนว่าค่าที่ได้ต้องมีค่าน้อยกว่าจำนวนสถานะทั้งหมดของแอทแทรคเตอร์ที่ได้เลือกไว้ก่อนหน้านี้ สามารถคำนวณได้ดังนี้

$$t(r,c) = \big(ran(r,c)\ mod\ (k(r,c) - 1)\big) + 1 \qquad (2.12)$$

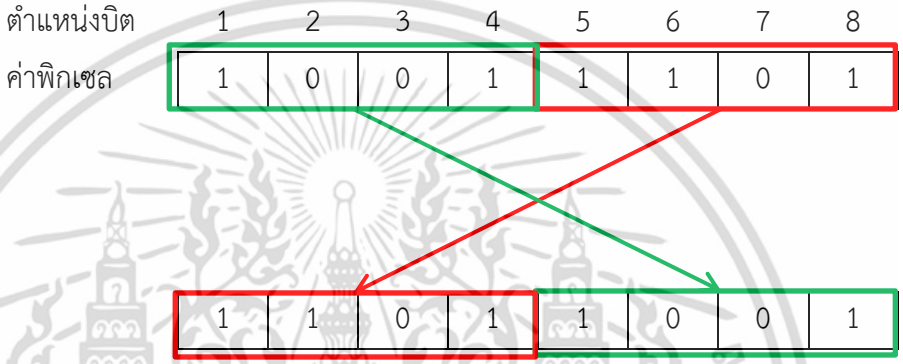
เมื่อ $t(r,c)$ คือ ค่าจำนวนสถานะที่ใช้ในการเข้ารหัสตำแหน่งแถวที่ r หลักที่ c

$ran(r,c)$ คือ ค่าที่ได้จากตัวสร้างตัวเลขสุ่มเทียมในตำแหน่งแถวที่ rหลักที่ c

$k(r,c)$ คือ จำนวนสถานะทั้งหมดของแอทแทรคเตอร์ของตำแหน่งแถวที่ r หลักที่ c

2.5.2.2 การสลับบิต

เมื่อรูปภาพผ่านขั้นตอนการเข้ารหัสเรียบร้อยแล้วจะถูกนำมาสลับบิตโดยการนำค่าความเข้มแสงในแต่ละพิกเซลมาแบ่งออกเป็น 2 ส่วน คือ เมื่อแปลงค่าพิกเซลเป็นเลขฐาน 2 ส่วนแรกคือตำแหน่งบิตที่ 1 ถึง 4 ส่วนที่สองคือตำแหน่งบิตที่ 5 ถึง 8 แล้วทำการสลับที่กันระหว่าง 2 ส่วน ดังรูปที่ 2.22



รูปที่ 2.22 วิธีการสลับบิต

2.5.3 การเข้ารหัสและถอดรหัส

สำหรับขั้นตอนการเข้ารหัสรูปภาพซึ่งใช้เข้ารหัสรูปภาพขนาด $r \times c$ พิกเซลและมีค่าความลึกของบิตเท่ากับ 8 ซึ่งสรุปได้ดังนี้

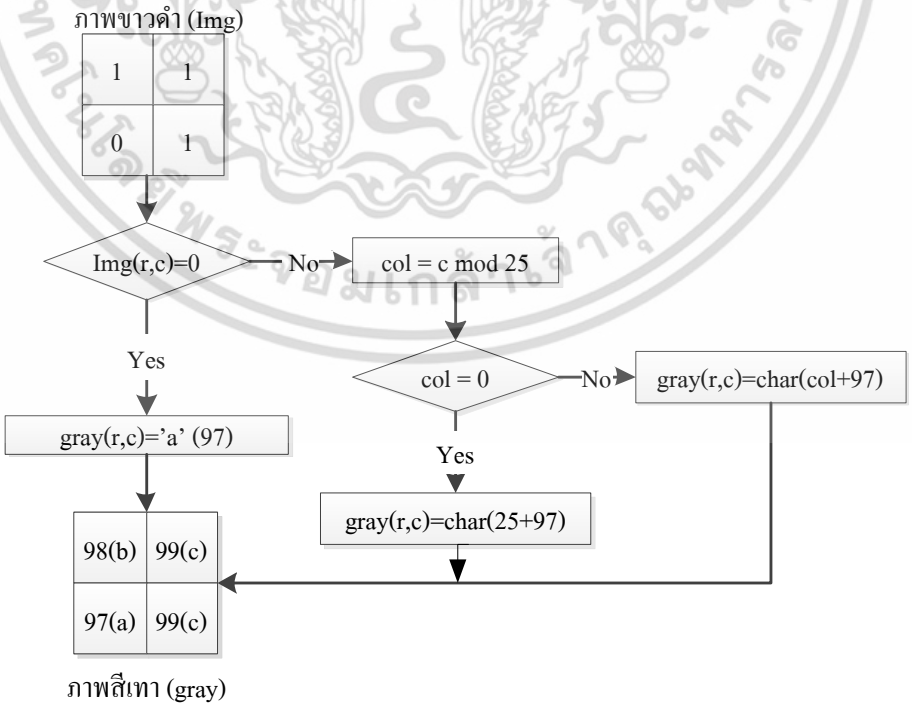
1. กำหนดค่ากุญแจลับ (rule, seedstate, seedtime)
2. หาแอทแทรคเตอร์ทั้งหมดจากค่า rule และเก็บค่าสถานะต่างๆ ที่ได้ไว้ในแถวลำดับ P ดังในรูปที่ 2.19 และรูปที่ 2.20
3. ทำการสุ่มตัวเลขด้วยตัวสร้างสุ่มเทียมโดยใช้ค่า seedstate และ seedtime ตามที่กำหนด เพื่อใช้สำหรับการหาสถานะเริ่มต้นของแอทแทรคเตอร์และจำนวนสถานะของแอทแทรคเตอร์ที่ใช้ในการเข้ารหัส โดยทำการสุ่มตัวเลขเก็บไว้ในแถวลำดับ S และ T ตามลำดับ โดยมีขนาดเท่ากับขนาดรูปภาพคือ $r \times c$
4. นำค่าความเข้มแสงของแต่ละจุดภาพมาทำการ Xor กับสถานะเริ่มต้นของแอทแทรคเตอร์และสถานะถัดไปของแอทแทรคเตอร์โดยจำนวนสถานะถัดไปจะขึ้นอยู่กับค่าสุ่มที่อยู่ในแถวลำดับ T ในตำแหน่งของจุดภาพดังกล่าว
5. นำค่าที่ได้จากการคำนวณในข้อ 4 มาทำการสลับบิตดังรูปที่ 2.22
6. สิ้นสุดการเข้ารหัสรูปภาพ

ในส่วนขั้นตอนการถอดรหัสรูปภาพมีลักษณะคล้ายกับการเข้ารหัส สามารถสรุปขั้นตอนได้ดังนี้

1. กำหนดค่ากุญแจลับ (rule , seedstate , seedtime) สำหรับใช้ในการถอดรหัส
2. เตรียมข้อมูลเช่นเดียวกับวิธีการเข้ารหัสในขั้นตอนที่ 2 และ 3
3. นำค่าความเข้มแสงของแต่ละจุดภาพมาทำการสลับบิต
4. จากนั้นนำค่าที่ได้ Xor กับสถานะของแผนภาพแอทแทรคเตอร์ที่ไม่ได้ใช้ในการเข้ารหัส
5. สิ้นสุดการถอดรหัสรูปภาพ

2.6 การเปลี่ยนภาพขาวดำให้เป็นภาพสีเทา

ภาพขาวดำมีระบบการเก็บข้อมูลที่แตกต่างกับภาพสีเทาและภาพสี เนื่องจากภาพขาวดำมีความลึกของบิตเท่ากับ 1 ดังนั้นค่าความเข้มแสงจะมีเพียง 2 ค่าคือ 0 กับ 1 เท่านั้น แต่ในการเข้ารหัสรูปภาพจำเป็นต้องใช้ค่าพิกเซลที่มี 8 บิตในการคำนวณ จึงต้องมีการเปลี่ยนภาพขาวดำให้เป็นภาพสีเทา วิธีที่ใช้ในการเปลี่ยนภาพขาวดำเป็นภาพสีเทามีด้วยกันหลายวิธี วิธีหนึ่งที่นิยมคือการเปลี่ยนความลึกของบิตจาก 1 เป็น 8 บิต เช่น หากค่าความเข้มแสงของภาพขาวดำเท่ากับ 1 (สีขาว) เมื่อเปลี่ยนเป็นภาพสีเทาค่าความเข้มแสงจะเท่ากับ 11111111 (สีขาว) เพื่อให้ความลึกเท่ากับ 8 บิต แต่มีวิธีนี้ไม่เหมาะกับการนำมาใช้ในการเข้ารหัสรูปภาพเนื่องจากมีความซ้ำซ้อนของพิกเซลของภาพสีเทาที่ผ่านการเปลี่ยนจากภาพขาวดำสูงมาก [24] ทำให้ประสิทธิภาพการเข้ารหัสลดลง ในงานวิจัยนี้นำวิธีการของ N.K. Sreelaja [17] มาประยุกต์ใช้ ซึ่งมีขั้นตอนเปลี่ยนภาพขาวดำดังรูปที่ 2.23



รูปที่ 2.23 แผนภาพขั้นตอนการเปลี่ยนภาพขาวดำเป็นภาพสีเทา

ให้ภาพขาวดำมีขนาด $r \times c$ พิกเซลและมีความลึกของบิตเท่ากับ 1 ซึ่งการเปลี่ยนภาพขาวดำให้เป็นภาพสีเทาสามารถสรุปขั้นตอนได้ตามที่แสดงในรูปที่ 2.23

เมื่อ $img(r,c)$ คือ ค่าพิกเซลของภาพขาวดำตำแหน่งแถวที่ r หลักที่ c

$gray(r,c)$ คือ ค่าพิกเซลของภาพสีเทาตำแหน่งแถวที่ r หลักที่ c

$char()$ คือ ฟังก์ชันการเปลี่ยนจากเลขฐานสิบเป็นตัวอักษร

โดยในอัลกอริทึม จะมีการตรวจสอบก่อนว่ามีพิกเซลใดที่มีค่าของพิกเซลเท่ากับ 0 หรือเป็นสีดำ จะเปลี่ยนพิกเซลนั้นเป็น a หรือ 97 (ค่ารหัสแอสกีของ a) ส่วนพิกเซลอื่นๆที่ค่าพิกเซลไม่เท่ากับ 0 จะเปลี่ยนเป็นตัวอักษรจาก b ถึง z ตามตำแหน่งของแถว

2.7 พารามิเตอร์ที่ใช้ในการวัดประสิทธิภาพการเข้ารหัสรูปภาพ

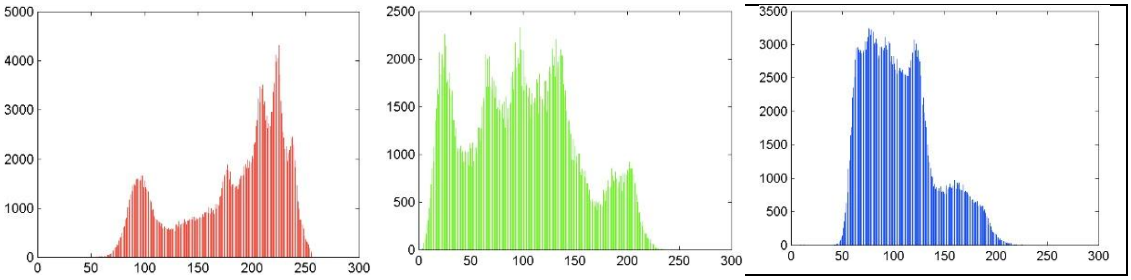
การวัดประสิทธิภาพการเข้ารหัสรูปภาพด้วยการมองด้วยตาเปล่าสามารถวัดประสิทธิภาพได้ในเบื้องต้นเท่านั้น มาตรฐานที่นิยมนำมาวิเคราะห์ประสิทธิภาพการเข้ารหัสรูปภาพเพื่อสามารถป้องกันการโจมตีในทุกประเภทมีดังต่อไปนี้

2.7.1 การแจกแจงของพิกเซล (Distribution of pixels)

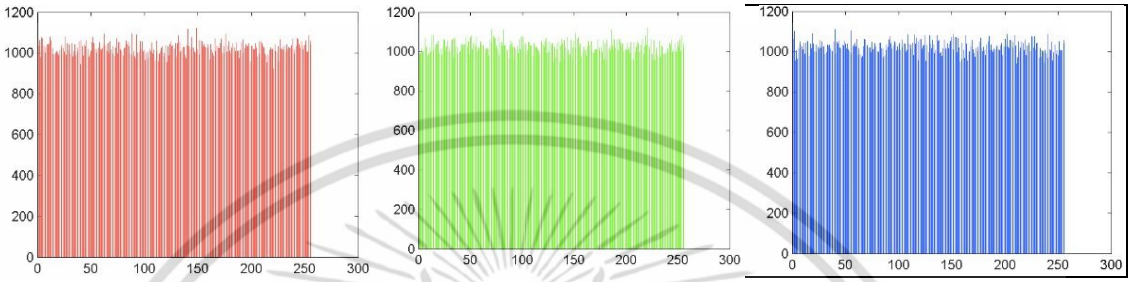
การวิเคราะห์การแจกแจงของพิกเซลเป็นการวิเคราะห์ทางสถิติประเภทหนึ่งโดยใช้ฮิสโตแกรมหรือกราฟที่แสดงจำนวนพิกเซลในแต่ละค่าความเข้มแสง[13-14] การวิเคราะห์ฮิสโตแกรมช่วยให้สามารถเห็นค่าความเข้มแสงที่ผิดปกติของภาพที่ผ่านการเข้ารหัสแล้วได้อย่างชัดเจน ทำให้ทราบได้ว่าภาพที่ผ่านการเข้ารหัสยังมีเค้าโครงจากภาพต้นฉบับอีกหรือไม่ โดยภาพที่ผ่านการเข้ารหัสด้วยวิธีการเข้ารหัสที่ดีและสามารถป้องกันการโจมตีแบบรู้ข้อมูลต้นฉบับ (Known-plaintext attack) ฮิสโตแกรมที่ได้ต้องมีการแจกแจงที่สม่ำเสมอในทุกความเข้มแสง (Uniform distribution)

สำหรับภาพสีซึ่งประกอบด้วยฮิสโตแกรมจำนวน 3 ฮิสโตแกรม คือฮิสโตแกรมของสีแดง (R) ฮิสโตแกรมสีเขียว (G) และฮิสโตแกรมสีน้ำเงิน (B) วิธีการเข้ารหัสที่ดีฮิสโตแกรมของภาพที่ผ่านการเข้ารหัสทั้งของสีแดง เขียว และน้ำเงินต้องมีความสม่ำเสมอทั้งสามสี ดังตัวอย่างในรูปที่ 2.24

ภาพต้นฉบับ (Lena)



ฮิสโตแกรมของภาพต้นฉบับ



ฮิสโตแกรมของภาพที่ผ่านการเข้ารหัส

รูปที่ 2.24 ฮิสโตแกรมของภาพต้นฉบับ (Lena) และภาพที่ผ่านการเข้ารหัสในแต่ละองค์ประกอบสี [6]

2.7.2 คุณสมบัติการแพร่ของการเข้ารหัส (Diffusion)

หลักการเข้ารหัสที่มีความปลอดภัยนั้นเมื่อมีการเปลี่ยนข้อมูลต้นฉบับเพียงเล็กน้อยต้องทำให้ข้อมูลที่ผ่านการเข้ารหัสแล้วเปลี่ยนไปเป็นจำนวนมาก [18] การเข้ารหัสรูปภาพเมื่อมีการเปลี่ยนแปลงข้อมูลรูปภาพต้นฉบับเพียงบิตเดียว ค่าพิกเซลของภาพที่ผ่านเข้ารหัสต้องเปลี่ยนไปทุกพิกเซลจึงเรียกได้ว่าวิธีการเข้ารหัสมีคุณสมบัติการแพร่ (Diffusion) [13-16]

คุณสมบัติการแพร่ของการเข้ารหัสถูกนำมาวิเคราะห์เพื่อใช้ในการป้องกันการโจมตีที่เรียกว่า “Differential Attack” ซึ่งเป็นการโจมตีประเภท Chosen Plaintext Attack ซึ่งเป็นวิธีการที่ผู้โจมตีทำการเปลี่ยนภาพต้นฉบับไปเล็กน้อย (บิตเดียว) แล้วนำภาพต้นฉบับที่มีการเปลี่ยนแปลงและภาพต้นฉบับเดิมไปเข้ารหัสเพื่อหาความแตกต่างของภาพทั้งสองในการหาความสัมพันธ์ของพิกเซลสำหรับใช้เป็นข้อมูลในการโจมตี พารามิเตอร์ที่นิยมใช้ในการตรวจสอบคุณสมบัติการแพร่ในการเข้ารหัสรูปภาพคือ Number of Pixel Change Rate (NPCR) และ Unified Average Change Intensity (UACI) [13-17]

1. NPCR (Number of Pixel Change Rate)

NPCR คืออัตราร้อยละของจำนวนของค่าพิกเซลที่แตกต่างกันซึ่งสามารถเปรียบเทียบได้สองลักษณะคือเปรียบเทียบระหว่างภาพต้นฉบับกับภาพที่ผ่านการเข้ารหัส และเปรียบเทียบระหว่างภาพต้นฉบับที่ผ่านการเข้ารหัสกับภาพต้นฉบับที่ถูกเปลี่ยนค่าเพียงเล็กน้อย (1 พิกเซล) ที่ผ่านการเข้ารหัสด้วยคีย์เดียวกัน สำหรับงานวิจัยนี้ทำการเปรียบเทียบในแบบที่สอง วิธีการเปรียบเทียบคือนำค่าพิกเซลในตำแหน่งเดียวกันของทั้ง 2 ภาพมาเทียบว่าเท่ากันหรือไม่ ถ้าไม่เท่ากันให้เป็น 1 ไม่เท่ากันให้เป็น 0 สมการในการคำนวณมีดังนี้

$$NPCR = \frac{\sum_{r,c} D(r,c)}{T} \times 100\% \tag{2.12}$$

$$D(r,c) = \begin{cases} 1 & C_1(r,c) \neq C_2(r,c) \\ 0 & C_1(r,c) = C_2(r,c) \end{cases} \tag{2.13}$$

เมื่อ $D(r,c)$ คือ ผลการเปรียบเทียบระหว่างพิกเซลของภาพที่ 1 และ 2 ตำแหน่งแถวที่ r หลักที่ c

$C_1(r,c)$ คือ ค่าความเข้มแสงของภาพที่ 1 ตำแหน่งแถวที่ r หลักที่ c

$C_2(r,c)$ คือ ค่าความเข้มแสงของภาพที่ 2 ตำแหน่งแถวที่ r หลักที่ c

T คือ จำนวนพิกเซลทั้งหมด

2. UACI (Unified Average Change Intensity)

UACI คือค่าเฉลี่ยของความแตกต่างของค่าพิกเซลระหว่างภาพ 2 ภาพเช่นเดียวกัน NPCR แต่จะนำค่าความเข้มแสงของคำนวณความแตกต่าง สมการในการคำนวณมีดังนี้

$$UACI = \frac{\sum_{r,c} |C_1(r,c) - C_2(r,c)|}{F \times T} \times 100\% \tag{2.14}$$

เมื่อ F คือ ค่าความเข้มแสงสูงสุดที่รองรับได้ของรูปภาพ

เนื่องจากการเข้ารหัสรูปภาพที่มีคุณสมบัติการแพร่ที่ดี ข้อมูลที่เข้ารหัสนั้นต้องเปลี่ยนไปทั้งหมดแม้มีการเปลี่ยนภาพต้นฉบับเพียงเล็กน้อย (1 พิกเซล) ดังนั้นค่า NPCR ต้องมีค่ามากกว่า 99% หรือเข้าใกล้ 100% มากที่สุด [26,27] และ UACI ต้องมีค่าใกล้เคียงหรือเท่ากับ 33% ซึ่งเป็นค่ามาตรฐาน [28,29]

2.7.3 ความสัมพันธ์ระหว่างพิกเซล (Correlation Coefficient)

การวิเคราะห์ความสัมพันธ์ (Correlation Coefficient) [16-19] เป็นการวิเคราะห์ความแปรปรวนระหว่าง 2 ค่าใดๆว่ามีความสัมพันธ์กันหรือไม่ ความสัมพันธ์อาจเป็นไปในทิศทางเดียวกันหรือทิศทางตรงกันข้ามกัน ในการเข้ารหัสรูปภาพจะใช้ค่าความสัมพันธ์ระหว่างพิกเซลในการวัดประสิทธิภาพวิธีการเข้ารหัสรูปภาพที่ดีต้องมีการซ่อนคุณสมบัติทั้งหมดระหว่างรูปภาพต้นฉบับและรูปภาพที่ผ่านการเข้ารหัสและแต่ละพิกเซลที่อยู่ติดกันของรูปภาพที่ผ่านการเข้ารหัสนั้นต้องมีความสัมพันธ์กันน้อยที่สุด นั่นคือวิธีการเข้ารหัสที่ดีจะต้องมีการทำลายความสัมพันธ์ระหว่างพิกเซลของภาพต้นฉบับ

ความสัมพันธ์ระหว่างพิกเซลที่อยู่ติดกันจะมีค่าอยู่ระหว่าง -1 ถึง 1 ซึ่งค่าความสัมพันธ์ที่มีค่าเข้าใกล้ 0 แสดงว่าแต่ละพิกเซลที่อยู่ติดกันของภาพที่ผ่านการเข้ารหัสมีความสัมพันธ์กันน้อยมาก แต่ค่าความสัมพันธ์ที่มีค่าเข้าใกล้หรือเท่ากับ 1 และ -1 แสดงว่าแต่ละพิกเซลที่อยู่ติดกันของภาพที่ผ่านการเข้ารหัสมีความสัมพันธ์กันมาก การหาค่าความสัมพันธ์ของ 2 พิกเซลทำได้โดยจับคู่พิกเซลที่อยู่ติดกันทั้งหมดในแนวนอน แนวตั้ง และแนวเฉียง มาคำนวณหาค่าความสัมพันธ์ดังสมการที่ 2.15-2.18 ดังนี้

$$Correlation\ Coefficient = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{2.15}$$

$$cov(x,y) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))(y_i - E(y)) \tag{2.16}$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i \tag{2.17}$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2 \tag{2.18}$$

เมื่อ $cov(x,y)$ คือ ค่าความแปรปรวนร่วมของพิกเซล x และ y

$D(x), D(y)$ คือ ค่าความแปรปรวนของพิกเซล x และ y

$E(x), E(y)$ คือ ค่าความคาดหมายของพิกเซล x และ y

T คือ จำนวนพิกเซลทั้งหมด

x, y คือ ค่าความเข้มแสงของพิกเซล x และค่าความเข้มแสงของพิกเซล y โดยที่ 2 พิกเซลนี้อยู่ติดกัน

2.7.4 Peak Signal-to-Noise Ratio (PSNR)

ปกติ PSNR ถูกใช้ในการวัดประสิทธิภาพการถอดรหัสรูปภาพและสามารถนำมาใช้สำหรับประเมินประสิทธิภาพของวิธีการเข้ารหัสได้ โดยค่า PSNR จะแสดงให้เห็นถึงความสัมพันธ์ระหว่างพิกเซลของรูปภาพต้นฉบับและรูปภาพที่ผ่านการเข้ารหัสซึ่งนำความแตกต่างพิกเซลของทั้งสองภาพมาใช้ในการคำนวณโดยการแสดงผลอยู่ในรูปแบบของเดซิเบล (dB)

ในการถอดรหัสรูปภาพ ค่า PSNR ของภาพที่ได้จากการถอดรหัสต้องมีค่ามากกว่า 30dB จึงสรุปได้ว่าภาพที่ได้จากการถอดรหัสมีความคล้ายคลึงหรือเหมือนกันภาพต้นฉบับ แต่สำหรับการเข้ารหัสที่มีประสิทธิภาพนั้นค่าที่ได้ต้องมีค่าที่น้อยว่า 10 dB [13] สมการในการคำนวณมีดังนี้

$$PSNR = 10 \times \log_{10}\left[\frac{255^2}{MSE}\right] \tag{2.19}$$

$$MSE = \frac{\sum_{r=1}^{W}\sum_{c=1}^{H}[P(r,c)-C(r,c)]^2}{T} \tag{2.20}$$

เมื่อ MSE คือ ค่าความผิดพลาดเฉลี่ยกำลังสอง

$P(r,c), C(r,c)$ คือ ค่าพิกเซลของภาพต้นฉบับและภาพที่ผ่านการเข้ารหัส ตำแหน่งแถวที่ r หลักที่ c

W คือ จำนวนพิกเซลในแนวนอน

H คือ จำนวนพิกเซลในแนวตั้ง

T คือ จำนวนพิกเซลทั้งหมด

2.7.5 จำนวนกุญแจที่เป็นไปได้ทั้งหมด (Key Space)

กุญแจลับที่ใช้ในการเข้ารหัสรูปภาพไม่ควรยาวหรือสั้นเกินไป ถ้าหากคีย์มีขนาดที่ใหญ่มากจะทำให้การเข้ารหัสมีความเร็วลดลงและไม่เหมาะสำหรับการเข้ารหัสแบบ Real-time หรือถ้าหากคีย์มีขนาดเล็กมากเกินไปอาจทำให้ผู้ไม่หวังดีสามารถคาดเดากุญแจได้ง่าย[16] ดังนั้นการเข้ารหัสรูปภาพควรใช้คีย์ที่มีขนาดใหญ่เพียงพอสำหรับการโจมตีแบบ Brute-force

2.7.6 ระยะเวลาที่ใช้ในการเข้ารหัส (Speed performance)

นอกเหนือจากวิเคราะห์ความปลอดภัยในการเข้ารหัสแล้วนั้น เวลาที่ใช้ในการเข้ารหัสและถอดรหัสยังเป็นสิ่งสำคัญในการชี้วัดวิธีการเข้ารหัสรูปภาพที่มีประสิทธิภาพ [16] ปัจจัยหลักที่มีผลกับเวลาที่ใช้ในการเข้ารหัสและถอดรหัสได้แก่ ประสิทธิภาพของอุปกรณ์ที่ใช้และอัลกอริทึมในการเข้ารหัส เป็นต้น

บทที่ 3

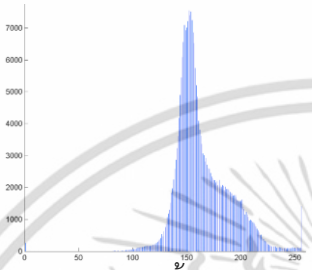
การปรับปรุงวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน

การนำภาพทั้งหมดในฐานข้อมูล USC-SIPI [6] ไปเข้ารหัสด้วยวิธีการของวนิดา[4] พบว่าภาพที่มีลักษณะโทนสีเดียวกันหรือใกล้เคียงกันเช่น รูปที่ 3.1(a) และ 3.2(a) เมื่อผ่านการเข้ารหัสแล้วจะสามารถมองเห็นเค้าโครงของภาพต้นฉบับและเมื่อนำค่าความเข้มแสงไปวาดกราฟจะได้ฮิสโตแกรมที่มีการแจกแจงพิกเซลที่ไม่สม่ำเสมอดังตัวอย่างในรูปที่ 3.1(d) และ 3.1(f) และการที่งานวิจัยเดิมไม่สามารถเข้ารหัสรูปภาพขาวดำได้ งานวิจัยนี้จึงทำการปรับปรุงขั้นตอนในงานวิจัยเดิมเพื่อให้สามารถเข้ารหัสภาพได้ทั้งหมดและมีการทดสอบประสิทธิภาพของวิธีการเข้ารหัสโดยผลลัพธ์ที่ได้ต้องใกล้เคียงกับค่ามาตรฐานในทุกพารามิเตอร์

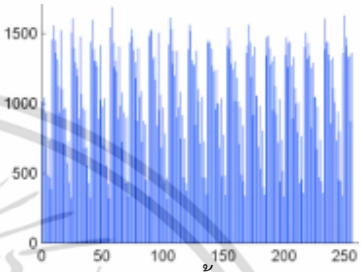
งานวิจัยนี้มีการปรับปรุงอัลกอริทึมด้วยกัน 2 ครั้งโดยครั้งที่ 1 ได้ทำการเพิ่มความสามารถในการปกปิดข้อมูลรูปภาพโดยทำการเพิ่มการ Pre-process ข้อมูลแต่ละพิกเซลก่อนนำไปเข้ารหัสโดยทำการ Xor กับค่าที่ผ่านการเข้ารหัสแล้วของพิกเซลก่อนหน้าเฉพาะในแถวเดียวกัน ซึ่งทำให้ภาพที่ผ่านการเข้ารหัสของทุกรูปภาพในฐานข้อมูล USC-SIPI ไม่แสดงเค้าโครงเดิมให้สามารถมองด้วยตาเปล่าได้และเพิ่มวิธีในการเปลี่ยนภาพขาวดำเป็นภาพสีเทาเพื่อให้สามารถนามาเข้ารหัสได้ [31] ซึ่งผลของงานวิจัยที่ได้รับการปรับปรุงในครั้งที่ 1 นั้นเมื่อนำไปวิเคราะห์ประสิทธิภาพด้วยวิธีมาตรฐานในการทดสอบการเข้ารหัสรูปภาพพบว่าค่า NPCR และ UACI มีความต่างจากค่ามาตรฐานมากจึงมีการปรับปรุงอัลกอริทึมในครั้งที่ 2 โดยนำค่าที่ผ่านการเข้ารหัสแล้วของพิกเซลสุดท้ายของแถวก่อนหน้ามาใช้ในการ Pre-process พิกเซลแรกของแถวถัดมาก่อนนำข้อมูลไปเข้ารหัสเพื่อให้ได้ค่าที่ดีในทุกพารามิเตอร์ [32]

(a) ภาพต้นฉบับ (Tiffany)

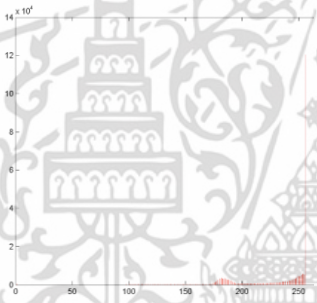
(b) ภาพที่ผ่านการเข้ารหัส



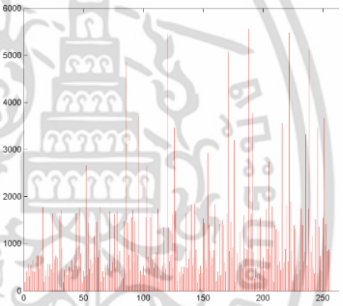
(c) ฮิสโตแกรมสีน้ำเงินของภาพ (a)



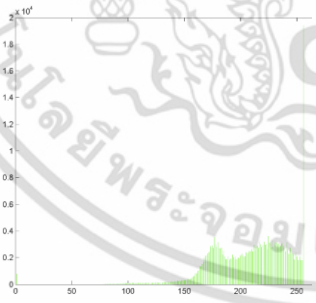
(d) ฮิสโตแกรมสีน้ำเงินของภาพ (b)



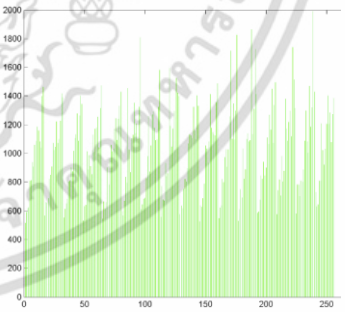
(e) ฮิสโตแกรมสีแดงของภาพ (a)



(f) ฮิสโตแกรมสีแดงของภาพ (b)

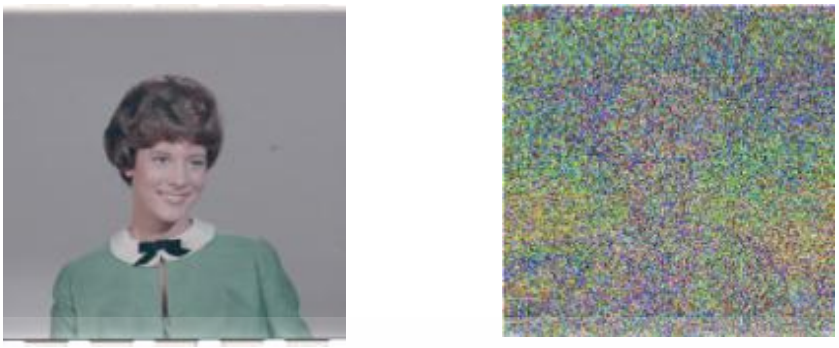


(g) ฮิสโตแกรมสีเขียวของภาพ (a)

