การเข้ารหัสลับข้อมูลโดยการใช้เซลลูลาร์ออโตมาตาร่วมกับระบบบอลวน

Data Encryption Scheme using Cellular Automata Sequences with Chaotic System

นางสาววันกวี มูลฐี 53113031-8

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีไทย - ญี่ปุ่น
ปีการศึกษา 2556

หัวข้อปริญญานิพนธ์	การเข้ารหัสลับข้อมูลโดยการใช้เซลลูลาร์ออโตมาตาร่วมกับระบบอลวน
โดย	นางสาววันกวี มูลฐี 53113031-8
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.วิมล แสนอุ้ม
อาจารย์ที่ปรึกษาปริญญานิพนธ์ร่วม	ผู้ช่วยศาสตราจารย์ ดร.วรากร ศรีเชวงทรัพย์ ศาสตราจารย์ ดร.ริวมาเอะ ซาบุโระ

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีไทย-ญี่ปุ่น อนุมัติให้นับปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

..... คณบดีคณะวิศวกรรมศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร. เลอเกียรติ์ วงศ์สารพิกูล)

วันที่.....เดือน.....พ.ศ.....

คณะกรรมการสอบปริญญานิพนธ์

..... ประธานกรรมการสอบ
(อาจารย์ ดร.กรกฎ เหมสถาปัตย์)

.....กรรมการสอบ
(อาจารย์ อัดนา เซ็งโต๊ะ)

.....กรรมการสอบ
(อาจารย์ สุรพล เอี่ยมประภาพร)

อาจารย์ที่ปรึกษาปริญญานิพนธ์

.....
(ผู้ช่วยศาสตราจารย์ ดร.วิมล แสนอุ้ม)

อาจารย์ที่ปรึกษาปริญญานิพนธ์ร่วม

.....
(ผู้ช่วยศาสตราจารย์ ดร.วรากร ศรีเชวงทรัพย์)

การเข้ารหัสลับข้อมูลโดยการใช้เซลลูลาร์ออโตมาตาร่วมกับระบบอลวน

วันกวี มูลฐี 53113031-8
อาจารย์ที่ปรึกษา : ผู้ช่วยศาสตราจารย์ ดร.วิมล แสนอุ้ม
อาจารย์ที่ปรึกษาร่วม : ผู้ช่วยศาสตราจารย์ ดร.วรากร ศรีเชวงทรัพย์
ศาสตราจารย์ ดร.ริวมาเอะ ซาบุโระ

งานวิจัยนี้ศึกษาการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาร่วมกับระบบอลวน เพื่อใช้ในการประยุกต์การเข้ารหัสลับข้อมูล เนื่องจากข้อมูลของภาพดิจิทัลมีขนาดใหญ่กว่าข้อมูลของข้อความ จึงทำให้การเข้ารหัสลับแบบเก่าใช้เวลามากในการเข้ารหัสลับ นอกจากนี้การเข้ารหัสลับแบบเก่านั้นมีความปลอดภัยลดน้อยลงจากเดิมมาก เพราะมีความซับซ้อนในการเข้ารหัสลับไม่มาก จึงถูกถอดรหัสลับได้ในเวลาเพียงเล็กน้อย เทคโนโลยีการเข้ารหัสลับภาพดิจิทัลจึงเป็นทางเลือกที่ทำให้ข้อมูลที่เข้ารหัสลับภาพดิจิทัลมีความซับซ้อนมากยิ่งขึ้น และเป็นการเพิ่มความปลอดภัยให้กับข้อมูลของภาพดิจิทัลอีกทางหนึ่ง เพราะฉะนั้นงานวิจัยนี้จึงเลือกศึกษาเทคโนโลยีการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวน เพื่อนำมาออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสลับภาพดิจิทัล และประยุกต์ใช้กับการเข้ารหัสลับข้อมูลไฟล์ชนิดอื่น ๆ

ผลลัพธ์ที่ได้จากการวิจัยพบว่า อัลกอริทึมที่นำเสนอมีค่าเอนโทรปีเข้าใกล้ 8 ซึ่งค่าดังกล่าวเป็นไปตามทฤษฎีและจากการเปรียบเทียบระหว่างภาพก่อนการเข้ารหัสลับภาพดิจิทัลและภาพหลังการเข้ารหัสลับภาพดิจิทัล แต่ละระนาบสีองค์ประกอบมีค่าสัมประสิทธิ์สหสัมพันธ์เข้าใกล้ศูนย์ ซึ่งแสดงถึงการไม่มีความสัมพันธ์กันระหว่างภาพก่อนการเข้ารหัสลับภาพดิจิทัลและภาพหลังการเข้ารหัสลับภาพดิจิทัล นอกจากนี้ค่าความถี่ของความเข้มแสงในแต่ละระนาบสีองค์ประกอบของภาพหลังเข้ารหัสลับภาพดิจิทัลมีค่าความถี่แต่ละช่วงความเข้มแสง (0-255) ที่ใกล้เคียงกัน ผลลัพธ์ดังกล่าวบ่งชี้ให้เห็นว่าการเข้ารหัสลับภาพดิจิทัลที่มีความปลอดภัยสูง และใช้ระยะเวลาในการเข้ารหัสลับภาพดิจิทัลน้อยลง

Data Encryption Scheme using Cellular Automata sequences with Chaotic System

Wankawee Moonthee 53113031-8

Project advisor: Asst. Prof. Wimol San-Um, Ph.D.

Project co-advisor: Asst. Prof. Warakorn Srichavengsup, Ph.D.

Prof. Ryumae Saburo, Ph.D.

Digital image encryption has played an important role in security of image storages. As digital image data is larger than the plain text, traditional encryption process for use in image encryption is therefore complicated, consuming long encryption time. In addition, those of traditional encryption processes have low level of security due to insufficient complexity in encrypted keys, resulting in weakness for all kind of data attacks. Consequently, it is needed to have a high-level security and robust digital image encryption. This project therefore studies the digital image encryption scheme using cellular automata sequences combined with chaotic systems.

This research results reveal that the proposed algorithm that utilizes a combination of cellular automata sequences and chaotic system has the entropy value of nearly 8 corresponding to the image entropy theory. From the comparison, between the encrypted images before and after, represented that each of bit planes Correlation Coefficient value have close to ZERO. The comparison between the original image and the encrypted image in terms of correlation shows that the correlation value is very close to zero, indicating that the encrypted image has high security. Besides, the histogram employed for a qualitative measure of the encrypted image of pixel values in the range (0-255) is relatively flat, showing that the color in image is fully distributed. Such results indicate that the proposed digital images encryption scheme using a combination of cellular automata sequences and chaotic system has high level of security with fast processing time duration.

กิตติกรรมประกาศ

โครงงานวิจัยนี้จะไม่สำเร็จลุล่วงหากไม่ได้รับการช่วยเหลือและสนับสนุนของสถาบันเทคโนโลยีไทย – ญี่ปุ่นที่ให้การสนับสนุนผู้วิจัยในทุกด้าน ขอบพระคุณอาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.วิมล แสนอุ้ม, ผู้ช่วยศาสตราจารย์ ดร.วรากร ศรีเชวงทรัพย์และศาสตราจารย์ ดร.ริวมาเอะ ซาบุโระ ที่แนะนำสิ่งต่าง ๆ ระหว่างการทำโครงงานวิจัยนี้ ท่านยังคอยช่วยเหลือทั้งทางด้านเอกสารและความรู้ใหม่ ๆ ที่ผู้วิจัยขาดตกบกพร่องไป นอกจากนี้ขอบคุณห้องวิจัยอิเล็กทรอนิกส์อัจฉริยะ (IES) ที่เอื้ออำนวยให้ผู้วิจัยได้มีสถานที่ทำงานวิจัยที่เหมาะสม และขอขอบคุณที่มหาวิทยาลัยโมโนซุคุริที่ให้ทุนสนับสนุนโครงการแลกเปลี่ยนนักวิจัยทำให้ผู้วิจัยได้รับความรู้ใหม่ ๆมากยิ่งขึ้น อีกทั้งขอบคุณห้องวิจัยของ ศ.ดร.ริวมาเอะ ซาบุโระ ที่เอื้อเฟื้อสถานที่ทำงานวิจัยระหว่างที่ผู้วิจัยพำนักอยู่ประเทศญี่ปุ่น ขอบคุณท่านคณะกรรมโครงงานวิจัยทุกท่านที่แนะนำสิ่งต่าง ๆ ให้ผู้วิจัยนำไปปรับปรุงเพื่อให้ได้งานวิจัยที่ดีที่สุดและเป็นประโยชน์สูงสุด

ขอบคุณท่านอาจารย์ของสถาบันเทคโนโลยีไทย-ญี่ปุ่นและมหาวิทยาลัยโมโนซุคุริที่ไม่ได้กล่าวนาม ที่สอนสิ่งต่าง ๆ จนนำมาใช้ประโยชน์ในการทำงานต่าง ๆ ให้สำเร็จลุล่วง ขอบคุณนายสุพจน์-ประนอม มูลฐีและเพื่อน รุ่นพี่ รุ่นน้อง ทุกท่านที่คอยสนับสนุนให้กำลังใจแม้ในยามที่ผู้วิจัยท้อจนการดำเนินงานสำเร็จลุล่วง

นางสาววันกวี มูลฐี

22 มีนาคม 2557

สารบัญ

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

สารบัญรูป

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมา และความสำคัญของปัญหา

เนื่องจากเทคโนโลยีการเข้ารหัสลับแบบเก่า เช่น Data Encryption Standard (DES) , RSA algorithm และ Advanced Encryption Standard (AES) เป็นต้น มีความเหมาะสมสำหรับการเข้ารหัสลับข้อความ แต่ไม่เหมาะสำหรับการเข้ารหัสลับภาพดิจิทัลโดยตรง เนื่องจากข้อมูลของภาพดิจิทัลมีขนาดใหญ่กว่าข้อมูลของข้อความ จึงทำให้การเข้ารหัสลับแบบเก่าใช้เวลามากในการเข้ารหัสลับ นอกจากนี้การเข้ารหัสลับแบบเก่านั้นมีความปลอดภัยลดน้อยลงจากเดิมมาก เพราะมีความซับซ้อนในการเข้ารหัสลับไม่มาก จึงถูกถอดรหัสลับได้ในเวลาเพียงเล็กน้อย

เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล เป็นเทคโนโลยีที่ใช้รักษาความปลอดภัยของรูปภาพและมีความซับซ้อนกว่าการเข้ารหัสข้อความ องค์ประกอบหลักของการเข้ารหัสลับภาพดิจิทัล คือ ข้อมูลที่ใช้ในการเข้ารหัสลับ ฟังก์ชันที่ใช้ในการเข้ารหัสลับภาพดิจิทัล ซึ่งเป็นตัวกำหนดความซับซ้อนของข้อมูลที่ได้จากการเข้ารหัสลับ และคีย์ที่ใช้สำหรับการเข้ารหัสลับภาพดิจิทัล เป็นตัวกำหนดข้อมูลที่เข้ารหัสลับภาพดิจิทัลให้มีความแตกต่างกัน นอกจากนี้ยังเป็นตัวถอดรหัสลับภาพดิจิทัลอีกด้วย

เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล ทำให้ข้อมูลที่เข้ารหัสลับภาพดิจิทัลมีความซับซ้อนมากยิ่งขึ้น เป็นการเพิ่มความปลอดภัยให้กับข้อมูลของภาพดิจิทัลอีกทางหนึ่ง เพราะฉะนั้นงานวิจัยนี้จึงเลือกศึกษาเทคโนโลยีการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวน เพื่อนำมาออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสลับภาพดิจิทัล และประยุกต์ใช้กับการเข้ารหัสลับข้อมูลไฟล์ชนิดอื่น ๆ

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อศึกษาวิธีการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตากับทฤษฎีอลวน

1.2.2 เพื่อปรับปรุงการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลให้มีประสิทธิภาพที่ดีขึ้น

1.2.3 เพื่อประยุกต์การเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตากับทฤษฎีอลวนเข้ากับเข้ารหัสลับและถอดรหัสลับไฟล์ประเภทอื่น

1.3 ขอบเขตของการศึกษา

1.3.1 ศึกษาทฤษฎีอลวนและเซลลูลาร์ออโตมาตา

1.3.2 ศึกษาการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัล

1.3.3 ศึกษาการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลที่มีการใช้เซลลูลาร์ออโตมาตาและทฤษฎีอลวน

1.3.4 ออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสลับภาพและถอดรหัสลับภาพดิจิทัลที่มีการใช้เซลลูลาร์ออโตมาตาและทฤษฎีอลวน

1.3.5 ปรับปรุงการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลที่มีการใช้เซลลูลาร์ออโตมาตาและทฤษฎีอลวน ให้มีประสิทธิภาพที่ดีขึ้น

1.3.6 ประยุกต์การเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตากับทฤษฎีอลวน เข้ากับการเข้ารหัสลับและถอดรหัสลับไฟล์ประเภทอื่น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ได้แบบจำลองการเข้ารหัสลับข้อมูลแบบใหม่ที่มีอัลกอริทึมที่เข้าใจง่าย อีกทั้งตัวผู้วิจัยยังได้ทักษะการคิดวิเคราะห์และออกแบบอัลกอริทึมอีกด้วย นอกจากนี้โครงงานวิจัยนี้ยังเป็นแนวทางในการพัฒนาการเข้ารหัสลับข้อมูลให้มีความซับซ้อนและความปลอดภัยมากขึ้น

