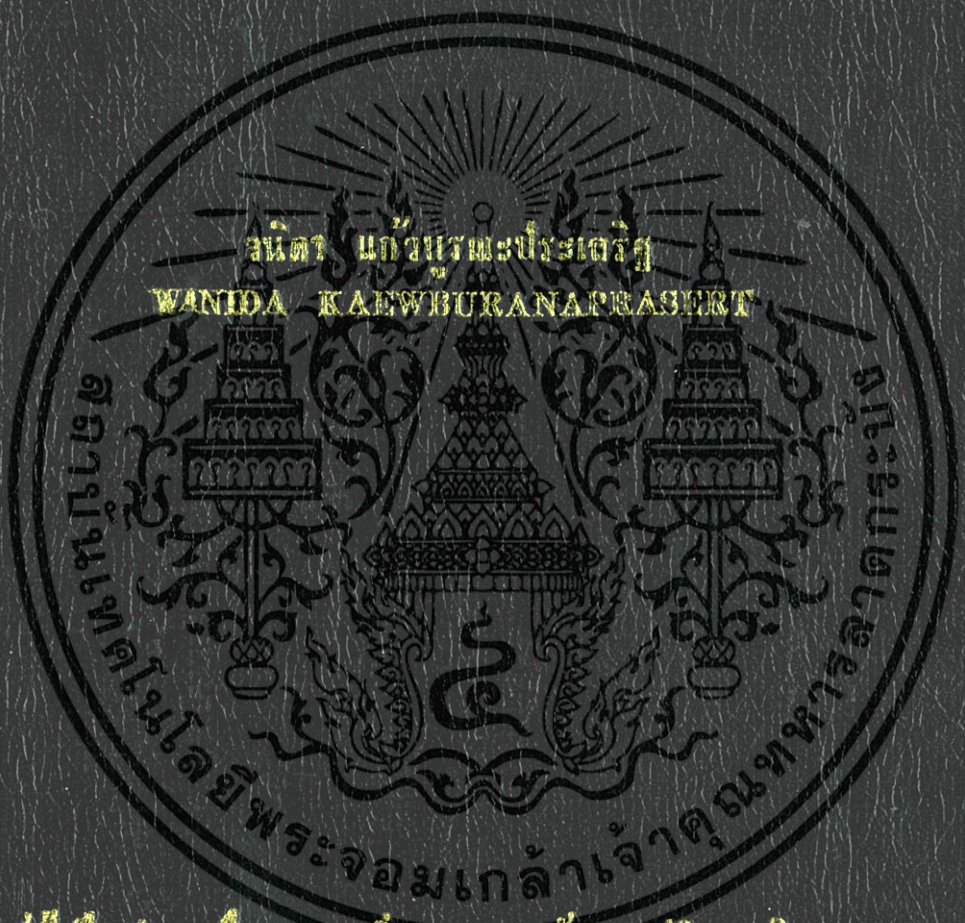
วิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตันแบบพื้นฐาน

IMAGE ENCRYPTION METHOD BASED ON ELEMENTARY CELLULAR AUTOMATA

วนิดา แก้วบูรพะประเสริฐ
WANIDA KAEWBURANAPRASERT



วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2554
KMITL-2011-SC-M-002-011

วิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน

IMAGE ENCRYPTION METHOD BASED ON ELEMENTARY CELLULAR AUTOMATA

วนิดา แก้วบูรณะประเสริฐ

WANIDA KAEWBURANAPRASERT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

สาขาวิชาวิทยาการคอมพิวเตอร์

คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2554

KMITL-2011-SC-M-002-011

คณะวิทยาศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ วิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน

Image encryption method based on elementary cellular automata

นักศึกษา นางสาววนิดา แก้วบูรณะประเสริฐ

รหัสประจำตัว 52650806

ปริญญา วิทยาศาสตรมหาบัณฑิต

สาขาวิชา วิทยาการคอมพิวเตอร์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.นันทิกา เบญจเทพานันท์

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.กรกช	ประชุมรักษ์	
ดร.รุ่งรัตน์	เวียงศรีพนาวัลย์	
รศ.ดร.ดำรัส	วงศ์สว่าง	
ผศ.ดร.นันทิกา	เบญจเทพานันท์	

วัน / เดือน/ ปี ที่สอบ 2 พฤษภาคม พ.ศ. 2554 เวลา 16.00 – 18.00 น.

สถานที่สอบ ณ ห้อง 216 ชั้น 2 อาคารจุฬาภรณวลัยลักษณ์ 1

คณะวิทยาศาสตร์รับรองแล้ว

(รองศาสตราจารย์ ดร.ดุษณี ธนะบริพัฒน์)

คณบดีคณะวิทยาศาสตร์

วันที่ 24 เดือน พ.ค. พ.ศ. 54

หัวข้อวิทยานิพนธ์	วิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน
นักศึกษา	นางสาววนิดา แก้วบูรณะประเสริฐ
รหัสประจำตัว	52650806
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	วิทยาการคอมพิวเตอร์
พ.ศ.	2554
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผศ.ดร.นันทิกา เบญจเทพานันท์

บทคัดย่อ

วิธีการเข้ารหัสรูปภาพโดยใช้เซลลูลาร์ออโตมาตา (cellular automata) ได้ถูกนำเสนอมาแล้วหลายวิธี วิธีหนึ่งคือการใช้แผนภาพการเปลี่ยนสถานะ (state – transition diagram) ของเซลลูลาร์ออโตมาตาแบบพื้นฐาน (elementary cellular automata) สร้างสตรีมของกุญแจ (key stream) สำหรับการเข้ารหัส ซึ่งวิธีนี้มีข้อเสียคือมีกุญแจที่ไม่สามารถปกปิดรูปภาพได้ (weak key) มากเกินไป ดังนั้นในงานวิจัยนี้จึงใช้ตัวสร้างเลขสุ่มเทียม (pseudo random number generator) เพื่อเลือกสถานะ (state) เริ่มต้นของแต่ละจุดภาพ (pixel) ซึ่งทำให้จำนวนของกุญแจทั้งหมดที่เป็นไปได้ (key space) มีจำนวนมากขึ้นรวมทั้งใช้การสลับที่ของบิต (bit) ของค่าความเข้มแสงของจุดภาพ เพื่อเพิ่มความสามารถในการปกปิดข้อมูลอีกด้วย จากผลการทดลองแสดงให้เห็นว่า วิธีที่นำเสนอนี้สามารถปกปิดข้อมูลได้ดีกว่าเดิม โดยที่ยังคงมีคุณสมบัติของความสับสน (confusion property) และคุณสมบัติของการแพร่ (diffusion property) และสามารถใช้ได้กับภาพทุกประเภท

คำสำคัญ : เซลลูลาร์ออโตมาตาแบบพื้นฐาน, การเข้ารหัสรูปภาพ

Thesis Title	Image Encryption Method Based on Elementary Cellular Automata
Student	Miss. Wanida Kaewburanaprasert
Student ID	52650806
Degree	Master of Science
Program	Computer Science
Year	2011
Thesis Advisor	Asst. Prof. Dr. Nunthika Benjathapanun

ABSTRACT

Recently, several image encryption methods based on cellular automata have been proposed. One technique is to use the state - transition diagram in elementary cellular automata to generate key stream. Nevertheless, the existing scheme has too many weak keys. Therefore, we proposed to extend the use of pseudo random number generator in the initial state of each pixel so that the key space is increased. Then we shift bits of each pixel in order to increase concealment. Our experimental results shown that our method provides better concealment in both confusion and diffusion aspects with all types of images.

Keywords : elementary cellular automata, image encryption

กิตติกรรมประกาศ

วิทยานิพนธ์นี้มิอาจจะสำเร็จลุล่วงไปได้ด้วยดี หากมิได้รับคำแนะนำ คำชี้แจง ความรู้ และความเอาใจใส่จาก ผศ.ดร.นันทิกา เบญจเทพานันท์ ผู้เป็นอาจารย์ที่ปรึกษา ซึ่งท่านได้สละเวลาให้กับข้าพเจ้าอย่างเต็มที่ จึงใคร่ขอขอบพระคุณเป็นอย่างสูง

ขอขอบพระคุณ ผศ.ดร.กรกช ประชุมรักษ์ ดร.รุ่งรัตน์ เวียงศรีพนาวัลย์ และรศ.ดร.ดำรัส วงศ์สว่าง คณะกรรมการสอบหัวข้อ และโครงร่างวิทยานิพนธ์ ที่กรุณาให้คำแนะนำตลอดจนข้อชี้แนะจนในที่สุดทำให้วิทยานิพนธ์ฉบับนี้สำเร็จลงได้

ขอขอบพระคุณบิดา มารดา และพี่ ที่สนับสนุนให้ได้เรียนในระดับที่ได้ตั้งใจ อีกทั้งยังได้ดูแลเรื่องค่าใช้จ่ายต่างๆ ระหว่างศึกษาเป็นอย่างดีอีกด้วย

ขอขอบคุณเพื่อนๆ ร่วมรุ่น และพี่น้องทุกคนที่ให้คำปรึกษา และช่วยอำนวยความสะดวกในด้านต่างๆ

สำหรับคุณงามความดีและประโยชน์อันใดที่เกิดขึ้นจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดา มารดา อาจารย์ทุกท่านซึ่งเป็นที่เคารพรักยิ่ง ตลอดจนญาติพี่น้อง รุ่นพี่และเพื่อนๆ ที่รักทุกคน

วนิดา แก้วบูรณะประเสริฐ

พฤษภาคม 2554

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

วิธีการแลกเปลี่ยนข้อมูลที่สำคัญในปัจจุบันที่เป็นที่นิยมวิธีหนึ่งคือการส่งข้อมูลผ่านทางอินเตอร์เน็ท ซึ่งเป็นช่องทางการติดต่อสื่อสารแบบสาธารณะที่ผู้ใช้ทุกคนสามารถเข้าถึงข้อมูลทั้งหมดได้และถือว่าเป็นช่องทางการส่งข้อมูลที่ไม่ปลอดภัย แต่เนื่องจากเป็นยุคของสังคมออนไลน์ที่มีการติดต่อสื่อสารและแลกข้อมูลข่าวสารผ่านทางอินเตอร์เน็ทกันมากขึ้น ดังนั้นผู้ใช้บางกลุ่มจึงไม่มีทางหลีกเลี่ยงการส่งผ่านข้อมูลส่วนตัวหรือข้อมูลสำคัญผ่านช่องทางนี้ได้ เช่น การกรอกข้อมูลที่อยู่และข้อมูลบัตรเครดิต เพื่อสั่งซื้อของผ่านทางอินเตอร์เน็ท การกรอกข้อมูลประวัติในการสมัรงานผ่านทางอินเตอร์เน็ทเป็นต้น นอกจากนี้ยังมีผู้ใช้บางกลุ่มที่ต้องการส่งข้อมูลบางอย่างให้เฉพาะคนรู้จักเท่านั้น ไม่ต้องการให้ผู้ที่ไม่รู้จักมาเห็นข้อมูลเหล่านี้ เช่นการส่งรูปภาพหรือวีดีโอส่วนตัวให้กับเพื่อนที่รู้จักได้ดู การคุยกันผ่านทางโปรแกรมออนไลน์ เป็นต้น ถ้าไม่มีระบบรักษาความปลอดภัยที่ดีพอก็สามารถทำให้ข้อมูลสำคัญเหล่านี้รั่วไหลได้

วิธีการหนึ่งซึ่งเป็นที่นิยมในการแก้ปัญหาเรื่องความปลอดภัยของข้อมูลคือการเข้ารหัสข้อมูล ซึ่งทำให้ผู้อื่นไม่สามารถเข้าถึงข้อมูลส่วนตัวหรือข้อมูลสำคัญได้ที่เข้ารหัสเอาไว้ได้ ยกเว้นเฉพาะผู้ที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น ซึ่งวิธีการที่ใช้ในการเข้ารหัสจะแตกต่างกันไปตามประเภทของข้อมูล สำหรับการเข้ารหัสข้อมูลประเภทรูปภาพปัญหาสำคัญคือความรวดเร็วในการเข้ารหัสเนื่องจากข้อมูลประเภทรูปภาพส่วนใหญ่แล้วจะมีขนาดใหญ่มาก ใช้เวลาในการประมวลผลนานจึงไม่เหมาะกับวิธีการเข้ารหัสข้อมูลแบบทั่วไป นอกจากนี้ยังมีรูปแบบการเก็บข้อมูลที่แตกต่างจากข้อมูลอื่นๆ ทั่วไป จึงได้มีการนำเซลลูลาร์ออโตมาตา (Cellular Automata) มาใช้ในการเข้ารหัสรูปภาพ เพราะมีคุณสมบัติที่สามารถนำไปปรับใช้กับฮาร์ดแวร์ได้โดยตรง รวมทั้งยังสามารถทำการประมวลผลแบบขนาน (parallel processing) ได้ด้วย จึงทำให้สามารถเข้ารหัสได้อย่างรวดเร็วยิ่งขึ้น

งานวิจัยที่นำเซลลูลาร์ออโตมาตามาใช้ในการเข้ารหัสรูปภาพมีอยู่เป็นจำนวนมากหนึ่งในนั้นคืองานวิจัยของ Jin [4] ซึ่งพบว่าแผนภาพการเปลี่ยนสถานะของเซลลูลาร์ออโตมาตาแบบพื้นฐานบางสถานะมีคุณสมบัติพิเศษคือ แผนภาพการเปลี่ยนสถานะจะวนกลับมาที่สถานะเริ่มต้นและนำคุณสมบัตินี้มาสร้างเป็นกุญแจในขั้นตอนการเข้ารหัสภาพสีเทา การศึกษางานวิจัยนี้พบว่ากุญแจบางกุญแจที่ตรงตามคุณสมบัติพิเศษนี้ไม่สามารถปกปิดภาพได้ ดังนั้นจึงต้องมีการปรับปรุงวิธีการเข้ารหัสใหม่เพื่อใหม่มีประสิทธิภาพที่ดีกว่าเดิม

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

งานวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนาขั้นตอนวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาที่มีอยู่แล้วให้มีประสิทธิภาพที่ดียิ่งขึ้น เพื่อเพิ่มความปลอดภัยให้กับข้อมูลด้วยการเพิ่มจำนวนกุญแจลับทั้งหมดที่เป็นไปได้ (key space) ของวิธีการเข้ารหัส และเพิ่มขั้นตอนการสลับที่บิต (bit) ของค่าความเข้มแสงเข้าไปในขั้นตอนการเข้ารหัสรูปภาพ เพื่อเพิ่มความสามารถในการปกปิดข้อมูลให้ดียิ่งขึ้นกว่าเดิม

1.3 สมมติฐานของการศึกษา

การเพิ่มจำนวนกุญแจลับทั้งหมดที่เป็นไปได้ของวิธีการเข้ารหัส ทำให้โอกาสที่ผู้โจมตีจะค้นพบกุญแจที่ใช้ในการเข้ารหัสเป็นไปได้ยากขึ้น และส่งผลให้ข้อมูลมีความปลอดภัยเพิ่มมากขึ้น รวมทั้งการเพิ่มขั้นตอนการสลับที่บิตของค่าความเข้มแสงเข้าไปในขั้นตอนการเข้ารหัสรูปภาพ ทำให้ข้อมูลมีการเปลี่ยนแปลงมากขึ้น และส่งผลให้ปกปิดข้อมูลให้ดีขึ้น และข้อมูลมีความปลอดภัยมากขึ้น

1.4 ขอบเขตการศึกษา

ขอบเขตของงานวิจัยมีรายละเอียดดังต่อไปนี้

1. ขั้นตอนวิธีการเข้ารหัสรูปภาพใช้ในการเข้ารหัสรูปภาพประเภทภาพสีเทา (grayscale image) และภาพสี (color image)

2. ภาพสีเทาที่ใช้ในการเข้ารหัสจะต้องมีค่าความเข้มแสงที่มีค่าความลึกของบิต (bit depth) เท่ากับ 8 หรือค่าความเข้มแสงของแต่ละจุดภาพ (pixel) ต้องมีค่าอยู่ระหว่าง 0 ถึง 255

3. ภาพสีที่ใช้ในการเข้ารหัสต้องเป็นภาพในระบบ RGB และมีค่าความเข้มแสงของแต่ละสีที่มีค่าความลึกของบิต (bit depth) เท่ากับ 8 หรือค่าความเข้มแสงของแต่ละสีของแต่ละจุดภาพ (pixel) ต้องมีค่าอยู่ระหว่าง 0 ถึง 255

4. เครื่องมือที่ใช้ในการประมวลผลภาพและพัฒนาโปรแกรมการเข้ารหัสและถอดรหัส คือ โปรแกรม Matlab รุ่น 7.11.0 (R2010b)

1.5 ขั้นตอนการศึกษาและดำเนินงานวิจัย

ขั้นตอนการศึกษาและดำเนินงานวิจัย มีดังต่อไปนี้

1. ศึกษาขั้นตอนวิธีการประมวลผลภาพเบื้องต้น รวมถึงศึกษาทฤษฎีเบื้องต้นเกี่ยวกับเซลลูลาร์ออโตมาตา และวิทยาการเข้ารหัสลับ (Cryptography)

2. ศึกษางานวิจัยที่เกี่ยวข้องกับการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตา

3. ตั้งสมมติฐานโดยคาดว่าการเพิ่มจำนวนกุญแจลับทั้งหมดที่เป็นไปได้ของวิธีการเข้ารหัสและการเพิ่มขั้นตอนการสลับที่บิตของค่าความเข้มแสงเข้าไปในขั้นตอนการเข้ารหัสรูปภาพ ทำให้วิธีการเข้ารหัสมีประสิทธิภาพมากขึ้น และเพิ่มความปลอดภัยของข้อมูลจากการถูกโจมตี

4. นำเสนอวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานที่ได้ปรับปรุงแล้ว

5. พัฒนาโปรแกรมตามวิธีการที่ได้นำเสนอ

6. วิเคราะห์ผลการทดลอง

7. สรุปผลการทดลองพร้อมเสนอแนวทางการพัฒนางานวิจัย

8. เขียนวิทยานิพนธ์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับจากการศึกษาและปรับปรุงขั้นตอนวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน มีดังต่อไปนี้

1. สามารถเข้ารหัสและถอดรหัสรูปภาพได้ทั้งภาพสีและภาพสีเทา
2. นำไปใช้เป็นแนวทางในการพัฒนาขั้นตอนวิธีการเข้ารหัสการเข้ารหัสรูปภาพด้วยวิธีอื่น
3. นำไปใช้เป็นแนวทางในการพัฒนาตัวสร้างเลขสุ่มเทียม
4. นำไปใช้เป็นแนวทางในการพัฒนาขั้นตอนวิธีการเข้ารหัสข้อมูลทั่วไป

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การศึกษางานวิจัยต่างๆ ที่ใช้เซลลูลาร์ออโตมาตาในการเข้ารหัสรูปภาพ ต้องอาศัยความรู้เบื้องต้นในหลากหลายสาขา เช่น ความรู้พื้นฐานเกี่ยวกับการประมวลผลภาพ (Image Processing) เซลลูลาร์ออโตมาตา และความรู้เบื้องต้นเกี่ยวกับการเข้ารหัส (Cryptography) เป็นต้น ดังนั้นในบทนี้จะอธิบายถึงงานวิจัยที่เกี่ยวข้องกับการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตา และทฤษฎีพื้นฐานต่างๆ ที่เกี่ยวข้องดังต่อไปนี้

2.1 การประมวลผลภาพดิจิตอล

2.1.1 ภาพดิจิตอล (Digital image)

นิยามของภาพดิจิตอลคือ ฟังก์ชัน 2 มิติ $f(x,y)$ ของค่าความเข้มแสง โดยมี x และ y เป็นตัวบอกตำแหน่งในระบบพิกัดฉาก [17] โดยค่าทั้งหมดนี้เป็นจำนวนเต็มบวกและเป็นจำนวนจำกัด ค่า $f(x,y)$ ถูกจัดเก็บอยู่ในรูปของแถวลำดับ (Array) 2 มิติ แต่ละตำแหน่ง (x,y) ของแถวลำดับเรียกว่าจุดภาพ (Pixel) [5]

2.1.2 ความลึกของบิต (bit depth)

ค่าความลึกของบิตคือจำนวนบิตที่ใช้ในการเก็บค่าความเข้มแสงของแต่ละจุดภาพ บอกถึงจำนวนของค่าความเข้มแสงทั้งหมดที่เป็นไปได้และค่าความเข้มแสงสูงสุดด้วย ตัวอย่างเช่นค่าความลึกของบิตเท่ากับ 1 หมายความว่าใน 1 จุดภาพใช้บิตในการเก็บค่าความเข้มแสงจำนวน 1 บิต ค่าความเข้มแสงทั้งหมดเท่ากับ 2^1 หรือเท่ากับ 2 และมีค่าความเข้มแสงสูงสุดเท่ากับ 2^1-1 หรือเท่ากับ 1 แต่ถ้าค่าความลึกของบิตเท่ากับ 8 ค่าความเข้มแสงทั้งหมดเท่ากับ 2^8 หรือเท่ากับ 256 และมีค่าสูงสุดเท่ากับ 2^8-1 หรือเท่ากับ 255

2.1.3 ประเภทสีของภาพ

ประเภทสีของภาพขึ้นอยู่กับค่าความลึกของบิตและระบบการจัดเก็บข้อมูลรูปภาพ ประเภทสีของภาพมีนิยามไว้หลากหลายรูปแบบ แต่ที่นิยมใช้เป็นส่วนใหญ่มีอยู่ 3 รูปแบบด้วยกัน ได้แก่ ประเภทภาพขาวดำ (binary image) ประเภทภาพสีเทา (grayscale image หรือ gray – level image) และประเภทภาพสี (color image)

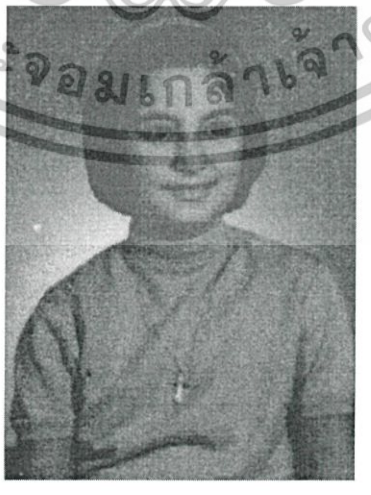
2.1.3.1 ประเภทภาพขาวดำ

ภาพขาวดำมีค่าความลึกของบิตเท่ากับ 1 [14] ดังนั้นค่าความเข้มของแสงมีเพียง 2 ค่าเท่านั้น คือ 0 ซึ่งมีค่าเท่ากับสีดำ และ 1 ซึ่งมีค่าเท่ากับสีขาว ระบบการจัดเก็บข้อมูลใช้แถวลำดับเพียงชุดเดียวในการเก็บข้อมูลความเข้มแสง

รูปที่ 2.1 ตัวอย่างภาพขาวดำ [5]

2.1.3.2 ประเภทภาพสีเทา

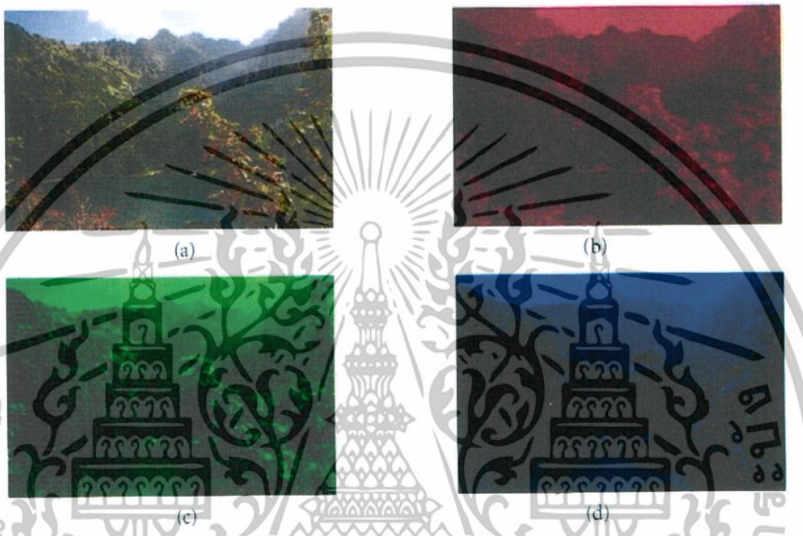
ภาพสีเทามีค่าความลึกของบิตตั้งแต่ 2 ขึ้นไป [14] และค่าที่นิยมใช้กันมากที่สุดคือ 8 ดังนั้นค่าความเข้มแสงมีทั้งหมด 256 ค่า คือตั้งแต่ 0 จนถึง 255 และใช้ระบบการจัดเก็บข้อมูลแบบเดียวกับภาพขาวดำ



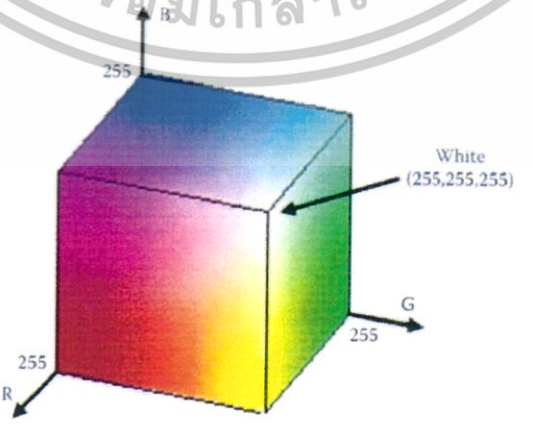
รูปที่ 2.2 ตัวอย่างภาพสีเทา [5]

2.1.3.3 ประเภทภาพสี

ภาพสีมีลักษณะคล้ายกับภาพสีเทาคือมีค่าความลึกของบิตเท่ากัน แต่มีระบบการจัดเก็บค่าความเข้มแสงแตกต่างกัน ระบบที่ใช้กับภาพสีเรียกว่าระบบ RGB คือใช้แถวลำดับจำนวน 3 ชุดในการเก็บค่าความเข้มแสง โดยชุดแรกเก็บค่าความเข้มแสงสีแดง (red) ชุดที่สองเก็บค่าความเข้มแสงสีเขียว (green) และชุดสุดท้ายเก็บค่าความเข้มแสงสีน้ำเงิน (blue) เมื่อนำแต่ละสีในตำแหน่งเดียวกันมาผสมกันจะได้สีของภาพในตำแหน่งนั้น



รูปที่ 2.3 ตัวอย่างภาพสี [14] (a) ตัวอย่างภาพสี
(b) แสดงเฉพาะค่าความเข้มแสงสีแดง
(c) แสดงเฉพาะค่าความเข้มแสงสีเขียว
(d) แสดงเฉพาะค่าความเข้มแสงสีน้ำเงิน

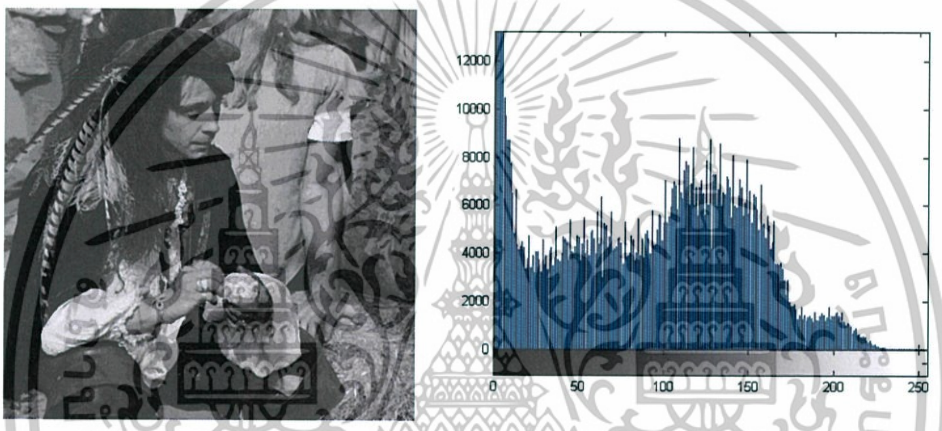


รูปที่ 2.4 สีที่ได้จากการผสมค่าความเข้มแสงทั้งสามสี เมื่อค่าความลึกของบิตเท่ากับ 8 [14]

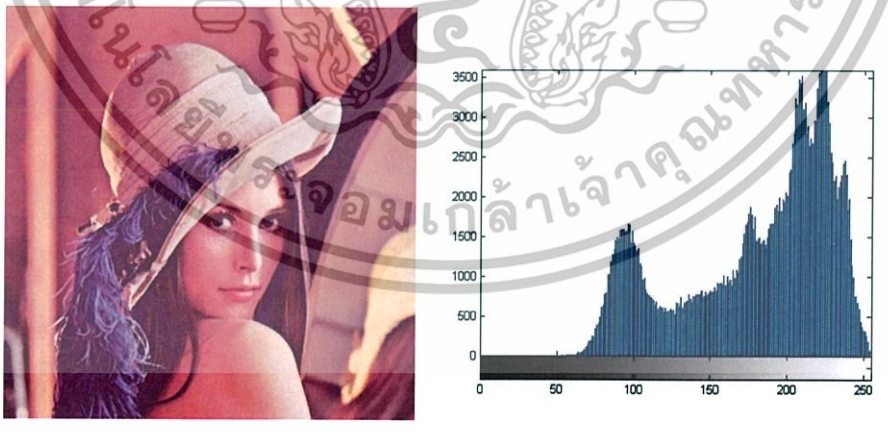
2.1.4 ฮิสโทแกรม (histogram)

ฮิสโทแกรมเป็นกราฟของฟังก์ชัน $f(x)$ แสดงความสัมพันธ์ระหว่างค่าความเข้มแสงกับจำนวนจุดภาพ เมื่อ x คือค่าความเข้มของแสงและ $f(x)$ คือจำนวนจุดภาพทั้งหมดในภาพที่มีค่าความเข้มแสงเท่ากับ x ฮิสโทแกรมเป็นข้อมูลสำคัญที่นำไปใช้ในการปรับปรุงคุณภาพของภาพ นอกจากนี้ยังแสดงถึงลักษณะการกระจายตัวของความเข้มแสงภายในภาพอีกด้วย