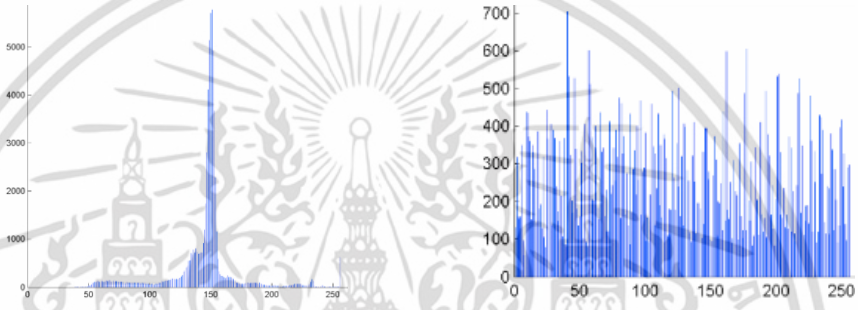


(h) ฮิสโตแกรมสีเขียวของภาพ (b)

รูปที่ 3.1 ภาพที่ผ่านการเข้ารหัสด้วยวิธีการเดิม (Tiffany)



(a) ภาพต้นฉบับ (Kate) (b) ภาพที่ผ่านการเข้ารหัส



(c) ฮิสโตแกรมสีน้ำเงินของภาพ (a) (d) ฮิสโตแกรมสีน้ำเงินของภาพ (b)

รูปที่ 3.2 ภาพที่ผ่านการเข้ารหัสด้วยวิธีการเดิม (Kate)

3.1 การวิเคราะห์ปัญหา

จากการทดลองพบว่าภาพที่เกิดปัญหาในการเข้ารหัสด้วยวิธีการของวนิดา คือภาพที่มีลักษณะโทนสีเดียวกัน เช่นรูปที่ 3.1(a) และ 3.2(a) ซึ่งเมื่อนำฮิสโตแกรมของภาพเหล่านี้มาวิเคราะห์พบว่าค่าความเข้มแสงบางค่ามีจำนวนมากกว่าค่าความเข้มแสงอื่นอย่างเห็นได้ชัดดังตัวอย่างในรูปที่ 3.1(c) และ 3.2(c) แสดงว่าภาพเหล่านี้ประกอบด้วยพิกเซลจำนวนมากที่มีความเข้มแสงในสีนั้นเป็นค่าเดียวกันหรือใกล้เคียงกันซึ่งจุดภาพบริเวณเดียวกันมักมีสีเดียวกันหรือโทนสีใกล้เคียงกันจึงมีความสัมพันธ์ระหว่างพิกเซลสูง(ทำให้บางภาพยังคงเค้าโครงของภาพต้นฉบับ) แม้ว่าอัลกอริทึมของวนิดาจะมีการทำลายความสัมพันธ์ของพิกเซลที่อยู่ใกล้เคียงกันในระหว่างการเข้ารหัสโดยการใช้กุญแจและการสลับบิตแต่ในภาพที่มีความซ้ำซ้อนของพิกเซลเป็นจำนวนมากเมื่อผ่านการเข้ารหัสความซ้ำซ้อนและความสัมพันธ์ยังคงอยู่

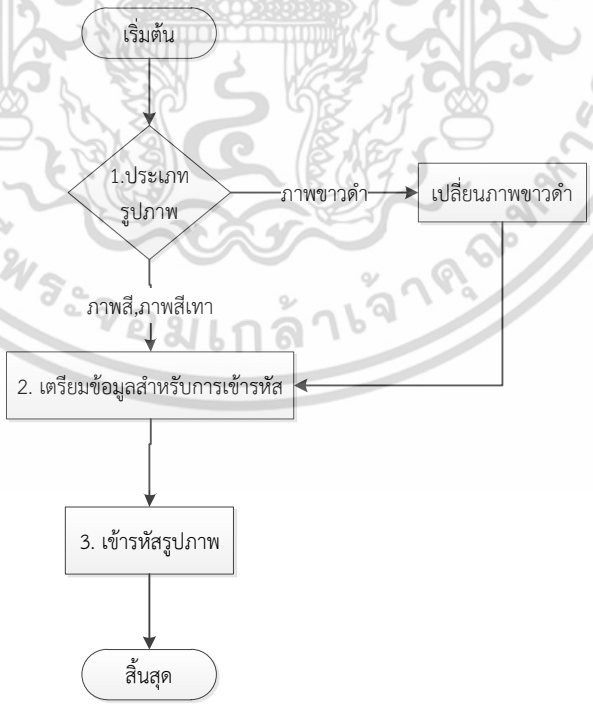
ดังนั้นในการปรับปรุงวิธีการเข้ารหัสในงานวิจัยนี้จึงมีการนำหลักการของการแพร่เข้ามาใช้เพื่อลดความซ้ำซ้อนของพิกเซลก่อนการเข้ารหัสและลดความสัมพันธ์ระหว่างพิกเซลของภาพที่ผ่านการเข้ารหัส โดยการเพิ่มขั้นตอนก่อนที่จะนำค่าแต่ละพิกเซลไปเข้ารหัส (Pre-process) ซึ่งวิธีการของ

งานวิจัยนี้สามารถนำไปใช้กับภาพขาวดำซึ่งมีความซ้ำซ้อนของข้อมูลสูงมากทำให้เข้ารหัสรูปภาพได้ทุกประเภทสี

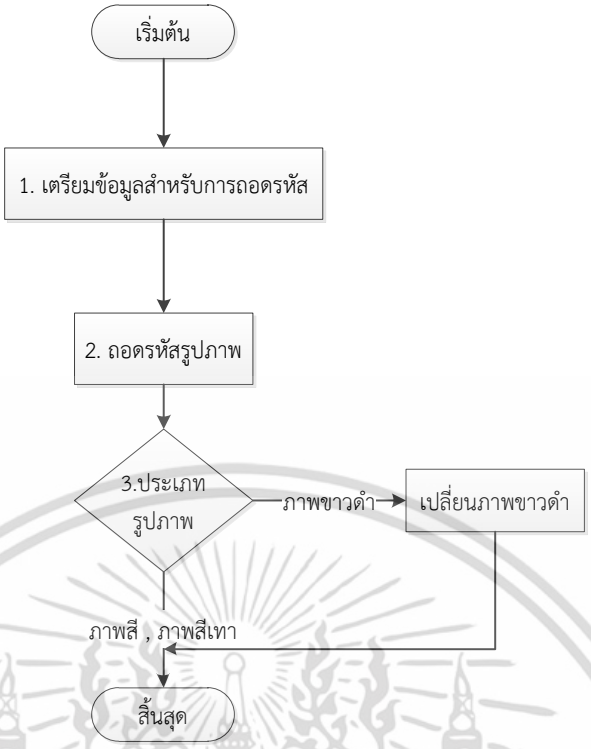
3.2 ขั้นตอนวิธีการเข้ารหัสรูปภาพ

ขั้นตอนการเข้ารหัสรูปภาพในงานวิจัยนี้ประกอบด้วย 3 ขั้นตอนดังรูปที่ 3.3 โดยขั้นตอนแรกเป็นขั้นตอนการตรวจสอบประเภทของรูปภาพ หากเป็นภาพขาวดำจะทำการเปลี่ยนภาพขาวดำเป็นภาพสีเทาก่อนที่ทำขั้นตอนต่อไป แต่ถ้าเป็นภาพสีเทาหรือภาพสีให้ทำขั้นตอนต่อไปได้ทันที ขั้นตอนนี้เป็นขั้นตอนที่เพิ่มขึ้นมาเพื่อให้สามารถเข้ารหัสรูปภาพได้ทุกประเภทสี ขั้นตอนที่สองเป็นขั้นตอนการเตรียมข้อมูลก่อนการเข้ารหัสซึ่งเป็นข้อมูลที่จำเป็นในการเข้ารหัส เช่น กุญแจลับที่ใช้ในการเข้ารหัส แอทแทรคเตอร์ที่ใช้ในการเข้ารหัส เป็นต้น ขั้นตอนสุดท้ายเป็นขั้นตอนการเข้ารหัสโดยนำข้อมูลในขั้นตอนที่สองมาทำการเข้ารหัส

ขั้นตอนการถอดรหัสจะประกอบด้วย 3 ขั้นตอนเช่นเดียวกันได้แก่ ขั้นตอนแรกเป็นการเตรียมข้อมูลเช่นเดียวกับการเข้ารหัส ขั้นตอนที่สองเป็นขั้นตอนการนำข้อมูลที่ได้จากขั้นตอนแรกมาทำการถอดรหัสรูปภาพ ขั้นตอนสุดท้ายเป็นการแยกประเภทสีของรูปภาพซึ่งหากรูปภาพต้นฉบับเป็นภาพขาวดำจะทำการเปลี่ยนจากภาพสีเทาเป็นภาพขาวดำเพื่อให้รูปภาพที่ผ่านการเข้ารหัสกลับมาเป็นประเภทสีแบบเดิมดังรูปที่ 3.4



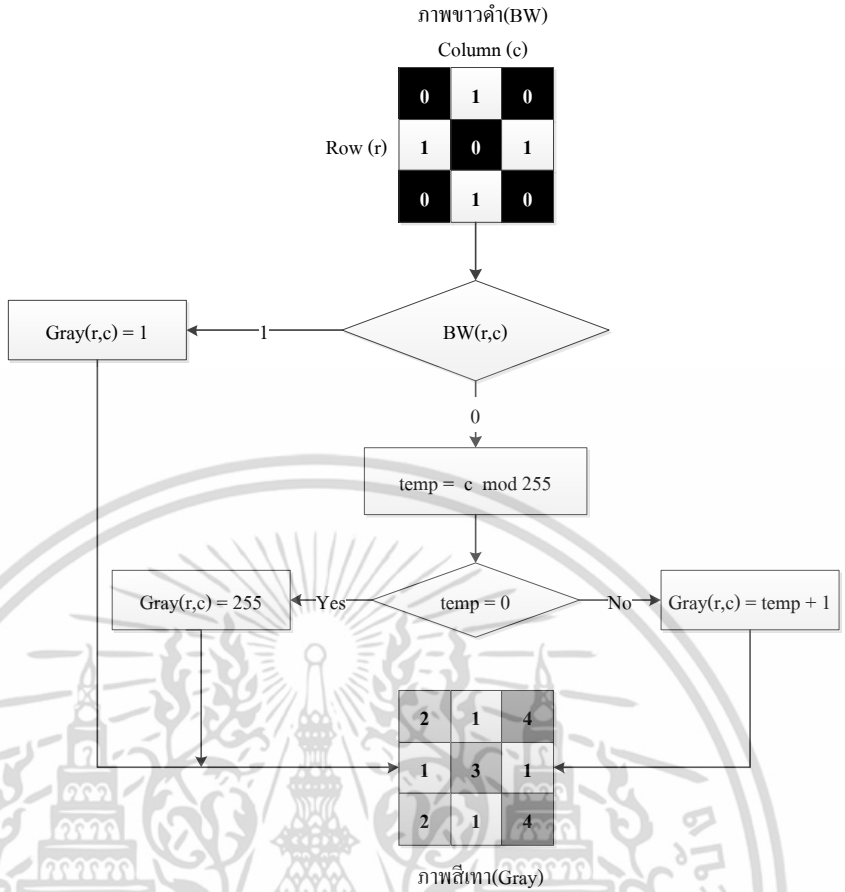
รูปที่ 3.3 ขั้นตอนทั้งหมดในการเข้ารหัสรูปภาพ



รูปที่ 3.4 ขั้นตอนทั้งหมดในการถอดรหัสรูปภาพ

3.3 การเปลี่ยนภาพขาวดำเป็นภาพสีเทา

เนื่องจากวิธีการเข้ารหัสในงานวิจัยนี้จะเข้ารหัสทีละพิกเซล และแต่ละพิกเซลจะมีค่าความลึกของบิตเท่ากับ 8 บิตจึงต้องมีการปรับค่าความลึกของบิตของภาพขาวดำที่มีเพียง 1 บิต (0 แทนสีดำ และ 1 แทนสีขาว) เป็น 8 บิต นั่นคือการเปลี่ยนภาพขาวดำเป็นภาพสีเทานั่นเอง งานวิจัยนี้นำวิธีการของ Sreelaja มาประยุกต์ใช้ โดยมีการเปลี่ยนความเข้มแสงในวิธีการของ Sreelaja ที่มีเพียง 26 ค่า (97 ถึง 122 หรือ ‘a’ ถึง ‘z’) เป็น 255 คือ 1 ถึง 255 ค่า เพื่อลดความซ้ำซ้อนของความเข้มแสงของภาพที่ใช้ในการเข้ารหัส ซึ่งการเปลี่ยนค่าความเข้มแสงจะเปลี่ยนเฉพาะพิกเซลสีดำ (ค่าความเข้มแสงเท่ากับ 0) ซึ่งมีค่าแตกต่างตามตำแหน่งของคอลัมน์ในแต่ละพิกเซล รูปที่ 3.5 แสดงตัวอย่างการเปลี่ยนรูปภาพขาวดำขนาด $r \times c$ พิกเซลเป็นภาพสีเทา



รูปที่ 3.5 ตัวอย่างขั้นตอนการเปลี่ยนรูปภาพขาวดำเป็นภาพสีเทา

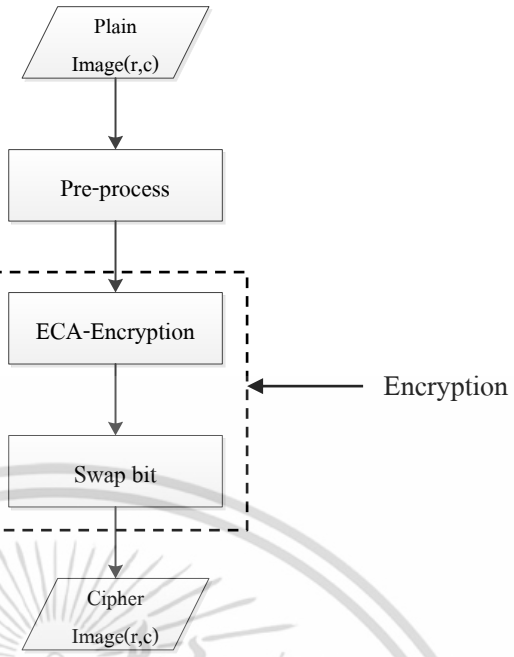
สำหรับการเปลี่ยนจากภาพสีเทากลับเป็นภาพขาวดำสามารถทำได้โดยตรวจสอบค่าพิกเซลถ้าพิกเซลใดของภาพสีเทามีค่าความเข้มแสงไม่เท่ากับ 1 ให้เปลี่ยนพิกเซลนั้นเป็น 0 ส่วนพิกเซลที่มีค่าเท่ากับ 1 จะมีค่าเท่าเดิม

3.4 การเตรียมข้อมูลสำหรับการเข้ารหัสและถอดรหัสรูปภาพ

ขั้นตอนการเตรียมข้อมูลที่ใช้ในขั้นตอนของการเข้ารหัสและถอดรหัสได้แก่การเตรียม แอทแทรคเตอร์ที่ใช้ในแต่ละพิกเซล จำนวนสถานะที่ใช้ในแต่ละพิกเซลและสถานะเริ่มต้นของแต่ละพิกเซล โดยมีวิธีการเช่นเดียวกับงานวิจัยเดิม ซึ่งได้อธิบายไว้ในหัวข้อ 2.5.3

3.5 การเข้ารหัสและถอดรหัสรูปภาพ

เมื่อเตรียมข้อมูลสำหรับการเข้ารหัสรูปภาพเรียบร้อยแล้วขั้นตอนต่อไปเป็นการเข้ารหัสรูปภาพ ในงานวิจัยนี้มีการเพิ่มขั้นตอนการ Pre-process ซึ่งจะนำค่าไซเฟอร์เท็กซ์ของพิกเซลก่อนหน้ามาทำการ Xor กับเพลนเท็กซ์ของพิกเซลที่จะเข้ารหัสซึ่งมีขั้นตอนดังรูปที่ 3.6



รูปที่ 3.6 ขั้นตอนการทำงานของการเข้ารหัส

```
For r = 1 to N_r
    For c = 1 to N_c
        If r = 1 และ c = 1
            temp = 0
        Elseif r ≠ 1 และ c = 1
            temp = pre(r − 1, N_c)
        Else
            temp = pre(r, c − 1)
        End if
        pre(r, c) = (plain(r, c) ⊕ temp)
        pre_c(r, c) = pre(r, c) ⊕ state_encrypt
        cipher(r, c) = swapbit(pre_c(r, c))
    End for
End for
```

รูปที่ 3.7 อัลกอริทึมในการเข้ารหัส

เมื่อ $pre(r,c)$ คือ ค่าความเข้มแสงของพิกเซลต้นฉบับตำแหน่งแถวที่ r และหลักที่ c ที่ผ่านการทำ Pre-process

$plain(r,c)$ คือ ค่าความเข้มแสงของภาพต้นฉบับในตำแหน่งแถวที่ r และหลักที่ c

$pre\_c(r,c)$ คือ ค่า $pre(r,c)$ ที่ผ่านการเข้ารหัสด้วยคีย์ที่ใช้สำหรับเข้ารหัส

$state\_encrypt$ คือ สถานะหรือคีย์ที่ได้จากขั้นตอนการเตรียมข้อมูลสำหรับใช้ในการเข้ารหัส

$cipher(r, c)$ คือ ค่าความเข้มแสงของภาพที่ผ่านการเข้ารหัสในตำแหน่งแถวที่ r หลักที่ c หรือในตำแหน่งก่อนหน้า

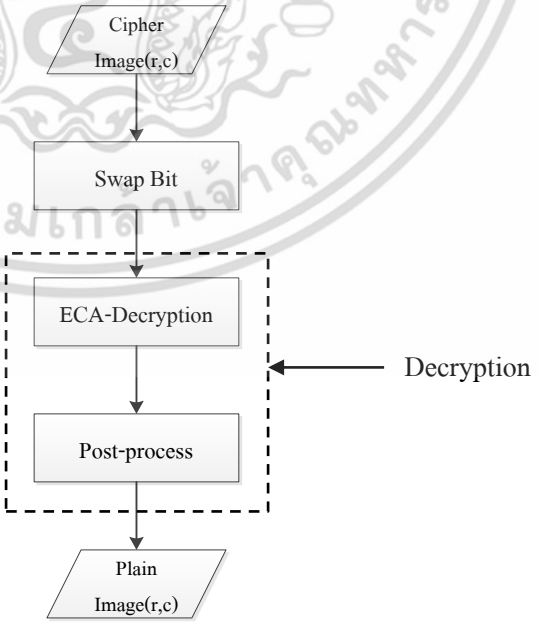
$swapbit()$ คือ ฟังก์ชันการสลับบิต

N_r, N_c คือ จำนวนแถวและหลักทั้งหมดของภาพต้นฉบับ

รูปที่ 3.7 แสดงอัลกอริทึมที่งานวิจัยนี้ใช้ในการเข้ารหัส โดยอัลกอริทึมนี้ทำการเพิ่มคุณสมบัติการแพร่หรือขั้นตอนการทำ Pre-process ดังสมการในบรรทัดที่ 3-10 เริ่มจากในพิกเซลแรกของแถวที่ 1 จะกำหนดค่าเริ่มต้นในตัวแปล $temp$ ให้เท่ากับ 0 ($temp$ เป็นตัวแปรในการเก็บข้อมูลชั่วคราว) และค่าถัดไปของ $temp$ จะขึ้นอยู่กับค่าความเข้มแสงของพิกเซลต้นฉบับที่ผ่านการทำ Pre-process ในตำแหน่งก่อนหน้าหรือค่า $pre(r, c-1)$ นั่นเอง โดยจะมีการทำ Pre-process ไปทีละพิกเซลตลอดทั้งแถวและหากเป็นพิกเซลแรกของแถวถัดไปจะนำค่าความเข้มแสงที่ผ่านการทำ Pre-process ของพิกเซลสุดท้ายของแถวก่อนหน้ามาทำการ Pre-process

จากนั้นเมื่อได้ค่าความเข้มแสงที่ผ่านการทำ Pre-process จะนำค่าที่ได้มา Xor กับค่าสถานะของแอทแทรคเตอร์ที่ได้จากการเตรียมข้อมูลในขั้นตอนก่อนหน้าและทำการสลับบิต (ดังที่ได้อธิบายในบทที่ 2) จะได้ค่าพิกเซลที่ผ่านการเข้ารหัส

สำหรับการถอดรหัสมีขั้นตอนเช่นเดียวกับการเข้ารหัสรูปภาพแต่แตกต่างกันที่ลำดับขั้นตอนดังรูปที่ 3.8



รูปที่ 3.8 ขั้นตอนการทำงานของการถอดรหัส

บทที่ 4

การทดลองและผลการทดลอง

บทนี้เป็นส่วนของผลการทดลองเพื่อวัดประสิทธิภาพของวิธีการที่ได้นำเสนอ เปรียบเทียบกับงานวิจัยของวนิดา [4] ซึ่งมีรายละเอียดดังต่อไปนี้

4.1 เครื่องมือและโปรแกรมที่ใช้ในการทดลอง

รายละเอียดของเครื่องคอมพิวเตอร์และโปรแกรมที่ใช้ในการทดลอง มีดังต่อไปนี้

หน่วยประมวลผลกลาง (CPU) : Intel Core i5 (Dual Core) 1.6 GHz

หน่วยความจำหลัก (RAM) : 2 GB

หน่วยความจำสำรอง (Hard Disk) : 30 GB

ระบบปฏิบัติการ (OS) : Microsoft Windows 7 Home Premium 32 bit

โปรแกรมที่ใช้ (Application) : Matlab

รุ่นของโปรแกรมที่ใช้ (Version) : 7.14.0 (2012a)

4.2 ข้อมูลรูปภาพที่ใช้ในการทดลอง

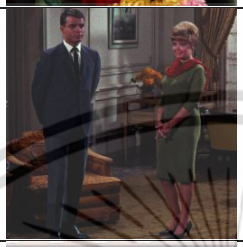
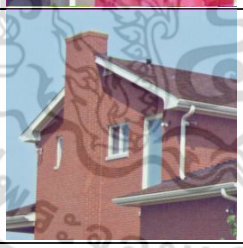
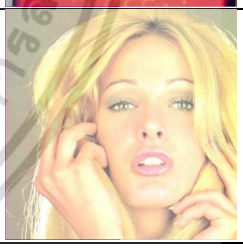
รูปภาพที่ใช้ในการทดลองมีทั้งหมด 44 รูป ประกอบด้วยภาพสีจำนวน 16 รูป และภาพสีเทาจำนวน 28 รูป ขนาดของภาพที่ใช้คือ 256×256 พิกเซล 512×512 พิกเซล และ 1024×1024 พิกเซลตามลำดับ โดยภาพที่ใช้มาจากฐานข้อมูลของ USC-SIPI [6] ในหมวดหมู่ Miscellaneous ซึ่งเป็นหมวดหมู่ของรูปภาพมาตรฐานที่ใช้ในงานวิจัยที่เกี่ยวกับการเข้ารหัสรูปภาพ จำนวนของรูปภาพและขนาดของรูปภาพที่ใช้ในการทดลองเป็นดังตารางที่ 4.1

ตารางที่ 4.1 จำนวนของรูปภาพแต่ละประเภทที่ใช้ในการทดลอง

ประเภทสีของภาพ	256×256	512×512	1024×1024	รวม
ภาพสีเทา	6	18	4	28
ภาพสี	8	8	0	16
ภาพขาวดำ	8	8	0	16
รวม	22	34	4	60

สำหรับภาพขาวดำนั้นได้มาจากการนำภาพสีภายในฐานข้อมูลจำนวน 16 รูป มาทำการเปลี่ยนเป็นภาพขาวดำโดยใช้โปรแกรม Matlab ภาพทุกภาพถูกจัดเก็บในรูปแบบไฟล์ TIFF รายชื่อและภาพทั้งหมดได้แสดงไว้ในภาคผนวก ก.

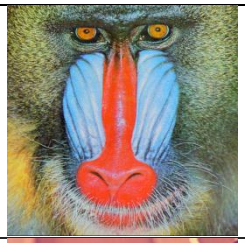
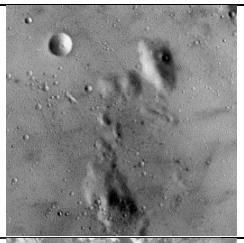
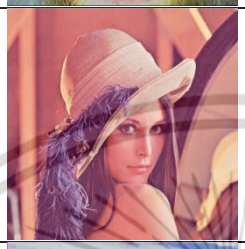
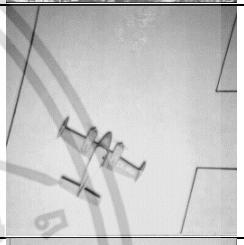
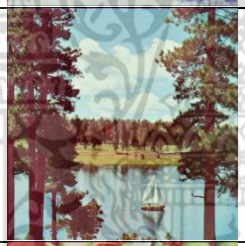
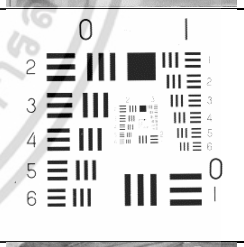
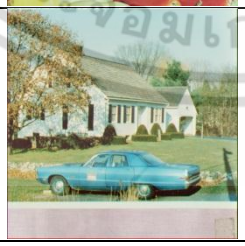
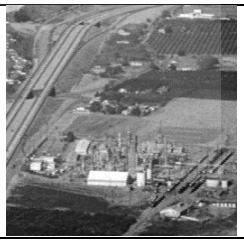
ตารางที่ 4.2 ตัวอย่างภาพที่ใช้ในการทดลอง

ชื่อภาพ	รูปภาพ	ชื่อภาพ	รูปภาพ
*Emma		Tree	
Couple		*Jelly beans 1	
*Kate		*Jelly beans 2	
*Nadear		Splash	
House		Tiffany	

* ชื่อที่ตั้งขึ้น

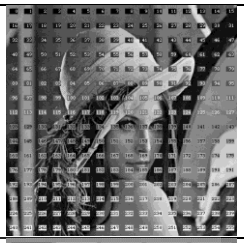
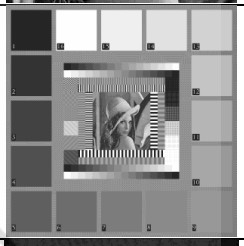
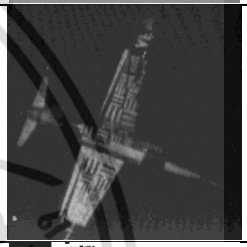
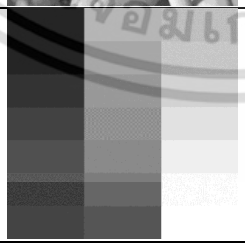
งานวิจัยนี้จะอ้างถึงรูปภาพด้วยชื่อที่ฐานข้อมูลตั้งไว้และจะมีการตั้งชื่อให้เพื่อความสะดวก สำหรับภาพที่ฐานข้อมูลไม่ได้ตั้งชื่อไว้ ตารางที่ 4.2 แสดงรูปภาพบางส่วนที่นำมาใช้ในการทดลอง

ตารางที่ 4.2 (ต่อ) ตัวอย่างภาพที่ใช้ในการทดลอง

ชื่อภาพ	รูปภาพ	ชื่อภาพ	รูปภาพ
Baboon		Moon surface	
Lena		*Aerial 1	
F-16		*Airplane 1	
Lake		Clock	
Pepper		Resolution Chart	
*Blue car		*Aerial 2	

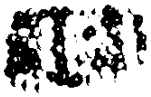
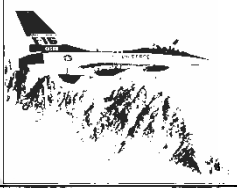
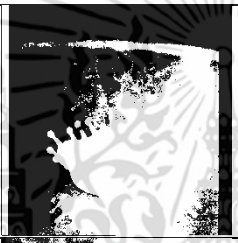
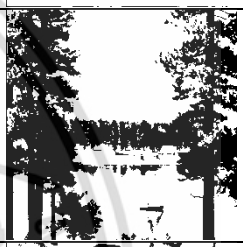
* ชื่อที่ตั้งขึ้น

ตารางที่ 4.2 (ต่อ) ตัวอย่างภาพที่ใช้ในการทดลอง

ชื่อภาพ	รูปภาพ	ชื่อภาพ	รูปภาพ
Man		*Lena Number	
Truck		*Test pattern	
*Airplane 2		*U-2	
*Boat		*Nadear_bw	
Elaine		*House_bw	
*Gray level		*Tree_bw	

***** ชื่อที่ตั้งขึ้น

ตารางที่ 4.2 (ต่อ) ตัวอย่างภาพที่ใช้ในการทดลอง

ชื่อภาพ	รูปภาพ	ชื่อภาพ	รูปภาพ
*Jelly bean 1_bw		*Lena_bw	
*Jelly bean 2_bw		*F-16_bw	
*Splash_bw		*Lake_bw	
*Tiffany_bw		*Pepper_bw	
*Baboon_bw		*Emma_bw	

* ชื่อที่ตั้งขึ้น

สำหรับคีย์ที่ใช้ในการทดลองนั้นเลือกใช้คีย์ (46,30,55) (14,53,61) (46,99,23) (80,65,96) (84,73,88) (183,5,80) (56,77,66) และ (213,78,11) เนื่องจากเป็น weak key (เมื่อนำคีย์ดังกล่าวเข้ารหัสด้วยวิธีการเดิมแล้วให้ผลที่ไม่ดี)

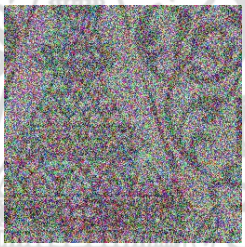
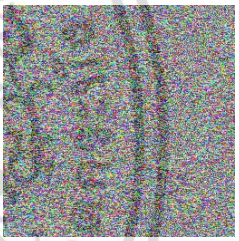
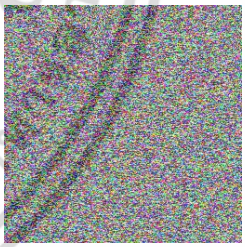
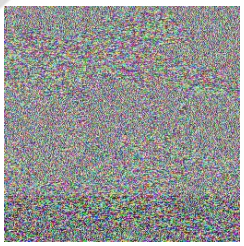
4.3 การวิเคราะห์ประสิทธิภาพ

4.3.1 ความสามารถในการปกปิดข้อมูล

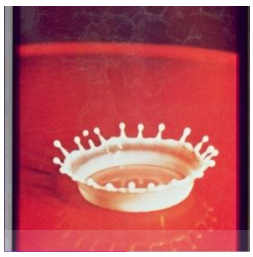
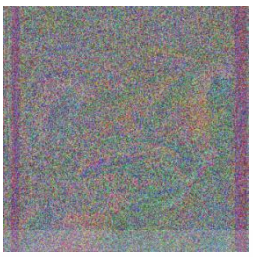
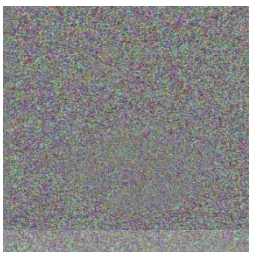
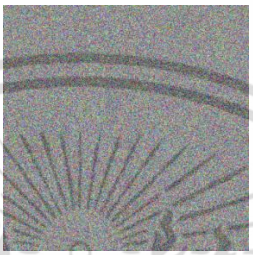
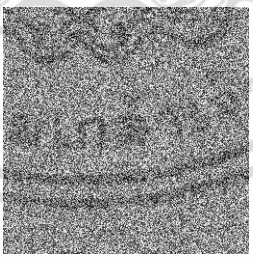
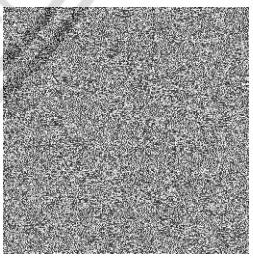
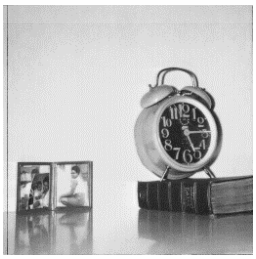
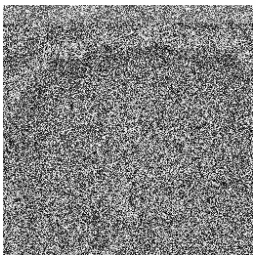
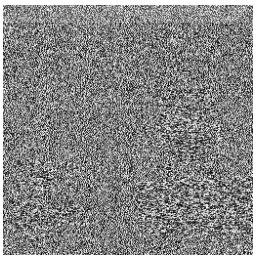
ในการเข้ารหัสด้วยวิธีการเดิมพบว่าในบางคีย์หรือภาพที่มีโทนสีเดียวกัน ภาพที่ผ่านการเข้ารหัสแล้วยังคงเค้าโครงของภาพต้นฉบับ