1.5 แผนงานและระยะเวลาในการดำเนินงาน

ตารางที่ 1.1 แผนงานและระยะเวลาการดำเนินงาน

ลำดับ	ขั้นตอนการดำเนินงาน	พ.ศ. 2556							พ.ศ. 2557		
		มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.
1	ศึกษาทฤษฎีอลวนและเซลลูลาร์ออโตมาตา										
2	ศึกษาการเข้ารหัสลับภาพดิจิทัล										
3	ศึกษาการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลที่มีการใช้เซลลูลาร์ออโตมาตาและทฤษฎีอลวน										
4	ออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสลับภาพดิจิทัลที่มีการใช้เซลลูลาร์ออโตมาตาและทฤษฎีอลวน										
5	ปรับปรุงการเข้ารหัสลับภาพดิจิทัลที่ออกแบบให้มีประสิทธิภาพที่ดีขึ้น										
6	ประยุกต์การเข้ารหัสลับภาพดิจิทัลที่ออกแบบเข้ากับการเข้ารหัสลับและถอดรหัสลับไฟล์ประเภทอื่น										
7	เขียนรายงานความก้าวหน้า										
8	นำเสนอผลงาน										

แผนงาน

ระยะเวลาทำงาน

บทที่ 2
หลักการพื้นฐาน ทฤษฎีและบทความวิจัยที่เกี่ยวข้อง

ในการทำโครงงานนี้ ผู้จัดทำได้ศึกษาหลักการพื้นฐานและงานวิจัยที่เกี่ยวข้อง และได้นำเสนอตามหัวข้อต่อไปนี้

1. เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล
2. การวิเคราะห์การเข้ารหัสลับภาพดิจิทัล
3. ทฤษฎีอลวน
4. เซลลูลาร์ออโตมาตา
5. โปรแกรมแมทแลป (MATLAB)
6. เอกสาร และงานวิจัยที่เกี่ยวข้อง

2.1 เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล

เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล เป็นเทคโนโลยีที่ใช้รักษาความปลอดภัยของรูปภาพและมีความซับซ้อนกว่าการเข้ารหัสข้อความ องค์ประกอบหลักของการเข้ารหัสลับภาพดิจิทัล คือ ข้อมูลที่ใช้ในการเข้ารหัสลับ ฟังก์ชันที่ใช้ในการเข้ารหัสลับภาพดิจิทัล ซึ่งเป็นตัวกำหนดความซับซ้อนของข้อมูลที่ได้จากการเข้ารหัสลับ และคีย์ที่ใช้สำหรับการเข้ารหัสลับภาพดิจิทัล เป็นตัวกำหนดข้อมูลที่เข้ารหัสลับภาพดิจิทัลให้มีความแตกต่างกัน นอกจากนี้ยังเป็นตัวถอดรหัสลับภาพดิจิทัลอีกด้วย

เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล ทำให้ข้อมูลที่เข้ารหัสลับภาพดิจิทัลมีความซับซ้อนมากยิ่งขึ้น เป็นการเพิ่มความปลอดภัยให้กับข้อมูลของภาพดิจิทัลอีกทางหนึ่ง

2.2 การวิเคราะห์การเข้ารหัสลับภาพดิจิทัล

2.2.1 Key Sensibility

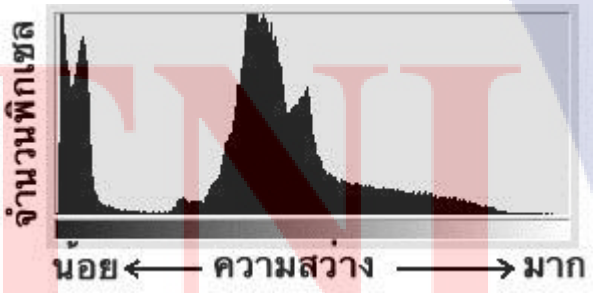
เนื่องจากมีเพียงคีย์เดียวเท่านั้นที่ใช้ในการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัล คีย์อื่นที่แตกต่างกันเพียงเล็กน้อยจะไม่สามารถใช้ในการถอดรหัสลับภาพดิจิทัลได้ จึงใช้ในการทดสอบความปลอดภัยของการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัล

2.2.2 การวิเคราะห์ทางสถิติ

ในบทความที่ตีพิมพ์ปี ค.ศ. 1949, แชนนอน (Shannon) ได้กล่าวไว้ว่า “มันมีความเป็นไปได้ที่จะอธิบายข้อมูลที่ถูกเข้ารหัสลับโดยการวิเคราะห์ทางสถิติ ” ดังนั้นเขาจึงนำเสนอวิธีการ 2 วิธีการจากพื้นฐานความซับซ้อนและการแพร่กระจายของข้อมูลเพื่อที่จะรับมือกับการโจมตีที่มีประสิทธิภาพขึ้นอยู่กับการวิเคราะห์ทางสถิติ ในบทความวิจัยปัจจุบัน การวิเคราะห์ทางสถิติได้รับการยอมรับและแสดงให้เห็นถึงความซับซ้อนและการแพร่กระจายของข้อมูลที่เป็นคุณสมบัติที่ป้องกันการโจมตีทางสถิติ โดยวิธีการทั้งสองคือ การวิเคราะห์ฮิสโตแกรมของภาพที่มีการเข้ารหัสลับภาพดิจิทัลและความสัมพันธ์ของค่าพิกเซลระหว่างภาพก่อนเข้ารหัสลับภาพดิจิทัลและหลังเข้ารหัสลับดิจิทัล

การวิเคราะห์ฮิสโตแกรม

ฮิสโตแกรมเป็นกราฟแสดงจำนวนพิกเซลที่ความสว่างต่างๆ ของภาพ จากภาพ2.1 ทางแนวนอนเป็นระดับความเข้มของแสงที่แบ่งระดับเป็น 256 ระดับ ที่เรียกว่าระดับสีเทา หรือ gray level โดยมีค่าตั้งแต่ 0-255 เมื่อระดับสีเทามีค่าต่ำ (ด้านซ้ายมือ) หมายถึงมีความเข้มของแสงน้อย มองเห็นเป็นสีดำ ค่าระดับสีเทามาก (ด้านขวามือ) หมายถึงมีความเข้มของแสงมาก มองเห็นเป็นสีขาว แกนตั้งของกราฟแสดงจำนวนพิกเซลในแต่ละความระดับสีเทาซึ่งเป็นค่าสัมพัทธ์



ภาพที่ 2.1 กราฟฮิสโตแกรม

การวิเคราะห์ฮิสโตแกรมนั้น เป็นการวิเคราะห์การเปลี่ยนแปลงของจำนวนพิกเซลในแต่ละระดับความเข้มของแสงในรูปก่อนเข้ารหัสลับภาพดิจิทัลและหลังการเข้ารหัสลับภาพดิจิทัล

การวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์

ค่าสหสัมพันธ์ (Correlation) เป็นสถิติที่ใช้หาความสัมพันธ์ระหว่างตัวแปร 2 ตัวแปร ซึ่งค่าสหสัมพันธ์ที่คำนวณได้ เรียกว่า ค่าสัมประสิทธิสหสัมพันธ์ (Correlation coefficient) ในการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปรสองตัว (Bivariate Correlation) บางครั้งเราเรียกว่าตัวแปรอิสระว่า ตัวแปรทำนาย (Predictor variable) และเรียกตัวแปรอีกตัวว่าตัวแปร เกณฑ์ (Criterion variable) (Diekhoff . 1992 : 211) ซึ่งโดยปกติจะเป็นตัวแปรตาม อย่างไรก็ตาม การที่จะทราบว่าตัวแปรทำนายตัวแปรใดเป็นตัวแปรเกณฑ์ ขึ้นอยู่กับงานวิจัยนั้นๆ ในการวิเคราะห์ค่าสหสัมพันธ์ระหว่างตัวแปร ถ้าหากทั้งสองตัวแปรมีระดับการวัดอันตรภาค (Interval scale) หรืออัตราส่วน (Ration scale) จะเรียกว่าการวิเคราะห์โดยใช้พาราเมทริก (Parametric procedure) แต่ถ้ามีระดับการวัดมาตรานามบัญญัติ (Nominal scale) หรือมาตราเรียงอันดับ (Ordinal scale) จะเรียกว่า การวิเคราะห์แบบไม่ใช้พาราเมทริก (Nonparametric procedure)

ค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน (Pearson ‘ s Correlation Coefficient)

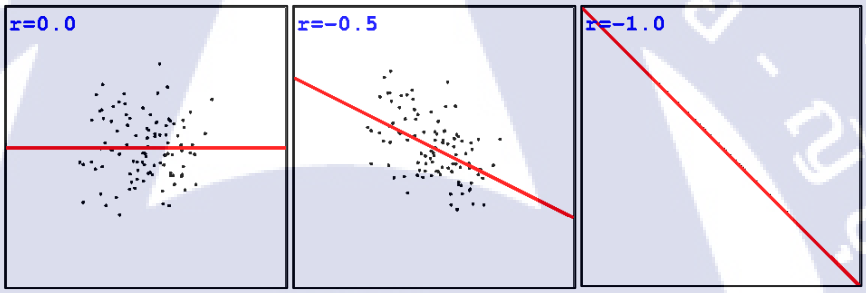
การคำนวณหาค่าสัมประสิทธิ์สหสัมพันธ์เพียรสัน หรือบางครั้งเรียกว่า สหสัมพันธ์อย่างง่าย (Simple Correlation) โดยใช้สัญลักษณ์ r ข้อมูลหรือระดับการวัดของตัวแปรแต่มาตราอันตรภาค ถึง มาตราอัตราส่วน โดยการหาความสัมพันธ์ระหว่างตัวแปรนั้นมักจะใช้สัญลักษณ์ของตัวแปรเป็นตัวแปร x และ Y โดยค่าสหสัมพันธ์เพียร์สัน (r) จะมีคุณสมบัติดังนี้

1. ถ้า r เป็นการวัดความสัมพันธ์เชิงเส้น
2. ถ้า r จะอยู่ระหว่าง -1 ถึง 1
3. ถ้า r จะมีลักษณะเหมือนความชันของเส้นการถดถอย
4. ถ้า r จะไม่เปลี่ยนแปลงเมื่อตัวแปรอิสระ (X) และตัวแปรตาม (Y) เปลี่ยนไปแบบเดียวกัน
5. ถ้า r จะไม่เปลี่ยนแปลงถ้าค่าสเกล (scale) ของตัวแปรใดตัวแปรหนึ่งเปลี่ยนไป (ค่าของตัวแปร X หรือ Y)
6. ถ้า r มีการแจกแจงแบบเดียวกันกับที (Student t distribution)

ทิศทางของความสัมพันธ์ (Direction of the Relationship)

ในการหาลักษณะความสัมพันธ์ระหว่างตัวแปรนั้นเราสามารถสร้างแผนภาพกระจัดกระจาย (Scatter plot) เพื่อดูทิศทางของความสัมพันธ์ได้โดยมีลักษณะความสัมพันธ์ 3 แบบคือ

1. สหสัมพันธ์ทางบวก (Positive Correlations) หมายถึงเมื่อตัวแปรตัวหนึ่งเพิ่มหรือลดลงอีกตัวแปรหนึ่งก็จะเพิ่มขึ้นหรือลดลงไปด้วย
2. สหสัมพันธ์ทางลบ (Negative Correlations) หมายถึงเมื่อตัวแปรตัวหนึ่งมีค่าเพิ่มขึ้นหรือลดลงอีกตัวหนึ่งจะมีค่าเพิ่มหรือลดลงตรงข้ามเสมอ
3. สหสัมพันธ์เป็นศูนย์ (Zero Correlations) หมายถึงตัวแปรสองตัวไม่มีความสัมพันธ์ซึ่งกันและกัน



ภาพที่ 2.2 ลักษณะของกราฟที่ค่า r = 1, .5 , 0, -.5 และ -1 ตามลำดับ

2.2.3 การวิเคราะห์เอนโทรปี

แนวคิดการวิเคราะห์เอนโทรปีของการเข้ารหัสลับภาพดิจิทัลถูกนำเสนอโดย เอ็ดเวิร์ด (Edward) เอนโทรปีเป็นการสุ่มรวบรวมข้อมูลสำหรับใช้ในการเข้ารหัสลับภาพดิจิทัลหรือการใช้งานอื่นๆที่ต้องการข้อมูลแบบสุ่ม โดยมักถูกเก็บรวบรวมจากแหล่งฮาร์ดแวร์ เอนโทรปีของภาพที่มีการเข้ารหัสลับภาพดิจิทัลที่มีค่าเข้าใกล้ 8 แสดงว่าขั้นตอนวิธีการเข้ารหัสลับภาพดิจตอลมีประสิทธิภาพการโจมตีเอนโทรปี

2.3 ทฤษฎีอลวน

เอ็ดเวิร์ด ลอเรนซ์ (Edward Lorenz) เป็นผู้ริเริ่มทฤษฎีความอลวน เขาได้สังเกตพฤติกรรมความอลวน ในขณะทำการทดลองทางด้านการพยากรณ์อากาศ ในปี ค.ศ. 1961 ลอเรนซ์ใช้คอมพิวเตอร์ซิมูเลชั่นแบบจำลองสภาพอากาศ ซึ่งในการคำนวณครั้งถัดมาเขาไม่ต้องการเริ่มซิมูเลชั่นจากจุดเริ่มต้นใหม่ เพื่อประหยัดเวลาในการคำนวณ เขาจึงใช้ข้อมูลในการคำนวณก่อนหน้านี้เพื่อเป็นค่าเริ่มต้น ปรากฏว่าค่าที่คำนวณได้มีความแตกต่างไปจากเดิมอย่างสิ้นเชิง เขาพบว่าสาเหตุเกิดจากการปัดเศษ ของค่าที่พิมพ์ออกมา จากค่าที่ใช้ในคอมพิวเตอร์ ซึ่งมีค่าน้อยมาก แต่สามารถนำไปสู่ความแตกต่างอย่างมากมาย เรียกว่า ไวต่อสภาวะเริ่มต้น คำว่า “butterfly effect” ซึ่งเป็นคำที่นิยมใช้เมื่อกล่าวถึงทฤษฎีความอลวน นั้นมีที่มาไม่ชัดเจน เริ่มปรากฏแพร่หลายหลังจากการบรรยายของ ลอเรนซ์ ในปี ค.ศ. 1972