ในกรณีที่เป็นภาพขาวดำหรือภาพสีเทาฮิสโทแกรมจะมีเพียงกราฟเดียวเนื่องจากมีการเก็บค่าความเข้มของแสงเพียงชุดเดียว แต่ถ้าเป็นภาพสีจะมี 3 กราฟเพราะเก็บค่าความเข้มแสงไว้ 3 ชุด คือสีแดง สีเขียว และสีน้ำเงิน

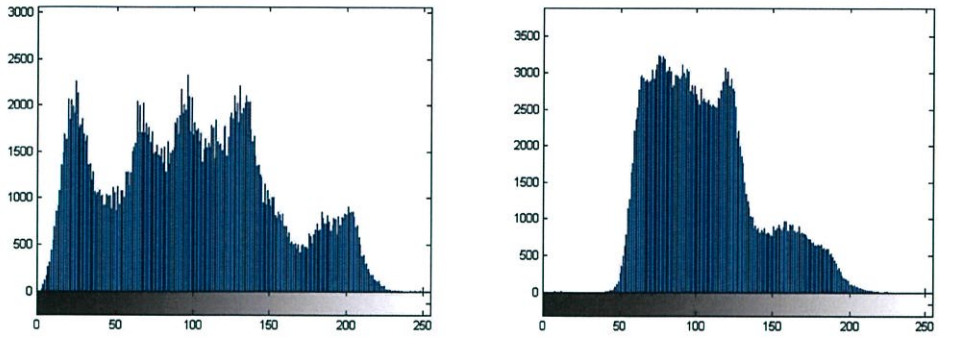


รูปที่ 2.5 ฮิสโทแกรมของภาพสีเทา



(a) (b)

รูปที่ 2.6 ฮิสโทแกรมของภาพสี (a) ภาพสีที่ใช้หาฮิสโทแกรม
(b) ฮิสโทแกรมสีแดงของภาพ (a)



(c) (d)

รูปที่ 2.6(ต่อ) (c) ฮิสโทแกรมสีเขียวของภาพ (a) (d) ฮิสโทแกรมสีน้ำเงินของภาพ (a)

2.2 เซลลูลาร์ออโตมาตา

เซลลูลาร์ออโตมาตาเป็นแบบจำลองทางคณิตศาสตร์ที่อธิบายถึงระบบต่างๆ ในธรรมชาติ ได้ถูกนำเสนอเป็นครั้งแรกโดย J. von Neumann และ Ulam ในชื่อ เซลลูลาร์สเปซ (cellular spaces) เพื่อสร้างเป็นแบบจำลองทางชีววิทยา หลังจากนั้นได้ถูกนำไปใช้กับงานหลากหลายรูปแบบ [13] ดังนั้นจึงทำให้เซลลูลาร์ออโตมาตามีความแตกต่างกันตามลักษณะการนำไปใช้ แต่มีลักษณะสำคัญที่เหมือนกันคือมีพื้นที่และเวลาเป็นแบบไม่ต่อเนื่อง (discrete) ประกอบด้วยแถวลำดับของเซล (cell) โดยปกติแล้วสามารถขยายได้ไม่จำกัด แต่ละเซลมีสถานะ (state) ของตัวเอง เซต (set) ของสถานะเป็นแบบจำกัดและเป็นจำนวนไม่ต่อเนื่อง เมื่อเซลลูลาร์ออโตมาตาพัฒนา (evolve) จากเวลา t ไปเป็นเวลา $t+1$ สถานะใหม่ของเซลจะถูกกำหนดโดยสถานะในช่วงเวลา t ของเซลที่อยู่ใกล้เคียงกัน ที่เรียกว่าย่านใกล้เคียง (neighborhood) โดยแต่ละเซลจะมีฟังก์ชันที่ใช้กำหนดค่าสถานะใหม่ตามสถานะของย่านใกล้เคียงเรียกว่ากฎ (rule) หรือสามารถเขียนในรูปสมการได้ว่า

$$s_i^{t+1} = f_i\left(s_{neighborhood}^{t}\right) \tag{2.1}$$

เมื่อ s_i^{t+1} คือ สถานะของเซลที่ i ในช่วงเวลา $t+1$

f_i คือ กฎของเซลที่ i

$s_{neighborhood}^{t}$ คือ สถานะของย่านใกล้เคียงของเซล i ในช่วงเวลา t

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

รูปที่ 2.7 เซลลูลาร์ออโตมาตาแบบ 1 มิติ

$t=0$

1	1	1	1	0	1	1	0
0	1	0	1	0	0	0	1
1	0	1	1	0	1	0	0
1	0	0	0	0	0	1	1
1	0	0	0	1	1	1	1
0	1	0	0	1	0	1	0
0	0	1	0	1	1	1	0
1	1	1	1	0	0	0	1

$t=1$

0	1	1	1	1	0	0	0
0	0	1	0	1	0	1	0
1	1	1	0	0	0	1	1
0	1	1	0	1	0	0	1
1	0	0	0	0	1	0	1
1	1	0	1	0	0	0	0
0	0	0	0	1	0	1	1
1	0	1	0	0	0	1	0

รูปที่ 2.8 เซลลูลาร์ออโตมาตาแบบ 2 มิติ

จากรูป 2.7 และ 2.8 เป็นตัวอย่างของเซลลูลาร์ออโตมาตา ช่องสี่เหลี่ยมแต่ละช่องคือเซล และตัวเลขที่อยู่ในแต่ละเซลคือสถานะของเซล ทั้งสองรูปมีเซตของสถานะเหมือนกัน คือ $\{0,1\}$ เมื่อเซลลูลาร์ออโตมาตาพัฒนาจากเวลา 0 ไปเป็นเวลา 1 ค่าสถานะของแต่ละเซลมีการเปลี่ยนแปลงตามกฎของแต่ละเซล บางครั้งเซลสองเซลที่มีค่าสถานะของย่านใกล้เคียงเหมือนกันแต่ ค่าสถานะของช่วงเวลาต่อไปมีค่าไม่เท่ากัน เนื่องจากทั้งสองเซลมีกฎที่แตกต่างกัน

เซลลูลาร์ออโตมาตาที่มีรูปแบบแตกต่างกันลักษณะของย่านใกล้เคียงและกฎของแต่ละเซลจะมีรูปแบบที่แตกต่างกันไปด้วย ตัวอย่างของเซลลูลาร์ออโตมาตารูปแบบต่างๆ มีดังต่อไปนี้

2.2.1 เซลลูลาร์ออโตมาตาแบบพื้นฐาน

เซลลูลาร์ออโตมาตาแบบพื้นฐานเป็นเซลลูลาร์ออโตมาตาที่มีรูปแบบอย่างง่ายที่สุด แถวลำดับของเซลเป็นแบบ 1 มิติ เซตของสถานะคือ $\{0,1\}$ หรือใช้สีขาวแทนค่าสถานะเท่ากับ 0 และสี

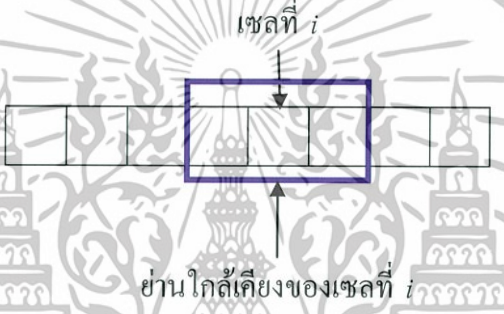
ดำแทนแทนสถานะเท่ากับ 1 ย่านใกล้เคียงของเซลประกอบด้วยเซล 3 เซล คือ เซลที่อยู่ด้านซ้ายของเซล เซลที่อยู่ด้านขวาของเซล และตัวเซลนั้นเอง (ตามรูป 2.9) กฎที่กำหนดให้กับเซลทุกๆ เซลจะใช้กฎเดียวกันหมด สามารถเขียนรูปสมการได้ว่า

$$s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t) \tag{2.2}$$

เมื่อ s_i^{t+1} คือ สถานะของเซลที่ i ในช่วงเวลา $t+1$

f คือ กฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

s_{i-1}^t, s_i^t และ s_{i+1}^t คือ สถานะของย่านใกล้เคียงของเซลที่ i ในช่วงเวลา t

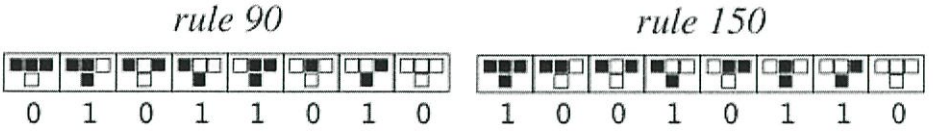


รูปที่ 2.9 ย่านใกล้เคียงของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

จากจำนวนเซลของย่านใกล้เคียงของเซลลูลาร์ออโตมาตาที่มี 3 เซล แต่ละเซลมีสถานะที่เป็นไปได้ทั้งหมด 2 สถานะ ดังนั้นแต่ละกฎจะต้องมีค่าของสถานะของย่านใกล้เคียงทั้งหมดที่เป็นไปได้ทั้งหมด 2^3 หรือ 8 ค่า และแต่ละค่าสามารถกำหนดค่าสถานะต่อไปได้อีก 2 ค่า ดังนั้นจำนวนกฎทั้งหมดที่เป็นไปได้ของเซลลูลาร์ออโตมาตาแบบพื้นฐานคือ $2^{2^3} = 2^8$ หรือ 256 กฎ

ตารางที่ 2.1 ตัวอย่างกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

สถานะของย่านใกล้เคียง	111	110	101	100	011	010	001	000
สถานะต่อไปของกฎ 90	0	1	0	1	1	0	1	0
สถานะต่อไปของกฎ 150	1	0	0	1	0	1	1	0



(a) (b)

รูปที่ 2.10 ตัวอย่างกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐานในแบบรูปภาพ [15]
(a) กฎ 90 (b) กฎ 150

จากตัวอย่างกฎของเซลลูลาร์ออโตมาตาในตาราง 2.1 เมื่อเรานำค่าสถานะของย่านใกล้เคียงที่เปลี่ยนเป็นเลขฐาน 10 มาเป็นเลขชี้กำลังของเลขยกกำลังที่มีเลขฐานเป็น 2 จากนั้นนำค่าเลขยกกำลังที่ได้ ไปคูณกับค่าสถานะในช่วงเวลาต่อไปของค่าสถานะของย่านใกล้เคียงนั้น แล้วนำค่าของทุกย่านใกล้เคียงของกฎที่คำนวณได้มาบวกกัน จะได้เป็นเลขฐาน 10 ที่เป็นชื่อเรียกของกฎนั้น

ในทางกลับกันเมื่อรู้ชื่อของกฎเป็นเลขฐาน 10 เราสามารถแปลงออกมาอยู่ในรูปของฟังก์ชันได้โดยเปลี่ยนกฎให้อยู่ในรูปของเลขฐาน 2 จะได้เป็นสถานะของช่วงเวลาต่อไปจำนวน 8 สถานะ และหาค่าสถานะของย่านใกล้เคียงของแต่ละสถานะต่อไปโดยแปลงค่าประจำตำแหน่งของแต่ละสถานะให้อยู่ในรูปเลขยกกำลังฐาน 2 แล้วนำเลขชี้กำลังมาแปลงเป็นเลขฐาน 2 จะได้เป็นค่าสถานะของย่านใกล้เคียงของสถานะในช่วงเวลาถัดไปนั้น

ตารางที่ 2.2 ขั้นตอนการแปลงกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐานเป็นเลขฐาน 10

สถานะย่านใกล้เคียง	สถานะต่อไป	
111	0	$\longrightarrow 111_2 = 7 \longrightarrow 2^7 \longrightarrow 0 \times 2^7 \longrightarrow 0$
110	1	$\longrightarrow 110_2 = 6 \longrightarrow 2^6 \longrightarrow 1 \times 2^6 \longrightarrow 64$
101	0	$\longrightarrow 101_2 = 5 \longrightarrow 2^5 \longrightarrow 1 \times 2^5 \longrightarrow 0$
100	1	$\longrightarrow 100_2 = 4 \longrightarrow 2^4 \longrightarrow 1 \times 2^4 \longrightarrow 16$
011	1	$\longrightarrow 011_2 = 3 \longrightarrow 2^3 \longrightarrow 1 \times 2^3 \longrightarrow 8$
010	0	$\longrightarrow 010_2 = 2 \longrightarrow 2^2 \longrightarrow 0 \times 2^2 \longrightarrow 0$
001	1	$\longrightarrow 001_2 = 1 \longrightarrow 2^1 \longrightarrow 1 \times 2^1 \longrightarrow 2$
000	0	$\longrightarrow 000_2 = 0 \longrightarrow 2^0 \longrightarrow 0 \times 2^0 \longrightarrow 0$
		$64+16+8+2=90$

ตารางที่ 2.3 ขั้นตอนการแปลงเลขฐาน 10 เป็นกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

$90 = 01011010_2$				
	ค่าประจำตำแหน่ง		สถานะย่านใกล้เคียง	สถานะต่อไป
0	128	$\longrightarrow 2^7 \longrightarrow 7 = 111_2 \longrightarrow$	111	0
1	64	$\longrightarrow 2^6 \longrightarrow 6 = 110_2 \longrightarrow$	110	1
0	32	$\longrightarrow 2^5 \longrightarrow 5 = 101_2 \longrightarrow$	101	0
1	16	$\longrightarrow 2^4 \longrightarrow 4 = 100_2 \longrightarrow$	100	1
1	8	$\longrightarrow 2^3 \longrightarrow 3 = 011_2 \longrightarrow$	011	1
0	4	$\longrightarrow 2^2 \longrightarrow 2 = 010_2 \longrightarrow$	010	0
1	2	$\longrightarrow 2^1 \longrightarrow 1 = 001_2 \longrightarrow$	001	1
0	1	$\longrightarrow 2^0 \longrightarrow 0 = 000_2 \longrightarrow$	000	0

2.2.2 เซลลูลาร์ออโตมาตาแบบ 2 มิติ

เซลลูลาร์ออโตมาตาแบบ 2 มิติส่วนใหญ่ จะกำหนดเซตของสถานะเป็น $\{0,1\}$ เช่นเดียวกับเซลลูลาร์ออโตมาตาแบบพื้นฐาน สำหรับย่านใกล้เคียงของเซลลูลาร์ออโตมาตาแบบ 2 มิติที่นิยมใช้มี 2 รูปแบบ (ตามรูป 2.11) ได้แก่ ย่านใกล้เคียงวอนนิวแมน (von Neumann neighborhoods) ที่มีจำนวนเซลทั้งหมด 5 เซล [13] ดังนั้นย่านใกล้เคียงของเซลในตำแหน่งแถวที่ i หลักที่ j คือ

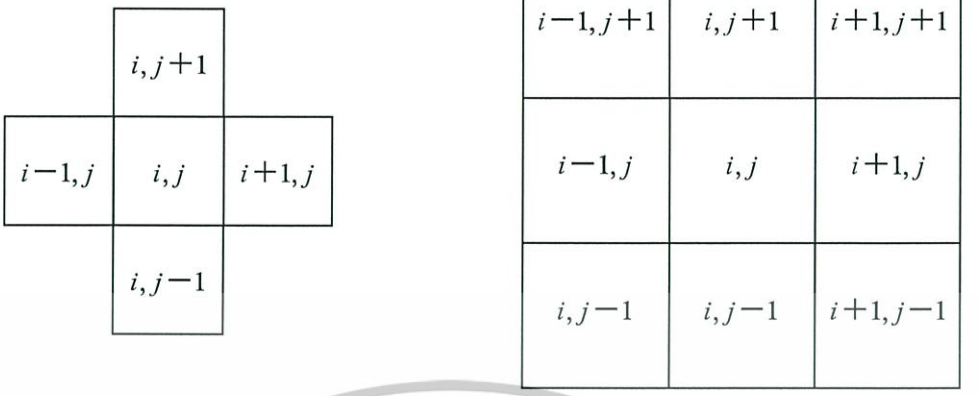
$$\text{neighborhood of } c_{i,j} = \left\{ c_{i,j}, c_{i-1,j}, c_{i+1,j}, c_{i,j-1}, c_{i,j+1} \right\} \tag{2.3}$$

เมื่อ $c_{i,j}$ คือ เซลในตำแหน่งแถวที่ i หลักที่ j

และย่านใกล้เคียงมัวร์ (Moore neighborhoods) ที่มีจำนวนเซลทั้งหมด 9 เซล [13] ดังนั้น ย่านใกล้เคียงของเซลในตำแหน่งแถวที่ i หลักที่ j คือ

$$\text{neighborhood of } c_{i,j} = \left\{ c_{i,j}, c_{i-1,j}, c_{i+1,j}, c_{i,j-1}, c_{i,j+1}, c_{i-1,j-1}, c_{i-1,j+1}, c_{i+1,j-1}, c_{i+1,j+1} \right\} \tag{2.4}$$

เมื่อ $c_{i,j}$ คือ เซลในตำแหน่งแถวที่ i หลักที่ j



รูปที่ 2.11 ย่านใกล้เคียงของเซลลูลาร์ออโตมาตาแบบ 2 มิติ
(a) ย่านใกล้เคียงวอนนิวแมน (b) ย่านใกล้เคียงมัวร์

กฎของเซลลูลาร์ออโตมาตาแบบ 2 มิติ มีหลายรูปแบบ ได้แก่ แบบทั่วไปคือเป็นฟังก์ชันของสถานะของย่านใกล้เคียง หรือแบบโทเทิลลิสติก (totalistic rule) ที่เป็นฟังก์ชันของผลรวมของสถานะของย่านใกล้เคียง เป็นต้น สำหรับกฎแบบทั่วไปสามารถเขียนเป็นสมการได้ว่า

$$s_{i,j}^{t+1} = f\left(s_{neighborhood}^{t}\right) \tag{2.5}$$

เมื่อ $s_{i,j}^{t+1}$ คือ สถานะของเซลในแถวที่ i หลักที่ j ในช่วงเวลา $t+1$

$s_{neighborhood}^{t}$ คือ สถานะของย่านใกล้เคียงของเซลในแถวที่ i หลักที่ j ในช่วงเวลา t

จำนวนกฎทั้งหมดของกฎแบบทั่วไปสำหรับย่านใกล้เคียงวอนนิวแมนคือ 2^{2^5} หรือ 2^{32} กฎ สำหรับย่านใกล้เคียงมัวร์มีจำนวน 2^{2^9} หรือ 2^{512} กฎ

ในส่วนของกฎแบบโทเทิลลิสติกสามารถเขียนเป็นสมการได้ว่า

$$s_{i,j}^{t+1} = f\left(\sum s_{neighborhood}^{t}\right) \tag{2.6}$$

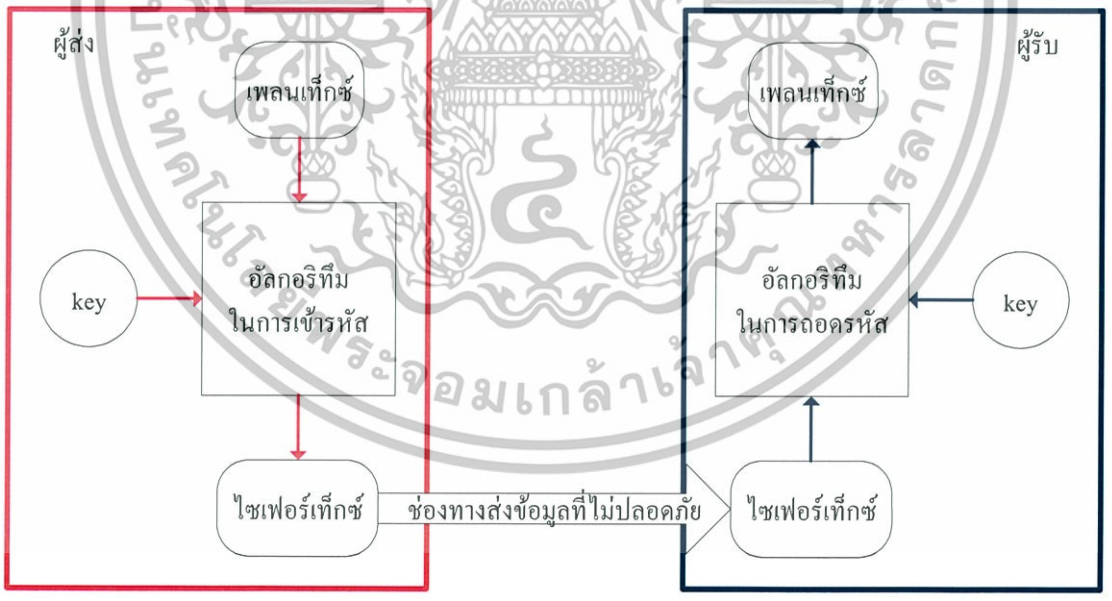
เมื่อ $s_{i,j}^{t+1}$ คือ สถานะของเซลในแถวที่ i หลักที่ j ในช่วงเวลา $t+1$

$\sum s^{t}_{neighborhood}$ คือ ผลรวมของสถานะของย่านใกล้เคียงของเซลในแถวที่ i หลักที่ j ในช่วงเวลา t

จำนวนกฎทั้งหมดของกฎแบบโทเทิลลิสติกสำหรับย่านใกล้เคียงวอนนิวแมนคือ 2^5 หรือ 32 กฎ สำหรับย่านใกล้เคียงมัวร์มีจำนวน 2^9 หรือ 512 กฎ

2.3 ทฤษฎีการเข้ารหัสลับเบื้องต้น

วิทยาการเข้ารหัสลับ (Cryptography) เป็นคำที่มาจากภาษากรีกแปลว่า "การเขียนความลับ" หมายถึง ศาสตร์และศิลป์ในการเปลี่ยนข้อความให้เป็นความลับและปลอดภัยจากการโจมตี [2] ข้อมูลสำคัญที่ผู้ส่งต้องการให้อีกฝ่ายรับรู้เรียกว่าเพลนเท็กซ์ (plaintext) ส่วนข้อความที่นำไปส่งผ่านช่องทางที่ไม่ปลอดภัยเรียกว่าไซเฟอร์เท็กซ์ (ciphertext) ซึ่งเป็นข้อความที่ได้จากการนำเพลนเท็กซ์ผ่านขั้นตอนการเข้ารหัสด้วยอัลกอริทึมในการเข้ารหัส (encryption algorithm) พร้อมกับกุญแจ (key) เมื่อผู้รับได้รับไซเฟอร์เท็กซ์แล้วนำไปผ่านขั้นตอนการถอดรหัสด้วยอัลกอริทึมในการถอดรหัส (decryption algorithm) พร้อมกับกุญแจที่ถูกต้อง ก็จะได้ข้อความเพลนเท็กซ์ที่ผู้ส่งต้องการส่งมาให้



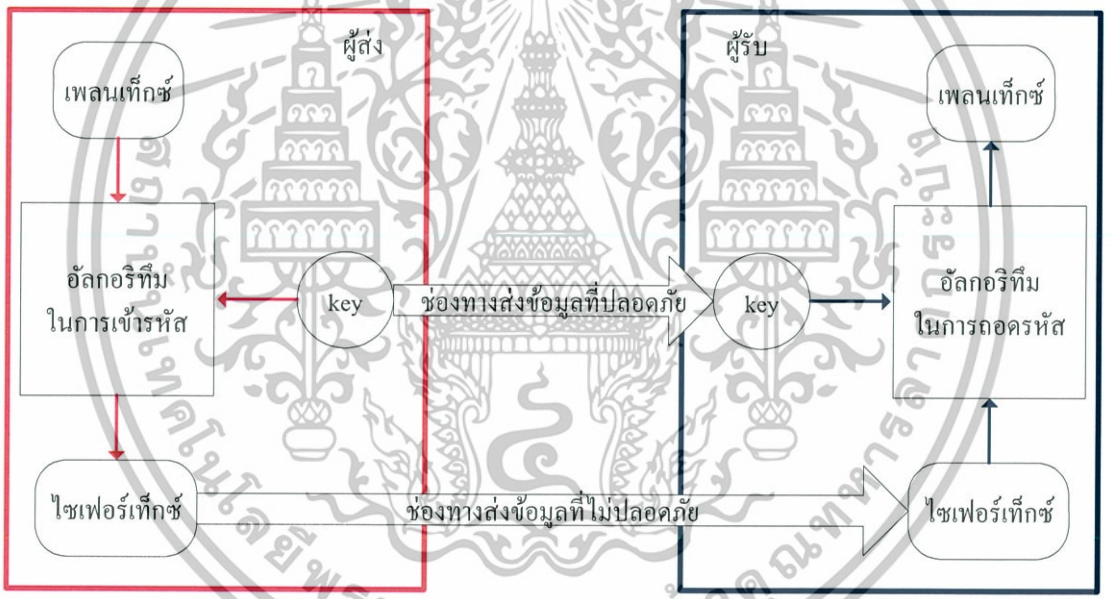
รูปที่ 2.12 การเข้ารหัสและการส่งข้อมูล

ในอดีตมีเพียงการเข้ารหัสและถอดรหัสข้อความด้วยกุญแจลับ (secret key) เท่านั้น แต่ในปัจจุบันกลไกในการเข้ารหัสสามารถแบ่งออกได้เป็น 3 ประเภท ได้แก่ การเข้ารหัสด้วยกุญแจแบบ

สมมาตร (Symmetric – Key Encipherment) การเข้ารหัสด้วยกุญแจแบบไม่สมมาตร (Asymmetric – Key Encipherment) และแฮชชิง (Hashing) [2] โดยในที่นี้จะขอกล่าวถึงเพียง 2 วิธีเท่านั้นคือ การเข้ารหัสด้วยกุญแจแบบสมมาตร และการเข้ารหัสด้วยกุญแจแบบไม่สมมาตร

2.3.1 การเข้ารหัสด้วยกุญแจแบบสมมาตร

การเข้ารหัสด้วยกุญแจแบบสมมาตรมีลักษณะสำคัญคือ กลไกการเข้ารหัสและถอดรหัสจะใช้กุญแจอันเดียวกัน เรียกว่ากุญแจลับ ซึ่งผู้ส่งและผู้รับข้อมูลจะต้องหาช่องทางอื่นที่ปลอดภัยในการแลกเปลี่ยนกุญแจลับเพื่อความปลอดภัย เนื่องจากตามทฤษฎีของ Kerckhoof (Kerckhoof's principle) ผู้ที่ต้องการโจมตีข้อมูลนั้นรู้ขั้นตอนวิธีการเข้ารหัสทั้งหมดแล้ว ยกเว้นเพียงแค่กุญแจที่ใช้ในการถอดรหัสข้อมูลเท่านั้น [2] ดังนั้นถ้าผู้โจมตีได้รับกุญแจลับมาก็สามารถถอดรหัสข้อมูลได้ ทำให้ข้อมูลไม่ปลอดภัย



รูปที่ 2.13 การเข้ารหัสด้วยกุญแจแบบสมมาตรและการส่งข้อมูล

ข้อเสียของวิธีการนี้นอกจากอุปสรรคในการแลกเปลี่ยนกุญแจลับระหว่างผู้รับและผู้ส่งแล้ว ถ้าผู้ส่งต้องการส่งข้อมูลให้กับผู้รับหลายคนโดยที่แต่ละคนจะได้รับข้อมูลไม่เหมือนกัน และไม่ต้องการให้ผู้รับทราบข้อมูลของผู้รับด้วยกันเอง แต่ต้องใช้วิธีการเข้ารหัสแบบเดียวกันผู้ส่งต้องสร้างกุญแจลับไว้ตามจำนวนของผู้รับที่จะได้รับข้อมูล

การเข้ารหัสด้วยกุญแจแบบสมมาตรสามารถแบ่งออกได้เป็น 2 ประเภท คือ สตรีมไซเฟอร์ (stream ciphers) และ บล็อกไซเฟอร์ (block ciphers)

2.3.1.1 สตรีมไซเฟอร์

สตรีมไซเฟอร์เป็นการเข้ารหัสทีละหน่วย เช่น บิต, ไบต์ หรือ คำ เป็นต้น เพลนเท็กซ์ทั้งหมดจะถูกมองเป็นสตรีม (stream) หรือ $P = p_1 p_2 p_3 \ldots p_n$ รวมทั้งกุญแจ $K = k_1 k_2 k_3 \ldots k_n$ และไซเฟอร์เท็กซ์ $C = c_1 c_2 c_3 \ldots c_n$ ที่ถูกมองเป็นสตรีมเช่นเดียวกัน สมการของการเข้ารหัสแบบสตรีมไซเฟอร์ [2] คือ

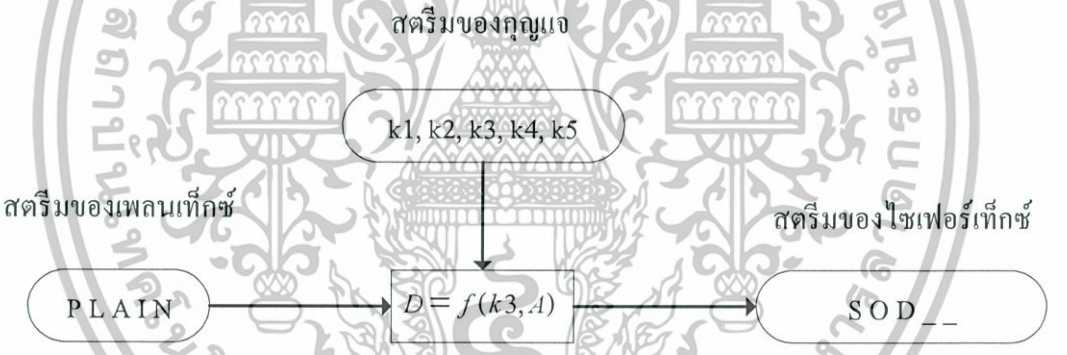
$$c_i = f\left(k_i, p_i\right) \tag{2.7}$$