ตารางที่ 4.3 แสดงภาพที่เข้ารหัสด้วยคีย์ (46,30,55) เปรียบเทียบระหว่างภาพที่เข้ารหัสด้วยวิธีเดิมและวิธีการใหม่ในงานวิจัยนี้ซึ่งเห็นได้ชัดว่าภาพที่ผ่านการเข้ารหัสด้วยวิธีการแบบใหม่ไม่คงเค้าโครงของภาพต้นฉบับ ในขณะที่ภาพที่เข้ารหัสด้วยวิธีแบบเดิมยังคงเค้าโครงของภาพต้นฉบับอยู่แม้ใช้คีย์เดียวกัน และการนำภาพที่มีลักษณะโทนสีเดียวกันไปเข้ารหัสเปรียบเทียบระหว่างวิธีการเข้ารหัสแบบเดิมและแบบใหม่โดยมีการทดลองในหลายคีย์ดังตัวอย่างในตารางที่ 4.4 ปรากฏชัดว่าการเข้ารหัสด้วยวิธีการใหม่สามารถปกปิดข้อมูลได้ในทุกคีย์ที่ใช้และทุกภาพที่มีลักษณะโทนสีเดียวกัน

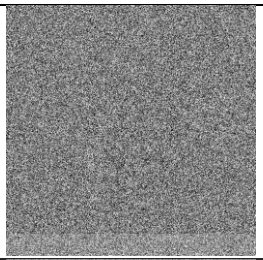
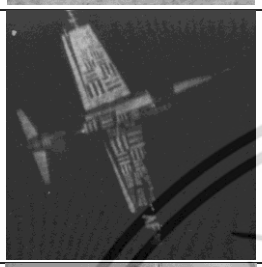
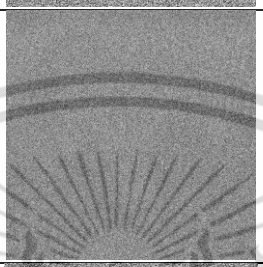
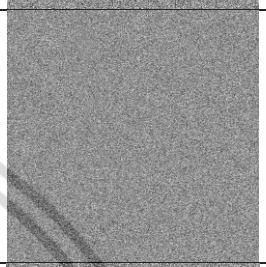
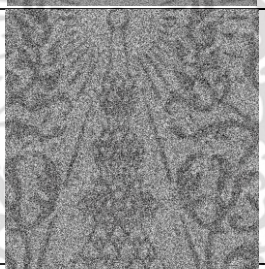
ตารางที่ 4.3 ตัวอย่างรูปภาพที่เข้ารหัสด้วยคีย์ (46,30,55)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		

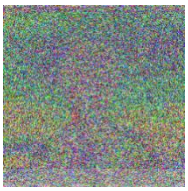
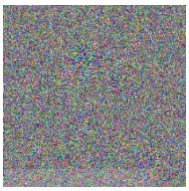
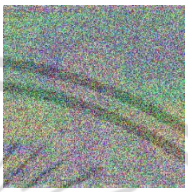
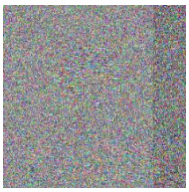
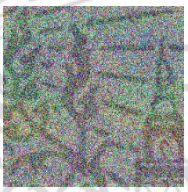
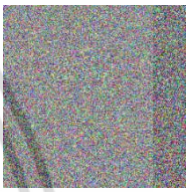
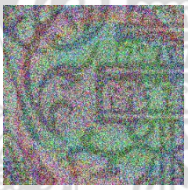
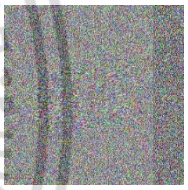
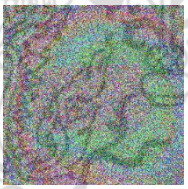
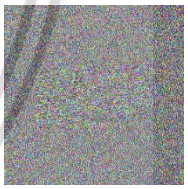
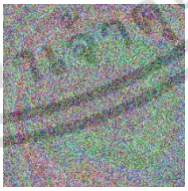
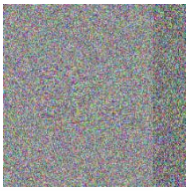
ตารางที่ 4.3 (ต่อ) ตัวอย่างรูปภาพที่เข้ารหัสด้วยคีย์ (46,30,55)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		
		
		
		

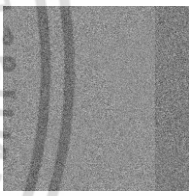
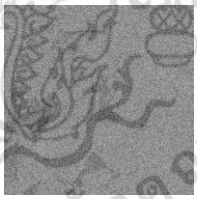
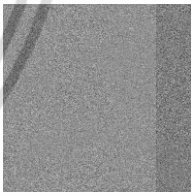
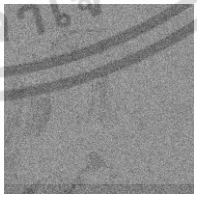
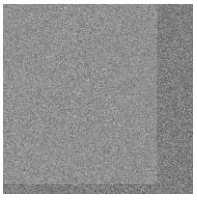
ตารางที่ 4.3 (ต่อ) ตัวอย่างรูปภาพที่เข้ารหัสด้วยคีย์ (46,30,55)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		
		

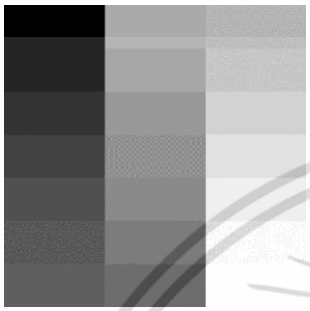
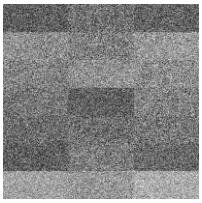
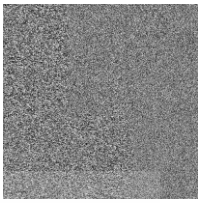
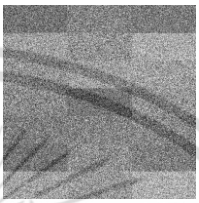
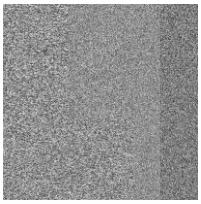
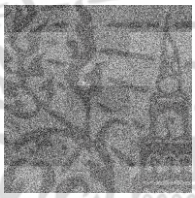
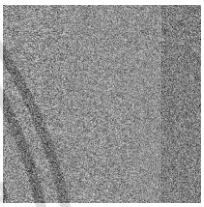
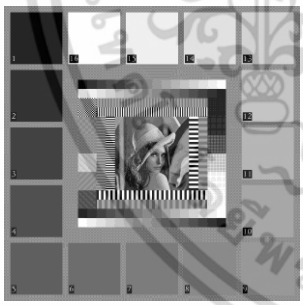
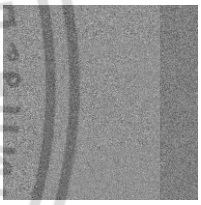
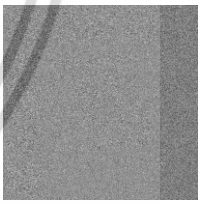
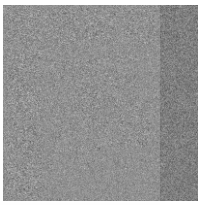
ตารางที่ 4.4 ตัวอย่างรูปภาพที่มีลักษณะโทนสีเดียวกันที่เข้ารหัสด้วยคีย์ต่างๆ

ภาพต้นฉบับ	คีย์	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
	(14,53,61)		
	(46,99,23)		
	(80,65,96)		
	(14,53,61)		
	(46,99,23)		
	(80,65,96)		

ตารางที่ 4.4 (ต่อ) ตัวอย่างรูปภาพที่มีลักษณะโทนสีเดียวกันที่เข้ารหัสด้วยคีย์ต่างๆ

ภาพต้นฉบับ	คีย์	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
	(14,53,61)		
	(46,99,23)		
	(80,65,96)		
	(14,53,61)		
	(46,99,23)		
	(80,65,96)		

ตารางที่ 4.4 (ต่อ) ตัวอย่างรูปภาพที่มีลักษณะโทนสีเดียวกันที่เข้ารหัสด้วยคีย์ต่างๆ

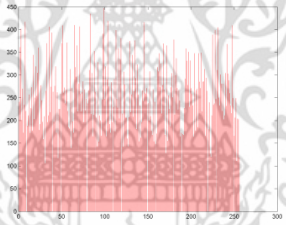
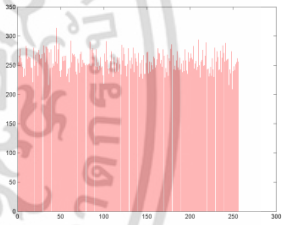
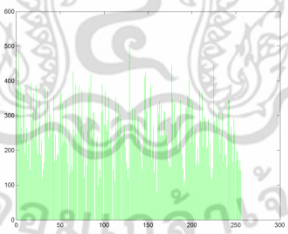
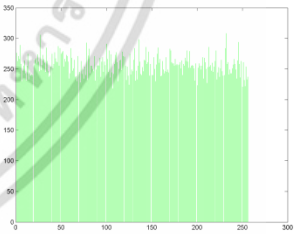
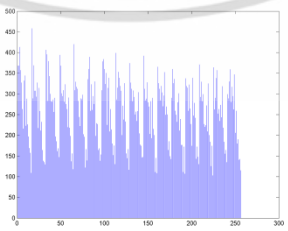
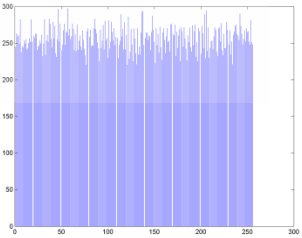
ภาพต้นฉบับ	คีย์	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
	(14,53,61)		
	(46,99,23)		
	(80,65,96)		
	(14,53,61)		
	(46,99,23)		
	(80,65,96)		

4.3.2 การแจกแจงของพิกเซล (Distribution of Pixels)

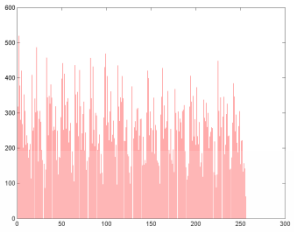
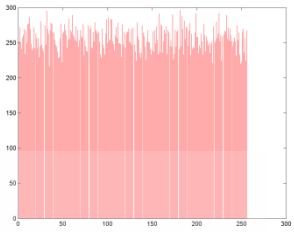
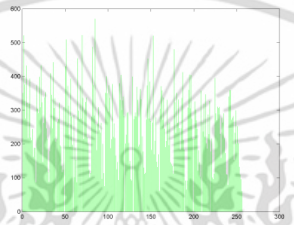
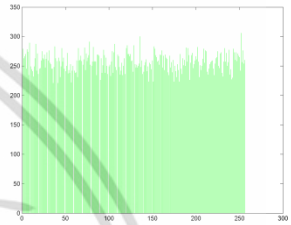
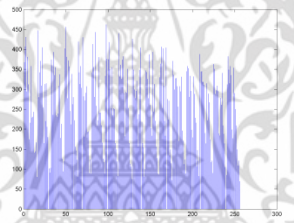
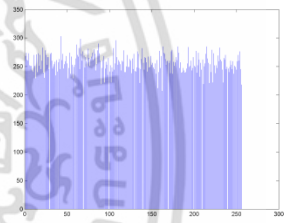
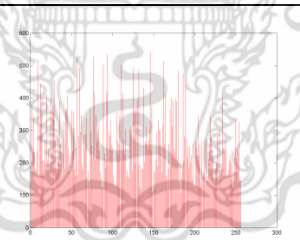
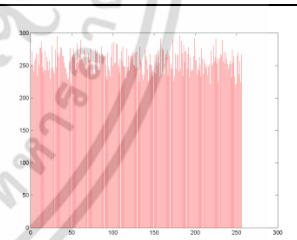
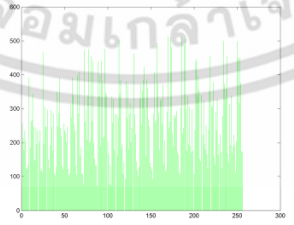
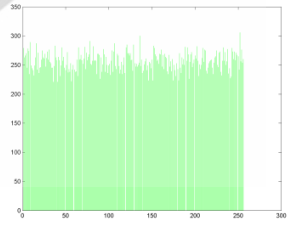
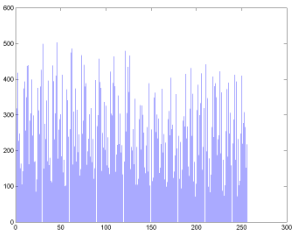
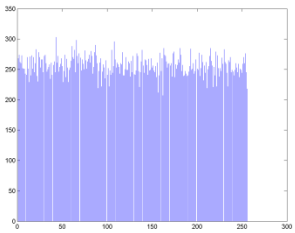
การวิเคราะห์การแจกแจงของพิกเซลเป็นวิธีการที่ได้รับความนิยมมากในการวิเคราะห์ประสิทธิภาพการเข้ารหัสรูปภาพ ซึ่งทำได้โดยนำกราฟฮิสโตแกรมมาวิเคราะห์การแจกแจงจำนวนพิกเซลในแต่ละค่าความเข้มแสง วิธีเข้ารหัสที่มีประสิทธิภาพกราฟฮิสโตแกรมของภาพที่ผ่านการเข้ารหัสต้องมีลักษณะราบเรียบสม่ำเสมอ

ตารางที่ 4.5 และ 4.6 แสดงตัวอย่างการเปรียบเทียบฮิสโตแกรมของภาพสีและภาพสีเทาที่ผ่านการเข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88) ปรากฏอย่างชัดเจนว่าภาพที่ได้จากขั้นตอนการเข้ารหัสด้วยวิธีการใหม่มีค่าฮิสโตแกรมที่สม่ำเสมอกว่าภาพที่ได้จากขั้นตอนการเข้ารหัสด้วยวิธีการเดิมในทุกภาพโดยเฉพาะภาพต้นฉบับที่มีโทนสีใกล้เคียงกัน จึงสามารถสรุปได้ว่าวิธีการเข้ารหัสแบบใหม่มีคุณสมบัติการแจกแจงพิกเซลที่ดีกว่าวิธีการเดิม

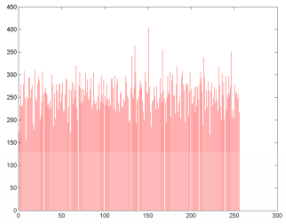
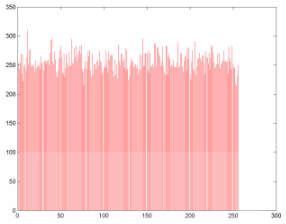
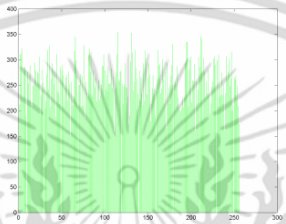
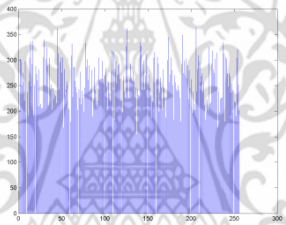
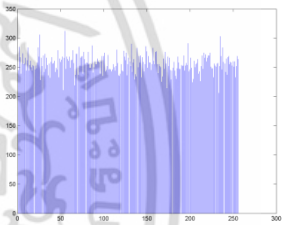
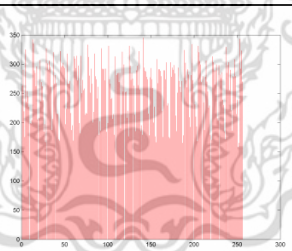
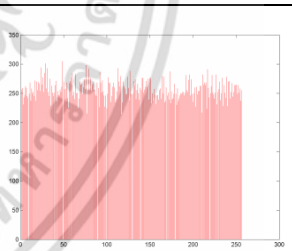
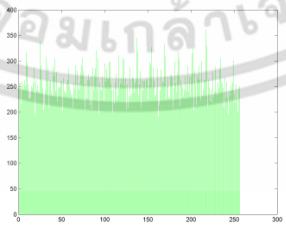
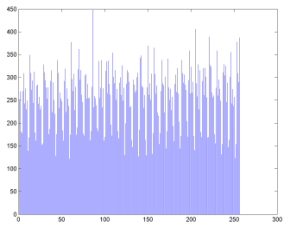
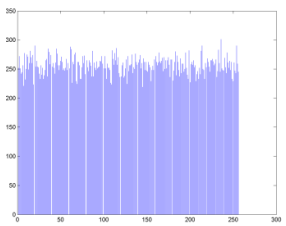
ตารางที่ 4.5 ฮิสโตแกรมของตัวอย่างภาพสีที่เข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88)

ภาพต้นฉบับ	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
	ฮิสโตแกรม(ภาพสี)	ฮิสโตแกรม(ภาพสี)
		
		
		

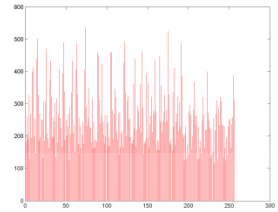
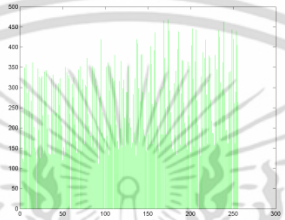
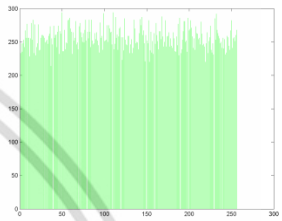
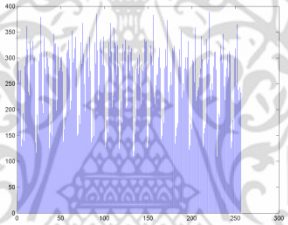
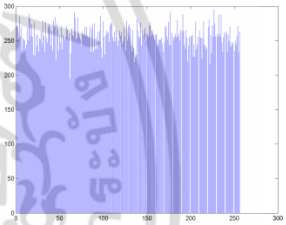
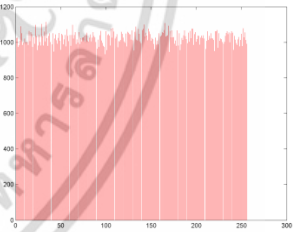
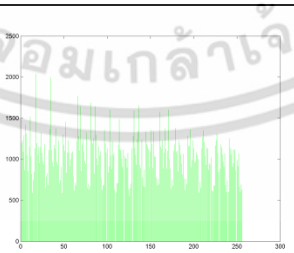
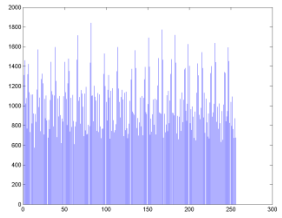
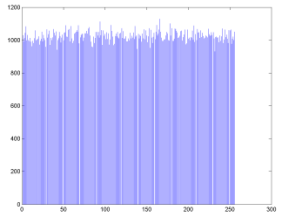
ตารางที่ 4.5 (ต่อ) ฮิสโตแกรมของตัวอย่างภาพสีที่เข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88)

ภาพต้นฉบับ	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
	ฮิสโตแกรม(ภาพสี)	ฮิสโตแกรม(ภาพสี)
		
		
		
		
		
		

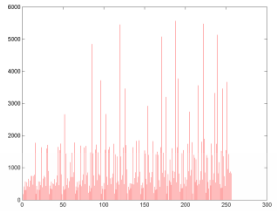
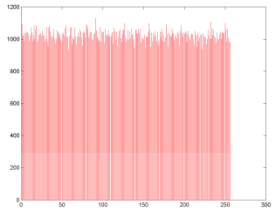
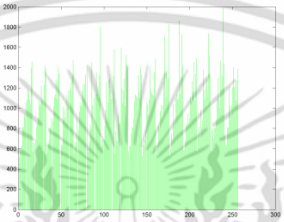
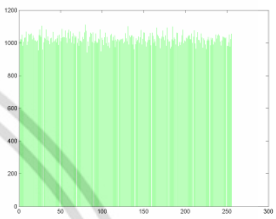
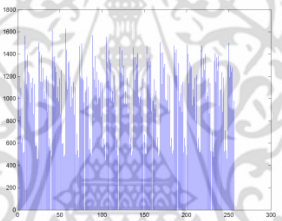
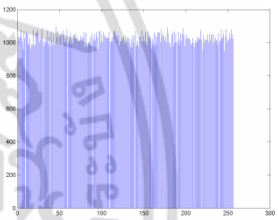
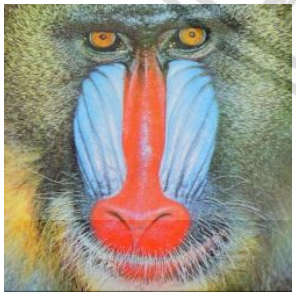
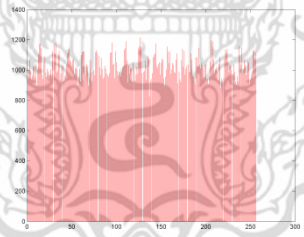
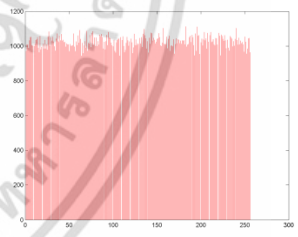
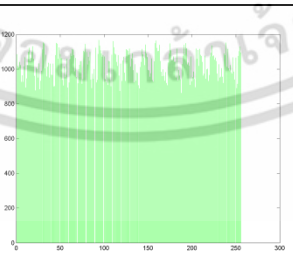
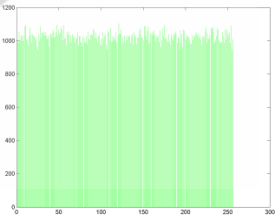
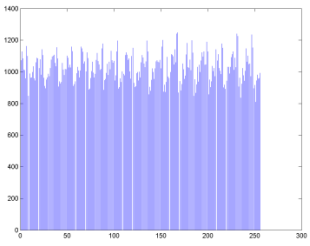
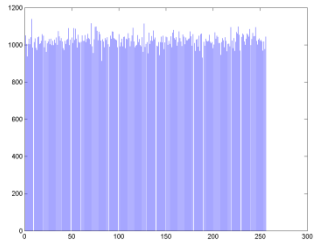
ตารางที่ 4.5 (ต่อ) ฮิสโตแกรมของตัวอย่างภาพสีที่เข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88)

ภาพต้นฉบับ	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
	ฮิสโตแกรม(ภาพสี)	ฮิสโตแกรม(ภาพสี)
		
		
		
		
		
		

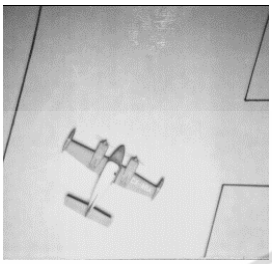
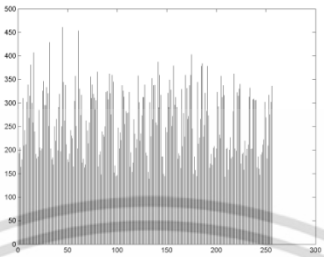
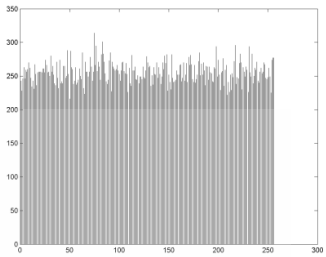
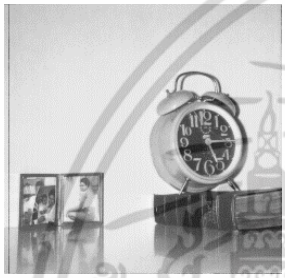
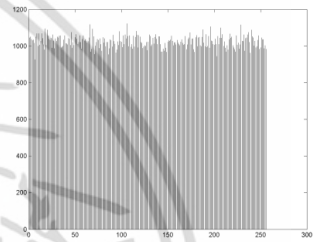
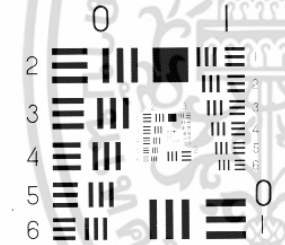
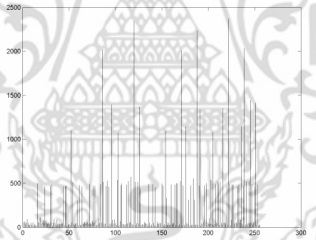
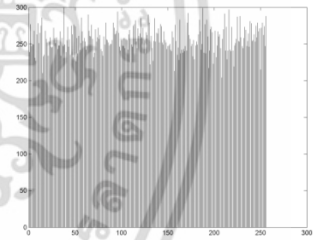
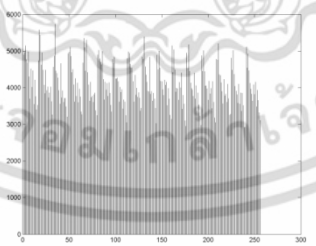
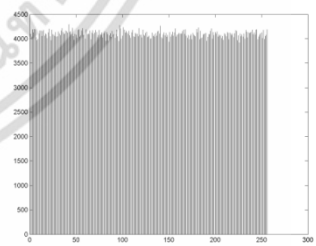
ตารางที่ 4.5 (ต่อ) ฮิสโตแกรมของตัวอย่างภาพสีที่เข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88)

ภาพต้นฉบับ	วิธีการเข้ารหัสแบบเดิม ฮิสโตแกรม(ภาพสี)	วิธีการเข้ารหัสแบบใหม่ ฮิสโตแกรม(ภาพสี)
		
		
		
		
		
		

ตารางที่ 4.5 (ต่อ) ฮิสโตแกรมของตัวอย่างภาพสีที่เข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88)

ภาพต้นฉบับ	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
	ฮิสโตแกรม(ภาพสี)	ฮิสโตแกรม(ภาพสี)
		
		
		
		
		
		

ตารางที่ 4.6 ฮิสโตแกรมของตัวอย่างภาพสีเทาและภาพขาวดำที่เข้ารหัสทั้งสองวิธีด้วยคีย์ (84,73,88)

ภาพต้นฉบับ	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
	ฮิสโตแกรม	ฮิสโตแกรม
		
		
		
		

4.3.3 คุณสมบัติการแพร่ของการเข้ารหัส (Diffusion)

คุณสมบัติการแพร่เป็นคุณสมบัติที่สำคัญอีกคุณสมบัติหนึ่งของการเข้ารหัสรูปภาพ ซึ่งเป็นคุณสมบัติที่ใช้ในการซ่อนความสัมพันธ์ระหว่างภาพต้นฉบับและภาพที่เข้ารหัส

สำหรับในการทดสอบคุณสมบัติการแพร่มีวิธีการคือนำภาพต้นฉบับและภาพต้นฉบับที่มีการเปลี่ยนแปลงเพียงเล็กน้อย (1 พิกเซล) ไปเข้ารหัสด้วยคีย์เดียวกัน จากนั้นหาความแตกต่างของภาพที่ผ่านการเข้ารหัสแล้วของทั้งสองภาพ เนื่องจากงานวิจัยเดิมนั้นไม่ได้ทดสอบคุณสมบัติการแพร่ของการเข้ารหัสรูปภาพจึงไม่มีการแสดงผลการทดสอบของงานวิจัยเดิม แต่จะแสดงผลการเปรียบเทียบระหว่างวิธีการของงานวิจัยนี้การปรับปรุงครั้งที่ 1 [31] ซึ่งจะมีการ Pre-process ค่าพิกเซลเฉพาะที่อยู่ในแถวเดียวกันเท่านั้นกับการปรับปรุงครั้งล่าสุดซึ่งมีการ Pre-process ค่าพิกเซลในแต่ละแถวและระหว่างแถวด้วย

ตารางที่ 4.7 อัตราเปอร์เซ็นต์ของจำนวนพิกเซลที่แตกต่างกันระหว่างภาพต้นฉบับและภาพที่ผ่านการเข้ารหัสแล้วของวิธีการในการปรับปรุงครั้งที่ 1 และวิธีการในการปรับปรุงครั้งที่ 2 ด้วยคีย์ (183,5,80)

ชื่อภาพ	ขนาดภาพ	NPCR ของวิธีการเข้ารหัสในการปรับปรุงครั้งที่ 1	NPCR ของวิธีการเข้ารหัสในการปรับปรุงครั้งที่ 2
Emma	256×256	0.001526 %	99.998474 %
Couple	256×256	0.001526 %	99.998474 %
Kate	256×256	0.001526 %	99.998474 %
Nadear	256×256	0.001526 %	99.998474 %
House	256×256	0.001526 %	99.998474 %
Tree	256×256	0.001526 %	99.998474 %
Jelly beans 1	256×256	0.001526 %	99.998474 %
Jelly beans 2	256×256	0.001526 %	99.998474 %
Splash	512×512	0.000381 %	99.999619 %
Tiffany	512×512	0.000381 %	99.999619 %
Baboon	512×512	0.000381 %	99.999619 %
Lena	512×512	0.000381 %	99.999619 %
F-16	512×512	0.000381 %	99.999619 %
Lake	512×512	0.000381 %	99.999619 %
Pepper	512×512	0.000381 %	99.999619 %

ตารางที่ 4.8 อัตราค่าเฉลี่ย (%) ของความแตกต่างระหว่างภาพต้นฉบับและภาพที่ผ่านการเข้ารหัสของวิธีการในการปรับปรุงครั้งที่ 1 และวิธีการในการปรับปรุงครั้งที่ 2 ด้วยคีย์ (183,5,80)

ชื่อภาพ	ขนาดภาพ	UACI ของวิธีการเข้ารหัสในการปรับปรุงครั้งที่ 1	UACI ของวิธีการเข้ารหัสในการปรับปรุงครั้งที่ 2
Emma	256×256	0.19 %	39.71 %
Couple	256×256	0.06 %	31.90 %
Kate	256×256	0.09 %	29.90 %
Nadear	256×256	0.08 %	38.64 %
House	256×256	0.11 %	35.52 %
Tree	256×256	0.20 %	29.95 %
Jelly beans 1	256×256	0.11 %	33.45 %
Jelly beans 2	256×256	0.08 %	27.14 %
Splash	512×512	0.10 %	39.73 %
Tiffany	512×512	0.05 %	34.55 %
Baboon	512×512	0.07 %	35.12 %
Lena	512×512	0.08 %	36.92 %
F-16	512×512	0.08 %	32.36 %
Lake	512×512	0.10 %	35.99 %
Pepper	512×512	0.20 %	38.19 %

วิธีการเข้ารหัสรูปภาพที่มีคุณสมบัติการแพร่ที่ดีคือวิธีการที่เมื่อมีการเปลี่ยนแปลงข้อมูลต้นฉบับเพียงเล็กน้อยข้อมูลที่ผ่านการเข้ารหัสแล้วนั้นต้องเปลี่ยนไปทั้งหมดเพื่อให้ยากต่อการคาดเดา ดังนั้นค่า NPCR ต้องมีค่ามากกว่า 99% หรือเข้าใกล้ 100% มากที่สุด [26,27] และค่า UACI ต้องมีค่าใกล้เคียงหรือเท่ากับ 33% [28,29]

ตารางที่ 4.7 และ 4.8 แสดงให้เห็นว่าการเข้ารหัสด้วยวิธีการที่ได้ปรับปรุงครั้งที่ 2 มีค่าอัตราร้อยละของจำนวนของค่าพิกเซลที่แตกต่าง (NPCR) และค่าเฉลี่ยของความแตกต่างระหว่างสองภาพ (UACI) ที่ดีกว่าวิธีการเข้ารหัสแบบเดิมอย่างมาก เนื่องจากในการเข้ารหัสด้วยวิธีการปรับปรุงครั้งที่ 1 นั้นการเปลี่ยนแปลงของพิกเซลใดพิกเซลหนึ่งในแถวจะกระทบเฉพาะกับพิกเซลที่อยู่แถวเดียวกันเท่านั้นทำให้ NPCR และ UACI มีค่าน้อยมากเนื่องจากการเปลี่ยนแปลงในแถวไม่มีผลกระทบกับพิกเซลในแถวอื่น ดังนั้นการที่มีการเชื่อมโยงค่าระหว่างแถวในการปรับปรุงครั้งที่ 2 ทำให้ค่า NPCR และ UACI เพิ่มขึ้นอย่างมากและเข้าใกล้กับค่ามาตรฐาน

4.3.4 การทดสอบความสัมพันธ์ระหว่างพิกเซล (Correlation Coefficient)

การทดสอบความสัมพันธ์ระหว่างพิกเซล (Correlation Coefficient) เป็นการวิเคราะห์ความสัมพันธ์ระหว่าง 2 พิกเซลใดๆที่อยู่ติดกันในภาพทั้งแนวตั้ง แนวนอน และแนวเฉียง ซึ่งวิธีการเข้ารหัสรูปภาพที่ดีควรมีการซ่อนความสัมพันธ์ทั้งหมดของรูปภาพและค่าความสัมพันธ์ระหว่างพิกเซล (Correlation Coefficient) ของการเข้ารหัสรูปภาพที่ดีควรมีค่าเข้าใกล้ 0

ตารางที่ 4.9 แสดงค่าความสัมพันธ์ระหว่างพิกเซลข้างเคียงของภาพตัวอย่างที่เข้ารหัสด้วยวิธีการเดิมเปรียบเทียบกับภาพที่เข้ารหัสด้วยวิธีการใหม่ทั้งในแนวตั้ง แนวนอน และแนวเฉียง โดยใช้คีย์ (84,232,321) ในการเข้ารหัสทั้งสองวิธี