ทฤษฎีความอลวน (Chaos theory) เป็นทฤษฎีที่อธิบายถึง ลักษณะพฤติกรรมของระบบพลวัตโดยลักษณะการเปลี่ยนแปลงของระบบที่เรียกว่าระบบอลวนนี้ จะมีลักษณะที่ปั่นป่วนจนดูคล้ายว่า การเปลี่ยนแปลงนั้นเป็นแบบสุ่มหรือไร้ระเบียบ (Random / Stochastic) แต่จริง ๆ แล้ว ระบบอลวนนี้ไม่เป็นระบบแบบสุ่ม หรือระบบที่มีระเบียบ (Deterministic)

2.3.1 แผนที่ความอลวน (Chaotic map)

ในทางคณิตศาสตร์ แผนที่ความอลวนเป็นฟังก์ชันวิวัฒนาการที่แสดงการจัดเรียงพฤติกรรมความอลวน แผนที่อาจจะกำหนดค่าตัวแปรโดยตัวแปรที่เวลาต่อเนื่องหรือไม่ต่อเนื่อง และแผนที่ที่ไม่ต่อเนื่องมักมีรูปแบบของฟังก์ชันซ้ำ แผนที่ความอลวนถูกพบบ่อยในการศึกษาพฤติกรรมที่เป็นพลวัต

แผนที่โลจิสติก (Logistic map)

ในงานวิจัยนี้ใช้แผนที่โลจิสติกในการศึกษาและทำความเข้าใจทฤษฎีความอลวน แผนที่โลจิสติกเป็นหนึ่งในแผนที่ความอลวนที่มีพฤติกรรมซับซ้อนและเป็นสมการไม่เป็นเชิงเส้น

แผนที่โลจิสติกเป็นที่นิยมในบทความวิจัยปี 1976 โดยนักชีววิทยาชื่อ โรเบิร์ต เมย์ (Robert May) แต่ผู้สร้างสมการแผนที่โลจิสติกแมพคือ Pierre François Verhulst

$$x_{n+1} = r x_n (1 - x_n)$$

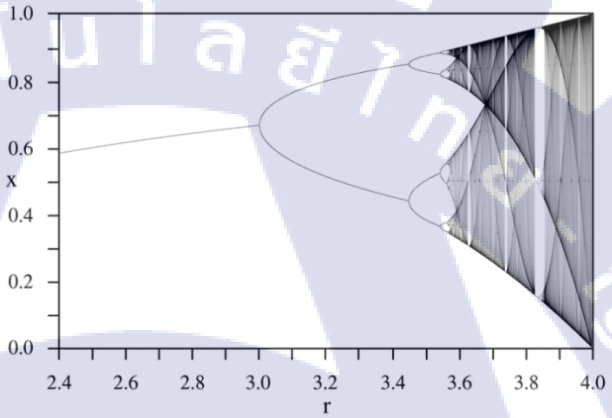
โดย x_n แทน แทนค่าข้อมูล ณ เวลาที่ n โดย x_n มีค่าอยู่ในช่วง 0 ถึง 1

r แทนค่าคงที่ในช่วง $0 \leq r \leq 4$

Bifurcation diagram

ในทางคณิตศาสตร์โดยเฉพาะอย่างยิ่งในระบบพลวัตนั้นไบเฟอเคชันไดอะแกรมจะแสดงค่าในระยะยาวที่เป็นไปได้ของระบบ ซึ่งเป็นฟังก์ชันของตัวแปรของไบเฟอเคชันในระบบ โดยฟังก์ชันดังกล่าวแทนค่าการแก้ปัญหาที่มั่งคงด้วยเส้นทึบและการแก้ปัญหาที่ไม่มั่นคงด้วยเส้นจุด

ไบเฟอเคชันของแผนที่โลจิสติกมีตัวแปร r ปรากฏบนแกนนอนของกราฟและแนวแกนตั้งแสดงความเป็นไปได้ของค่าของข้อมูลในระยะยาวของฟังก์ชันโลจิสติกดังภาพที่ 2.3 สำหรับ r ที่อยู่ในช่วง 3.87-4.0 นั้นเป็นระบบแบบพลวัตมากที่สุด



ภาพที่ 2.3 ไบเฟอเคชันไดอะแกรมของแผนที่โลจิสติก

แผนที่สัมบูรณ์ (Absolute map)

แผนที่สัมบูรณ์ถูกนำมาใช้ในงานวิจัยนี้ สมการแผนที่สัมบูรณ์ถูกสร้างขึ้นโดยอาจารย์ ผศ.ดร.วิมล แสนอุ้ม สมการนี้มีโครงสร้างทางคณิตศาสตร์อย่างง่าย เนื่องจากใช้เพียงแค่การสัมบูรณ์ การคูณและการลบ แต่กลับได้ผลลัพท์ที่ซับซ้อน

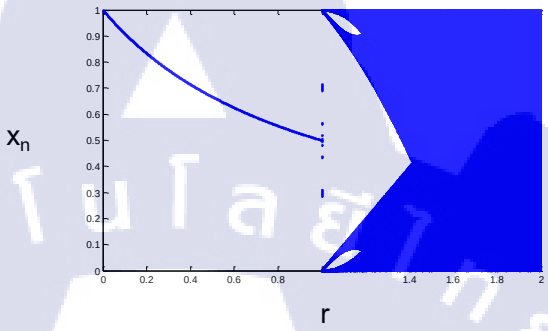
$$x_{n+1} = | rx_n - 1 |$$

โดย x_n แทน แทนค่าข้อมูล ณ เวลาที่ n โดย x_n มีค่าอยู่ในช่วง 0 ถึง 1

r แทนค่าคงที่ในช่วง $0 \le r \le 2$

Bifurcation diagram

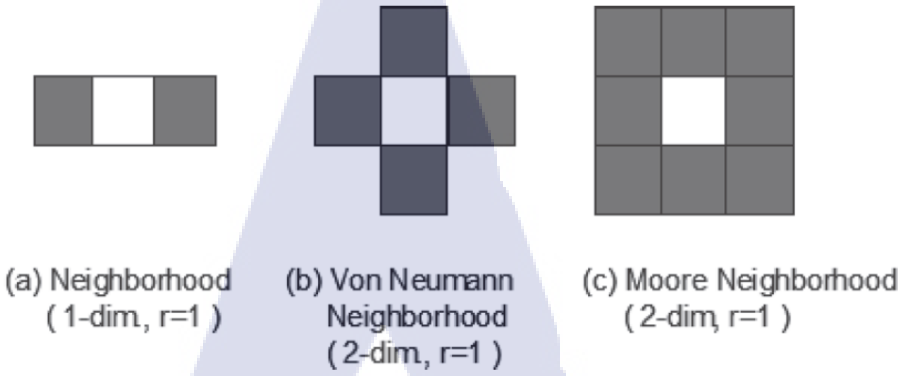
ไบเฟอเคชันของแผนที่สัมบูรณ์มีตัวแปร r ปรากฏบนแกนนอนของกราฟและแนวแกนตั้งแสดงความเป็นไปได้ของค่าของข้อมูลในระยะยาวของฟังก์ชันสัมบูรณ์ดังภาพที่ 2.4 สำหรับ r ที่อยู่ในช่วง 1.5-2.0 นั้นเป็นระบบแบบพลวัตมากที่สุด



ภาพที่ 2.4 ไบเฟอเคชันไดอะแกรมของแผนที่สัมบูรณ์

2.4 เซลลูลาร์ออโตมาตา

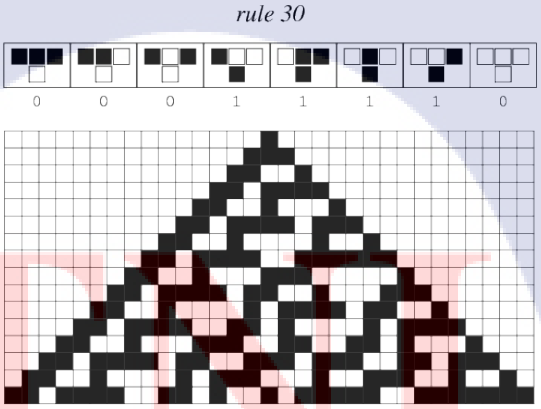
เซลล์ลูลาร์ออโตมาตามีลักษณะเป็นแบบจำลองไม่ต่อเนื่อง ประกอบด้วยเซลล์จำนวนมาก ซึ่งมีลักษณะคล้ายกับช่องตารางบนกระดานหมากรุก ซึ่งในแต่และเซลล์จะแทนด้วยตัวเลขซึ่งแสดงสถานะของเซลล์นั้นๆ และมีเวลากำกับในแต่ละเซลล์ด้วย โดยที่ในแต่ละเซลล์จะถูกควบคุมการทำงานด้วยกฎการเปลี่ยนแปลงแบบจำลอง Cellular Automata จึงถือได้ว่าเป็นแบบจำลองพลวัต ที่มีลักษณะเชิงพื้นที่และมิติของเวลาเป็นองค์ประกอบสำคัญ โดยมีองค์ประกอบของส่วนต่างๆ ด้วยกัน 5 ส่วน ได้แก่ พื้นที่เซลล์ (Cell space) ประกอบด้วยด้านสองด้านเป็นรูปเซลล์สี่เหลี่ยมจัตุรัส, สถานะเซลล์ (Cell states) สถานะของเซลล์จะแสดงถึงสถานภาพของแต่ละพื้นที่ในแต่ละเซลล์, ช่วงเวลา (Time steps)แสดงถึงช่วงเวลาระหว่างเหตุการณ์ในแต่ละเวลาที่ใช้ในการวิเคราะห์ความเปลี่ยนแปลง, กฎการเปลี่ยนแปลง (Transition rules) เป็นองค์ประกอบที่สำคัญที่สุดของแบบจำลอง Cellular Automata ใช้ในการวิเคราะห์การเปลี่ยนแปลงเพื่อที่จะกำหนดการเปลี่ยนแปลงอย่างเป็นพลวัต ซึ่งกฎการเปลี่ยนแปลงนี้โดยปกติจะระบุถึงสถานะของเซลล์ก่อนและเซลล์หลังการเปลี่ยนแปลง และองค์ประกอบสุดท้าย เซลล์รอบข้าง (Neighborhood) แบ่งตามมิติคือ ชนิดแรกเป็นแบบ 1 มิติที่มีเพียงเซลล์เพื่อนบ้านแค่ 2 เซลล์ และชนิดที่ 2 คือแบบที่ 2 มิติซึ่งมี 2 แนวคิดที่ได้กล่าวถึงเซลล์รอบข้างไว้โดย Neumannได้เสนอไว้ว่ามี 4 เซลล์รอบข้างล้อมรอบ ในขณะที่ Moore เสนอไว้ว่ามี 8 เซลล์รอบข้างล้อมรอบ



ภาพที่ 2.5 ชนิดของเซลล์เพื่อนบ้าน

2.4.1 Cellular Automata rule

ในงานวิจัยนี้ใช้กฎที่ 30 ในแบบ 1 มิติสำหรับการพัฒนาการเข้ารหัสลับภาพดิจิทัลและการประยุกต์ใช้กับการเข้ารหัสลับข้อมูล กฎที่ 30 เป็น 1 ในกฎขอเซลลูลาร์ออโตมาตาพื้นฐานที่ถูกนำเสนอโดย สตีเฟ่น วุลเฟรม (Stephen Wolfram) ในปี ค.ศ. 1983 โดยการระบุให้สถานะของเซลล์ที่อยู่ในบรรทัดถัดไปขึ้นอยู่กับสถานะของเซลล์ปัจจุบันและเซลล์เพื่อนบ้าน โดยกฎที่ 30 ถูกแปลงเป็นเลขฐานสอง $30=00011110_2$ เพื่อใช้ในการระบุสถานะของเซลล์ถัดไป



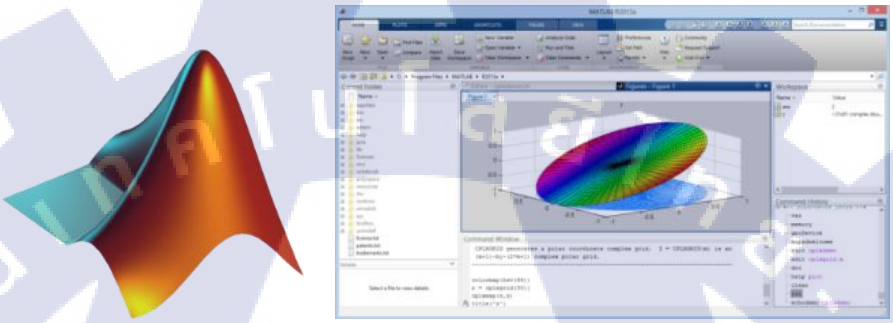
ภาพที่ 2.6 ตัวอย่างการสร้างเซลลูลาร์ออโตมาตาด้วยกฎที่ 30

2.5 โปรแกรมแมทแลป (MATLAB)