เมื่อ c_i คือ ค่าในตำแหน่งที่ i ในสตรีมของไซเฟอร์

f คือ ฟังก์ชันในการเข้ารหัส

k_i คือ ค่าในตำแหน่งที่ i ในสตรีมของกุญแจ

p_i คือ ค่าในตำแหน่งที่ i ในสตรีมของเพลนเท็กซ์



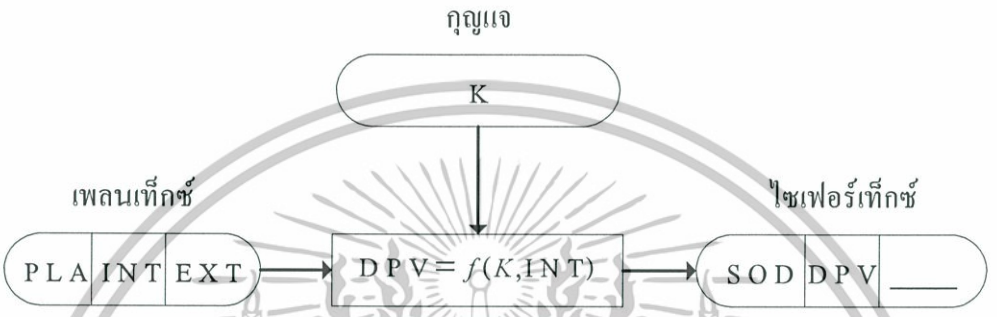
รูปที่ 2.14 การเข้ารหัสของสตรีมไซเฟอร์ในตำแหน่งที่ 3

2.3.1.2 บล็อกไซเฟอร์

บล็อกไซเฟอร์เป็นวิธีการเข้ารหัสที่แบ่งเพลนเท็กซ์ออกเป็นกลุ่มขนาดเท่ากัน แล้วทำการเข้ารหัสทีละกลุ่ม ตามนิยามของบล็อกไซเฟอร์แล้วจะใช้กุญแจเพียงอันเดียวในการเข้ารหัสทุกๆ กลุ่ม บล็อกของไซเฟอร์จะขึ้นอยู่กับบล็อคของเพลนเท็กซ์ ถึงแม้มีเพียงตำแหน่งเดียวในบล็อคของเพลนเท็กซ์มีการเปลี่ยนแปลง อาจส่งผลกระทบกับทุกตำแหน่งในบล็อกของไซเฟอร์เท็กซ์ได้ สมการของการเข้ารหัสแบบบล็อกไซเฟอร์ [2] คือ

$$c_i = f(k, p_i) \tag{2.8}$$

เมื่อ c_i คือ บล็อคที่ i ของไซเฟอร์เท็กซ์
f คือ ฟังก์ชันในการเข้ารหัส
k คือ กุญแจลับ
p_i คือ บล็อคที่ i ของเพลนเท็กซ์



รูปที่ 2.15 การเข้ารหัสบล็อกไซเฟอร์ในตำแหน่งบล็อกที่ 2

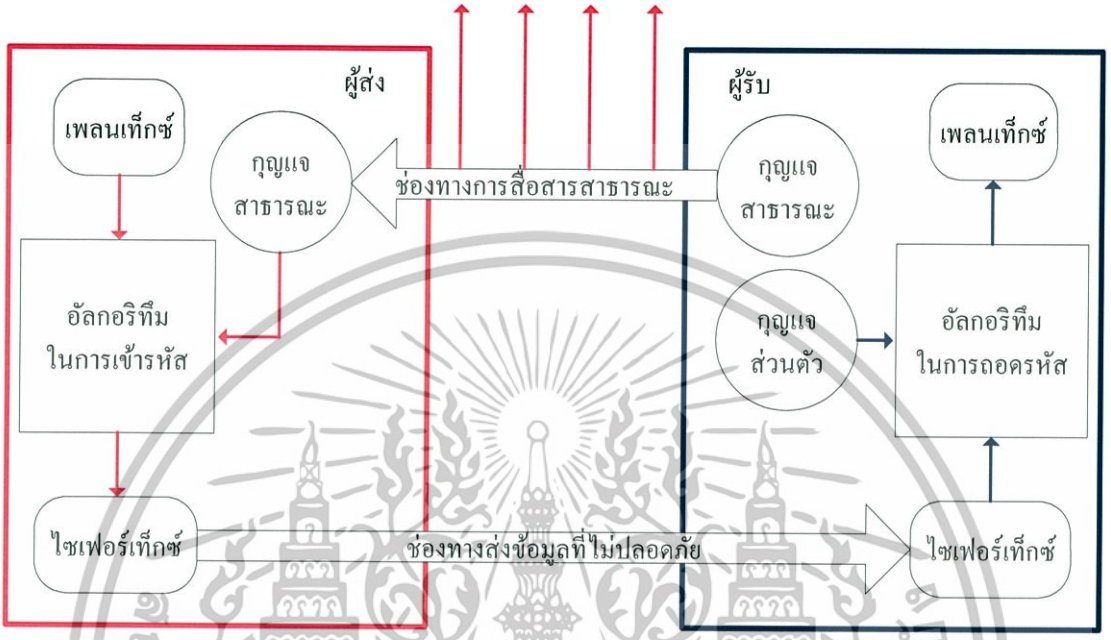
สำหรับขั้นตอนการเข้ารหัสแบบบล็อกไซเฟอร์ควรมีคุณสมบัติสำคัญ 2 อย่าง คือคุณสมบัติของการแพร่ (diffusion) และคุณสมบัติของความสับสน (confusion) คุณสมบัติของการแพร่เป็นความสามารถในการซ่อนความสัมพันธ์ระหว่างไซเฟอร์เท็กซ์กับเพลนเท็กซ์ เพื่อป้องกันการโจมตีจากการใช้วิธีการทางสถิติกับไซเฟอร์เท็กซ์เพื่อค้นหาเพลนเท็กซ์ จากคุณสมบัติของการแพร่ถ้ามีการเปลี่ยนแปลงของเพลนเท็กซ์เพียงเล็กน้อยจะส่งผลกระทบให้มีการเปลี่ยนแปลงในไซเฟอร์เท็กซ์เป็นจำนวนมาก [2]

คุณสมบัติของความสับสนเป็นความสามารถในการซ่อนความสัมพันธ์ระหว่างไซเฟอร์เท็กซ์กับกุญแจลับ เพื่อป้องกันการโจมตีด้วยไซเฟอร์เท็กซ์เพื่อค้นหากุญแจลับ จากคุณสมบัติของความสับสนถ้ามีการเปลี่ยนแปลงของกุญแจลับเพียงเล็กน้อยจะส่งผลกระทบให้มีการเปลี่ยนแปลงในไซเฟอร์เท็กซ์เป็นจำนวนมาก [2]

2.3.2 การเข้ารหัสด้วยกุญแจแบบไม่สมมาตร

การเข้ารหัสด้วยกุญแจแบบไม่สมมาตร ประกอบด้วยกุญแจ 2 แบบ คือ กุญแจสาธารณะ (public key) และกุญแจส่วนตัว (private key) กุญแจสาธารณะเป็นกุญแจที่ใช้ในการเข้ารหัสเพลนเท็กซ์ ส่วนกุญแจส่วนตัวเป็นกุญแจที่ใช้ในการถอดรหัสไซเฟอร์เท็กซ์ ถึงแม้ผู้โจมตีจะรู้กุญแจสาธารณะก็ไม่สามารถถอดรหัสด้วยกุญแจสาธารณะได้ ดังนั้นเมื่อต้องการจะส่งข้อความด้วยวิธีการนี้ ผู้รับข้อความจะต้องประกาศกุญแจสาธารณะให้ผู้ส่งข้อความรู้โดยไม่จำเป็นที่จะต้องใช้

ช่องทางที่ปลอดภัยและต้องเก็บกุญแจส่วนตัวไว้เป็นความลับ ผู้ส่งข้อความจึงนำกุญแจสาธารณะมาใช้กับขั้นตอนวิธีการเข้ารหัสจากนั้นจึงส่งไปยังผู้รับ เมื่อผู้รับได้รับข้อความแล้วจึงนำมาผ่านขั้นตอนการถอดรหัสกับกุญแจส่วนตัว ก็จะได้รับเพลนเท็กซ์ที่ผู้ส่งต้องการส่งมาให้



รูปที่ 2.16 การเข้ารหัสด้วยกุญแจแบบไม่สมมาตรและการส่งข้อมูล

2.4 งานวิจัยที่เกี่ยวข้องกับการเข้ารหัสด้วยเซลลูลาร์ออโตมาตา

จากการศึกษางานวิจัยที่เกี่ยวข้องกับการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตา พบว่าส่วนใหญ่แล้วจะเป็นวิธีการเข้ารหัสด้วยกุญแจแบบสมมาตร นอกจากนี้ยังมีการนำเซลลูลาร์ออโตมาตาไปใช้งานในวัตถุประสงค์ที่แตกต่างกัน ซึ่งสามารถแบ่งออกได้เป็น 2 กลุ่มดังต่อไปนี้

2.4.1 งานวิจัยที่นำเซลลูลาร์ออโตมาตาใช้เป็นขั้นตอนการเข้ารหัส

งานวิจัยในกลุ่มนี้เป็นงานวิจัยที่นำเซลลูลาร์ออโตมาตามาใช้เพื่อเป็นส่วนหนึ่งของฟังก์ชันที่ใช้ในการเข้ารหัส โดยส่วนใหญ่จะใช้เพลนเท็กซ์เป็นสถานะเริ่มต้นของเซลลูลาร์ออโตมาตา แล้วใช้การเปลี่ยนสถานะของเซลลูลาร์ออโตมาตาเป็นฟังก์ชันในการเข้ารหัสเพื่อให้ได้ไซเฟอร์เท็กซ์

ตัวอย่างของงานวิจัยในกลุ่มนี้ ได้แก่ งานวิจัยของ Puhua [8] ซึ่งเป็นหนึ่งในงานวิจัยที่ใช้วิธีการเข้ารหัสด้วยกุญแจแบบไม่สมมาตร แต่ละเซลมีกฎที่แตกต่างกัน ลักษณะเช่นนี้เรียกว่าเซลลูลาร์ออโตมาตาแบบไม่ยูนิฟอร์ม (non – uniform) ฟังก์ชันที่ใช้ในการเข้ารหัสเป็นกฎของเซลลูลาร์ออโตมาตาที่เป็นฟังก์ชันเชิงเส้นบางส่วน (partially linear function) ที่มีคุณสมบัติคือ

กุญแจสาธารณะเป็นฟังก์ชันไม่เชิงเส้น (non linear function) แต่กุญแจส่วนตัวเป็นฟังก์ชันเชิงเส้น จึงทำให้สามารถถอดรหัสได้อย่างรวดเร็ว

งานวิจัยของ F. Maleki และคณะ [3] ใช้เซลลูลาร์ออโตมาตาแบบ 1 มิติแบบไม่ยูนิฟอร์มชนิดพิเศษ ที่กฎของเซลลูลาร์ออโตมาตาใช้สถานะของย่านใกล้เคียงมากกว่า 1 ช่วงเวลา เช่นเดียวกับงานวิจัยของ Maryam และคณะ [6],[7] ที่ใช้กฎของเซลลูลาร์ออโตมาตาในลักษณะเดียวกัน แต่นำมาใช้กับเซลลูลาร์ออโตมาตาแบบ 2 มิติ และใช้ Chaos Mapping ในการเลือกกฎของแต่ละเซล

2.4.2 งานวิจัยที่นำเซลลูลาร์ออโตมาตาสร้างกุญแจ

งานวิจัยในกลุ่มนี้เป็นกลุ่มที่นำเซลลูลาร์ออโตมาตาใช้สร้างเป็นตัวสร้างเลขสุ่มเทียม (pseudo random number generator) เพื่อสร้างสตรีมของกุญแจลับเพื่อใช้ในการเข้ารหัสข้อมูล ตัวอย่างของงานวิจัยในกลุ่มนี้ได้แก่ งานวิจัยของ Zhao และคณะ [16] ใช้เซลลูลาร์ออโตมาตา 1 มิติแบบไม่ยูนิฟอร์ม และใช้เจเนติกอัลกอริทึม (genetic algorithm) ในการเลือกสถานะเริ่มต้นและกฎของแต่ละเซลเพื่อสร้างเลขสุ่มเทียม

งานวิจัยของ Rong – Jian Chen และคณะ [9],[10],[11] ใช้เซลลูลาร์ออโตมาตา 2 มิติแบบยูนิฟอร์ม (uniform) คือ ใช้กฎเดียวกันกับทุกเซลในเซลลูลาร์ออโตมาตาในการสร้างเป็นตัวสร้างเลขสุ่มเทียม และใช้ฟังก์ชันในการเข้ารหัสที่มีความซับซ้อนมาก

และสุดท้ายเป็นงานวิจัยของ Jin [4] ที่แตกต่างจากงานวิจัยอื่นโดยใช้คุณสมบัติพิเศษที่ได้จากแผนภาพการเปลี่ยนสถานะ (state – transition diagram) ของเซลลูลาร์ออโตมาตาแบบพื้นฐาน คืออาศัยคุณสมบัติการวนกลับที่เดิมของแผนภาพการเปลี่ยนสถานะเป็นตัวสร้างเลขสุ่มเทียม

2.5 ขั้นตอนวิธีของงานวิจัยที่เกี่ยวข้อง

สำหรับงานวิจัยที่เกี่ยวข้องในที่นี้หมายถึงงานวิจัยของ Jin [4] ที่ใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานในการเข้ารหัสรูปภาพ โดยข้อดีของวิธีนี้คือสามารถทำงานได้อย่างรวดเร็วถึงแม้ว่ารูปภาพจะมีขนาดใหญ่ก็ตาม แต่ข้อเสียคือมีกุญแจที่ไม่สามารถปกปิดข้อมูลรูปภาพได้มากเกินไป สำหรับรายละเอียดของงานวิจัยนี้มีดังต่อไปนี้

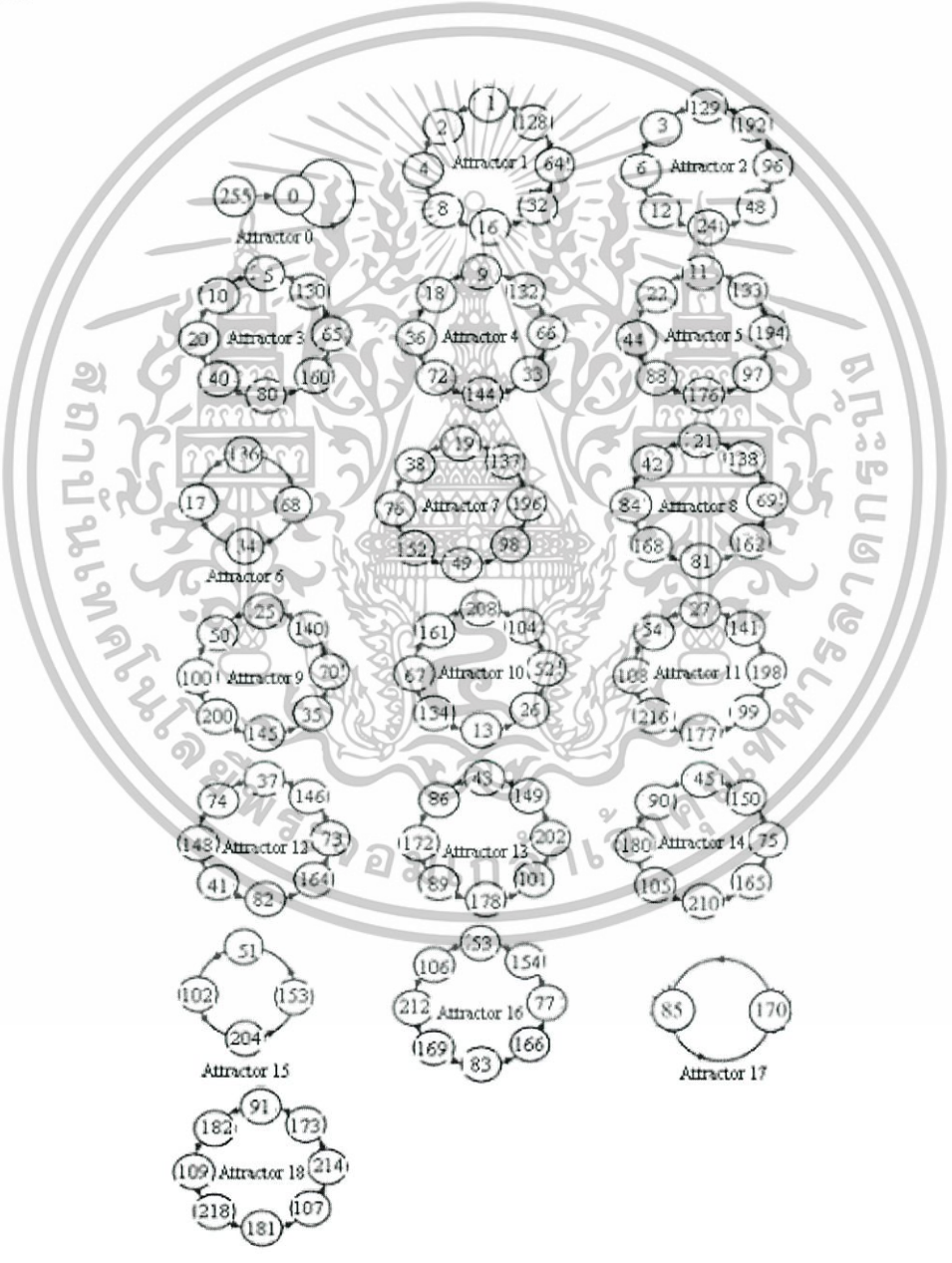
2.5.1 แอทแทรคเตอร์ (Attractor)

ในงานวิจัยนี้ใช้เซลลูลาร์ออโตมาตาแบบพื้นฐานที่กำหนดเงื่อนไขเพิ่มเติมต่างๆ ดังนี้

1. จำนวนเซลของเซลลูลาร์ออโตมาตาเป็นแบบจำกัดและมีจำนวนเพียง 8 เซล

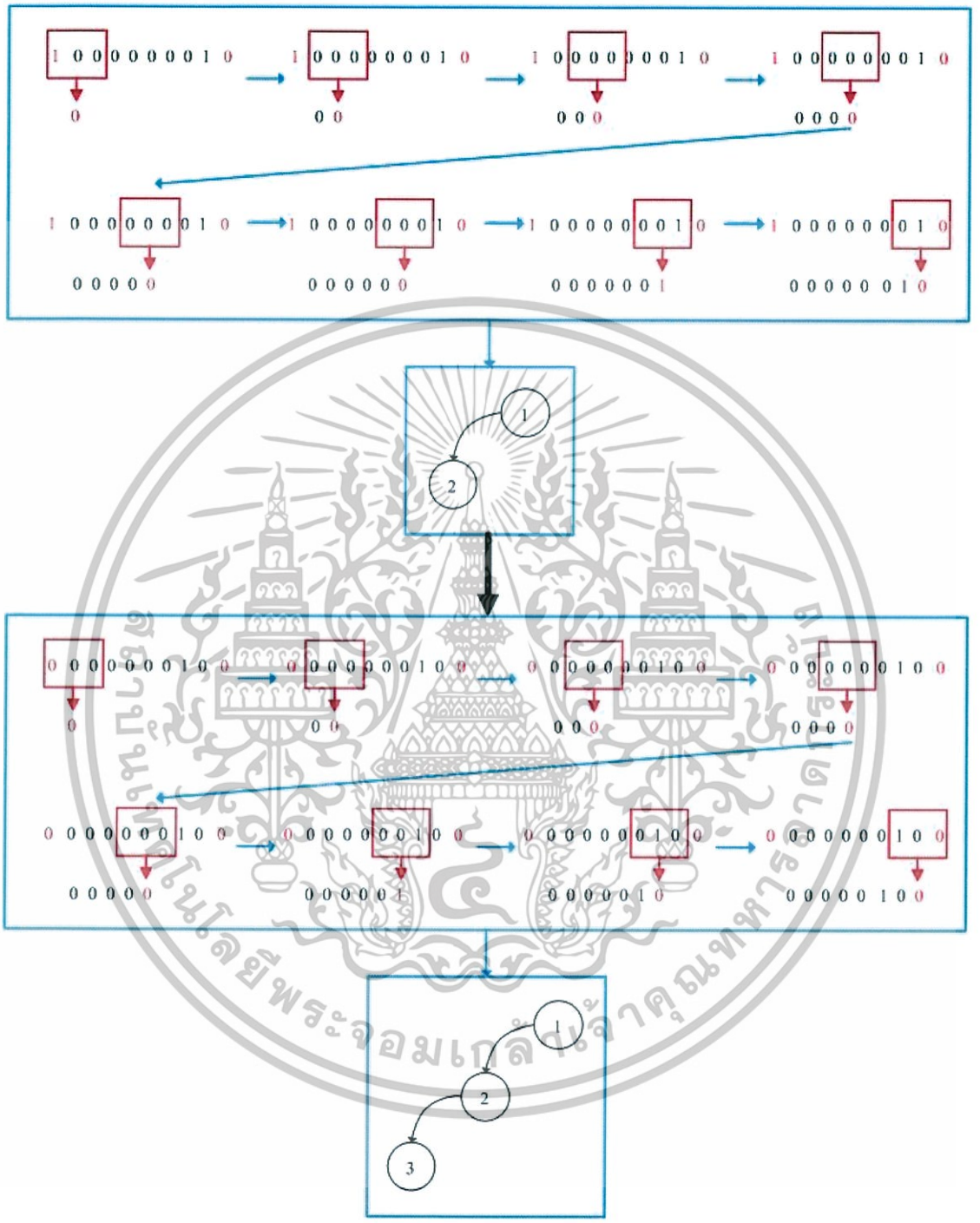
2. เงื่อนไขขอบเขตของเซลลูลาร์ออโตมาตาเป็นแบบคาบ (periodic boundary) คือ เมื่อสุดขอบที่เซลที่ 8 แล้วให้กลับไปเริ่มต้นใหม่ที่เซลที่ 1 ในทางกลับกัน ถ้าสุดขอบที่เซลที่ 1 ให้กลับไปเริ่มต้นที่เซลที่ 8

จากเงื่อนไขของทั้ง 2 ข้อด้านบนเมื่อนำมาลองเขียนเป็นแผนภาพการเปลี่ยนสถานะตามกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน พบว่าบางกฎจะได้กราฟ (graph) ที่มีลักษณะเป็นวง (cycle) ซึ่งเราจะเรียกกราฟที่มีลักษณะเป็นวงเหล่านี้ว่าแอทแทรคเตอร์ จากรูปที่ 2.17 เป็นตัวอย่างของแอท-แทรคเตอร์ทั้งหมดที่สร้างได้จากกฎ 42 โดยขั้นตอนการแอทแทรคเตอร์สามารถดูตัวอย่างได้จากรูปที่ 2.18



รูปที่ 2.17 แผนภาพการเปลี่ยนสถานะของกฎ 42 [4]

สถานะของย่านใกล้เคียง	111	110	101	100	011	010	001	000
สถานะต่อไป	0	0	1	0	1	0	1	0



รูปที่ 2.18 ตัวอย่างขั้นตอนการสร้างแอทแทรคเตอร์ที่ 1 ของกฎ 42

ในแอทแทรคเตอร์เหล่านี้ยังมีแอทแทรคเตอร์บางส่วนที่มีคุณสมบัติพิเศษดังต่อไปนี้

$$state(1) \oplus state(2) \oplus \cdots \oplus state(k) = 0 \qquad (2.9)$$

เมื่อ $state(i)$ คือ สถานะที่ i ของแอทแทรคเตอร์

k คือ จำนวนสถานะทั้งหมดของแอทแทรคเตอร์

เมื่อเรานำเลขฐาน 2 ขนาด 8 ตำแหน่งใดๆ มาทำการ exclusive – or กับสมการที่ 2.9 จะได้สมการใหม่เป็น

$$d \oplus state(1) \oplus state(2) \oplus \cdots \oplus state(k) = d \oplus 0 = d \tag{2.10}$$

เมื่อ d คือ เลขฐาน 2 ขนาด 8 ตำแหน่ง

จากสมการ 2.10 จะเห็นได้ว่าเมื่อเรานำค่า d ทำการ exclusive – or กับทุกสถานะของแอทแทรคเตอร์จะได้ค่าเท่าเดิม ดังนั้นถ้าเรานำมาประยุกต์ใช้กับการเข้ารหัสโดย นำค่าที่ต้องการเข้ารหัสทำการ exclusive – or กับสถานะของแอทแทรคเตอร์เพียงบางส่วนตามสมการดังต่อไปนี้

$$cipher = plain \oplus state(1) \oplus state(2) \oplus \cdots \oplus state(t) \tag{2.11}$$

เมื่อ $cipher$ คือ ไซเฟอร์เท็กซ์

$plain$ คือ เพลนเท็กซ์ที่เป็นเลขฐาน 2 ขนาด 8 ตำแหน่ง

t คือ จำนวนสถานะที่น้อยกว่าสถานะทั้งหมดของแอทแทรคเตอร์

จากสมการ 2.11 จะได้ไซเฟอร์เท็กซ์ และเมื่อนำไซเฟอร์เท็กซ์ไปทำการ exclusive – or กับสถานะที่เหลือของแอทแทรคเตอร์จะได้เป็นเพลนเท็กซ์ตามสมการต่อไปนี้

$$plain = cipher \oplus state(t+1) \oplus state(t+2) \oplus \cdots \oplus state(k) \tag{2.12}$$

เมื่อ $plain$ คือ เพลนเท็กซ์ที่ได้จากการถอดรหัส

$cipher$ คือ ไซเฟอร์เท็กซ์ที่ได้รับ

t คือ จำนวนสถานะที่ใช้ในการเข้ารหัส

k คือ จำนวนสถานะทั้งหมดของแอทแทรคเตอร์

2.5.2 กุญแจที่ใช้ในการเข้ารหัส

กุญแจลับที่ใช้สำหรับวิธีการนี้ประกอบด้วย 3 ส่วนดังต่อไปนี้

1. rule หมายถึงกฎที่ใช้ในการสร้างแผนภาพการเปลี่ยนสถานะเพื่อหาแอทแทรคเตอร์
2. stateone หมายถึงสถานะเริ่มต้นที่ใช้ในการสร้างแอทแทรคเตอร์ และเป็นสถานะเริ่มต้นในการเข้ารหัส
3. seed หมายถึงค่าที่กำหนดให้กับตัวเลขสุ่มเทียมเพื่อสุ่มจำนวนสถานะที่ใช้ในการเข้ารหัส

ดังนั้นกุญแจลับที่ใช้ในการเข้ารหัสและถอดรหัสคือ (rule, stateone, seed) โดยที่จำนวนของกุญแจทั้งหมดที่สามารถใช้ได้มีค่าประมาณ $256\times256\times N$ โดย N คือจำนวนตัวเลขสูงสุดที่สามารถกำหนดให้กับค่า seed ได้

2.5.3 ขั้นตอนวิธีการเข้ารหัสและถอดรหัส

สำหรับขั้นตอนวิธีการเข้ารหัสรูปภาพนี้เป็นขั้นตอนวิธีสำหรับการเข้ารหัสรูปภาพขนาด $m\times n$ จุดภาพและมีค่าความลึกของบิตเท่ากับ 8 ซึ่งสามารถสรุปได้ดังนี้

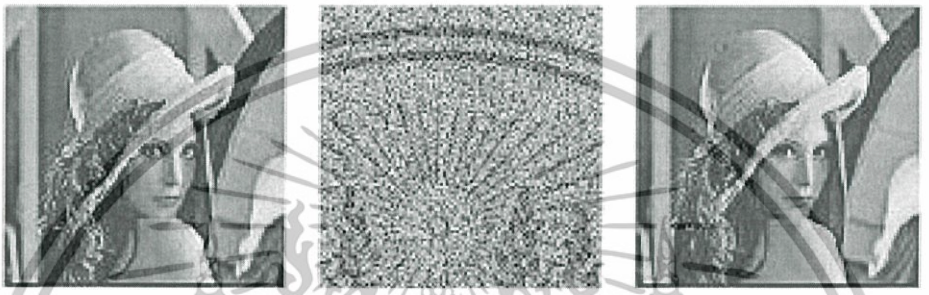
1. กำหนดค่ากุญแจลับได้แก่ (rule, stateone, seed)
2. สร้างแผนภาพการเปลี่ยนสถานะ โดยสถานะเริ่มต้นคือค่า stateone ที่กำหนดและเปลี่ยนสถานะตาม rule จนได้เป็นแอทแทรคเตอร์
3. ทำการสุ่มตัวเลขด้วยตัวสร้างเลขสุ่มเทียมโดยใช้ค่า seed ตามที่กำหนด โดยทำการสุ่มตัวเลขออกมาแล้วทำการเก็บไว้ในแถวลำดับ T ที่มีขนาดเท่ากับภาพคือ $m\times n$ และทุกค่าจะต้องน้อยกว่าจำนวนสถานะทั้งหมดในแอทแทรคเตอร์
4. นำค่าความเข้มแสงของแต่ละจุดภาพทำการ exclusive – or กับแอทแทรคเตอร์ตามสมการ 2.11 โดยที่ค่า i คือค่าในแถวลำดับ T ที่ตำแหน่งเดียวกับจุดภาพ
5. สิ้นสุดขั้นตอนการเข้ารหัสภาพ

ในส่วนของขั้นตอนการถอดรหัสภาพมีลักษณะคล้ายกับการเข้ารหัสซึ่งสามารถสรุปได้ดังนี้

1. สร้างแผนภาพการเปลี่ยนสถานะ โดยสถานะเริ่มต้นคือค่า stateone ที่ได้รับจากกุญแจลับ และเปลี่ยนสถานะตาม rule จนได้เป็นแอทแทรคเตอร์
2. ทำการสุ่มตัวเลขด้วยตัวสร้างเลขสุ่มเทียมโดยใช้ค่า seed ตามที่ได้รับจากกุญแจลับ โดยทำการสุ่มตัวเลขออกมาแล้วทำการเก็บไว้ในแถวลำดับ T ที่มี

ขนาดเท่ากับภาพไซเฟอร์เท็กซ์ และทุกค่าจะต้องน้อยกว่าจำนวนสถานะทั้งหมดในแอทแทรคเตอร์

3. นำค่าความเข้มแสงของแต่ละจุดภาพไซเฟอร์เท็กซ์ทำการ exclusive – or กับแอทแทรคเตอร์ตามสมการ 2.12 โดยที่ค่า t คือค่าในแถวลำดับ T ที่ตำแหน่งเดียวกับจุดภาพ
4. สิ้นสุดขั้นตอนการเข้าถอดรหัส



(a) (b) (c)