ตารางที่ 4.9 ค่าความสัมพันธ์ระหว่างพิกเซลข้างเคียงของภาพที่ผ่านการเข้ารหัสด้วยวิธีการเดิมและวิธีการใหม่ ทั้งในแนวตั้ง แนวนอน และแนวเฉียง

ชื่อภาพ	ค่าความสัมพันธ์ระหว่างพิกเซล (Correlation Coefficient)					
	แนวตั้ง		แนวนอน		แนวเฉียง	
	วิธีการเดิม	วิธีการใหม่	วิธีการเดิม	วิธีการใหม่	วิธีการเดิม	วิธีการใหม่
Couple	0.0188	0.0136	0.0131	0.0004	0.0124	0.0022
Kate	0.0316	0.0018	0.0247	0.0020	0.0339	-0.0027
Nadear	0.0200	0.0010	0.0199	0.0041	0.0153	0.0009
Jelly beans 1	0.0450	-0.0107	0.0495	-0.0034	0.0450	0.0017
Jelly beans 2	0.0381	-0.0094	0.0414	0.0059	0.0401	0.0032
Splash	0.0216	-0.0060	0.0236	-0.0039	0.0191	0.0015
Tiffany	0.0433	-0.0211	0.0430	-0.0016	0.0423	-0.0011
F-16	0.0122	-0.0091	0.0137	-0.0001	0.0085	-0.0004
Peppers	0.0053	-0.0027	-0.0018	0.0008	0.0063	-0.0030
Airplane 1	0.0245	-0.0173	0.0290	-0.0073	0.0259	0.0067
Clock	0.0078	-0.0017	0.0166	0.0008	0.0032	0.0043
Airplane 2	0.0224	-0.0126	0.0241	-0.0001	0.0215	0.0004
Truck	0.0092	0.0020	0.0056	-0.0011	0.0061	0.0008
U-2	0.0029	0.0035	0.0010	-0.0002	0.0015	0.0007
Boat	0.0113	-0.0031	0.0039	-0.0017	0.0031	0.0009
Gray Level	0.0569	-0.0073	0.0588	-0.0001	0.0566	-0.00218

ตารางที่ 4.10 ร้อยละค่าเฉลี่ยความสัมพันธ์ระหว่างพิกเซลข้างเคียงในแนวตั้ง แนวนอน และแนวเฉียง

ชื่อภาพ	ร้อยละค่าเฉลี่ยความสัมพันธ์ระหว่างพิกเซลข้างเคียง					
	วิธีการเดิม		วิธีการใหม่		ความแตกต่าง	
	ค่าเฉลี่ยทั้งสามแนว	คิดเป็นร้อยละ	ค่าเฉลี่ยทั้งสามแนว	คิดเป็นร้อยละ	ค่าความแตกต่าง	คิดเป็นร้อยละ
Couple	0.0148	1.48	0.0055	0.55	0.0093	0.93
Kate	0.0301	3.01	0.0004	0.04	0.0297	2.97
Nadear	0.0185	1.85	0.0021	0.21	0.0164	1.64
Jelly beans 1	0.0465	4.65	0.0042	0.42	0.0423	4.23
Jelly beans 2	0.0399	3.99	0.0061	0.61	0.0338	3.38
Splash	0.0215	2.15	0.0028	0.28	0.0187	1.87
Tiffany	0.0429	4.29	0.0080	0.8	0.0349	3.49
F-16	0.0115	1.15	0.0032	0.32	0.0083	0.83
Peppers	0.0044	0.44	0.0008	0.08	0.0036	0.36
Airplane 1	0.0264	2.64	0.0059	0.59	0.0205	2.05
Clock	0.0092	0.92	0.0011	0.11	0.0081	0.81
Airplane 2	0.0226	2.26	0.0041	0.41	0.0185	1.85
Truck	0.0069	0.69	0.0005	0.05	0.0064	0.64
U-2	0.0014	0.14	0.0013	0.13	0.0001	0.01
Boat	0.0061	0.61	0.0013	0.13	0.0048	0.48
Gray Level	0.0575	5.75	0.0032	0.32	0.0543	5.43

จากตารางที่ 4.9 พบว่าภาพที่เข้ารหัสด้วยวิธีการใหม่มีค่าความสัมพันธ์ระหว่างพิกเซลข้างเคียงเข้าใกล้ 0 มากกว่าภาพที่เข้ารหัสด้วยวิธีการเดิมทั้งในแนวนอน แนวตั้ง และแนวเฉียง เมื่อนำค่าสัมบูรณ์ของความสัมพันธ์ระหว่างพิกเซลทั้งสามแนวมาหาค่าเฉลี่ยและคิดเป็นร้อยละโดยถ้าพิกเซลที่อยู่ติดกันมีความสัมพันธ์กันมาก (ค่าความสัมพันธ์เข้าใกล้ 1 หรือ -1) คิดเป็นร้อยละ 100 จะได้ผลลัพธ์ดังในตารางที่ 4.10 ในการคำนวณค่าเฉลี่ยความสัมพันธ์และร้อยละค่าเฉลี่ยความสัมพันธ์มีสมการดังนี้

$$\text{ค่าเฉลี่ยความสัมพันธ์} = \frac{|CC_H|+|CC_V|+|CC_D|}{3} \quad (4.1)$$

$$\text{ร้อยละค่าเฉลี่ยความสัมพันธ์} = \frac{|CC_H|+|CC_V|+|CC_D|}{3} \times 100 \quad (4.2)$$

เมื่อ $CC_H\ CC_v$ และ CC_D คือ ค่าความสัมพันธ์ระหว่างพิกเซลในแนวตั้ง แนวนอน และแนวเฉียง

ร้อยละค่าเฉลี่ยของภาพที่เข้ารหัสด้วยวิธีการใหม่จะมีค่าไม่ถึงร้อยละ 1 ในขณะที่วิธีการเดิมมีค่าเฉลี่ยอยู่ที่ร้อยละ 2.25 ซึ่งต่างกันอย่างมีนัยสำคัญ เช่น ในกรณีที่ต้องการผลที่ต้องการการซ่อนความสัมพันธ์มาก นั่นหมายความว่าการเข้ารหัสแบบใหม่สามารถซ่อนความสัมพันธ์ของภาพที่ผ่านการเข้ารหัสได้ดีกว่างานวิจัยเดิมจึงทำให้ไม่มีข้อมูลที่สามารถใช้ในการคาดเดารูปภาพต้นฉบับหรือคีย์ได้

4.3.5 การวัดประสิทธิภาพการเข้ารหัส

การวัดประสิทธิภาพวิธีการถอดรหัสที่เป็นนิยมคือการใช้ Peak Signal-to-Noise Ratio (PSNR) โดยค่า PSNR จะแสดงให้เห็นถึงความสัมพันธ์ระหว่างภาพที่ผ่านการเข้ารหัสและภาพที่ได้หลังจากการถอดรหัสซึ่งต้องมีค่ามากกว่า 30 เดซิเบล (dB) จึงถือว่าเป็นการถอดรหัสที่ยอมรับได้ แต่สำหรับการวัดประสิทธิภาพการเข้ารหัสนั้นค่า PSNR ที่ได้ต้องมีค่าน้อยกว่า 10 dB [13]

ตารางที่ 4.11 ค่าประสิทธิภาพของการเข้ารหัสทั้งสองวิธีด้วยคีย์ (213,78,11)

ชื่อภาพ	ค่าประสิทธิภาพการเข้ารหัส (PSNR) , (dB)	
	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
Emna	7.52	7.33
Couple	6.62	6.27
Tree	8.35	8.20
Jelly beans 1	8.73	8.63
Jelly beans 2	8.71	8.66
Tiffany	7.77	7.11
Pepper	8.34	8.11
Resolution chart	6.90	4.97
Aerial 2	9.35	9.24
Man	8.32	8.03
Airplane	6.53	6.35
Gray level	7.89	7.61
Lena number	8.45	8.24
Ruler	6.95	4.80

จากผลการทดลองในตาราง 4.11 แสดงให้เห็นว่าการเข้ารหัสด้วยวิธีการเข้ารหัสแบบเดิมของวนิดาและวิธีการเข้ารหัสแบบใหม่ในงานวิจัยนี้มีค่า PSNR น้อยกว่า 10 dB ในทุกภาพตัวอย่าง แต่ค่า PSNR ที่เป็นผลลัพธ์ของวิธีการใหม่ลดลงจากการเข้ารหัสด้วยวิธีการเดิม ดังนั้นสามารถสรุปได้ว่าทั้งสองวิธีมีคุณสมบัติในการเข้ารหัสรูปภาพแต่การเข้ารหัสด้วยวิธีการใหม่มีประสิทธิภาพดีกว่าการเข้ารหัสด้วยวิธีการเดิม

4.3.6 การวิเคราะห์จำนวนคีย์ทั้งหมดที่เป็นไปได้ (Key space)

เนื่องจากงานวิจัยนี้ได้ใช้คีย์ในรูปแบบเดียวกับงานวิจัยเดิม [4] ซึ่งคีย์ที่ใช้ในงานวิจัยประกอบด้วย 3 ส่วนดังนี้

rule คือ กฎทั้งหมดของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

seedstate คือ ค่าเริ่มต้นในการสร้างเลขสุ่มเทียมสำหรับหาสถานะเริ่มต้นในแต่ละพิกเซล

seedtime คือ ค่าเริ่มต้นในการสร้างเลขสุ่มเทียมสำหรับหาจำนวนสถานะที่ใช้ในการเข้ารหัสในแต่ละพิกเซล

จำนวนกฎที่สามารถสร้างเป็นแอทแทรคเตอร์ได้มีทั้งหมด 128 กฎ (กฎที่สามารถนำไปใช้ในการเข้ารหัสได้ สามารถดูได้จากภาคผนวก ข.) สำหรับในการหาค่าสถานะเริ่มต้นและจำนวนสถานะในการเข้ารหัสมีการใช้ตัวสร้างสุ่มเทียมเดียวกันซึ่งตัวสร้างเลขสุ่มเทียมนั้นมีชื่อว่า ISAAC : (Indirection, Shift, Accumulate, Add, and Count)[24] เป็นตัวสร้างสุ่มเทียมที่มีความปลอดภัยสูงและสามารถกำหนดค่าเริ่มต้นในการสร้างเลขสุ่มเทียมได้สูงสุดถึง 2^{8192}-1 หรือประมาณ 10^{2466} ดังนั้นจำนวนคีย์ทั้งหมดที่เป็นไปได้ของงานวิจัยนี้คือ $128 \times 2^{8192} \times 2^{8192}$ ซึ่งถือว่ามีขนาดใหญ่เพียงพอสำหรับป้องกันการโจมตีแบบ Brute-force

4.3.7 ระยะเวลาที่ใช้ในการเข้ารหัส (Speed performance)

จากการทดลองวัดระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัสของรูปภาพทั้งหมดด้วยคีย์ (102,35,12) ทั้งการเข้ารหัสด้วยวิธีการเดิมและวิธีการใหม่สามารถสรุปได้ตามตารางที่ 4.12

ตารางที่ 4.12 ระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัสของแต่ละรูปภาพมีหน่วยเป็นวินาที

ชื่อภาพ	เข้ารหัสด้วยวิธีการเดิม		เข้ารหัสด้วยวิธีการใหม่	
	เข้ารหัส	ถอดรหัส	เข้ารหัส	ถอดรหัส
Emma	16.96	18.45	13.74	16.90
Couple	14.48	18.03	16.37	14.95
Kate	16.26	19.01	16.33	14.28
Nadear	13.53	15.97	16.30	12.39
House	14.27	15.38	16.84	15.50
Jelly beans 2	15.99	18.42	17.31	16.11
Splash	50.40	49.07	67.37	53.96
Tiffany	58.74	61.82	61.24	59.48
Baboon	55.49	64.73	59.57	58.18
Lena	54.28	66.14	65.82	56.03
F-16	57.85	64.60	65.98	60.43
Lake	60.70	54.85	66.32	54.80
Moon surface	4.85	4.73	5.07	4.89
Aerial 1	5.76	6.09	5.12	4.97
Clock	6.78	6.26	5.66	7.01
Resolution chart	6.09	6.51	5.08	4.80
Boat	21.82	20.75	23.70	22.45
Elaine	21.79	21.70	23.27	20.68
Gray level	18.12	19.94	22.45	19.01
Blue car	59.38	61.19	60.52	53.62

จากข้อมูลในตารางที่ 4.12 เวลาที่ใช้ในการเข้ารหัสของวิธีการเดิมเปรียบเทียบวิธีการใหม่ไม่แตกต่างกันมาก เมื่อนำมาแบ่งกลุ่มตามประเภทสีและขนาดของภาพพบว่าระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัสจะมีความแตกต่างกัน โดยภาพขาวดำและภาพสีเทาใช้เวลาน้อยกว่าภาพสี เนื่องจากภาพสีต้องทำการเข้ารหัสหรือถอดรหัสถึง 3 รอบในแต่ละพิกเซล ขณะที่ภาพสีเทาและภาพขาวดำเข้ารหัสหรือถอดรหัสในแต่ละพิกเซลเพียงรอบเดียว ตารางที่ 4.13 แสดงระยะเวลาเฉลี่ยในการเข้ารหัสภาพแต่ละประเภท

ตารางที่ 4.13 ระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสของแต่ละรูปภาพมีหน่วยเป็นวินาที

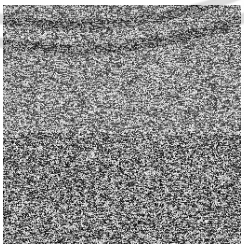
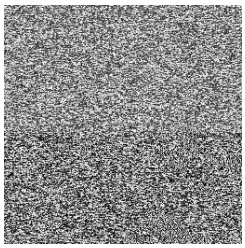
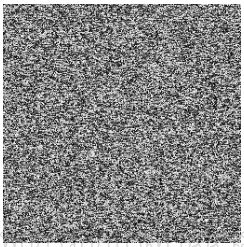
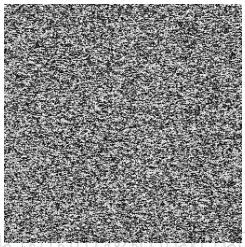
ประเภทสี	ขนาด	เข้ารหัสด้วยวิธีการเดิม		เข้ารหัสด้วยวิธีการใหม่	
		เข้ารหัส	ถอดรหัส	เข้ารหัส	ถอดรหัส
ภาพสีเทา	256×256	5.575	5.50	5.85	5.54
ภาพสีเทา	512×512	21.09	20.78	22.22	21.14
ภาพสีเทา	1024×1024	80.48	83.67	90.53	85.29
ภาพสี	256×256	15.05	17.06	16.46	17.59
ภาพสี	512×512	55.20	59.26	61.11	63.23

4.3.8 การทดสอบเข้ารหัสภาพขาวดำ

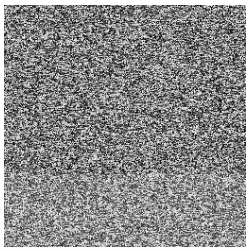
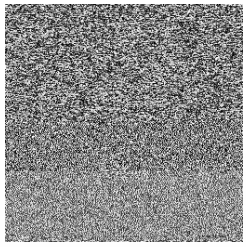
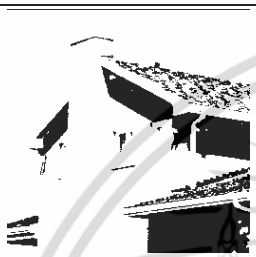
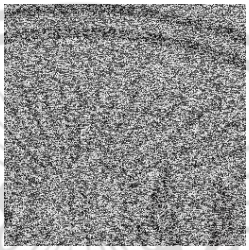
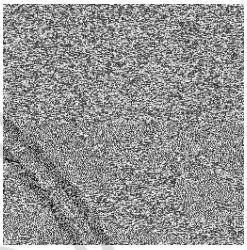
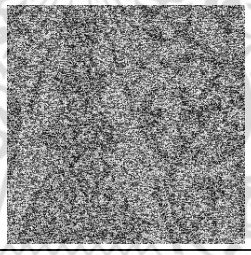
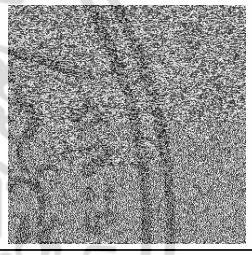
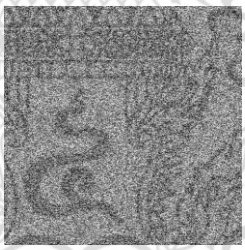
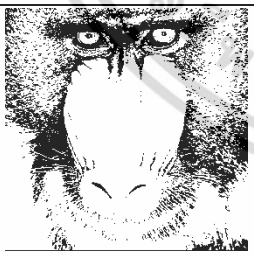
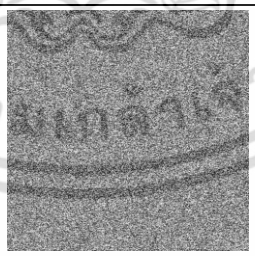
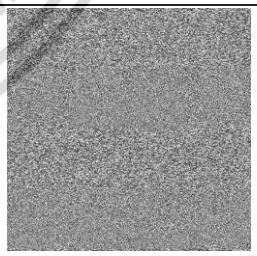
การเข้ารหัสด้วยวิธีการเดิมไม่สามารถเข้ารหัสภาพขาวดำในวิธีการใหม่จึงปรับปรุงให้สามารถเข้ารหัสรูปภาพขาวดำได้โดยมีการเพิ่มวิธีการในการเตรียมภาพขาวดำเพื่อให้สามารถนำมาเข้ารหัสรูปภาพได้โดยทำการเปลี่ยนภาพขาวดำเป็นภาพสีเทา วิธีการทั่วไปในการเปลี่ยนภาพขาวดำเป็นภาพสีเทาเมื่อนำภาพสีเทาไปเข้ารหัสจะให้ผลที่ไม่ดี งานวิจัยนี้จึงนำวิธีการของ Sreelaja มาใช้โดยทำการปรับปรุงจากเดิมมี 26 ความเข้มแสง เป็น 255 ความเข้มแสง ทำให้ภาพต้นฉบับมีความซ้ำซ้อนกันเพิ่มมากขึ้นและให้ผลที่ดีในทุกภาพ

ในการทดสอบการ เข้ารหัสภาพขาวดำโดยใช้พารามิเตอร์ในการวัดประสิทธิภาพเช่นเดียวกับการเข้ารหัสภาพสีหรือภาพสีเทา โดยมีการเปรียบเทียบระหว่างการเข้ารหัสภาพขาวดำที่มีการเปลี่ยนภาพขาวดำเป็นภาพสีเทาด้วยวิธีของ Sreelaja [17] และการเปลี่ยนภาพขาวดำเป็นภาพสีเทาด้วยวิธีที่ทำการปรับปรุงในงานวิจัยนี้

ตารางที่ 4.14 ตัวอย่างรูปภาพขาวดำที่ผ่านการเข้ารหัสด้วยวิธีการใหม่

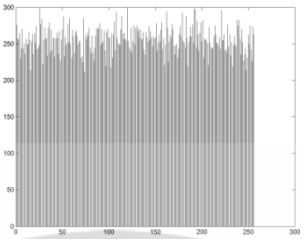
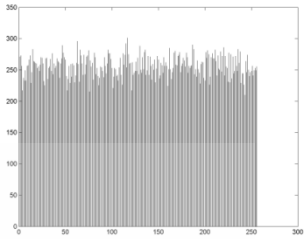
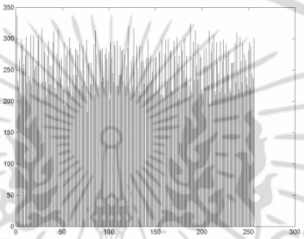
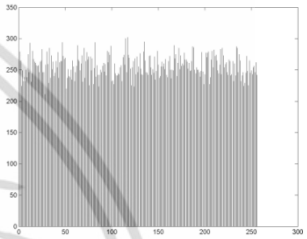
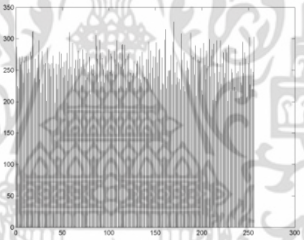
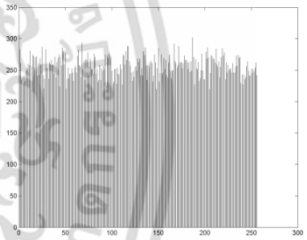
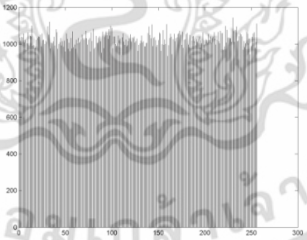
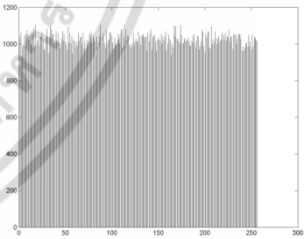
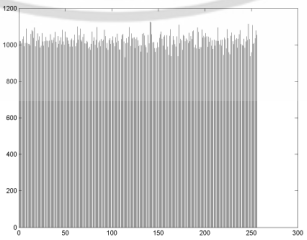
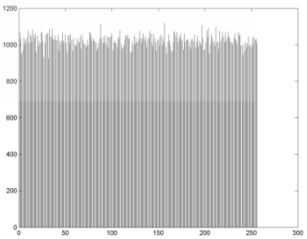
ภาพต้นฉบับ	วิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทา	
	วิธีของ Sreelaja	วิธีของงานวิจัยนี้
		
		

ตารางที่ 4.14 (ต่อ) ตัวอย่างรูปภาพขาวดำที่ผ่านการเข้ารหัสด้วยวิธีการใหม่

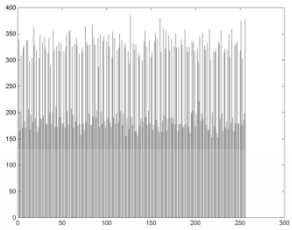
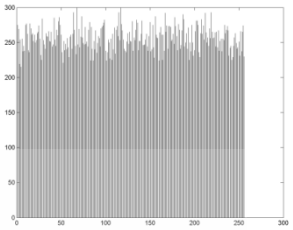
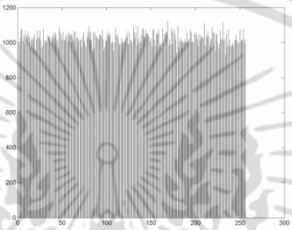
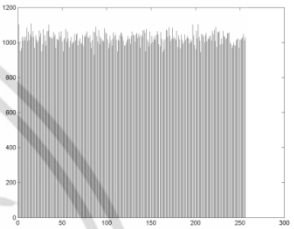
ภาพต้นฉบับ	วิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทา	
	วิธีของ Sreelaja	วิธีของงานวิจัยนี้
		
		
		
		
		

ในการทดสอบการเข้ารหัสรูปภาพขาวดำโดยใช้วิธีการของ Sreelaja และ วิธีการของงานวิจัยนี้ในการเปลี่ยนจากภาพขาวดำเป็นภาพสีเทาพบว่าภาพที่ผ่านการเข้ารหัสจากภาพสีเทาของทั้งสองวิธีสามารถปกปิดเค้าโครงของรูปภาพต้นฉบับได้ทั้งหมดดังผลในตารางที่ 4.14

ตารางที่ 4.15 ฮิสโตแกรมของรูปภาพขาวดำที่ผ่านการเข้ารหัสด้วยวิธีการใหม่

ภาพต้นฉบับ	วิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทา	
	วิธีของ Sreelaja	วิธีของงานวิจัยนี้
		
		
		
		
		

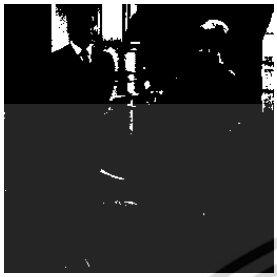
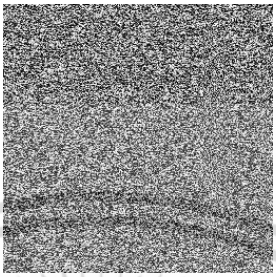
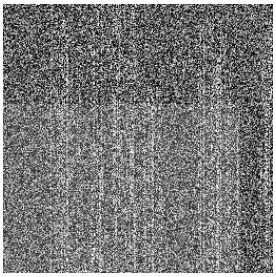
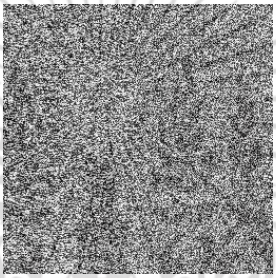
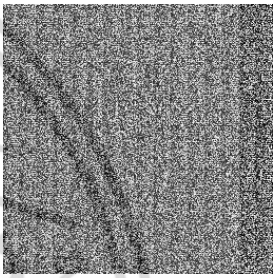
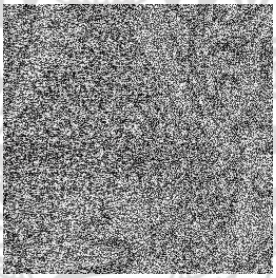
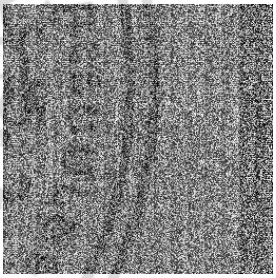
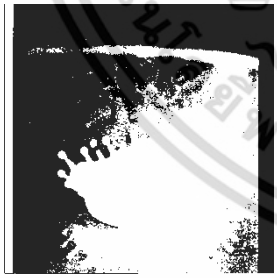
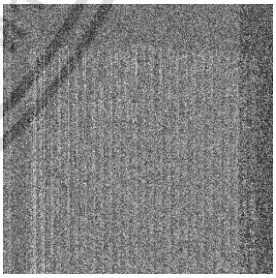
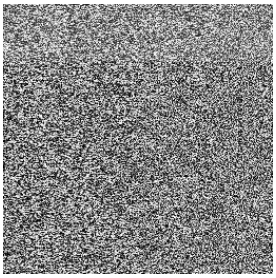
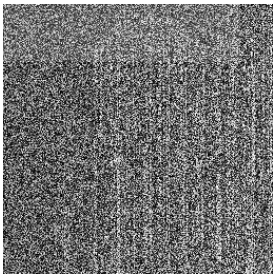
ตารางที่ 4.15 (ต่อ) ฮิสโตแกรมของรูปภาพขาวดำที่ผ่านการเข้ารหัสด้วยวิธีการใหม่

ภาพต้นฉบับ	วิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทา	
	วิธีของ Sreelaja	วิธีของงานวิจัยนี้
		
		

จากตารางที่ 4.15 ฮิสโตแกรมของภาพขาวดำที่เข้ารหัสโดยใช้วิธีของงานวิจัยนี้ในการเปลี่ยนภาพสีขาวดำเป็นภาพสีเทามีความสม่ำเสมอมากกว่าการใช้วิธีของ Sreelaja เนื่องจากวิธีการในงานวิจัยนี้ได้เพิ่มจำนวนค่าของพิกเซลที่เป็นไปได้เมื่อเปลี่ยนเป็นภาพสีเทาซึ่งมีจำนวนทั้งหมด 255 ค่า แต่ค่าพิกเซลที่เป็นไปได้ของ Sreelaja มีจำนวน 24 ค่า ดังนั้นเมื่อนำภาพสีเทาที่ได้จากวิธีของ Sreelaja ไปเข้ารหัสจึงเกิดความซ้ำซ้อนสูงและทำให้ฮิสโตแกรมไม่สม่ำเสมอ

เมื่อนำวิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทาที่ได้ทำการปรับปรุงมาใช้ในการเข้ารหัสรูปภาพด้วยวิธีการของวนิดา พบว่าภาพที่ผ่านการเข้ารหัสยังคงสามารถมองเห็นเค้าโครงของภาพเดิมได้เมื่อเทียบกับการเข้ารหัสด้วยวิธีใหม่ ดังตารางที่ 4.16 จึงสามารถสรุปได้ว่าการเข้ารหัสด้วยวิธีการเดิมไม่สามารถทำลายความสัมพันธ์ระหว่างพิกเซลจึงทำให้สามารถมองเห็นเค้าโครงของภาพต้นฉบับ

ตารางที่ 4.16 ตัวอย่างรูปภาพขาวดำที่ผ่านการเข้ารหัสด้วยวิธีการใหม่และวิธีการของวนิดาที่ใช้วิธีการเปลี่ยนภาพขาวดำของงานวิจัยนี้

ภาพต้นฉบับ	วิธีการเข้ารหัสภาพขาวดำที่ใช้วิธีการเปลี่ยนภาพขาวดำของงานวิจัยนี้	
	วิธีของงานวิจัยนี้	วิธีของวนิดา
		
		
		
		
		

ตารางที่ 4.17 ร้อยละค่าเฉลี่ยความสัมพันธ์ระหว่างพิกเซลข้างเคียง

ชื่อภาพ	วิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทา	
	วิธีของ Sreelaja (%)	วิธีของงานวิจัยนี้ (%)
Emma_bw	58.9	7.3
Couple_bw	59.4	35.6
Kate_bw	58.2	27.4
Nadear_bw	59.2	37.8
House_bw	59.1	9.5
Splash_bw	61.0	10.9
Baboon_bw	60.1	45.5
Lena_bw	60.5	15.6
Peppers_bw	60.3	42.5

ตารางที่ 4.17 แสดงร้อยละค่าเฉลี่ยความสัมพันธ์ระหว่างพิกเซลข้างเคียงของภาพขาวดำที่เข้ารหัสโดยใช้วิธีการในการเปลี่ยนภาพสีขาวดำเป็นภาพสีเทาของ Sreelaja และวิธีของงานวิจัยนี้ ซึ่งวิธีการที่ใช้ในงานวิจัยนี้ให้ค่าความสัมพันธ์ที่ลดลงอย่างมากซึ่งสรุปได้ว่าวิธีการเปลี่ยนภาพสีดำเป็นภาพสีเทาในงานวิจัยนี้มีความสามารถในการซ่อนข้อมูลที่จะนำไปใช้ในการคาดเดาภาพต้นฉบับหรือคีย์ได้ดีกว่าวิธีการของ Sreelaja ค่อนข้างมาก

ตารางที่ 4.18 ระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัสมีหน่วยเป็นวินาที

ชื่อภาพ	วิธีการเปลี่ยนภาพขาวดำเป็นภาพสีเทา			
	วิธีของ Sreelaja		วิธีของงานวิจัยนี้	
	เข้ารหัส	ถอดรหัส	เข้ารหัส	ถอดรหัส
Emma_bw	5.99	4.95	5.17	4.97
Couple_bw	5.12	4.89	5.2	4.91
Kate_bw	5.14	5.08	5.23	4.86
Splash_bw	18.26	16.9	18.28	18.35
Baboon_bw	18.62	18.21	21.25	17.61
Lena_bw	18.37	16.91	18.22	16.81
Pepper_bw	18.39	17.4	18.95	16.91

ตารางที่ 4.18 แสดงเวลาที่ใช้ในการเข้ารหัสและถอดรหัสของวิธีการของ Sreelaja และวิธีการในงานวิจัยนี้มีความใกล้เคียงกันทั้งสองวิธี

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลการวิจัย

งานวิจัยนี้ได้นำวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานของวนิดา [4] มาปรับปรุงโดยเพิ่มขั้นตอนการทำ Pre-process ด้วยการนำค่าของพิกเซลก่อนหน้ามาเป็นข้อมูลร่วมในการเข้ารหัสเพื่อลดความซ้ำซ้อนของพิกเซลในภาพที่ผ่านการเข้ารหัสแล้ว และมีการเพิ่มขั้นตอนการเปลี่ยนภาพขาวดำเป็นภาพสีเทาเพื่อให้สามารถเข้ารหัสภาพขาวดำซึ่งในงานวิจัยวนิดา [4] ไม่สามารถทำได้

ผลการทดลองแสดงให้เห็นว่าในการเข้ารหัสด้วยวิธีใหม่ภาพที่ผ่านการเข้ารหัสสามารถปกปิดเค้าโครงของภาพต้นฉบับได้ทุกประเภทและทุกลักษณะของภาพ อีกทั้งมีกราฟฮิสโตแกรมที่มีการแจกแจงที่สม่ำเสมอและมีคุณสมบัติการแพร่ที่สามารถลดความสัมพันธ์ระหว่างภาพต้นฉบับและภาพที่เข้ารหัส ดังนั้นภาพที่ผ่านการเข้ารหัสจึงมีความปลอดภัยและทนทานต่อการโจมตีมากกว่าวิธีเดิมอย่างชัดเจน สามารถสรุปความแตกต่างของการเข้ารหัสด้วยวิธีการในงานวิจัยนี้กับวิธีการเดิมได้สองส่วนดังนี้

1. สิ่งที่ได้ปรับปรุงจากงานวิจัยเดิม
    - ลดความสัมพันธ์ระหว่างพิกเซลข้างเคียงของภาพที่ผ่านการเข้ารหัส
    - สามารถปกปิดเค้าโครงภาพต้นฉบับในการเข้ารหัสรูปภาพด้วยทุกคีย์
    - สามารถปกปิดเค้าโครงภาพต้นฉบับในการเข้ารหัสรูปภาพได้ทุกลักษณะภาพ (โทนสีเดียวกัน)
    - การแจกแจงพิกเซล (ฮิสโตแกรม) มีความสม่ำเสมอในการเข้ารหัสรูปภาพทุกลักษณะและทุกคีย์
    - สามารถป้องกันการโจมตีแบบ Differential Attack
2. สิ่งที่เพิ่มเติมจากงานวิจัยเดิม
    - การเข้ารหัสภาพขาวดำ

5.2 ข้อเสนอแนะ

1. เนื่องจากเวลาในการเข้ารหัสและถอดรหัสมีความล่าช้าหากภาพนั้นเป็นภาพที่มีขนาดใหญ่มาก จึงจำเป็นต้องเพิ่มประสิทธิภาพการเข้ารหัสและถอดรหัสให้มีความเร็วเพิ่มขึ้น
2. ในการเข้ารหัสภาพขาวดำบางภาพที่มีความซ้ำซ้อนของพิกเซลสูง เช่น ภาพที่มีพิกเซลสีขาวหรือพิกเซลสีดำเป็นจำนวนมาก เมื่อวิเคราะห์ฮิสโตแกรมของภาพขาวดำที่ผ่านการเข้ารหัสดังกล่าว กราฟฮิสโตแกรมมีค่าไม่สม่ำเสมอดังนั้นควรพัฒนาอัลกอริทึมในการเข้ารหัสภาพขาวดำให้มีประสิทธิภาพเพิ่มมากขึ้น

เอกสารอ้างอิง

[1] Chen R. J. and Lai J. L. "Image Security System using Recursive Cellular Automata Substitution" **Pattern Recognition-PR**. 2007, Vol. 40. No.5. pp. 1621-1631.