MATLAB (Matrix Laboratory) เป็นซอฟต์แวร์ในการคำนวณและการเขียนโปรแกรมพัฒนาขึ้นโดย MathWorks, MATLAB ที่มีความสามารถครอบคลุมตั้งแต่ การพัฒนาอัลกอริทึม การสร้างแบบจำลองทางคณิตศาสตร์และการทำซิมูเลชั่นของระบบ นอกจากนั้นยังสามารถใช้งานร่วมกับภาษาอื่นๆได้ เช่น C, C++, Java, และ FORTRAN

แม้ว่า MATLAB จะมีจุดประสงค์การใช้งานหลักอยู่ที่การคำนวณทางคณิตศาสตร์ แต่ก็ยังมีความสามารถในการคำนวณเชิงสัญลักษณ์ได้ด้วยแถบเครื่องมือ MuPAD และส่วนที่ออกแบบสำหรับระบบสมองกลฝังตัวและการพลวัตรได้แก่ package พิเศษ, Simulink, การจำลองกราฟฟิกแบบ multi-domain และ Model-Based

ในปี 2004 MATLAB มีผู้ใช้งานทั้งในภาคอุตสาหกรรมและภาคการศึกษาประมาณหนึ่งล้านคน ซึ่งมาจากพื้นฐานที่แตกต่างกันเช่น วิศวกร นักวิทยาศาสตร์ หรือแม้กระทั่งนั่งธุรกิจ โดยถูกใช้อย่างแพร่หลายทั้งในสถาบันการวิจัยหรือสถานประกอบการ



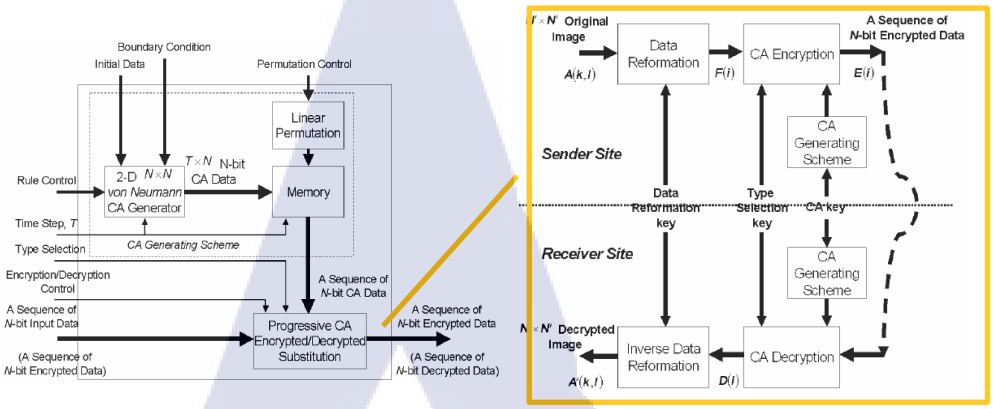
ภาพที่ 2.7 โปรแกรม MATLAB

2.6 เอกสาร และงานวิจัยที่เกี่ยวข้อง

งานวิจัยนี้ศึกษาเอกสารและงานวิจัยดังต่อไปนี้

2.6.1 Image Encryption/Decryption System Using 2-D Cellular Automata

การเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาแบบ 2 มิติ เน้นทางด้านการนำเซลล์ลูลาร์ออโตมาตาแบบ 2 มิติมาใช้ในการเข้ารหัสลับภาพดิจิทัลเป็นหลัก โดยใช้ generalized CA transform (GCAT) เป็นฟังก์ชันในการเข้ารหัสลับภาพดิจิทัล จุดเด่นของงานวิจัยฉบับนี้คือ การถอดรหัสลับภาพดิจิทัลแล้วไม่มีการสูญเสียข้อมูลเลย (Loss-less) นอกจากนี้รูปแบบการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลที่นำเสนอนี้ ใช้ทรัพยากรคอมพิวเตอร์ในการคำนวณสมการลดลง



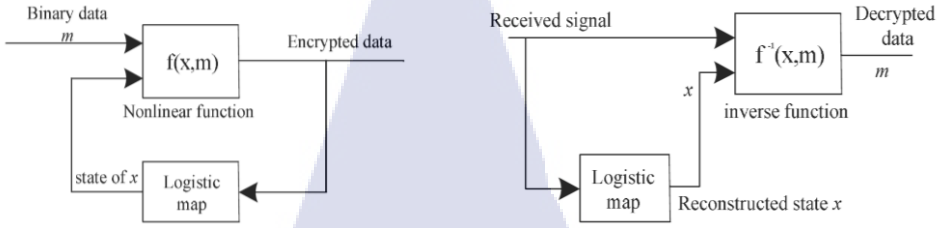
ภาพที่ 2.8 รูปแบบการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา

2.6.2 Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function

การเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบอลวนแบบไม่เป็นเชิงเส้นนี้ ใช้สมการ Logistic map คือ $x_{n+1} = r x_n (1 - x_n)$ โดยใช้ r ในช่วง 3.57 ≤ r ≤ 4 ซึ่ง Logistic map เป็นสมการหนึ่งที่มีคุณสมบัติเป็นระบบอลวนในการเข้ารหัสลับภาพดิจิทัล โดยที่มีค่าสภาวะเริ่มต้นเป็นกุญแจในการเข้ารหัสลับภาพดิจิทัลดังภาพที่ 2.9 (ก) และถอดรหัสลับภาพดิจิทัลดังภาพที่ 2.9 (ข)

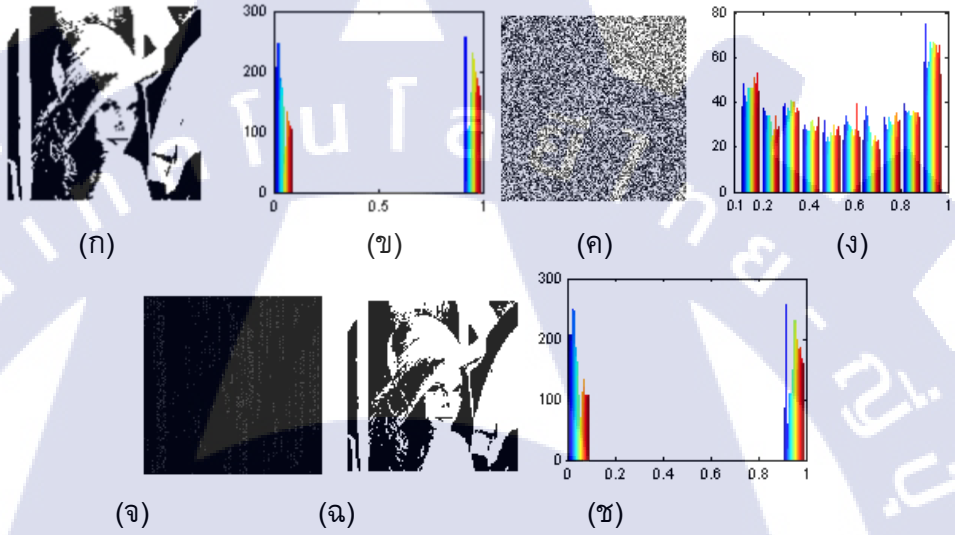
ภาพที่ใช้เข้ารหัสลับภาพดิจิทัลเป็นภาพขาวดำดังภาพที่ 2.10 (ก) ได้กราฟฮิสโตแกรมดังภาพที่ 2.10 (ข) หลังจากการเข้ารหัสลับภาพดิจิทัลได้ผลลัพธ์ดังภาพที่ 2.10 (ค) และภาพที่ 2.10 (ง) เป็นกราฟฮิสโตแกรมของภาพที่เข้ารหัสลับภาพดิจิทัล นอกจากนี้ยังมีการวัดประสิทธิภาพของคีย์ที่ใช้ในการเข้ารหัสลับภาพดิจิทัล หากใช้คีย์ที่ไม่ถูกต้องในการถอดรหัสลับภาพดิจิทัลจะได้ผลลัพธ์ดังภาพที่ 2.10 (จ) ในทางกลับกันหากใช้คีย์ที่ถูกต้องในการถอดรหัสลับภาพดิจิทัลจะได้ผลลัพธ์ดังภาพที่ 2.10 (ฉ) และมีกราฟฮิสโตแกรมดังภาพที่ 2.10 (ช)

ผลที่ได้จากการจำลองเข้ารหัสและถอดรหัสจากการใช้โปรแกรม MATLAB ในการเขียนโปรแกรมตามกระบวนการที่นำเสนอคือ สามารถถอดรหัสได้ถูกต้องและมีความน่าเชื่อของข้อมูล รูปแบบที่นำเสนอสามารถนำไปใช้กับฮาร์ดแวร์ได้จริง เนื่องจากมีกลไกที่เรียบง่าย ใช้เวลารวดเร็วในการเข้ารหัสและข้อมูลที่เข้ารหัสมีความปลอดภัย



(ก) (ข)

ภาพที่ 2.9 รูปแบบการเข้ารหัสลับและการถอดรหัสลับภาพดิจิทัล



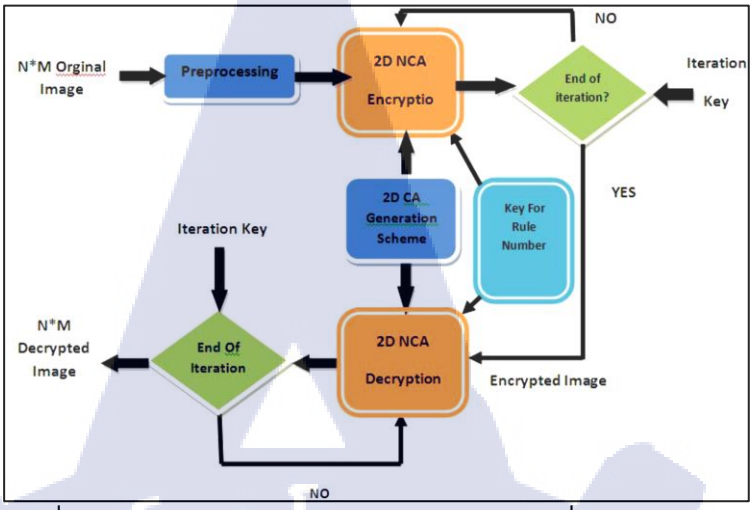
(ก) (ข) (ค) (ง)

(จ) (ฉ) (ช)

ภาพที่ 2.10 กราฟฮิสโตแกรมที่ได้จากการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัล

2.6.3 An Image Encryption System by Indefinite Cellular Automata and Chaos

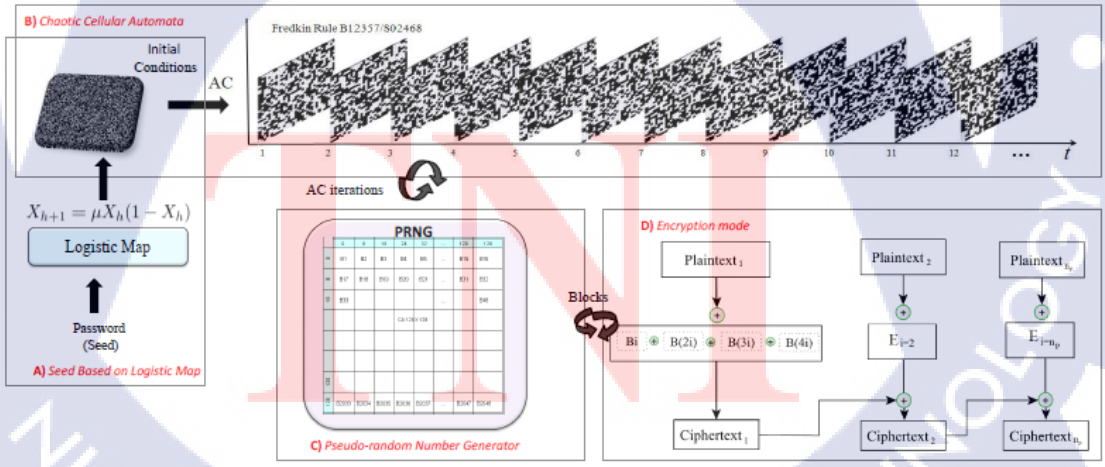
การเข้ารหัสลับภาพดิจิทัลโดยเซลลูลาร์ออโตมาตาและระบบอลวนเป็นการเข้ารหัสลับโดยการนำเอาเซลลูลาร์ออโตมาตาและระบบอลวนมาใช้ ซึ่งรูปแบบที่งานวิจัยฉบับนี้นำเสนอคือการนำสมการเคออสมากำหนดค่าเริ่มต้นของเซลล์ลูลาร์ออโตมาตาในแต่ละเซลล์ และนำกฎการเปลี่ยนแปลงของเซลล์ลูลาร์ออโตมาตามาใช้ในการกำหนดค่าใหม่จากข้อมูลที่ได้จากสมการเคออส จากนั้นจึงนำสิ่งที่ได้เตรียมไว้มาใช้ในการเข้ารหัสลับภาพดิจิทัล งานวิจัยฉบับนี้มีจุดเด่นที่การถอดรหัสลับภาพดิจิทัลแล้วไม่มีการสูญเสียข้อมูลเลย (Loss-less) มีความปลอดภัยสูงและใช้ระยะเวลาในการประมวลผลน้อย



ภาพที่ 2.11 อัลกอริทึมการเข้ารหัสลับภาพดิจิทัลที่งานวิจัยนำเสนอ

2.6.4 Chaotic Encryption Method Based on Life-Like Cellular Automata

การเข้ารหัสลับระบบอลวนบนพื้นฐานเซลลูลาร์ออโตมาตาชนิด Life-Like เสนอการใช้สมการ Logistic map ในการกำหนดค่าเริ่มต้นของเซลลูลาร์ออโตมาตา และใช้กฎของ Fredkin (B1357/S02468) ซึ่งเป็นเซลล์ลูลาร์ออโตมาตาแบบ 2 มิติและเป็นชนิด Life-Like ในการสร้างระนาบเพื่อใช้ในการเข้ารหัสลับ จุดเด่นของงานวิจัยฉบับนี้คือ การใช้เซลลูลาร์ออโตมาตาชนิดนี้ให้คุณภาพในการสุ่มค่าที่ดีกว่าแบบอื่น และมีความเรียบง่าย ทำให้ลดต้นทุนในการดำเนินการ