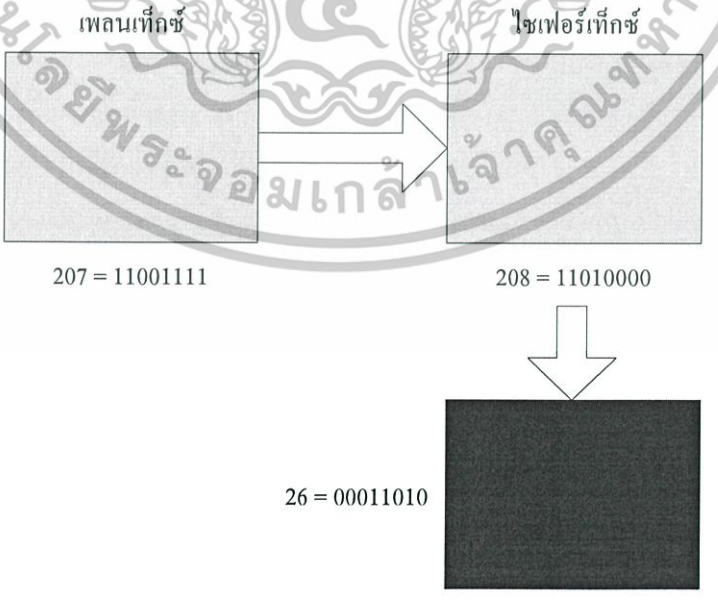
รูปที่ 2.19 ตัวอย่างรูปที่เข้ารหัสและถอดรหัสตามวิธีการของ Jin [4]
(a) ภาพต้นฉบับ (b) ภาพที่เข้ารหัส (c) ภาพที่ถอดรหัส

บทที่ 3
วิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน

งานวิจัยนี้เป็นงานวิจัยที่ทำการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานที่ปรับปรุงมาจากงานวิจัย [4] เนื่องจากมีข้อเสียคือมีกุญแจที่ไม่สามารถปกปิดข้อมูลรูปภาพได้มากเกินไป ต่อจากนี้จะเป็นการอธิบายถึงแนวคิดในการปรับปรุงงานวิจัย และขั้นตอนวิธีของงานวิจัยนี้

3.1 การปรับปรุงวิธีการเข้ารหัส

จุดมุ่งหมายของการปรับปรุงมีอยู่ 2 อย่างด้วยกัน ได้แก่ การปรับปรุงเพื่อเพิ่มจำนวนกุญแจลับทั้งหมดที่สามารถใช้ในการเข้ารหัสได้ (key space) และการปรับปรุงเพื่อเพิ่มความสามารถในการปกปิดข้อมูล ในส่วนของการปรับปรุงเพื่อเพิ่มจำนวนกุญแจลับทั้งหมดที่สามารถใช้ได้ จะทำการปรับปรุงด้วยการใช้ตัวสร้างเลขสุ่มเทียมเพื่อเลือกสถานะเริ่มต้นของทุกๆ จุดภาพ จากเดิมที่ใช้สถานะเริ่มต้นเดียวกันในทุกๆ จุดภาพ สำหรับการปรับปรุงเพื่อเพิ่มความสามารถในการปกปิดข้อมูล จะทำการปรับปรุงโดยการเพิ่มขั้นตอนของการสลับตำแหน่งบิตของค่าความเข้มแสงในแต่ละจุดภาพ เนื่องจากข้อมูลประเภทรูปภาพ ถึงแม้ค่าความเข้มแสงจะแตกต่างกันแต่ถ้าบิตที่แตกต่างกันเป็นบิตในตำแหน่งที่มีค่านัยสำคัญน้อยที่สุด หรือที่เรียกว่า Least – Significant Bit เมื่อมองด้วยสายตาแล้วไม่สามารถบ่งบอกความแตกต่างได้ ดังนั้นถ้าใช้การสลับตำแหน่งของบิตจะช่วยเพิ่มความแตกต่างได้



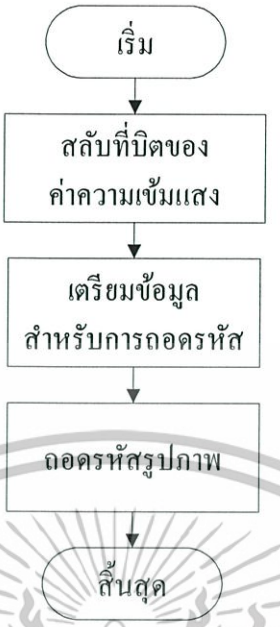
รูปที่ 3.1 เปรียบเทียบความแตกต่างของภาพก่อนและหลังสลับที่บิต

3.2 ขั้นตอนวิธีการเข้ารหัสรูปภาพ

ขั้นตอนวิธีการเข้ารหัสรูปภาพที่ได้ผ่านการปรับปรุงแล้วสามารถแบ่งได้เป็น 3 ขั้นตอน ได้แก่ ขั้นตอนการเตรียมข้อมูลก่อนการเข้ารหัส ซึ่งเป็นการเตรียมข้อมูลที่จำเป็นในการเข้ารหัสเช่น กุญแจลับที่ใช้ในการเข้ารหัส แอทแทรคเตอร์ที่ใช้ในการเข้ารหัส เป็นต้น ขั้นตอนที่สองเป็นขั้นตอนของการเข้ารหัสโดยนำข้อมูลที่เตรียมไว้ในขั้นตอนแรกทำการเข้ารหัส ขั้นตอนสุดท้ายเป็นขั้นตอนของการสลับที่บิตของค่าความเข้มแสงของแต่ละจุดภาพ ซึ่งขั้นตอนนี้เป็นขั้นตอนที่เพิ่มขึ้นมาเพื่อช่วยให้ปกปิดข้อมูลได้ดียิ่งขึ้น

ในส่วนของขั้นตอนการถอดรหัสคล้ายกับขั้นตอนการเข้ารหัส สามารถแบ่งออกได้เป็น 3 ขั้นตอนเช่นกัน โดยที่ขั้นตอนแรกเป็นการสลับตำแหน่งของบิตเพื่อให้ข้อมูลกลับมาอยู่ในตำแหน่งเดิม ขั้นตอนที่สองเป็นการเตรียมข้อมูลในการถอดรหัสเช่นเดียวกับขั้นตอนวิธีการเข้ารหัส และขั้นตอนสุดท้ายเป็นขั้นตอนการถอดรหัสรูปภาพ

รูปที่ 3.2 ขั้นตอนการเข้ารหัสรูปภาพ



รูปที่ 3.3 ขั้นตอนการถอดรหัสรูปภาพ

3.3 กุญแจลับในการเข้ารหัส

เนื่องจากมีการปรับปรุงขั้นตอนวิธีการเข้ารหัสใหม่จึงทำให้กุญแจลับที่ใช้ในการเข้ารหัสมีการเปลี่ยนแปลงจากเดิมที่ใช้ (rule, statecone, seed) ต้องปรับเปลี่ยนใหม่เป็น (rule, seedstate, seedtime) เมื่อ rule ยังคงหมายถึงกฎของเซลลูลาร์ออโตมาตาที่ใช้สร้างแผนภาพการเปลี่ยนสถานะเช่นเดิม seedstate หมายถึงค่าตัวเลขที่ใช้กำหนดให้กับตัวสร้างเลขสุ่มเทียมเพื่อเลือกสถานะเริ่มต้นของแอทแทรคเตอร์ของแต่ละจุดภาพ และ seedtime หมายถึงตัวเลขที่กำหนดให้กับตัวสร้างเลขสุ่มเทียมเพื่อเลือกจำนวนสถานะที่ใช้ในการเข้ารหัสเช่นเดียวกับค่า seed ของกุญแจแบบเดิม

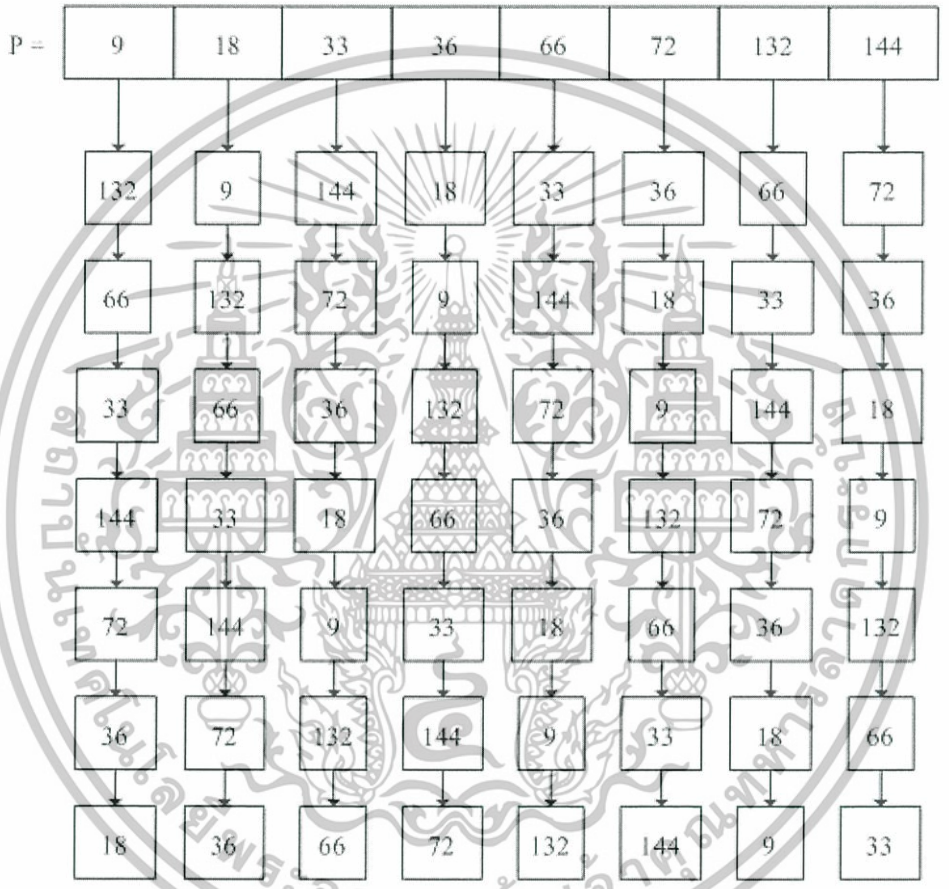
3.4 การเตรียมข้อมูลสำหรับการเข้ารหัสและถอดรหัสรูปภาพ

ข้อมูลที่จำเป็นต้องใช้ในขั้นตอนของการเข้ารหัสประกอบด้วยแอทแทรคเตอร์ที่ใช้ของแต่ละจุดภาพ และจำนวนของสถานะที่ใช้ในการเข้ารหัสของแต่ละจุดภาพ ต่างจากวิธีการเดิมที่ทุกจุดภาพใช้แอทแทรคเตอร์เดียวกันทั้งหมด ทำให้ขั้นตอนการเตรียมข้อมูลมีความยุ่งยากซับซ้อนมากขึ้น สามารถแบ่งออกเป็นขั้นตอนย่อยได้ดังต่อไปนี้

3.4.1 การหาแอทแทรคเตอร์ทั้งหมด

ข้อมูลที่จำเป็นต้องใช้ในขั้นตอนการเข้ารหัสที่สำคัญคือแอทแทรคเตอร์ สำหรับขั้นตอนในการหาแอทแทรคเตอร์เริ่มต้นจากการสร้างแผนภาพการเปลี่ยนสถานะของกฎตามค่า rule ของ

กุญแจลับ โดยใช้สถานะเริ่มต้นทุกสถานะที่เป็นไปได้ซึ่งมีทั้งหมด 256 สถานะ โดยในสถานะเหล่านี้จะมีบางส่วนที่ไม่สามารถสร้างเป็นแอทแทรคเตอร์ได้ และยังมีอีกบางส่วนที่เป็นแอทแทรคเตอร์แล้ว แต่ไม่มีคุณสมบัติตามสมการ 2.9 ซึ่งไม่สามารถนำมาใช้งานในการเข้ารหัสได้ ดังนั้นจึงต้องใช้แถวลำดับ P ในการเก็บค่าสถานะที่สามารถใช้ในการเข้ารหัสรูปภาพได้ นอกจากนี้แถวลำดับ P อาจจะมีลักษณะโครงสร้างแบบพิเศษเพื่อเก็บค่าแอทแทรคเตอร์ของแต่ละสถานะเริ่มต้นเพื่อช่วยลดระยะเวลาในการคำนวณด้วย



รูปที่ 3.4 ตัวอย่างโครงสร้างพิเศษที่ใช้เก็บค่าแอทแทรคเตอร์ของกฎ 2

จากตัวอย่างในรูป 3.4 เป็นโครงสร้างแบบลิ้งค์ลิสต์ (Linked – List) ที่นำมาใช้ในการเก็บค่าแอทแทรคเตอร์ของกฎ 2 ที่มีสถานะเริ่มต้นแตกต่างกัน โดยค่าของสถานะเริ่มต้นจะถูกเก็บอยู่ในแถวลำดับ P และแต่ละสถานะเริ่มต้นจะชี้ไปยังสถานะต่อไปของตัวเอง จนกว่าจะครบทุกสถานะของแอทแทรคเตอร์ ซึ่งวิธีนี้ช่วยให้การคำนวณรวดเร็วขึ้น แต่ต้องแลกกับการใช้พื้นที่ในการเก็บข้อมูลเพิ่มมากขึ้น

3.4.2 การหาสถานะเริ่มต้น

การหาสถานะเริ่มต้นของแต่ละจุดภาพเริ่มต้นจากการกำหนดค่า seedstate ตามค่าของกุญแจที่กำหนดไว้ให้กับตัวสร้างเลขสุ่มเทียม และกำหนดให้สร้างตัวเลขเป็นจำนวนเท่ากับจำนวนจุดภาพที่ใช้ในการเข้ารหัส สมมติว่าภาพที่ต้องการเข้ารหัสมีขนาดเท่ากับ $m \times n$ ให้ทำการสุ่มตัวเลขทั้งหมด $m \times n$ จำนวน และเก็บค่าที่ได้ไว้ในแถวลำดับ S

3.4.3 การหาแอทแทรคเตอร์ของแต่ละจุดภาพ

เมื่อได้ทำการเตรียมข้อมูลของทั้งสองส่วนข้างต้นแล้ว ขั้นตอนต่อไปเป็นการหาแอทแทรคเตอร์ที่ใช้ในการเข้ารหัสของแต่ละจุดภาพ ด้วยการหาสถานะเริ่มต้นของแอทแทรคเตอร์โดย

$$start(i,j) = p((s(i,j) \mod q) + 1) \tag{3.1}$$

เมื่อ $start(i,j)$ คือ สถานะเริ่มต้นของจุดภาพในตำแหน่งแถวที่ i หลักที่ j

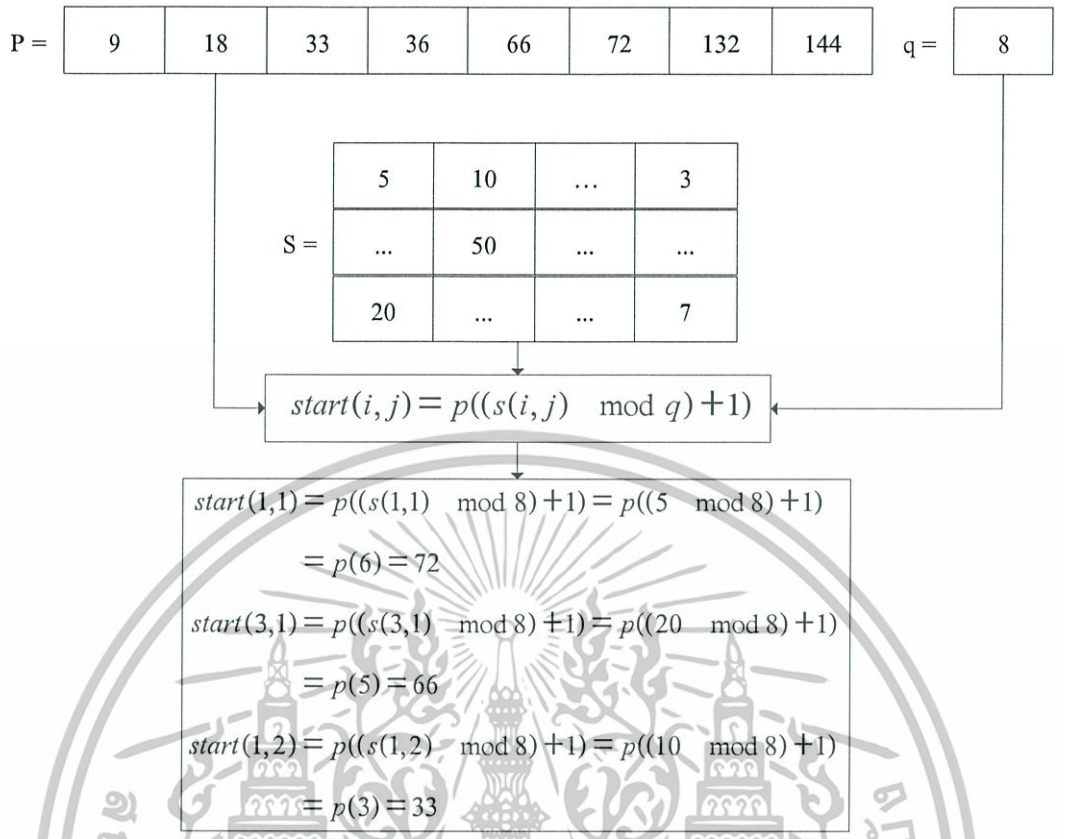
$s(i,j)$ คือ ค่าภายในแถวลำดับ S ตำแหน่งแถวที่ i หลักที่ j

q คือ จำนวนสถานะทั้งหมดในแถวลำดับ P

$p(i)$ คือ ค่าภายในแถวลำดับ P ที่ตำแหน่ง i

เมื่อคำนวณได้สถานะเริ่มต้นเรียบร้อยแล้วต้องสร้างแอทแทรคเตอร์เพื่อใช้ในการเข้ารหัสข้อมูลอีกครั้ง แต่ถ้าแถวลำดับ P มีลักษณะโครงสร้างแบบพิเศษที่เก็บแอทแทรคเตอร์ของแต่ละสถานะเริ่มต้นเอาไว้ก็ไม่จำเป็นต้องทำการหาแอคแทรคเตอร์ซ้ำอีก ทำให้ลดระยะเวลาการคำนวณลงได้ในระดับหนึ่ง

จากรูปที่ 3.5 เป็นตัวอย่างการคำนวณหาแอทแทรคเตอร์ของแต่ละจุดภาพ แอทแทรคเตอร์ที่ใช้เป็นแอทแทรคเตอร์ที่สร้างจากกฎ 2 ซึ่งมีอยู่เพียงแอทแทรคเตอร์เดียวและมีจำนวนสถานะในแอทแทรคเตอร์เท่ากับ 8 ดังนั้นจำนวนสถานะที่อยู่ในแถวลำดับ $P(q)$ เท่ากับ 8



รูปที่ 3.5 ตัวอย่างการคำนวณหาสถานะเริ่มต้น

3.4.4 การหาจำนวนสถานะในการเข้ารหัส

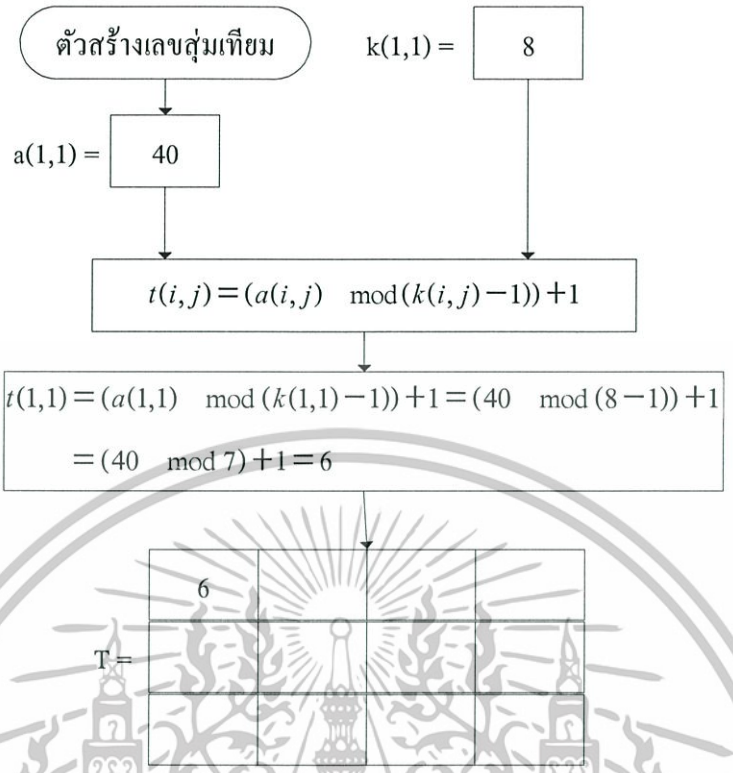
สำหรับขั้นตอนการหาจำนวนสถานะที่ใช้ในการเข้ารหัสมีขั้นตอนเช่นเดียวกับการหาสถานะเริ่มต้น โดยเริ่มจากการกำหนดกำหนดค่า seedtime ตามค่าของกุญแจที่กำหนดไว้ให้กับตัวสร้างเลขสุ่มเทียม และกำหนดให้สร้างตัวเลขเป็นจำนวนเท่ากับจำนวนจุดภาพที่ใช้ในการเข้ารหัส สมมติว่าภาพที่ต้องการเข้ารหัสมีขนาดเท่ากับ $m \times n$ ให้ทำการสุ่มตัวเลขทั้งหมด $m \times n$ จำนวน และเก็บค่าที่ได้ไว้ในแถวลำดับ T แต่ก่อนที่จะเก็บค่าลงในแถวลำดับต้องแน่ใจก่อนว่าตัวเลขที่จะเก็บค่านี้ต้องน้อยกว่าจำนวนสถานะทั้งหมดของแอทแทรคเตอร์ โดยคำนวณตามสมการดังต่อไปนี้

$$t(i,j) = (a(i,j) \mod (k(i,j) - 1)) + 1 \tag{3.2}$$

เมื่อ $t(i,j)$ คือ ค่าที่เก็บในแถวลำดับ T ตำแหน่งแถวที่ i หลักที่ j

$a(i,j)$ คือ ค่าที่ได้จากตัวสร้างเลขสุ่มเทียมตำแหน่งแถวที่ i หลักที่ j

$k(i,j)$ คือ จำนวนสถานะทั้งหมดของแอทแทรคเตอร์ของตำแหน่งแถวที่ i หลักที่ j



รูปที่ 3.6 ตัวอย่างการคำนวณหาจำนวนสถานะในการเข้ารหัส

จากขั้นตอนวิธีที่กล่าวมาทั้งหมดเป็นขั้นตอนของการเตรียมข้อมูลสำหรับการเข้ารหัส สำหรับขั้นตอนวิธีการถอดรหัสนั้นก็ใช้ขั้นตอนวิธีการเตรียมข้อมูลแบบเดียวกัน เพียงแต่ใช้กุญแจในการถอดรหัสที่ได้รับมา แทนกุญแจที่กำหนดเอง

3.5 การเข้ารหัสและถอดรหัสรูปภาพ

เมื่อเตรียมข้อมูลที่จำเป็นสำหรับการเข้ารหัสรูปภาพเรียบร้อยแล้วขั้นตอนต่อไปเป็นการเข้ารหัสรูปภาพ ตามสมการต่อไปนี้

$$cipher(i,j)=pixel(i,j)\oplus state(1,i,j)\oplus state(2,i,j)\oplus\cdots\oplus state(t(i,j),i,j) \quad (3.3)$$

เมื่อ $cipher(i,j)$ คือ ค่าที่เข้ารหัสได้ในตำแหน่งจุดภาพแถวที่ i หลักที่ j

$pixel(i,j)$ คือ ค่าความเข้มแสงที่ตำแหน่งจุดภาพแถวที่ i หลักที่ j

$state(l,i,j)$ คือ สถานะที่ l ของแอทแทรคเตอร์ของตำแหน่งจุดภาพแถวที่ i หลักที่ j

สำหรับขั้นตอนการถอดรหัสรูปภาพ ให้ทำการถอดรหัสตามสมการดังต่อไปนี้

$$decryp(i,j) = cipher(i,j) \oplus state(t(i,j)+1,i,j) \oplus \cdots \oplus state(k,i,j) \qquad (3.4)$$

เมื่อ $decryp(i,j)$ คือ ค่าที่ถอดรหัสได้ในตำแหน่งจุดภาพแถวที่ i หลักที่ j

$cipher(i,j)$ คือ ค่าความเข้มแสงของไซเฟอร์เท็กซ์ (ได้จากการเข้ารหัสตามสมการ 3.3) ที่ตำแหน่งจุดภาพแถวที่ i หลักที่ j

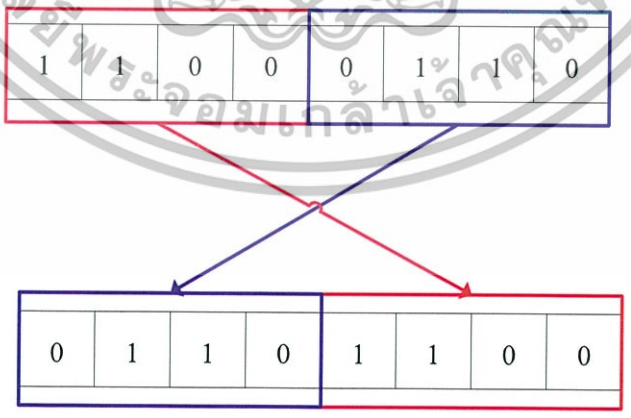
$state(l,i,j)$ คือ สถานะที่ l ของแอทแทรคเตอร์ของตำแหน่งจุดภาพแถวที่ i หลักที่ j

$state(k,i,j)$ คือ สถานะสุดท้ายของแอทแทรคเตอร์ของตำแหน่งแถวที่ i หลักที่ j

3.6 การสลับที่บิตของค่าความเข้มแสง

ในขั้นตอนนี้เป็นการสลับที่บิตของค่าความเข้มแสงเพื่อเพิ่มความสามารถในการปกปิดข้อมูล เมื่อรูปภาพผ่านขั้นตอนการเข้ารหัสเรียบร้อยแล้วจะถูกนำมาสลับที่บิตโดยแต่ละจุดภาพค่าความเข้มแสงจะถูกแบ่งเป็น 2 กลุ่ม คือ กลุ่มแรกคือบิตในตำแหน่งที่ 1 ถึงตำแหน่งที่ 4 กลุ่มที่สองเป็นบิตในตำแหน่งที่ 5 ถึงตำแหน่งที่ 8 แล้วทำการสลับที่โดยสลับที่บิตของทั้ง 2 กลุ่มนี้โดยนำบิตกลุ่มแรกไปวางในตำแหน่งของกลุ่มที่สองและนำบิตกลุ่มที่สองมาวางในตำแหน่งของกลุ่มแรก

สำหรับการถอดรหัสก็ทำการสลับที่ของบิตเช่นเดียวกับการเข้ารหัส แตกต่างกันที่ขั้นตอนการสลับที่บิตของการถอดรหัสนั้นต้องทำเป็นขั้นตอนแรกสุด



รูปที่ 3.7 การสลับที่บิตของค่าความเข้มแสง

บทที่ 4

การทดลองและผลการทดลอง

จากการปรับปรุงวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาที่ได้นำเสนอไว้ในส่วนของบทที่ 3 เพื่อเป็นการทดสอบประสิทธิภาพของวิธีการที่ได้นำเสนอไป ในบทนี้จึงเป็นส่วนของการทดลอง เพื่อวัดประสิทธิภาพของการเข้ารหัสซึ่งมีรายละเอียดดังต่อไปนี้

4.1 เครื่องมือและโปรแกรมที่ใช้ในการทดลอง

รายละเอียดของเครื่องคอมพิวเตอร์และโปรแกรมที่ใช้ในการทดลองเข้ารหัสและถอดรหัสมีดังต่อไปนี้

หน่วยประมวลผลกลาง (CPU) : AMD Phenom II X6 processor 1055T 2.8 GHz
หน่วยความจำหลัก (RAM) : 4 GB
หน่วยความจำสำรอง(Hard Disk) : 1.5 TB
ระบบปฏิบัติการ (OS) : Windows 7 Home Premium 64-bit
โปรแกรมที่ใช้ : Matlab
รุ่นของโปรแกรมที่ใช้ : 7.11.0 (R2010b)

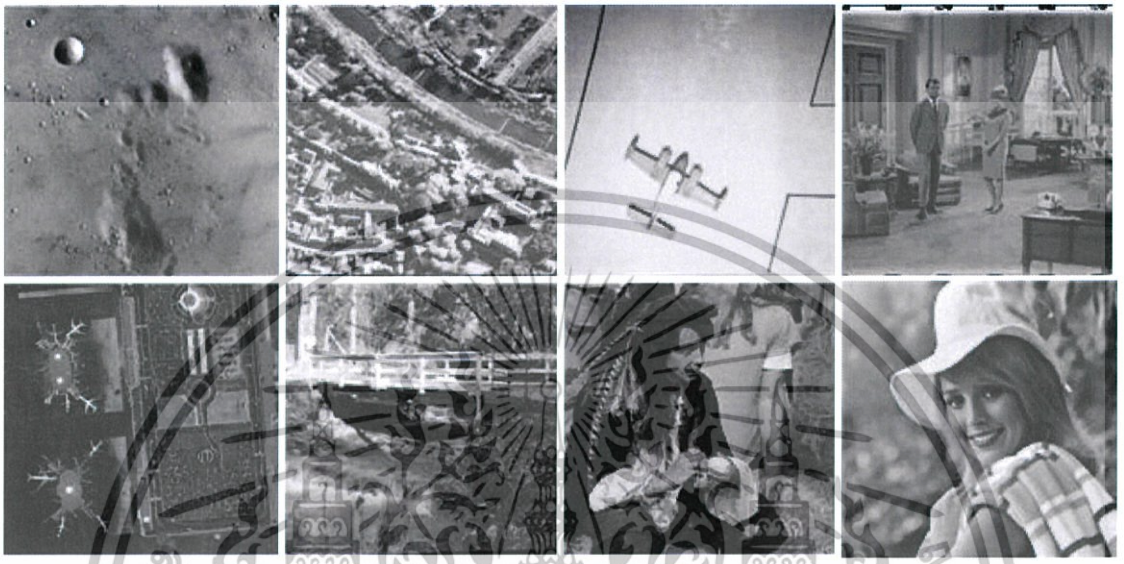
4.2 ข้อมูลภาพที่ใช้ในการทดลอง

รูปภาพที่นำมาใช้ในการทดลองเป็นรูปภาพที่ได้มาจากฐานข้อมูลของ USC – SIPI [1] ในหมวด Miscellaneous ซึ่งเป็นหมวดของรูปภาพมาตรฐานที่ใช้งานที่เกี่ยวข้องกับการประมวลผลภาพ มีทั้งหมด 44 รูป ประกอบไปด้วยภาพสีและภาพสีเทาที่มีขนาดของภาพเท่ากับ 256×256, 512×512 และ 1024×1024 จุดภาพ รูปภาพทุกภาพบันทึกอยู่ในรูปแบบของ TIFF ประเภทของรูปภาพจากฐานข้อมูลสามารถสรุปได้ตามตาราง 4.1