[2] R. Chen et al. "Image Encryption/Decryption System using 2d Cellular Automata" **ISCE'06.** 2006. pp. 1-6.

[3] Jun J. "Image Encryption Method Based on Elementary Cellular Automata" **SOUTHEASTCON**. 2009. Vol.9.

[4] วนิดา แก้วบูรณะประเสริฐ และนันทิกา เบญจเทพานันท์ "การปรับปรุงวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน", **8th Int. Joint Conf. on Computer Science and Software Engineering (JSCSSE)**. 2011.

[5] Anonymous. (ม.ป.ป.) "**ภาพดิจิทัล.**" สืบค้นเมื่อ 2 ม.ค. 2558. จาก http://th.wikipedia.org/wiki/%E0%B8%A0%E0%B8%B2%E0%B8%9E%E0%B8%94%E0%B8%B4%E0%B8%88%E0%B8%B4%E0%B8%97%E0%B8%B1%E0%B8%A5

[6] Allan G.(2006) "**The USC-SIPI Image Database:Version 5**" สืบค้นเมื่อ 1 ส.ค. 2557. จาก http://sipi.usc.edu/database/

[7] Petrou M. and Bosdogiani P. "Image Processing: The Fundamentals" **John Wiley & Sons Ltd**. 1999.

[8] Qidwai U. and Chen C.H. "Digital image processing: an algorithmic approach with MATLAB." **Taylor and Francis Group**. 2010.

[9] Behrouz A. Forouzan, "Cryptography and Network Security." **McGraw-Hill**. 2008.

[10] Stephen W. "Cellular automata and Complexity: collected paper" **Addison–Wesley Publishing**. 1994.

[11] Puhua G**.** "Cellular automaton public-key cryptosystem" **Complex Systems.** 1987, Vol. 1. pp.51-57.

[12] Habibipour M., Yaghobi M., Rahan– Q S. and Souzanchi-K Z. "An Image Encryption System by Indefinite Cellular Automata and Chaos" **2nd Int. Conf. on Signal Processing Systems (ICSPS)**, 2010, Vol. 3. pp. 23-27

[13] Habibipour M., Yaghobi M. and Rahan S. "An Image Encryption System by 2D Memorized Cellular Automata and Chaos Mapping" **6th Int. Conf. on Digital**

Content, Multimedia Technology and its Application (IDC), 2010. pp 331-336

[14] Xuelong Z., Qianmu L., Manwu X. and Fengyu L. "A Symmetric Cryptography Based on Extended Cellular Automata" **IEEE Int. Conf. on Systems. Man and Cybernetics.** 2005, Vol. 1. pp. 499-503.

[15] Chen R. J. and Lai J. L. "Novel Stream Cipher Using 2-D Hybrid CA and Variable Ordered Recursive CA Substitution" **IFIP Int. conf. on Network and Parallel Computing,** 2008. pp. 74 – 81.

[16] Chen R. J., Chen Y. H., Chen C. S. and Lai J. L. "Image Encryption/Decryption System Using 2D Cellular Automata" **IEEE Tenth Int. Symposium on Consumer Electronics**, 2006. pp. 1-6.

[17] Sreelaja N.K. and Vijayalakshmi Pai G.A. "Stream Cipher for Binary Image Encryption using Ant Colony Optimization based Key Generation" **Applied Soft Computing**, 2012, Vol.12. pp. 2879-2895.

[18] Ahmad J. and Ahmed F. "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" **IJVIPNS-IJENS**, 2012, Vol.12. pp. 18-31.

[19] Pareek N. K "Design and Analysis of a Novel Digital Image Encryption Scheme" **2nd Int. Journal of Network Security & Its Applications (IJNSA)**, March, 2012.

[20] Biham E. and Shamir A. "Differential Cryptanalysis of DES-like Cryptosystems", **10th Annual Int. Cryptology Conference on Advances Cryptology SpringerVerlag.** 1991.

[21] El-Fishawy N. and Zaid O. "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms," **Int. Journal of Network Security,** 2007, Vol. 5, No. 3, pp. 241–251.

[22] Kamali S., Shakerian R., Hedayati M., and Rahmani M., "A new modified version of advanced encryption standard based algorithm for image encryption," **IEEE Int. Conf. on Electronics and Information Engineering (ICEIE)**, 2010, Vol. 1, pp. V1–141

[23] Rinki P., Vijay Kumar T., and Vineet R., "A Survey On Different Image Encryption and Decryption Techniques," **(IJCSIT) Int. Journal of Computer Science and Information Technologies**, Vol. 4 (1), 2013, pp.113 – 116.

[24] Robert J. Jenkin Jr., **ISAAC : A fast cryptography random number generator.**

สืบค้นเมื่อ 20 ม.ค. 2557. จาก http://www.burtleburtle.net/bob/rand/isaacafa.html

[26] G. Chen, Y. Mao, and C. Chui, “A Symmetric Image Encryption Scheme Based on 3d Chaotic Cat Maps,” Chaos, Solitons & Fractals, vol. 12, 2004, pp. 749–761.

[27] Shima R. M., and Supriya M., **“**An Uncompressed Image Encryption Algorithm Based on DNA Sequences,” (**CCSEA) Int. Conference on Computer Science, Engineering and Applications**, 2011, pp. 258–270.

[28] Lini A., Neenu D., “Secure image encryption algorithms: A review”, **(IJCSIT) Int. Journal of Computer Science and Information Technologies**, Vol. 2 (4), 2013, pp.186 – 189

[29] Rhouma R. ,Soumaya M. and Safya B., OCML-based colour image encryption, **Chaos Solitons & Fractals**, 2007, pp. 309-318.

[30] Shiguo Lian, Multimedia Content Encryption: Techniquesand Applications. **Taylor & Francis Group**, LLC, 2009.

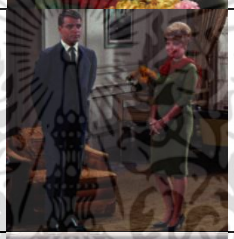
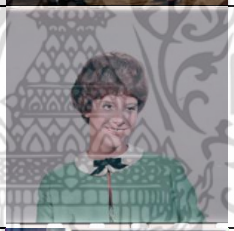
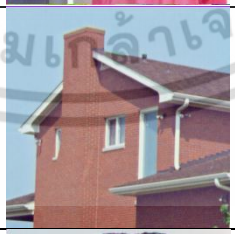
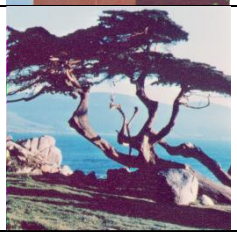
[31] มงคล ทองไกรแก้ว และรุ่ งรัตน์ เวียงศรีพนาวัลย์, “การปรับปรุงการใช้เซลลู ลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ,” **The Tenth National Conf. on Computing and Information Technology**, 2014, pp. 589-594.

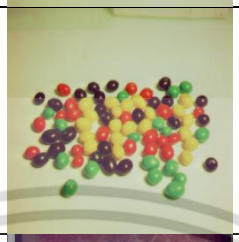
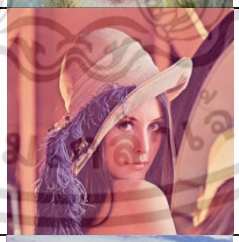
[32] มงคล ทองไกรแก้ว และรุ่ งรัตน์ เวียงศรีพนาวัลย์, “การวิเคราะห์และปรับปรุงประสิทธิภาพการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ,” **(ICSEC 2014) Int. Computer Science and Engineering Conf.**, 2014, pp. 133-138.

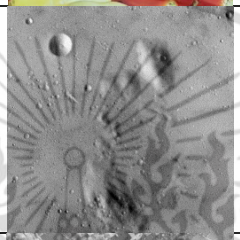
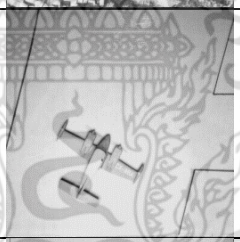
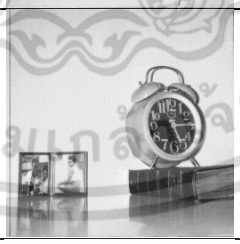
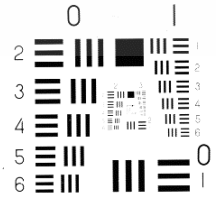
ภาคผนวก ก

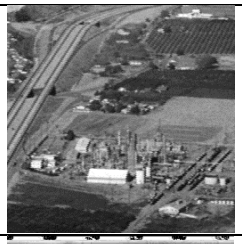
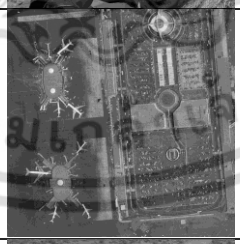
รูปภาพที่ใช้ในการทดลอง

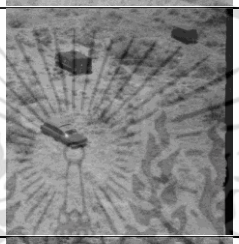
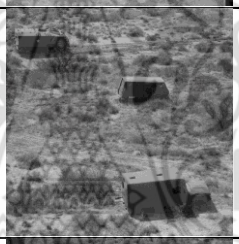
สามารถดาวน์โหลดจาก http://sipi.use.edu/database/ [6]

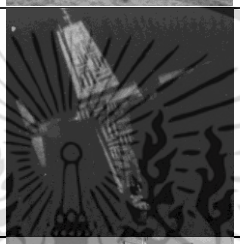
ชื่อภาพ	รูปภาพ	ขนาด
4.1.01.tiff		256×256
4.1.02.tiff		256×256
4.1.03.tiff		256×256
4.1.04.tiff		256×256
4.1.05.tiff		256×256
4.1.06.tiff		256×256

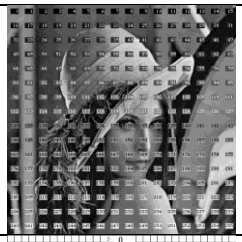
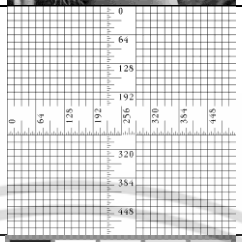
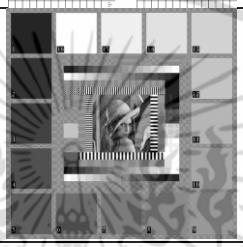
ชื่อภาพ	รูปภาพ	ขนาด
4.1.07.tiff		256×256
4.1.08.tiff		256×256
4.2.01.tiff		512×512
4.2.02.tiff		512×512
4.2.03.tiff		512×512
4.2.04.tiff		512×512
4.2.05.tiff		512×512

ชื่อภาพ	รูปภาพ	ขนาด
4.2.06.tiff		512×512
4.2.07.tiff		512×512
5.1.09.tiff		256×256
5.1.10.tiff		256×256
5.1.11.tiff		256×256
5.1.12.tiff		256×256
5.1.13.tiff		256×256

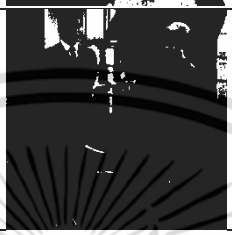
ชื่อภาพ	รูปภาพ	ขนาด
5.1.14.tiff		256×256
5.2.08.tiff		512×512
5.2.09.tiff		512×512
5.2.10.tiff		512×512
5.3.01.tiff		1024×1024
5.3.02.tiff		1024×1024
7.1.01.tiff		512×512

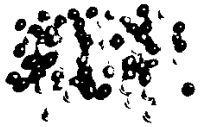
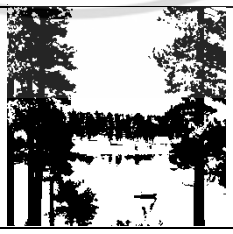
ชื่อภาพ	รูปภาพ	ขนาด
7.1.02.tiff		512×512
7.1.03.tiff		512×512
7.1.04.tiff		512×512
7.1.05.tiff		512×512
7.1.06.tiff		512×512
7.1.07.tiff		512×512
7.1.08.tiff		512×512

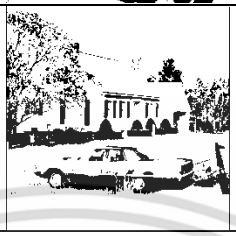
ชื่อภาพ	รูปภาพ	ขนาด
7.1.09.tiff		512×512
7.1.10.tiff		512×512
7.2.01.tiff		1024×1024
Boat.512.tiff		512×512
Elaine.512.tiff		512×512
Gray21.512.tiff		512×512
House.tiff		512×512

ชื่อภาพ	รูปภาพ	ขนาด
Number.512.tiff		512×512
Ruler.512.tiff		512×512
Testpat.1.tiff		1024×1024

รูปภาพขาวดำที่ใช้ในการทดลอง

ชื่อภาพ	รูปภาพ	ขนาด
4.1.01_BW.tiff		256×256
4.1.02_BW.tiff		256×256
4.1.03_BW.tiff		256×256
4.1.04_BW.tiff		256×256
4.1.05_BW.tiff		256×256
4.1.06_BW.tiff		256×256
4.1.07_BW.tiff		256×256

ชื่อภาพ	รูปภาพ	ขนาด
4.1.08_BW.tiff		256×256
4.2.01_BW.tiff		512×512
4.2.02_BW.tiff		512×512
4.2.03_BW.tiff		512×512
4.2.04_BW.tiff		512×512
4.2.05_BW.tiff		512×512
4.2.06_BW.tiff		512×512

ชื่อภาพ	รูปภาพ	ขนาด
4.2.07_BW.tiff		512×512
House_BW.tiff		512×512

ภาคผนวก ข

กฎและสถานะทั้งหมด

กฎ	สถานะของแอทแทรคเตอร์
2	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
3	9 -> 228 -> 18 -> 201 -> 36 -> 147 -> 72 -> 39 -> 144 -> 78 -> 33 -> 156 -> 66 -> 57 -> 132 -> 114, 19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100
10	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18, 51 -> 153 -> 204 -> 102
11	252 -> 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129, 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3, 240 -> 30 -> 195 -> 120 -> 15 -> 225 -> 60 -> 135, 153 -> 204 -> 102 -> 51
14	129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 102 -> 51 -> 153 -> 204, 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53, 43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105
15	3 -> 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126, 5 -> 245 -> 20 -> 215 -> 80 -> 95 -> 65 -> 125, 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129 -> 252, 9 -> 237 -> 36 -> 183 -> 144 -> 222 -> 66 -> 123, 10 -> 235 -> 40 -> 175 -> 160 -> 190 -> 130 -> 250, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120, 18 -> 219 -> 72 -> 111 -> 33 -> 189 -> 132 -> 246, 23 -> 209 -> 92 -> 71 -> 113 -> 29 -> 197 -> 116, 27 -> 201 -> 108 -> 39 -> 177 -> 156 -> 198 -> 114,

กฎ	สถานะของแอทแทรคเตอร์
15	43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105, 46 -> 163 -> 184 -> 142 -> 226 -> 58 -> 139 -> 232, 51 -> 153 -> 204 -> 102, 53 -> 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101, 54 -> 147 -> 216 -> 78 -> 99 -> 57 -> 141 -> 228
16	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
17	9 -> 114 -> 132 -> 57 -> 66 -> 156 -> 33 -> 78 -> 144 -> 39 -> 72 -> 147 -> 36 -> 201 -> 18 -> 228, 19 -> 100 -> 137 -> 50 -> 196 -> 25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200
18	3 -> 132 -> 75 -> 48 -> 72 -> 180, 6 -> 9 -> 150 -> 96 -> 144 -> 105, 12 -> 18 -> 45 -> 192 -> 33 -> 210, 24 -> 36 -> 90 -> 129 -> 66 -> 165
22	5 -> 141 -> 80 -> 216, 10 -> 27 -> 160 -> 177, 20 -> 54 -> 65 -> 99, 40 -> 108 -> 130 -> 198
24	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
27	1 -> 254 -> 2 -> 253 -> 4 -> 251 -> 8 -> 247 -> 16 -> 239 -> 32 -> 223 -> 64 -> 191 -> 128 -> 127, 9 -> 246 -> 18 -> 237 -> 36 -> 219 -> 72 -> 183 -> 144 -> 111 -> 33 -> 222 -> 66 -> 189 -> 132 -> 123, 17 -> 238 -> 34 -> 221 -> 68 -> 187 -> 136 -> 119
30	131 -> 196 -> 111 -> 33 -> 243 -> 28 -> 38 -> 123 -> 9 -> 159 -> 224 -> 49 -> 219 -> 72 -> 252 -> 7 -> 137 -> 222 -> 66 -> 231 -> 56 -> 76 -> 246 -> 18 -> 63 -> 193 -> 98 -> 183 -> 144 -> 249 -> 14 -> 19 -> 189 -> 132 -> 207 -> 112 -> 152 -> 237 -> 36 -> 126, 119 -> 17 -> 187 -> 136 -> 221 -> 68 -> 238 -> 34

กฎ	สถานะของแอทแทรคเตอร์
34	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
35	9 -> 228 -> 18 -> 201 -> 36 -> 147 -> 72 -> 39 -> 144 -> 78 -> 33 -> 156 -> 66 -> 57 -> 132 -> 114, 25 -> 196 -> 50 -> 137 -> 100 -> 19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98
38	11 -> 140 -> 194 -> 35 -> 176 -> 200 -> 44 -> 50, 22 -> 25 -> 133 -> 70 -> 97 -> 145 -> 88 -> 100
39	1 -> 253 -> 2 -> 251 -> 4 -> 247 -> 8 -> 239 -> 16 -> 223 -> 32 -> 191 -> 64 -> 127 -> 128 -> 254, 9 -> 237 -> 18 -> 219 -> 36 -> 183 -> 72 -> 111 -> 144 -> 222 -> 33 -> 189 -> 66 -> 123 -> 132 -> 246, 17 -> 221 -> 34 -> 187 -> 68 -> 119 -> 136 -> 238
42	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6, 5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18, 27 -> 141 -> 198 -> 99 -> 177 -> 216 -> 108 -> 54, 43 -> 149 -> 202 -> 101 -> 178 -> 89 -> 172 -> 86, 45 -> 150 -> 75 -> 165 -> 210 -> 105 -> 180 -> 90, 51 -> 153 -> 204 -> 102, 53 -> 154 -> 77 -> 166 -> 83 -> 169 -> 212 -> 106
43	252 -> 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129, 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3, 204 -> 102 -> 51 -> 153, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120, 202 -> 101 -> 178 -> 89 -> 172 -> 86 -> 43 -> 149, 45 -> 150 -> 75 -> 165 -> 210 -> 105 -> 180 -> 90, 53 -> 154 -> 77 -> 166 -> 83 -> 169 -> 212 -> 106
45	7 -> 113 -> 149 -> 158 -> 131 -> 184 -> 202 -> 79 -> 193 -> 92 -> 101 -> 167 -> 224 -> 46 -> 178 -> 211 -> 112 -> 23 -> 89 -> 233 -> 56 -> 139 -> 172 -> 244 ->

กฎ	สถานะของแอทแทรคเตอร์
45	28 -> 197 -> 86 -> 122 -> 14 -> 226 -> 43 -> 61, 13 -> 103 -> 161 -> 236 -> 52 -> 157 -> 134 -> 179 -> 208 -> 118 -> 26 -> 206 -> 67 -> 217 -> 104 -> 59
46	129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 141 -> 198 -> 99 -> 177 -> 216 -> 108 -> 54 -> 27, 153 -> 204 -> 102 -> 51
47	6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129 -> 252, 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3 -> 249, 204 -> 102 -> 51 -> 153, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120
48	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
49	132 -> 57 -> 66 -> 156 -> 33 -> 78 -> 144 -> 39 -> 72 -> 147 -> 36 -> 201 -> 18 -> 228 -> 9 -> 114, 137 -> 50 -> 196 -> 25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200 -> 19 -> 100
52	13 -> 19 -> 52 -> 76 -> 208 -> 49 -> 67 -> 196, 26 -> 38 -> 104 -> 152 -> 161 -> 98 -> 134 -> 137
53	1 -> 127 -> 128 -> 191 -> 64 -> 223 -> 32 -> 239 -> 16 -> 247 -> 8 -> 251 -> 4 -> 253 -> 2 -> 254, 9 -> 123 -> 132 -> 189 -> 66 -> 222 -> 33 -> 111 -> 144 -> 183 -> 72 -> 219 -> 36 -> 237 -> 18 -> 246, 17 -> 119 -> 136 -> 187 -> 68 -> 221 -> 34 -> 238
54	68 -> 238 -> 17 -> 187, 136 -> 221 -> 34 -> 119, 23 -> 184 -> 197 -> 46 -> 113 -> 139 -> 92 -> 226, 29 -> 163 -> 116 -> 142 -> 209 -> 58 -> 71 -> 232
56	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132

กฎ	สถานะของแอทแทรคเตอร์
58	217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55
59	246 -> 27 -> 237 -> 54 -> 219 -> 108 -> 183 -> 216 -> 111 -> 177 -> 222 -> 99 -> 189 -> 198 -> 123 -> 141, 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157
62	206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185
63	27 -> 237 -> 54 -> 219 -> 108 -> 183 -> 216 -> 111 -> 177 -> 222 -> 99 -> 189 -> 198 -> 123 -> 141 -> 246, 55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236
66	132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
74	131 -> 194 -> 224 -> 176 -> 56 -> 44 -> 14 -> 11, 7 -> 133 -> 193 -> 97 -> 112 -> 88 -> 28 -> 22, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18, 27 -> 155 -> 218 -> 216 -> 220 -> 214 -> 198 -> 230 -> 182 -> 54 -> 55 -> 181 -> 177 -> 185 -> 173 -> 141 -> 205 -> 109 -> 108 -> 110 -> 107 -> 99 -> 115 -> 91
75	11 -> 227 -> 58 -> 169 -> 133 -> 241 -> 29 -> 212 -> 194 -> 248 -> 142 -> 106 -> 97 -> 124 -> 71 -> 53 -> 176 -> 62 -> 163 -> 154 -> 88 -> 31 -> 209 -> 77 -> 44 -> 143 -> 232 -> 166 -> 22 -> 199 -> 116 -> 83, 19 -> 203 -> 98 -> 121 -> 76 -> 47 -> 137 -> 229 -> 49 -> 188 -> 38 -> 151 -> 196 -> 242 -> 152 -> 94
80	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132, 51 -> 102 -> 204 -> 153
81	126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3, 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6, 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225 -> 15, 153 -> 51 -> 102 -> 204

กฎ	สถานะของแอทแทรคเตอร์
83	1 -> 254 -> 128 -> 127 -> 64 -> 191 -> 32 -> 223 -> 16 -> 239 -> 8 -> 247 -> 4 -> 251 -> 2 -> 253, 9 -> 246 -> 132 -> 123 -> 66 -> 189 -> 33 -> 222 -> 144 -> 111 -> 72 -> 183 -> 36 -> 219 -> 18 -> 237, 17 -> 238 -> 136 -> 119 -> 68 -> 187 -> 34 -> 221
84	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 51 -> 102 -> 204 -> 153, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149, 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165
85	3 -> 126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249, 5 -> 125 -> 65 -> 95 -> 80 -> 215 -> 20 -> 245, 6 -> 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243, 9 -> 123 -> 66 -> 222 -> 144 -> 183 -> 36 -> 237, 10 -> 250 -> 130 -> 190 -> 160 -> 175 -> 40 -> 235, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225, 18 -> 246 -> 132 -> 189 -> 33 -> 111 -> 72 -> 219, 23 -> 116 -> 197 -> 29 -> 113 -> 71 -> 92 -> 209, 27 -> 114 -> 198 -> 156 -> 177 -> 39 -> 108 -> 201, 43 -> 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165, 46 -> 232 -> 139 -> 58 -> 226 -> 142 -> 184 -> 163, 51 -> 102 -> 204 -> 153, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149, 54 -> 228 -> 141 -> 57 -> 99 -> 78 -> 216 -> 147
86	131 -> 70 -> 237 -> 9 -> 159 -> 112 -> 200 -> 189 -> 33 -> 243 -> 14 -> 25 -> 183 -> 36 -> 126 -> 193 -> 35 -> 246 -> 132 -> 207 -> 56 -> 100 -> 222 -> 144 -> 249 -> 7 -> 140 -> 219 -> 18 -> 63 -> 224 -> 145 -> 123 -> 66 -> 231 -> 28 -> 50 -> 111 -> 72 -> 252, 187 -> 34 -> 119 -> 68 -> 238 -> 136 -> 221 -> 17

กฎ	สถานะของแอทแทรคเตอร์
88	7 -> 13 -> 28 -> 52 -> 112 -> 208 -> 193 -> 67, 14 -> 26 -> 56 -> 104 -> 224 -> 161 -> 131 -> 134, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132, 27 -> 59 -> 107 -> 99 -> 103 -> 109 -> 108 -> 236 -> 173 -> 141 -> 157 -> 181 -> 177 -> 179 -> 182 -> 54 -> 118 -> 214 -> 198 -> 206 -> 218 -> 216 -> 217 -> 91
89	13 -> 124 -> 197 -> 89 -> 26 -> 248 -> 139 -> 178 -> 52 -> 241 -> 23 -> 101 -> 104 -> 227 -> 46 -> 202 -> 208 -> 199 -> 92 -> 149 -> 161 -> 143 -> 184 -> 43 -> 67 -> 31 -> 113 -> 86 -> 134 -> 62 -> 226 -> 172, 25 -> 122 -> 200 -> 211 -> 70 -> 158 -> 50 -> 244 -> 145 -> 167 -> 140 -> 61 -> 100 -> 233 -> 35 -> 79
98	130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
101	7 -> 116 -> 77 -> 203 -> 14 -> 232 -> 154 -> 151 -> 28 -> 209 -> 53 -> 47 -> 56 -> 163 -> 106 -> 94 -> 112 -> 71 -> 212 -> 188 -> 224 -> 142 -> 169 -> 121 -> 193 -> 29 -> 83 -> 242 -> 131 -> 58 -> 166 -> 229, 11 -> 110 -> 88 -> 115 -> 194 -> 155 -> 22 -> 220 -> 176 -> 230 -> 133 -> 55 -> 44 -> 185 -> 97 -> 205
105	5 -> 114 -> 80 -> 39, 10 -> 228 -> 160 -> 78, 15 -> 105 -> 240 -> 150, 20 -> 201 -> 65 -> 156, 27 -> 95 -> 177 -> 245, 30 -> 210 -> 225 -> 45, 40 -> 147 -> 130 -> 57, 54 -> 190 -> 99 -> 235, 60 -> 165 -> 195 -> 90, 75 -> 135 -> 180 -> 120, 108 -> 125 -> 198 -> 215, 141 -> 175 -> 216 -> 250

กฎ	สถานะของแอทแทรคเตอร์
106	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
112	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132, 27 -> 54 -> 108 -> 216 -> 177 -> 99 -> 198 -> 141, 43 -> 86 -> 172 -> 89 -> 178 -> 101 -> 202 -> 149, 45 -> 90 -> 180 -> 105 -> 210 -> 165 -> 75 -> 150, 51 -> 102 -> 204 -> 153, 53 -> 106 -> 212 -> 169 -> 83 -> 166 -> 77 -> 154
113	126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3, 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6, 153 -> 51 -> 102 -> 204, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225, 106 -> 212 -> 169 -> 83 -> 166 -> 77 -> 154 -> 53, 43 -> 86 -> 172 -> 89 -> 178 -> 101 -> 202 -> 149, 45 -> 90 -> 180 -> 105 -> 210 -> 165 -> 75 -> 150
114	220 -> 179 -> 110 -> 217 -> 55 -> 236 -> 155 -> 118 -> 205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103
115	123 -> 198 -> 189 -> 99 -> 222 -> 177 -> 111 -> 216 -> 183 -> 108 -> 219 -> 54 -> 237 -> 27 -> 246 -> 141, 236 -> 155 -> 118 -> 205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103 -> 220 -> 179 -> 110 -> 217 -> 55
116	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 27 -> 54 -> 108 -> 216 -> 177 -> 99 -> 198 -> 141, 51 -> 102 -> 204 -> 153
117	192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3 -> 126, 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6 -> 252, 51 -> 102 -> 204 -> 153, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225

กฎ	สถานะของแอทแทรคเตอร์
118	205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103 -> 220 -> 179 -> 110 -> 217 -> 55 -> 236 -> 155 -> 118
119	27 -> 246 -> 141 -> 123 -> 198 -> 189 -> 99 -> 222 -> 177 -> 111 -> 216 -> 183 -> 108 -> 219 -> 54 -> 237, 55 -> 236 -> 155 -> 118 -> 205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103 -> 220 -> 179 -> 110 -> 217
120	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
122	7 -> 141 -> 223 -> 112 -> 216 -> 253, 191 -> 224 -> 177 -> 251 -> 14 -> 27, 127 -> 193 -> 99 -> 247 -> 28 -> 54, 108 -> 254 -> 131 -> 198 -> 239 -> 56
126	131 -> 198 -> 239 -> 56 -> 108 -> 254, 7 -> 141 -> 223 -> 112 -> 216 -> 253, 14 -> 27 -> 191 -> 224 -> 177 -> 251, 28 -> 54 -> 127 -> 193 -> 99 -> 247
129	1 -> 124 -> 57 -> 16 -> 199 -> 147, 2 -> 248 -> 114 -> 32 -> 143 -> 39, 4 -> 241 -> 228 -> 64 -> 31 -> 78, 8 -> 227 -> 201 -> 128 -> 62 -> 156
130	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
131	49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100 -> 19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70
135	248 -> 118 -> 33 -> 189 -> 24 -> 199 -> 179 -> 9 -> 237 -> 192 -> 62 -> 157 -> 72 -> 111 -> 6 -> 241 -> 236 -> 66 -> 123 -> 48 -> 143 -> 103 -> 18 -> 219 -> 129 -> 124 -> 59 -> 144 -> 222 -> 12 -> 227 -> 217 -> 132 -> 246 -> 96 -> 31 -> 206 -> 36 -> 183 -> 3, 17 -> 221 -> 136 -> 238 -> 68 -> 119 -> 34 -> 187
138	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18,

กฎ	สถานะของแอทแทรคเตอร์
138	15 -> 135 -> 195 -> 225 -> 240 -> 120 -> 60 -> 30, 39 -> 147 -> 201 -> 228 -> 114 -> 57 -> 156 -> 78, 51 -> 153 -> 204 -> 102, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126
139	252 -> 126 -> 63 -> 159 -> 207 -> 231 -> 243 -> 249, 228 -> 114 -> 57 -> 156 -> 78 -> 39 -> 147 -> 201, 204 -> 102 -> 51 -> 153
142	129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 102 -> 51 -> 153 -> 204, 15 -> 135 -> 195 -> 225 -> 240 -> 120 -> 60 -> 30, 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53, 43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126
143	252 -> 126 -> 63 -> 159 -> 207 -> 231 -> 243 -> 249, 51 -> 153 -> 204 -> 102, 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53 -> 149, 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106 -> 43, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105
144	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
145	25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200 -> 19 -> 100 -> 137 -> 50 -> 196
146	3 -> 132 -> 75 -> 48 -> 72 -> 180, 6 -> 9 -> 150 -> 96 -> 144 -> 105, 12 -> 18 -> 45 -> 192 -> 33 -> 210, 24 -> 36 -> 90 -> 129 -> 66 -> 165
147	187 -> 17 -> 238 -> 68, 119 -> 34 -> 221 -> 136, 23 -> 226 -> 92 -> 139 -> 113 -> 46 -> 197 -> 184, 29 -> 232 -> 71 -> 58 -> 209 -> 142 -> 116 -> 163