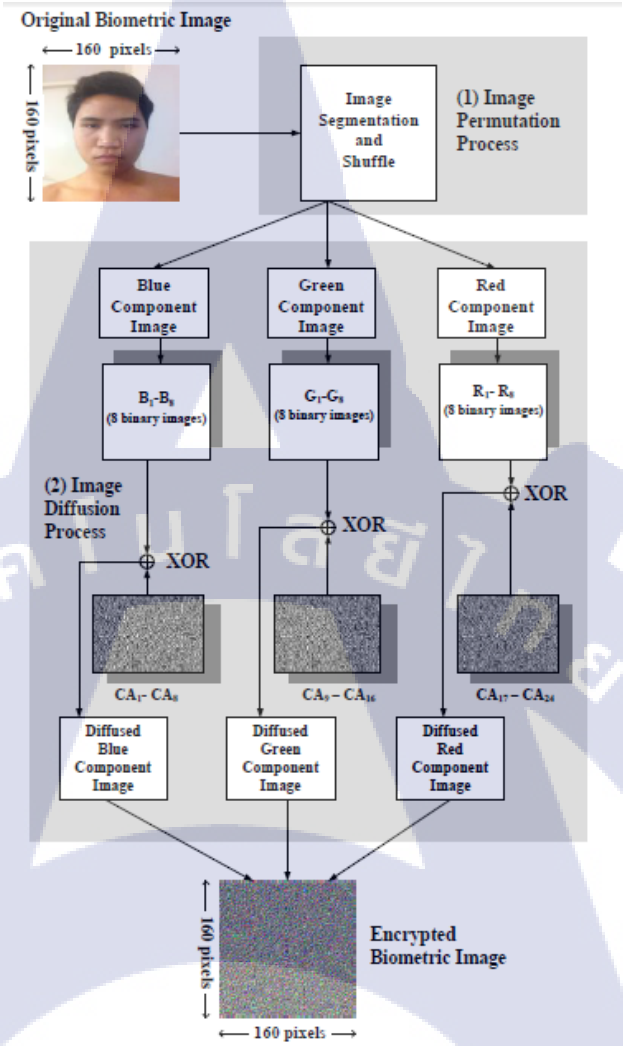
ภาพที่ 2.12 รูปแบบการเข้ารหัสลับภาพดิจิทัลที่นำเสนอ

2.6.5 A Novel Image Security System Based on Cellular Automata and Improved Chaotic System

ระบบการรักษาความปลอดภัยแบบใหม่บนพื้นฐานเซลลูลาร์ออโตมาตาและระบบอลวน ใช้แผนที่มาตรฐาน (Standard map) ในการออกแบบอัลกอริทึมการเข้ารหัสลับภาพดิจิทัล แผนที่มาตรฐานเป็นสมการที่ถูกนำมาใช้เพื่อตรวจสอบสถานะการเปลี่ยนแปลงกฎระเบียบของแต่ละเซลล์เพื่อการสุ่มเทียมของอัลกอริทึม การทดลองการจำลองและการวิเคราะห์การรักษาความปลอดภัยระบุว่าอัลกอริทึมที่นำเสนอมีพื้นที่ใหญ่เพียงพอสำหรับพื้นที่คีย์ (key space) กับภาพที่เข้ารหัส แสดงให้เห็นถึงการกระจายที่ดีและความซับซ้อนที่ดีเยี่ยม นอกจากนี้อัลกอริทึมดังกล่าวสามารถต้านทานการโจมตีได้อย่างงมีประสิทธิภาพ

2.6.6 Digital Biometric Facial Image Encryption using Chaotic Cellular Automata for Secure Image Storages

การเข้ารหัสลับภาพผิวหน้าไบโอเมตริกแบบดิจิทัลโดยใช้ระบบอลวนและเซลลูลาร์ออโตมาตาสำหรับการเก็บรักษาความปลอดภัยนี้ แบ่งเป็น 2 ส่วนหลักๆ คือ permutation เป็นการทำให้ภาพต้นแบบไม่อยู่ในสภาพเดิม ในที่นี้ทำการสลับตำแหน่งของพิกเซล จากนั้นเป็นส่วนของ diffusion ซึ่งส่วนนี้ได้มีการนำเซลล์ลูลาร์ออโตมาตาแบบ 1 มิติ มาใช้ในการเข้ารหัสลับภาพดิจิทัล จุดเด่นของงานวิจัยฉบับนี้คือ การเข้ารหัสลับภาพดิจิทัลมีความรวดเร็วและมีความปลอดภัยสูง



ภาพที่ 2.13 กระบวนการเข้ารหัสลับภาพดิจิทัลที่นำเสนอ

บทที่ 3
การออกแบบและการพัฒนา

งานวิจัยนี้แบ่งการทำงานออกเป็น 3 ส่วน ในส่วนแรกเป็นการศึกษาเกี่ยวกับเทคโนโลยีการเข้ารหัสลับภาพดิจิทัล ทฤษฎีอลวน เซลลูลาร์ออโตมาตาและงานวิจัยที่เกี่ยวข้อง นอกจากนั้นยังศึกษาการเขียนโปรแกรม MATLAB สำหรับการจำลองการเข้ารหัสลับภาพดิจิทัล ส่วนต่อมาเป็นการออกแบบและพัฒนาการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัลให้มีประสิทธิภาพที่ดีขึ้น ในส่วนสุดท้ายเป็นการประยุกต์ใช้อัลกอริทึมที่ได้ออกแบบเข้ากับการเข้ารหัสลับข้อมูลไฟล์ชนิดต่างๆ

3.1 การศึกษาทฤษฎีที่ต้องใช้ในงานวิจัย

งานวิจัยนี้จำเป็นต้องศึกษาในเรื่องดังต่อไปนี้

3.1.1 เทคโนโลยีการเข้ารหัสลับภาพดิจิทัล

3.1.2 ทฤษฎีอลวน

3.1.3 เซลลูลาร์ออโตมาตา

3.1.4 การวิเคราะห์งานวิจัย

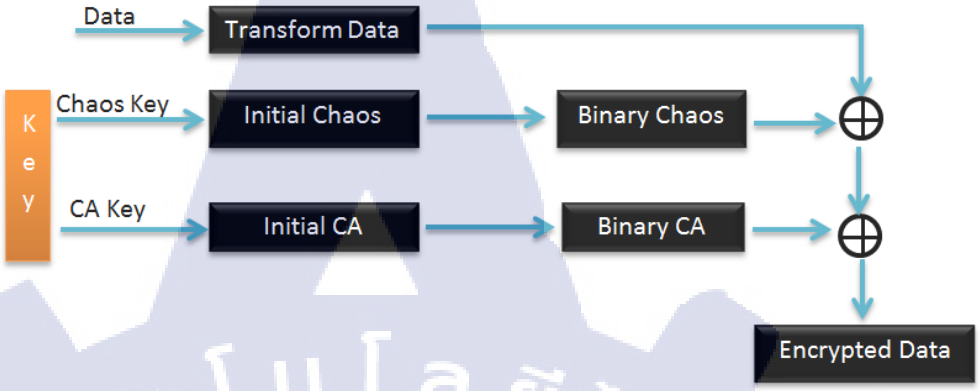
3.1.5 ศึกษาการเขียนโปรแกรม MATLAB เพิ่มเติม

3.2 การออกแบบอัลกอริทึมที่ใช้ในงานวิจัย

จากการวิเคราะห์การเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบอลวนเพียงอย่างเดียว พบว่ามีความซับซ้อนและสามารถป้องกันการโจมตีได้อย่างมีประสิทธิภาพ เช่นเดียวกับการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาเพียงอย่างเดียว เนื่องด้วยทั้งเซลลูลาร์ออโตมาตาและระบบอลวนนั้นมีคุณสมบัติเป็นระบบพลวัต จึงทำให้ยากต่อการถอดรหัสลับภาพดิจิทัลและการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวนมีความความปลอดภัยและความซับซ้อนในการถอดรหัสลับภาพดิจิทัลเพิ่มมากขึ้นเป็น 2 เท่า

กระบวนการทำงานของอัลกอริทึมที่ออกแบบนี้จำเป็นต้องเปลี่ยนข้อมูลของภาพให้เป็นข้อมูลในเลขฐานสองก่อนการเข้ารหัสลับภาพดิจิทัล และมีการสร้างชุดข้อมูลด้วยระบบอลวนเพื่อนำมาใช้ในการเข้ารหัสลับภาพดิจิทัลในขั้นแรก เมื่อได้ข้อมูลที่เข้ารหัสลับภาพดิจิทัลแล้วจึงทำการสร้างชุดข้อมูลด้วยเซลลูลาร์ออโตมาตาขึ้น เพื่อนำมาใช้ในการเข้ารหัสลับภาพดิจิทัลกับข้อมูลที่ผ่านการเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบอลวน ดังนั้นคีย์ที่ใช้ในการเข้ารหัสลับ

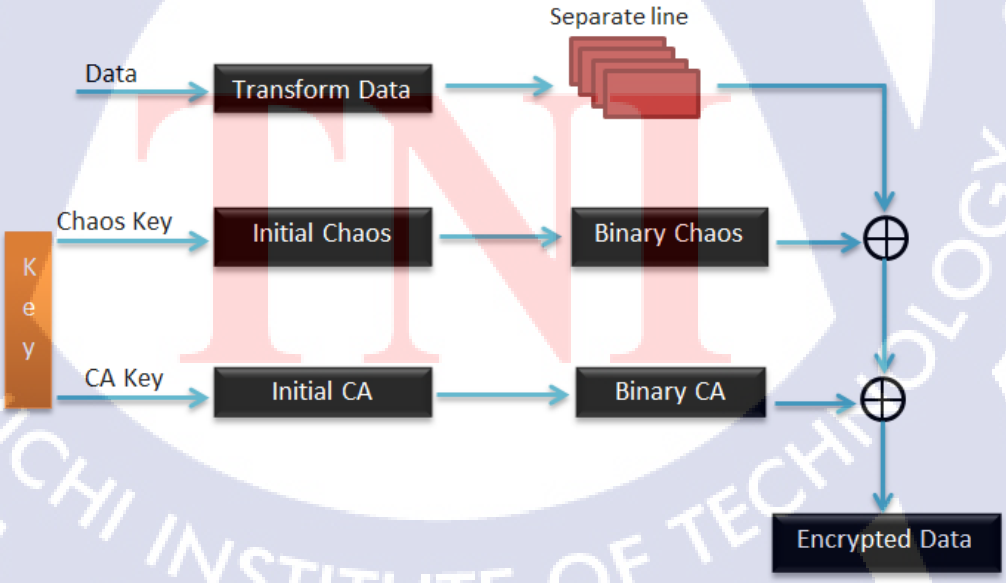
ภาพดิจิทัลโดยการใช้อัลกอริทึมที่ออกแบบนี้มาจากการสร้างชุดข้อมูลของระบบอลวนและเซลลูลาร์ออโตมาตา



ภาพที่ 3.1 อัลกอริทึมการเข้ารหัสลับภาพดิจิทัลที่ออกแบบ

3.3 การประยุกต์ใช้อัลกอริทึมกับการเข้ารหัสลับข้อมูล

เมื่อทำการปรับปรุงอัลกอริทึมที่ออกแบบจนมีประสิทธิภาพที่ดีขึ้น หลังจากนั้นจึงนำอัลกอริทึมดังกล่าวมาประยุกต์เข้ากับการเข้ารหัสลับข้อมูลไฟล์ชนิดอื่น แต่เนื่องจากข้อมูลของไฟล์ชนิดอื่นนั้นมีลักษณะการเก็บข้อมูลเป็นบรรทัด จึงจำเป็นต้องเปลี่ยนการแปลงข้อมูลไฟล์ชนิดอื่นให้มีการเข้ารหัสลับทีละบรรทัดแทนการนำข้อมูลทั้งหมดมาเข้ารหัสลับภายในครั้งเดียว



ภาพที่ 3.2 อัลกอริทึมการเข้ารหัสลับข้อมูล

บทที่ 4
ผลการทดลองและการวิเคราะห์

4.1 ผลลัพธ์การเข้ารหัสลับ

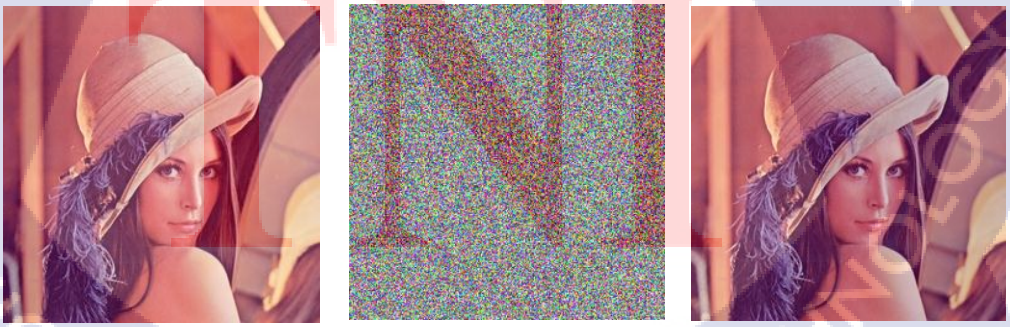
ผลลัพธ์ของการเข้ารหัสลับทั้งการเข้ารหัสลับภาพดิจิทัลและการเข้ารหัสลับข้อมูลในแต่ละอัลกอริทึมเป็นดังต่อไปนี้