ตารางที่ 4.1 จำนวนของรูปภาพแต่ละประเภทในฐานข้อมูล USC – SIPI

ประเภทของภาพ	256×256	512×512	1024×1024	รวม
ภาพสีเทา	6	18	4	28
ภาพสี	8	8	0	16
รวม	14	26	4	44

รูปที่ใช้ในการทดลองนอกจากจะใช้ภาพจากฐานข้อมูลแล้ว ยังใช้ภาพที่ได้จากการเปลี่ยนภาพสีของฐานข้อมูลเป็นภาพสีเทาด้วย โดยใช้โปรแกรม Matlab ในการเปลี่ยนภาพสีให้เป็นภาพสี-เทา ซึ่งมีทั้งหมด 16 ภาพ ดังนั้นจำนวนของรูปภาพที่ใช้ในการทดลองมีทั้งหมด 60 ภาพ รายชื่อและภาพทั้งหมดได้แสดงไว้ในภาคผนวก ก



รูปที่ 4.1 ตัวอย่างภาพสีเทาที่ใช้ในการทดลอง

รูปที่ 4.2 ตัวอย่างภาพสีที่ใช้ในการทดลอง

4.3 การวิเคราะห์จำนวนกุญแจทั้งหมดที่เป็นไปได้

จากงานวิจัย [4] ได้ประเมินจำนวนกุญแจทั้งหมดที่เป็นไปได้ไว้ดังนี้

rule กฎทั้งหมดของเซลลูลาร์ออโตมาตาแบบพื้นฐานมีจำนวนเท่ากับ 256

stateone สถานะเริ่มต้นทั้งหมดที่เป็นไปได้มีจำนวนเท่ากับ 256

seed ค่าสูงสุดที่สามารถกำหนดให้กับตัวสร้างเลขสุ่มเทียมได้สมมติให้มีค่าเท่ากับ N

ดังนั้นจำนวนกุญแจทั้งหมดที่เป็นไปได้ เท่ากับ $256 \times 256 \times N$

จากการทดสอบหาแทรกเตอร์ทั้งหมดของทุกกฎและทุกสถานะเริ่มต้นพบว่า บางกฎก็ไม่สามารถหาแอทแทรคเตอร์ได้ รวมทั้งบางสถานะของบางกฎก็ไม่สามารถนำมาใช้ในการเข้ารหัสได้เช่นกัน กฎและสถานะที่สามารถใช้ในการเข้ารหัสได้สามารถดูได้ที่ภาคผนวก ข โดยกฎและสถานะที่ใช้ได้มีจำนวนทั้งหมดเท่ากับ 3664 ดังนั้นจำนวนกุญแจทั้งหมดที่เป็นไปได้ที่แท้จริงของวิธีการเดิมเท่ากับ $3664 \times N$

สำหรับขั้นตอนวิธีการเข้ารหัสแบบใหม่ที่มีกุญแจลับคือ (rule, seedstate, seedtime) เนื่องจากขั้นตอนการเลือกสถานะเริ่มต้นและจำนวนสถานะที่ใช้ในการเข้ารหัส ใช้ตัวสร้างเลขสุ่มเทียมตัวเดียวกัน สมมติให้รับค่าสูงสุดได้เท่ากับ N และจำนวนกฎที่สามารถใช้ในการเข้ารหัสได้มีทั้งหมด 128 กฎดังนั้นจำนวนกุญแจทั้งหมดที่เป็นไปได้มีค่าเท่ากับ $128 \times N \times N$ หรือ $128 \times N^2$

สำหรับค่าสูงสุดที่สามารถกำหนดให้กับตัวสร้างเลขสุ่มเทียมนั้นโดยส่วนใหญ่แล้วจะมีขนาดใหญ่มาก เช่น Mersenne twister generator ที่เป็นตัวสร้างเลขสุ่มเทียมหลักของโปรแกรม Matlab สามารถกำหนดตัวเลขได้ถึง $2^{32}-1$ หรือประมาณ 4×10^9

ตัวสร้างเลขสุ่มเทียมที่ใช้ในการทดลองนี้มีชื่อว่า ISAAC (Indirection, Shift, Accumulate, Add, and Count)[12] เป็นตัวสร้างเลขสุ่มเทียมที่มีความปลอดภัยสูง และสามารถกำหนดตัวเลขให้กับตัวสร้างเลขสุ่มได้สูงสุดถึง $2^{8192}-1$ หรือประมาณ 10^{2466} ดังนั้นจำนวนกุญแจทั้งหมดที่เป็นไปได้ของวิธีการเดิมคือ 3664×2^{8192} และจำนวนกุญแจทั้งหมดที่เป็นไปได้ของวิธีการใหม่คือ $128 \times 2^{8192} \times 2^{8192}$ ซึ่งเห็นได้ชัดเจนว่าวิธีการใหม่นี้มีจำนวนกุญแจที่เป็นไปได้ทั้งหมดมากกว่าวิธีการเดิม

4.4 ระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัส

จากการทดลองวัดระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัสของรูปภาพทั้งหมด ด้วยกุญแจลับที่แตกต่างกันทั้งหมด 8 กุญแจลับ ได้แก่ (2, 72, 15), (3, 72, 15), (42, 53, 15), (42, 99, 53), (42, 99, 54) และ (42, 99, 55) สามารถสรุปได้ตามตารางที่ 4.2

ตารางที่ 4.2 ระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสของแต่ละรูปภาพในหน่วยวินาที

ชื่อภาพ	เข้ารหัส	ถอดรหัส	รวม
4.1.01.tiff	15.571094	15.430553	31.0028403
4.1.01_gray.tiff	6.0813685	5.953866	12.0363635
4.1.02.tiff	15.63859	15.421027	31.0608093
4.1.02_gray.tiff	6.0961459	5.9694141	12.0666871
4.1.03.tiff	15.622443	15.475318	31.0989233
4.1.03_gray.tiff	6.0787354	6.017445	12.0972921
4.1.04.tiff	15.648096	15.49091	31.140194
4.1.04_gray.tiff	6.0860516	5.9902606	12.0774245
4.1.05.tiff	15.651317	15.504567	31.1570698
4.1.05_gray.tiff	6.0754499	5.9663641	12.042924
4.1.06.tiff	15.621669	15.454764	31.0776178
4.1.06_gray.tiff	6.0884414	5.9616405	12.051185
4.1.07.tiff	15.595912	15.475589	31.0726811
4.1.07_gray.tiff	6.0597816	5.9724084	12.0332881
4.1.08.tiff	15.585118	15.438989	31.0252865
4.1.08_gray.tiff	6.0905548	5.9677615	12.0594408
4.2.01.tiff	59.153521	59.220499	118.375284
4.2.01_gray.tiff	21.368529	21.134736	42.5044293
4.2.02.tiff	59.413889	59.295338	118.710492
4.2.02_gray.tiff	21.357155	21.119918	42.4782284
4.2.03.tiff	59.458631	59.185886	118.645776
4.2.03_gray.tiff	21.31221	21.179873	42.4932389
4.2.04.tiff	59.443512	59.275816	118.72058
4.2.04_gray.tiff	21.31551	21.128028	42.4447061
4.2.05.tiff	59.246431	59.149368	118.397053
4.2.05_gray.tiff	21.258115	21.067148	42.3264186
4.2.06.tiff	59.253969	59.204169	118.459391
4.2.06_gray.tiff	21.300311	21.061547	42.3630231
4.2.07.tiff	59.176541	59.019229	118.197048

ตารางที่ 4.2(ต่อ) ระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสของแต่ละรูปภาพในหน่วยวินาที

ชื่อภาพ	เข้ารหัส	ถอดรหัส	รวม
4.2.07_gray.tiff	21.398291	21.159958	42.5593988
5.1.09.tiff	6.0756248	5.9463994	12.0231294
5.1.10.tiff	6.0893776	5.9670984	12.0578325
5.1.11.tiff	6.09421	5.9555975	12.0509369
5.1.12.tiff	6.1017963	5.9782686	12.0811768
5.1.13.tiff	6.1107288	5.9807698	12.0926183
5.1.14.tiff	6.0995419	5.96012	12.060783
5.2.08.tiff	21.341977	21.18059	42.5237176
5.2.09.tiff	21.2966	21.163009	42.460761
5.2.10.tiff	21.277426	21.119793	42.3983766
5.3.01.tiff	82.474848	81.848078	164.324158
5.3.02.tiff	82.569554	82.064288	164.635085
7.1.01.tiff	21.285858	21.14795	42.4349605
7.1.02.tiff	21.365944	21.111346	42.4784405
7.1.03.tiff	21.281421	21.146902	42.4295018
7.1.04.tiff	21.286068	21.144787	42.4320038
7.1.05.tiff	21.347683	21.089608	42.4384503
7.1.06.tiff	21.322332	21.086519	42.4100023
7.1.07.tiff	21.325158	21.153243	42.4795726
7.1.08.tiff	21.349709	21.090975	42.4418456
7.1.09.tiff	21.376528	21.172637	42.5503161
7.1.10.tiff	21.301454	21.082836	42.3854485
7.2.01.tiff	82.936702	81.98096	164.918905
boat.512.tiff	21.352214	21.163444	42.5168165
elaine.512.tiff	21.368827	21.160459	42.5304629
gray21.512.tiff	21.286645	21.151124	42.4389323
house.tiff	59.249415	59.301135	118.55181
house_gray.tiff	21.353565	21.154504	42.5092233
numbers.512.tiff	21.342028	21.174153	42.5173413

ตารางที่ 4.2(ต่อ) ระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสของแต่ละรูปภาพในหน่วยวินาที

ชื่อภาพ	เข้ารหัส	ถอดรหัส	รวม
ruler.512.tiff	21.31387	21.137031	42.4520578
testpat.1k.tiff	82.634443	81.817983	164.453704

จากตารางที่ 4.2 เมื่อนำรูปภาพทั้งหมดมาแบ่งกลุ่มตามลักษณะสีของภาพ และขนาดของภาพตามตารางที่ 4.3 พบว่าระยะเวลาที่ใช้ในการเข้ารหัสและถอดรหัสของภาพแตกต่างกัน โดยภาพสีเทาจะใช้เวลาน้อยกว่า เนื่องจากภาพสีต้องทำการเข้ารหัสหรือถอดรหัสถึง 3 ครั้งในแต่ละจุดภาพ ขณะที่ภาพสีเทาจะทำเพียงครั้งเดียว

ตารางที่ 4.3 ระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสของรูปภาพแต่ละกลุ่มในหน่วยวินาที

ประเภทของภาพ	เข้ารหัส	ถอดรหัส	รวม
ภาพสีเทา ขนาด 256×256	6.087701	5.97053	12.05936
ภาพสีเทา ขนาด 512×512	21.32636	21.13393	42.46145
ภาพสีเทา ขนาด 1024×1024	82.65389	81.92783	164.583
ภาพสี ขนาด 256×256	15.61678	15.46146	31.07943
ภาพสี ขนาด 512×512	59.29949	59.20643	118.5072

จากตาราง 4.4 แสดงระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสเพียงจุดภาพเดียวของทั้งภาพสีและภาพสีเทา และจากหัวข้อที่ 4.3 ที่วิเคราะห์จำนวนกุญแจที่เป็นไปได้ทั้งหมดเอาไว้ ดังนั้นเวลาที่ใช้ในการทดลองถอดรหัสด้วยกุญแจทั้งหมดหรือที่เรียกว่า brute force สามารถคำนวณได้จาก ระยะเวลาเฉลี่ยที่ใช้ในการถอดรหัสหนึ่งจุดภาพ × จำนวนกุญแจทั้งหมดที่เป็นไปได้ $(128\times 2^{8192}\times 2^{8192})$ × ขนาดของภาพ ซึ่งสรุปได้ตามตาราง 4.5

ตารางที่ 4.4 ระยะเวลาเฉลี่ยที่ใช้ในการเข้ารหัสและถอดรหัสหนึ่งจุดภาพในหน่วยวินาที

ประเภทของภาพ	เข้ารหัส	ถอดรหัส	รวม
ภาพสีเทา ขนาด 256×256	0.00009289	0.00009110	0.00018401
ภาพสีเทา ขนาด 512×512	0.00008135	0.00008062	0.00016198
ภาพสีเทา ขนาด 1024×1024	0.00007882	0.00007813	0.00015696
เฉลี่ย	0.00008436	0.00008329	0.00016765
ภาพสี ขนาด 256×256	0.00023829	0.00023592	0.00047423
ภาพสี ขนาด 512×512	0.00022621	0.00022585	0.00045207
เฉลี่ย	0.00023225	0.00023089	0.00046315

ตารางที่ 4.5 ระยะเวลาเฉลี่ยที่ใช้ในทดลองการถอดรหัสด้วยกุญแจทั้งหมดโดยประมาณในหน่วยปี

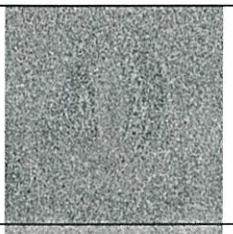
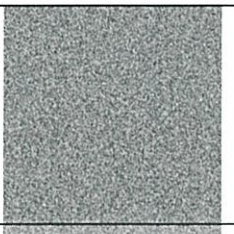
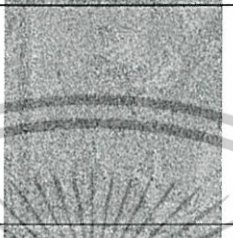
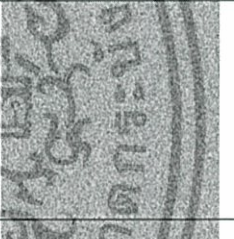
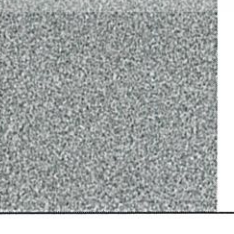
ประเภทของภาพ	เวลาที่ใช้ในการถอดรหัส
ภาพสีเทา ขนาด 256×256	2.6359×10^{4927}
ภาพสีเทา ขนาด 512×512	1.0626×10^{4928}
ภาพสีเทา ขนาด 1024×1024	4.2504×10^{4928}
ภาพสี ขนาด 256×256	7.3641×10^{4927}
ภาพสี ขนาด 512×512	2.9456×10^{4928}

4.5 การทดสอบความสามารถในการปกปิดข้อมูลรูปภาพ

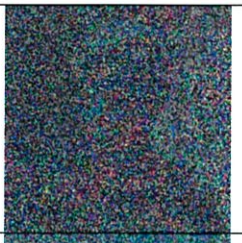
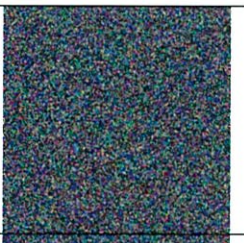
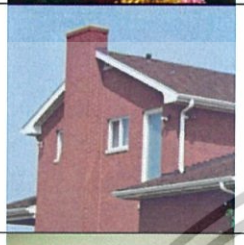
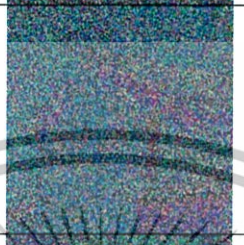
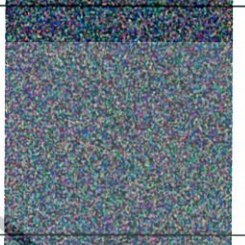
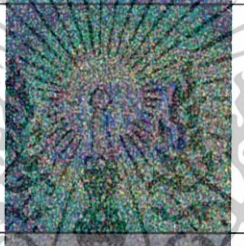
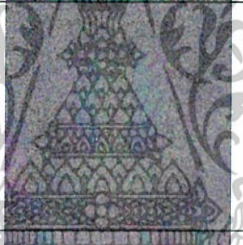
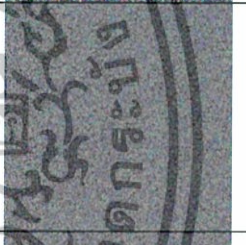
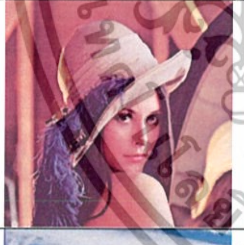
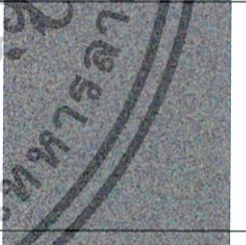
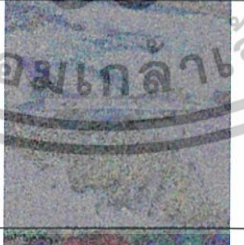
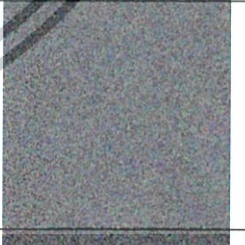
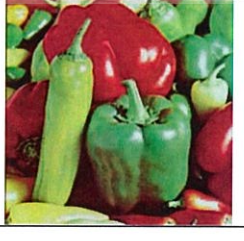
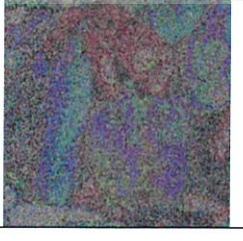
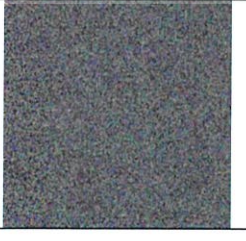
จากการทดลองเข้ารหัสรูปภาพด้วยวิธีการเดิมพบว่าบางกุญแจลับที่มีแอทแทรคเตอร์มีคุณสมบัติตรงตามสมการ 2.9 ไม่สามารถปกปิดข้อมูลภาพได้ แต่เมื่อนำกุญแจเดียวกันนี้มาใช้ในการเข้ารหัสด้วยวิธีที่นำเสนอในบทที่ 3 พบว่าสามารถปกปิดข้อมูลได้ดีกว่าวิธีการเดิมมาก ดังนั้นวิธีการเข้ารหัสแบบใหม่นี้สามารถแก้ไขปัญหากุญแจที่ไม่ดีของวิธีการเดิมได้

จากตาราง 4.6 แสดงตัวอย่างของภาพที่เข้ารหัสด้วยกุญแจ (42, 53, 15) ซึ่งเป็นกุญแจที่ [4] ระบุว่าเป็นกุญแจที่สามารถปกปิดข้อมูลได้ดี และตาราง 4.7 แสดงตัวอย่างของภาพที่เข้ารหัสด้วยกุญแจ (42,99,53) ซึ่งเป็นกุญแจที่วิธีการเข้ารหัสแบบเก่าไม่สามารถปกปิดข้อมูลได้

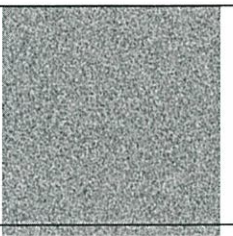
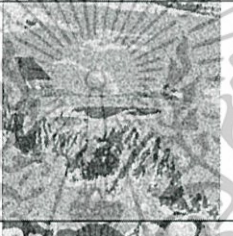
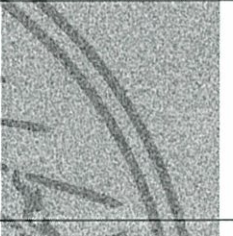
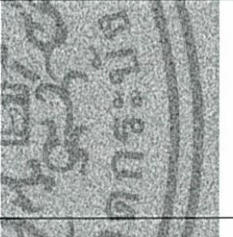
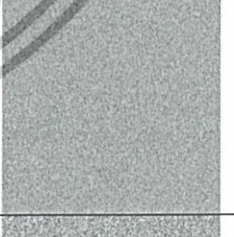
ตารางที่ 4.6 ตัวอย่างรูปภาพที่เข้ารหัสด้วยกุญแจ (42, 53, 15)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		
		
		
		
		

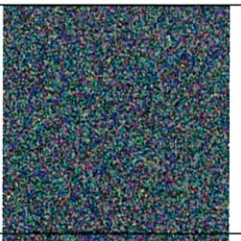
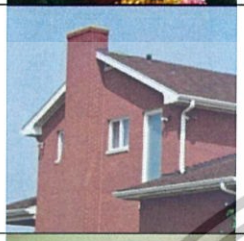
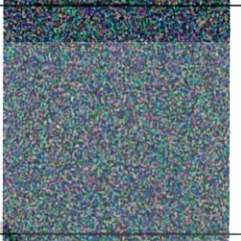
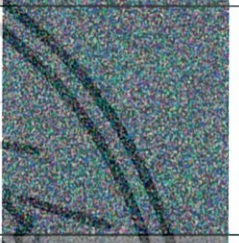
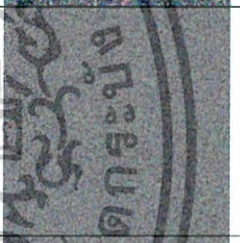
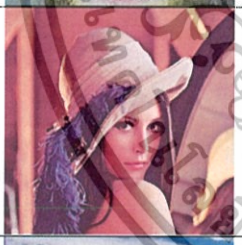
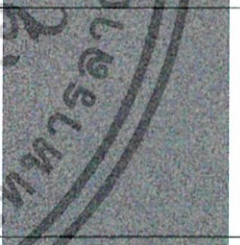
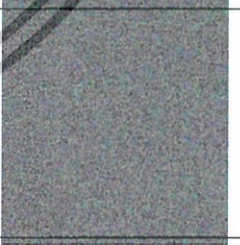
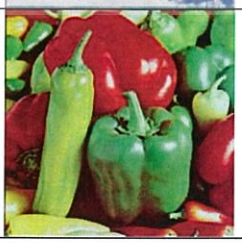
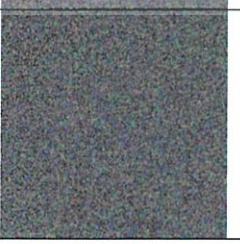
ตารางที่ 4.6(ต่อ) ตัวอย่างรูปภาพที่เข้ารหัสด้วยกุญแจ (42, 53, 15)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		
		
		
		
		

ตารางที่ 4.7 ตัวอย่างรูปภาพที่เข้ารหัสด้วยคุณแจ (42, 99, 53)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		
		
		
		
		

ตารางที่ 4.7(ต่อ) ตัวอย่างรูปภาพที่เข้ารหัสด้วยกุญแจ (42, 99, 53)

ภาพต้นฉบับ	ภาพที่เข้ารหัสด้วยวิธีการเดิม	ภาพที่เข้ารหัสด้วยวิธีการใหม่
		
		
		
		
		
		
		

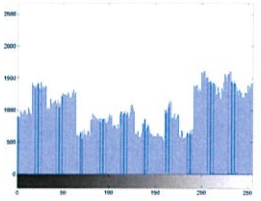
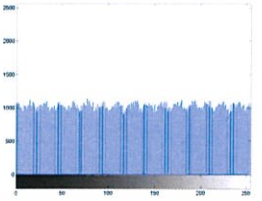
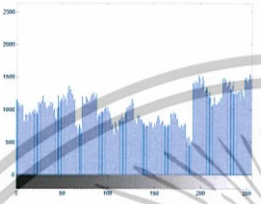
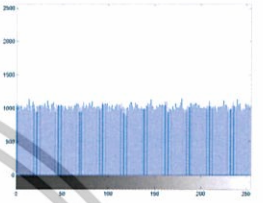
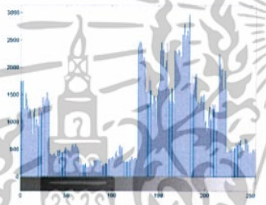
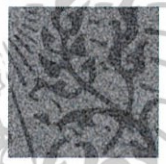
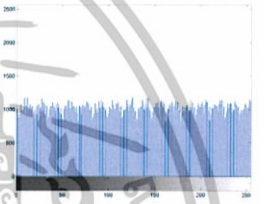
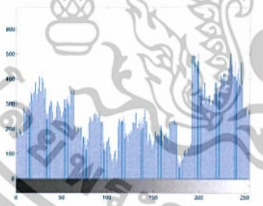
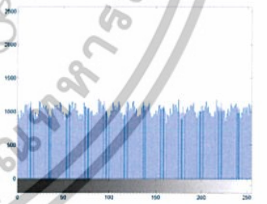
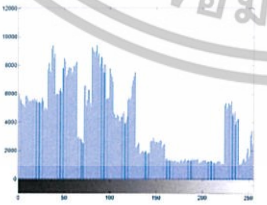
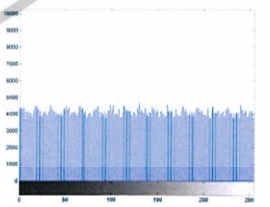
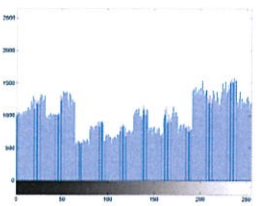
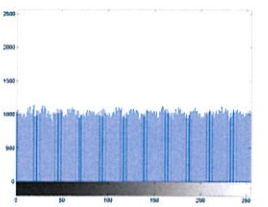
4.6 การทดสอบคุณสมบัติของความสับสน

คุณสมบัติของความสับสนเป็นคุณสมบัติที่สำคัญอย่างหนึ่งของการเข้ารหัสแบบบล็อกไซเฟอร์ เป็นคุณสมบัติที่ต้องการซ่อนความสัมพันธ์ระหว่างไซเฟอร์เท็กซ์และกุญแจลับเพื่อป้องกันการโจมตีด้วยไซเฟอร์เท็กซ์เพื่อค้นหากุญแจลับ

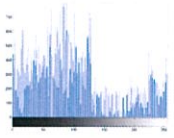
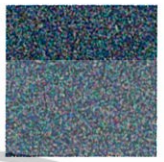
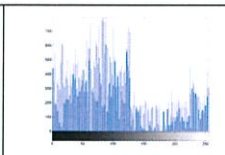
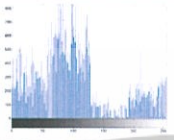
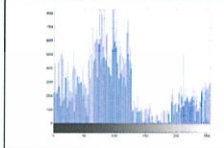
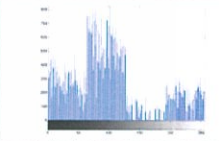
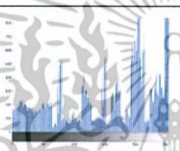
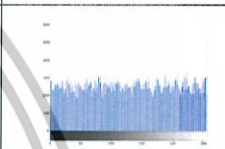
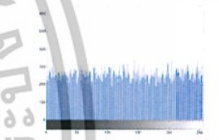
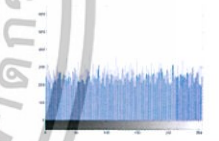
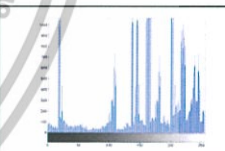
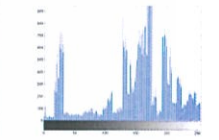
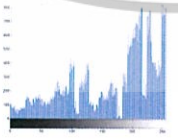
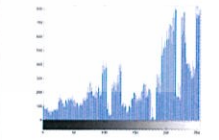
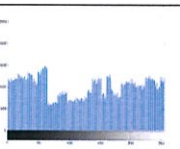
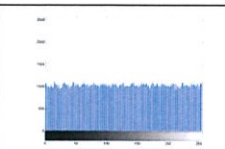
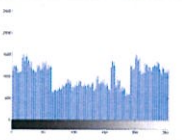
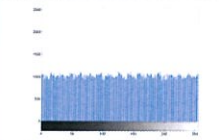
สำหรับการทดสอบคุณสมบัติของความสับสนใช้การเปรียบเทียบค่าฮิสโทแกรมของภาพที่เข้ารหัส ถ้ามีคุณสมบัติของความสับสนค่าฮิสโทแกรมจะมีลักษณะราบเรียบสม่ำเสมอ เนื่องจากค่าความเข้มของแสงมีการกระจายตัวไม่ได้มีเฉพาะค่าใดค่าหนึ่งเพียงอย่างเดียว

จากตาราง 4.8 และ 4.9 แสดงตัวอย่างการเปรียบเทียบฮิสโทแกรมของภาพที่ผ่านการเข้ารหัสทั้งสองวิธีด้วยกุญแจ (42, 99, 53) เห็นได้ชัดเจนว่าภาพที่ได้จากขั้นตอนการเข้ารหัสด้วยวิธีการใหม่มีค่าฮิสโทแกรมที่ราบเรียบสม่ำเสมอกว่าภาพที่ได้จากขั้นตอนการเข้ารหัสด้วยวิธีการเดิม ดังนั้นวิธีการเข้ารหัสแบบใหม่มีคุณสมบัติของความสับสนที่ดีกว่าวิธีการเดิม

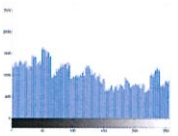
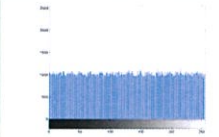
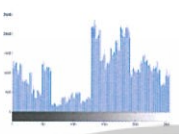
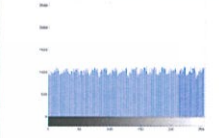
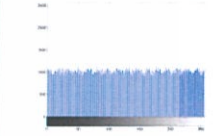
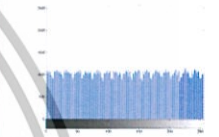
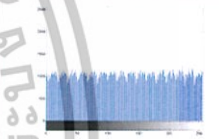
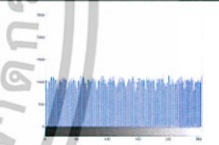
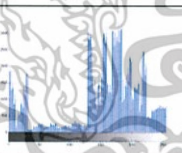
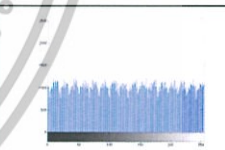
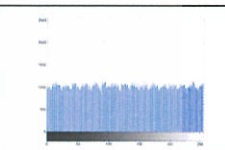
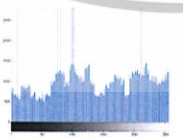
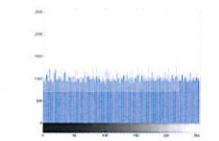
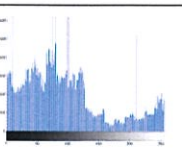
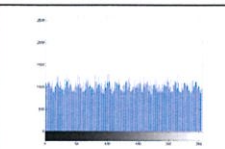
ตารางที่ 4.8 เปรียบเทียบฮิสโทแกรมของภาพสีเทาที่เข้ารหัสทั้งสองวิธีด้วยกุญแจ (42, 99, 53)