กฎ	สถานะของแอทแทรคเตอร์
149	62 -> 220 -> 9 -> 123 -> 48 -> 199 -> 155 -> 33 -> 111 -> 6 -> 248 -> 115 -> 36 -> 237 -> 192 -> 31 -> 110 -> 132 -> 189 -> 24 -> 227 -> 205 - > 144 -> 183 -> 3 -> 124 -> 185 -> 18 -> 246 -> 96 -> 143 -> 55 -> 66 -> 222 -> 12 -> 241 -> 230 -> 72 -> 219 -> 129, 17 -> 119 -> 34 -> 238 -> 68 -> 221 -> 136 -> 187
150	5 -> 141 -> 80 -> 216, 10 -> 27 -> 160 -> 177, 15 -> 150 -> 240 -> 105, 20 -> 54 -> 65 -> 99, 30 -> 45 -> 225 -> 210, 39 -> 250 -> 114 -> 175, 40 -> 108 -> 130 -> 198, 57 -> 215 -> 147 -> 125, 60 -> 90 -> 195 -> 165, 75 -> 120 -> 180 -> 135, 78 -> 245 -> 228 -> 95, 156 -> 235 -> 201 -> 190
151	250 -> 114 -> 175 -> 39, 245 -> 228 -> 95 -> 78, 235 -> 201 -> 190 -> 156, 215 -> 147 -> 125 -> 57
152	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
154	55 -> 211 -> 205 -> 244 -> 115 -> 61 -> 220 -> 79, 110 -> 167 -> 155 -> 233 -> 230 -> 122 -> 185 -> 158
155	244 -> 115 -> 61 -> 220 -> 79 -> 55 -> 211 -> 205, 233 -> 230 -> 122 -> 185 -> 158 -> 110 -> 167 -> 155
161	1 -> 124 -> 57 -> 16 -> 199 -> 147, 2 -> 248 -> 114 -> 32 -> 143 -> 39, 4 -> 241 -> 228 -> 64 -> 31 -> 78, 8 -> 227 -> 201 -> 128 -> 62 -> 156

กฎ	สถานะของแอทแทรคเตอร์
162	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
163	19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100
166	11 -> 140 -> 194 -> 35 -> 176 -> 200 -> 44 -> 50, 22 -> 25 -> 133 -> 70 -> 97 -> 145 -> 88 -> 100
168	95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222
169	95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222
170	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6, 5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18, 15 -> 135 -> 195 -> 225 -> 240 -> 120 -> 60 -> 30, 23 -> 139 -> 197 -> 226 -> 113 -> 184 -> 92 -> 46, 27 -> 141 -> 198 -> 99 -> 177 -> 216 -> 108 -> 54, 29 -> 142 -> 71 -> 163 -> 209 -> 232 -> 116 -> 58, 39 -> 147 -> 201 -> 228 -> 114 -> 57 -> 156 -> 78, 43 -> 149 -> 202 -> 101 -> 178 -> 89 -> 172 -> 86, 45 -> 150 -> 75 -> 165 -> 210 -> 105 -> 180 -> 90, 51 -> 153 -> 204 -> 102, 53 -> 154 -> 77 -> 166 -> 83 -> 169 -> 212 -> 106, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126, 95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222
171	252 -> 126 -> 63 -> 159 -> 207 -> 231 -> 243 -> 249, 228 -> 114 -> 57 -> 156 -> 78 -> 39 -> 147 -> 201, 204 -> 102 -> 51 -> 153, 202 -> 101 -> 178 -> 89 -> 172 -> 86 -> 43 -> 149, 45 -> 150 -> 75 -> 165 -> 210 -> 105 -> 180 -> 90, 53 -> 154 -> 77 -> 166 -> 83 -> 169 -> 212 -> 106,

กฎ	สถานะของแอทแทรคเตอร์
171	95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222
172	237 -> 246 -> 123 -> 189 -> 222 -> 111 -> 183 -> 219
173	62 -> 158 -> 143 -> 167 -> 227 -> 233 -> 248 -> 122, 124 -> 61 -> 31 -> 79 -> 199 -> 211 -> 241 -> 244, 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111, 25 -> 73 -> 201 -> 200 -> 74 -> 78 -> 70 -> 82 -> 114 -> 50 -> 146 -> 147 -> 145 -> 148 -> 156 -> 140 -> 164 -> 228 -> 100 -> 37 -> 39 -> 35 - > 41 -> 57
174	129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 135 -> 195 -> 225 -> 240 -> 120 -> 60 -> 30 -> 15, 141 -> 198 -> 99 -> 177 -> 216 -> 108 -> 54 -> 27, 153 -> 204 -> 102 -> 51, 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126 -> 63, 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
175	249 -> 252 -> 126 -> 63 -> 159 -> 207 -> 231 -> 243, 237 -> 246 -> 123 -> 189 -> 222 -> 111 -> 183 -> 219, 51 -> 153 -> 204 -> 102
176	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
177	19 -> 100 -> 137 -> 50 -> 196 -> 25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200
180	13 -> 19 -> 52 -> 76 -> 208 -> 49 -> 67 -> 196, 26 -> 38 -> 104 -> 152 -> 161 -> 98 -> 134 -> 137
182	207 -> 183 -> 75 -> 252 -> 123 -> 180, 159 -> 111 -> 150 -> 249 -> 246 -> 105, 63 -> 222 -> 45 -> 243 -> 237 -> 210, 219 -> 165 -> 126 -> 189 -> 90 -> 231
183	252 -> 123 -> 180 -> 207 -> 183 -> 75, 249 -> 246 -> 105 -> 159 -> 111 -> 150,

กฎ	สถานะของแอทแทรคเตอร์
183	243 -> 237 -> 210 -> 63 -> 222 -> 45, 231 -> 219 -> 165 -> 126 -> 189 -> 90
184	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132, 95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222
185	190 -> 95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125, 123 -> 189 -> 222 -> 111 -> 183 -> 219 -> 237 -> 246
186	235 -> 245 -> 250 -> 125 -> 190 -> 95 -> 175 -> 215, 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111 -> 183
187	250 -> 125 -> 190 -> 95 -> 175 -> 215 -> 235 -> 245, 246 -> 123 -> 189 -> 222 -> 111 -> 183 -> 219 -> 237
188	111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222
189	123 -> 189 -> 222 -> 111 -> 183 -> 219 -> 237 -> 246
190	189 -> 222 -> 111 -> 183 -> 219 -> 237 -> 246 -> 123
191	237 -> 246 -> 123 -> 189 -> 222 -> 111 -> 183 -> 219
194	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
202	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
208	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132, 15 -> 30 -> 60 -> 120 -> 240 -> 225 -> 195 -> 135, 39 -> 78 -> 156 -> 57 -> 114 -> 228 -> 201 -> 147, 51 -> 102 -> 204 -> 153, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159
209	126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63, 114 -> 228 -> 201 -> 147 -> 39 -> 78 -> 156 -> 57, 102 -> 204 -> 153 -> 51
210	47 -> 206 -> 188 -> 59 -> 242 -> 236 -> 203 -> 179, 94 -> 157 -> 121 -> 118 -> 229 -> 217 -> 151 -> 103

กฎ	สถานะของแอทแทรคเตอร์
211	242 -> 236 -> 203 -> 179 -> 47 -> 206 -> 188 -> 59, 229 -> 217 -> 151 -> 103 -> 94 -> 157 -> 121 -> 118
212	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 51 -> 102 -> 204 -> 153, 15 -> 30 -> 60 -> 120 -> 240 -> 225 -> 195 -> 135, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149, 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159
213	126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63, 102 -> 204 -> 153 -> 51, 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149 -> 53, 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43 -> 106, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165
216	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132
224	95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183
225	95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183
226	130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18, 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175 -> 95, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183
227	250 -> 245 -> 235 -> 215 -> 175 -> 95 -> 190 -> 125, 246 -> 237 -> 219 -> 183 -> 111 -> 222 -> 189 -> 123
228	246 -> 237 -> 219 -> 183 -> 111 -> 222 -> 189 -> 123
229	241 -> 229 -> 199 -> 151 -> 31 -> 94 -> 124 -> 121, 227 -> 203 -> 143 -> 47 -> 62 -> 188 -> 248 -> 242, 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111,

กฎ	สถานะของแอทแทรคเตอร์
229	19 -> 82 -> 114 -> 98 -> 74 -> 78 -> 76 -> 73 -> 201 -> 137 -> 41 -> 57 -> 49 -> 37 -> 39 -> 38 -> 164 -> 228 -> 196 -> 148 -> 156 -> 152 -> 146 -> 147
230	183 -> 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219
231	246 -> 237 -> 219 -> 183 -> 111 -> 222 -> 189 -> 123
234	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18
240	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132, 15 -> 30 -> 60 -> 120 -> 240 -> 225 -> 195 -> 135, 23 -> 46 -> 92 -> 184 -> 113 -> 226 -> 197 -> 139, 27 -> 54 -> 108 -> 216 -> 177 -> 99 -> 198 -> 141, 29 -> 58 -> 116 -> 232 -> 209 -> 163 -> 71 -> 142, 39 -> 78 -> 156 -> 57 -> 114 -> 228 -> 201 -> 147, 43 -> 86 -> 172 -> 89 -> 178 -> 101 -> 202 -> 149, 45 -> 90 -> 180 -> 105 -> 210 -> 165 -> 75 -> 150, 51 -> 102 -> 204 -> 153, 53 -> 106 -> 212 -> 169 -> 83 -> 166 -> 77 -> 154, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159, 95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183
241	126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63, 114 -> 228 -> 201 -> 147 -> 39 -> 78 -> 156 -> 57, 102 -> 204 -> 153 -> 51, 106 -> 212 -> 169 -> 83 -> 166 -> 77 -> 154 -> 53, 43 -> 86 -> 172 -> 89 -> 178 -> 101 -> 202 -> 149, 45 -> 90 -> 180 -> 105 -> 210 -> 165 -> 75 -> 150, 95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183
242	125 -> 250 -> 245 -> 235 -> 215 -> 175 -> 95 -> 190, 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111

กฎ	สถานะของแอทแทรคเตอร์
243	250 -> 245 -> 235 -> 215 -> 175 -> 95 -> 190 -> 125, 246 -> 237 -> 219 -> 183 -> 111 -> 222 -> 189 -> 123
244	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129, 15 -> 30 -> 60 -> 120 -> 240 -> 225 -> 195 -> 135, 27 -> 54 -> 108 -> 216 -> 177 -> 99 -> 198 -> 141, 51 -> 102 -> 204 -> 153, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183
245	126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63, 123 -> 246 -> 237 -> 219 -> 183 -> 111 -> 222 -> 189, 51 -> 102 -> 204 -> 153
246	183 -> 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219
247	246 -> 237 -> 219 -> 183 -> 111 -> 222 -> 189 -> 123
248	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132

ภาคผนวก ค

งานวิจัยที่ตีพิมพ์

การปรับปรุงการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ
An Improved Method for Elementary Cellular Automata Image Encryption Scheme

มงคล ทองไกรแก้ว (Mongkol Thongkraikaew)[1] และรุ่งรัตน์ เวียงศรีพนาวัลย์ (Rungrat Wiangsripanawan) [2]

[1,2]สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

mongkol_ttm@hotmail.com[1], kwrungra@kmitl.ac.th[2]

บทคัดย่อ

งานวิจัยนี้ปรับปรุงขั้นตอนการเข้ารหัสรูปภาพด้วยวิธีการของเซลลูลาร์ออโตมาตาพื้นฐาน (Elementary Cellular Automata) เพื่อแก้ปัญหาให้กับภาพที่เข้ารหัสด้วยวิธีการเดิมให้ผลที่ไม่ดี เช่น ภาพที่เข้ารหัสแล้วไม่สามารถปกปิดเค้าโครงของภาพเดิมและภาพที่เข้ารหัสแล้วฮิสโตแกรมให้ค่าที่ไม่สม่ำเสมอ โดยเพิ่มขั้นตอนการพรี โพรเซส (Pre-process) เพื่อให้ค่าของแต่ละพิกเซลก่อนนำไปเข้ารหัสให้มีความกระจายมากขึ้น อีกทั้งมีการนำหลักการการเปลี่ยนภาพขาวดำเป็นภาพสีเทา มาใช้ร่วมกับการเข้ารหัสที่ปรับปรุงขึ้นมาใหม่ ทำให้สามารถเข้ารหัสภาพขาวดำซึ่งแต่เดิมไม่สามารถทำได้ ผลการทดลองแสดงให้เห็นว่าการเข้ารหัสแบบใหม่สามารถเข้ารหัสภาพได้ทุกประเภท ทุกรูปแบบและปกปิดข้อมูลได้ดีกว่าเดิม

คำสำคัญ: เข้ารหัสรูปภาพ เซลลูลาร์ออโตมาตา ภาพขาวดำ

Abstract

This paper presents a method to improve the existing Elementary Cellular Automata Image Encryption Scheme that has some problems. First, some cipher images keep their traces such as the border of the heads or bodies which can be seen with bare eyes. Second, the histograms of some cipher images are not distributed well. Third, it cannot encrypt the black-and-white images. We improve the randomness of the cipher image by adding a pre-processing step to each pixel before encryption. We also apply the method to converse a black-and-white image to a grey-scale image and then use our improved scheme to encrypt it. The experimental results show that with our improvement, all types of images (color, grey-scale and black-and-white) can be encrypted and a better concealment is obviously provided.

Keyword: Image Encryption, Elementary Cellular Automata, Black-and-White Image.

1. บทนำ

ปัจจุบันมีการใช้งานรูปภาพอย่างกว้างขวางทั้งในโซเชียลเน็ตเวิร์คและสื่อมัลติมีเดีย ข้อมูลรูปภาพส่วนใหญ่ถูกแบ่งปันผ่านเครือข่ายอินเทอร์เน็ตซึ่งไม่ปลอดภัย จึงมีการนำวิธีการของการเข้ารหัสแบบสมมาตร (Symmetric Key Cryptography) เช่น อัลกอริทึม AES มาใช้เพื่อเพิ่มความปลอดภัย แต่การที่ AES เข้ารหัสแบบบล็อก (Block Cipher) ซึ่งไม่เหมาะกับการเข้ารหัสรูปภาพที่มีขนาดใหญ่และต้องการความรวดเร็ว การเข้ารหัสรูปภาพเหมาะกับวิธีการเข้ารหัสแบบสตรีม (Stream Cipher) ซึ่งเป็นการเข้ารหัสแบบสมมาตรอีกประเภทหนึ่ง ที่เน้นความเร็ว อย่างไรก็ดี การนำอัลกอริทึมสำหรับเข้ารหัสข้อมูลทั่วๆ ไปทางสตรีม เช่น RC4 ซึ่งไม่ได้ถูกออกแบบมาให้เข้ารหัสข้อมูลรูปภาพมาเข้ารหัสไฟล์รูปภาพอาจจะให้ผลลัพธ์ที่ไม่ดี เพราะข้อมูลหรือพิกเซลของรูปภาพมีความซ้ำซ้อนสูงกว่าข้อมูลประเภทตัวอักษรมาก เมื่อเข้ารหัสแล้วอาจทำให้มีเค้าโครงของภาพต้นฉบับหลงเหลืออยู่ หรือให้ค่าฮิตโตแกรมที่ไม่กระจาย

ปัจจุบันมีผู้เสนอวิธีเข้ารหัสรูปภาพหลากหลายวิธี เซลลูลาร์ออโตมาตาเป็นหนึ่งในนั้นมีการนำเซลลูลาร์ออโตมาตาทั้งแบบ 2 มิติ และ 1 มิติมาประยุกต์ใช้ในการเข้ารหัส สำหรับในงานวิจัยนี้ได้นำงานวิจัยของ [1,2] มาปรับปรุง ซึ่งใช้เซลลูลาร์ออโตมาตาแบบ 1 มิติ ในการสร้างคีย์และการเข้ารหัส ข้อดีของวิธีการนี้คือมีความซับซ้อนน้อยกว่าวิธีการอื่น และใช้เวลาน้อย อย่างไรก็ดีจากการทดลองกับภาพในฐานข้อมูล USC-SIPI

[3] พบว่าการเข้ารหัสแบบเดิมใน [1] นั้นให้ผลที่ไม่ดีอย่างมากกับภาพที่มีพิกเซลโทนสีเดียวกันในจำนวนมากๆ เช่น ภาพท้องฟ้า ภาพทะเล เนื่องจากภาพที่ได้จากการเข้ารหัสจะเห็นเค้าโครงของภาพเดิม และการเข้ารหัสด้วยวิธีการเดิมนั้นไม่สามารถเข้ารหัสภาพขาวดำ (Black and White) ได้

ดังนั้นในงานวิจัยนี้จึงทำการเพิ่มขั้นตอนก่อนที่จะนำข้อมูลของแต่ละพิกเซลไปเข้ารหัสโดยมีวัตถุประสงค์ในการลดความซ้ำซ้อนของค่าของพิกเซลตั้งต้น และ มีการนำหลักการของ [6] มาประยุกต์ ในการเปลี่ยนภาพขาวดำ ให้เป็นภาพสีเทา แล้วจึงนำภาพสีเทานำไปเข้ารหัส

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 เซลลูลาร์ออโตมาตา

2.1.1 เซลลูลาร์ออโตมาตาพื้นฐาน

เซลลูลาร์ออโตมาตา [2,4] เป็นแบบจำลองทางคณิตศาสตร์ที่ใช้ในการอธิบายระบบต่างๆ ที่สามารถแยกองค์ประกอบเป็นส่วนๆและเกี่ยวข้องกับเวลาที่เปลี่ยนแปลงแบบไม่ต่อเนื่อง (discrete) เรียกแต่ละส่วนว่าเซล (cell) แต่ละเซลมีสถานะ (state) ของตัวเองและเปลี่ยนแปลงเมื่อเวลาเปลี่ยน t ไป $t+1$ สถานะใหม่ถูกกำหนดโดยสถานะของย่านข้างเคียง (neighborhood) ของเซล ณ เวลา t โดยในแต่ละเซลมีฟังก์ชันหรือเรียกว่ากฎ (rule) เป็นตัวกำหนดสถานะใหม่ โดยการเปลี่ยนสถานะสามารถคำนวณได้ดังสมการที่ (1)

$$s_i^{t+1} = f_i(s_{neighborhood}^t) \quad (1)$$

ให้ s_i^{t+1} แทนค่าสถานะของเซล i ที่เวลา $t+1$, f_i แทนฟังก์ชันหรือกฎของตำแหน่ง i $s_{neighborhood}^t$ แทนค่าสถานะของย่านข้างเคียงที่เวลา t

เซลลูลาร์ออโตมาตาประเภท 1 มิติ มีค่าสถานะของแต่ละเซลเป็นได้เพียง 0 และ 1 เท่านั้น กำหนดให้สถานะย่านข้างเคียงของเซลคือ $s_{i-1}^t, s_i^t, s_{i+1}^t$ สถานะใหม่ของเซล i จะมีค่าดังสมการที่ (2)

$$s_i^{t+1} = f_i(s_{i-1}^t, s_i^t, s_{i+1}^t) \quad (2)$$

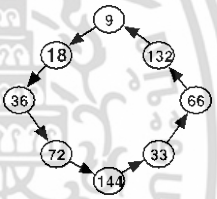
จากสมการที่ (2) เห็นว่าสถานะย่านข้างเคียงมี 3 ค่า แสดงว่ารูปแบบสถานะย่านข้างเคียงมีทั้งหมด $2^3 = 8$ รูปแบบ และมีกฎได้ทั้งหมด $2^8 = 256$ กฎ ยกตัวอย่างการเปลี่ยนสถานะใหม่ในแต่ละกฎในตารางที่ 1

ตารางที่ 1: กฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

ตำแหน่ง	7	6	5	4	3	2	1	0
สถานะย่านข้างเคียง	111	110	101	100	011	010	001	000
กฎ 90 (01011010)	0	1	0	1	1	0	1	0
กฎ 150 (10010110)	1	0	0	1	0	1	1	0
กฎ 255 (11111111)	1	1	1	1	1	1	1	1

2.1.2 แอทแทรคเตอร์(Attractor)

เซลลูลาร์ออโตมาตาพื้นฐาน มีจำนวนเซลจำนวน 8 เซลเท่านั้น ดังนั้นการหาค่าสถานะใหม่ของเซลที่ 1 และ 8 จะไม่มีสถานะย่านข้างเคียง s_{i-1}^t และ s_{i+1}^t ตามลำดับ จึงได้มีการนำเงื่อนไขแบบคาบ (periodic boundary) มาประยุกต์ใช้ โดยตั้งค่าสถานะใหม่ของเซลที่ 1 ให้มีสถานะย่านข้างเคียงคือสถานะของเซลที่ 8 และตั้งค่าสถานะย่านข้างเคียงของเซลที่ 8 คือค่าสถานะของเซลที่ 1



ภาพที่ 1: แผนภาพการเปลี่ยนสถานะแอทแทรคเตอร์ของกฎที่ 2

ดังนั้นเมื่อมีการเปลี่ยนสถานะไปเรื่อยๆ ค่าของทุกเซลจะวนกลับมาเท่ากับค่าสถานะเริ่มต้น เรียกคุณสมบัติแบบนี้ว่า *แอทแทรคเตอร์ (Attractor)* [2] สามารถเขียนเป็นแผนภาพตัวอย่างได้ตามภาพที่ 1 ในการคำนวณหาแอทแทรคเตอร์คำนวณจากกฎและสถานะเริ่มต้น ซึ่งจะมีบางสถานะในบางกฎเท่านั้นที่จะมีคุณสมบัติเป็นแอทแทรคเตอร์ได้ ซึ่งเมื่อนำสถานะทั้งหมดของแอทแทรคเตอร์ มา exclusive-or (xor) ค่าที่ได้จะเท่ากับ 0 สามารถเขียนเป็นสมการได้ดังนี้

$$st(1) \oplus st(2) \oplus \ldots \oplus st(k) = 0 \quad (3)$$

ให้ $st(1), st(2)$ คือค่าสถานะของช่วงเวลาที่ 1 และ 2, k แทนจำนวนสถานะทั้งหมดของแอทแทรคเตอร์ และ $\oplus$ แทนตัวดำเนินการ xor

2.2 การเข้ารหัสรูปภาพ

ในหลายบทความวิจัยมีการนำทฤษฎีต่างๆ มาประยุกต์ เพื่อเสนอวิธีการเข้ารหัสที่เหมาะสมสำหรับเข้ารหัสรูปภาพโดยเฉพาะ [5-6] วิธีที่ได้รับความนิยมเป็นอย่างมากคือวิธีที่ Zhang และคณะ[7] นำหลักการ Choatic system โดยใช้ Choatic map ช่วยในการสลับข้อมูลที่ซ้ำกันให้เกิดความวุ่นวายของข้อมูลจนทำให้ไม่เหลือเค้าโครงของวัตถุหลงเหลืออยู่ อีกวิธีหนึ่งคือการสร้างสตรีมไซเฟอร์สำหรับเข้ารหัสรูปภาพโดยเฉพาะ ซึ่งแต่ละงานวิจัยมีการนำเสนอวิธีการเข้ารหัสและสร้างคีย์ที่แตกต่างกันเช่น ใช้ Ant Colony Optimization (ACO) ในการสร้างคีย์สำหรับเข้ารหัส [8] เป็นต้น

2.3 การเข้ารหัสรูปภาพโดยใช้เซลลูลาร์ออโตมาตา

Wolfram [9] ศึกษาและริเริ่มการเข้ารหัสข้อมูลรูปภาพโดยใช้หลักการของเซลลูลาร์ออโตมาตา Chen และ Lai [10-11] นำเซลลูลาร์ออโตมาตาแบบ 2 มิติมาใช้ในการสร้างตัวเลขสุ่มเทียม (Pseudorandom Number Generator) Li และคณะ [12] นำเซลลูลาร์ออโตมาตาแบบ 2 มิติ มาใช้ในขั้นตอนการเข้ารหัส

สำหรับเซลลูลาร์ออโตมาตาแบบพื้นฐานนั้น Jun[2] นำคุณสมบัติพิเศษในการเปลี่ยนสถานะของแอทแทรคเตอร์ในสมการที่ (3) มาประยุกต์ใช้ดังนี้

$$plain \oplus st(1) \oplus st(2) \oplus \dots \oplus st(t) = cipher \quad (4)$$

$$cipher \oplus st(t+1) \oplus \dots \oplus st(k) = plain \quad (5)$$

ให้ $plain$ คือค่าของพิกเซลก่อนทำการเข้ารหัส $cipher$ คือค่าของพิกเซลหลังทำการเข้ารหัสแล้ว t แทนจำนวนสถานะที่น้อยกว่าสถานะทั้งหมดและ k แทนจำนวนสถานะทั้งหมด

วนิดา และ นันทิกา [1] นำงานวิจัยของ Jun มาปรับปรุงโดยนำวิธีการของตัวเลขสุ่มเทียมมาเพิ่มขนาดของจำนวนคีย์สเปซให้เพิ่มขึ้นจำนวนมากขึ้น และ ปรับปรุงวิธีการในการเข้ารหัสให้สามารถเข้ารหัสได้ทั้งภาพสีและภาพสีเทา (Gray scale)

2.4 ปัญหาของการเข้ารหัสด้วยวิธีการของวนิดา

วิธีการเข้ารหัสของวนิดามีข้อเสียคือ ภาพบางภาพเช่น ภาพท้องฟ้าและภาพที่ 4(a) เมื่อเข้ารหัสแล้วคงเหลือเค้าโครงบางอย่างของภาพต้นฉบับ และภาพบางภาพเมื่อเข้ารหัสแล้วฮิสโตแกรมของภาพที่ผ่านการเข้ารหัสให้ค่าไม่สม่ำเสมอ และวิธีการนี้ไม่สามารถเข้ารหัสภาพขาวดำได้

3. วิธีการเข้ารหัสภาพแบบใหม่

เนื่องจากงานวิจัยนี้นำวิธีการของวนิดามาปรับปรุง จึงขอกล่าวถึงวิธีการของวนิดาดังนี้

3.1 วิธีการเข้ารหัสของเดิม

งานวิจัยของวนิดา คีย์ที่ใช้ในการเข้ารหัสคือ (rule,seedstate,seedtime) rule แทนกฎที่ใช้ในการเข้ารหัส seedstate แทนค่าเริ่มต้นที่ใช้ในการหาตัวเลขสุ่มเทียมเพื่อหาสถานะเริ่มต้นและ seedtime แทนจำนวนสถานะที่ใช้ในการเข้ารหัส ตารางที่ 2 แสดงการเข้ารหัสแบบเดิมดังนี้

สำหรับการถอดรหัสนั้น จะมีวิธีเหมือนกับการเข้ารหัส โดยเริ่มจากคำนวณหาค่าเริ่มต้นต่างๆจากคีย์ จากนั้นนำพิกเซลที่จะถอดรหัสมาสลับบิตเช่นเดียวกับการเข้ารหัส เมื่อได้ค่าทั้งหมดให้ทำการถอดรหัสด้วยสมการที่ 8 ดังนี้

$$p\_pic(r,c) = c\_pix(r,c) \oplus st(t+1,r,c) \oplus \dots \oplus st(k,r,c) \quad (8)$$

ตารางที่ 2: วิธีการเข้ารหัสแบบเดิม

1) นำกฎมาหาค่าของแอทแทรคเตอร์เก็บไว้ในอาร์เรย์ P
2) สุ่มสถานะเริ่มต้นจาก seedstate เก็บไว้ในอาร์เรย์ S
3) สุ่มจำนวนสถานะที่ใช้ในการเข้ารหัสจาก seedtime เก็บไว้ในอาร์เรย์ T
4) กำหนดสถานะเริ่มต้นให้กับแต่ละพิกเซลด้วยสมการ

$$st(1,r,c) = P((S(r,c) \bmod q) + 1 \quad (6)$$

5) เข้ารหัสแต่ละพิกเซล

$$p\_pix(r,c) \oplus st(1,h,v) \oplus \dots \oplus st(t,h,v) = c\_pix \quad (7)$$
$$t = T(r,c) \bmod k - 1$$

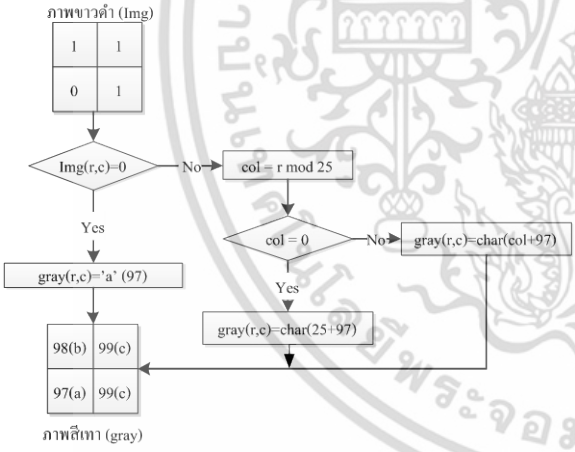
6) สลับบิต

ให้ $st(i,r,c)$ แทนสถานะที่ i ของพิกเซลตำแหน่งแถว r และหลัก c, $S(r,c)$ แทนค่าตัวเลขสุ่มที่อยู่ในอาร์เรย์ S ที่แถว r และหลัก c, $P(i)$ แทนค่าสถานะของอาร์เรย์ P ที่ตำแหน่ง i, q แทนจำนวนสถานะทั้งหมดที่อยู่ในอาร์เรย์ P, $p\_pix(r,c)$ แทนพิกเซลเพลนเท็กซ์ที่ตำแหน่งแถว r และหลัก c, c_pix แทนพิกเซลไซเฟอร์เท็กซ์ที่ตำแหน่งแถว r และหลัก c และ $T(r,c)$ แทนค่าตัวเลขสุ่มที่อยู่ในอาร์เรย์ T

3.2 วิธีการเข้ารหัสแบบใหม่

วิธีการเข้ารหัสแบบใหม่ปรับปรุงข้อเสียของวิธีเข้ารหัสแบบเดิม โดยปรับปรุงอัลกอริทึมในการเข้ารหัสให้สามารถเข้ารหัสภาพได้ทุกประเภท และเพิ่มประสิทธิภาพการปกปิดข้อมูล โดยเพิ่มขั้นตอนสองขั้นตอนคือ หนึ่ง ขั้นตอนการเปลี่ยนจากภาพขาวดำเป็นภาพสีเทาในกรณีที่รูปภาพที่เข้ารหัสเป็นภาพขาวดำ ขั้นตอนที่สอง ในส่วนของอัลกอริทึมในการเข้ารหัส มีการทำพรีโปรเซสโดยการนำพิกเซลของ เพลนเท็กซ์ ณ ตำแหน่งนั้นไป xor กับพิกเซลไซเฟอร์ก่อนหน้า ก่อนที่จะนำพิกเซลนั้นไปเข้ารหัส

แผนผังในภาพที่ 3 แสดงขั้นตอนในการเข้ารหัสแบบใหม่ ซึ่งสังเกตได้ว่า ไม่ว่าจะเป็นภาพสี ภาพสีเทา และ ภาพขาวดำ วิธีการในการเข้ารหัสเหมือนกันทั้งหมดแต่ภาพขาวดำจะมีการแปลงภาพขาวดำเป็นภาพสีเทาก่อน ซึ่งงานวิจัยนำวิธีการของ Sreelaja [6] มาประยุกต์ในการเปลี่ยนภาพขาวดำเป็นภาพสีเทา ซึ่งขั้นตอนในการเปลี่ยนภาพขาวดำเป็นภาพสีเทาสามารถดูได้ในภาพที่ 2



ภาพที่ 2: ขั้นตอนการเปลี่ยนภาพขาวดำเป็นภาพสีเทา [6]

หลังจากได้ภาพเรียบร้อยแล้ว (ภาพสี ภาพสีเทา ภาพสีที่ถูกแปลงมาจากภาพขาวดำ) ก่อนที่จะนำแต่ละพิกเซลไปเข้ารหัสในวิธีการเดิม ให้นำพิกเซลนั้นไปทำพรีโปรเซสในสมการที่ (9) ก่อนนำไปเข้ารหัสในสมการที่ (10) และสิ้นสุดด้วยการสลับบิตตามแบบการเข้ารหัสแบบเดิม

$$pre\_pix(r,c) = p\_pix(r,c) \oplus c\_pix(r,c-1) \quad (9)$$

ถ้า $p\_pix(r,0)$: i ={1…m} ค่า $c\_pix(r,c-1) = 0$

$$c\_pix(r,c) = pre\_pix(r,c) \oplus st(1,r,c) \oplus \ldots \oplus st(t,r,c) \quad (10)$$