4.1.1 ผลลัพธ์ที่ได้จากการเข้ารหัสลับภาพดิจิทัล

การทดสอบประสิทธิภาพของการเข้ารหัสลับภาพดิจิทัลเพื่อปรับปรุงให้ได้อัลกอริทึมที่ดีที่สุด จำเป็นต้องทดสอบการทำงานของอัลกอริทึมในแต่ละช่วงการทำงาน โดยแบ่งอัลกอริทึมที่นำเสนอออกเป็น 3 อัลกอริทึม ได้แต่ การเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบบอลวน, การเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา และการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบบอลวน ซึ่งได้ผลลัพธ์ดังต่อไปนี้

1. ผลลัพธ์จากการเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบบอลวน

ภาพที่ 4.1 (ก) เป็นภาพก่อนการเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบบอลวน ซึ่งหลังจากผ่านการเข้ารหัสลับภาพดิจิทัลแล้วเป็นไปตามภาพที่ 4.1 (ข) เมื่อทดลองถอดรหัสลับภาพดิจิทัลโดยการใช้ระบบบอลวนแล้วได้ผลลัพธ์ดังภาพที่ 4.1 (ค)

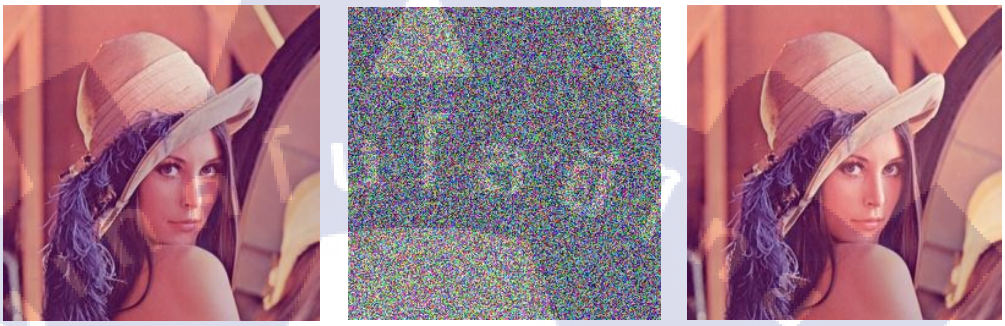


(ก) (ข) (ค)

ภาพที่ 4.1 ภาพที่ได้จากการเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบบอลวน

2. ผลลัพธ์จากการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา

จากการทดลองการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา โดยการนำภาพที่ 4.2 (ก) มาทำการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาแล้วได้ภาพที่มีความซับซ้อนดังภาพที่ 4.2 (ข) และเมื่อทำการถอดรหัสลับภาพดิจิทัลแล้วสามารถได้ภาพเดียวกับภาพก่อนเข้ารหัสลับภาพดิจิทัลดังภาพที่ 4.2 (ค)

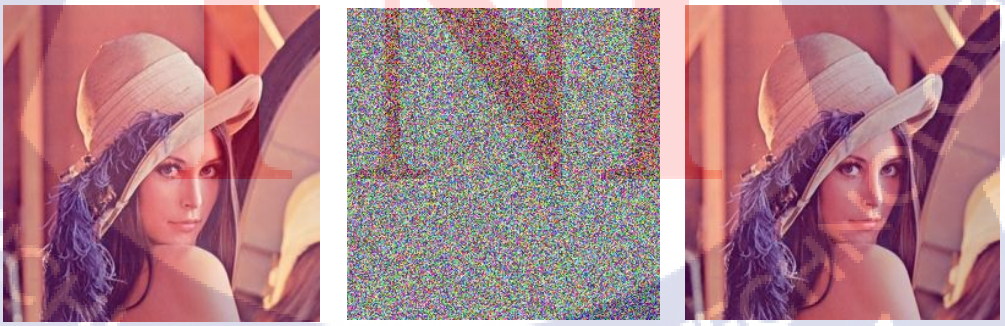


(ก) (ข) (ค)

ภาพที่ 4.2 ภาพที่ได้จากการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา

3. ผลลัพธ์จากการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวน

เมื่อนำเซลลูลาร์ออโตมาตาและระบบอลวนมาใช้ในการเข้ารหัสลับภาพดิจิทัล โดยใช้ภาพที่ 4.3 (ก) ในการเข้ารหัสลับภาพดิจิทัล พบว่าภาพที่ผ่านการเข้ารหัสลับภาพดิจิทัลดังภาพที่ 4.3 (ข) มีความซับซ้อนเช่นเดียวกับการเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบอลวนและการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา และสามารถถอดรหัสลับภาพดิจิทัลได้ดังภาพที่ 4.3 (ค)



(ก) (ข) (ค)

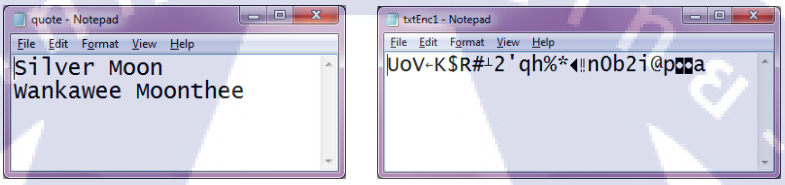
ภาพที่ 4.3 ภาพที่ได้จากการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา และระบบอลวน

4.1.2 ผลลัพธ์ที่ได้จากการเข้ารหัสลับข้อมูล

หลังจากที่ปรับปรุงอัลกอริทึมที่นำเสนอให้มีประสิทธิภาพที่ดีขึ้น แล้วจึงทำการประยุกต์ใช้กับการเข้ารหัสลับข้อมูลไฟล์ชนิดอื่นได้ผลลัพธ์ดังนี้

1. ผลลัพธ์จากการเข้ารหัสข้อมูลชนิด Text File

ภาพที่ 4.4 (ก) เป็นไฟล์ที่ใช้ทดสอบการเข้ารหัสลับข้อมูลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวน และได้ผลลัพธ์ดังภาพที่ 4.4 (ข) ซึ่งเป็นตัวอักษรที่ไม่สามารถแปลความหมายได้

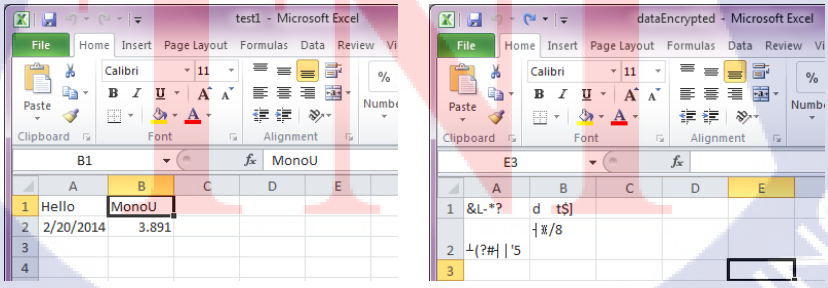


(ก) (ข)

ภาพที่ 4.4 ผลลัพธ์จากการเข้ารหัสข้อมูลชนิด Text File

2. ผลลัพธ์จากการเข้ารหัสข้อมูลชนิด Excel File

หลังจากที่นำข้อมูลชนิด Excel File ดังภาพที่ 4.5 (ก) มาเข้ารหัสลับข้อมูลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวนได้ผลลัพธ์ดังภาพที่ 4.5 (ข) ซึ่งเป็นอักษรที่ไม่สามารถแปลความหมายได้เช่นเดียวกับข้อมูลชนิด Text File



(ก) (ข)

ภาพที่ 4.5 ผลลัพธ์จากการเข้ารหัสข้อมูลชนิด Excel File

4.2 การวิเคราะห์ประสิทธิภาพการเข้ารหัสลับภาพดิจิทัล

4.2.1 การวิเคราะห์ประสิทธิภาพและความปลอดภัย

ทฤษฎีที่ใช้ในการวิเคราะห์ประสิทธิภาพและความปลอดภัยนั้นมีหลายทฤษฎีด้วยกัน แต่งานวิจัยชิ้นนี้ได้เลือกใช้ทฤษฎีดังต่อไปนี้

1. การวิเคราะห์เอนโทรปี

เอนโทรปีเป็นการสุ่มรวบรวมข้อมูลสำหรับใช้ในการเข้ารหัสลับภาพดิจิทัลหรือการใช้งานอื่นๆที่ต้องการข้อมูลแบบสุ่ม เพื่อวัดประสิทธิภาพการรักษาความปลอดภัยจากการถูกโจมตีจากภายนอก ค่าเอนโทรปีที่มีประสิทธิภาพที่ดีที่สุดคือ 8 จากการทดสอบประสิทธิภาพของแต่ละอัลกอริทึมได้ผลลัพธ์ดังตารางที่ 4.1

ตารางที่ 4.1 ค่าของเอนโทรปีในแต่ละอัลกอริทึมที่ใช้ในการเข้ารหัสลับภาพดิจิทัล

Type	Red	Green	Blue
Chaos	7.9972	7.9973	7.9971
CA	7.9975	7.9973	7.9972
Chaos&CA	7.9976	7.9969	7.9971

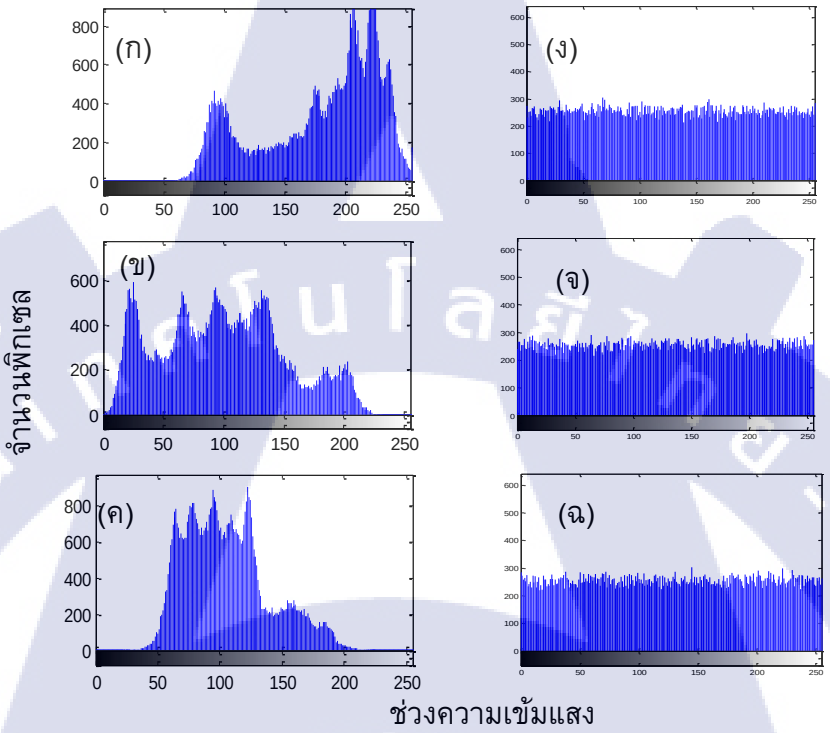
จากตารางข้างต้น แสดงให้เห็นว่าค่าของเอนโทรปีมีค่าที่เข้าใกล้ 8 ซึ่งหมายความว่ามีประสิทธิภาพมากในด้านความปลอดภัยของการเข้ารหัสลับภาพดิจิทัล

2. การวิเคราะห์ฮิสโตแกรม

2.1 ภาพฮิสโตแกรมของภาพการเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบอลวน

การวิเคราะห์ฮิสโตแกรมจำเป็นต้องเปรียบเทียบระหว่างภาพฮิสโตแกรมของภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลังเข้ารหัสลับภาพดิจิทัล ซึ่งแต่ละภาพประกอบด้วย 3 ระนาบ โดยภาพที่ 4.6 (ก) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีแดง (R) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.6 (ข) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีเขียว (G) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.6 (ค) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบ

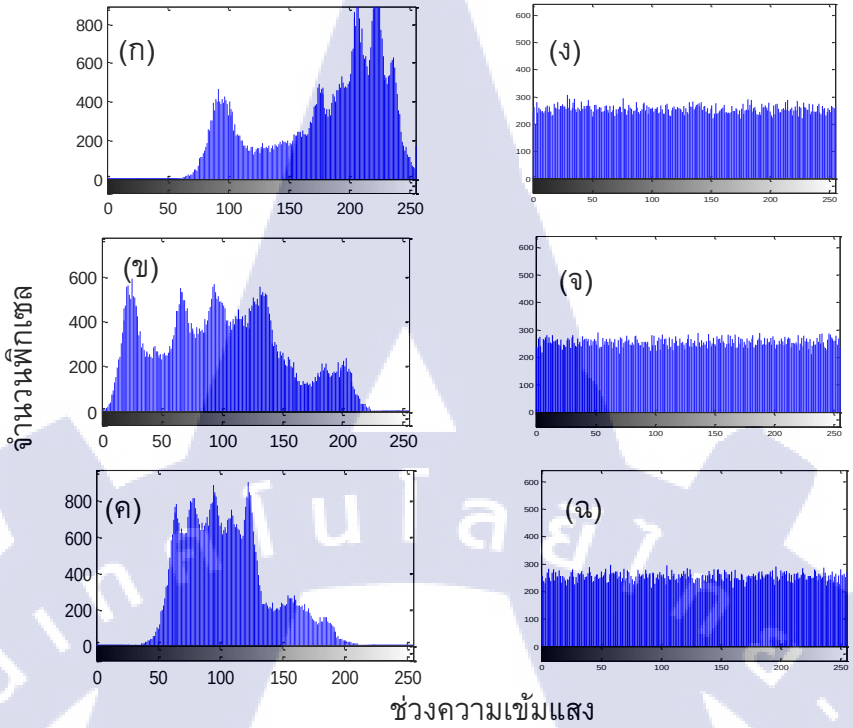
สีน้ำเงิน (B) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล และ ภาพที่ 4.6 (ง) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีแดง (R) ของภาพหลังเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.6 (จ) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีเขียว (G) ของภาพหลังเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.6 (ฉ) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีน้ำเงิน (B) ของภาพหลังเข้ารหัสลับภาพดิจิทัล



ภาพที่ 4.6 ฮิสโตแกรมของภาพก่อนเข้ารหัสลับและภาพหลังเข้ารหัสลับภาพดิจิทัลโดยการใช้ระบบอลวน

2.2 ภาพฮิสโตแกรมของภาพการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตา

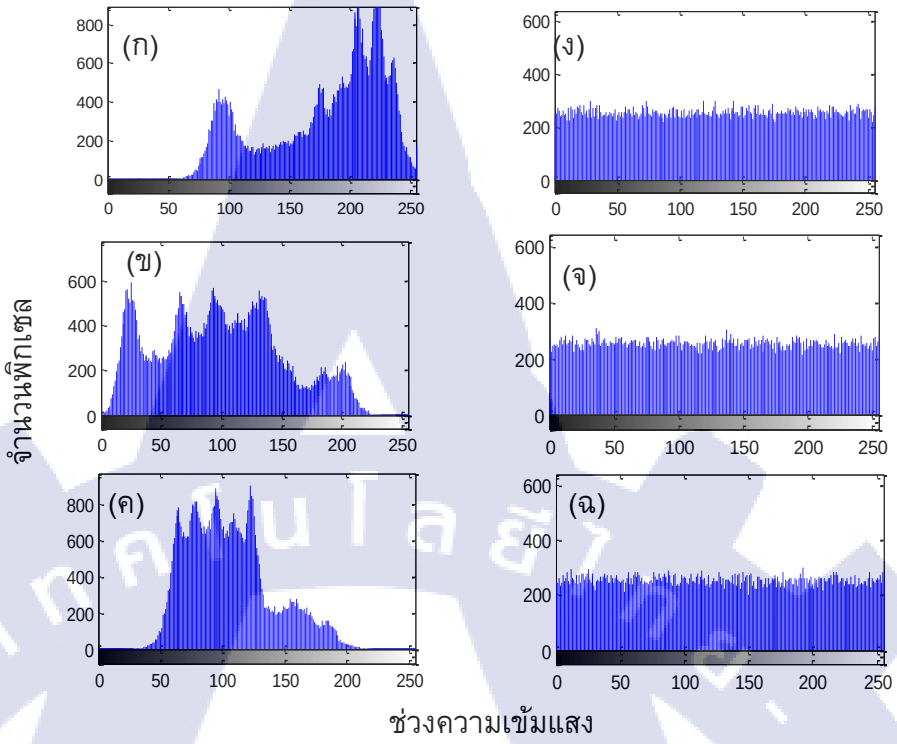
การวิเคราะห์ฮิสโตแกรมจำเป็นต้องเปรียบเทียบระหว่างภาพฮิสโตแกรมของภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลังเข้ารหัสลับภาพดิจิทัล ซึ่งแต่ละภาพประกอบด้วย 3 ระนาบ โดยภาพที่ 4.7 (ก) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีแดง (R) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.7 (ข) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีเขียว (G) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.7 (ค) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีน้ำเงิน (B) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล และ ภาพที่ 4.7 (ง) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีแดง (R) ของภาพหลังเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.7 (จ) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีเขียว (G) ของภาพหลังเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.7 (ฉ) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีน้ำเงิน (B) ของภาพหลังเข้ารหัสลับภาพดิจิทัล



ภาพที่ 4.7 ฮิสโตแกรมของภาพก่อนเข้ารหัสลับและภาพหลังเข้ารหัสลับภาพดิจิทัล โดยการใช้เซลลูลาร์ออโตมาตา

2.3 ภาพฮิสโตแกรมของภาพการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ ออโตมาตาและระบบอลวน

การวิเคราะห์ฮิสโตแกรมจำเป็นต้องเปรียบเทียบระหว่างภาพฮิสโตแกรมของภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลังเข้ารหัสลับภาพดิจิทัล ซึ่งแต่ละภาพประกอบด้วย 3 ระนาบ โดยภาพที่ 4.8 (ก) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีแดง (R) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.8 (ข) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีเขียว (G) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.8 (ค) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีน้ำเงิน (B) ของภาพก่อนเข้ารหัสลับภาพดิจิทัล และ ภาพที่ 4.8 (ง) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีแดง (R) ของภาพหลังเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.8 (จ) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีเขียว (G) ของภาพหลังเข้ารหัสลับภาพดิจิทัล, ภาพที่ 4.8 (ฉ) เป็นภาพฮิสโตแกรมระนาบองค์ประกอบสีน้ำเงิน (B) ของภาพหลังเข้ารหัสลับภาพดิจิทัล



ภาพที่ 4.8 ฮิสโตแกรมของภาพก่อนเข้ารหัสลับและภาพหลังเข้ารหัสลับภาพดิจิทัล โดยการใช้เซลลูลาร์ออโตมาตาและระบบบอลวน

จากการวิเคราะห์จำนวนความถี่ของความเข้มแสงในแต่ละระนาบระหว่างภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลังเข้ารหัสลับภาพดิจิทัล มีจำนวนความถี่ของความเข้มแสงที่แตกต่างกันมาก ภาพก่อนเข้ารหัสลับภาพดิจิทัลนั้นมีการแบ่งแยกสีในแต่ละระนาบอย่างชัดเจนซึ่งเป็นปกติของรูปภาพ แต่ภาพหลังการเข้ารหัสลับภาพดิจิทัลนั้นมีความถี่ของความเข้มแสงแต่ละช่วงสีในปริมาณใกล้เคียงกัน จึงยากต่อการคาดเดารูปภาพ ทำให้มีความปลอดภัยในการเข้ารหัสลับภาพดิจิทัล

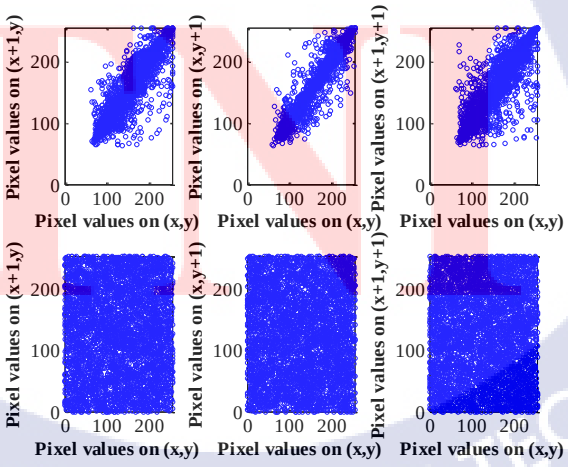
3. การวิเคราะห์สัมประสิทธิ์สหสัมพันธ์

สัมประสิทธิ์สหพันธ์เป็นการตรวจสอบความสัมพันธ์ระหว่างข้อมูล 2 ชุด ซึ่งในงานวิจัยนี้ได้ทำการตรวจสอบความสัมพันธ์ระหว่างภาพก่อนเข้ารหัสลับภาพดิจิทัลกับภาพหลังเข้ารหัสลับภาพดิจิทัลของแต่ละอัลกอริทึมดังตารางที่ 4.3

ตารางที่ 4.2 ค่าสัมประสิทธิ์สหสัมพันธ์ในแต่ละอัลกอริทึม

Correlation Coefficient between		Value		
Original image	Encrypted image	Chaos	CA	Chaos&CA
Red	Red	0.0005	0.0009	-0.0041
Red	Green	-0.0064	0.001	0.0121
Red	Blue	-0.0061	-0.0016	0.0008
Green	Red	0.001	0.0012	-0.004
Green	Green	-0.0078	0.0028	0.0111
Green	Blue	-0.0052	-0.0028	0.0004
Blue	Red	-0.0005	0.0021	-0.0042
Blue	Green	-0.0071	0.0033	0.0089
Blue	Blue	-0.0016	-0.0041	-0.0011

จากค่าสัมประสิทธิ์สหสัมพันธ์ในตารางข้างต้นแสดงให้เห็นว่ามีค่าเข้าใกล้ 0 นั่นหมายความว่า ระหว่างภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลงเข้ารหัสลับภาพดิจิทัลในแต่ละระนาบไม่มีความสัมพันธ์ซึ่งกันและกัน จึงไม่สามารถหาจุดเชื่อมโยงระหว่าง 2 ภาพได้ และในแต่อัลกอริทึมนั้นมีค่าที่ใกล้เคียงกัน แต่เนื่องจากการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวนมีความซับซ้อนของอัลกอริทึมในการเข้ารหัสลับภาพดิจิทัลมากกว่า ถึงแม้ว่าค่าสัมประสิทธิ์สหสัมพันธ์ที่ได้จะมากกว่าอัลกอริทึมอื่นแต่ยังอยู่ในขอบเขตที่เหมาะสม เพราะฉะนั้นการเข้ารหัสลับภาพดิจิทัลโดยการใช้เซลลูลาร์ออโตมาตาและระบบอลวนมีประสิทธิภาพมากในการป้องกันการโจมตีจากภายนอก



ภาพที่ 4.9 ตัวอย่างสัมประสิทธิ์สหสัมพันธ์ (ระนาบองค์ประกอบสีแดง) ในแนวแกนตั้ง แกนนอน และแนวทแยง ของภาพก่อนเข้ารหัสลับกับภาพหลังเข้ารหัสลับ

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 ผลการดำเนินงาน

จากการดำเนินงานวิจัยนี้ พบว่าผลลัพธ์ที่ได้เป็นไปตามวัตถุประสงค์ของงานวิจัยดังนี้

1. สามารถอธิบายเทคโนโลยีการเข้ารหัสลับภาพดิจิทัล รวมถึงทฤษฎีอลวนและเซลลูลาร์ออโตมาตา
2. สามารถออกแบบอัลกอริทึมที่ใช้ในการเข้ารหัสลับภาพดิจิทัลและปรับปรุงให้มีประสิทธิภาพที่ดีกว่าเดิม
3. สามารถนำอัลกอริทึมที่ออกแบบและพัฒนามาประยุกต์ใช้เข้ากับการเข้ารหัสลับข้อมูลไฟล์ชนิดอื่นได้

ผลลัพธ์ที่ได้จากการวิจัยพบว่า อัลกอริทึมที่นำเสนอมีค่าเอนโทรปีเข้าใกล้ 8 ซึ่งค่าดังกล่าวเป็นไปตามทฤษฎีและจากการเปรียบเทียบระหว่างภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลังเข้ารหัสลับภาพดิจิทัลในแต่ละระนาบมีค่าสัมประสิทธิ์สหพันธ์มีค่าเข้าใกล้ศูนย์แสดงถึงการไม่มีความสัมพันธ์กันระหว่างภาพก่อนเข้ารหัสลับภาพดิจิทัลและภาพหลังเข้ารหัสลับภาพดิจิทัล นอกจากนี้ค่าความถี่ของความเข้มแสงในแต่ละระนาบของภาพหลังเข้ารหัสลับภาพดิจิทัลมีค่าความถี่แต่ละช่วงความเข้มแสง (0-255) ที่ใกล้เคียงกัน ผลลัพธ์ดังกล่าวบ่งชี้ถึงสถานะของการเข้ารหัสลับภาพดิจิทัลที่มีความปลอดภัยสูงมาก และใช้ระยะเวลาในการเข้ารหัสลับภาพดิจิทัลน้อยลง

5.2 ปัญหาและอุปสรรค

5.2.1 จำเป็นต้องศึกษาหลายๆ เรื่องที่เกี่ยวข้องกับโครงงงาน

5.2.2 ทักษะการเขียนโปรแกรม MATLAB ไม่เพียงพอและมีฟังก์ชั่นอื่น ๆ อีกมากมายที่ต้องศึกษาเพิ่มเติม มันทำให้เกิดปัญหามากขึ้นในการเขียนโปรแกรม

5.2.3 ข้อมูลที่เกี่ยวข้องกับการเข้ารหัสลับภาพดิจิทัลโดยการใช้การใช้เซลล์ลูลาร์ออโตมาตาและระบบอลวนมีกรณีศึกษาน้อย

5.2.4 ทฤษฎีการวัดประสิทธิภาพการทำงานของการเข้ารหัสภาพดิจิทัลเป็นเรื่องใหม่ในการศึกษา มันจะต้องใช้เวลาในการเรียนรู้

5.2.5 การประยุกต์ใช้โดยการเข้ารหัสข้อมูลที่มีปัญหามากมายเกี่ยวกับข้อจำกัดของการเขียนโปรแกรมเพราะโปรแกรม MATLAB ไม่สามารถนำเข้าไฟล์บางประเภท

5.3 ข้อเสนอแนะ

เนื่องด้วยโปรแกรม MATLAB มีข้อจำกัดเรื่องชนิดของไฟล์ในการอิมพอร์ต จึงอยากให้มีการประยุกต์ใช้กับโปรแกรมอื่นเพื่อใช้ในการแก้ไขข้อจำกัดของโปรแกรม MATLAB และอยากให้มีส่วนติดต่อกับผู้ใช้ (Graphic User Interface) เพื่อง่ายต่อการใช้งาน นอกจากนี้อยากให้ศึกษาการวิเคราะห์ประสิทธิภาพการเข้ารหัสลับของข้อมูลเพิ่มเติม

บรรณานุกรม

S. Cheepchol, W. San-Um, S. Kiattisin and A. Leelasantitham , 2013, **Digital Biometric Facial Image Encryption using Chaotic Cellular Automata for Secure Image Storages**

RAVI SHANKER YADAV, MHD. RIZWAN BEG and MANISH MADHAVA TRIPATHI, 2013**, Image encryption techniques: a critical comparison**

The MathWorks, Inc., 2013, **Data Import and Export** [Online], Available, http://www.mathworks.com/ [2013, September 7]

LOU Yuefang, HU Tianqiao, 2012, **A Novel Image Security System Based on Cellular Automata and Improved Chaotic System**

Francesco Berto , Jacopo Tagliabue , Stanford University, 2012, **Cellular Automata** [Online], Available, http://plato.stanford.edu/entries/cellular-automata/ [2013, July 27]

H. Ogras, M. Turk, 2012, **Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function**

Varsha S.Nemade, R.B.Wagh, 2012, **Review of different image encryption techniques**

Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, 2012, **A Secure Image Encryption Algorithm Based on Rubik's Cube Principle** [Online], Available, http://www.hindawi.com/ [2013, August 2]

Jeremy Kun, 2012, **The Cellular Automaton Method for Cave Generation** [Online], Available, http: //www.jeremykun.com [2013, October 23]

Marina Jeaneth Machicao, Anderson G. Marco, Odemir M. Bruno, 2011, **Chaotic Encryption Method Based on Life-Like Cellular Automata**

Maryam Habibipour, Mehdi Yaghobi, Saeed Rahati-Q, Zohreh souzanchi-k, 2010, **An Image Encryption System by 2D Memorized Cellular Automata and Chaos Mapping**

Maryam Habibipour, Mehdi Yaghobi, Saeed Rahati-Q, Zohreh souzanchi-k, 2010, **An Image Encryption System by Indefinite Cellular Automata and Chaos**

MathWorld, **Cellular Automaton** [Online], Available, http://mathworld.wolfram.com [2013, July 19]

MathWorld, **Logistic Map** [Online], Available, http://mathworld.wolfram.com [2013, August 16]

LOTUS_ETC, 2009, **CHAOS** [Online], Available, http: //www.vcharkarn.com [2013, July 18]

KEN-ICHI MAEDA, AND CHIAKI SAKAMA, 2007, **Identifying Cellular Automata Rules**

N.K. Pareek, Vinod Patidar, K.K. Sud, 2006, **Image encryption using chaotic logistic map**

Rong-Jian Chen, Yuan-Hsin Chen, Chao-Shen Chen, and Jui-Lin Lai, 2006, **Image Encryption/Decryption System Using 2-D Cellular Automata**

G. Alvarez, A. Hernandez, L. Hernandezl, A. Marin, and G. Rodriguez4, 2005, **A new graphic cryptosystem based on one-dimen**

ภาคผนวก

ภาคผนวก ก

คำสั่งโปรแกรม MATLAB

(ส่วนการเข้ารหัสลับและถอดรหัสลับภาพดิจิทัล)

```
%%%%%%%%%%%%%%%%%%%%% Import image part %%%%%%%%%%%%%%%%%%%%%%%%%%%%%
Pic = imread ('lena.jpg');
siz = size(Pic);

pic11 = (Pic(:,:,1));
pic12 = (Pic(:,:,2));
pic13 = (Pic(:,:,3));

imgDouble1 = double(dec2bin(reshape(pic11,[],1)))-48;
imgDouble2 = double(dec2bin(reshape(pic12,[],1)))-48;
imgDouble3 = double(dec2bin(reshape(pic13,[],1)))-48;

%%%%%%%%%%%%%%%%% Generate binary chaos part %%%%%%%%%%%%%%%%%%%%%%%%%
N = siz(1);
                                M = siz(2);
initialstate1 = zeros(1,N*M*8);
initialstate2 = zeros(1,N*M*8);
initialstate3 = zeros(1,N*M*8);

r = 1.9999;
initialstate1(1) = 0.05;
initialstate2(1) = 0.3;
initialstate3(1) = 0.02;

for i=1:(N*M*8)-1
    initialstate1(i+1) = abs( r*initialstate1(i) - 1);
    initialstate2(i+1) = abs( r*initialstate2(i) - 1);
    initialstate3(i+1) = abs( r*initialstate3(i) - 1);

    if initialstate1(i) < 0.5
        initialstate1(i) = 0;
    else
        initialstate1(i) = 1;
    end
    if initialstate2(i) < 0.5
        initialstate2(i) = 0;
    else
        initialstate2(i) = 1;
    end
     if initialstate3(i) < 0.5
        initialstate3(i) = 0;
    else
        initialstate3(i) = 1;
    end
end

if initialstate1(1) < 0.5
        initialstate1(1) = 0;
    else
        initialstate1(1) = 1;
 end
 if initialstate2(1) < 0.5
        initialstate2(1) = 0;
  else
        initialstate2(1) = 1;
 end
 if initialstate3(1) < 0.5
```

```
        initialstate3(1) = 0;
    else
        initialstate3(1) = 1;
end

 initialstate1 = reshape(initialstate1,N*M,8);
 initialstate2 = reshape(initialstate2,N*M,8);
 initialstate3 = reshape(initialstate3,N*M,8);

%%%%%%%%%%%%%%%%% Generate binary CA part %%%%%%%%%%%%%%%%%%%%%%%%%
S1=wolframfx(30);
S2=wolframfx(45);
S3=wolframfx(135);
cut1 = S1(386:785,777:1288);
cut2 = S1(486:885,800:1311);
cut3 = S1(486:885,850:1361);
cut4 = S1(470:869,850:1361);
cut5 = S1(486:885,770:1281);
cut6 = S1(386:785,780:1291);
cut7 = S1(400:799,789:1300);
cut = [cut1 cut2 cut3 cut4 cut5; cut4 cut5 cut6 cut7 cut1; cut7 cut1
cut3 cut5 cut6; cut2 cut4 cut6 cut1 cut3; cut3 cut5 cut7 cut6 cut4];
p1 = reshape(cut(1:M*2,1:N*4),[],8);

cut1 = S2(388:787,780:1291);
cut2 = S2(488:887,780:1291);
cut3 = S2(488:887,777:1288);
cut4 = S2(480:879,777:1288);
cut5 = S2(488:887,780:1291);
cut6 = S2(488:887,777:1288);
cut7 = S2(388:787,780:1291);
cut = [cut1 cut2 cut3 cut4 cut5; cut4 cut5 cut6 cut7 cut1; cut7 cut1
cut3 cut5 cut6; cut2 cut4 cut6 cut1 cut3; cut3 cut5 cut7 cut6 cut4];
p2 = reshape(cut(1:M*2,1:N*4),[],8);
cut1 = S3(388:787,780:1291);
cut2 = S3(400:799,790:1301);
cut3 = S3(450:849,790:1301);
cut4 = S3(500:899,799:1310);
cut5 = S3(400:799,790:1301);
cut6 = S3(450:849,790:1301);
cut7 = S3(388:787,780:1291);
cut = [cut1 cut2 cut3 cut4 cut5; cut4 cut5 cut6 cut7 cut1; cut7 cut1
cut3 cut5 cut6; cut2 cut4 cut6 cut1 cut3; cut3 cut5 cut7 cut6 cut4];
p3 = reshape(cut(1:M*2,1:N*4),[],8);

%%%%%%%%%%%%%%%%%%%% Exclusive-OR encryption part %%%%%%%%%%%%%%%%%%
chiper1  =  xor(imgDouble1,initialstate1);
chiper2  =  xor(imgDouble2,initialstate2);
chiper3  =  xor(imgDouble3,initialstate3);

chiper11 =  xor(chiper1,p1);
chiper21 =  xor(chiper2,p2);
chiper31 =  xor(chiper3,p3);
```

```
%%%%%%%%%%%%%%%%%% Exclusive-OR decryption part %%%%%%%%%%%%%%%%%%%%%
chiper1  =  xor(imgDouble1,p1);
chiper2  =  xor(imgDouble2,p2);
chiper3  =  xor(imgDouble3,p3);

chiper11 =  xor(chiper1,initialstate1);
chiper21 =  xor(chiper2,initialstate2);
chiper31 =  xor(chiper3,initialstate3);

%%%%%%%%%%%%%%%% Convert binary data to image part %%%%%%%%%%%%%%%%%%%
chiper12 = reshape(bin2dec(num2str(chiper11)),N,M);
chiper22 = reshape(bin2dec(num2str(chiper21)),N,M);
chiper32 = reshape(bin2dec(num2str(chiper31)),N,M);

enc = zeros(N,M,3);
enc(:,:,1) = chiper12;
enc(:,:,2) = chiper22;
enc(:,:,3) = chiper32;
encrypted=uint8(enc);
```

ภาคผนวก ข

คำสั่งโปรแกรม MATLAB

(ส่วนการเข้ารหัสลับและถอดรหัสลับข้อมูล)

```
%%%%%%%%%%%%%%%%%%%%%%%% Import file function %%%%%%%%%%%%%%%%%%%%%%%%
function data = importfile(workbookFile, sheetName, range)
%IMPORTFILE Import numeric data from a spreadsheet
%   DATA = IMPORTFILE(FILE) reads all numeric data from the first
worksheet
%   in the Microsoft Excel spreadsheet file named FILE and returns
the
%   numeric data.
%
%   DATA = IMPORTFILE(FILE,SHEET) reads from the specified worksheet.
%
%   DATA = IMPORTFILE(FILE,SHEET,RANGE) reads from the specified
worksheet
%   and from the specified RANGE. Specify RANGE using the syntax
%   'C1:C2',where C1 and C2 are opposing corners of the region.%
% Example:
%   untitled = importfile('Data.xlsx','data7-1-14','A1:C5');
%
%   See also XLSREAD.

% Auto-generated by MATLAB on 2014/01/10 14:47:36

%% Input handling

% If no sheet is specified, read first sheet
if nargin == 1 || isempty(sheetName)
    sheetName = 1;
end

% If no range is specified, read all data
if nargin <= 2 || isempty(range)
    range = '';
end

%% Import the data
[~, ~, data] = xlsread(workbookFile, sheetName, range);
data(cellfun(@(x) ~isempty(x) && isnumeric(x) && isnan(x),data)) =
{''};
end


%%%%%%%%%%%%%%%%%%%%%%%% Import file part %%%%%%%%%%%%%%%%%%%%%%%%
%% For Text File %%
a = importdata('C:\Users\SILVERMOON\Google
Drive\MATLAB_CODE\myCode\quote.txt');

%% For Excel File %%
a = importfile('C:\Users\SILVERMOON\Google
Drive\MATLAB_CODE\myCode\test1.xlsx',1);

%%%%%%%%%%%%%%%%%%          Generate          binary          chaos
part %%%%%%%%%%%%%%%%%%%%%%%%
r = 1.9999;
initialstate1(1) = 0.05;

for i=1:(N*M*7)-1
```

```
    initialstate1(i+1) = abs( r*initialstate1(i) - 1);

    if initialstate1(i) < 0.5
        initialstate1(i) = 0;
    else
        initialstate1(i) = 1;
    end
end

if initialstate1(1) < 0.5
        initialstate1(1) = 0;
    else
        initialstate1(1) = 1;
 end

%%%%%%%%%%%%%%%% Generate binary CA part %%%%%%%%%%%%%%%%%%%%%%%%
S1=wolframfx(30);
  CA = reshape([S1(391:705,895:1139) S1(405:719,926:1170)],[],7);

%%%%%%%%%%%%%%%% Data encryption part %%%%%%%%%%%%%%%%%%%%%%%%%%%
  k=0;
for i = 1:sizeA(1)
    for j = 1:sizeA(2)
        if ischar(a{i,j}) ~= 0
           b = double(dec2bin(a{i,j}'))-48;
        else
           b = double(dec2bin(num2str(a{i,j})'))-48;
        end
       clear size
       s = size(b);
       l = length(b);
       if l ~= 0
           x = s(1,1);
           y = s(1,2);
       else
           x = 0;
           y = 0;
       end
       chaos = initialstate1(1+k:x+k,1:y);
       Cell = CA(1+k:x+k,1:y);
       k= k+x;

       if isempty(b) ~=  1
         %%% XOR Part %%%
        chiper1  =  xor(b,chaos);
        chiper11 =  xor(chiper1,Cell);
        data{i,j} = char(bin2dec(num2str(chiper11))');
       else
        data{i,j} = char(bin2dec(num2str(b))');
       end
    end
end


%%%%%%%%%%%%%%%% Data decryption part %%%%%%%%%%%%%%%%%%%%%%%%%%%
k=0;
for i = 1:sizeA(1)
```

```
    for j = 1:sizeA(2)
        if ischar(a{i,j}) ~= 0
           b = double(dec2bin(a{i,j}'))-48;
        else
           b = double(dec2bin(num2str(a{i,j})'))-48;
        end
       clear size
       s = size(b);
       l = length(b);
       if l ~= 0
           x = s(1,1);
           y = s(1,2);
       else
           x = 0;
           y = 0;
       end
       chaos = initialstate1(1+k:x+k,1:y);
       Cell = CA(1+k:x+k,1:y);
       k= k+x;

       if isempty(b) ~=  1
         %%% XOR Part %%%
        chiper1  =  xor(b,Cell);
        chiper11 =  xor(chiper1,chaos);
        data1{i,j} = char(bin2dec(num2str(chiper11))');
       else
        data1{i,j} = char(bin2dec(num2str(b))');
       end
    end
end
```