วิธีการเข้ารหัสแบบเดิม		วิธีการเข้ารหัสแบบใหม่	
ภาพที่เข้ารหัส	ฮิสโทแกรม	ภาพที่เข้ารหัส	ฮิสโทแกรม
			
			
			
			
			
			
			

ตารางที่ 4.9 เปรียบเทียบฮิสโทแกรมของภาพสีที่เข้ารหัสทั้งสองวิธีด้วยกุญแจ (42, 99, 53)

วิธีการเข้ารหัสแบบเดิม			วิธีการเข้ารหัสแบบใหม่		
ภาพที่เข้ารหัส	ฮิสโทแกรม		ภาพที่เข้ารหัส	ฮิสโทแกรม	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	
	สีน้ำเงิน			สีน้ำเงิน	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	
	สีน้ำเงิน			สีน้ำเงิน	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	
	สีน้ำเงิน			สีน้ำเงิน	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	

ตารางที่ 4.9(ต่อ) เปรียบเทียบฮิสโทแกรมของภาพสีที่เข้ารหัสทั้งสองวิธีด้วยกุญแจ (42, 99, 53)

วิธีการเข้ารหัสแบบเดิม			วิธีการเข้ารหัสแบบใหม่		
ภาพที่เข้ารหัส	ฮิสโทแกรม		ภาพที่เข้ารหัส	ฮิสโทแกรม	
	สีน้ำเงิน			สีน้ำเงิน	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	
	สีน้ำเงิน			สีน้ำเงิน	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	
	สีน้ำเงิน			สีน้ำเงิน	
	สีแดง			สีแดง	
	สีเขียว			สีเขียว	
	สีน้ำเงิน			สีน้ำเงิน	

4.7 การทดสอบคุณสมบัติของการแพร่

คุณสมบัติของการแพร่เป็นคุณสมบัติที่สำคัญอีกอย่างหนึ่งของการเข้ารหัสแบบบล็อกไซเฟอร์ เป็นคุณสมบัติที่ต้องการซ่อนความสัมพันธ์ระหว่างไซเฟอร์เท็กซ์และเพลนเท็กซ์เพื่อป้องกันการโจมตีด้วยไซเฟอร์เท็กซ์เพื่อค้นหาเพลนเท็กซ์

สำหรับการทดสอบคุณสมบัติของการแพร่ใช้การเปรียบเทียบความแตกต่างของภาพที่เข้ารหัสด้วยกุญแจลับที่แตกต่างกัน ซึ่งกุญแจลับที่แตกต่างกันนี้มีความแตกต่างกันเพียง 1 บิตเท่านั้น โดยแบ่งความแตกต่างของกุญแจลับออกเป็น 3 รูปแบบดังต่อไปนี้

1. กุญแจทั้งสองแตกต่างกันที่ตำแหน่งของ rule กุญแจที่ใช้ในการทดสอบกุญแจแรกคือ (2, 75, 15) กุญแจที่สองคือ (3, 72, 15)

2. กุญแจทั้งสองแตกต่างกันที่ตำแหน่งของ seedstate กุญแจที่ใช้ในการทดสอบกุญแจแรกคือ (101, 28, 15) กุญแจที่สองคือ (101, 29, 15)

3. กุญแจทั้งสองแตกต่างกันที่ตำแหน่งของ seedtime กุญแจที่ใช้ในการทดสอบกุญแจแรกคือ (42, 99, 54) กุญแจที่สองคือ (42, 99, 55)

วิธีที่ใช้วัดความแตกต่างระหว่างภาพทั้งสองภาพจะใช้การคำนวณหาอัตราการเปลี่ยนแปลงของจุดภาพหรือเรียกว่า NPCR (Number Pixel Change Rate) ซึ่งสามารถคำนวณได้ตามสมการดังต่อไปนี้

$$NPCR(A,B) = \frac{\sum_{i,j} D(i,j)}{r} \times 100\% \qquad (4.1)$$

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

เมื่อ $NPCR(A,B)$ คือ อัตราการเปลี่ยนแปลงของจุดภาพระหว่างภาพ A และภาพ B

r คือ จำนวนจุดภาพทั้งหมดของภาพ A และภาพ B

$A(i,j)$ คือ ค่าความเข้มแสงของภาพ A ในแถวที่ i หลักที่ j

$B(i,j)$ คือ ค่าความเข้มแสงของภาพ B ในแถวที่ i หลักที่ j

ขั้นตอนวิธีการเข้ารหัสรูปภาพที่มีคุณสมบัติของการแพร่จะมีค่าอัตราการเปลี่ยนแปลงของจุดภาพที่สูง จากการเปรียบเทียบอัตราการเปลี่ยนแปลงของจุดภาพของวิธีการเข้ารหัสทั้งสองวิธีซึ่ง

สรุปได้ในตารางที่ 4.10 พบว่าวิธีการเข้ารหัสแบบใหม่มีอัตราการเปลี่ยนแปลงของจุดภาพที่ใกล้เคียงกับวิธีการเข้ารหัสแบบเดิม ดังนั้นวิธีการเข้ารหัสแบบใหม่จึงมีคุณสมบัติของการแพร่

ตารางที่ 4.10 อัตราการเปลี่ยนแปลงของจุดภาพของกุญแจที่แตกต่างกัน 3 รูปแบบ

ชื่อภาพ	กุญแจที่เปลี่ยนกฎ		กุญแจที่เปลี่ยน seedstate		กุญแจที่เปลี่ยน seedtime	
	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
4.1.01.tiff	76.35	87.22	87.50	86.47	80.06	80.48
4.1.01_gray.tiff	38.14	49.14	50.72	49.09	41.23	41.88
4.1.02.tiff	77.33	86.98	86.80	86.65	80.17	80.96
4.1.02_gray.tiff	39.16	49.50	49.66	48.79	41.48	42.47
4.1.03.tiff	88.73	87.31	85.79	86.73	80.40	80.95
4.1.03_gray.tiff	52.87	49.64	48.05	48.57	41.85	42.28
4.1.04.tiff	78.42	86.86	87.34	86.12	80.18	80.92
4.1.04_gray.tiff	41.50	49.53	51.30	48.77	41.47	42.14
4.1.05.tiff	80.14	87.10	86.62	86.60	80.16	80.67
4.1.05_gray.tiff	41.39	49.20	51.53	48.55	41.57	42.40
4.1.06.tiff	79.49	87.15	85.99	86.54	80.04	80.80
4.1.06_gray.tiff	43.47	49.74	51.06	48.41	41.71	42.51
4.1.07.tiff	86.97	87.02	87.14	86.45	80.21	80.56
4.1.07_gray.tiff	49.17	49.90	49.25	48.46	41.69	42.09
4.1.08.tiff	86.30	87.15	87.19	86.42	80.08	80.62
4.1.08_gray.tiff	48.37	49.62	50.52	48.48	41.88	42.05
4.2.01.tiff	78.71	87.12	87.85	86.43	80.11	80.75
4.2.01_gray.tiff	35.80	49.53	50.25	48.65	41.57	42.39
4.2.02.tiff	87.48	86.95	88.35	86.53	80.30	80.85
4.2.02_gray.tiff	47.79	49.77	50.69	48.58	41.64	42.09
4.2.03.tiff	79.43	87.11	87.51	86.47	80.11	80.69
4.2.03_gray.tiff	43.39	49.42	50.72	48.58	41.70	42.17
4.2.04.tiff	79.13	87.16	86.90	86.45	80.18	80.71

ตารางที่ 4.10(ต่อ) อัตราการเปลี่ยนแปลงของจุดภาพของกุญแจที่แตกต่างกัน 3 รูปแบบ

ชื่อภาพ	กุญแจที่เปลี่ยนกฎ		กุญแจที่เปลี่ยน seedstate		กุญแจที่เปลี่ยน seedtime	
	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
4.2.04_gray.tiff	43.82	49.29	50.40	48.63	41.53	42.33
4.2.05.tiff	85.20	87.15	84.29	86.55	80.16	80.73
4.2.05_gray.tiff	46.45	49.43	46.30	48.47	41.68	42.28
4.2.06.tiff	80.24	86.98	86.94	86.51	80.05	80.72
4.2.06_gray.tiff	42.89	49.65	51.68	48.73	41.64	42.36
4.2.07.tiff	80.94	87.17	87.58	86.51	80.20	80.79
4.2.07_gray.tiff	43.11	49.50	49.78	48.74	41.54	42.06
5.1.09.tiff	44.85	49.44	49.68	48.26	41.80	42.00
5.1.10.tiff	42.12	49.42	49.49	48.69	41.54	42.32
5.1.11.tiff	49.25	49.82	48.17	48.63	41.76	42.69
5.1.12.tiff	45.18	49.76	50.18	49.03	41.72	42.48
5.1.13.tiff	46.99	48.07	52.57	48.59	41.75	42.02
5.1.14.tiff	38.81	49.35	50.30	48.74	41.74	41.84
5.2.08.tiff	42.93	49.54	50.08	48.84	41.66	42.15
5.2.09.tiff	49.27	49.46	48.62	48.81	41.75	42.27
5.2.10.tiff	39.49	49.57	50.31	48.72	41.73	42.19
5.3.01.tiff	41.22	49.46	49.75	48.71	41.60	42.22
5.3.02.tiff	35.91	49.38	51.01	48.64	41.61	42.29
7.1.01.tiff	36.19	49.68	49.73	48.69	41.44	42.23
7.1.02.tiff	52.29	49.50	54.99	48.75	41.60	42.35
7.1.03.tiff	49.90	49.34	48.58	48.73	41.67	42.41
7.1.04.tiff	43.47	49.45	49.27	48.95	41.55	42.24
7.1.05.tiff	38.93	49.36	49.97	48.75	41.61	42.16
7.1.06.tiff	36.03	49.31	49.33	48.64	41.48	42.30
7.1.07.tiff	35.69	49.37	50.10	48.72	41.62	42.23
7.1.08.tiff	50.82	49.16	48.90	48.69	41.53	42.40

ตารางที่ 4.10(ต่อ) อัตราการเปลี่ยนแปลงของจุดภาพของกุญแจที่แตกต่างกัน 3 รูปแบบ

ชื่อภาพ	กุญแจที่เปลี่ยนกฎ		กุญแจที่เปลี่ยน seedstate		กุญแจที่เปลี่ยน seedtime	
	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่	วิธีการเข้ารหัสแบบเดิม	วิธีการเข้ารหัสแบบใหม่
7.1.09.tiff	45.32	49.40	49.82	48.78	41.66	42.22
7.1.10.tiff	42.78	49.31	49.33	48.68	41.63	42.26
7.2.01.tiff	39.79	49.23	48.61	48.74	41.60	42.18
boat.512.tiff	49.37	49.30	49.64	48.65	41.55	42.19
elaine.512.tiff	44.04	49.57	50.10	48.71	41.74	42.05
gray21.512.tiff	43.30	49.51	49.59	48.67	41.67	42.27
house.tiff	84.52	87.05	86.92	86.41	80.07	80.60
house_gray.tiff	48.22	49.54	48.61	48.56	41.64	42.20
numbers.512.tiff	40.68	49.52	49.60	48.67	41.62	42.23
ruler.512.tiff	46.49	48.18	52.52	48.65	41.74	42.29
testpat.1k.tiff	45.63	49.91	49.04	48.66	41.64	42.25
เฉลี่ย	53.86	59.47	59.84	58.76	51.91	52.50

บทที่ 5
สรุปผลและข้อเสนอแนะ

5.1 สรุปผลและวิเคราะห์ผลการทดลอง

วิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐานที่ได้นำเสนอไปนั้น เป็นวิธีการที่ใช้คุณสมบัติพิเศษของเซลลูลาร์ออโตมาตาแบบพื้นฐาน ที่แผนภาพการเปลี่ยนสถานะของเซลลูลาร์ออโตมาตาแบบพื้นฐานได้วนกลับไปยังสถานะเริ่มต้น ซึ่งเรียกว่าแอทแทรคเตอร์ ได้ถูกนำมาใช้ในการสร้างกุญแจสำหรับการเข้ารหัสรูปภาพ ซึ่งวิธีที่ได้นำเสนอนี้เป็นวิธีการที่ได้ปรับปรุงจากงานวิจัย [4] ด้วยการใช้ตัวสร้างเลขสุ่มเทียมเลือกสถานะเริ่มต้นของแอทแทรคเตอร์ที่ใช้กับแต่ละตำแหน่งจุดภาพ เพื่อเป็นการเพิ่มจำนวนกุญแจทั้งหมดที่เป็นไปได้ในการเข้ารหัส นอกจากนี้ ยังใช้การสลับตำแหน่งของบิตของค่าความเข้มแสงในแต่ละตำแหน่งของจุดภาพเพื่อช่วยเพิ่มความสามารถในการปกปิดข้อมูลให้ดียิ่งขึ้นอีกด้วย

ในส่วนของการทดสอบประสิทธิภาพของวิธีการเข้ารหัสที่ได้นำเสนอไว้ในบทที่ 4 ได้แสดงให้เห็นว่าวิธีการเข้ารหัสแบบใหม่นี้สามารถแก้ไขกุญแจที่มีปัญหาในวิธีการเข้ารหัสแบบเดิมที่ไม่สามารถปกปิดข้อมูลได้ ให้สามารถปกปิดข้อมูลได้ดียิ่งขึ้นกว่าเดิม รวมทั้งยังมีคุณสมบัติของความสับสนและคุณสมบัติของการแพร่ที่เป็นคุณสมบัติที่สำคัญของการเข้ารหัสแบบบล็อคไซเฟอร์อีกด้วย

สำหรับข้อจำกัดของวิธีการเข้ารหัสที่ปรับปรุงแล้วคือ ยังมีกุญแจบางส่วนที่ยังไม่สามารถปกปิดข้อมูลได้ นอกจากนี้จำนวนกุญแจทั้งหมดที่เป็นไปได้ในการเข้ารหัสข้อมูลอาจจะยังน้อยเกินไปเมื่อเทียบกับวิธีการเข้ารหัสแบบอื่น

5.2 แนวทางการพัฒนางานวิจัย

1. ปรับปรุงวิธีการเข้ารหัสให้สามารถใช้กับรูปภาพหลากหลายประเภทขึ้น เช่น ให้สามารถใช้กับภาพขาวดำได้ เป็นต้น

2. ปรับปรุงขั้นตอนการเข้ารหัสให้สามารถนำแอทแทรคเตอร์ที่ไม่มีคุณสมบัติตามสมการที่ 2.9 มาใช้ในการเข้ารหัสได้

3. เปลี่ยนวิธีการเข้ารหัสรูปภาพให้เป็นการเข้ารหัสข้อมูลทั่วไป

เอกสารอ้างอิง

[1] Allan G. Weber, **The USC–SIPI Image Database: Version 5.** [Online]. Available : http://sipi.usc.edu/database/. 2006.

[2] Behrouz A. Forouzan, **Cryptography and Network Security.** McGraw – Hill, 2008.

[3] F. Maleki, A. Mohades, S. Mehdi Hashemi and M.E. Shiri, **An Image Encryption System by Cellular Automata with Memory.** The Third International Conference on Availability, Reliability and Security, 2008. pp.1266 – 1271.

[4] Jin Jun, **Image Encryption Method Based on Elementary Cellular Automata.** IEEE Southeastcon, 2009. pp. 345 – 349.

[5] Maria Petrou and Panagiota Bosdogiani, **Image Processing : the fundamentals.** John Wiley & Sons Ltd, 1999.

[6] Maryam Habibipour, Mehdi Yaghobi, Saeed Rahati – Q and Zohreh souzanchi – K, **An Image Encryption System by Indefinite Cellular Automata and Chos.** 2nd International Conference on Signal Processing Systems (ICSPS), vol. 3, 2010. pp. 23 – 27.

[7] M.Habibipour, R.Maarefdoust, M. Yaghobi and S. Rahati, **An Image Encryption System by 2D Memorized Cellular Automata and Chaos Mapping.** 6th International Conference on Digital Content, Multimedia Technology and its Applications (IDC), 2010. pp. 331 – 336

[8] Puhua G., **Cellular automaton public-key cryptosystem.** Complex Systems, vol. 1,1987. pp. 51 – 57.

[9] Rong – Jian Chen and Jui – Lin Lai, **Novel Stream Cipher Using 2-D Hybrid CA and Variable Ordered Recursive CA Substitutions.** IFIP International conference on Netwoek and Parallel Computing, 2008. pp. 74 – 81.

[10] Rong – Jian Chen, Wen – Kai Lu and Jui – Lin Lai, **Image Encryption Using Progressive Cellular Automata Substitution and SCAN.** IEEE International Symposium on Circuits and Systems, 2005. pp. 1690 – 1693.

[11] Rong – Jian Chen, Yuan – Hsin Chen, Chao – Shen Chen and Jui – Lin Lai, **Image Encryption/Decryption System Using 2-D Cellular Automata.** IEEE Tenth Internationa Symposium on Consumer Electronics, 2006. pp. 1 – 6.

เอกสารอ้างอิง(ต่อ)

[12] Robert J. Jenkins Jr., **ISAAC : a fast cryptographic random number generator.** [online]. Available : http://www.burtleburtle.net/bob/rand/isaacafa.html.

[13] Stephen W., **Cellular automata and complexity : collected papers.** Addison – Wesley Publishing, 1994.

[14] Uvais Qidwai and C.H. Chen, **Digital image processing : an algorithmic approach with MATLAB.** Taylor and Francis Group, 2010.

[15] Weisstein, Eric W., **Elementary Cellular Automaton.** [Online]. Available : http://mathworld.wolfram.com/ElementaryCellularAutomaton.html. 2011.

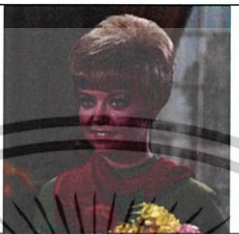
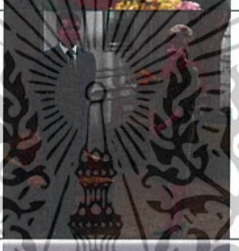
[16] Zhao Xuelong, Li Qianmu, Xu Manwu and Liu Fengyu, **A Symmetric Cryptography Based on Extended Cellular Automata.** IEEE International Conference on Systems, Man and Cybernetics, vol. 1, 2005. pp. 499 – 503

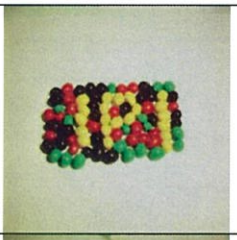
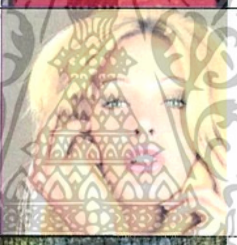
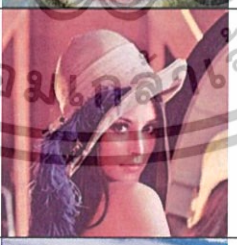
[17] นิรุธ อำนวยศิลป์. **การประมวลผลภาพและวีดีโอด้วย C/C++. เล่ม 1,** ด่านสุทธาการพิมพ์.

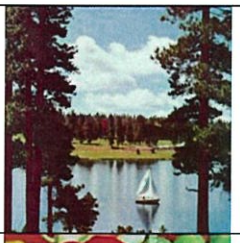
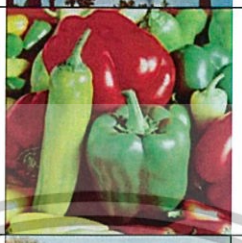
ภาคผนวก ก

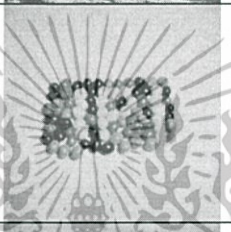
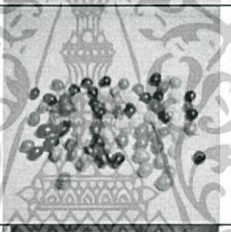
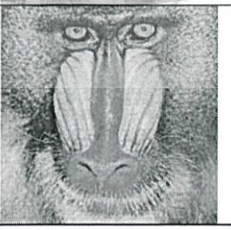
รูปภาพที่ใช้ในการทดลอง

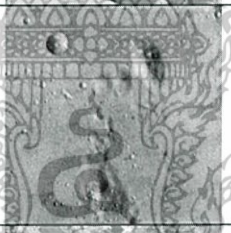
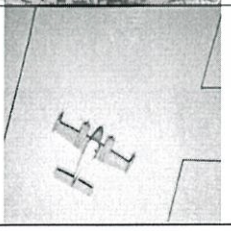
สามารถดาวน์โหลดได้จาก http://sipi.usc.edu/database/ [1]

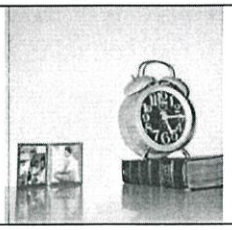
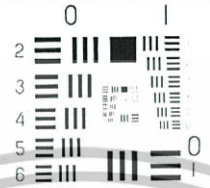
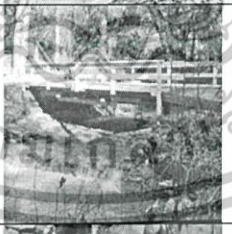
ชื่อภาพ	รูปภาพ	ขนาด
4.1.01.tiff		256×256
4.1.02.tiff		256×256
4.1.03.tiff		256×256
4.1.04.tiff		256×256
4.1.05.tiff		256×256
4.1.06.tiff		256×256

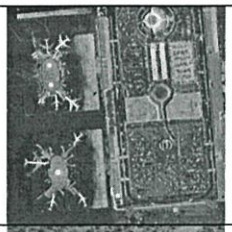
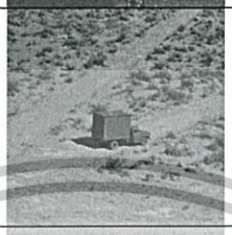
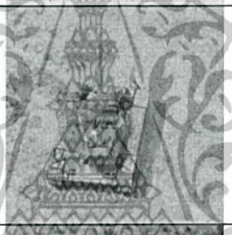
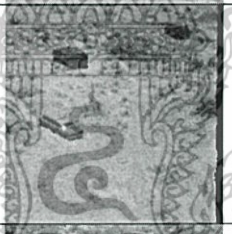
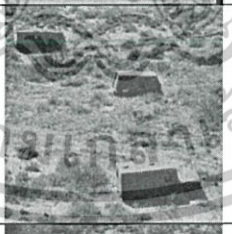
ชื่อภาพ	รูปภาพ	ขนาด
4.1.07.tiff		256×256
4.1.08.tiff		256×256
4.2.01.tiff		512×512
4.2.02.tiff		512×512
4.2.03.tiff		512×512
4.2.04.tiff		512×512
4.2.05.tiff		512×512

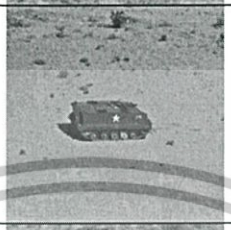
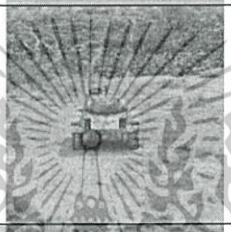
ชื่อภาพ	รูปภาพ	ขนาด
4.2.06.tiff		512×512
4.2.07.tiff		512×512
house.tiff		512×512
4.1.01_gray.tiff		256×256
4.1.02_gray.tiff		256×256
4.1.03_gray.tiff		256×256
4.1.04_gray.tiff		256×256

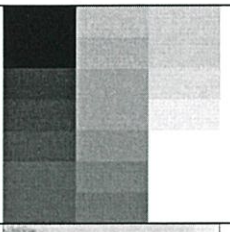
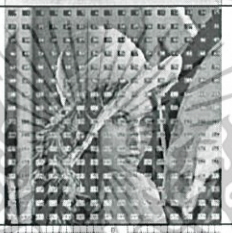
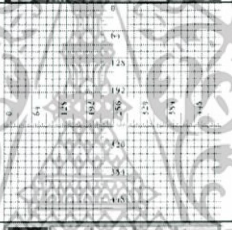
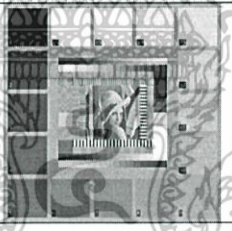
ชื่อภาพ	รูปภาพ	ขนาด
4.1.05_gray.tiff		256×256
4.1.06_gray.tiff		256×256
4.1.07_gray.tiff		256×256
4.1.08_gray.tiff		256×256
4.2.01_gray.tiff		512×512
4.2.02_gray.tiff		512×512
4.2.03_gray.tiff		512×512

ชื่อภาพ	รูปภาพ	ขนาด
4.2.04_gray.tiff		512×512
4.2.05_gray.tiff		512×512
4.2.06_gray.tiff		512×512
4.2.07_gray.tiff		512×512
5.1.09.tiff		256×256
5.1.10.tiff		256×256
5.1.11.tiff		256×256

ชื่อภาพ	รูปภาพ	ขนาด
5.1.12.tiff		256×256
5.1.13.tiff		256×256
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

ชื่อภาพ	รูปภาพ	ขนาด
5.3.02.tiff		1024×1024
7.1.01.tiff		512×512
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

ชื่อภาพ	รูปภาพ	ขนาด
7.1.07.tiff		512×512
7.1.08.tiff		512×512
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

ชื่อภาพ	รูปภาพ	ขนาด
gray21.512.tiff		512×512
house_gray.tiff		512×512
numbers.512.tiff		512×512
ruler.512.tiff		512×512
testpat.1k.tiff		1024×1024

ภาคผนวก ข

กฎและแอทแทรคเตอร์ที่สามารถใช้ในการเข้ารหัสได้

กฎ	สถานะ
2	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
3	9 -> 228 -> 18 -> 201 -> 36 -> 147 -> 72 -> 39 -> 144 -> 78 -> 33 -> 156 -> 66 -> 57 -> 132 -> 114 -> 9, 19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100 -> 19
10	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9, 51 -> 153 -> 204 -> 102 -> 51
11	3 -> 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3, 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129 -> 252 -> 6, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120 -> 15, 51 -> 153 -> 204 -> 102 -> 51
14	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106 -> 43, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105 -> 45, 51 -> 153 -> 204 -> 102 -> 51, 53 -> 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53,

กฎ	สถานะ
15	3 -> 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3, 5 -> 245 -> 20 -> 215 -> 80 -> 95 -> 65 -> 125 -> 5, 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129 -> 252 -> 6, 9 -> 237 -> 36 -> 183 -> 144 -> 222 -> 66 -> 123 -> 9, 10 -> 235 -> 40 -> 175 -> 160 -> 190 -> 130 -> 250 -> 10, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120 -> 15, 18 -> 219 -> 72 -> 111 -> 33 -> 189 -> 132 -> 246 -> 18, 23 -> 209 -> 92 -> 71 -> 113 -> 29 -> 197 -> 116 -> 23, 27 -> 201 -> 108 -> 39 -> 177 -> 156 -> 198 -> 114 -> 27, 43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106 -> 43, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105 -> 45, 46 -> 163 -> 184 -> 142 -> 226 -> 58 -> 139 -> 232 -> 46, 51 -> 153 -> 204 -> 102 -> 51, 53 -> 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53, 54 -> 147 -> 216 -> 78 -> 99 -> 57 -> 141 -> 228 -> 54
16	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9
17	9 -> 114 -> 132 -> 57 -> 66 -> 156 -> 33 -> 78 -> 144 -> 39 -> 72 -> 147 -> 36 -> 201 -> 18 -> 228 -> 9, 19 -> 100 -> 137 -> 50 -> 196 -> 25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200 -> 19
18	3 -> 132 -> 75 -> 48 -> 72 -> 180 -> 3, 6 -> 9 -> 150 -> 96 -> 144 -> 105 -> 6, 12 -> 18 -> 45 -> 192 -> 33 -> 210 -> 12, 24 -> 36 -> 90 -> 129 -> 66 -> 165 -> 24
22	5 -> 141 -> 80 -> 216 -> 5, 10 -> 27 -> 160 -> 177 -> 10, 20 -> 54 -> 65 -> 99 -> 20, 40 -> 108 -> 130 -> 198 -> 40

กฎ	สถานะ
24	1 -> 254 -> 2 -> 253 -> 4 -> 251 -> 8 -> 247 -> 16 -> 239 -> 32 -> 223 -> 64 -> 191 -> 128 -> 127 -> 1, 9 -> 246 -> 18 -> 237 -> 36 -> 219 -> 72 -> 183 -> 144 -> 111 -> 33 -> 222 -> 66 -> 189 -> 132 -> 123 -> 9, 17 -> 238 -> 34 -> 221 -> 68 -> 187 -> 136 -> 119 -> 17
27	1 -> 254 -> 2 -> 253 -> 4 -> 251 -> 8 -> 247 -> 16 -> 239 -> 32 -> 223 -> 64 -> 191 -> 128 -> 127 -> 1, 9 -> 246 -> 18 -> 237 -> 36 -> 219 -> 72 -> 183 -> 144 -> 111 -> 33 -> 222 -> 66 -> 189 -> 132 -> 123 -> 9, 17 -> 238 -> 34 -> 221 -> 68 -> 187 -> 136 -> 119 -> 17
30	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 -> 131 -> 196 -> 111 -> 33 -> 243 -> 28 -> 38 -> 123 -> 9 -> 159 -> 224 -> 49 -> 219 -> 72 -> 252 -> 7, 17 -> 187 -> 136 -> 221 -> 68 -> 238 -> 34 -> 119 -> 17
34	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
35	9 -> 228 -> 18 -> 201 -> 36 -> 147 -> 72 -> 39 -> 144 -> 78 -> 33 -> 156 -> 66 -> 57 -> 132 -> 114 -> 9, 19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100 -> 19
38	11 -> 140 -> 194 -> 35 -> 176 -> 200 -> 44 -> 50 -> 11, 22 -> 25 -> 133 -> 70 -> 97 -> 145 -> 88 -> 100 -> 22
39	1 -> 253 -> 2 -> 251 -> 4 -> 247 -> 8 -> 239 -> 16 -> 223 -> 32 -> 191 -> 64 -> 127 -> 128 -> 254 -> 1, 9 -> 237 -> 18 -> 219 -> 36 -> 183 -> 72 -> 111 -> 144 -> 222 -> 33 -> 189 -> 66 -> 123 -> 132 -> 246 -> 9, 17 -> 221 -> 34 -> 187 -> 68 -> 119 -> 136 -> 238 -> 17