เมื่อ $pre\_pix(r,c)$ แทนค่าสถานะก่อนทำการ xor กับสถานะในการเข้ารหัส

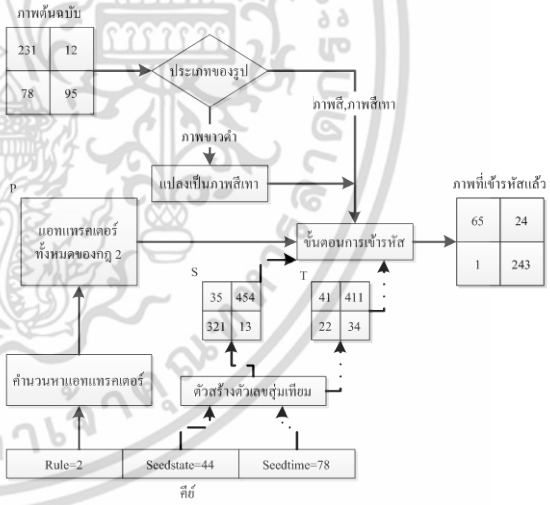
ขั้นตอนของการถอดรหัสมีวิธการเช่นเดียวกับการถอดรหัสวิธีเดิมโดยนำพิกเซลไซเฟอร์เท็กซ์ไปสลับบิตและทำการถอดรหัสตามปกติดังสมการที่ (2) จากนั้นให้นำค่านั้นไป xor กับค่าของพิกเซลไซเฟอร์ก่อนหน้า จึงจะได้ค่าพิกเซล เพลนเท็กซ์ดังสมการที่ (12) เมื่อทำจนครบทุกพิกเซลจะได้ภาพต้นฉบับคืนมายกเว้นในกรณีที่ภาพต้นฉบับเป็นภาพขาวดำ ให้ทำวิธีการย้อนกลับสมการในการแปลงภาพสีเทาเป็นภาพขาวดำ

$$pre\_pix(r,c) = c\_pix(r,c) \oplus st(t+1,r,c) \oplus \ldots \oplus st(k,r,c) \quad (11)$$

$$p\_pix(r,c) = pre\_pix(r,c) \oplus c\_pix(r,c-1) \quad (12)$$

ถ้า $c\_pix(r,0)$: i ={1…m} ค่า $c\_pix(r,c-1) = 0$

เมื่อ $pre\_pix(r,c)$ แทนค่าสถานะก่อนทำการ xor กับสถานะในการถอดรหัส



ภาพที่ 3: ขั้นตอนการเข้ารหัสวิธีใหม่

4. ผลการทดลอง

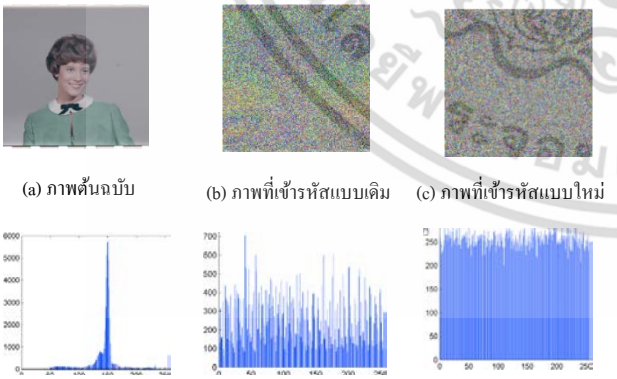
รูปภาพที่ใช้ในการทดสอบในงานวิจัยนี้นำมาจากฐานข้อมูล USC-SIPI [3] ประกอบด้วยภาพสีและภาพสีเทา ในส่วนของภาพขาวดำนั้นได้ทำการแปลงมาจากภาพสีเทาบางส่วน ขนาดของพิกเซลของภาพที่ใช้มี 3 ขนาดคือ 256 × 256, 512 × 512 และ 1024 × 1024 ตามลำดับ ในการทดลองใช้

กฎเดียวกันเข้ารหัสในการเข้ารหัสแบบเก่าละแบบใหม่ ทดสอบโดยคุณสมบัติต่อไปนี้

4.1 การปกปิดข้อมูล (*Information Concealing*)

วิธีการเข้ารหัสที่ดีไม่ควรเหลือเค้าโครงของภาพเดิมและค่าฮิสโตแกรมของภาพที่เข้ารหัสแล้วควรจะมีการกระจายอย่างสม่ำเสมอ ซึ่งการเข้ารหัสของงานวิจัยเดิมให้ผลไม่ดีกับภาพที่มีค่าพิกเซลบางพิกเซลจำนวนมาก เช่น ภาพที่ 4(b) เมื่อดูฮิสโต-แกรมของภาพต้นฉบับ (ภาพ 4(d)) สังเกตได้ว่าค่าพิกเซลของสีน้ำเงินที่บริเวณตรงกลางมากกว่าพิกเซลอื่นมาก เมื่อนำค่านั้นไปเข้ารหัสจะได้ผลลัพธ์ที่มีค่าซ้ำกันในจำนวนมาก ทำให้เค้าโครงของภาพเดิมคงอยู่ (ภาพ 4(b)) ยิ่งไปกว่านั้นฮิสโตแกรมของภาพที่เข้ารหัสแล้ว ให้ค่าที่ไม่กระจายแต่เมื่อนำภาพ 4(a) ไปเข้ารหัสด้วยวิธีการใหม่พบว่าภาพที่เข้ารหัสแบบใหม่ไม่หลงเหลือเค้าโครงของภาพที่สามารถเห็นด้วยตาเปล่าและฮิส-โตแกรมให้ผลดีกว่าภาพเดิมมากดังภาพ 4(f) ในภาพที่ 5 พบว่าภาพที่ได้จากการเข้ารหัสแบบเดิมและแบบใหม่ไม่สามารถจำแนกความแตกต่างได้ด้วยตาเปล่าแต่เมื่อดูด้วยฮิสโตแกรมในภาพ 5(e) และ 5(f) พบว่าการเข้ารหัสแบบใหม่ให้ผลดีกว่าการเข้ารหัสแบบเดิมค่อนข้างมาก

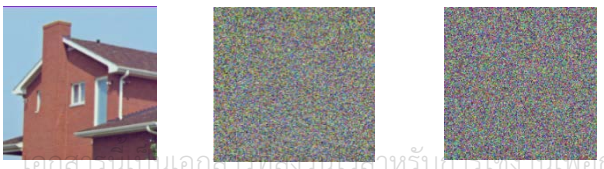
ฮิสโตแกรมในภาพที่ 6 และ 7 แสดงให้เห็นว่าแม้การเข้ารหัสแบบเดิมให้ผลของฮิสโตแกรมค่อนข้างดี แต่เมื่อนำมาเข้ารหัสด้วยวิธีการใหม่พบว่าการเข้ารหัสแบบใหม่ให้ผลที่ดีกว่าเสมอ



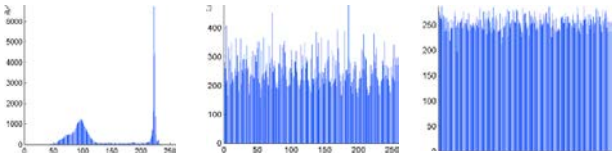
(a) ภาพต้นฉบับ (b) ภาพที่เข้ารหัสแบบเดิม (c) ภาพที่เข้ารหัสแบบใหม่

(d) ฮิสโตแกรมภาพต้นฉบับ (e) ฮิสโตแกรมของวิธีเดิม (f) ฮิสโตแกรมของวิธีใหม่

ภาพที่ 4: เปรียบเทียบภาพและฮิสโตแกรมของทั้งสองวิธี

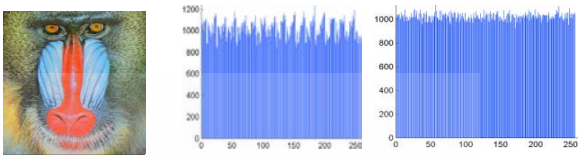


(a) ภาพต้นฉบับ (b) ภาพที่เข้ารหัสแบบเดิม (c) ภาพที่เข้ารหัสแบบใหม่



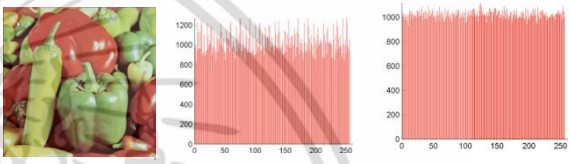
(d) ฮิสโตแกรมของต้นฉบับ (e) ฮิสโตแกรมของวิธีเดิม (f) ฮิสโตแกรมของวิธีใหม่

ภาพที่ 5: เปรียบเทียบภาพและฮิสโตแกรมโตแกรมของทั้งสองวิธี



(a) ภาพต้นฉบับ (b) ฮิสโตแกรมของวิธีเดิม (c) ฮิตโตแกรมของวิธีใหม่

ภาพที่ 6: เปรียบเทียบฮิสโตแกรมโตแกรมของทั้งสองวิธี



(a) ภาพต้นฉบับ (b) ฮิสโตแกรมของวิธีเดิม (c) ฮิสโตแกรมของวิธีใหม่

ภาพที่ 7: เปรียบเทียบฮิสโตแกรมโตแกรมของทั้งสองวิธี

(a) ภาพขาวดำ ต้นฉบับ (b) ภาพขาวดำที่เข้ารหัสแล้ว

ภาพที่ 8: ผลการเข้ารหัสภาพขาวดำ

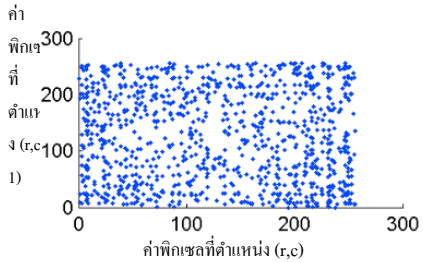
จากผลการทดลองสรุปได้ว่าการเข้ารหัสด้วยวิธีการใหม่ปกปิดข้อมูลได้ดีกว่าเดิมในภาพทุกประเภท

4.2 ความสัมพันธ์ระหว่างพิกเซล (*Correlation Coefficient*)

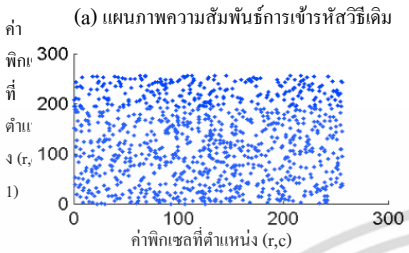
ในการทดสอบคุณสมบัติ Diffusion และ Confusion นั้น ทดสอบด้วยการคำนวณค่าความสัมพันธ์ระหว่าง 2 พิกเซลที่อยู่ติดกันของภาพที่เข้ารหัสแล้ว โดยสุ่มคู่พิกเซลที่อยู่ติดกันจำนวน 1000 คู่ ทั้งในแนวนอน แนวตั้ง และแนวเฉียง มาคำนวณหาค่าความสัมพันธ์ดังสมการต่อไปนี้

$$C_r = \frac{(N\sum_{j=1}^{N} x_j y_j - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j)}{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_i)^2)(N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_i)^2)} \quad (13)$$

เมื่อ x_j และ y_j แทนค่าพิกเซลที่อยู่ติดกันและ N แทนจำนวนคู่พิกเซลทั้งหมดที่เลือกมาใช้ในการคำนวณ



(a) แผนภาพความสัมพันธ์การเข้ารหัสวิธีเดิม



(b) แผนภาพความสัมพันธ์การเข้ารหัสวิธีใหม่

ภาพที่ 9: แผนภาพความสัมพันธ์ระหว่างสองพิกเซลทั้งสองวิธี

จากภาพที่ 9 สรุปได้ว่าการเข้ารหัสด้วยวิธีการใหม่มีความสัมพันธ์ของ 2 พิกเซลที่อยู่ติดกันน้อยกว่าการเข้ารหัสด้วยวิธีเดิม โดยสังเกตจากการกระจายตัวของจุดบนแผนภาพความสัมพันธ์

4.3 ความแตกต่างของรูปภาพ (*Differential Analysis*)

ทดสอบโดยเปรียบเทียบความแตกต่างของภาพที่เข้ารหัสแล้วที่มีคีย์ที่แตกต่างกันเพียงเล็กน้อย [13] ซึ่งงานวิจัยนี้ใช้การคำนวณหาอัตราการเปลี่ยนแปลงของพิกเซล หรือที่เรียกว่า NPCR (Number pixel change rate) อัลกอริทึมในการคำนวณมีดังนี้

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (14)$$

$$D(i,j) = \begin{cases} 1 & A(i,j) \neq B(i,j) \\ 0 & A(i,j) = B(i,j) \end{cases}$$

เมื่อ W และ H คือ ความกว้างและความยาวทั้งหมดของรูปภาพ

ตารางที่ 3: NPCR

รูปภาพ	คีย์ที่ 1	คีย์ที่ 2	NPCR
1	(14,37,56)	(10,37,56)	99.23 %
2	(86,14,70)	(86,15,70)	99.62 %
3	(2,56,32)	(2,56,33)	99.14 %

การทดสอบแบ่งเป็น 3 รูปแบบคือ 1.ค่าของกฎแตกต่างกัน 1 บิต 2.ค่า seedstate แตกต่างกัน 1 บิต 3.ค่า seedtime แตกต่างกัน 1 บิต

5. สรุป

งานวิจัยนี้ทำการปรับปรุงอัลกอริทึมในการเข้ารหัสและเพิ่มขั้นตอนในการเปลี่ยนภาพขาวดำให้เป็นภาพสีเทาเพื่อให้สามารถเข้ารหัสภาพขาวดำได้ จากผลการทดลองแสดงให้เห็นว่างานวิจัยนี้สามารถปกปิดข้อมูลได้ดีกว่าวิธีเดิมมากและสามารถเข้ารหัสภาพขาวดำได้ด้วย

เอกสารอ้างอิง

[1] วนิดา แก้วบูรณะประเสริฐ และ นันทิกา เบญจเทพานันท์, "การปรับปรุงวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน" *8th Int. Joint Conf. on Computer Science and Software Engineering (JSCSSE)*, 2011.

[2] J. Jun, "Image encryption method based on elementary cellular automata" *SOUTHEASTCON, vol. 9*, 2009.

[3] G. Allan, "The USC-SIPI Image Database:Version 5" [Online]. Available: http://sipi.usc.edu/database/, 2006.

[4] J. Jun, "An image encryption based on elementary cellular automata" *Opt Laser Eng*, vol. 50, pp. 1836-1843, 2012.

[5] J. Lang, "Image encryption based on the reality preserving multiple-parameter fractional Fourier transform and chaos permutation" *Opt Laser Eng* , vol. 50, pp. 929-937, 2012.

[6] S.K. Rajput and Naveen K. Nishchal, "Image encryption and authentication verification using fractional non-conventional joint transform correlator" *Opt Laser Eng*, vol. 50,no. 10, pp. 1474-1483, 2012.

[7] L. Zhang, X. Liao and X. Wang, "An image encryption approach based on chaotic maps" *Chaos Solitions and Fractals*, vol. 24, pp. 759-765, 2005.

[8] N.K. Sreelaja and G.A. Vijayalakshmi Pai, "Stream cipher for binary image encryption using Ant Colony Optimization based key generation" *Applied Soft Computing*, vol. 12, pp. 2879-2895, 2012.

[9] Wolfram, "Cryptography with cellular automata" *Crypto-89, Spriger*, vol. 218, pp. 429-432, 1986.

[10] R. Chen and J. Lai, "Image security system using recursive cellular automata substitution" *Pattern Recognition*, vol. 40, no. 5, pp. 1621-1631, 2007.

[11] R. Chen et al., "Image encryption/decryption system using 2-d cellular automata" *ISCE'06*, pp. 1-6, 2006.

[12] Y. Li, L. Yuanxiang and Xia Xuewen, "Image encryption algorithm based on self-adaptive symmetrical-coupled toggle cellular automata" *2008 Congress on Image and Signal Processing*, vol. 3, pp. 32-36, 2008.

[13] J. Ahmad and F. Ahmed, "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" *IJVIPNS-IJENS*, vol. 12, pp. 18-31, 2012.

การวิเคราะห์และปรับปรุงประสิทธิภาพการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ
An Analysis and Improvement of Elementary Cellular Automata Image Encryption

มงคล ทองไกรแก้ว[1] และ รุ่งรัตน์ เวียงศรีพนาวัลย์[2]
[1,2]ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, กรุงเทพมหานคร
Email: mongkol_ttm@hotmail.com[1], kwrungra@kmitl.ac.th[2]

บทคัดย่อ

งานวิจัยนี้ทำการวิเคราะห์และเปรียบเทียบประสิทธิภาพการปกปิดข้อมูลของวิธีการเข้ารหัสรูปภาพที่ใช้หลักการของเซลลูลาร์ออโต-มาตาแบบพื้นฐานโดยปัจจัยที่ใช้ในการวิเคราะห์ ได้แก่ ความสม่ำเสมอของฮิสโตแกรมของภาพที่ผ่านการเข้ารหัส (Cipher image) ความสามารถของคุณสมบัติการแพร่ (Diffusion) จากค่า Number of Pixel Change Rate (NPCR) และค่า Unified Average Change Intensity (UACI) ความสัมพันธ์ของพิกเซลข้างเคียง (Correlation Coefficient) และค่า Peak Signal-to-Noise Ratio (PSNR) นอกจากนี้ได้นำเสนอวิธีการปรับปรุงวิธีการเข้ารหัสเดิมให้มีความสามารถในการปกปิดข้อมูลที่ให้ผลลัพธ์ที่ดีในทุกคุณสมบัติ

คำสำคัญ: การเข้ารหัสรูปภาพ, เซลลูลาร์ออโตมาตาพื้นฐาน, วิเคราะห์ประสิทธิภาพ

Abstract

This paper analyses and compares the security efficiency of algorithms which use elementary cellular automata to encrypt an image. A number of factors are used to measure the efficiency of the algorithms namely the histogram of the cipher image, Number of Pixel Change Rate (NPCR) and Unified Average Change Intensity (UACI) values for diffusion property, the correlation between the adjacent pixels of the cipher image and Peak Signal-to-Noise Ratio (PSNR). We also propose a method to improve the existing algorithm so that good results in all factors are provided.

Keywords: Image Encryption, Elementary Cellular Automata, Analysis

1. บทนำ

ทุกวันนี้การเติบโตของเครือข่ายคอมพิวเตอร์และการพัฒนาเทคโนโลยีเป็นไปอย่างรวดเร็ว ข้อมูลดิจิตอลบางข้อมูลเป็นข้อมูลที่ต้องการความลับระหว่างผู้ส่งและผู้รับเช่น ข้อมูลทางทหารและธุรกรรมทางการเงิน จึงได้มีการนำวิธีการเข้ารหัสมาใช้เพื่อเพิ่มความปลอดภัยของข้อมูลเมื่อมีการส่งข้อมูลเหล่านี้ผ่านอินเทอร์เน็ตซึ่งเป็นเครือข่ายที่ไม่ปลอดภัย มาตรฐานการเข้ารหัสข้อมูลที่ได้รับความนิยมคือ Advanced Encryption Standard (AES) ซึ่งสามารถปกปิดข้อมูลตัวอักษรได้อย่างมีประสิทธิภาพ แต่การที่ข้อมูลรูปภาพมีความแตกต่างจากข้อมูลตัวอักษรมาก [1] เนื่องจากประกอบด้วยพิกเซล (จุดภาพ) จำนวนมากทำให้ข้อมูลมีขนาดใหญ่และการที่พิกเซลในบริเวณเดียวกันมักมีค่าความเข้มแสงเดียวกันหรือใกล้เคียงกันทำให้ข้อมูลมีความซ้ำซ้อนสูงและมีความสัมพันธ์ระหว่างพิกเซลข้างเคียงมาก การเข้ารหัสโดยวิธีทั่วไป เช่น AES จะใช้เวลานานและปกปิดข้อมูลได้ไม่ดี จึงไม่เป็นที่นิยมนำมาใช้เข้ารหัสข้อมูลชนิดรูปภาพ [1] ดังนั้นจำเป็นต้องมีวิธีการเข้ารหัสข้อมูลรูปภาพที่เหมาะสมกับคุณสมบัติที่กล่าวมา เซลลูลาร์ออโตมาตาเป็นวิธีหนึ่งที่สามารถนำมาประยุกต์ใช้ในการเข้ารหัส [2] โดย Chen และ Lai [3-4] ได้นำเซลลูลาร์ออโตมาตาแบบ 2 มิติมาใช้ในการสร้างตัวเลขสุ่มเทียมเพื่อใช้ในการเข้ารหัสและ Jun [5] ได้เป็นผู้ริเริ่มในการนำคุณสมบัติของการเปลี่ยนสถานะของเซลลูลาร์ออโตมาตาแบบพื้นฐานมาประยุกต์ใช้กับการเข้ารหัสรูปภาพ ซึ่งวนิดา [6] ได้ปรับปรุงงานวิจัยของ Jun โดยเพิ่มประสิทธิภาพการปกปิดข้อมูลและเพิ่มจำนวนคีย์ มงคล [7] ได้เพิ่มการปกปิดข้อมูลสำหรับภาพที่เมื่อเข้ารหัสแล้วสามารถวิเคราะห์ทางสถิติได้ (ค่าของฮิสโตแกรมไม่สม่ำเสมอ) และเพิ่มการเข้ารหัสภาพขาวดำ อย่างไรก็ดีในการวัดประสิทธิภาพวิธีการเข้ารหัสรูปภาพที่ดีนั้น การมองด้วยตาเปล่า การวิเคราะห์ทางสถิติ (ความสม่ำเสมอของฮิสโตแกรม) สามารถบอกประสิทธิภาพได้ในระดับหนึ่งเท่านั้น วิธีการเข้ารหัสที่ดีต้องมีคุณสมบัติการแพร่ (Diffusion), คุณสมบัติความสับสน (Confusion), มีคีย์สเปซ (Key space) ขนาดใหญ่และสามารถปกปิดความสัมพันธ์ของพิกเซลข้างเคียงในภาพที่ผ่านการเข้ารหัสแล้วได้เป็นอย่างดี งานวิจัยนี้จึงทำการวิเคราะห์และเปรียบเทียบประสิทธิภาพการปกปิดข้อมูลของวิธีการเข้ารหัสรูปภาพของ วนิดา [6] และ มงคล [7] โดยนำพารามิเตอร์ที่นิยมใช้ในการวัดประสิทธิการเข้ารหัสรูปภาพได้แก่ ความสม่ำเสมอของฮิสโตแกรม คุณสมบัติการแพร่ ค่าความสัมพันธ์ของพิกเซล (Correlation Coefficient) การวัดค่า PSNR [1][8-10] และได้ทำการปรับปรุงวิธีเข้ารหัสของมงคล [7] ให้มีประสิทธิภาพดีขึ้นทั้งภาพสีและภาพขาวดำ โดยงานวิจัยของมงคลยังให้ค่าฮิสโตแกรมที่ไม่สม่ำเสมอในการเข้ารหัสภาพขาวดำ ซึ่งจากผลการทดลองแสดงให้เห็นว่าวิธีการเข้ารหัสแบบใหม่นั้น ให้ค่าฮิสโตแกรมในการเข้ารหัส

ภาพขาวดำที่ดีกว่างานวิจัยเดิมและให้ผลลัพธ์ของค่าพารามิเตอร์ที่ใช้ในการทดสอบใกล้เคียงกับค่ามาตรฐานสำหรับเข้ารหัสรูปภาพในทุกพารามิเตอร์

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 เซลลูลาร์ออโตมาตา (*Cellular Automata*)

เซลลูลาร์ออโตมาตา (CA) เป็นแบบจำลองที่ใช้อธิบายรูปแบบของระบบต่างๆ ที่องค์ประกอบภายในระบบมีการเปลี่ยนแปลงสถานะตามช่วงเวลาที่เปลี่ยนไป [5] โดยใน CA ประกอบด้วยเซลล์ (Cell) หลายเซลล์ที่มีสถานะ (State) ของตนเองและค่าสถานะจะเปลี่ยนจากเวลา t ไปยัง $t+1$ ซึ่งค่าสถานะใหม่ขึ้นอยู่กับสถานะย่านข้างเคียง (Neighborhood) ของเซลล์ตนเอง ณ เวลา t โดยแต่ละเซลล์มีฟังก์ชันหรือกฎ (Rule) เป็นตัวกำหนดสถานะใหม่ สมการการเปลี่ยนสถานะใหม่มีดังนี้

$$s_i^{t+1} = f_i(s_{neighborhood}^t) \quad (1)$$

ให้ s_i^{t+1} แทนค่าสถานะใหม่ของเซลล์ i, f_i แทนฟังก์ชันหรือกฎของเซลล์ i และ $s_{neighborhood}^t$ แทนค่าสถานะย่านข้างเคียง ณ เวลา t

เซลลูลาร์ออโตมาตาพื้นฐาน (Elementary Cellular Automata : ECA) เป็นเซลลูลาร์ออโตมาตาแบบ 1 มิติ ซึ่งสถานะใหม่ของเซลล์ขึ้นอยู่กับค่าสถานะของ 3 เซลล์ข้างเคียงคือ s_{i-1}^t, s_i^t และ s_{i+1}^t สามารถเขียนเป็นสมการได้ดังนี้

$$s_i^{t+1} = f_i(s_{i-1}^t, s_i^t, s_{i+1}^t) \quad (2)$$

ค่าสถานะใน ECA มีค่าได้เพียง 0 กับ 1 เท่านั้น และการที่มีเซลล์สถานะย่านข้างเคียง 3 เซลล์ ทำให้ความน่าจะเป็นของค่าสถานะย่านข้างเคียงมีได้ 8 รูปแบบและมีกฎได้ทั้งหมด 256 กฎ ตารางที่ 1 เป็นการยกตัวอย่างค่าสถานะใหม่ของบางกฎในแต่ละสถานะย่านข้างเคียง

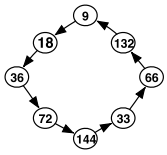
ตารางที่ 1 กฎของเซลลูลาร์ออโตมาตาพื้นฐาน

สถานะย่านข้างเคียง	111	110	101	100	011	010	001	000
กฎ 45	0	0	1	0	1	1	0	1
กฎ 128	1	0	0	0	0	0	0	0
กฎ 255	1	1	1	1	1	1	1	1

2.1.1 แอทแทรคเตอร์ (*Attractor*)

ในการเข้ารหัสรูปภาพ Jun [5] ได้กำหนดจำนวนเซลลูลาร์ออโตมาตาพื้นฐานมีจำนวน 8 เซลล์และได้นำเงื่อนไขแบบคาบ (Periodic boundary) มาประยุกต์ เนื่องจากการหาค่าสถานะใหม่ของเซลล์ที่ 1 และ 8 ไม่มีสถานะย่านข้างเคียง จึงกำหนดให้สถานะย่านข้างเคียง s_{i-1}^t ของเซลล์ที่ 1 คือ เซลล์ที่ 8 และ สถานะย่านข้างเคียง s_{i+1}^t ของเซลล์ที่ 8 คือ เซลล์ที่ 1 ตามลำดับ

เมื่อระบุสถานะเริ่มต้นให้กับทุกเซลล์และกำหนดกฎในการเปลี่ยนสถานะ เมื่อมีการเปลี่ยนสถานะไปเรื่อยๆ ค่าสถานะของทุกเซลล์จะวนกลับมาเท่ากับค่าเริ่มต้น ซึ่งเรียกคุณสมบัติลักษณะนี้ว่า *แอทแทรคเตอร์ (Attractor)* สามารถเขียนเป็นแผนภาพได้ดังรูปที่ 1



รูปที่ 1 แผนภาพการเปลี่ยนสถานะแอทแทรคเตอร์ของกฎที่ 2

2.2 การเข้ารหัสรูปภาพโดยใช้เซลลูลาร์ออโตมาตาพื้นฐาน

Jun [5] นำคุณสมบัติในการเปลี่ยนสถานะของแอทแทรคเตอร์ คือเมื่อนำสถานะทั้งหมดมา exclusive-or (xor) ค่าที่ได้จะเท่ากับ 0 ซึ่งเมื่อนำมาประยุกต์ใช้ในการเข้ารหัสสามารถเขียนสมการได้ดังนี้

$$st(1) \oplus st(2) \oplus \ldots \oplus st(k) = 0 \quad (3)$$

$$plain \oplus st(1) \oplus st(2) \oplus \ldots \oplus st(t) = cipher \quad (4)$$

$$cipher \oplus st(t+1) \oplus \ldots \oplus st(k) = plain \quad (5)$$

ให้ $st(i)$ แทนสถานะลำดับที่ i, k แทนจำนวนสถานะทั้งหมดของแอทแทรคเตอร์ $\oplus$ แทนตัวดำเนินการ xor, $plain$ แทนข้อมูลต้นฉบับ $cipher$ แทนข้อมูลที่ถูกเข้ารหัสและ t แทนจำนวนสถานะที่ใช้ในการเข้ารหัส

3. ค่าพารามิเตอร์สำหรับวัดประสิทธิภาพการเข้ารหัสรูปภาพ

การวัดประสิทธิภาพความปลอดภัยของวิธีการเข้ารหัสรูปภาพสามารถแบ่งออกเป็นสองส่วนหลักคือส่วนของคีย์ซึ่งประกอบด้วยคีย์สเปซ (จำนวนคีย์ที่เป็นไปได้ทั้งหมด) และคุณสมบัติ Confusion (ความสัมพันธ์ของคีย์และข้อความที่ผ่านการเข้ารหัสแล้ว [1]) และส่วนของการปกปิดข้อมูล ซึ่งในส่วนนี้จะกล่าวถึงค่าพารามิเตอร์ที่ใช้ในการวัดประสิทธิภาพการปกปิดข้อมูลของวิธีการเข้ารหัสรูปภาพเท่านั้น

3.1 การแจกแจงของพิกเซล (*Distribution of pixels*)

ฮิสโตแกรม [8] คือกราฟที่แสดงถึงจำนวนพิกเซลในแต่ละความเข้มแสง ซึ่งสามารถนำมาวัดประสิทธิภาพของอัลกอริทึมในการเข้ารหัสรูปภาพได้ การเข้ารหัสรูปภาพที่มีประสิทธิภาพ ฮิสโตแกรมต้องเป็นกราฟที่มีการแจกแจงแบบสม่ำเสมอ (Uniform Distribution) คือทุกค่าความเข้มแสงมีจำนวนที่เท่ากันหรือใกล้เคียงกัน

3.2 คุณสมบัติการแพร่ของการเข้ารหัส (*Diffusion*)

คุณสมบัติการแพร่ของการเข้ารหัสใช้ในการป้องกันการโจมตีที่เรียกว่า Differential Attack ซึ่งเป็นการโจมตีประเภท Chosen Plaintext Attack [11] วิธีการคือผู้โจมตีทำการเปลี่ยนภาพต้นฉบับไปเล็กน้อย (เช่น บิตเดียว) นำภาพทั้งสองภาพไปเข้ารหัส และทำการหาความแตกต่างของภาพที่เข้ารหัสแล้วของภาพเดิมและภาพที่ผ่านการเข้ารหัสของภาพใหม่ เพื่อหาความสัมพันธ์ของพิกเซล วิธีการเข้ารหัสที่มีคุณสมบัติการแพร่ ผู้โจมตีจะไม่สามารถหาความสัมพันธ์ของภาพก่อนและหลังการเข้ารหัสจากค่าความแตกต่างเหล่านี้ได้ การเปลี่ยนข้อมูลต้นฉบับเพียงพิกเซลเดียวข้อมูลที่ถูกเข้ารหัสต้องมีการเปลี่ยนไปทั้งหมดหรือมากที่สุด สิ่งที่นิยมใช้วัดคุณสมบัติการแพร่ในการเข้ารหัสรูปภาพ คือ Number of

Pixel Change Rate *(NPCR)* และ Unified Average Change Intensity *(UACI)* [1][8-10]

Number of Pixel Change Rate คืออัตราร้อยละของจำนวนของค่าพิกเซลต่างกันระหว่างภาพ 2 ภาพและ Unified Average Change Intensity คือค่าเฉลี่ยของความแตกต่างระหว่างภาพ 2 ภาพ ซึ่งค่า NPCR และ UACI ในการเข้ารหัสที่มีประสิทธิภาพควรมีค่าใกล้เคียง 100% และ 33% ตามลำดับ [1][8-10]

ให้ C_1 และ C_2 แทนภาพที่ถูกเข้ารหัสแล้วของภาพ 2 ภาพซึ่งมีพิกเซลต่างกันจำนวนหนึ่งพิกเซลเท่านั้น สมการในการคำนวณมีดังนี้

$$NPCR = \frac{\sum_{i,j} D(r,c)}{T} \times 100\% \quad (6)$$

$$D(r,c) = \begin{cases} 1 & C_1(r,c) \neq C_2(r,c) \\ 0 & C_1(r,c) = C_2(r,c) \end{cases}$$

$$UACI = \frac{\sum_{r,c} |C_1(r,c) - C_2(r,c)|}{F \times T} \times 100\% \quad (7)$$

ให้ $C_1(r,c)$ และ $C_2(r,c)$ แทนค่าพิกเซลที่ถูกเข้ารหัสของภาพ 1 และ 2 ที่ตำแหน่งแถว r และหลัก c, F แทนค่าความเข้มแสงสูงสุดที่รองรับได้ และ T แทนจำนวนพิกเซลทั้งหมด

3.3 ความสัมพันธ์ระหว่างพิกเซล (*Correlation Coefficient*)

นิยามของค่าความสัมพันธ์ (Correlation Coefficient) คือค่าที่บ่งบอกถึงความใกล้เคียงระหว่าง 2 ค่าใดๆ [8] ซึ่งมีค่าระหว่าง -1 ถึง 1 ถ้ามีค่าเข้าใกล้ -1 และ 1 แสดงว่าสองค่านั้นมีความสัมพันธ์กัน แต่ถ้ามีค่าเป็น 0 แสดงว่าสองค่านั้นไม่มีความสัมพันธ์กัน ในการเข้ารหัสรูปภาพใช้ค่าความสัมพันธ์ (Correlation Coefficient) ในสองลักษณะ คือ หนึ่งใช้แสดงความสัมพันธ์ระหว่างภาพต้นฉบับและภาพที่ผ่านการเข้ารหัส สองใช้แสดงความสัมพันธ์ระหว่าง 2 พิกเซลข้างเคียงในภาพที่ผ่านการเข้ารหัสแล้ว ซึ่งวิธีการเข้ารหัสที่ดีค่าความสัมพันธ์ต้องมีค่าใกล้เคียง 0 เนื่องจากต้องการซ่อนคุณสมบัติของภาพต้นฉบับที่มีข้อมูลซ้ำซ้อน [1]

งานวิจัยส่วนใหญ่เน้นที่ค่าความสัมพันธ์ระหว่าง 2 พิกเซลข้างเคียง[1] ดังนั้นกำหนดให้ x และ y คือค่าพิกเซลที่อยู่ข้างเคียงกันของภาพที่ผ่านการเข้ารหัสแล้ว สมการในการหาค่าความสัมพันธ์มีดังนี้

$$Correlation\ Coefficient = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (8)$$

$$cov(x,y) = \frac{1}{T}\sum_{i=}^{N}(x_i - E(x))(y_i - E(y)) \quad (9)$$

$$E(x) = \frac{1}{T}\sum_{i=}^{N} x_i \quad (10)$$

$$D(x) = \frac{1}{T}\sum_{i=}^{N}(x_i - E(x))^2 \quad (11)$$

ให้ $cov(x,y)$ แทนค่าความแปรปรวนร่วมของพิกเซล x และ y, $D(x), D(y)$ แทนค่าความแปรปรวนของพิกเซล x และ y, $E(x), E(y)$ แทนค่าความคาดหมายของพิกเซล x และ y

3.4 *Peak Signal-to-Noise Ratio (PSNR)*

PSNR เป็นพารามิเตอร์ที่ถูกใช้ในการบอกประสิทธิภาพของวิธีการเข้ารหัสรูปภาพ โดยเป็นค่าที่ใช้บอกถึงคุณภาพที่เปลี่ยนไประหว่างภาพต้นฉบับและภาพที่ถูกเข้ารหัสซึ่งค่าที่ดีควรอยู่ระหว่าง 30-50 dB แต่สำหรับการเข้ารหัสรูปภาพค่าที่เหมาะสมควรน้อยกว่า 10 dB [8] จึงจะแสดงว่าภาพต้นฉบับและภาพที่เข้ารหัสไม่มีความสัมพันธ์กัน สมการในการคำนวณมีดังนี้

$$PSNR = 10 \times \log_{10}\left[\frac{255^2}{MSE}\right] \quad (12)$$

$$MSE = \frac{\sum_{r=1}^{W}\sum_{c=1}^{H}[P(r,c) - C(r,c)]^2}{T} \quad (13)$$

ให้ MSE หมายถึงค่าความผิดพลาดเฉลี่ยกำลังสอง W และ H แทนความกว้างและความสูงของภาพ $P(r,c)$ และ $C(r,c)$ แทนค่าพิกเซลของภาพต้นฉบับและภาพที่ถูกเข้ารหัส

4. วิธีการเข้ารหัสภาพ

เนื่องจากข้อมูลประเภทรูปภาพเป็นข้อมูลที่มีความสัมพันธ์กันมาก [1] ดังนั้นการเข้ารหัสรูปภาพที่ดีต้องสามารถลดความสัมพันธ์ระหว่างพิกเซลให้มากที่สุดเพื่อป้องกันการโจมตีของผู้ไม่หวังดี งานวิจัยนี้จึงปรับปรุงการเข้ารหัสแบบวิธีวนิดา [6] และมงคล [7] โดยเพิ่มขั้นตอนก่อนที่จะนำพิกเซลไปเข้ารหัส อีกทั้งยังปรับปรุงอัลกอริทึมในการเตรียมข้อมูลของภาพขาวดำให้ดีขึ้น คีย์ที่ใช้สำหรับการเข้ารหัสวิธีแบบใหม่ยังคงใช้คีย์แบบเดิม คือ (rule,seedstate,seedtime) โดย rule แทนกฎที่ใช้สร้างแอทแทรคเตอร์ seedstate แทนค่าเริ่มต้นสำหรับสุ่มสถานะเริ่มต้นและ seedtime แทนค่าเริ่มต้นสำหรับสุ่มจำนวนสถานะที่ให้ในการเข้ารหัส ขั้นตอนการเข้ารหัสมีดังนี้

4.1 ขั้นตอนการเตรียมข้อมูล

การเตรียมข้อมูลใช้วิธีการเดียวกับมงคล [7] โดยนำ rule หาค่าสถานะเริ่มต้นทั้งหมดของแอทแทรคเตอร์เก็บไว้ในอาร์เรย์ P และสุ่มค่าจากการใช้ค่าเริ่มต้น seedstate และ seedtime เก็บไว้ในอาร์เรย์ S และ T ตามลำดับ ซึ่งมีขนาดอาร์เรย์เท่ากับขนาดของภาพที่จะเข้ารหัส จากนั้นทำการกำหนดสถานะเริ่มต้นให้กับแต่ละพิกเซลและกำหนดจำนวนสถานะในการเข้ารหัส ดังสมการ (14) และ (15) ตามลำดับ

$$state(1) = P((S(r,c)\ mod\ q) + 1) \quad (14)$$

$$time(r,c) = \big(T(r,c)\ mod\ (N-1)\big) + 1 \quad (15)$$

ให้ $state(1)$ แทนสถานะเริ่มต้นของพิกเซลตำแหน่งแถว r หลักที่ c, q แทนจำนวนสถานะเริ่มต้นทั้งหมดในแถวลำดับ P, $time(r,c)$ แทนจำนวนสถานะในการเข้ารหัสของพิกเซลตำแหน่งแถว r หลักที่ c, N แทนจำนวนสถานะทั้งหมดของแอทแทรคเตอร์

หลังจากเตรียมข้อมูลแล้ว อัลกอริทึมจะทำการตรวจสอบว่าเป็นภาพขาวดำหรือไม่ ถ้าเป็นภาพขาวดำจะทำการเปลี่ยนเป็นภาพสีเทา ซึ่งงานวิจัยนี้ได้ปรับปรุงอัลกอริทึมงานวิจัยของมงคล [7] ที่ได้นำวิธีการของ Sreelaja [12] มาประยุกต์ใช้โดยงานวิจัยเดิมเมื่อเปลี่ยนเป็นภาพสีเทาจะ

มีค่าความเข้มแสงตั้งแต่ 97 ถึง 122 ซึ่งมีค่าเพียง 26 ค่า จึงมีความซ้ำซ้อนกันสูงมาก แต่งานวิจัยใหม่มีค่าความเข้มแสงของภาพสีเทาได้ 255 ค่า ซึ่งช่วยลดความซ้ำซ้อนลงได้ อัลกอริทึมมีดังนี้

ตารางที่ 2 อัลกอริทึมการเปลี่ยนจากภาพขาวดำเป็นภาพสีเทา

```
For r = 1 ถึงจำนวนแถวทั้งหมดของรูปภาพ
    For c = 1 ถึงจำนวนหลักทั้งหมดของรูปภาพ
        If bw(r,c) = 1
            gray(r,c) = 1
        Else
            column = r ⊕ 255
            If column = 0
                gray(r,c) = 255
            else
                gray(r,c) = column
            End if
        End if
    End for
End for
```

ให้ $bw(r,c)$ แทนค่าพิกเซลของภาพขาวดำ $gray(r,c)$ แทนพิกเซลภาพสีเทาตำแหน่งแถว r และหลักที่ c

4.2 ขั้นตอนการเข้ารหัส

การเข้ารหัสได้ปรับปรุงวิธีของมงคล [7] ในส่วนของขั้นตอน Preprocess (บรรทัดที่ 5-9) คือในพิกเซลแรกของทุกแถว(ยกเว้นแถวที่ 1) จะนำค่าพิกเซลสุดท้ายของแถวก่อนหน้ามาใช้ในการเข้ารหัสด้วย

ตารางที่ 3 อัลกอริทึมการเข้ารหัส

```
For r = 1 ถึงจำนวนแถวทั้งหมดของรูปภาพ(N_r)
    For c = 1 ถึงจำนวนหลักทั้งหมดของรูปภาพ(N_c)
        If r = 1 และ c = 1
            temp = 0
        Eleseif r ≠ 1 และ c = 1
            temp = pre(r − 1, N_c)
        Else
            temp = pre(r, c − 1)
        End if
        pre(r,c) = (plain(r,c) ⊕ temp )
        pre_c(r,c) = pre(r,c) ⊕ state_encrypt
        cipher(r,c) = swapbit(pre_c(r,c))
    End for
End for
```

ให้ $pre(r,c)$ แทนพิกเซลต้นฉบับที่ผ่านการทำพรีโปรเซส $pre\_c(r,c)$ แทนค่าพิกเซลที่ผ่านการเข้ารหัส $plain(r,c)$ แทนค่าพิกเซลของภาพต้นฉบับตำแหน่งแถว r และหลักที่ c, $state\_encrypt$ แทนสถานะหรือคีย์ที่ใช้สำหรับการเข้ารหัสดังสมการที่ (4), $swapbit()$ แทนฟังก์ชันการสลับบิต $cipher(r,c)$ แทนค่าพิกเซลของภาพที่เข้ารหัสแล้ว และ N_c, N_r แทนจำนวนแถวและหลักทั้งหมด

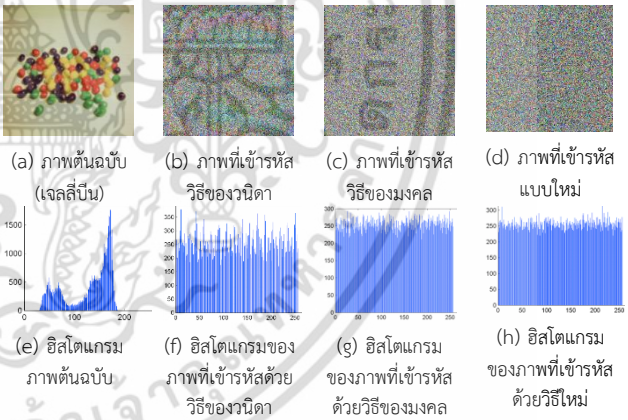
ขั้นตอนการถอดรหัส เริ่มจากการเตรียมข้อมูลเหมือนกับการเข้ารหัส จากนั้นนำภาพที่ผ่านการเข้ารหัสทำการสลับบิตและทำการถอดรหัสเช่นเดียวกับการเข้ารหัสแต่จะใช้สมการที่ (5) จากนั้นหากรูปภาพเป็นภาพขาวดำให้ทำวิธีย้อนกลับของอัลกอริทึมของตารางที่ 2 เพื่อเปลี่ยนจากภาพสีเทาเป็นภาพขาวดำดังเดิม

5. ผลการทดลอง

ในงานวิจัยนี้นำภาพจากฐานข้อมูล USC-SIPI [13] เพื่อใช้ในการเปรียบเทียบประสิทธิภาพในการปกปิดข้อมูลของวิธีการเข้ารหัสของวนิดา [6], วิธีการเข้ารหัสของมงคล [7] และวิธีการเข้ารหัสที่ได้รับการปรับปรุง โดยใช้พารามิเตอร์ที่กล่าวไปแล้วในส่วนที่ 3 และใช้คีย์เดียวกันในทุกวิธีการเข้ารหัส ซึ่งได้เลือกภาพเจลลี่บีน ภาพทิฟฟานี่ ภาพสีเทา (gray21.512) และภาพหญิงสาว (4.1.03) ที่ถูกแปลงเป็นภาพขาวดำ ซึ่งเป็นภาพมีความซ้ำซ้อนของข้อมูลสูงมาใช้ในการทดสอบ

5.1 การกระจายของพิกเซล

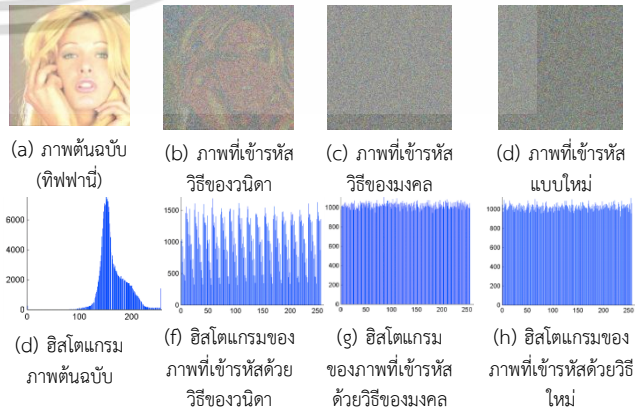
ผลการทดลองในรูปที่ 2 – รูปที่ 4 แสดงว่าวิธีการเข้ารหัสของวนิดาไม่สามารถปกปิดเค้าโครงของภาพที่มีความซ้ำซ้อนของข้อมูลสูง (ความเข้มแสงของพิกเซลส่วนใหญ่เป็นค่าเดียวกันหรือใกล้เคียงกัน) จากการสังเกตด้วยตาได้ ซึ่งให้ผลในลักษณะเดียวกับการวิเคราะห์ค่าฮิสโต-แกรมของภาพที่ผ่านการเข้ารหัสแล้ว (รูปที่ 2(f), 3(f) และ 4(f)) กล่าวคือมีการกระจายของพิกเซลที่ไม่สม่ำเสมอ โดยเฉพาะในรูปที่ 3(f) และ 4(f) ส่วนวิธีการเข้ารหัสภาพของมงคลและวิธีการเข้ารหัสแบบใหม่ ภาพสีและภาพสีเทาที่ผ่านการเข้ารหัสแล้วฮิสโตแกรมมีการกระจายพิกเซลอย่างสม่ำเสมอและไม่คงเค้าโครงของภาพต้นฉบับให้สังเกตได้



(a) ภาพต้นฉบับ (เจลลี่บีน) (b) ภาพที่เข้ารหัสวิธีของวนิดา (c) ภาพที่เข้ารหัสวิธีของมงคล (d) ภาพที่เข้ารหัสแบบใหม่

(e) ฮิสโตแกรมภาพต้นฉบับ (f) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของวนิดา (g) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของมงคล (h) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีใหม่

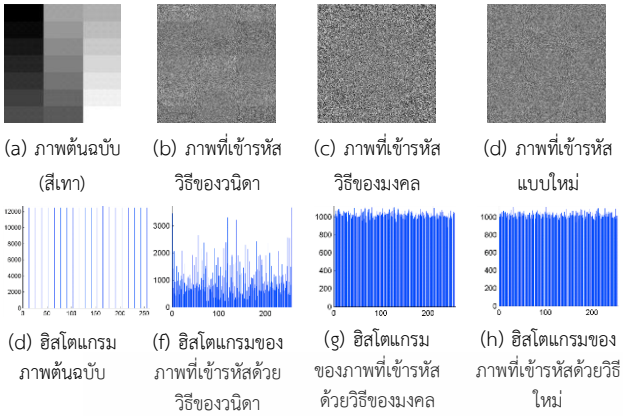
รูปที่ 2 เปรียบเทียบฮิสโตแกรมในการเข้ารหัสภาพเจลลี่บีน



(a) ภาพต้นฉบับ (ทิฟฟานี่) (b) ภาพที่เข้ารหัสวิธีของวนิดา (c) ภาพที่เข้ารหัสวิธีของมงคล (d) ภาพที่เข้ารหัสแบบใหม่

(d) ฮิสโตแกรมภาพต้นฉบับ (f) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของวนิดา (g) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของมงคล (h) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีใหม่

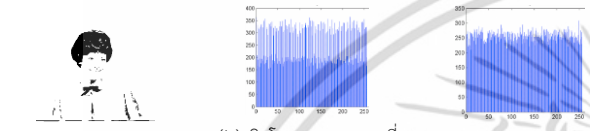
รูปที่ 3 เปรียบเทียบฮิสโตแกรมในการเข้ารหัสภาพทิฟฟานี่



(a) ภาพต้นฉบับ (สีเทา) (b) ภาพที่เข้ารหัสวิธีของวนิดา (c) ภาพที่เข้ารหัสวิธีของมงคล (d) ภาพที่เข้ารหัสแบบใหม่

(d) ฮิสโตแกรมภาพต้นฉบับ (f) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของวนิดา (g) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของมงคล (h) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีใหม่

รูปที่ 4 เปรียบเทียบฮิสโตแกรมในการเข้ารหัสภาพสีเทา



(a) ภาพต้นฉบับ(สีขาวดำ) (b) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีของมงคล (c) ฮิสโตแกรมของภาพที่เข้ารหัสด้วยวิธีใหม่

รูปที่ 5 เปรียบเทียบฮิสโตแกรมในการเข้ารหัสภาพขาวดำ

ภาพขาวดำที่มีพิกเซลสีขาว (ค่าความเข้มแสงเท่ากับ 1) ในจำนวนมากเช่นรูปที่ 5(a) เมื่อเปลี่ยนเป็นภาพสีเทาจะมีความซ้ำซ้อนกันสูง การเข้ารหัสของมงคลไม่สามารถกระจายพิกเซลได้ดีเท่าที่ควร 5(b) แต่งานวิจัยใหม่สามารถลดความซ้ำซ้อนและกระจายพิกเซลดีขึ้นอย่างเห็นได้ชัด 5(c)

5.2 คุณสมบัติการแพร่ของการเข้ารหัส

ผลการทดลองในตารางที่ 6 และ ตารางที่ 7 สรุปได้ว่า การเข้ารหัสด้วยวิธีการใหม่ให้ค่าการแพร่ ทั้ง NPCR และ UACI ดีกว่าวิธีการเดิมทั้งสองวิธีมาก และค่า NPCR และ UACI ของวิธีการเข้ารหัสของมงคลดีกว่าวิธีการเข้ารหัสของวนิดามากเช่นกัน

ตารางที่ 4 ค่า NPCR (%)

รูปภาพ	ขนาดภาพ	NPCR (วนิดา)	NPCR (มงคล)	NPCR (วิธีใหม่)
เจลลี่บีน	256×256	0.0015	0.3906	99.9895
ทิฟฟานี่	512×512	0.0038	0.1953	99.9907
สีเทา	512×512	0.0039	0.1952	99.9996
ขาวดำ	512×512	-	0.1952	99.9941

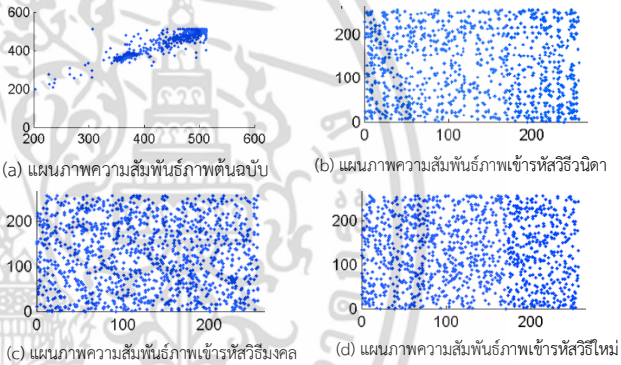
ตารางที่ 5 ค่า UACI (%)

รูปภาพ	ขนาดภาพ	UACI (วนิดา)	UACI (มงคล)	UACI (วิธีใหม่)
เจลลี่บีน	256×256	0.0002	0.1162	29.2464
ทิฟฟานี่	512×512	0.0001	0.0338	17.2432
สีเทา	512×512	0.0001	0.0587	8.36
ขาวดำ	512×512	-	0.0241	6.27

เนื่องจากในการเข้ารหัสของวนิดานั้นแต่ละพิกเซลเข้ารหัสโดยไม่มีความเกี่ยวข้องกันเลย ดังนั้นการเปลี่ยนแปลงค่าของพิกเซลใดพิกเซลหนึ่งจึงไม่มีผลต่อการเข้ารหัสของพิกเซลอื่น ส่วนการเข้ารหัสของมงคลจะมีผลต่อการเข้ารหัสของพิกเซลถัดไปที่อยู่ภายในแถวเดียวกันเท่านั้น ซึ่งการที่ในงานวิจัยนี้ปรับปรุงการเข้ารหัสโดยการนำค่าของพิกเซลหลักสุดท้ายของแถวก่อนหน้ามาใช้ในการเข้ารหัสของพิกเซลแรกในแถวถัดไปด้วย ทำให้การเปลี่ยนแปลงพิกเซลใดพิกเซลหนึ่งจะมีผลต่อพิกเซลที่เหลือทั้งหมด ซึ่งสามารถอธิบายได้ดังนี้ ในภาพต้นฉบับที่มีขนาด $W \times H$ การเปลี่ยนแปลงค่าพิกเซลหนึ่งพิกเซลของภาพนี้ จะมีผลกับพิกเซลที่เข้ารหัสแล้วจำนวน $1, W$ และ $W \times H$ ในแต่ละวิธีการเข้ารหัสตามลำดับ

5.3 ความสัมพันธ์ระหว่างพิกเซลข้างเคียง

ในการวิเคราะห์ความสัมพันธ์ในงานวิจัยนี้เป็นการหาความสัมพันธ์ระหว่างสองพิกเซลข้างเคียงในแนวนอน แนวตั้งและแนวเฉียงโดยทำการสุ่ม 1200 คู่ของพิกเซลข้างเคียงและคำนวณโดยใช้สมการ (8) โดยเปรียบเทียบระหว่างวิธีการเข้ารหัสทั้ง 3 แบบ



(a) แผนภาพความสัมพันธ์ภาพต้นฉบับ (b) แผนภาพความสัมพันธ์ภาพเข้ารหัสวิธีวนิดา (c) แผนภาพความสัมพันธ์ภาพเข้ารหัสวิธีมงคล (d) แผนภาพความสัมพันธ์ภาพเข้ารหัสวิธีใหม่

รูปที่ 6 แผนภาพความสัมพันธ์ระหว่างพิกเซลข้างเคียง

ตารางที่ 6 ค่าความสัมพันธ์ระหว่างสองพิกเซลข้างเคียง

ทิศทางพิกเซลข้างเคียง	ภาพต้นฉบับ	ภาพที่เข้ารหัสวิธีวนิดา	ภาพที่เข้ารหัสวิธีมงคล	ภาพที่เข้ารหัสแบบใหม่
แนวนอน	0.9027	0.0150	0.0107	0.0091
แนวตั้ง	0.9382	0.0127	0.0012	0.0009
แนวเฉียง	0.8623	0.0165	0.0030	0.0009
ค่าเฉลี่ย	0.9010	0.0147	0.0049	0.0036

จากผลการทดลองข้างต้น การเข้ารหัสด้วยวิธีแบบใหม่มีความสัมพันธ์ระหว่างพิกเซลข้างเคียงลดลงกว่าวิธีการเข้ารหัสแบบเดิมอย่างเห็นได้ชัด ซึ่งทำให้ไม่มีข้อมูลที่สามารถใช้ในการคาดเดารูปภาพต้นฉบับหรือคีย์ลับได้

5.4 คุณภาพของรูปภาพ

ค่า PSNR ในตารางที่ 7 ของทั้งสามวิธีให้ค่าที่ไม่แตกต่างกันและเป็นค่าที่ยอมรับในการเข้ารหัสที่ดี (<10 dB)

ตารางที่ 7 ค่า PSNR (dB)

รูปภาพ	PSNR (วนิดา)	PSNR (มงคล)	PSNR (วิธีใหม่)
เจลลี่บีน	8.8987	8.6873	8.6675
ทิฟฟานี่	7.8329	7.0931	7.1000
สีเทา	7.9032	7.6100	7.5915

5.5 การวิเคราะห์ในส่วนของคีย์

งานวิจัยนี้ไม่มีการเปลี่ยนแปลงในส่วนของคีย์ที่ใช้ ดังนั้นจำนวนคีย์ที่เป็นไปได้ทั้งหมดมีค่าเท่าเดิม คือ $256 \times 2^{8196} \times 2^{8196}$ และ มีคุณสมบัติ Confusion (Key Analysis) ดังผลการทดลองใน [6]

5.6 สรุปการวัดประสิทธิภาพของแต่ละวิธี

ตารางที่ 8 สรุปได้ดังนี้ 1) วิธีการเข้ารหัสของวนิดามีปัญหากับภาพที่มีความซ้ำซ้อนของข้อมูลสูงเนื่องจากภาพที่ถูกเข้ารหัสสามารถสังเกตเค้าโครงภาพต้นฉบับได้ด้วยตาและค่าฮิสโตแกรมไม่สม่ำเสมออีกทั้งค่า NPCR และ UACI ยังน้อยกว่าค่ามาตรฐานสูงมากทำให้ไม่ปลอดภัยจากการโจมตีแบบ Differential Attack 2) วิธีการเข้ารหัสของมงคลสามารถเข้ารหัสภาพสีได้ทุกรูปและภาพขาวดำบางรูปแต่ไม่ปลอดภัยในการโจมตีแบบ Differential Attack เนื่องจากค่า NPCR และ UACI ยังต่ำกว่าค่ามาตรฐานอยู่มาก 3).การเข้ารหัสแบบใหม่สามารถเข้ารหัสภาพได้ทุกประเภทและมีความทนทาน (Resistance) สูงต่อการโจมตีแบบ Differential Attack เนื่องจากค่า NPCR และ UACI มีค่าใกล้เคียงค่ามาตรฐานและการเข้ารหัสนี้ให้ค่าความสัมพันธ์ระหว่างพิกเซลข้างเคียงดีที่สุดเนื่องจากมีค่าเข้าใกล้ 0

วิธีการเข้ารหัสแบบใหม่สามารถปกปิดข้อมูลได้ดีเนื่องจากมีนำค่าของพิกเซลหนึ่งพิกเซลก่อนหน้ามาใช้ในการเข้ารหัสของทุกพิกเซล ทำให้เมื่อมีพิกเซลใดพิกเซลหนึ่งเปลี่ยนแปลงจะมีผลกับพิกเซลอื่นๆ แต่วิธีการของมงคลนั้นจะมีผลกับพิกเซลในแถวเดียวกันเท่านั้นและวิธีการของวนิดาจะไม่มีผลกับพิกเซลอื่น

ตารางที่ 8 สรุปการวัดประสิทธิภาพ

คุณสมบัติ	งานวิจัยวนิดา	งานวิจัยมงคล	งานวิจัยใหม่
สามารถสังเกตได้ด้วยตาเปล่า	เฉพาะบางรูป บางคีย์	ไม่สามารถมองเห็นด้วยตาเปล่าทุกรูปและทุกคีย์	ไม่สามารถมองเห็นด้วยตาเปล่าทุกรูปและทุกคีย์
Histogram (Uniform Distribution)	ไม่สม่ำเสมอในบางรูปและบางคีย์	ไม่สม่ำเสมอในบางรูปและบางคีย์เฉพาะภาพขาวดำ	สม่ำเสมอในทุกรูปและทุกคีย์
NPCR (100%)	น้อยกว่า 0.01%	น้อยกว่า 1%	มากกว่า 98%
UACI (33%)	น้อยกว่า 0.001%	น้อยกว่า 0.1%	8%-30%
Correlation Coefficient	น้อยกว่า 0.1	น้อยกว่า 0.02	น้อยกว่า 0.01
PSNR (<10 dB)	น้อยว่า 10 dB	น้อยว่า 10 dB	น้อยว่า 10 dB
Key Analysis	น้อยกว่า 97%	มากกว่า 99%	มากกว่า 99%
Key Space	$256 \times 2^{8196} \times 2^{8196}$	$256 \times 2^{8196} \times 2^{8196}$	$256 \times 2^{8196} \times 2^{8196}$

6. สรุป

งานวิจัยนี้นำวิธีการวิเคราะห์ประสิทธิภาพของวิธีการเข้ารหัสรูปภาพที่นิยมใช้กันแพร่หลายมาใช้ในการวิเคราะห์ประสิทธิภาพของวิธีการเข้ารหัสรูปภาพที่ใช้ ECA และได้นำเสนอวิธีการปรับปรุงวิธีการเข้ารหัสเดิมเพื่อให้ผลลัพธ์ของภาพที่ผ่านการเข้ารหัสแล้วมีประสิทธิภาพที่ดีในการปกปิดข้อมูล อีกทั้งยังเพิ่มประสิทธิภาพการเข้ารหัสภาพขาวดำ ผลการทดลองสรุปได้ว่าวิธีการเข้ารหัสแบบใหม่ให้ผลลัพธ์ที่ดีในทุกคุณสมบัติที่เกี่ยวข้องของภาพทุกประเภท

เอกสารอ้างอิง

[1] N. K Pareek, “Design and Analysis of a Novel Digital Image Encryption Scheme”, 2rd International Journal of Network Security & Its Applications (IJNSA), March, 2012.

[2] Wolfram, “Cryptography with Cellular Automata”, Crypto89 Springer, vol.218, pp.429-432, 1986.

[3] R. Chen and J. Lai, “Image Security System using Recursive Cellular Automata Substitution” *Pattern Recognition*, vol. 40, no. 5, pp. 1621-1631, 2007.

[4] R. Chen et al., “Image Encryption/Decryption System using 2d Cellular Automata” *ISCE’06*, pp. 1-6, 2006.

[5] J. Jun, “Image Encryption Method Based on Elementary Cellular Automata”, SOUTHEASTCON, vol.9, 2009.

[6] วนิดา แก้วบูรณะประเสริฐ และ นันทิกา เบญจเทพานันท์, “การปรับปรุงวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน”, 8th Int. Joint Conf. on Computer Science and Software Engineering (JSCSSE), 2011.

[7] มงคล ทองไกรแก้ว และ รุ่งรัตน์ เวียงศรีพนาวัลย์, “การปรับปรุงการใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ”, 10th National Conference on Computing and Information Technology (NCCIT), pp.589-594, 2014.

[8] J. Ahmad and F. Ahmed, “Efficiency Analysis and Security Evaluation of Image Encryption Schemes”, IJVIPNS-IJENS, vol.12, pp.18-31, 2012.

[9] H. Khanzadi,M. Eshghi and S.E. Borujeni, “Image Encryption Using Random Bit Sequence Based on Chaotic Maps”, Arab J Sci Eng, vol.39, pp.1039-1047,2014.

[10] Z. Zhua and W. Zhangc, “A Chaos-based Symmetric Image Encryption Scheme Using a Bit-level Permutation”, Information Sciences, vol.181, pp.1171-1186, 2011.

[11] E.Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems”, 10th Annual International Cryptology Conference on Advances Cryptology SpringerVerlag, 1991.

[12] N.K. Sreelaja and G.A. Vijayalakshmi Pai, “Stream Cipher for Binary Image Encryption using Ant Colony Optimization based Key Generation”, Applied Soft Computing, vol.12, pp.2879-2895, 2012.

[13] G. Allan, “The USC-SIPI Image Database:Version 5” [Online]. Available: http://sipi.usc.edu/database/, 2006.

ประวัติผู้เขียน

ชื่อ	นายมงคล ทองไกรแก้ว
วัน เดือน ปีเกิด	13 มิถุนายน 2531
ที่อยู่ปัจจุบัน	3191/74 อาคารซิตี้โฮม ซ.สุขุมวิท 101/2 ถ.สุขุมวิท แขวงบางนา เขตบานา กรุงเทพมหานคร 10260
ประวัติการศึกษา	(2553) วิทยาศาตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ เกรดเฉลี่ย 3.01 มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี (2557) วิทยาศาตรมหาบัณฑิต สาขาวิทยาการคอมพิวเตอร์ เกรดเฉลี่ย 3.62 สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ผลงานทางวิชาการ	1.The Tenth National Conference on Computing and Information Technology (NCCIT2014) 2. International Computer Science and Engineering Conference (ICSEC2014)