กฎ	สถานะ
42	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9, 27 -> 141 -> 198 -> 99 -> 177 -> 216 -> 108 -> 54 -> 27, 43 -> 149 -> 202 -> 101 -> 178 -> 89 -> 172 -> 86 -> 43, 45 -> 150 -> 75 -> 165 -> 210 -> 105 -> 180 -> 90 -> 45, 51 -> 153 -> 204 -> 102 -> 51, 53 -> 154 -> 77 -> 166 -> 83 -> 169 -> 212 -> 106 -> 53
43	3 -> 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3, 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129 -> 252 -> 6, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120 -> 15, 43 -> 149 -> 202 -> 101 -> 178 -> 89 -> 172 -> 86 -> 43, 45 -> 150 -> 75 -> 165 -> 210 -> 105 -> 180 -> 90 -> 45, 51 -> 153 -> 204 -> 102 -> 51, 53 -> 154 -> 77 -> 166 -> 83 -> 169 -> 212 -> 106 -> 53
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 -> 28 -> 197 -> 86 -> 122 -> 14 -> 226 -> 43 -> 61 -> 7, 13 -> 103 -> 161 -> 236 -> 52 -> 157 -> 134 -> 179 -> 208 -> 118 -> 26 -> 206 -> 67 -> 217 -> 104 -> 59 -> 13
46	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 27 -> 141 -> 198 -> 99 -> 177 -> 216 -> 108 -> 54 -> 27, 51 -> 153 -> 204 -> 102 -> 51
47	3 -> 249 -> 12 -> 231 -> 48 -> 159 -> 192 -> 126 -> 3, 6 -> 243 -> 24 -> 207 -> 96 -> 63 -> 129 -> 252 -> 6, 15 -> 225 -> 60 -> 135 -> 240 -> 30 -> 195 -> 120 -> 15, 51 -> 153 -> 204 -> 102 -> 51
48	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130 -> 5, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9

กฎ	สถานะ
49	9 -> 114 -> 132 -> 57 -> 66 -> 156 -> 33 -> 78 -> 144 -> 39 -> 72 -> 147 -> 36 -> 201 -> 18 -> 228 -> 9, 19 -> 100 -> 137 -> 50 -> 196 -> 25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200 -> 19
52	13 -> 19 -> 52 -> 76 -> 208 -> 49 -> 67 -> 196 -> 13, 26 -> 38 -> 104 -> 152 -> 161 -> 98 -> 134 -> 137 -> 26
53	1 -> 127 -> 128 -> 191 -> 64 -> 223 -> 32 -> 239 -> 16 -> 247 -> 8 -> 251 -> 4 -> 253 -> 2 -> 254 -> 1, 9 -> 123 -> 132 -> 189 -> 66 -> 222 -> 33 -> 111 -> 144 -> 183 -> 72 -> 219 -> 36 -> 237 -> 18 -> 246 -> 9, 17 -> 119 -> 136 -> 187 -> 68 -> 221 -> 34 -> 238 -> 17
54	17 -> 187 -> 68 -> 238 -> 17, 23 -> 184 -> 197 -> 46 -> 113 -> 139 -> 92 -> 226 -> 23, 29 -> 163 -> 116 -> 142 -> 209 -> 58 -> 71 -> 232 -> 29, 34 -> 119 -> 136 -> 221 -> 34
56	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130 -> 5, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9
58	55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55
59	27 -> 237 -> 54 -> 219 -> 108 -> 183 -> 216 -> 111 -> 177 -> 222 -> 99 -> 189 -> 198 -> 123 -> 141 -> 246 -> 27, 55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55
62	55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55
63	27 -> 237 -> 54 -> 219 -> 108 -> 183 -> 216 -> 111 -> 177 -> 222 -> 99 -> 189 -> 198 -> 123 -> 141 -> 246 -> 27, 55 -> 217 -> 110 -> 179 -> 220 -> 103 -> 185 -> 206 -> 115 -> 157 -> 230 -> 59 -> 205 -> 118 -> 155 -> 236 -> 55
66	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9

กฎ	สถานะ
74	7 -> 133 -> 193 -> 97 -> 112 -> 88 -> 28 -> 22 -> 7, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9, 11 -> 131 -> 194 -> 224 -> 176 -> 56 -> 44 -> 14 -> 11, 27 -> 155 -> 218 -> 216 -> 220 -> 214 -> 198 -> 230 -> 182 -> 54 -> 55 -> 181 -> 177 -> 185 -> 173 -> 141 -> 205 -> 109 -> 108 -> 110 -> 107 -> 99 -> 115 -> 91 -> 27
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 -> 11, 19 -> 203 -> 98 -> 121 -> 76 -> 47 -> 137 -> 229 -> 49 -> 188 -> 38 -> 151 -> 196 -> 242 -> 152 -> 94 -> 19
80	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129 -> 3, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9, 51 -> 102 -> 204 -> 153 -> 51
81	3 -> 126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3, 6 -> 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225 -> 15, 51 -> 102 -> 204 -> 153 -> 51
83	1 -> 254 -> 128 -> 127 -> 64 -> 191 -> 32 -> 223 -> 16 -> 239 -> 8 -> 247 -> 4 -> 251 -> 2 -> 253 -> 1, 9 -> 246 -> 132 -> 123 -> 66 -> 189 -> 33 -> 222 -> 144 -> 111 -> 72 -> 183 -> 36 -> 219 -> 18 -> 237 -> 9, 17 -> 238 -> 136 -> 119 -> 68 -> 187 -> 34 -> 221 -> 17
84	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129 -> 3, 43 -> 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165 -> 45, 51 -> 102 -> 204 -> 153 -> 51, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149 -> 53

กฎ	สถานะ
85	3 -> 126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3, 5 -> 125 -> 65 -> 95 -> 80 -> 215 -> 20 -> 245 -> 5, 6 -> 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6, 9 -> 123 -> 66 -> 222 -> 144 -> 183 -> 36 -> 237 -> 9, 10 -> 250 -> 130 -> 190 -> 160 -> 175 -> 40 -> 235 -> 10, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225 -> 15, 18 -> 246 -> 132 -> 189 -> 33 -> 111 -> 72 -> 219 -> 18, 23 -> 116 -> 197 -> 29 -> 113 -> 71 -> 92 -> 209 -> 23, 27 -> 114 -> 198 -> 156 -> 177 -> 39 -> 108 -> 201 -> 27, 43 -> 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165 -> 45, 46 -> 232 -> 139 -> 58 -> 226 -> 142 -> 184 -> 163 -> 46, 51 -> 102 -> 204 -> 153 -> 51, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149 -> 53, 54 -> 228 -> 141 -> 57 -> 99 -> 78 -> 216 -> 147 -> 54
86	7 -> 140 -> 219 -> 18 -> 63 -> 224 -> 145 -> 123 -> 66 -> 231 -> 28 -> 50 -> 111 -> 72 -> 252 -> 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, 17 -> 187 -> 34 -> 119 -> 68 -> 238 -> 136 -> 221 -> 17
88	7 -> 13 -> 28 -> 52 -> 112 -> 208 -> 193 -> 67 -> 7, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9, 14 -> 26 -> 56 -> 104 -> 224 -> 161 -> 131 -> 134 -> 14, 27 -> 59 -> 107 -> 99 -> 103 -> 109 -> 108 -> 236 -> 173 -> 141 -> 157 -> 181 -> 177 -> 179 -> 182 -> 54 -> 118 -> 214 -> 198 -> 206 -> 218 -> 216 -> 217 -> 91 -> 27
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 -> 13, 25 -> 122 -> 200 -> 211 -> 70 -> 158 -> 50 -> 244 -> 145 -> 167 -> 140 -> 61 -> 100 -> 233 -> 35 -> 79 -> 25

กฎ	สถานะ
98	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 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 -> 7, 11 -> 110 -> 88 -> 115 -> 194 -> 155 -> 22 -> 220 -> 176 -> 230 -> 133 -> 55 -> 44 -> 185 -> 97 -> 205 -> 11
105	5 -> 114 -> 80 -> 39 -> 5, 10 -> 228 -> 160 -> 78 -> 10, 15 -> 105 -> 240 -> 150 -> 15, 20 -> 201 -> 65 -> 156 -> 20, 27 -> 95 -> 177 -> 245 -> 27, 30 -> 210 -> 225 -> 45 -> 30, 40 -> 147 -> 130 -> 57 -> 40, 54 -> 190 -> 99 -> 235 -> 54, 60 -> 165 -> 195 -> 90 -> 60, 75 -> 135 -> 180 -> 120 -> 75, 108 -> 125 -> 198 -> 215 -> 108, 141 -> 175 -> 216 -> 250 -> 141
106	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
112	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129 -> 3, 5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130 -> 5, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9, 27 -> 54 -> 108 -> 216 -> 177 -> 99 -> 198 -> 141 -> 27, 43 -> 86 -> 172 -> 89 -> 178 -> 101 -> 202 -> 149 -> 43, 45 -> 90 -> 180 -> 105 -> 210 -> 165 -> 75 -> 150 -> 45, 51 -> 102 -> 204 -> 153 -> 51 53 -> 106 -> 212 -> 169 -> 83 -> 166 -> 77 -> 154 -> 53

กฎ	สถานะ
113	3 -> 126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3, 6 -> 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225 -> 15, 43 -> 86 -> 172 -> 89 -> 178 -> 101 -> 202 -> 149 -> 43, 45 -> 90 -> 180 -> 105 -> 210 -> 165 -> 75 -> 150 -> 45, 51 -> 102 -> 204 -> 153 -> 51, 53 -> 106 -> 212 -> 169 -> 83 -> 166 -> 77 -> 154 -> 53
114	55 -> 236 -> 155 -> 118 -> 205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103 -> 220 -> 179 -> 110 -> 217 -> 55
115	27 -> 246 -> 141 -> 123 -> 198 -> 189 -> 99 -> 222 -> 177 -> 111 -> 216 -> 183 -> 108 -> 219 -> 54 -> 237 -> 27, 55 -> 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 -> 3, 27 -> 54 -> 108 -> 216 -> 177 -> 99 -> 198 -> 141 -> 27, 51 -> 102 -> 204 -> 153 -> 51
117	3 -> 126 -> 192 -> 159 -> 48 -> 231 -> 12 -> 249 -> 3, 6 -> 252 -> 129 -> 63 -> 96 -> 207 -> 24 -> 243 -> 6, 15 -> 120 -> 195 -> 30 -> 240 -> 135 -> 60 -> 225 -> 15, 51 -> 102 -> 204 -> 153 -> 51
118	55 -> 236 -> 155 -> 118 -> 205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103 -> 220 -> 179 -> 110 -> 217 -> 55
119	27 -> 246 -> 141 -> 123 -> 198 -> 189 -> 99 -> 222 -> 177 -> 111 -> 216 -> 183 -> 108 -> 219 -> 54 -> 237 -> 27, 55 -> 236 -> 155 -> 118 -> 205 -> 59 -> 230 -> 157 -> 115 -> 206 -> 185 -> 103 -> 220 -> 179 -> 110 -> 217 -> 55
120	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130 -> 5, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9

กฎ	สถานะ
122	7 -> 141 -> 223 -> 112 -> 216 -> 253 -> 7, 14 -> 27 -> 191 -> 224 -> 177 -> 251 -> 14, 28 -> 54 -> 127 -> 193 -> 99 -> 247 -> 28, 56 -> 108 -> 254 -> 131 -> 198 -> 239 -> 56
126	7 -> 141 -> 223 -> 112 -> 216 -> 253 -> 7, 14 -> 27 -> 191 -> 224 -> 177 -> 251 -> 14, 28 -> 54 -> 127 -> 193 -> 99 -> 247 -> 28, 56 -> 108 -> 254 -> 131 -> 198 -> 239 -> 56
129	1 -> 124 -> 57 -> 16 -> 199 -> 147 -> 1, 2 -> 248 -> 114 -> 32 -> 143 -> 39 -> 2, 4 -> 241 -> 228 -> 64 -> 31 -> 78 -> 4, 8 -> 227 -> 201 -> 128 -> 62 -> 156 -> 8
130	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
131	19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100 -> 19
135	3 -> 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 -> 17
138	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9, 15 -> 135 -> 195 -> 225 -> 240 -> 120 -> 60 -> 30 -> 15, 39 -> 147 -> 201 -> 228 -> 114 -> 57 -> 156 -> 78 -> 39, 51 -> 153 -> 204 -> 102 -> 51, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126 -> 63
139	39 -> 147 -> 201 -> 228 -> 114 -> 57 -> 156 -> 78 -> 39, 51 -> 153 -> 204 -> 102 -> 51, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126 -> 63

กฎ	สถานะ
142	3 -> 129 -> 192 -> 96 -> 48 -> 24 -> 12 -> 6 -> 3, 15 -> 135 -> 195 -> 225 -> 240 -> 120 -> 60 -> 30 -> 15, 43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106 -> 43, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105 -> 45, 51 -> 153 -> 204 -> 102 -> 51, 53 -> 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126 -> 63
143	43 -> 169 -> 172 -> 166 -> 178 -> 154 -> 202 -> 106 -> 43, 45 -> 165 -> 180 -> 150 -> 210 -> 90 -> 75 -> 105 -> 45, 51 -> 153 -> 204 -> 102 -> 51, 53 -> 149 -> 212 -> 86 -> 83 -> 89 -> 77 -> 101 -> 53, 63 -> 159 -> 207 -> 231 -> 243 -> 249 -> 252 -> 126 -> 63
144	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9
145	19 -> 100 -> 137 -> 50 -> 196 -> 25 -> 98 -> 140 -> 49 -> 70 -> 152 -> 35 -> 76 -> 145 -> 38 -> 200 -> 19
146	3 -> 132 -> 75 -> 48 -> 72 -> 180 -> 3, 6 -> 9 -> 150 -> 96 -> 144 -> 105 -> 6, 12 -> 18 -> 45 -> 192 -> 33 -> 210 -> 12, 24 -> 36 -> 90 -> 129 -> 66 -> 165 -> 24
147	17 -> 238 -> 68 -> 187 -> 17, 23 -> 226 -> 92 -> 139 -> 113 -> 46 -> 197 -> 184 -> 23, 29 -> 232 -> 71 -> 58 -> 209 -> 142 -> 116 -> 163 -> 29, 34 -> 221 -> 136 -> 119 -> 34
149	3 -> 124 -> 185 -> 18 -> 246 -> 96 -> 143 -> 55 -> 66 -> 222 -> 12 -> 241 -> 230 -> 72 -> 219 -> 129 -> 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, 17 -> 119 -> 34 -> 238 -> 68 -> 221 -> 136 -> 187 -> 17

กฎ	สถานะ
150	5 -> 141 -> 80 -> 216 -> 5, 10 -> 27 -> 160 -> 177 -> 10, 15 -> 150 -> 240 -> 105 -> 15, 20 -> 54 -> 65 -> 99 -> 20, 30 -> 45 -> 225 -> 210 -> 30, 39 -> 250 -> 114 -> 175 -> 39, 40 -> 108 -> 130 -> 198 -> 40, 57 -> 215 -> 147 -> 125 -> 57, 60 -> 90 -> 195 -> 165 -> 60, 75 -> 120 -> 180 -> 135 -> 75, 78 -> 245 -> 228 -> 95 -> 78, 156 -> 235 -> 201 -> 190 -> 156,
151	39 -> 250 -> 114 -> 175 -> 39, 57 -> 215 -> 147 -> 125 -> 57, 78 -> 245 -> 228 -> 95 -> 78, 156 -> 235 -> 201 -> 190 -> 156
152	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9
154	55 -> 211 -> 205 -> 244 -> 115 -> 61 -> 220 -> 79 -> 55, 110 -> 167 -> 155 -> 233 -> 230 -> 122 -> 185 -> 158 -> 110
155	55 -> 211 -> 205 -> 244 -> 115 -> 61 -> 220 -> 79 -> 55, 110 -> 167 -> 155 -> 233 -> 230 -> 122 -> 185 -> 158 -> 110
161	1 -> 124 -> 57 -> 16 -> 199 -> 147 -> 1, 2 -> 248 -> 114 -> 32 -> 143 -> 39 -> 2, 4 -> 241 -> 228 -> 64 -> 31 -> 78 -> 4, 8 -> 227 -> 201 -> 128 -> 62 -> 156 -> 8
162	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
163	19 -> 200 -> 38 -> 145 -> 76 -> 35 -> 152 -> 70 -> 49 -> 140 -> 98 -> 25 -> 196 -> 50 -> 137 -> 100 -> 19
166	11 -> 140 -> 194 -> 35 -> 176 -> 200 -> 44 -> 50 -> 11, 22 -> 25 -> 133 -> 70 -> 97 -> 145 -> 88 -> 100 -> 22

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

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

กฎ	สถานะ
184	5 -> 10 -> 20 -> 40 -> 80 -> 160 -> 65 -> 130 -> 5, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9, 95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190 -> 95, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
185	95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190 -> 95, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
186	95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190 -> 95, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
187	95 -> 175 -> 215 -> 235 -> 245 -> 250 -> 125 -> 190 -> 95, 111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
188	111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
189	111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
190	111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
191	111 -> 183 -> 219 -> 237 -> 246 -> 123 -> 189 -> 222 -> 111
194	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
202	9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9
208	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129 -> 3, 9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9, 15 -> 30 -> 60 -> 120 -> 240 -> 225 -> 195 -> 135 -> 15, 39 -> 78 -> 156 -> 57 -> 114 -> 228 -> 201 -> 147 -> 39, 51 -> 102 -> 204 -> 153 -> 51, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63
209	39 -> 78 -> 156 -> 57 -> 114 -> 228 -> 201 -> 147 -> 39, 51 -> 102 -> 204 -> 153 -> 51, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63
210	47 -> 206 -> 188 -> 59 -> 242 -> 236 -> 203 -> 179 -> 47, 94 -> 157 -> 121 -> 118 -> 229 -> 217 -> 151 -> 103 -> 94
211	47 -> 206 -> 188 -> 59 -> 242 -> 236 -> 203 -> 179 -> 47, 94 -> 157 -> 121 -> 118 -> 229 -> 217 -> 151 -> 103 -> 94

กฎ	สถานะ
212	3 -> 6 -> 12 -> 24 -> 48 -> 96 -> 192 -> 129 -> 3, 15 -> 30 -> 60 -> 120 -> 240 -> 225 -> 195 -> 135 -> 15, 43 -> 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165 -> 45, 51 -> 102 -> 204 -> 153 -> 51, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149 -> 53, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63
213	43 -> 106 -> 202 -> 154 -> 178 -> 166 -> 172 -> 169 -> 43, 45 -> 105 -> 75 -> 90 -> 210 -> 150 -> 180 -> 165 -> 45, 51 -> 102 -> 204 -> 153 -> 51, 53 -> 101 -> 77 -> 89 -> 83 -> 86 -> 212 -> 149 -> 53, 63 -> 126 -> 252 -> 249 -> 243 -> 231 -> 207 -> 159 -> 63
216	9 -> 18 -> 36 -> 72 -> 144 -> 33 -> 66 -> 132 -> 9
224	95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175 -> 95, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111
225	95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175 -> 95, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111
226	5 -> 130 -> 65 -> 160 -> 80 -> 40 -> 20 -> 10 -> 5, 9 -> 132 -> 66 -> 33 -> 144 -> 72 -> 36 -> 18 -> 9, 95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175 -> 95, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111
227	95 -> 190 -> 125 -> 250 -> 245 -> 235 -> 215 -> 175 -> 95, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111
228	111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111
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 -> 19, 31 -> 94 -> 124 -> 121 -> 241 -> 229 -> 199 -> 151 -> 31, 47 -> 62 -> 188 -> 248 -> 242 -> 227 -> 203 -> 143 -> 47, 111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111
230	111 -> 222 -> 189 -> 123 -> 246 -> 237 -> 219 -> 183 -> 111

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

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

ภาคผนวก ค
งานวิจัยที่ตีพิมพ์

2011 Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE)

May 11-13, 2011

Faculty of ICT, Mahidol University
Nakhon Pathom, THAILAND

Editors :
Jarernsri L. Mitrpanont
Sudsanguan Ngamsuriyaroj

National Sessions

2011 Eighth International Joint Conference
on Computer Science and Software Engineering (JCSSE)

การปรับปรุงวิธีการเข้ารหัสรูปภาพด้วยเซลลูลาร์ออโตมาตาแบบพื้นฐาน

Extended Image Encryption Method Based on Elementary Cellular Automata

วนิดา แก้วบูรณะประเสริฐ และ ผศ.ดร.นันทิกา เบญจเทพานันท์
สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ถ.ฉลองกรุง แขวงลำปาทิว เขตลาดกระบัง กรุงเทพฯ 10520
Email : cat__own@hotmail.com, kbnunthi@kmitl.ac.th

***บทคัดย่อ*—วิธีการเข้ารหัสรูปภาพโดยใช้เซลลูลาร์ออโตมาตา (cellular automata) ได้ถูกนำเสนอมาแล้วหลายวิธี วิธีหนึ่งคือการใช้แผนภาพการเปลี่ยนสถานะ (state - transition diagram) ของเซลลูลาร์ออโตมาตาแบบพื้นฐาน (elementary cellular automata) สร้างคีย์สตรีม (key stream) สำหรับการเข้ารหัส ซึ่งวิธีนี้มีข้อเสียคือ สามารถใช้ได้กับภาพสีเทา (grayscale image) บางประเภทเท่านั้น ดังนั้นในงานวิจัยนี้จึงใช้ตัวสร้างเลขสุ่มเทียม (pseudo random number genarator) เพื่อเลือกสถานะ (state) เริ่มต้นของแต่ละพิกเซล (pixel) ซึ่งทำให้ขนาดของ key space มีขนาดใหญ่ขึ้น รวมทั้งใช้การสลับที่ของบิต (bit) ในค่าพิกเซลเพื่อเพิ่มความสามารถในการปกปิดข้อมูลอีกด้วย จากผลการทดลองแสดงให้เห็นว่า วิธีที่นำเสนอนี้สามารถปกปิดข้อมูลได้ดีกว่าเดิม โดยที่ยังคงมีคุณสมบัติของ confusion และ diffusion และสามารถใช้ได้กับภาพทุกประเภท**

คำสำคัญ : เซลลูลาร์ออโตมาตาแบบพื้นฐาน, การเข้ารหัสรูปภาพ

***Abstract*—Recently, several image encryption methods based on cellular automata have been proposed. One technique is to use the state - transition diagram in elementary cellular automata to generate key stream. Nevertheless, the existing scheme cannot be applied with all types of images. Therefore, we proposed to extend the use of pseudo random number generator in the initial state of each pixel so that the key space is increased. Then we shift bits of each pixel in order to increase concealment. Our experimental results shown that our method provides better concealment in both confusion and diffusion aspects with all types of images.**

Keywords-component; elementary cellular automata; image encryption

I. บทนำ

วิธีการแลกเปลี่ยนข้อมูลที่สำคัญในปัจจุบันที่เป็นที่นิยมวิธีหนึ่งคือการส่งข้อมูลผ่านทางอินเตอร์เน็ท ซึ่งเป็นช่องทางการติดต่อสื่อสารแบบสาธารณะที่ผู้ใช้ทุกคนสามารถเข้าถึงข้อมูลทั้งหมดได้ ทำให้เกิดปัญหาในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับให้กับผู้รับข้อมูล วิธีการหนึ่งที่นำมาใช้ในการแก้ปัญหานี้คือการเข้ารหัสข้อมูล ซึ่งทำให้ผู้อื่นไม่สามารถเข้าถึงข้อมูลส่วนนี้ได้ ยกเว้นผู้ที่ได้รับอนุญาตเท่านั้น ซึ่งวิธีการที่ใช้ในการเข้ารหัสจะแตกต่างกันไปตามประเภทของข้อมูล สำหรับการเข้ารหัสข้อมูลประเภทรูปภาพ ปัญหาสำคัญคือความรวดเร็วในการเข้ารหัส เนื่องจากข้อมูลประเภทรูปภาพส่วนใหญ่แล้วจะมีขนาดใหญ่มาก รวมทั้งวิธีการที่ใช้จะต้องแตกต่างจากการเข้ารหัสข้อมูลทั่วไป จึงได้มีการนำเซลลูลาร์ออโตมาตามาใช้ในการเข้ารหัสรูปภาพ เนื่องมาจากคุณสมบัติที่สามารถนำไปปรับใช้กับฮาร์ดแวร์ได้โดยตรง รวมทั้งยังสามารถทำการประมวลผลแบบขนาน (parallel processing) ได้ด้วย จึงทำให้สามารถเข้ารหัสได้อย่างรวดเร็ว

งานวิจัยที่นำเซลลูลาร์ออโตมาตามาใช้ในการเข้ารหัสรูปภาพสามารถแบ่งได้เป็น 2 ประเภท ประเภทแรกคือ การนำเซลลูลาร์ออโตมาตามาเป็นขั้นตอนวิธีในการเข้ารหัสรูปภาพโดยตรง ได้แก่ งานวิจัยของ P.Guan [1] ขั้นตอนการเข้ารหัสและถอดรหัสเป็นแบบฟังก์ชันเชิงเส้นบางส่วน (partially linear function) โดยใช้ฟังก์ชันไม่เชิงเส้น (non – linear function) ในการเข้ารหัส และสามารถถอดรหัสได้ด้วยฟังก์ชันเชิงเส้น (linear function) ถ้าทราบฟังก์ชันตั้งต้นซึ่งเปรียบเหมือนเป็น trapdoor งานวิจัยของ F.Maleki และคณะ [2] และงานวิจัยของ M.Habibipour และคณะ [3], [4] ใช้เซลลูลาร์ออโตมาตาแบบ non – uniform โดยใช้กฎ (rule) ที่เป็นฟังก์ชันของย่านใกล้เคียง (neighborhood) ของหลายๆ ช่วงเวลาเป็น

ขั้นตอนของการเข้ารหัสและถอดรหัส

ประเภทที่สองคือการนำเซลลูลาร์ออโตมาตามาใช้สร้างตัวสร้างเลขสุ่มเทียม เพื่อใช้เป็นคีย์สตรีมร่วมกับฟังก์ชันในการเข้ารหัสรูปภาพ ได้แก่ งานวิจัยของ Z.Xuelong และคณะ [5] ใช้เจเนติกอัลกอริทึมในการเลือกกฎของเซลลูลาร์ออโตมาตาให้กับแต่ละเซลล์ (cell) เพื่อสร้างเป็นตัวสร้างเลขสุ่มเทียมขึ้นมา ในขณะที่งานวิจัยของ R.-J.Chen และคณะ [6], [7] และ [8] ใช้เซลลูลาร์ออโตมาตาแบบ 2 มิติในการสร้างตัวสร้างเลขสุ่มเทียม

เนื่องจากการเข้ารหัสโดยใช้เจเนติกอัลกอริทึม และเซลลูลาร์ออโตมาตาแบบ 2 มิติ มีขั้นตอนซับซ้อน ใช้เวลานานกว่าของ J.Jun [9] ซึ่งพบว่าบางแผนภาพการเปลี่ยนสถานะ ของเซลลูลาร์ออโตมาตาแบบพื้นฐานมีคุณสมบัติพิเศษคือ แผนภาพการเปลี่ยนสถานะจะวนกลับมาที่สถานะ (state) เริ่มต้น และนำคุณสมบัตินี้มาสร้างคีย์สตรีมในการเข้ารหัสภาพสีเทา

ในการศึกษางานวิจัยของ J.Jun [9] พบว่า ไม่สามารถใช้กับการเข้ารหัสภาพสี และคีย์บางคีย์ที่ตรงตามคุณสมบัติพิเศษ ไม่สามารถเข้ารหัสกับภาพสีเทาได้ ดังนั้นงานวิจัยนี้ได้เพิ่มการใช้ตัวสร้างเลขสุ่มเทียมในการเลือกสถานะเริ่มต้น รวมทั้งใช้การสลับที่ของบิตในค่าพิกเซล ทำให้สามารถปกปิดข้อมูลได้ทั้งภาพสีและสีเทา

โครงสร้างของบทความประกอบด้วย หัวข้อที่ 2 อธิบายถึงทฤษฎีที่เกี่ยวข้องซึ่งก็คือลักษณะและคุณสมบัติของเซลลูลาร์ออโตมาตาแบบพื้นฐาน ที่สามารถนำไปใช้ในการสร้าง คีย์สตรีม ได้ หัวข้อที่ 3 อธิบายถึงวิธีการเข้ารหัส ซึ่งจะแบ่งออกเป็นวิธีการเดิมที่ได้นำเสนอโดย J.Jun กับวิธีการใหม่ที่เราได้ทำการปรับปรุงจากวิธีการเดิม หัวข้อที่ 4 เป็นผลการทดลอง และหัวข้อที่ 5 เป็นการสรุปผล

II. ทฤษฎีที่เกี่ยวข้อง

A. เซลลูลาร์ออโตมาตาแบบพื้นฐาน

เซลลูลาร์ออโตมาตาเป็น discrete dynamical system ประกอบด้วยเซลล์ $C = \{c_1, c_2, \ldots, c_n\}$ โดยในแต่ละตำแหน่งของเซลล์จะมีค่าที่เป็นไปได้ทั้งหมดในจำนวนจำกัด ที่เรียกว่าสถานะ $S = \{s_1, s_2, \ldots, s_k\}$ โดยค่าของสถานะเป็นฟังก์ชันของตำแหน่งของเซลล์ที่ i และเวลาที่ t แทนด้วย $s(i,t)$ หรือ s_i^t เมื่อเวลาเปลี่ยนจาก t ไปเป็น $t+1$ ค่าของสถานะจะเปลี่ยนแปลงไป โดยขึ้นอยู่กับค่าของสถานะของเซลล์ที่อยู่ใกล้เคียงกัน เรียกว่าย่านใกล้เคียง หรือกล่าวได้ว่า ค่าของสถานะของเซลล์ที่ i ในเวลาที่ $t+1$ เป็นฟังก์ชันของย่านใกล้เคียง $s_i^t = f(neighborhood)$ โดยฟังก์ชันนี้เรียกว่ากฎ

สำหรับเซลลูลาร์ออโตมาตาแบบพื้นฐานเป็นเซลลูลาร์ออโตมาตาแบบ 1 มิติ ที่มีสถานะเป็น 0,1 เท่านั้น และย่านใกล้เคียงคือ s_{i-1}^t, s_i^t และ s_{i+1}^t ดังนั้นฟังก์ชันที่กำหนดค่าของสถานะในช่วงเวลาที่ $t+1$ คือ $s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t)$

สำหรับกฎของเซลลูลาร์ออโตมาตาแบบพื้นฐานมีทั้งหมด 256 กฎ และได้มีการกำหนดเลขที่ใช้เรียกแทนกฎต่างๆ ซึ่งเลขเหล่านี้เมื่อนำมาแปลงเป็นเลขฐานสองแล้ว สามารถนำมาอธิบายฟังก์ชันในการกำหนดสถานะในช่วงเวลาที่ $t+1$ ได้ จากตารางที่ I แสดงให้เห็นว่า เมื่อเราแทนเลขประจำตำแหน่งให้เป็นเลขฐานสองจำนวน 3 บิต จะได้เป็นค่าของย่านใกล้เคียง และค่าของสถานะในช่วงเวลาที่ $t+1$ มีค่าเท่ากับค่าของเลขฐานสองของกฎในตำแหน่งที่ตรงกับ ย่านใกล้เคียง

ตารางที่ I
กฎของเซลลูลาร์ออโตมาตาแบบพื้นฐาน

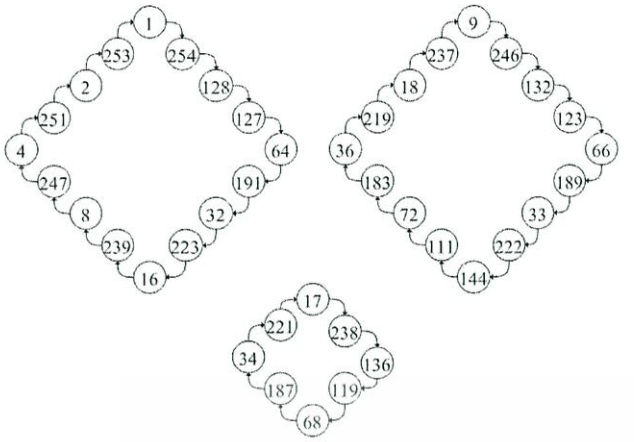
ตำแหน่งที่	7	6	5	4	3	2	1	0
ย่านใกล้เคียง	111	110	101	100	011	010	001	000
กฎ 30 (00011110)	0	0	0	1	1	1	1	0
กฎ 60 (00111100)	0	0	1	1	1	1	0	0
กฎ 90 (01011010)	0	1	0	1	1	0	1	0

B. แผนภาพการเปลี่ยนสถานะและแอทแทรคเตอร์ (attractor)

จากเซลลูลาร์ออโตมาตาแบบพื้นฐานที่ได้อธิบายไว้ข้างต้น ถ้ากำหนดให้มีจำนวนเซลล์เป็นแบบจำกัดจำนวน 8 เซลล์ กำหนดให้เงื่อนไขขอบเขตเป็นเงื่อนไขขอบเขตแบบคาบ (periodic boundary) หมายถึง ย่านใกล้เคียงของเซลล์ที่อยู่ตำแหน่งที่ 1 และ 8 เกิดปัญหาที่ตำแหน่ง s_{i-1}^t และ s_{i+1}^t ขาดไป ให้นำค่ามาจากเซลล์ที่อยู่ริมขอบอีกด้านหนึ่งมาใช้แทน จากการสังเกตพบว่าในบางกลุ่มของสถานะเริ่มต้น เมื่อทำการเปลี่ยนสถานะไปในช่วงระยะเวลาหนึ่ง ค่าของสถานะในทุกๆ เซลล์จะมีค่าเท่ากับสถานะในช่วงเริ่มต้น เมื่อนำมาเขียนเป็นแผนภาพการเปลี่ยนสถานะจะได้เป็นกราฟแบบ cycle ซึ่งเราเรียกว่า แอทแทรคเตอร์

สำหรับเซลลูลาร์ออโตมาตาแบบพื้นฐานที่มีความยาวจำนวน 8 เซลล์ จำนวนสถานะเริ่มต้นทั้งหมดที่เป็นไปได้คือ 256 สถานะ เมื่อทดลองสร้างแผนภาพการเปลี่ยนสถานะของทุกๆ สถานะจะได้แอทแทรคเตอร์จำนวนหนึ่ง ซึ่งในแอทแทรคเตอร์เหล่านี้จะมีแอทแทรคเตอร์บางส่วนที่มีคุณสมบัติดังต่อไปนี้

$$state(1) \oplus state(2) \oplus \cdots \oplus state(k) = 0 \qquad (1)$$



รูปที่ 1. แผนภาพการเปลี่ยนสถานะของกฎ 83

เมื่อ $state(i)$ คือ ค่าของสถานะในทุกเซลล์ในช่วงเวลาที่ i ของแอทแทรคเตอร์ ซึ่งหลังจากนี้จะเรียกว่าสถานะที่ i ของแอทแทรคเตอร์ และ $\oplus$ คือ exclusive or จากคุณสมบัติในสมการที่ 1 จะได้ว่า

$$d \oplus state(1) \oplus state(2) \oplus \cdots \oplus state(k) = d \oplus 0 = d \quad (2)$$

จากสมการที่ 2 ถ้าเรานำค่าใดๆ ไปทำการ exclusive or กับทุกสถานะในแอทแทรคเตอร์จะได้ค่าเท่าเดิม จากคุณสมบัตินี้เราสามารถนำมาประยุกต์ใช้ในการเข้ารหัสรูปภาพได้

III. วิธีการเข้ารหัสรูปภาพ

ขั้นตอนวิธีการเข้ารหัสที่จะนำเสนอต่อไปนี้ เป็นวิธีการที่นำไปใช้กับรูปภาพ ที่ค่าของพิกเซลสามารถเขียนอยู่ในรูปของเลขฐานสองขนาด 8 บิตได้ ขนาดของรูปภาพเท่ากับ $m \times n$ พิกเซล ซึ่งจะแบ่งออกเป็นวิธีการเดิมที่ได้นำเสนอไว้ใน [9] และวิธีการใหม่ที่ได้ทำการปรับปรุงจากเดิม

A. วิธีการเข้ารหัสแบบเดิม

สำหรับขั้นตอนวิธีการเข้ารหัสแบบเดิมนั้น คีย์ที่ใช้คือ (rule, stateone, seed) โดยที่ stateone คือสถานะที่ 1 หรือสถานะเริ่มต้นของแอทแทรคเตอร์ ที่ใช้ rule คือกฎที่ใช้ในการสร้าง แอทแทรคเตอร์ และ seed คือ ค่าที่ใช้กับตัวสร้างเลขสุ่มเทียมเพื่อสร้างตัวเลขแบบสุ่มขึ้นมาจำนวนหนึ่ง

ขั้นตอนในการเข้ารหัสเริ่มต้นที่ ทำการหาแอทแทรคเตอร์ตาม stateone และ rule ตามที่คีย์กำหนดมาให้ และทำการสุ่มตัวเลขตาม seed ที่ได้จากคีย์ เก็บไว้ในอาเรย์ T ขนาดเท่ากับจำนวนพิกเซลคือ $m \times n$ เมื่อคำนวณค่าต่างๆ เรียบร้อยแล้ว ทำการเข้ารหัสรูปภาพโดย

$$en\_pix(r,c) = pix(r,c) \oplus state(1) \oplus \cdots \oplus state(l) \quad (3)$$
$$l = (t(r,c) \mod k) + 1$$

เมื่อ $en\_pix(r,c)$ คือ ค่าของพิกเซลที่เข้ารหัสแล้วในตำแหน่งแถวที่ r หลักที่ c, $pix(r,c)$ คือ ค่าของพิกเซลต้นฉบับที่ต้องการเข้ารหัสในตำแหน่งแถวที่ r หลักที่ c, $t(r,c)$ คือ ค่าภายในอาเรย์ T ที่ตำแหน่งแถวที่ r หลักที่ c และ k คือ จำนวนสถานะทั้งหมดของแอทแทรคเตอร์

สำหรับขั้นตอนในการถอดรหัสมีขั้นตอนเหมือนกับการเข้ารหัส แต่มีความแตกต่างกันที่สมการ สำหรับสมการที่ใช้ในการถอดรหัส คือ

$$de\_pix(r,c) = en\_pix(r,c) \oplus state(l+1) \oplus \cdots \oplus state(k) \quad (4)$$

เมื่อ $de\_pix(r,c)$ คือ ค่าของพิกเซลที่ถอดรหัสได้ในตำแหน่งแถวที่ r แถวที่ c จากสมการที่ 4 จะพบว่าเป็นขั้นตอนในการทำ exclusive or เพื่อให้เป็นไปตามสมการที่ 2 ดังนั้นค่าที่ได้จะเป็นค่าของพิกเซลต้นฉบับที่ได้ทำการเข้ารหัสเอาไว้

B. วิธีการเข้ารหัสแบบใหม่

วิธีการเดิมนั้นมีข้อเสียเนื่องมาจากมีโอกาสที่ค่าพิกเซลเดียวกันเมื่อผ่านขั้นตอนการเข้ารหัสแล้วยังได้เป็นค่าเดียวกันอยู่ วิธีการใหม่ที่จะนำเสนอต่อไปนี้จึงพยายามลดโอกาสในการเกิดเหตุการณ์แบบนี้ให้น้อยลงกว่าเดิม ด้วยการเพิ่มจำนวนแอทแทรคเตอร์ที่ใช้ในการเข้ารหัส และเพิ่มขั้นตอนการสุ่มสถานะเริ่มต้นในการเข้ารหัสของแต่ละพิกเซล รวมทั้งใช้การสลับที่บิตของพิกเซล เพื่อช่วยเพิ่มความสามารถในการปกปิดข้อมูลรูปภาพอีกด้วย เนื่องจากข้อมูลประเภทรูปภาพความสำคัญของบิตในแต่ละตำแหน่งไม่เท่ากัน ถึงแม้จะเข้ารหัสได้ค่าแตกต่างกันแต่ถ้าแตกต่างกันเพียงตำแหน่งเดียว และเป็นตำแหน่งที่มีความสำคัญน้อยที่สุด ที่เรียกว่า Least - Significant Bit เมื่อมองด้วยสายตาแล้วทำให้ไม่สามารถแยกความแตกต่างกันได้ ดังนั้นการสลับตำแหน่งของบิตจะช่วยทำให้ปัญหานี้ลดน้อยลง

จากแนวคิดที่ได้กล่าวไว้ข้างต้น จึงต้องมีการปรับเปลี่ยนคีย์ใหม่เป็น (rule,seedstate,seedtime) โดยที่ seedstate และ seedtime คือค่าที่กำหนดให้กับตัวสร้างเลขสุ่มเทียม เพื่อสร้างตัวเลขสุ่มสำหรับกำหนดสถานะเริ่มต้นและจำนวนสถานะที่ใช้ในการเข้ารหัสของแต่ละพิกเซลตามลำดับ

ขั้นตอนในการเข้ารหัสเริ่มต้นจาก คำนวณหาแอทแทรคเตอร์ทั้งหมดของ rule ที่ได้รับค่ามาจากคีย์ที่มีคุณสมบัติตามสมการ 1 แล้วเก็บค่า state ทั้งหมดของแอทแทรคเตอร์เหล่านั้นไว้ในอาเรย์ P และทำการสุ่มตัวเลขโดยใช้ seedstate และ seedtime ในการสุ่มตัวเลขอย่างละชุดเก็บ

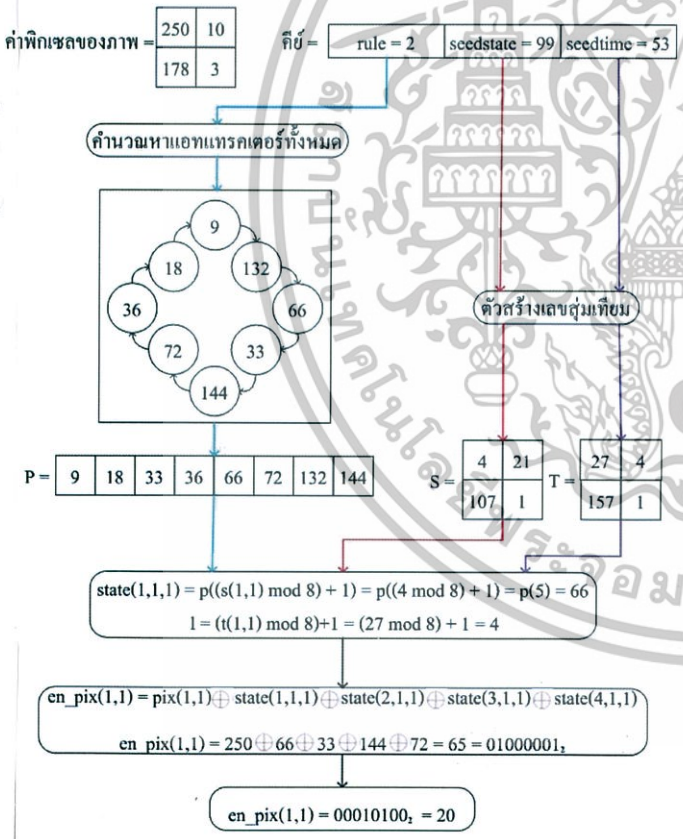
ไว้ในอาเรย์ S และ T ขนาด $m \times n$ เพื่อใช้ในการเลือกสถานะเริ่มต้นและจำนวนสถานะที่ใช้ในการเข้ารหัสตามลำดับ เมื่อคำนวณเรียบร้อยแล้วก่อนที่จะทำการเข้ารหัสแต่ละพิกเซลตามสมการ 3 ให้ทำการหาแอทแทรคเตอร์ที่จะใช้สำหรับแต่ละพิกเซลก่อนตามสมการ

$$state(1, r, c) = p((s(r, c) \mod q) + 1) \quad (5)$$

เมื่อ $state(i, r, c)$ คือสถานะที่ i ของแอทแทรคเตอร์ที่ใช้กับพิกเซลในแถวที่ r หลักที่ c, $p(i)$ คือ ค่าของสถานะที่เก็บไว้ใน P ที่ตำแหน่งที่ i, $s(r, c)$ ค่าของตัวเลขที่สุ่มโดยใช้ seedstate ที่เก็บไว้ใน S ในแถวที่ r หลักที่ c และ q คือจำนวนสถานะทั้งหมดที่เก็บอยู่ในอาเรย์ P

เมื่อได้สถานะเริ่มต้นของแอทแทรคเตอร์ของแต่ละพิกเซลในภาพแล้ว จึงทำการหาแอทแทรคเตอร์ตามสถานะเริ่มต้นและ rule ที่ได้จาก seed จากนั้นจึงทำการเข้ารหัสตามสมการที่ 3 และนำค่าที่ได้มาทำการสลับตำแหน่งบิต โดยนำค่าบิตในตำแหน่งที่ 1 ถึง 4 ไปไว้ในตำแหน่งที่ 5 ถึง 8 และนำค่าบิตในตำแหน่งที่ 5 ถึง 8 มาไว้ในตำแหน่งที่ 1 ถึง 4 สามารถดูตัวอย่างขั้นตอนการเข้ารหัสแบบใหม่ได้จากรูปที่ 2

สำหรับขั้นตอนในการถอดรหัส เริ่มต้นด้วยการคำนวณค่าต่างๆ ที่



รูปที่ 2. ตัวอย่างการเข้ารหัสด้วยวิธีการแบบใหม่ในตำแหน่งพิกเซลแถวที่ 1 หลักที่ 1

จำเป็นต้องใช้ ซึ่งใช้วิธีการคำนวณแบบเดียวกันกับการเข้ารหัส นำรูปภาพที่ผ่านการเข้ารหัสที่ได้รับมาทำการสลับตำแหน่งบิตของค่าพิกเซลแบบเดียวกับการเข้ารหัส จากนั้นจึงนำมาทำการถอดรหัสตามสมการที่ 4 เมื่อทำการถอดรหัสเรียบร้อยแล้ว ภาพที่ได้จะมีค่าพิกเซลที่เท่ากันกับภาพต้นฉบับทุกประการ

IV. ผลการทดลอง

สำหรับการทดสอบวิธีการที่ได้นำเสนอนี้ ได้ทำการทดลองกับรูปภาพจากฐานข้อมูล USC-SIPI โดยใช้รูปภาพในหมวดของ Miscellaneous จำนวน 44 รูป ประกอบไปด้วยภาพสีและภาพสีเทา ที่มีขนาดที่แตกต่างกันอยู่ 3 ขนาด เป็นการทดสอบประสิทธิภาพและคุณสมบัติต่างๆ ซึ่งสามารถแบ่งได้ดังต่อไปนี้

A. การวิเคราะห์ขนาดของ key space

วิธีการเข้ารหัสที่มี key space ที่มีขนาดใหญ่มาก ทำให้โอกาสที่ถูกโจมตีด้วยวิธี brute force เป็นไปได้ยากกว่าวิธีการที่มี key space ขนาดเล็กกว่า สำหรับคีย์ของวิธีที่ได้นำเสนอนี้ ในส่วนของ rule สำหรับเซลลูลาร์ออโตมาตาแบบพื้นฐานมีกฎที่เป็นไปได้ทั้งหมด 256 กฎ ส่วนของ seedstate และ seedtimes ขึ้นอยู่กับตัวสร้างเลขสุ่มเทียมที่ใช้ในการเข้ารหัสสามารถใช้ได้เป็นจำนวนสูงสุดเท่าใด สมมติให้มีค่าเท่ากับ M ดังนั้น key space มีขนาดเท่ากับ $256 \times M \times M$ หรือ $256 \times M^2$ เห็นได้ชัดเจนว่าจากวิธีการเดิมที่มี key space ขนาด $256 \times 256 \times M$ วิธีการใหม่นี้มีขนาด key space ที่ใหญ่กว่า ทำให้การโจมตีเป็นไปได้ยากกว่า

B. การวิเคราะห์ความสามารถในการปกปิดข้อมูล

จากการทดสอบการเข้ารหัสด้วยวิธีการเดิมกับภาพสีส่วนใหญ่ พบว่าไม่สามารถปกปิดข้อมูลได้หมด นอกจากนี้ยังมีบางคีย์ที่ไม่สามารถปกปิดข้อมูลภาพที่เป็นภาพสีเทาได้อีกด้วย แต่เมื่อนำคีย์เหล่านั้นมาใช้กับวิธีการใหม่ที่ได้นำเสนอนี้ พบว่าสามารถปกปิดข้อมูลได้ดี ตัวอย่างเช่น คีย์ = (42,99,53) จากผลการทดสอบเข้ารหัสทั้งสองวิธีที่แสดงในรูปที่ 3 แสดงให้เห็นว่า วิธีการใหม่สามารถปกปิดข้อมูลได้ดีกว่าวิธีการเดิมมาก

C. Confusion property

คุณสมบัติ confusion หมายถึง ความสัมพันธ์ระหว่างคีย์และข้อความที่ผ่านการเข้ารหัสมาแล้ว ต้องมีความซับซ้อนให้มากที่สุดเท่าที่จะเป็นไปได้ เพื่อทำให้วิธีการโจมตีด้วยเทคนิคการใช้ข้อความที่เข้ารหัสแล้วเพียงอย่างเดียว (ciphertext only attacks) เป็นไปได้ยากขึ้น [9]

จากการเปรียบเทียบฮิสโทแกรม (histogram) ของภาพที่เข้ารหัสทั้ง

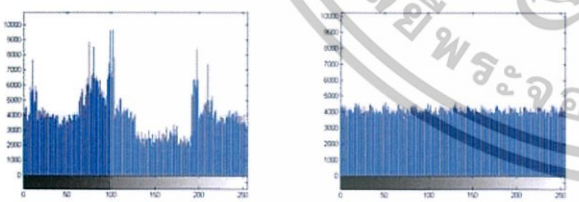
(a) ต้นฉบับสีเทา (b) วิธีเข้ารหัสแบบเดิม (c) วิธีเข้ารหัสแบบใหม่

(d) ต้นฉบับสี (e) วิธีเข้ารหัสแบบเดิม (f) วิธีเข้ารหัสแบบใหม่

รูปที่ 3. ภาพที่ได้จากการทดสอบการเข้ารหัสทั้งสองวิธี

สองวิธีด้วยคีย์เดียวกัน คือ (42,99,53) ของภาพสีเทาที่แสดงในรูปที่ 4 และของภาพสีในรูปที่ 5 ค่าของพิกเซลในภาพที่เข้ารหัสด้วยวิธีการใหม่มีการกระจายตัวที่ดีกว่าวิธีการเดิม ทำให้โอกาสในการโจมตีด้วยการหาความสัมพันธ์ระหว่างค่าพิกเซลในภาพที่เข้ารหัสแล้วเป็นไปได้ยากขึ้น ซึ่งเป็นไปตามคุณสมบัติของ confusion

(a) ภาพที่เข้ารหัสด้วยวิธีการเดิม (b) ภาพที่เข้ารหัสด้วยวิธีการใหม่

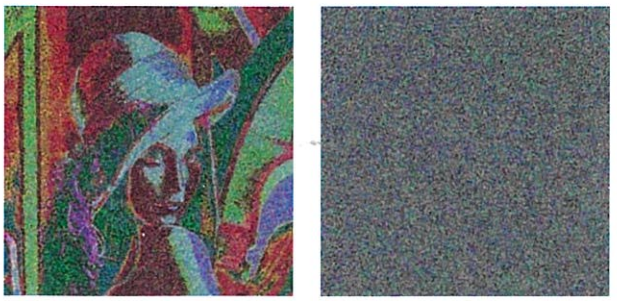


(c) ฮิสโทแกรมของภาพวิธีการเดิม (d) ฮิสโทแกรมของภาพวิธีการใหม่

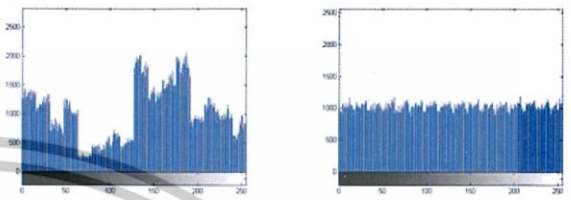
รูปที่ 4. เปรียบเทียบฮิสโทแกรมของภาพสีเทาที่ผ่านการเข้ารหัสทั้งสองวิธี

D. Diffusion property

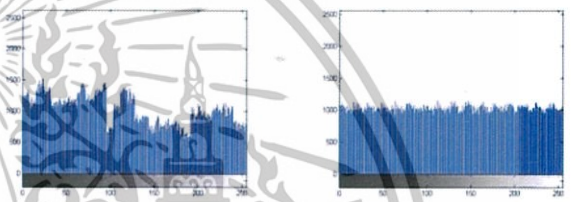
คุณสมบัติ diffusion หมายความว่า เมื่อมีการเปลี่ยนแปลงของภาพต้นฉบับหรือคีย์เพียงแค่เล็กน้อย จะส่งผลกระทบให้ภาพที่เข้ารหัสมีการ



(a) ภาพที่เข้ารหัสด้วยวิธีการเดิม (b) ภาพที่เข้ารหัสด้วยวิธีการใหม่



(c) ฮิสโทแกรมสีแดงของวิธีการเดิม (d) ฮิสโทแกรมสีแดงของวิธีการใหม่



(e) ฮิสโทแกรมสีเขียวของวิธีการเดิม (f) ฮิสโทแกรมสีเขียวของวิธีการใหม่

(g) ฮิสโทแกรมสีน้ำเงินของวิธีการเดิม (h) ฮิสโทแกรมสีน้ำเงินของวิธีการใหม่

รูปที่ 5. เปรียบเทียบฮิสโทแกรมของภาพสีที่ผ่านการเข้ารหัสทั้งสองวิธี

เปลี่ยนแปลงไปเป็นอย่างมาก [9]

สำหรับการทดสอบในส่วนนี้จะทำการเปรียบเทียบความแตกต่างของภาพสีที่ผ่านการเข้ารหัสด้วยคีย์ที่แตกต่างกันด้วยวิธีการใหม่ ลักษณะของคีย์ที่แตกต่างกันแบ่งออกได้เป็น 3 รูปแบบ ได้แก่ แบบแรกคีย์ทั้งสองมีความแตกต่างกันเฉพาะค่าในตำแหน่ง rule แบบที่สองแตกต่างกันเฉพาะค่าในตำแหน่ง seedstate และแบบที่สามแตกต่างกันเฉพาะค่าในตำแหน่ง seedtime และคีย์ทั้งสองมีความแตกต่างกันเพียง 1 บิตเท่านั้น การเปรียบเทียบความแตกต่างของภาพใช้การคำนวณหาอัตราการเปลี่ยนแปลงของพิกเซลหรือเรียกว่า NPCR (number pixel change rate) [2]

ตามสมการดังต่อไปนี้

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

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

เมื่อ $A(i,j)$ และ $B(i,j)$ คือค่าพิกเซลในแถวที่ i หลักที่ j ของภาพ A และ B ตามลำดับ ซึ่งสามารถสรุปผลออกมาได้ตามตารางที่ II แสดงให้เห็นว่าเมื่อมีการเปลี่ยนแปลงของคีย์เพียงเล็กน้อย ก็ทำให้ภาพที่เข้ารหัสมีความแตกต่างกันมาก ซึ่งเป็นไปตามคุณสมบัติของ diffusion

ตารางที่ II
NPCR ของ คีย์ ที่แตกต่างกันทั้ง 3 รูปแบบ

แบบที่	คีย์ แรก	คีย์ สอง	NPCR
1	(2,72,15)	(3,72,15)	87.09
2	(101,28,15)	(101,29,15)	86.71
3	(42,99,54)	(42,99,55)	83.51

V. สรุป

จากวิธีการเดิมที่ใช้คุณสมบัติพิเศษของเซลลูลาร์ออโตมาตาแบบพื้นฐานที่แผนภาพการเปลี่ยนสถานะจะวนกลับมาที่สถานะเริ่มต้น ในการสร้างคีย์สตรีมสำหรับการเข้ารหัส สำหรับงานวิจัยนี้ได้เพิ่มขนาดของ key space โดยการใช้ตัวสร้างเลขสุ่มเทียม สุ่มเลือกสถานะเริ่มต้นในการเข้ารหัสของแต่ละพิกเซลในภาพ พร้อมทั้งสลับตำแหน่งของบิตในพิกเซลเพื่อเพิ่มคุณสมบัติการปกปิดข้อมูลรูปภาพ จากผลการทดลองแสดงให้เห็นว่าวิธีการนี้สามารถปกปิดข้อมูลได้ดีกว่าเดิมมาก รวมทั้งสามารถนำไปใช้กับภาพสีที่วิธีการเดิมทำไม่ได้ แต่ยังคงคุณสมบัติของ confusion และ diffusion ตามเดิม

หนังสืออ้างอิง

[1] P. Guan, "Cellular automaton public-key cryptosystem," *Complex Systems*, vol. 1, pp. 51 – 57, 1987.

[2] F. Maleki, A. Mohades, S. M. Hashemi, and M. E. Shiri, "An image encryption system by cellular automata with memory," in *Proc. Third Int. Conf. Availability, Reliability and Security ARES 08*, 2008, pp. 1266–1271.

[3] M. Habibipour, R. Maarefdoust, M. Yaghobi, and S. Rahati, "An image encryption system by 2d memorized cellular automata and chaos mapping," in *Proc. 6th Int Digital Content, Multimedia Technology and its Applications (IDC) Conf*, 2010, pp. 331–336.

[4] M. Habibipour, M. Yaghobi, S. Rahati-Q, and Z. Souzanchi-k, "An image encryption system by indefinite cellular automata and chaos," in *Proc. 2nd Int Signal Processing Systems (ICSPS) Conf*, vol. 3, 2010.

[5] Z. Xuelong, L. Qianmu, X. Manwu, and L. Fengyu, "A symmetric cryptography based on extended cellular automata," in *Proc. IEEE Int Systems, Man and Cybernetics Conf*, vol. 1, 2005, pp. 499–503.

[6] R.-J. Chen, W.-K. Lu, and J.-L. Lai, "Image encryption using progressive cellular automata substitution and scan," in *Proc. IEEE Int. Symp. Circuits and Systems ISCAS 2005*, 2005, pp. 1690–1693.

[7] R.-J. Chen, Y.-H. Chen, C.-S. Chen, and J.-L. Lai, "Image encryption/decryption system using 2-d cellular automata," in *Proc. IEEE Tenth Int. Symp. Consumer Electronics ISCE '06*, 2006, pp. 1–6.

[8] R.-J. Chen and J.-L. Lai, "Novel stream cipher using 2-d hybrid ca and variable ordered recursive ca substitutions," in *Proc. IFIP Int. Conf. Network and Parallel Computing NPC 2008*, 2008, pp. 74–81.

[9] J. Jun, "Image encryption method based on elementary cellular automata," in *Proc. IEEE Southeastcon SOUTHEASTCON '09*, 2009, pp. 345–349.

ประวัติผู้เขียน

ชื่อ – สกุล	นางสาววนิดา แก้วบูรณะประเสริฐ
วัน เดือน ปีเกิด	5 ตุลาคม 2529
ที่อยู่	69/2 ซอยทุ่งเศรษฐี
	แขวงดอกไม้ เขตประเวศ
	จังหวัดกรุงเทพฯ 10250

ประวัติการศึกษา

2551 จบการศึกษาปริญญาวิทยาศาสตรบัณฑิต
สาขาคณิตศาสตร์ประยุกต์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง