การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้

ADAPTIVE PIXEL-SELECTION FRACTIONAL CHAOTIC MAP LATTICES FOR IMAGE CRYPTOGRAPHY

จิระศักดิ์ สิทธิกร
JIRASAK SITTIGORN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2559
KMITL-2016-EN-D-018-013

การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้

ADAPTIVE PIXEL-SELECTION FRACTIONAL CHAOTIC MAP LATTICES FOR IMAGE CRYPTOGRAPHY

จิระศักดิ์ สิทธิกร
JIRASAK SITTIGORN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2559
KMITL-2016-EN-D-018-013

ADAPTIVE PIXEL-SELECTION FRACTIONAL CHAOTIC MAP LATTICES FOR IMAGE CRYPTOGRAPHY

JIRASAK SITTIGORN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
DOCTOR OF ENGINEERING IN ELECTRICAL ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2016

KMITL-2016-EN-D-018-013

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้

Thesis Title Adaptive Pixel-Selection Fractional Chaotic Map Lattices for Image Cryptography

นักศึกษา นายจิระศักดิ์ สิทธิกร

รหัสประจำตัว 52610103

ปริญญา วิศวกรรมศาสตรดุษฎีบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.อรฉัตร จิตต์โสภักตร์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ (ร่วม) รศ.ดร.กิตติ ไพฑูรย์วัฒนกิจ

อาจารย์ที่ปรึกษาวิทยานิพนธ์ (ร่วม) รศ.ดร.จเร สุรวัฒน์ปัญญา

หมายเลขวิทยานิพนธ์ KMITL-2016-EN-D-018-013

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.สุรพันธุ์	เอื้อไพบูลย์	
ผศ.ดร.ยุทธนา	คิดใจเดียว	
ศ.ดร.โกสินทร์	จำนงไทย	
รศ.ดร.เกียรติกูล	เจียรนัยธนะกิจ	
รศ.ดร.อรฉัตร	จิตต์โสภักตร์	

วัน / เดือน/ ปี ที่สอบ วันพฤหัสบดีที่ 3 ธันวาคม พ.ศ. 2558 เวลา 09.00-11.00 น.
สถานที่สอบ ณ อาคาร A ชั้น 5 ห้องประชุม 4

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 3 ธันวาคม พ.ศ. 2558

หัวข้อวิทยานิพนธ์	การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้
นักศึกษา	นายจิระศักดิ์ สิทธิกร
รหัสประจำตัว	52610103
ปริญญา	วิศวกรรมศาสตรดุษฎีบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2558
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ.ดร.อรฉัตร จิตต์โสภักตร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	รศ.ดร.กิตติ ไพฑูรย์วัฒนกิจ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	รศ.ดร.จเร สุรวัฒน์ปัญญา

บทคัดย่อ

งานวิจัยนี้ทำการศึกษาเกี่ยวกับการเข้ารหัสข้อมูลภาพ บนพื้นฐานของทฤษฎีความยุ่งเหยิง (Chaotic Theory) เป็นทฤษฎีที่สามารถนำมาใช้สร้างชุดข้อมูลที่มีลักษณะคล้ายกับเลขสุ่มเทียม ซึ่งถูกนำมาประยุกต์ใช้ในการเข้ารหัสข้อมูล (Cryptography) โครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (Chaotic Map Lattices) เป็นหนึ่งในกระบวนการเข้ารหัส และถอดรหัสภาพ ที่ใช้ค่าพารามิเตอร์ (Parameters) ลำดับการวนซ้ำ (Number of Iterations) และ จำนวนรอบในกระบวนการเข้ารหัส (Number of Cycles) เป็นกุญแจลับ (Secret Keys) ในการเข้ารหัสข้อมูลภาพ ซึ่งจำนวนและความหลากหลายของของกุญแจลับที่ใช้นั้นมีผลต่อความปลอดภัย

วิทยานิพนธ์นี้นำเสนอกระบวนการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (Adaptive Pixel-selection Fractional Chaotic Map Lattices for Image Cryptography) ซึ่งเป็นการปรับปรุงกระบวนการเข้ารหัสภาพเพื่อเพิ่มความปลอดภัย โดยใช้พลวัตเชิงเศษส่วนของความยุ่งเหยิง (Fractional Chaotic) ซึ่งมีลำดับการอนุพันธ์ที่เป็นเศษส่วน (Fractional-Order) เป็นกุญแจลับตัวใหม่ โดยจะทำให้เกิดความเป็นพลวัตความยุ่งเหยิงใหม่ในช่วงของค่าพารามิเตอร์ที่แตกต่างกัน นอกจากนั้นยังเพิ่มกระบวนการสลับลำดับการเข้ารหัสจุดภาพโดยใช้พลวัตความยุ่งเหยิงอีกชุดในการกำหนดลำดับ ทำให้เกิดประสิทธิผลการเข้ารหัสข้อมูลภาพเพิ่มขึ้น ซึ่งได้ทำการทดสอบประสิทธิผลของการเข้ารหัสภาพด้วย การวิเคราะห์ผลการเข้ารหัสภาพ การวิเคราะห์ฮิสโตแกรม (Histogram Analysis) การวิเคราะห์ข้อมูลเอนโทรปี (Information Entropy Analysis) การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์ (Correlation Coefficient Analysis) การวิเคราะห์ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ (Cross-correlation Coefficient Analysis) ค่าเฉลี่ยการเปลี่ยนระดับสีเทา (Gray Modification Average Value) และ การวิเคราะห์ขนาดของกุญแจลับ (Key Space Analysis)

Thesis	Adaptive Pixel-Selection Fractional Chaotic Map Lattices for Image Cryptography
Student	Mr. Jirasak Sittigorn
Student ID.	52610103
Degree	Doctor of Engineering
Program	Electrical Engineering
Year	2015
Thesis Advisor	Assoc.Prof.Dr.Orachat Chitsobhuk
Thesis Co-Advisor	Assoc.Prof.Dr.Kitti Paithoonwattanakij
Thesis Co-Advisor	Assoc.Prof.Dr.Charray Surawatpunya

ABSTRACT

Chaotic theory has been employed in cryptography application for establishing a sequence of data closest to pseudorandom number. Image cryptography with Chaotic Map Lattices (CML) uses the chaos parameters, the number of iterations and the number of cycles for encryption as secret keys. Amount of secret keys has a great impact on security in cryptography.

Adaptive Pixel-Selection Fractional Chaotic Map Lattices (APFCML) enhances the encryption security by introducing a novel non-integer fractional order concept as secret keys. Fractional chaos is modified chaos with a fractional differential equation containing derivatives of non-integer order. A non-integer order has an effect on the range of chaos's parameter. Moreover, the encryption sequence has been adaptively selected based on another chaos generator. In the experiments, the measurement indices of originality preservation, visual inspection, histogram analysis, entropy analysis, correlation coefficient analysis, cross-correlation coefficient analysis, gray modification average value and key space analysis are used to evaluate the performance.

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา รศ.ดร.อรฉัตร จิตต์โสภักตร์ รศ.ดร.กิตติ ไพฑูรย์วัฒนกิจ และ รศ.ดร.จเร สุรวัฒน์ปัญญา ที่ให้ความช่วยเหลือ ให้คำชี้แนะในการแก้ปัญหา ตลอดจนให้ความรู้และประการณ์ที่ดีแก่ข้าพเจ้า

ขอขอบคุณ รศ.ดร.เกียรติกูล เจียรนัยธนะกิจ ที่ให้คำแนะนำ และแง่มุมที่เป็นประโยชน์ในการทำวิจัย

สำหรับคุณงามความดีอันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดามารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

จิระศักดิ์ สิทธิกร

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญตาราง (ต่อ)

ตารางที่ หน้า

สารบัญภาพ

สารบัญภาพ (ต่อ)

ภาพที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันการติดต่อสื่อสารผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นที่นิยมมากขึ้น ทั้งการใช้งานในชีวิตประจำวัน การประกอบธุรกิจต่าง ๆ จนถึงเรื่องที่มีความสำคัญมาก เช่น การทำธุรกรรมทางการเงินบนระบบอิเล็กทรอนิกส์ และการสื่อสารที่เกี่ยวข้องกับความมั่นคงทางทหาร ทำให้ความปลอดภัยในการสื่อสารเป็นสิ่งที่มีความสำคัญอย่างมาก [1-2]

วิธีหนึ่งในการทำให้เกิดความปลอดภัยในการสื่อสาร คือ การรักษาความลับของข้อมูล โดยการเข้ารหัสข้อมูล (Cryptography) ซึ่งจะทำการ ซ่อนข้อมูล หรือเปลี่ยนข้อมูล ที่ต้องการสื่อสารไว้ [3] ประกอบด้วย กระบวนการเข้ารหัสข้อมูล (Encryption Algorithm) และกระบวนการถอดรหัสข้อมูล (Decryption Algorithm) โดยอาศัยกุญแจ (Key) ในการเข้ารหัส และถอดรหัส ซึ่งแบ่งออกเป็น 2 ประเภทใหญ่ ๆ คือ กระบวนการเข้ารหัสแบบสมมาตร (Symmetric Key Algorithms) และกระบวนการเข้ารหัสแบบอสมมาตร (Asymmetric Key Algorithms)

การใช้พลวัตความยุ่งเหยิงในการสื่อสาร มีทั้งในระบบที่มีความต่อเนื่อง (Continuous Systems) และระบบที่มีความไม่ต่อเนื่อง (Discrete Systems) ในช่วงเริ่มแรกมักใช้ในระบบที่มีความต่อเนื่อง เพื่อใช้ประโยชน์จากการทำให้เป็นจังหวะเดียวกัน (Synchronization) ของเคออส [4-8] แต่จากการศึกษาที่ผ่านมาในการทำให้เป็นจังหวะเดียวกันมีผลทำให้ภายในระบบการสื่อสารมีประสิทธิภาพที่ต่ำลง เนื่องจากทำให้เกิดความไม่ปลอดภัย [9-11] และเกิดความล่าช้าในการทำให้เป็นจังหวะเดียวกันของค่าพารามิเตอร์ [12] จึงเริ่มมีการใช้งานพลวัตความยุ่งเหยิง ในระบบที่มีความไม่ต่อเนื่องมากขึ้น โดยพลวัตความยุ่งเหยิง (Chaotic System) จะขึ้นอยู่กับ ค่าเงื่อนไขตั้งต้น (Initial Conditions) และ ค่าพารามิเตอร์ (Parameters) ซึ่งมีความไวต่อการเปลี่ยนอย่างมาก คือ เมื่อมีการเปลี่ยนค่าเงื่อนไขตั้งต้น หรือ ค่าพารามิเตอร์ เพียงเล็กน้อยจะทำให้ระบบเปลี่ยนแปลงไปอย่างมหาศาล ซึ่งพลวัตความยุ่งเหยิงนี้ถูกนำมาประยุกย์ใช้ในกระบวนการเข้ารหัสแบบสมมาตร [4-7,13,14] โดยใช้ ค่าเงื่อนไขตั้งต้น และ ค่าพารามิเตอร์ เป็นกุญแจหลักในการเข้า และถอดรหัส ซึ่งทำให้พลวัตความยุ่งเหยิงยากต่อการโจมตีด้วยพจนานุกรม (Dictionary Attack)

กระบวนการเข้ารหัสลับด้วยพลวัตความยุ่งเหยิงสำหรับระบบที่มีความไม่ต่อเนื่อง ซึ่งเป็นที่นิยมวิธีหนึ่งได้แก่ เคออสทิคแมพ (Chaotic Map) โดยการสร้างเลขสุ่มเทียม (Pseudo Random Number Generator) เป็นชุดเลขฐานสองที่ใช้สำหรับการเข้ารหัสลับข้อความปกติ (Plain Text) เพื่อเปลี่ยนเป็นข้อความรหัส (Cipher Text) [13,15-19] โดยใช้ค่าการกำหนดเงื่อนไขเริ่มต้น และค่าพารามิเตอร์ เป็นกุญแจลับ (Secret Keys) ในกระบวนการสร้างกลุ่มข้อมูลที่ใช้ในการเข้ารหัส

ข้อความ แต่ไม่สามารถนำไปใช้ในการเข้ารหัสภาพได้ เนื่องจากข้อมูลภาพมีลักษณะเป็น 2 มิติ Kaneko ได้นำเสนอโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (Chaotic Map Lattices : CML) [20] ซึ่งเป็นแบบจำลองพื้นฐานที่นำประโยชน์ของความเป็นพลวัตในระบบไม่เป็นเชิงเส้น (Nonlinear System) มาใช้ในเชิงวิทยาศาสตร์ และวิศวกรรมศาสตร์ และได้มีการนำโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิงมาใช้ในการเข้ารหัสข้อมูลที่มีความต่อเนื่อง [12,21] Wang และผู้ร่วมวิจัยอื่น [22] พบว่าการสื่อสารโดยใช้วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิงมีความปลอดภัยมากกว่าการติดต่อสื่อสารโดยใช้เคออสทิคแมพเดี่ยว (Single Map) เนื่องจากพลวัตความยุ่งเหยิงที่ไม่ต่อเนื่องจะสร้างชุดข้อมูลส่วนที่เป็นคาบขึ้นมาในบางช่วงทำให้สามารถใช้คอมพิวเตอร์มาคาดเดาผลได้

โครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) เป็นกระบวนการเข้ารหัสข้อมูลโดยอาศัยทฤษฎีความยุ่งเหยิง [23] ซึ่งหากไม่มีกุญแจที่ถูกต้องก็ไม่สามารถถอดรหัสออกมาได้ ซึ่งโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง ใช้ค่าพารามิเตอร์ระบบ ลำดับการวนซ้ำ (Number of Iterations) และ จำนวนรอบในกระบวนการเข้ารหัส (Number of Cycles) เป็นกุญแจในการเข้าและถอดรหัสภาพ ซึ่งมีข้อจำกัดที่จำนวนกุญแจ โดยใช้กุญแจเพียง 3 ชนิดตามที่กล่าวมา และมีความยาวของกุญแจจำกัด หรือมีค่ากุญแจที่ใช้ได้อย่างจำกัด เช่น ค่าพารามิเตอร์ระบบซึ่งใช้ลอจิสติกแมพ (Logistic Map) จะเกิดความยุ่งเหยิงที่นำมาใช้งานได้ในช่วง $3.57 < r < 4$ งานวิจัยนี้ได้ประยุกต์การนำรูปแบบลอจิสติกที่ลำดับมีค่าเป็นเศษส่วน (Fractional-Order Logistic Model) ซึ่งเป็นพลวัตเชิงเศษส่วนของความยุ่งเหยิง (Fractional Chaotic) มาใช้แทนลอจิสติกแมพ เนื่องจากพลวัตเชิงเศษส่วนของความยุ่งเหยิงมีความซับซ้อนมากกว่าพลวัตของความยุ่งเหยิงทั่วไป [24] เพราะมีตัวแปรที่ใช้ควบคุม หรือพิจารณาการเปลี่ยนแปลงภายระบบพลวัตเพิ่มขึ้น ด้วยการนำโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิงมาใช้นี้ ทำให้ระบบที่นำเสนอมีกุญแจเพิ่มขึ้นได้แก่ ลำดับการอนุพันธ์ที่เป็นเศษส่วน (Fractional-Order) ซึ่งค่าลำดับการอนุพันธ์ที่เป็นเศษส่วนแต่ละค่าจะทำให้เกิดความยุ่งเหยิงในแต่ละช่วงค่าพารามิเตอร์ที่แตกต่างกัน และเมื่อใช้กุญแจสองตัวนี้ผสานกัน สามารถทำให้มีค่ากุญแจที่ใช้งานเพิ่มขึ้นอย่างมหาศาล นอกจากนี้งานวิจัยนี้ยังทำการปรับกระบวนการในการเข้ารหัสภาพ จากที่มีการเข้ารหัสตามลำดับจุดภาพเป็นการเข้ารหัสตามลำดับที่กำหนดโดยใช้พลวัตของความยุ่งเหยิงอีกชุดหนึ่ง ซึ่งทำให้มีจำนวนกุญแจที่ใช้เข้ารหัสเพิ่มขึ้น และยากต่อการถอดรหัสเนื่องจากลำดับในการเข้ารหัสมีการเปลี่ยนแปลงไป

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วิทยานิพนธ์นี้ได้ศึกษา การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และได้ปรับปรุงส่วนที่เป็นข้อจำกัดในการเข้ารหัสภาพ [25] และ พัฒนาให้มีความปลอดภัยมากยิ่งขึ้น ทั้งในด้านของการเพิ่มจำนวนกุญแจ และประสิทธิผลของการเข้ารหัสที่ดีกว่า โดยภายในวิทยานิพนธ์นี้ได้กล่าวถึงการทำงานของการเข้ารหัส และถอดรหัสภาพ 3 รูปแบบ ได้แก่

1.2.1 การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (Chaotic Map Lattices for Image Cryptography)

โครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) เป็นกระบวนการเข้ารหัส และถอดรหัสภาพ ที่ผู้วิจัยได้ศึกษาการทำงาน และนำมาเป็นต้นแบบในการพัฒนาในงานวิจัย โดยโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ใช้ลอจิสติกแมพเป็นพลวัตของความยุ่งเหยิง ซึ่งใช้กุญแจในการเข้ารหัส 3 ชนิด ได้แก่ ค่าพารามิเตอร์ ลำดับการวนซ้ำ และจำนวนรอบในกระบวนการเข้ารหัส โดยกุญแจที่ใช้งานมีความยาวของกุญแจจำกัดโดยเฉพาะค่าพารามิเตอร์ ในงานวิจัยนี้ได้เปลี่ยนพลวัตของความยุ่งเหยิงที่ใช้งานทำให้มีกุญแจที่ใช้งานเพิ่มขึ้นและความยาวของกุญแจเพิ่มขึ้น ทั้งยังได้ปรับปรุงส่วนของสมการ โดยทำการเปลี่ยนค่าในเงื่อนไขการใช้งานพลวัตของความยุ่งเหยิงที่นำมาใช้ เพื่อแก้ปัญหาในส่วนของถอดรหัสภาพ

1.2.2 การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (Fractional Chaotic Map Lattices for Image Cryptography)

โครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) เป็นกระบวนการเข้ารหัส และถอดรหัสภาพที่พัฒนามาจาก โครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) โดยเปลี่ยนส่วนที่เป็นพลวัตความยุ่งเหยิง จากลอจิสติกแมพ เป็นรูปแบบลอจิสติกลำดับที่เป็นเศษส่วน ทำให้มีกุญแจที่ใช้เข้ารหัสเพิ่มขึ้นมาได้แก่ ลำดับการอนุพันธ์ที่เป็นเศษส่วน ซึ่งค่าลำดับการอนุพันธ์ที่เป็นเศษส่วนแต่ละค่านั้นจะทำให้เกิดความยุ่งเหยิงในแต่ละช่วงค่าพารามิเตอร์ที่แตกต่างกัน เมื่อนำมาใช้งานร่วมกันเป็นผลให้เกิดความหลากหลายของกุญแจขึ้นอย่างมหาศาล

1.2.3 การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (Adaptive Pixel-selection Fractional Chaotic Map Lattices for Image Cryptography) [36]

แม้โครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) จะมีจำนวนกุญแจที่ใช้งานมากกว่า โครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) แต่ยังให้ประสิทธิผลของการเข้ารหัสไม่ต่างกันมากในทุกตัวชี้วัด เนื่องจากมีความเป็นพลวัตความยุ่งเหยิงเหมือนกัน แล้วหลักการเข้ารหัสของวิธีทั้งสองอาศัยข้อมูลของจุดภาพ (Pixels) ที่อยู่ติดกันเป็นลำดับค่าเงื่อนไขตั้งต้นในการเข้ารหัสจุดภาพถัดไป ทำให้ผลการเข้ารหัสไม่ต่างกันมาก

โครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) เป็นกระบวนการเข้ารหัส และถอดรหัสภาพที่พัฒนาจากทั้งสองวิธี โดยการสลับลำดับจุดภาพของการเข้ารหัส ซึ่งลำดับดังกล่าวใช้พลวัตความยุ่งเหยิงอีกตัวในการสร้าง ทำให้มีกุญแจที่ใช้งานเพิ่มขึ้น ทั้งยังให้ประสิทธิผลของการเข้ารหัสที่มากขึ้นด้วย เนื่องจากลำดับในการเข้ารหัสมีการสลับไปมาทำให้ค่าที่เปลี่ยนไปนั้นมีการกระจายตัวมากขึ้น ทั้งการที่มีลำดับที่ไม่แน่นอนยังทำให้ยากในการถอดรหัสมากขึ้น

1.3 ขอบเขตการวิจัย

งานวิจัยได้ทำการศึกษาการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ทำการทดลองนำรูปแบบลอจิสติกลำดับที่เป็นเศษส่วน มาใช้แทนลอจิสติกแมพเป็นการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ ได้นำเสนอการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ซึ่งมีการใช้จำนวนกุญแจลับที่มากกว่า ทั้งยังได้ประสิทธิผลของการเข้ารหัสที่ดีกว่า โดยภายในวิทยานิพนธ์ได้ทำการทดสอบประสิทธิผลของการเข้ารหัสภาพด้วย การวิเคราะห์ผลการเข้ารหัสภาพ การวิเคราะห์ฮิสโตแกรม (Histogram Analysis) การวิเคราะห์ข้อมูลเอนโทรปี (Information Entropy) [27] การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์ (Correlation Coefficient Analysis) การวิเคราะห์ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ (Cross-correlation Coefficient Analysis) [28-29] ค่าเฉลี่ยการเปลี่ยนระดับสีเทา (Gray Modification Average Value) [30] และ การวิเคราะห์ขนาดของกุญแจลับ (Key Space Analysis) [31]

1.4 การดำเนินการวิจัย

ในการวิจัยได้ศึกษา การเข้ารหัสถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ปรับปรุงส่วนที่เป็นข้อจำกัด และทำการทดลองเปรียบเทียบกับการเข้ารหัสถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และการเข้ารหัสถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (AFCML) โดยทดสอบประสิทธิผลของการเข้ารหัสด้วย การเข้ารหัสภาพ การวิเคราะห์ฮิสโตแกรม การวิเคราะห์ข้อมูลเอนโทรปี การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์ การวิเคราะห์ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ ค่าเฉลี่ยการเปลี่ยนระดับสีเทา และ การวิเคราะห์ขนาดของกุญแจลับ

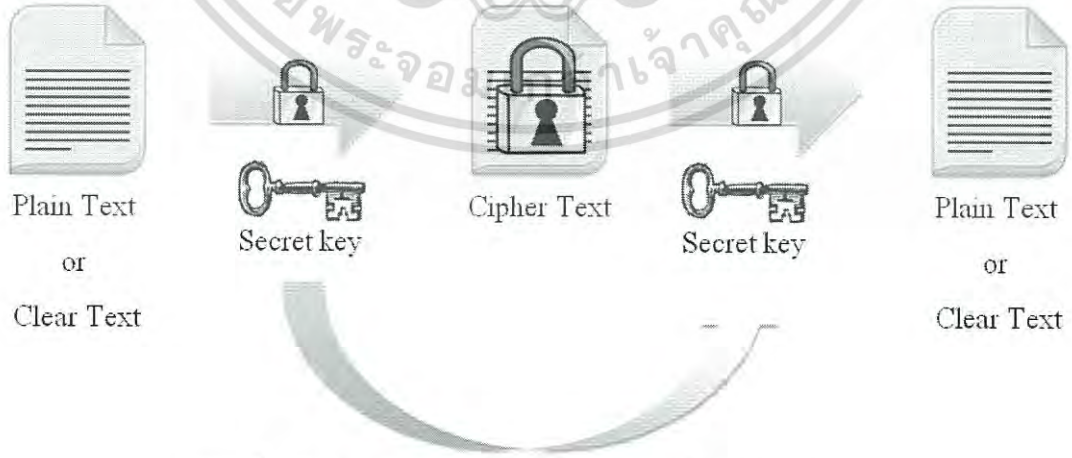
บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูล เป็นการนำทฤษฎีทางคณิตศาสตร์ มาใช้เปลี่ยนข้อมูลที่ต้องการสื่อสาร หรือ เปลี่ยนข้อความปกติ เป็นข้อความรหัส ที่ถูกทำการเข้ารหัส หรือข้อความที่ไม่สามารถอ่านได้ โดยผ่านกระบวนการต่าง ๆ ด้วยกุญแจ เพื่อป้องกันไม่ให้ผู้ที่ไม่มีกุญแจ หรือไม่มีสิทธิ์ สามารถนำข้อมูลไปใช้งานได้ และเมื่อข้อมูลลับที่ผ่านการเข้ารหัสส่งถึงผู้รับ ผู้รับที่มีกุญแจที่ถูกต้องเท่านั้น สามารถเปลี่ยนข้อมูลลับกลับเป็นข้อมูลต้นฉบับที่ผู้ส่งต้องการสื่อสารได้ โดยทั่วไปเรียกกระบวนการเปลี่ยนข้อความปกติเป็นข้อความรหัสด้วยกุญแจว่า การเข้ารหัสข้อมูล และเรียกกระบวนการเปลี่ยนข้อความรหัสที่ไม่สามารถอ่านได้กลับเป็นข้อความปกติว่า การถอดรหัสข้อมูล [13] กระบวนการเข้ารหัสข้อมูลแบ่งออกเป็น 2 ประเภทใหญ่ ๆ ตามลักษณะของกุญแจ ได้แก่

2.1.1 กระบวนการเข้ารหัสแบบสมมาตร

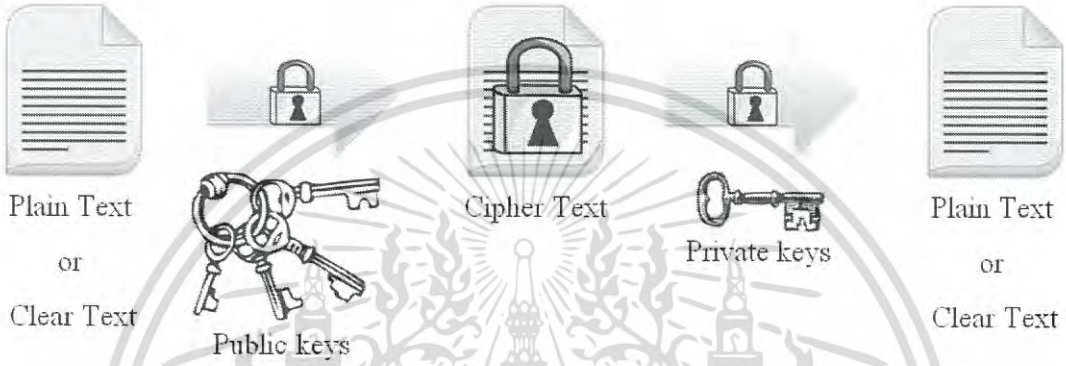
กระบวนการเข้ารหัสแบบสมมาตรจะใช้กุญแจเพียง 1 ชุด ในการเข้ารหัสข้อมูล และการถอดรหัสข้อมูล ซึ่งเป็นกุญแจเดียวกันดัง ภาพที่ 2.1 เรียกว่า กุญแจลับ (Secret Key) แบ่งการเข้ารหัสได้เป็น 2 ลักษณะย่อ คือ แบบบล็อค (Block Algorithms) ซึ่งจะทำการเข้ารหัสทีละบล็อค (1 บล็อคประกอบด้วยหลายไบต์) และแบบสตรีม (Stream Algorithms) ซึ่งจะทำการเข้ารหัสทีละไบต์



ภาพที่ 2.1 กระบวนการเข้ารหัส-ถอดรหัสแบบสมมาตร

2.1.2 กระบวนการเข้ารหัสแบบอสมมาตร

กระบวนการเข้ารหัสนี้จะใช้กุญแจ 2 ชุด โดยใช้กุญแจสาธารณะ (Public Keys) ในการเข้ารหัส และใช้กุญแจกอีกชุดที่เรียกว่า กุญแจส่วนตัว (Private Keys) ในการถอดรหัสข้อมูล ในทางปฏิบัติจะให้กุญแจสาธารณะกับผู้ที่ต้องการจะส่งข้อมูลให้ แล้วเก็บกุญแจส่วนตัวซึ่งต่างกันไว้สำหรับเปิดข้อมูลนั้น โดยจะไม่เปิดเผยกุญแจส่วนตัวกับผู้อื่นให้ทราบ ดังภาพที่ 2.2



ภาพที่ 2.2 กระบวนการเข้ารหัส-ถอดรหัสแบบอสมมาตร

สำหรับข้อดี และข้อด้อยของกระบวนการเข้ารหัสแบบสมมาตร และ กระบวนการเข้ารหัสแบบอสมมาตร สามารถสรุปดังตารางที่ 2.1

ตารางที่ 2.1 ข้อดีและข้อด้อยของ กระบวนการเข้ารหัสแบบสมมาตร และ กระบวนการเข้ารหัสแบบอสมมาตร

	กระบวนการเข้ารหัสแบบสมมาตร	กระบวนการเข้ารหัสแบบอสมมาตร
ข้อดี	ทำงานได้รวดเร็ว ง่ายต่อการใช้งาน	บริหารจัดการกุญแจง่าย สามารถใช้งานร่วมกับลายมือชื่อดิจิตอล (Digital Signature)
ข้อด้อย	ปัญหาในการบริหารจัดการกุญแจลับ	ใช้เวลาในการคำนวณการเข้าและถอดรหัสมาก

2.2 พลวัตความยุ่งเหยิง

ทฤษฎีความยุ่งเหยิง เป็นทฤษฎีที่อธิบายถึงระบบพลวัต โดยมีลักษณะของระบบที่ไม่เป็นเชิงเส้น และมีความยุ่งเหยิงตัวอย่างเช่น การสร้างเลขสุ่มเทียม ที่สร้างชุดข้อมูลให้มีลักษณะคล้ายการสุ่ม แม้ว่าจะมีลักษณะคล้ายความเป็นคาบอยู่ในบางช่วง แต่ก็ไม่ใช่คาบ และไม่สามารถคาดเดาได้ เพราะ

มีความยุ่งเหยิงซ่อนอยู่ภายใน ลักษณะความไม่เป็นเชิงเส้นของพลวัตความยุ่งเหยิง คล้ายการสุ่ม แต่ไม่ใช่การสุ่มจริง และจากการที่สามารถคำนวณค่าที่จะเกิดขึ้นในสถานะลำดับต่าง ๆ ได้แน่นอนทำให้สามารถนำทฤษฎีความยุ่งเหยิงมาใช้เป็นในกระบวนการเข้ารหัส และกระบวนการถอดรหัสได้ โดยการเปลี่ยนแปลงที่เกิดขึ้น ขึ้นอยู่กับค่าเงื่อนไขตั้งต้น และค่าพารามิเตอร์ ซึ่งค่าทั้งสองนี้มีความไวต่อระบบอย่างมาก คือ หากมีการเปลี่ยนแปลงค่าใดค่าหนึ่งในสองค่านี้เพียงเล็กน้อยจะทำให้ระบบเกิดการเปลี่ยนแปลงไปอย่างมหาศาล

ลอจิสติกแมพ เป็นการแปลงพหุนาม (Polynomial Mapping) ของ 2 ระดับขั้น ซึ่งมักใช้ในการหาจำนวนเชิงซ้อน เป็นพื้นฐานของพลวัตความยุ่งเหยิงที่ไม่ต่อเนื่อง สมการลอจิสติกถูกสร้างโดย Pierre François Verhulst [32] สามารถเขียนให้อยู่ในรูปสมการได้ดังสมการที่ 2.1

$$x_{n+1} = rx_n\left(1-x_n\right) \tag{2.1}$$

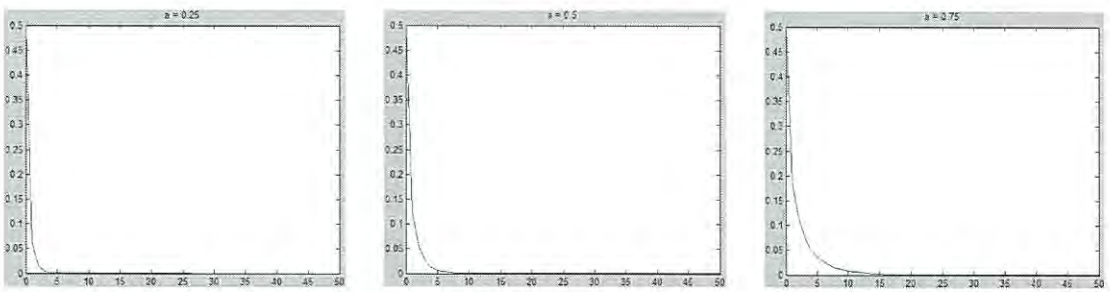
เมื่อ x_n เป็นค่าในระบบที่ลำดับการวนซ้ำที่ n

r เป็นค่าพารามิเตอร์

n เป็นลำดับการวนซ้ำ

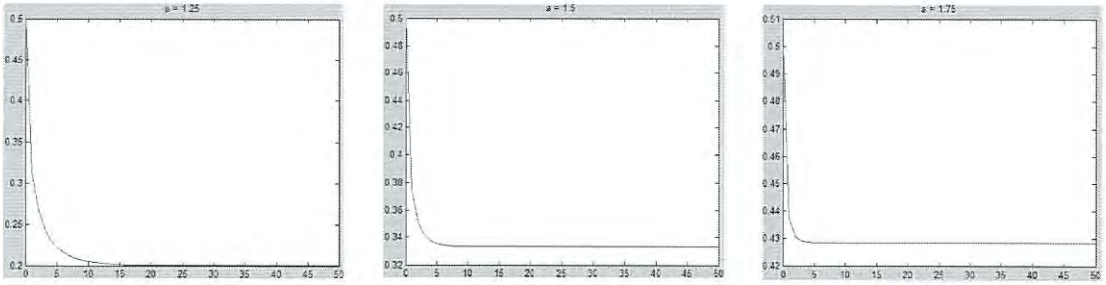
โดยที่การกำหนดค่าเงื่อนไขตั้งต้นในระบบ x_0 จะต้องมีค่าอยู่ในช่วง 0 ถึง 1 และผลลัพธ์ของลอจิสติกแมพ ลำดับต่าง ๆ ที่ได้จะอยู่ในช่วงของค่าต่ำสุด $x_{\min} = \frac{r^2}{4}\left(1-\frac{r}{4}\right)$ และ ค่าสูงสุด $x_{\max} = \frac{r}{4}$ ดังนั้นค่าในระบบที่ลำดับการวนซ้ำที่ 0 (x_0) จึงต้องกำหนดค่าให้ไม่เกินค่าในช่วงที่กำหนดด้วย ส่วนค่าที่เป็นพารามิเตอร์ r จะต้องมีค่าเป็นบวก ซึ่งเป็นตัวที่กำหนดผลกระทบผลลัพธ์ของสมการลอจิสติกแมพ

เมื่อทำการทดสอบโดยกำหนดเงื่อนไขเริ่มต้น $x_0 = 0.5$ และกำหนดค่าพารามิเตอร์ให้มีค่าต่างกัน แล้วแสดงผลจากสมการลอจิสติกแมพจำนวน 51 ลำดับ ได้ผลลัพธ์ดังภาพที่ 2.3 ถึง ภาพที่ 2.8



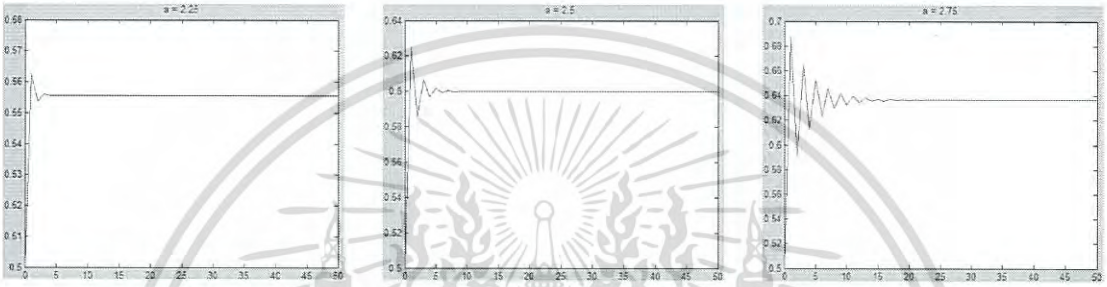
ก) $r = 0.25$ ข) $r = 0.5$ ค) $r = 0.75$

ภาพที่ 2.3 ผลของสมการลอจิสติกแมพ จำนวน 51 ลำดับ เมื่อใช้ค่าพารามิเตอร์ $0 < r < 1$



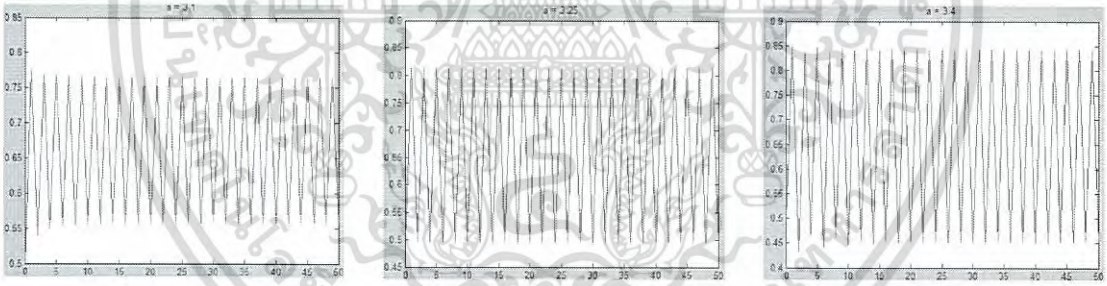
ก) $r = 1.25$ ข) $r = 1.5$ ค) $r = 1.75$

ภาพที่ 2.4 ผลของสมการลอจิสติกแมพ จำนวน 51 ลำดับ เมื่อใช้ค่าพารามิเตอร์ $1 < r < 2$



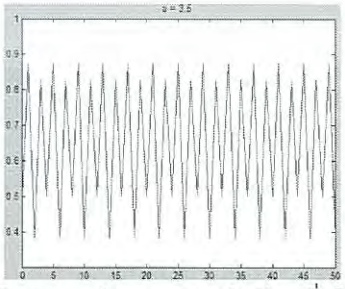
ก) $r = 2.25$ ข) $r = 2.5$ ค) $r = 2.75$

ภาพที่ 2.5 ผลของสมการลอจิสติกแมพ จำนวน 51 ลำดับ เมื่อใช้ค่าพารามิเตอร์ $2 < r < 3$

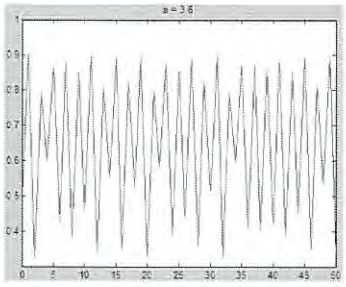


ก) $r = 3.1$ ข) $r = 3.25$ ค) $r = 3.45$

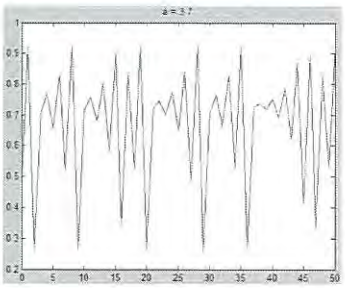
ภาพที่ 2.6 ผลของสมการลอจิสติกแมพ จำนวน 51 ลำดับ เมื่อใช้ค่าพารามิเตอร์ $3 < r < 1 + \sqrt{6}$



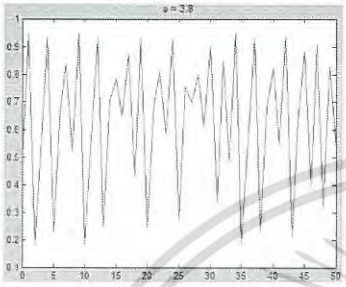
ภาพที่ 2.7 ผลของสมการลอจิสติกแมพ จำนวน 51 ลำดับ เมื่อใช้ค่าพารามิเตอร์ $r = 3.5$



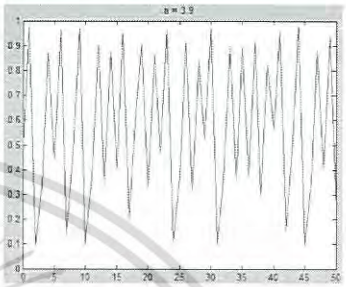
ก) $r = 3.6$



ข) $r = 3.7$



ค) $r = 3.8$



ง) $r = 3.9$

ภาพที่ 2.8 ผลของสมการลอจิสติกแมพ จำนวน 51 ลำดับ เมื่อใช้ค่าพารามิเตอร์ $3.57 < r < 4$

ผลจากการกำหนดค่าพารามิเตอร์ต่าง ๆ ในสมการลอจิสติกแมพ จะเป็นตัวกำหนดผลลัพธ์ในลำดับการวนซ้ำต่าง ๆ

จากภาพที่ 2.3 ก) เมื่อกำหนดค่าพารามิเตอร์ r เป็น 0.25 ค่าที่ลำดับการวนซ้ำที่ 0 จะมีค่าเท่ากับ 0.5 (x_0) หลังจากนั้นผลลัพธ์จะมีค่าลู่เข้าสู่ค่า 0 (ลำดับการวนซ้ำ 4) และเมื่อกำหนดค่าพารามิเตอร์ r เป็น 0.5 หรือ 0.75 ก็มีแนวโน้มเช่นเดียวกัน

จากภาพที่ 2.4 ข) เมื่อกำหนดค่าพารามิเตอร์ r เป็น 1.5 ค่าที่ลำดับการวนซ้ำที่ 0 จะมีค่าเท่ากับ 0.5 (x_0) หลังจากนั้นผลลัพธ์จะมีค่าลู่เข้าสู่ค่า 0.33 (เริ่มที่ลำดับการวนซ้ำที่ 8) และผลจากภาพที่ 2.5 ค) เมื่อกำหนดค่าพารามิเตอร์ r เป็น 2.75 ค่าที่ลำดับการวนซ้ำที่ 1 เป็นต้นไปจะมีการเปลี่ยนแปลงไปมาแล้วค่าลู่เข้าสู่ค่า 0.636

จากภาพที่ 2.6 เมื่อกำหนดค่าพารามิเตอร์ r อยู่ในช่วง $3 < r < 1+\sqrt{6}$ ค่าผลลัพธ์จะมีการแกว่งอยู่ระหว่างค่าจำนวน 2 ค่า และจากภาพที่ 2.7 เมื่อกำหนดค่าพารามิเตอร์ r อยู่ในช่วง $1+\sqrt{6} < r < 3.54$ ค่าผลลัพธ์จะมีการแกว่งอยู่ระหว่างค่าจำนวน 4 ค่า

เมื่อทำการกำหนดค่าพารามิเตอร์อยู่ในช่วง $3.57 < r < 4$ ดังภาพที่ 2.8 จะทำให้ผลลัพธ์ที่ได้มีลักษณะเป็นพลวัตความยุ่งเหยิง และจากผลการทดสอบการกำหนดค่าพารามิเตอร์ r ในลอจิสติกแมพ สามารถสรุปแนวโน้มผลลัพธ์ของลอจิสติกแมพได้ดังตารางที่ 2.2

ตารางที่ 2.2 ความสัมพันธ์ระหว่างค่าพารามิเตอร์ r ในลอจิสติกแมพ

ค่าพารามิเตอร์ r	ผลลัพธ์ (แนวโน้มของ x_n)
$0 < r < 1$	ลู่เข้าสู่ค่า 0
$1 < r < 2$	ลู่เข้าสู่ค่า $\frac{r-1}{r}$
$2 < r < 3$	มีการแกว่งในช่วงแรก แล้วลู่เข้าสู่ค่า $\frac{r-1}{r}$
$3 < r < 1+\sqrt{6}$	เริ่มจากค่าการกำหนดเงื่อนไขเริ่มต้น หลังจากนั้นผลลัพธ์ที่ได้จะอยู่ระหว่างค่า 2 ค่า
$1+\sqrt{6} < r < 3.54$	เริ่มจากค่าการกำหนดเงื่อนไขเริ่มต้น หลังจากนั้นผลลัพธ์ที่ได้จะอยู่ระหว่างค่า 4 ค่า
$3.57 < r < 4$	ผลลัพธ์ที่มีลักษณะเป็นพลวัตความยุ่งเหยิง
$r > 3.57$	ผลลัพธ์ที่ได้จะเริ่มจากค่าการกำหนดเงื่อนไขเริ่มต้น หลังจากนั้นผลลัพธ์ที่ได้จะอยู่ระหว่างค่า 8, 16, 32, ... , 2^b จำนวน

2.3 รูปแบบลอจิสติกลำดับที่เป็นเศษส่วน

รูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน มาจากคณิตศาสตร์ที่ใช้หลักการปริพันธ์ และการอนุพันธ์ ด้วยลำดับการอนุพันธ์ที่เป็นเศษส่วน ซึ่งถูกนำมาใช้พัฒนาในรูปแบบประยุกต์ทางฟิสิกส์ และใช้ในทางวิศวกรรมศาสตร์ การอนุพันธ์ด้วยลำดับที่เป็นเศษส่วน สามารถเขียนให้อยู่ในรูปสมการได้ดังสมการที่ 2.2

$$\frac{d^n x^{\mu}}{dx^n} = \frac{\Gamma(\mu+1)}{\Gamma(\mu-n+1)} x^{\mu-n} \tag{2.2}$$

โดยที่ $\Gamma(\ )$ คือ ฟังก์ชันแกมมา (Grammar Functions) ซึ่งเป็นฟังก์ชันทางคณิตศาสตร์ที่เป็นส่วนขยายของฟังก์ชันแฟกทอเรียลบนจำนวนเชิงซ้อน โดยคุณสมบัติของฟังก์ชันแกมมาที่นำมาใช้ใน รูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน คือ $n! = \Gamma(n+1)$ และ $\Gamma(z+1) = z\Gamma(z)$ [33-35]

เมื่อแปลงสมการลอจิสติกแมพสมการที่ (2.1) ให้อยู่ในรูปของฟังก์ชันจะได้ดังสมการที่ 2.3

$$f(x) = rx(1-x) \tag{2.3}$$

และเมื่อทำการอนุพันธ์ฟังก์ชันด้วยลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) สมการที่ 2.3 จะได้ผลดังสมการที่ 2.4

$$
\begin{aligned}
D_x^{\alpha} f(x) &= r\left[\frac{\Gamma(2)x^{1-\alpha}}{\Gamma(2-\alpha)} - \frac{\Gamma(3)x^{2-\alpha}}{\Gamma(3-\alpha)}\right] \\
&= r\left[\frac{1!x^{1-\alpha}}{\Gamma(2-\alpha)} - \frac{2!x^{2-\alpha}}{\Gamma(3-\alpha)}\right] \\
&= r\left[\frac{x^{1+\alpha}}{\Gamma(2+\alpha)} - \frac{2x^{2+\alpha}}{\Gamma(3+\alpha)}\right] \\
&= r\left[\frac{x^{1+\alpha}}{(1+\alpha)\Gamma(1+\alpha)} - \frac{2x^{2+\alpha}}{(2+\alpha)(1+\alpha)\Gamma(1+\alpha)}\right] ::::: \Gamma(z+1) = z\Gamma(z) \\
&= \frac{rx^{1+\alpha}}{(1+\alpha)\Gamma(1+\alpha)} \times \left(1 - \frac{2x}{(2+\alpha)}\right) \\
&= \frac{rx^{1+\alpha}}{\Gamma(\alpha+2)} \times \left(1 - \frac{2x}{\alpha+2}\right)
\end{aligned}
\tag{2.4}
$$

ซึ่งสามารถเขียนในรูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วนได้ดังสมการที่ 2.5

$$
x_{n+1} = \frac{rx_n^{1+\alpha}}{\Gamma(\alpha+2)} \times \left(1 - \frac{2x_n}{\alpha+2}\right) \tag{2.5}
$$

เมื่อ x_n เป็นค่าในระบบที่ลำดับการวนซ้ำที่ n

r เป็นค่าพารามิเตอร์

n เป็นลำดับการวนซ้ำ

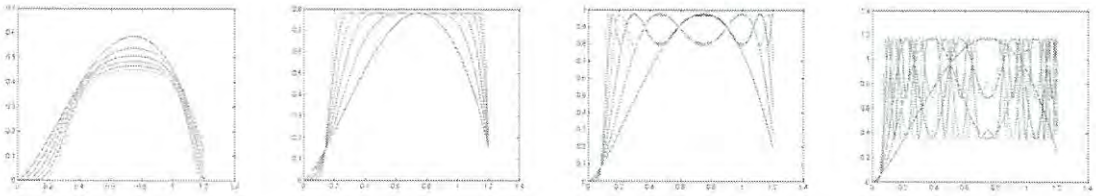
α เป็นลำดับการอนุพันธ์ที่เป็นเศษส่วน

จากสมการรูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน สามารถใช้ค่าลำดับการอนุพันธ์ที่เป็นเศษส่วน α ได้ตั้งแต่ $-\infty$ ถึง ∞ ซึ่งค่า α แต่ละค่าจะทำให้เป็นพลวัตความยุ่งเหยิงได้เฉพาะบางช่วงของค่าพารามิเตอร์ (r) เช่นเดียวกับลอจิสติกแมพ

เมื่อทำการทดสอบสมการรูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน ที่ลำดับการวนซ้ำที่ n ตั้งแต่ 1 ถึง 6 โดยทำการทดสอบที่ ค่าลำดับการอนุพันธ์ที่เป็นเศษส่วน $\alpha = \frac{1}{2}$ และค่าลำดับการอนุพันธ์ที่เป็นเศษส่วน $\alpha = \frac{1}{4}$ ได้ผลดังภาพที่ 2.9 และภาพที่ 2.10 ตามลำดับ

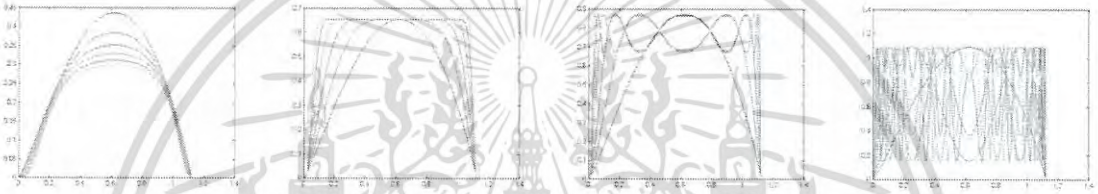
จากการสังเกตภาพที่ 2.9 พบว่าที่ค่าลำดับการอนุพันธ์ที่เป็นเศษส่วน $\alpha = \frac{1}{2}$ ผลลัพธ์ที่ได้มีจะลักษณะเป็นพลวัตความยุ่งเหยิงที่ค่าพารามิเตอร์ $r = 6$ และที่ค่าลำดับการอนุพันธ์ที่เป็นเศษส่วน $\alpha = \frac{1}{4}$ ในภาพที่ 2.10 ผลลัพธ์ที่ได้มีจะลักษณะเป็นพลวัตความยุ่งเหยิงที่ค่าพารามิเตอร์ $r = 5$ พบว่าเมื่อใช้ค่าลำดับการอนุพันธ์ที่เป็นเศษส่วน α ต่างกันเกิดจะความเป็นพลวัตความยุ่งเหยิงที่ค่าพารามิเตอร์ต่างกัน สำหรับช่วงที่เกิดความเป็นพลวัตความยุ่งเหยิงในระบบสามารถตรวจสอบได้

จาก ไลพูนอฟ เอกซ์โปเนนท์ (Lyapunov Exponent) และแผนภาพไบฟูลเคชัน (Bifurcation Diagram)



ก) $r=3$ ข) $r=4$ ค) $r=5$ ง) $r=6$

ภาพที่ 2.9 ผลการทดลองสมการรูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน ที่ ค่า $\alpha=\frac{1}{2}$



ก) $r=2$ ข) $r=3$ ค) $r=4$ ง) $r=5$

ภาพที่ 2.10 ผลการทดลองสมการรูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน ที่ ค่า $\alpha=\frac{1}{4}$

2.4 ไลพูนอฟ เอกซ์โปเนนท์

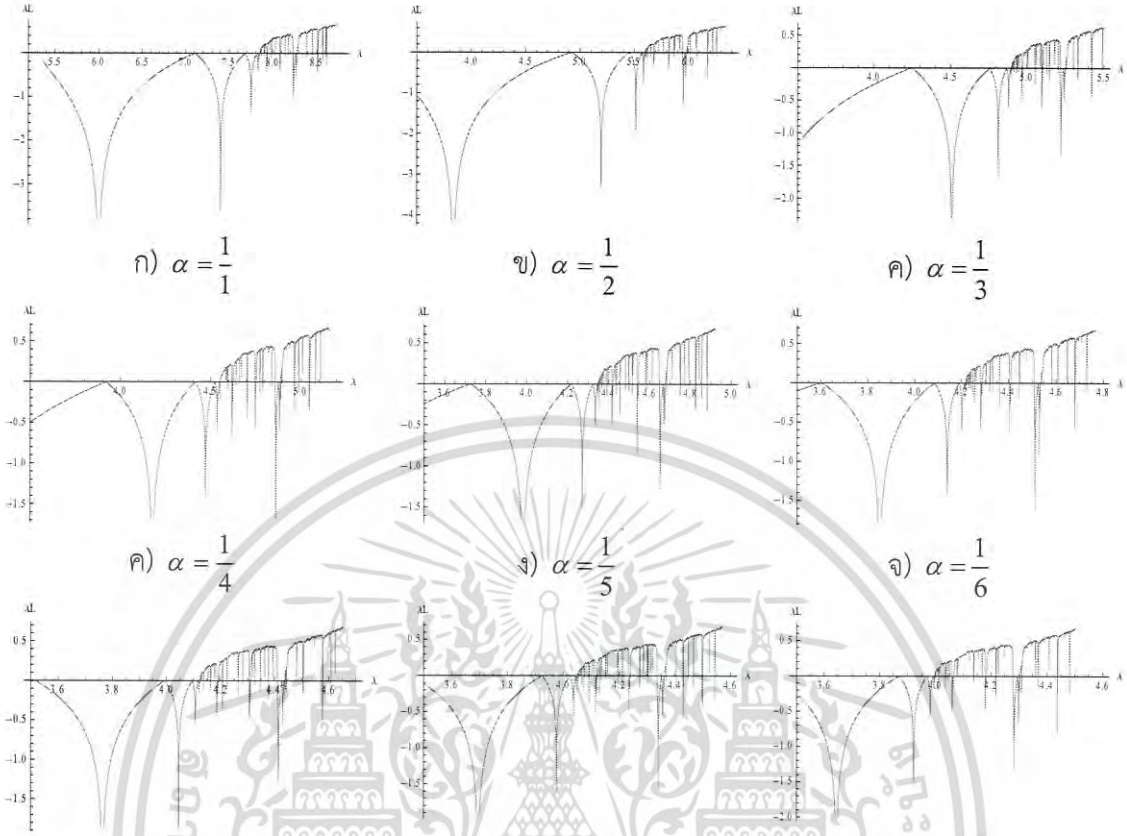
ไลพูนอฟ เอกซ์โปเนนท์ เป็นค่าทางคณิตศาสตร์ที่ใช้วัดค่าเฉลี่ยความเป็นเสถียรภาพในระบบพลวัตเทียบกับสภาวะตั้งต้น ถ้าค่าไลพูนอฟ เอกซ์โปเนนท์ ที่ได้จากระบบหรือสมการมีค่าเป็นบวก สามารถสรุปได้ว่าที่สภาวะในระบบหรือสมการช่วงนั้น จะมีความพลวัตความยุ่งเหยิง สมการหาค่าไลพูนอฟ เอกซ์โปเนนท์ เขียนได้ดังสมการที่ 2.6

$$\lambda=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\ln\left|\frac{df(x_i)}{dx}\right|_{x_i} \tag{2.6}$$

เมื่อ λ เป็นค่าไลพูนอฟ เอกซ์โปเนนท์

$\frac{df(x_i)}{dx}$ เป็นการอนุพันธ์ฟังก์ชัน $f(x_i)$ ที่ต้องการทดสอบ

จากการหาค่าไลพูนอฟ เอกซ์โปเนนท์ ของสมการการอนุพันธ์ลำดับที่เป็นเศษส่วน ในสมการที่ 2.5 ด้วยลำดับการอนุพันธ์ที่เป็นเศษส่วน α ที่ค่า $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}$ และ $\frac{1}{9}$ ได้ผลดังภาพที่ 2.11



ก) $\alpha = \frac{1}{1}$ ข) $\alpha = \frac{1}{2}$ ค) $\alpha = \frac{1}{3}$

ค) $\alpha = \frac{1}{4}$ ง) $\alpha = \frac{1}{5}$ จ) $\alpha = \frac{1}{6}$

ฉ) $\alpha = \frac{1}{7}$ ช) $\alpha = \frac{1}{8}$ ซ) $\alpha = \frac{1}{9}$

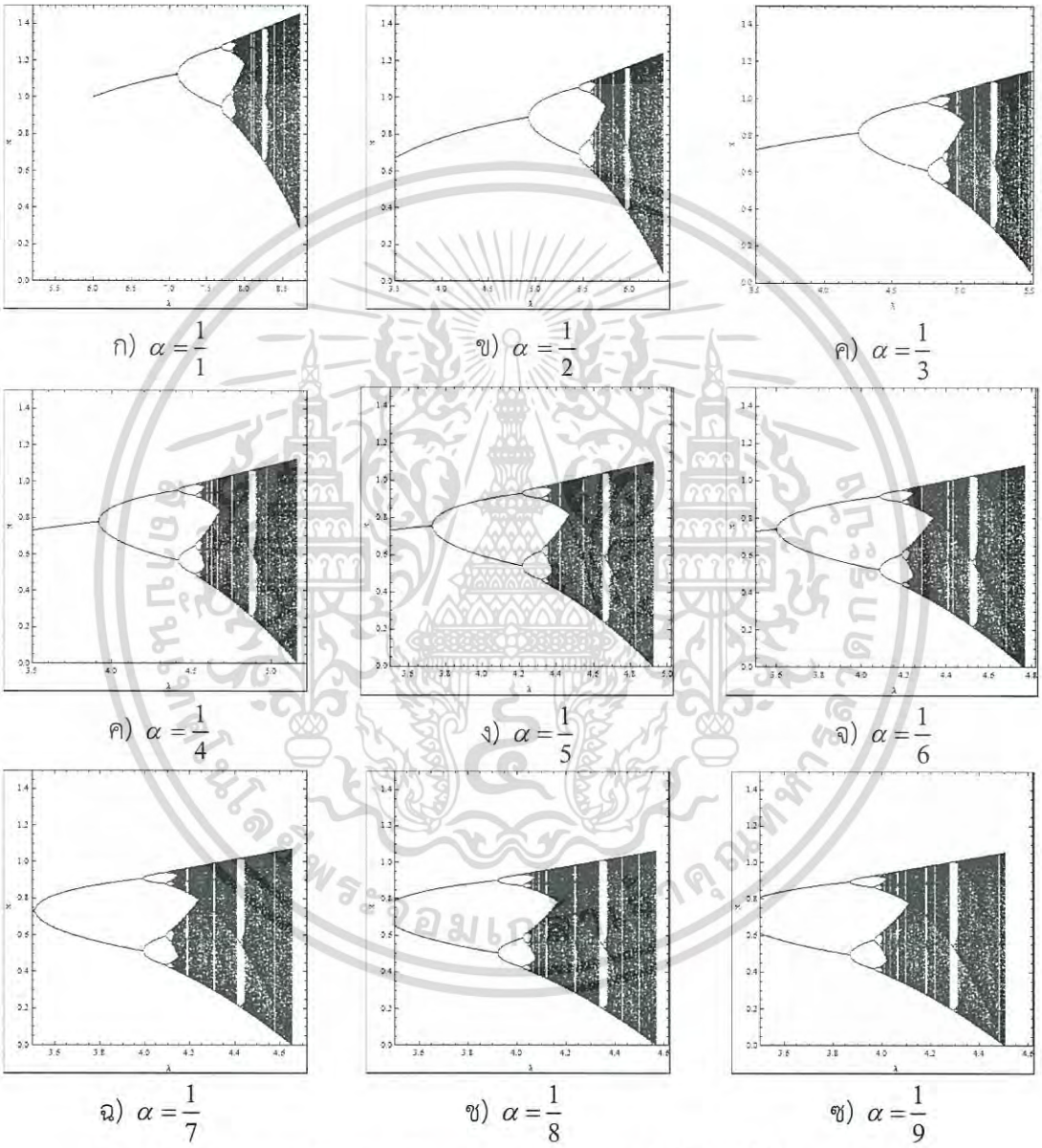
ภาพที่ 2.11 ค่าไลพูนอฟเอกซ์โปเนนท์ ของสมการการอนุพันธ์ลำดับที่เป็นเศษส่วน

จากภาพที่ 2.11 ก) ที่ลำดับการอนุพันธ์ที่เป็นเศษส่วน $\alpha = \frac{1}{2}$ แสดงให้เห็นว่า ในช่วงของพารามิเตอร์ 5.61-6.35 มีค่าไลพูนอฟ เอกซ์โปเนนท์ มากกว่า 0 หมายความว่าเป็นช่วงที่เกิดพลวัตความยุ่งเหยิง ซึ่งสามารถนำช่วงพารามิเตอร์นี้ที่เกิดจากลำดับการอนุพันธ์ที่เป็นเศษส่วนไปใช้งานเป็นกุญแจลับได้

2.5 แผนภาพไบฟูลเคชัน

ทฤษฎีไบฟูลเคชัน เป็นการศึกษาการเปลี่ยนแปลงของกลุ่มค่าที่อยู่ในระบบพลวัต ที่สามารถอธิบายปรากฏการณ์ที่เกิดขึ้นในระบบเมื่อค่าที่เกิดในระบบเปลี่ยนแปลงไปตามเวลา ซึ่งสามารถแสดงถึงค่าที่จะเกิดขึ้นได้ในเวลาต่าง ๆ และยังบอกถึงจุดที่เกิดความสมดุลระบบพลวัต เมื่อนำมาใช้งานกับสมการการอนุพันธ์ลำดับที่เป็นเศษส่วนจะสามารถแสดงว่าช่วงของค่าพารามิเตอร์ใดที่จะทำให้สมการเกิดความเป็นพลวัตความยุ่งเหยิง

แผนภาพไบฟูลเคชัน ของสมการการอนุพันธ์ลำดับที่เป็นเศษส่วน ในสมการที่ 2.5 ด้วยลำดับการอนุพันธ์ที่เป็นเศษส่วน α ที่ค่า $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}$ และ $\frac{1}{9}$ ได้ผลดังภาพที่ 2.12 โดยช่วงที่เกิดความเป็นพลวัตความยุ่งเหยิง คือ ช่วงในแผนภาพไบฟูลเคชันที่มีจำนวนค่าเกิดขึ้นมาก (เป็นช่วงสีดำ)



ก) $\alpha = \frac{1}{1}$ ข) $\alpha = \frac{1}{2}$ ค) $\alpha = \frac{1}{3}$

ค) $\alpha = \frac{1}{4}$ ง) $\alpha = \frac{1}{5}$ จ) $\alpha = \frac{1}{6}$

ฉ) $\alpha = \frac{1}{7}$ ช) $\alpha = \frac{1}{8}$ ซ) $\alpha = \frac{1}{9}$

ภาพที่ 2.12 แผนภาพไบฟูลเคชันของสมการการอนุพันธ์ลำดับที่เป็นเศษส่วน

จากภาพที่ 2.12 ก) ในแผนภาพไบฟูลเคชันที่ลำดับการอนุพันธ์ที่เป็นเศษส่วน $\alpha = \frac{1}{2}$ แสดงให้เห็นว่า ในช่วงของพารามิเตอร์ 5.61-6.35 มีค่าเกิดขึ้นเป็นจำนวนมาก (มีแถบสีดำเกิดขึ้นใน

แผนภาพไบฟูลเคชัน) หมายความว่าเป็นช่วงที่เกิดพลวัตความยุ่งเหยิง ซึ่งสามารถนำช่วงพารามิเตอร์นี้ที่เกิดจากลำดับการอนุพันธ์ที่เป็นเศษส่วนไปใช้งานเป็นกุญแจลับได้

ผลของค่าไลพูนอฟ เอกซ์โปเนนท์ และแผนภาพไบฟูลเคชัน ของสมการการอนุพันธ์ลำดับที่เป็นเศษส่วน จากภาพที่ 2.11 และ ภาพที่ 2.12 สรุปได้ว่าช่วงที่สมการที่ลำดับการอนุพันธ์ที่เป็นเศษส่วนต่าง ๆ เกิดความเป็นพลวัตความยุ่งเหยิงอยู่ในช่วงค่าพารามิเตอร์ต่าง ๆ ดังตารางที่ 2.3

ตารางที่ 2.3 การเกิดความเป็นพลวัตความยุ่งเหยิงรูปแบบลอจิสติกลำดับที่เป็นเศษส่วนที่ลำดับการอนุพันธ์ที่เป็นเศษส่วน และช่วงค่าพารามิเตอร์ต่าง ๆ

ลำดับการอนุพันธ์ที่เป็นเศษส่วน	ค่าพารามิเตอร์	ช่วงของค่าพารามิเตอร์ที่เป็นพลวัตความยุ่งเหยิง
1/1	7.85-8.72	0.87
1/2	5.61-6.35	0.74
1/3	4.90-5.5	0.6
1/4	4.55-5.15	0.6
1/5	4.35-4.92	0.57
1/6	4.22-4.77	0.55
1/7	4.13-4.65	0.52
1/8	4.05-4.57	0.52
1/9	4.00-4.51	0.51

จากตารางที่ 2.3 สามารถใช้งานรูปแบบลอจิสติกลำดับที่เป็นเศษส่วน โดยเลือกใช้งานลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) และค่าพารามิเตอร์ (r) เป็นกุญแจลับในการเข้ารหัส เมื่อพิจารณาแนวโน้มของช่วงที่เกิดความเป็นพลวัตความยุ่งเหยิงแต่และลำดับการอนุพันธ์ที่เป็นเศษส่วนพบว่า เมื่อเศษส่วนมีค่าน้อยลงจะทำให้ช่วงของความเป็นพลวัตความยุ่งเหยิงที่พารามิเตอร์ลดลง แต่ทว่ายังสามารถใช้ลำดับการอนุพันธ์ที่เป็นเศษส่วนนอกเหนือจากค่า $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}$ และ $\frac{1}{9}$ ที่ยกตัวอย่างมา โดยเมื่อผสานคู่ของลำดับการอนุพันธ์ที่เป็นเศษส่วนที่มีอย่างไม่จำกัด กับช่วงของพารามิเตอร์ที่เกิดความเป็นพลวัตความยุ่งเหยิง ทำให้เกิดจำนวนกุญแจลับอย่างอนันต์

บทที่ 3
การเข้ารหัส และถอดรหัสภาพ

การเข้ารหัส และถอดรหัสของภาพด้วย วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ที่เสนอโดย A. N. Pisarchik [23] ใช้ทฤษฎีความยุ่งเหยิงในการเข้ารหัสภาพโดยอาศัยข้อมูลจุดภาพที่อยู่ภายในภาพมาเป็นค่าเงื่อนไขตั้งต้นของจุดภาพลำดับถัดไป โดยมีการแปลงค่าระดับสีภาพซึ่งเป็นจำนวนเต็มเปลี่ยนเป็นค่าที่อยู่ในช่วงของพลวัตความยุ่งเหยิง และสามารถแปลงค่ากลับเป็นค่าในช่วงระดับสีภาพ E. Solak [25] ได้ทำการทดสอบกระบวนการเข้ารหัสลับ และถอดรหัสลับของภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) แล้วพบว่าเกิดกรณีที่ไม่สามารถแปลงค่าที่อยู่ในช่วงการทำงานของพลวัตความยุ่งเหยิงกลับเป็นค่าในช่วงระดับสีภาพได้ และยังพบว่าบางกระบวนการทำงานทำให้เกิดปัญหาในการใช้งานพลวัตความยุ่งเหยิง

วิทยานิพนธ์นี้ จึงนำเสนอการเข้ารหัสลับ และถอดรหัสลับของภาพ โดยอาศัยหลักการของ A. N. Pisarchik [23] และคำแนะนำของ E. Solak [25] โดยทำการปรับสมการในการแปลงค่าระหว่างค่าในช่วงระดับสีภาพ และคาที่อยู่ในช่วงของพลวัตความยุ่งเหยิง ทั้งยังทำการทดลองเปลี่ยนพลวัตความยุ่งเหยิงจากลอจิสติกแมพ เป็นรูปแบบลอจิสติกลำดับที่เป็นเศษส่วนทำให้จากเดิมที่การเข้ารหัส และถอดรหัสของภาพด้วย วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ที่ใช้ค่าพารามิเตอร์ ลำดับการวนซ้ำ และ จำนวนรอบในกระบวนการเข้ารหัสเป็นกุญแจลับ มีกุญแจลับที่ใช้งานเพิ่มขึ้นได้แก่ลำดับการอนุพันธ์ที่เป็นเศษส่วน ซึ่งจะทำให้เกิดความยุ่งเหยิงในแต่ละช่วงค่าพารามิเตอร์ที่แตกต่างกัน และเมื่อใช้ลำดับการอนุพันธ์ที่เป็นเศษส่วนกับค่าพารามิเตอร์เป็นกุญแจร่วมกัน สามารถทำให้มีค่ากุญแจที่ใช้งานเพิ่มขึ้นอย่างมหาศาล สุดท้ายได้ปรับกระบวนการบางส่วนโดยการสลับลำดับจุดภาพของการเข้ารหัส ซึ่งลำดับดังกล่าวได้ใช้พลวัตความยุ่งเหยิงอีกตัวในการสร้าง ทำให้ไม่สามารถคาดเดาได้ว่ามีลำดับการเข้ารหัสอย่างไร เพื่อเพิ่มความปลอดภัยในการเข้ารหัส และยังเป็นผลให้ประสิทธิผลของการเข้ารหัสที่ดีขึ้น เพราะค่าในการเข้ารหัสมีการกระจายตัวมากขึ้น ทั้งยังช่วยเพิ่มกุญแจที่ใช้งาน และทำให้ประสิทธิผลของการเข้ารหัสที่มากขึ้นด้วย

3.1 การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

A. N. Pisarchik ได้นำเสนอวิธีการเข้ารหัสลับ และถอดรหัสลับของภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) [23] โดยเริ่มจากสมการลอจิสติกแมพ (สมการที่ 2.1) ซึ่งให้ผลลัพธ์ที่ลำดับการวนซ้ำต่าง ๆ เป็นจำนวนจริงอยู่ในช่วง $[x_{\min}, x_{\max}]$ ทว่าข้อมูลภาพแต่ละลำดับเป็นค่าที่อยู่ในจุดภาพเป็นจำนวนเต็มอยู่ในช่วง [0, 255] และในการนำลอจิสติกแมพมาใช้กับการ

เข้ารหัสภาพกรณีที่เป็นภาพสีปกติจะมีข้อมูลในส่วนของจุดภาพที่ประกอบส่วนของสีแดง สีเขียว และสีน้ำเงิน โดยเขียนแทนด้วยตัวแปร $C=(C_r,C_g,C_b)$ จะประมวลผลขนานแยกแต่ละองค์ประกอบของสี โดยจำเป็นต้องทำการแปลงค่าจำนวนเต็ม C เป็นจำนวนจริง $x_C=(x_C^r,x_C^g,x_C^b)$ เพื่อทำให้ค่าที่ได้อยู่ในช่วง $[x_{\min},x_{\max}]$ ตามสมการที่ (3.1)

$$x_c = x_{\min} + \delta x \cdot \left(\frac{C}{255}\right) \tag{3.1}$$

เมื่อ $\delta x = x_{\max} - x_{\min}$

$$x_{\max} = \frac{r}{4}$$

$$x_{\min} = \frac{r^2}{4}\left(1-\frac{r}{4}\right)$$

และเมื่อต้องการเปลี่ยนจำนวนจริง x_n ที่เป็นตัวแทนค่าในแต่ละจุดภาพจากลอจิสติกแมพกลับเป็นจำนวนเต็ม C ในช่วง [0, 255] จะใช้สมการที่ (3.2)

$$C = round\left[(x_n - x_{\min})\cdot\frac{255}{\delta x}\right] \tag{3.2}$$

จากการศึกษา พบว่าสมการที่ (3.1) และ (3.2) เป็นผลให้การถอดรหัสที่จุดภาพต้นฉบับที่มีค่าเป็น 0 หรือ 255 หลายจุดเกิดความผิดพลาดขึ้น [25, 36] จึงได้ทำการปรับสมการแปลงค่าจากจำนวนเต็มเป็นจำนวนจริง โดยปรับจากสมการที่ (3.1) เป็นสมการที่ (3.3) และทำการปรับสมการแปลงค่าจากจำนวนจริงจำนวนเต็ม โดยปรับจากสมการที่ (3.2) เป็นสมการที่ (3.4) [36]

$$x_c = x_{\min} + \delta x \cdot \left(\frac{C+1}{257}\right) \tag{3.3}$$

$$C = round\left[(x_n - x_{\min})\cdot\frac{257}{\delta x} - 1\right] \tag{3.4}$$

ในการกำหนดค่าเงื่อนไขตั้งต้น $x_c = x_0$ ที่แตกต่างกันในสมการลอจิสติกแมพเพียงเล็กน้อย จะทำผลลัพธ์ที่ได้นั้นแตกต่างกันอย่างมหาศาล ดังนั้นค่าเงื่อนไขตั้งต้นจึงเป็นตัวกำหนดที่สำคัญในลำดับการวนซ้ำต่าง ๆ ของโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ทั้งในการเข้ารหัสลับ

ของภาพ และถอดรหัสลับของภาพ ในการเข้ารหัสลับของภาพจะใช้ค่าเงื่อนไขตั้งต้น x_0^i ในแผนที่ตาราง i จะนำค่าในลำดับสุดท้ายของแผนที่ตารางก่อนหน้า $i-1$ มาใช้งาน จากสมการที่ 2.1 จะให้ผลลัพธ์ที่มีความเป็นพลวัตความยุ่งเหยิง เมื่อทำการกำหนดค่าพารามิเตอร์อยู่ในช่วง $3.57 < r < 4$

3.1.1 กระบวนการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

ในกระบวนการเข้ารหัสสรุปเป็นขั้นตอนได้ดังนี้

I. ทำการแปลงข้อมูลภาพที่ประกอบด้วยจุดภาพ $M \times N$ เป็น m ลำดับ (โดยที่ $m = M \times N$) ดังนั้นลำดับที่ i จะเป็น $i = 1, 2, 3, ..., m$ แล้วทำการแปลงค่าสีในแต่ละจุดภาพในแต่ละองค์ประกอบของสีตามสมการที่ (3.3)

II. เริ่มใช้ค่าในลำดับสุดท้ายที่ทำการแปลงค่าแล้ว คือ x_c^m มาเป็นค่าการกำหนดเงื่อนไขเริ่มต้นของจุดภาพแรก $x_0^i = x_c^m (i = 1)$ ดังสมการที่ (3.5) (จุดภาพอื่น ๆ ใช้ค่าการกำหนดเงื่อนไขเริ่มต้น ดังสมการที่ (3.6))

III. หลังจากทำการคำนวณจากสมการลอจิสติกแมพ จากสมการที่ (2.1) ในแต่ละจุดภาพลำดับ n จะได้ผลลัพธ์ x_n^i ให้นำไปรวมกับค่าสีในแต่ละจุดภาพที่ทำการแปลงค่าแล้ว x_c^i ผลลัพธ์ที่ได้จะนำไปเป็นค่าการกำหนดเงื่อนไขเริ่มต้น

IV. เมื่อทำการคำนวณลอจิสติกแมพทั้งหมดครบ m จุดภาพแล้วต้องมีการพิจารณาค่าในแต่ละจุดภาพที่ได้ตามเงื่อนไขเริ่มต้นของลอจิสติกแมพ คือ $x_0 \in [x_{\min}, x_{\max}]$ ดังนั้นหากค่าที่ได้ไม่อยู่ในเงื่อนไข คือ ถ้า $x_n^i + x_c^i > x_{\max}$ จะต้องทำการแปลงค่าให้อยู่ในเงื่อนไขโดยการลบค่าออกด้วย δx หรือ $2\delta x$ ตามสมการที่ (3.7)

V. จากนั้นจะทำซ้ำขั้นตอนที่ II. ถึง IV. อีกจำนวน J รอบ โดยใช้ค่าการกำหนดเงื่อนไขเริ่มต้นของจุดภาพแรกรอบที่ $j+1$ เป็นค่าสุดท้ายของจุดภาพที่ได้จากรอบก่อนหน้า j ดังนี้ $x_0^1(j+1) = x_c^m(j)$

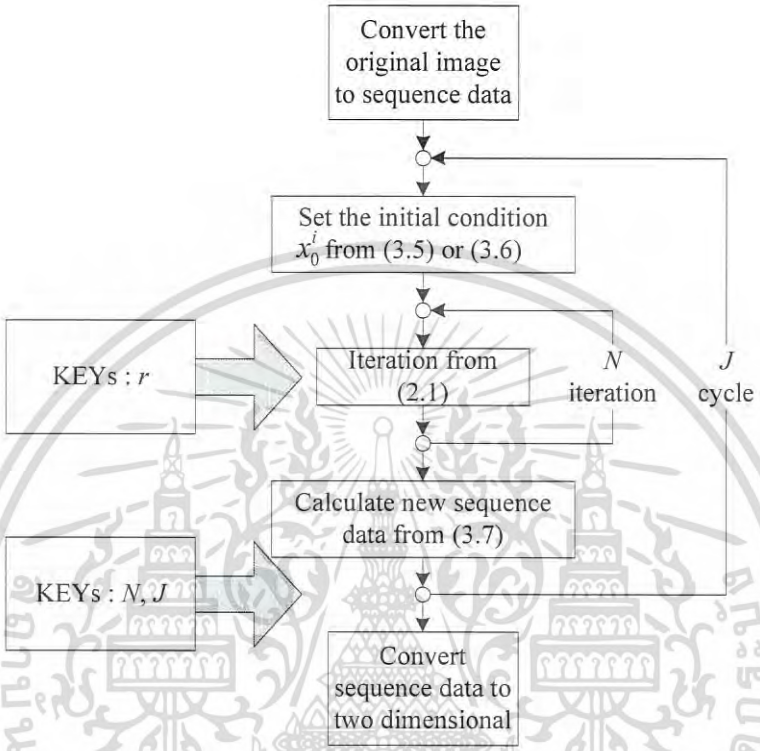
VI. หลังจากทำการคำนวณลอจิสติกแมพครบทั้งหมดนี้แล้วจะทำการเปลี่ยนค่าที่ได้จากจำนวนจริงกลับเป็นค่าสีที่เป็นจำนวนเต็มค่า [0, 255] ตามสมการที่ (3.4) จะได้ภาพที่เข้ารหัสแล้ว

ขั้นตอนการเข้ารหัสที่กล่าวมาสามารถสรุปได้เป็นสมการที่ (3.5) ถึงสมการที่ (3.7) และแผนภาพแสดงการทำงานได้ดังภาพที่ 3.1

$$x_0^i(j) = x_c^m(j-1) \text{ เมื่อ } i = 1 \tag{3.5}$$

$$x_0^{i+1}(j) = x_c^i(j) \text{ เมื่อ } i > 1 \tag{3.6}$$

$$x_c^i(j)=\begin{cases} x_n^i(j-1)+x_c^i(j-1) & x_n^i(j-1)+x_c^i(j-1)\le x_{\max} \\ x_n^i(j-1)+x_c^i(j-1)-\delta x & \text{เมื่อ } x_{\max}<x_n^i(j-1)+x_c^i(j-1)\le 2x_{\max}-x_{\min} \\ x_n^i(j-1)+x_c^i(j-1)-2\delta x & 2x_{\max}-x_{\min}<x_n^i(j-1)+x_c^i(j-1) \end{cases} \quad (3.7)$$



ภาพที่ 3.1 แผนภาพกระบวนการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

3.1.2 กระบวนการถอดรหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

กระบวนการถอดรหัสเริ่มจากการแปลงค่าสีในแต่ละจุดภาพที่ผ่านกระบวนการเข้ารหัส โดยแยกตามองค์ประกอบของสีตามสมการที่ (3.3) เป็น $x_c^i(j)$ ในกระบวนการถอดรหัสจะทำย้อนกลับกับกระบวนการเข้ารหัส คือจะเริ่มคำนวณลอจิสติกแมพจากจุดภาพสุดท้าย หรือลำดับสุดท้าย ย้อนกลับไปยังจุดภาพแรก โดยกระบวนการถอดรหัสสรุปเป็นขั้นตอนได้ดังนี้

I. ทำการเริ่มต้นถอดรหัสภาพเพื่อให้ได้ผลลัพธ์ในรอบที่ $j-1$ โดยพิจารณาจากค่าในรอบที่ j เริ่มกระบวนการที่จุดภาพสุดท้าย m สำหรับค่าการกำหนดเงื่อนไขเริ่มต้นในรอบที่ $j-1$ จะใช้ค่าในจุดภาพก่อนหน้าในรอบที่ j ตัวอย่างเช่น $x_0^m(j-1)=x_c^{m-1}(j)$ หลังจากทำการคำนวณลอจิสติกแมพในแต่ละจุดภาพลำดับ n จะได้ผลเป็น $x_n^m(j-1)$ แล้วจะนำไปลบกับค่า $x_c^m(j)$ ได้ผลลัพธ์เป็น $x_c^m(j-1)$ ใหม่

II. สำหรับจุดภาพที่ $m-1$ ถึงจุดภาพที่ 2 จะใช้ค่าการกำหนดเงื่อนไขเริ่มต้นในรอบที่ j จุดภาพที่ $i-1$ มาใช้เช่นกันสามารถเขียนได้ดังสมการที่ (3.8)

III. จากนั้นจะทำซ้ำขั้นตอนที่ I. และ II. ย้อนไปจนถึงจุดภาพลำดับที่ 2

IV. แต่เมื่อพิจารณาที่จุดภาพตำแหน่งแรก (ในรอบที่ $j-1$) จะใช้ข้อมูลตำแหน่งสุดท้ายในรอบที่ $j-1$ เป็นค่าการกำหนดเงื่อนไขเริ่มต้นสามารถเขียนได้ดังสมการที่ (3.9) เมื่อทำการคำนวณลอจิสติกแมพทั้งหมด m จุดภาพแล้วต้องมีการพิจารณาค่าในแต่ละจุดภาพที่ได้ตามเงื่อนไขเริ่มต้นของลอจิสติกแมพ ดังนั้นหากค่าที่ได้ไม่อยู่ในเงื่อนไขคือ ถ้า $x_c^i(j)-x_n^i(j-1)<0$ จะต้องทำการแปลงค่าให้อยู่ในเงื่อนไขโดยการบวกค่า δx หรือ $2\delta x$ เพิ่มขึ้น ตามสมการที่ (3.10)

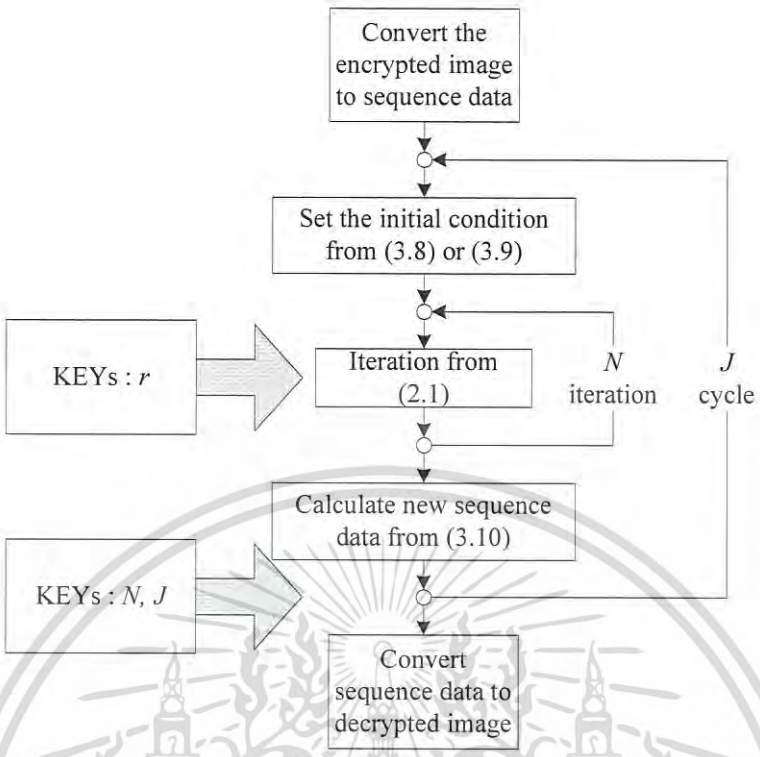
V. จากนั้นจะทำซ้ำขั้นตอนทั้งหมดอีกจำนวน J รอบ แล้วทำการเปลี่ยนค่าที่ได้จากจำนวนจริงกลับเป็นค่าสีที่เป็นจำนวนเต็มตามสมการที่ (3.4)

ขั้นตอนการถอดรหัสที่กล่าวมาสามารถสรุปได้เป็นสมการที่ (3.8) ถึงสมการที่ (3.10) และแผนภาพแสดงการทำงานได้ดังภาพที่ 3.2

$$x_0^i(j-1)=x_c^{i-1}(j) \text{ เมื่อ } i>1 \tag{3.8}$$

$$x_0^i(j-1)=x_c^m(j-1) \text{ เมื่อ } i=1 \tag{3.9}$$

$$x_c^i(j-1)=\begin{cases} x_c^i(j)-x_n^i(j-1) & x_{\min}\le x_c^i(j)-x_n^i(j-1) \\ x_c^i(j)-x_n^i(j-1)+\delta x & \text{เมื่อ } -x_{\max}+2x_{\min}<x_c^i(j)-x_n^i(j-1)\le x_{\min} \\ x_c^i(j)-x_n^i(j-1)+2\delta x & x_c^i(j)-x_n^i(j-1)<-x_{\max}+2x_{\min} \end{cases} \tag{3.10}$$



ภาพที่ 3.2 แผนภาพกระบวนการถอดรหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง ใช้กุญแจลับทั้งหมด 3 ตัว ได้แก่ ค่าพารามิเตอร์ (r) ลำดับการวนซ้ำ (N) และจำนวนรอบในกระบวนการเข้ารหัส (J) ของ โครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ซึ่งความปลอดภัยขึ้นอยู่กับการเปลี่ยนค่ากุญแจลับต่าง ๆ ที่จะใช้งานเหล่านี้

3.2 การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)

การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) อาศัยลอจิสติกแมพซึ่งมีคุณสมบัติที่เป็นพลวัตความยุ่งเหยิง เป็นส่วนสำคัญในการเข้ารหัส และถอดรหัสภาพ และจากบทที่ 2 กล่าวถึงเรื่องรูปแบบลอจิสติกลำดับที่เป็นเศษส่วน ด้วยการอนุพันธ์ลำดับการอนุพันธ์ที่เป็นเศษส่วนของลอจิสติกแมพ ซึ่งมีคุณสมบัติเป็นพลวัตความยุ่งเหยิงเช่นกัน โดยมีส่วนของลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) เป็นตัวแปรที่เพิ่มขึ้นมา ซึ่งสามารถนำมาใช้เป็นกุญแจลับตัวใหม่ ทำให้จำนวนของกุญแจลับเพิ่มขึ้นอย่างมหาศาลจากการผสมผสานความสัมพันธ์ของกุญแจลับลำดับการอนุพันธ์ที่เป็นเศษส่วน และค่าพารามิเตอร์

กระบวนการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) สามารถทำได้ โดยใช้สมการที่ (2.5) แทนสมการที่ (2.1) ใน การเข้ารหัส และ

ถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) โดยเปลี่ยน ค่าสูดสุดของพลวัตความยุ่งเหยิงเป็นดังสมการที่ (3.11) และ ค่าต่ำสุดเป็นดังสมการที่ (3.12)

$$x_{\max} = \frac{r(1+\alpha)^{1+\alpha}}{2^{1+\alpha}\Gamma(\alpha+2)}\left(1-\frac{\alpha+1}{\alpha+2}\right) \tag{3.11}$$

$$x_{\min} = \frac{r\left(\frac{r(1+\alpha)^{1+\alpha}}{2^{1+\alpha}\Gamma(\alpha+2)}\left(1-\frac{\alpha+1}{\alpha+2}\right)\right)^{1+\alpha}}{\Gamma(\alpha+2)}\left(1-\frac{2\left(\frac{r(1+\alpha)^{1+\alpha}}{2^{1+\alpha}\Gamma(\alpha+2)}\left(1-\frac{\alpha+1}{\alpha+2}\right)\right)}{\alpha+2}\right) \tag{3.12}$$

3.3 การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

สำหรับการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) พัฒนาการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ที่มีกุญแจลับลำดับการอนุพันธ์ที่เป็นเศษส่วนเพิ่มขึ้นมาแล้ว โดยเพิ่มความซับซ้อนในการเข้ารหัส และถอดรหัสภาพ ด้วยการเพิ่มขั้นตอนการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) โดยมีการสลับลำดับในการเข้ารหัส ซึ่งลำดับที่สลับนี้มาจากการใช้พลวัตความยุ่งเหยิงอีกตัว นอกจากทำให้จำนวนกุญแจลับเพิ่มขึ้นแล้วยังทำให้ประสิทธิผลในการเข้ารหัสดีขึ้นด้วย

3.3.1 กระบวนการเข้ารหัสด้วยการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

ในกระบวนการเข้ารหัสสรุปเป็นขั้นตอนได้ดังนี้

I. ทำการแปลงข้อมูลภาพที่ประกอบด้วยจุดภาพ $M \times N$ เป็น m ลำดับ (โดยที่ $m = M \times N$) ดังนั้นลำดับที่ i จะเป็น $i = 1, 2, 3, ..., m$

II. สร้างลำดับของจุดภาพที่จะทำการเข้ารหัส โดยอาศัยพลวัตความยุ่งเหยิงจากลอจิสติกแมพ (สมการที่ 2.1) สร้างค่าจำนวน m ลำดับ แล้วใช้จุดภาพที่ตำแหน่งที่มีค่าลอจิสติกแมพน้อยที่สุดเป็นจุดภาพลำดับแรกในการเข้ารหัส x^{1st} เรียงลำดับจนถึงค่าลอจิสติก แมพมากที่สุดเป็นจุดภาพลำดับสุดท้ายในการเข้ารหัส x^{last}

III. ทำการแปลงค่าสีในแต่ละจุดภาพในแต่ละองค์ประกอบของสีตามสมการที่ (3.3)

IV. ใช้ค่าในตำแหน่งลำดับ (สุดท้ายจากข้อ II.) ที่ทำการแปลงค่าแล้ว คือ x_c^{last} มาเป็นค่าการกำหนดเงื่อนไขเริ่มต้นของจุดภาพแรก $x_0^i = x_c^{last}\ (i = 1^{st})$ ดังสมการที่ (3.13)

V. หลังจากทำการคำนวณจากสมการลำดับการอนุพันธ์ที่เป็นเศษส่วน (สมการที่ 2.5) ในแต่ละจุดภาพลำดับ n จะได้ผลลัพธ์ x_n^i ให้นำไปรวมกับค่าสีในแต่ละจุดภาพที่ทำการแปลงค่าแล้ว x_c^i ผลลัพธ์ที่ได้จะนำไปเป็นค่าการกำหนดเงื่อนไขเริ่มต้น

VI. เมื่อทำการคำนวณลอจิสติกแมพทั้งหมด m จุดภาพแล้วต้องมีการพิจารณาค่าในแต่ละจุดภาพที่ได้ตามเงื่อนไขเริ่มต้นของลอจิสติกแมพ คือ $x_0 \in [x_{\min}, x_{\max}]$ ดังนั้นหากค่าที่ได้ไม่อยู่ในเงื่อนไข คือ ถ้า $x_n^i + x_c^i > x_{\max}$ จะต้องทำการแปลงค่าให้อยู่ในเงื่อนไขโดยการลบค่าออกด้วย δx หรือ $2\delta x$ ตามสมการที่ (3.15)

VII. จากนั้นจะทำซ้ำขั้นตอนที่ IV. และ VI. จำนวน J รอบ โดยใช้ค่าการกำหนดเงื่อนไขเริ่มต้นของจุดภาพแรกรอบที่ $j+1$ เป็นค่าสุดท้ายของจุดภาพที่ได้จากรอบก่อนหน้า j ดังนี้ $x_0^1(j+1) = x_c^m(j)$

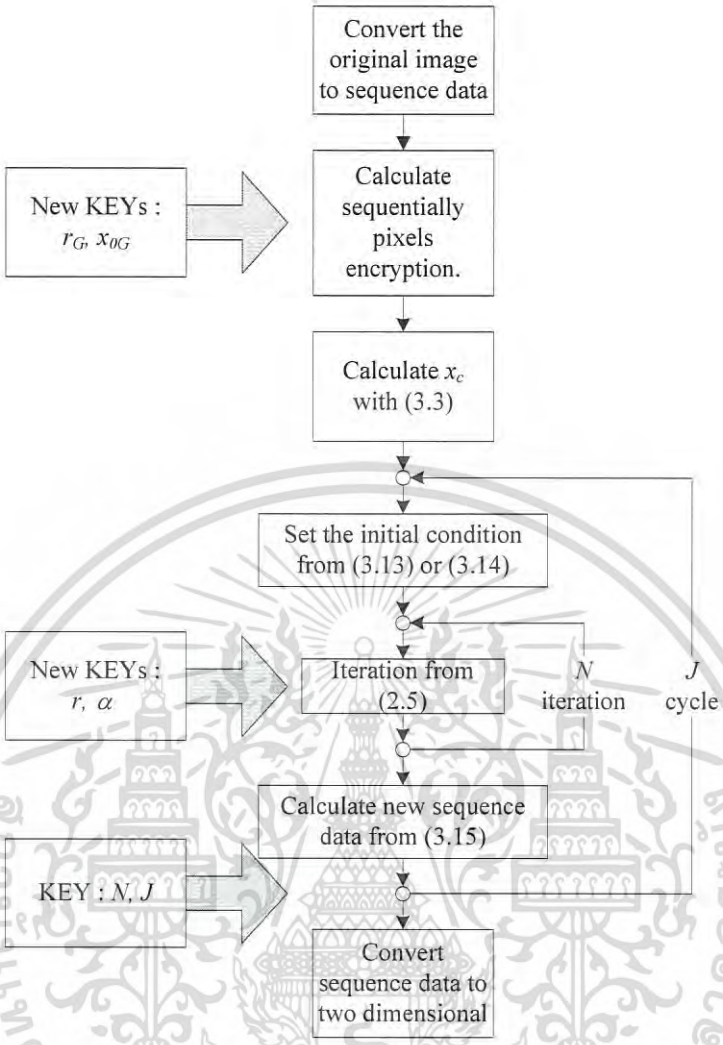
VIII. หลังจากทำการคำนวณลอจิสติกแมพครบทั้งหมดนี้แล้วจะทำการเปลี่ยนค่าที่ได้จากจำนวนจริงกลับเป็นค่าสีที่เป็นจำนวนเต็มค่า [0, 255] ตามสมการที่ (3.4) จะได้ภาพที่เข้ารหัสแล้ว

ขั้นตอนการเข้ารหัสที่กล่าวมาสามารถสรุปได้เป็นสมการที่ (3.13) ถึงสมการที่ (3.15) และแผนภาพแสดงการทำงานได้ดังภาพที่ 3.3

$$x_0^i(j) = x_c^{last}(j-1) \quad ;if \quad i = 1^{st} \tag{3.13}$$

$$x_0^i(j) = x_c^{i-1}(j) \quad ;if \quad i \neq 1^{st} \tag{3.14}$$

$$x_c^i(j) = \begin{cases} x_n^i(j-1) + x_c^i(j-1) & if \quad x_n^i(j-1) + x_c^i(j-1) \le x_{\max} \\ x_n^i(j-1) + x_c^i(j-1) - \delta x & if \quad x_{\max} < x_n^i(j-1) + x_c^i(j-1) \le 2x_{\max} - x_{\min} \\ x_n^i(j-1) + x_c^i(j-1) - 2\delta x & if \quad 2x_{\max} - x_{\min} < x_n^i(j-1) + x_c^i(j-1) \end{cases} \tag{3.15}$$



ภาพที่ 3.3 แผนภาพกระบวนการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

3.3.2 กระบวนการถอดรหัสด้วยการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

กระบวนการถอดรหัสเริ่มจากการแปลงค่าสีในแต่ละจุดภาพที่ผ่านกระบวนการเข้ารหัส โดยแยกตามองค์ประกอบของสีตามสมการที่ (3.3) เป็น $x_c^i(j)$ ในกระบวนการถอดรหัสจะทำย้อนกลับกับกระบวนการเข้ารหัส โดยกระบวนการถอดรหัสสรุปเป็นขั้นตอนได้ดังนี้

I. สร้างลำดับของจุดภาพที่จะทำการถอด โดยอาศัยพลวัตความยุ่งเหยิงจากลอจิสติกแมพดังสมการที่ (2.1) สร้างค่าจำนวน m ลำดับ แล้วใช้จุดภาพที่ตำแหน่งที่มีค่าลอจิสติกแมพน้อยที่สุดเป็นจุดภาพลำดับแรกในการเข้ารหัส $x^{1^{st}}$ เรียงลำดับจนถึงค่าลอจิสติกแมพมากที่สุดเป็นจุดภาพลำดับสุดท้ายในการเข้ารหัส

II. ทำการเริ่มต้นถอดรหัสภาพเพื่อให้ได้ผลลัพธ์ในรอบที่ $j-1$ โดยพิจารณาจากค่าในรอบที่ j เริ่มกระบวนการที่จุดภาพสุดท้าย $last$ สำหรับค่าการกำหนดเงื่อนไขเริ่มต้นในรอบที่ $j-1$ จะใช้ค่าในจุดภาพก่อนหน้าในรอบที่ j ตัวอย่างเช่น $x_0^{last}(j-1) = x_c^{last-1}(j)$ หลังจากทำการคำนวณลอจิสติกแมพในแต่ละจุดภาพลำดับ n จะได้ผลเป็น $x_n^{last}(j-1)$ แล้วจะนำไปลบกับค่า $x_c^{lat}(j)$ ได้ผลลัพธ์เป็น $x_c^{last}(j-1)$ ใหม่

III. สำหรับจุดภาพลำดับที่ $last-1$ จะใช้ค่าการกำหนดเงื่อนไขเริ่มต้นในรอบที่ j จุดภาพที่ $i-1$ มาใช้เช่นกันสามารถเขียนได้ดังสมการที่ (3.16)

IV. จากนั้นจะทำซ้ำขั้นตอนที่ II. และ III. ย้อนไปจนถึงจุดภาพลำดับที่ 2

V. แต่เมื่อพิจารณาที่จุดภาพตำแหน่งแรก (ในรอบที่ $j-1$) จะใช้ข้อมูลตำแหน่งสุดท้ายในรอบที่ $j-1$ เป็นค่าการกำหนดเงื่อนไขเริ่มต้นสามารถเขียนได้ดังสมการที่ (3.17) เมื่อทำการคำนวณลอจิสติกแมพทั้งหมด m จุดภาพแล้วต้องมีการพิจารณาค่าในแต่ละจุดภาพที่ได้ตามเงื่อนไขเริ่มต้นของลอจิสติกแมพ ดังนั้นหากค่าที่ได้ไม่อยู่ในเงื่อนไขคือ ถ้า $x_c^i(j) - x_n^i(j-1) < 0$ จะต้องทำการแปลงค่าให้อยู่ในเงื่อนไขโดยการบวกค่า δx หรือ $2\delta x$ เพิ่มขึ้น ตามสมการที่ (3.18)

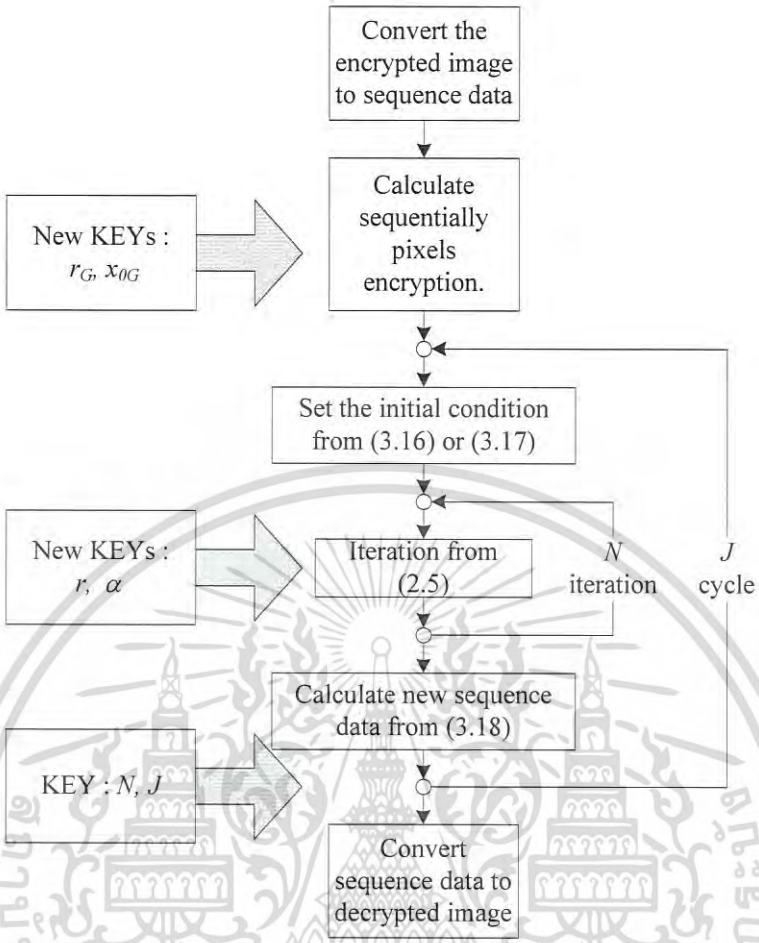
VI. จากนั้นจะทำซ้ำขั้นตอนทั้งหมดอีกจำนวน J รอบ แล้วทำการเปลี่ยนค่าที่ได้จากจำนวนจริงกลับเป็นค่าสีที่เป็นจำนวนเต็มตามสมการที่ (3.4)

ขั้นตอนการถอดรหัสที่กล่าวมาสามารถสรุปได้เป็นสมการที่ (3.16) ถึงสมการที่ (3.16) และแผนภาพแสดงการทำงานได้ดังภาพที่ 3.4

$$x_0^i(j-1) = x_c^{i-1}(j) \quad ;if \quad i \neq 1^{st} \tag{3.16}$$

$$x_0^i(j-1) = x_c^{last}(j-1) \quad ;if \quad i = 1^{st} \tag{3.17}$$

$$x_c^i(j-1) = \begin{cases} x_c^i(j) - x_n^i(j-1) & if \quad x_c^i(j) - x_n^i(j-1) \geq x_{\min} \\ x_c^i(j) - x_n^i(j-1) + \delta x & if \quad -x_{\max} + 2x_{\min} \leq x_c^i(j) - x_n^i(j-1) < x_{\min} \\ x_c^i(j) - x_n^i(j-1) + 2\delta x & if \quad x_c^i(j) - x_n^i(j-1) < -x_{\max} + 2x_{\min} \end{cases} \tag{3.18}$$

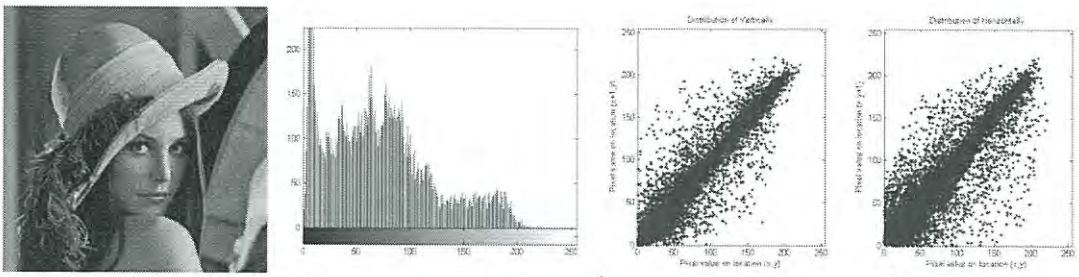


ภาพที่ 3.4 แผนภาพกระบวนการถอดรหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

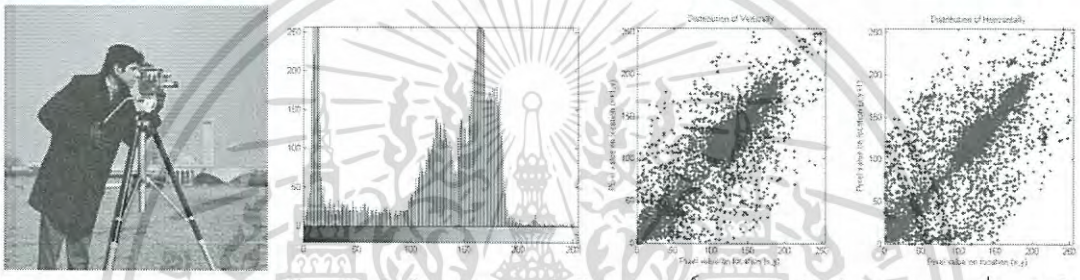
บทที่ 4
การทดสอบ และผลการทดสอบ

ในงานวิจัยนี้ได้ทำการทดสอบการเข้ารหัสภาพเฉดเทาขนาด 128 × 128 จุดภาพ จำนวน 3 ภาพ ได้แก่ Lena Cameraman และ Mandril ดังภาพที่ 4.1 ถึง ภาพที่ 4.3 ด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) แล้วทำการเปรียบเทียบประสิทธิผลของการเข้ารหัสภาพโดยใช้เครื่องมือต่าง ๆ ได้แก่ การวิเคราะห์ผลการเข้ารหัสภาพ การวิเคราะห์ฮิสโตแกรม การวิเคราะห์ข้อมูลเอนโทรปี การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์ การวิเคราะห์ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ ค่าเฉลี่ยการเปลี่ยนระดับสีเทา และ การวิเคราะห์ขนาดของกุญแจลับ

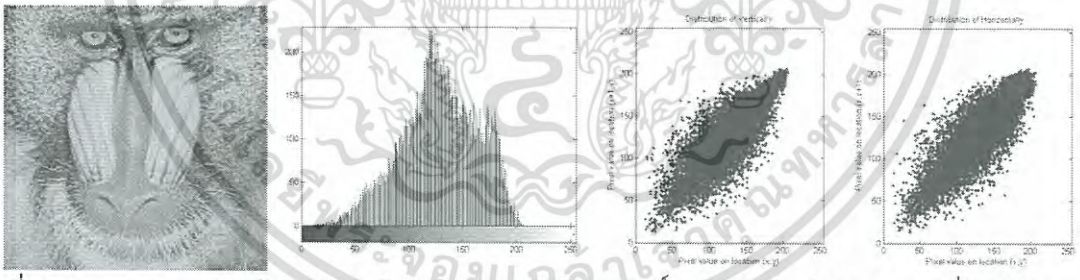
สำหรับการเข้ารหัสภาพ ด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ที่ใช้กุญแจลับ 3 ตัวในการเข้ารหัส และถอดรหัส ได้แก่ ค่าพารามิเตอร์ (r) ลำดับการวนซ้ำ (N) และจำนวนรอบในกระบวนการเข้ารหัส (J) ภายในวิทยานิพนธ์นี้ ใช้ค่าพารามิเตอร์ $r = 3.9$ เนื่องจากค่าพารามิเตอร์ในช่วง $3.57 < r < 4$ จะทำให้ระบบซึ่งใช้ลอจิสติกแมพนั้นเกิดความยุ่งเหยิง [32] สำหรับวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ที่มีกุญแจลับเพิ่มขึ้นมาได้แก่ลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) ในวิทยานิพนธ์ได้เลือกใช้ $\alpha = \frac{1}{2}$ และค่าพารามิเตอร์ $r = 5.9$ มาทดสอบ ซึ่งระบบที่ใช้รูปแบบลอจิสติกลำดับที่เป็นเศษส่วนจะเกิดความยุ่งเหยิงในช่วงค่าพารามิเตอร์ $5.61 < r < 6.35$ เมื่อใช้ $\alpha = \frac{1}{2}$ ดังตารางที่ 2.3 และวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ได้ใช้ค่ากุญแจจาก 2 วิธีเบื้องต้น ส่วนค่าลำดับการวนซ้ำ และ จำนวนรอบในกระบวนการเข้ารหัส ของทั้ง 3 วิธี จะใช้ค่าตั้งแต่ 1-10 เพื่อวิเคราะห์ผลที่เกิดขึ้นในแต่ละค่ากุญแจในแต่ละวิธี โดยตัวอย่างของกุญแจลับสรุปดังตารางที่ 4.1



ภาพที่ 4.1 ภาพ Lena ต้นฉบับ ฮิสโทแกรม และ สัมประสิทธิ์ความสัมพันธ์ของจุดภาพที่ติดกันในแนวแกนตั้ง และในแนวแกนนอน



ภาพที่ 4.2 ภาพ Cameraman ต้นฉบับ ฮิสโทแกรม และ สัมประสิทธิ์ความสัมพันธ์ของจุดภาพที่ติดกันในแนวแกนตั้ง และในแนวแกนนอน



ภาพที่ 4.3 ภาพ Mandril ต้นฉบับ ฮิสโทแกรม และ สัมประสิทธิ์ความสัมพันธ์ของจุดภาพที่ติดกันในแนวแกนตั้ง และในแนวแกนนอน

ตารางที่ 4.1 กุญแจลับที่ใช้ในกระบวนการเข้ารหัสและถอดรหัสแต่ละแบบ

กุญแจลับ	ค่าที่ใช้ทดสอบในแต่ละกระบวนการ			คำอธิบาย
	CML	FCML	APFCML	
r	3.9	5.90	5.90	ค่าพารามิเตอร์ของพลวัตความยุ่งเหยิง
N	1-10	1-10	1-10	ลำดับการวนซ้ำ
J	1-10	1-10	1-10	จำนวนรอบในกระบวนการเข้ารหัส
α	-	1/2	1/2	ลำดับการอนุพันธ์ที่เป็นเศษส่วนของพลวัตความยุ่งเหยิงสำหรับรูปแบบลอจิสติกลำดับที่เป็นเศษส่วน
r_G	-	-	3.9	ค่าพารามิเตอร์ของพลวัตความยุ่งเหยิงใช้กำหนดลำดับจุดภาพในการเข้ารหัส
x_{0G}	-	-	0.5	ค่าเงื่อนไขตั้งต้นของพลวัตความยุ่งเหยิงใช้กำหนดลำดับจุดภาพในการเข้ารหัส

4.1 การวิเคราะห์ผลการเข้ารหัสภาพ

เมื่อการทดสอบการเข้ารหัสภาพ ด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ในการทดสอบการเข้ารหัสภาพได้ใช้กุญแจลับตามตารางที่ 4.1 โดยเปลี่ยนกุญแจลับเฉพาะค่าลำดับการวนซ้ำ N และจำนวนรอบในกระบวนการเข้ารหัส J แล้วทำการสังเกตเปรียบเทียบ และวิเคราะห์ผลจากการเข้ารหัสด้วยตา

เมื่อนำภาพ Lena มาทดสอบการเข้ารหัสภาพ โดยใช้จำนวนรอบในกระบวนการเข้ารหัส $J=1$ และค่าลำดับการวนซ้ำ $N=1-4$ ด้วยกระบวนการเข้ารหัสวิธีต่าง ๆ ได้ผลดังภาพที่ 4.4 แล้วเมื่อเปลี่ยนจำนวนรอบในกระบวนการเข้ารหัสเป็น $J=2,3,4$ และ 5 ได้ผลลัพธ์ดังภาพที่ 4.5 ถึงภาพที่ 4.8 ตามลำดับ

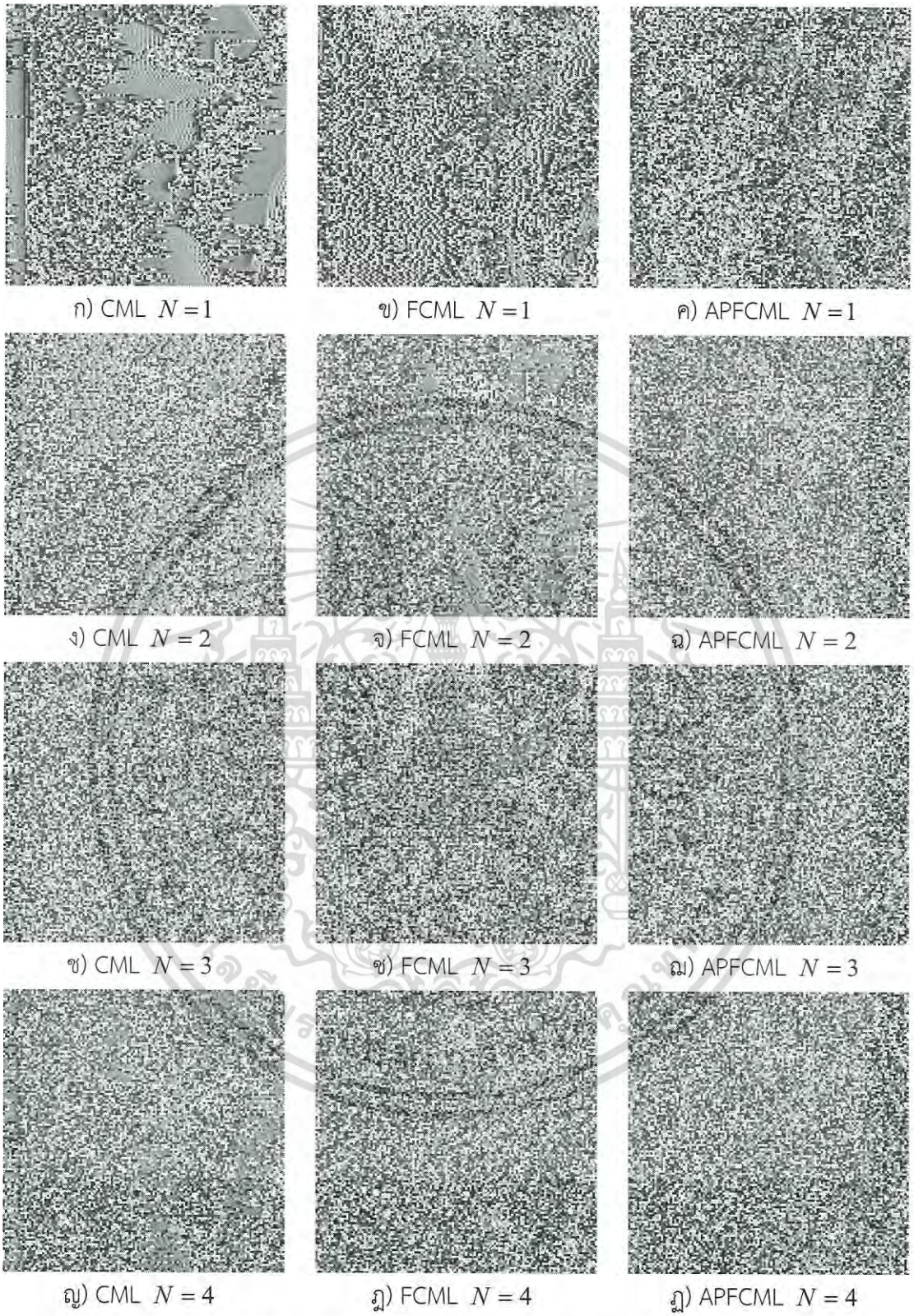
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.4 การเข้ารหัสภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=1$



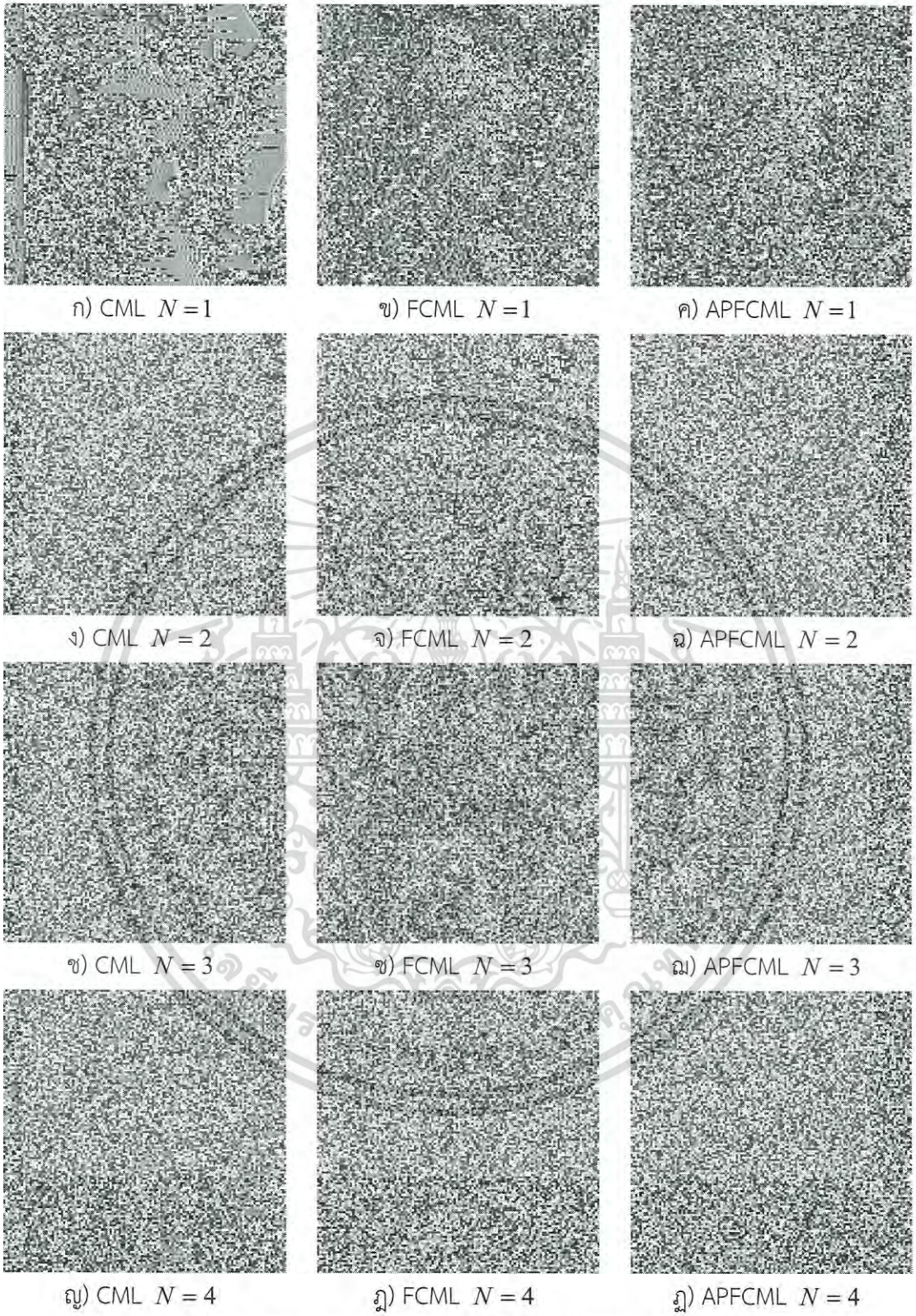
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.5 การเข้ารหัสภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=2$



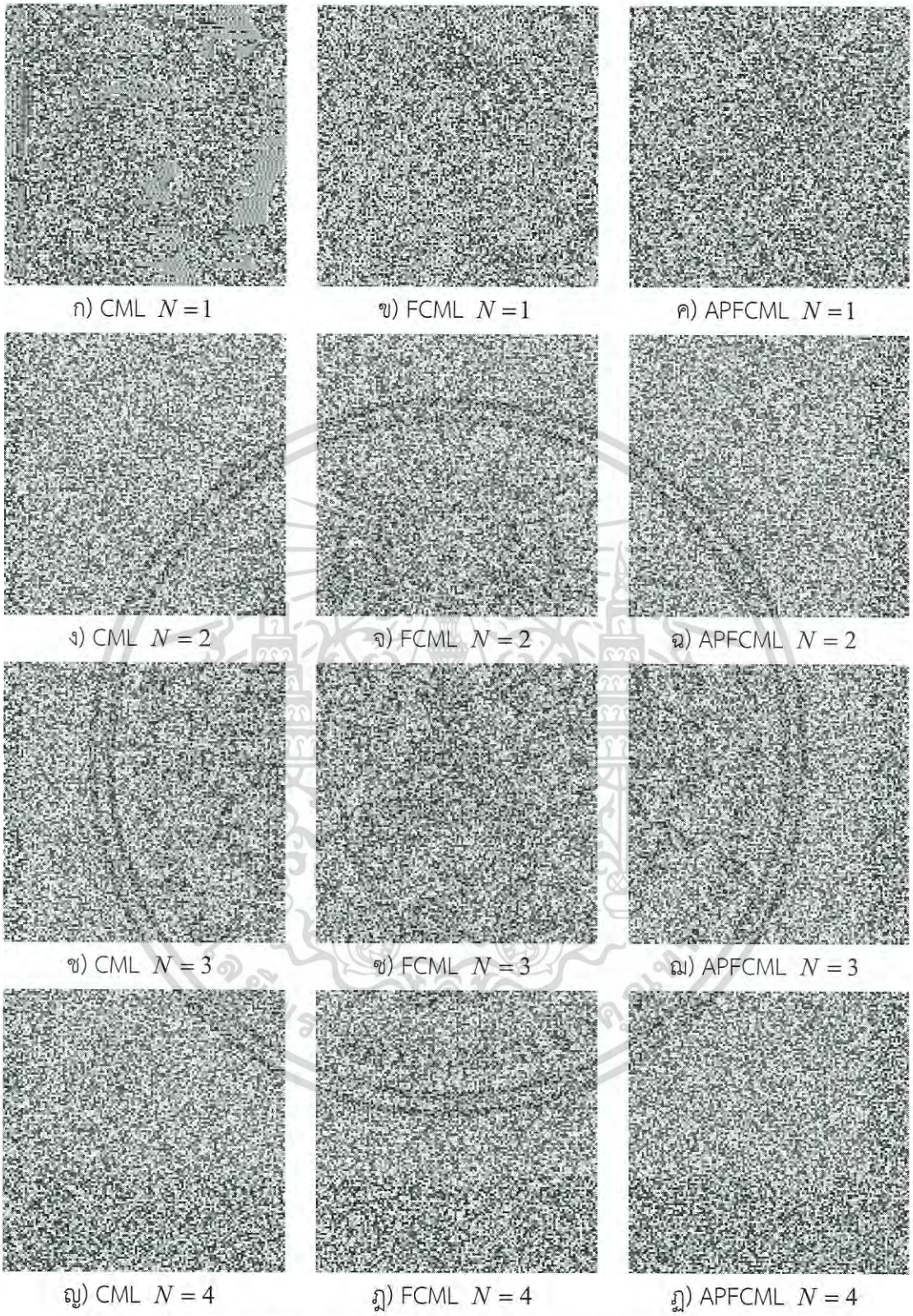
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.6 การเข้ารหัสภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=3$



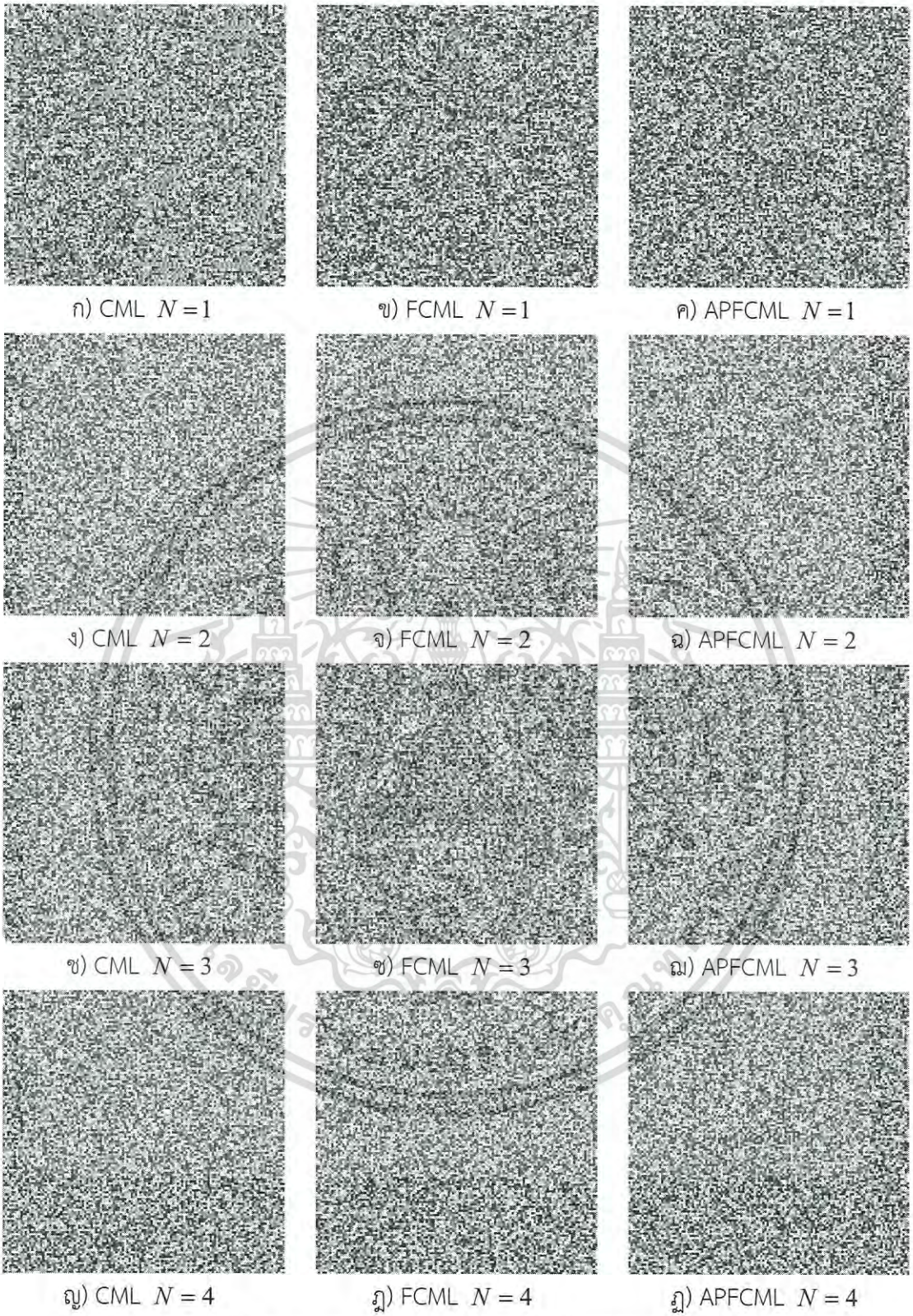
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.7 การเข้ารหัสภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=4$



ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.8 การเข้ารหัสภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=5$

ผลจากการทดลองการเข้ารหัสภาพ โดยใช้จำนวนรอบในกระบวนการเข้ารหัส $J=1$ ในภาพที่ 4.4 พบว่าเมื่อทำการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ที่ค่าลำดับการวนซ้ำ $N=1-4$ ยังปรากฏรายละเอียดของภาพต้นฉบับอยู่ ทว่าการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) จะเห็นรายละเอียดของภาพต้นฉบับน้อยกว่าอีกสองวิธี

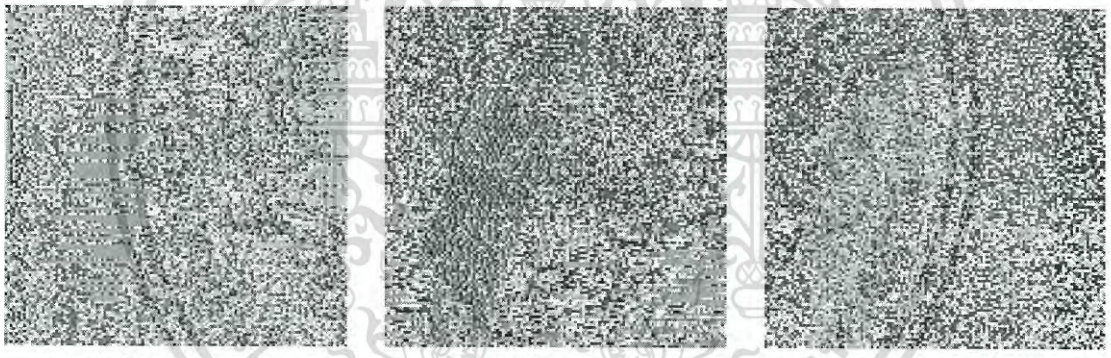
เมื่อทำการทดลองการเข้ารหัสภาพ โดยใช้จำนวนรอบในกระบวนการเข้ารหัส $J=2$ และ $J=3$ โดยใช้ค่าลำดับการวนซ้ำ $N=1$ พบว่ามีเพียงการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ที่ยังปรากฏรายละเอียดของภาพต้นฉบับอยู่เล็กน้อย ส่วนการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ไม่ปรากฏรายละเอียดของภาพต้นฉบับ ดังในภาพที่ 4.5 และ ภาพที่ 4.6 ซึ่งจากผลการใช้รหัสภาพสรุปได้ว่า การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) สามารถใช้งานจำนวนกุญแจลับได้มากกว่าอีกสองวิธี คือ เมื่อใช้ค่าลำดับการวนซ้ำ $N=1$ สามารถเริ่มใช้ได้ดีตั้งแต่ใช้จำนวนรอบในกระบวนการเข้ารหัสตั้งแต่ (J) 2 ขึ้นไป ซึ่งอีก 2 วิธียังไม่สามารถซ่อนภาพต้นฉบับได้หมด ส่งผลให้ช่วงการเลือกใช้งานพารามิเตอร์ได้หลากหลายเพิ่มขึ้น

ผลลัพธ์จากการเข้ารหัสภาพ ด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ทั้ง 3 วิธี จะไม่ปรากฏรายละเอียดของภาพต้นฉบับเลย เมื่อทำการทดลองการเข้ารหัสภาพ โดยใช้จำนวนรอบในกระบวนการเข้ารหัส $J=4$ และ $J=5$ ดังในภาพที่ 4.7 และ ภาพที่ 4.8

และเมื่อนำภาพ Cameraman มาทดสอบการเข้ารหัสภาพ เช่นเดียวกันภาพ Lena โดยการเข้ารหัสภาพ Cameraman ด้วยจำนวนรอบในกระบวนการเข้ารหัสเป็น $J=1,2,3,4$ และ 5 ได้ผลลัพธ์ดังภาพที่ 4.9 ถึงภาพที่ 4.13 และการเข้ารหัสภาพ Mandril ด้วยจำนวนรอบในกระบวนการเข้ารหัสเป็น $J=1,2,3,4$ และ 5 ได้ผลลัพธ์ดังภาพที่ 4.14 ถึงภาพที่ 4.18 ตามลำดับ

ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

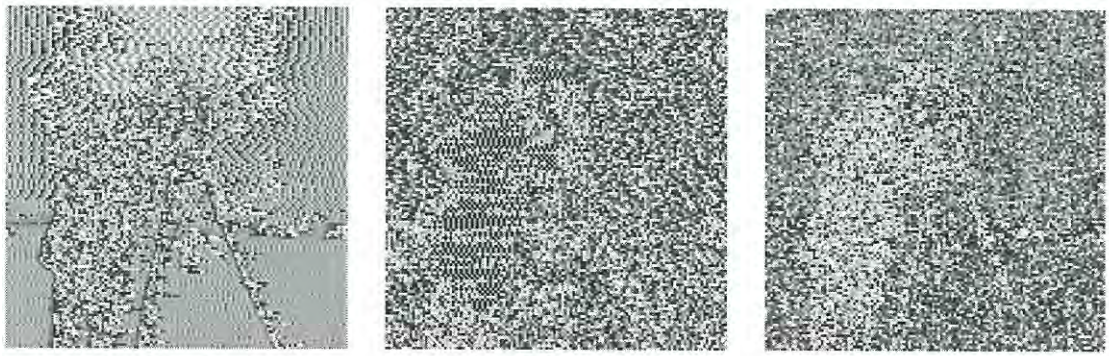
ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$



ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

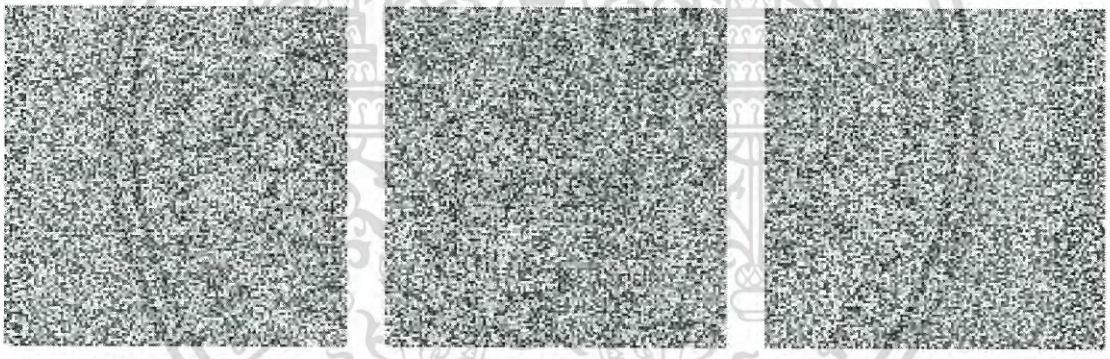
ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.9 การเข้ารหัสภาพ Cameraman ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=1$



ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

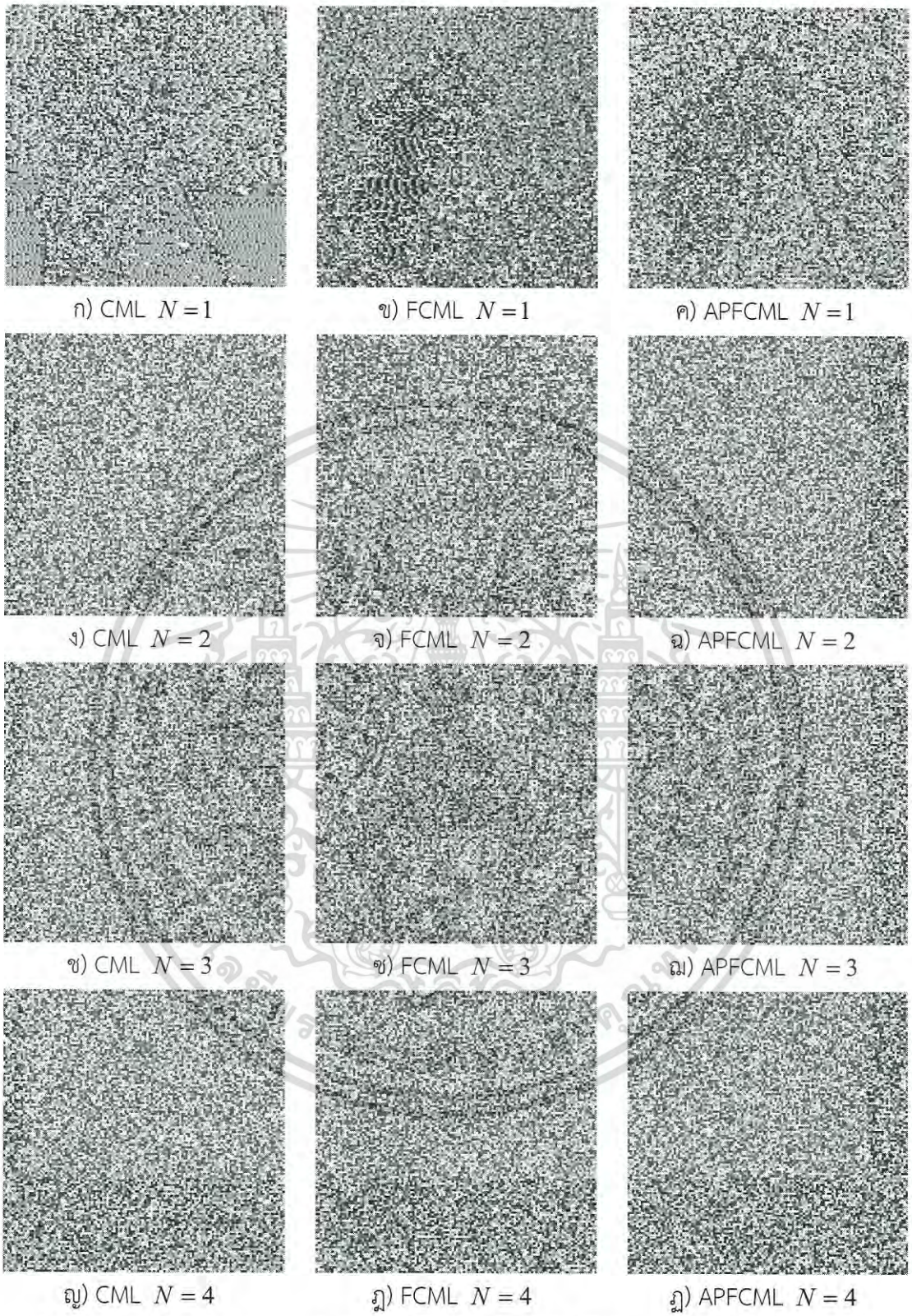
ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$



ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.10 การเข้ารหัสภาพ Cameraman ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=2$



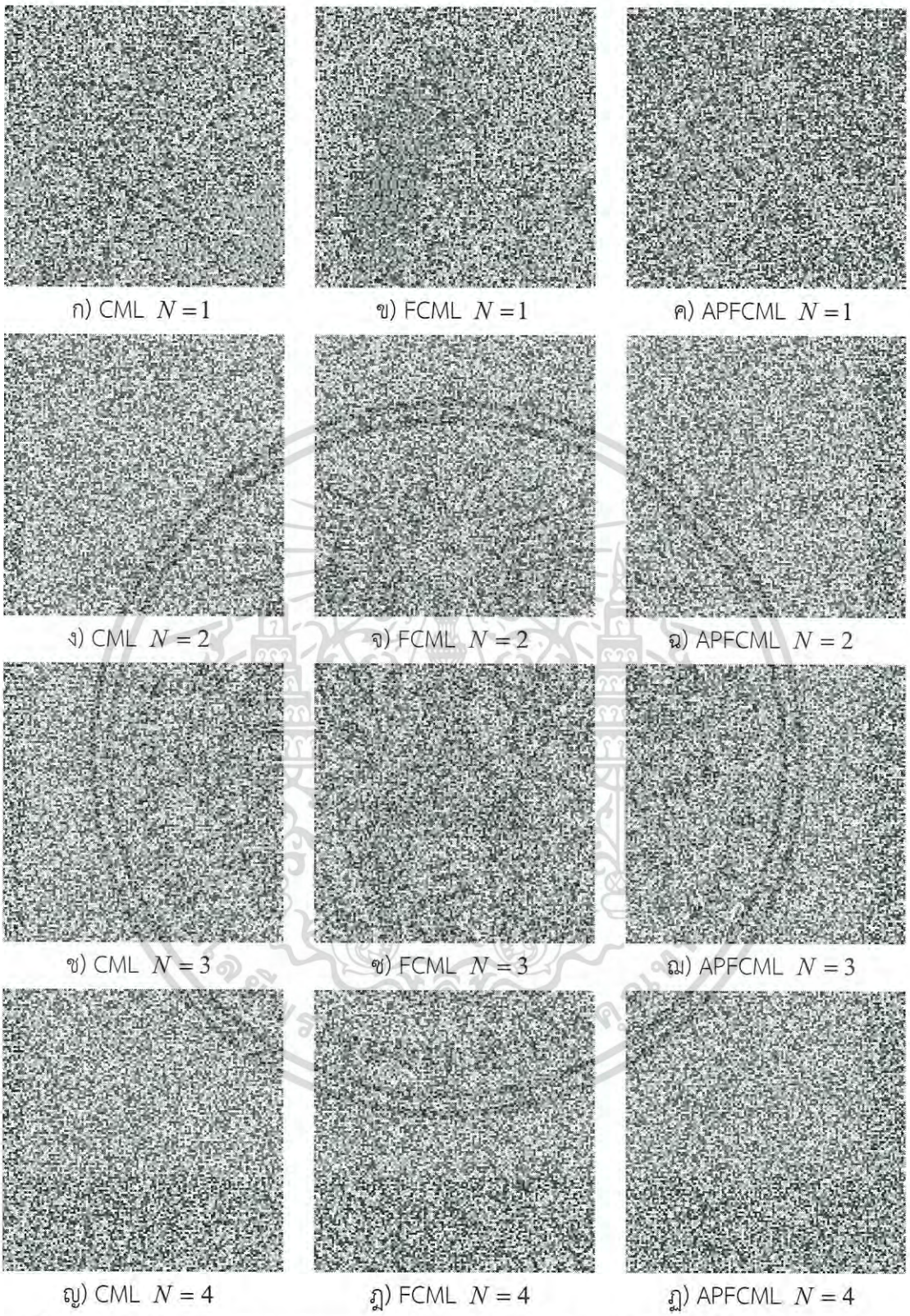
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.11 การเข้ารหัสภาพ Cameraman ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=3$



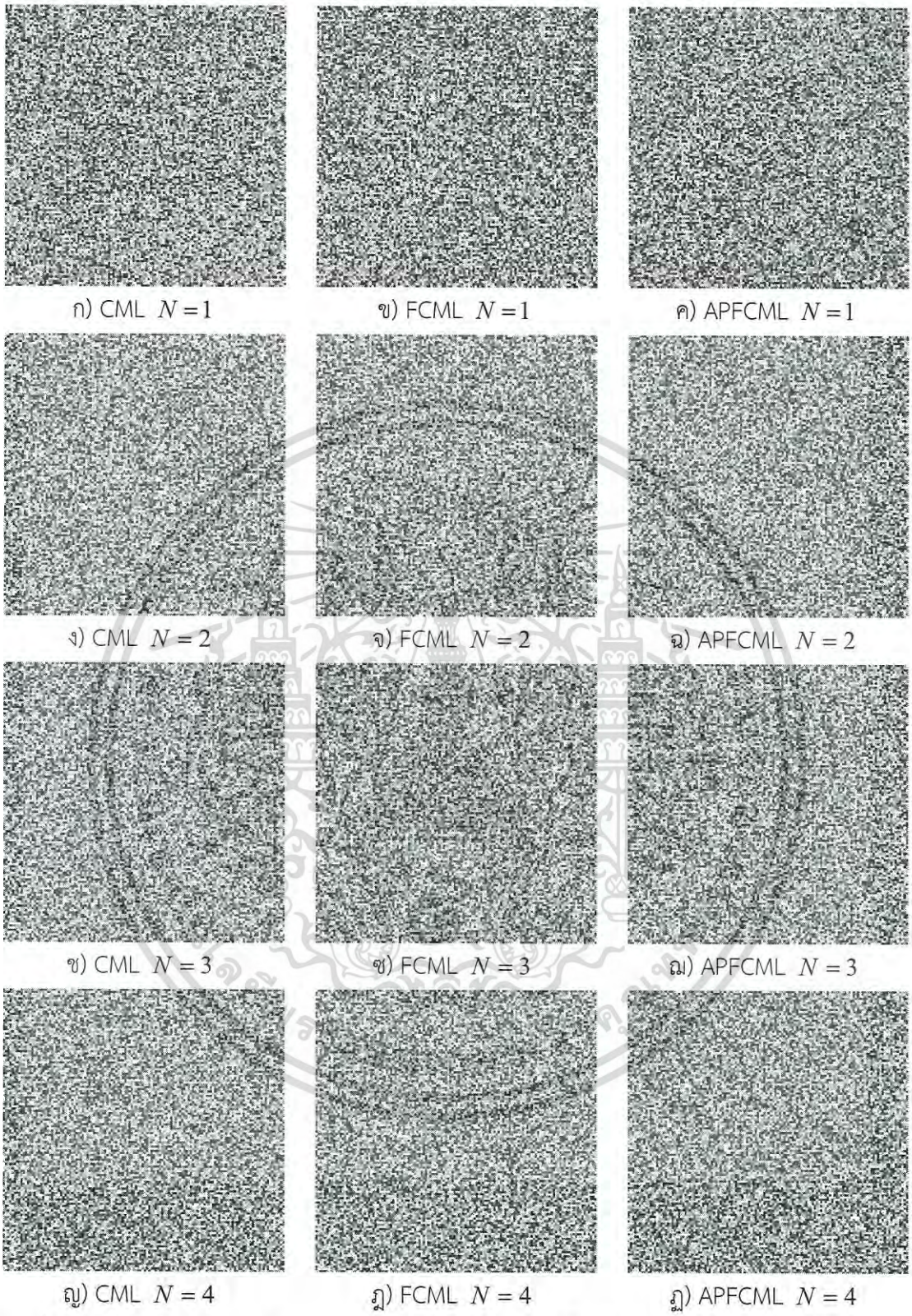
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.12 การเข้ารหัสภาพ Cameraman ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=4$



ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

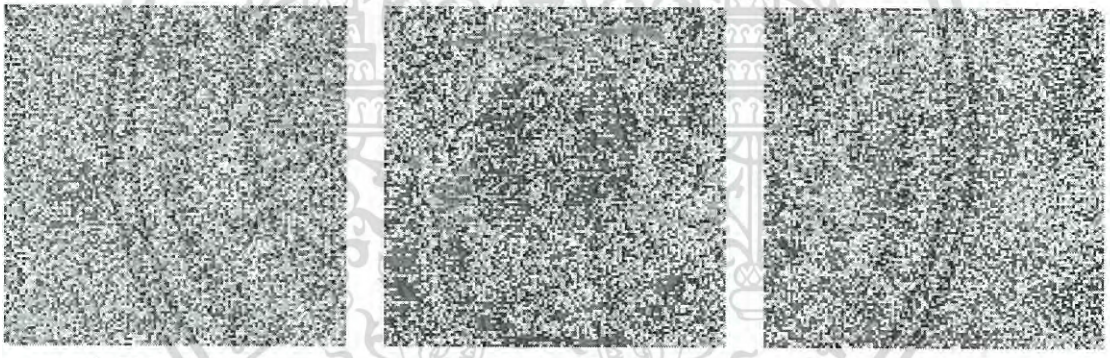
ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.13 การเข้ารหัสภาพ Cameraman ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=5$

ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

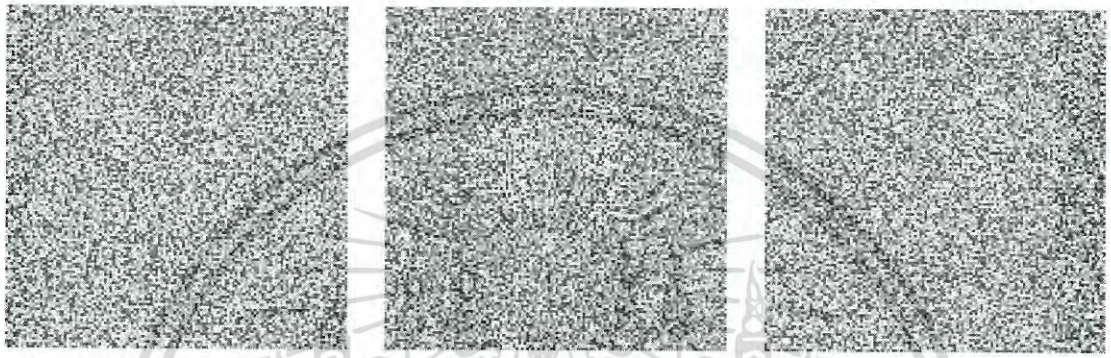


ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

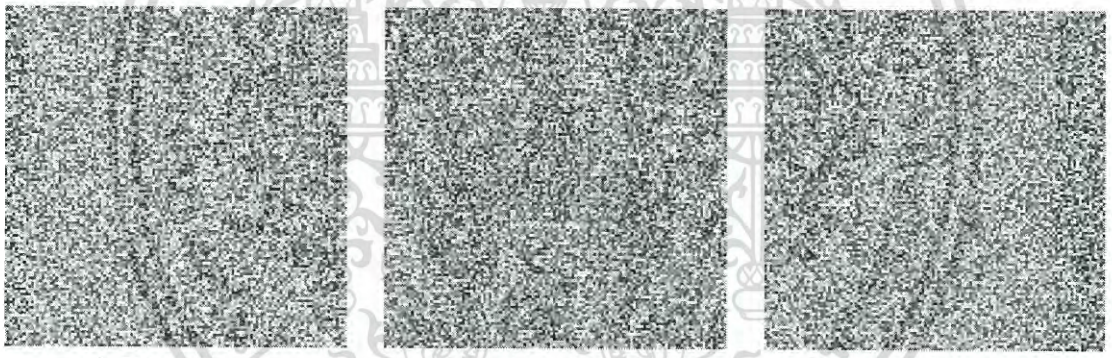
ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.14 การเข้ารหัสภาพ Mandril ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=1$

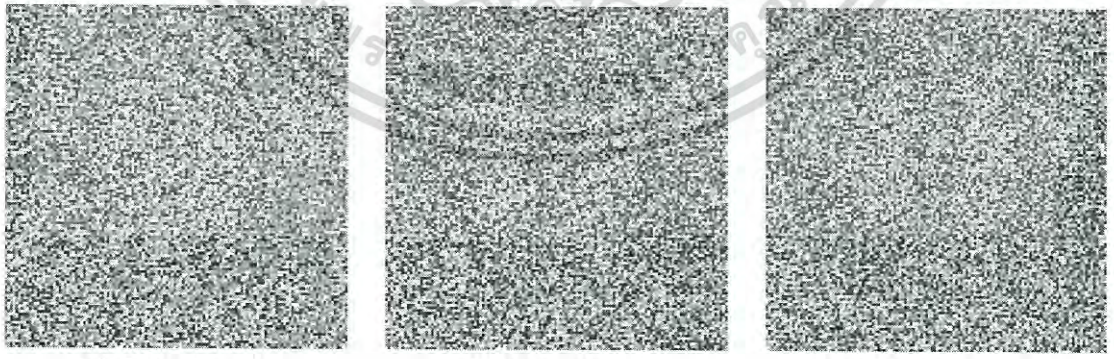
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$



ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

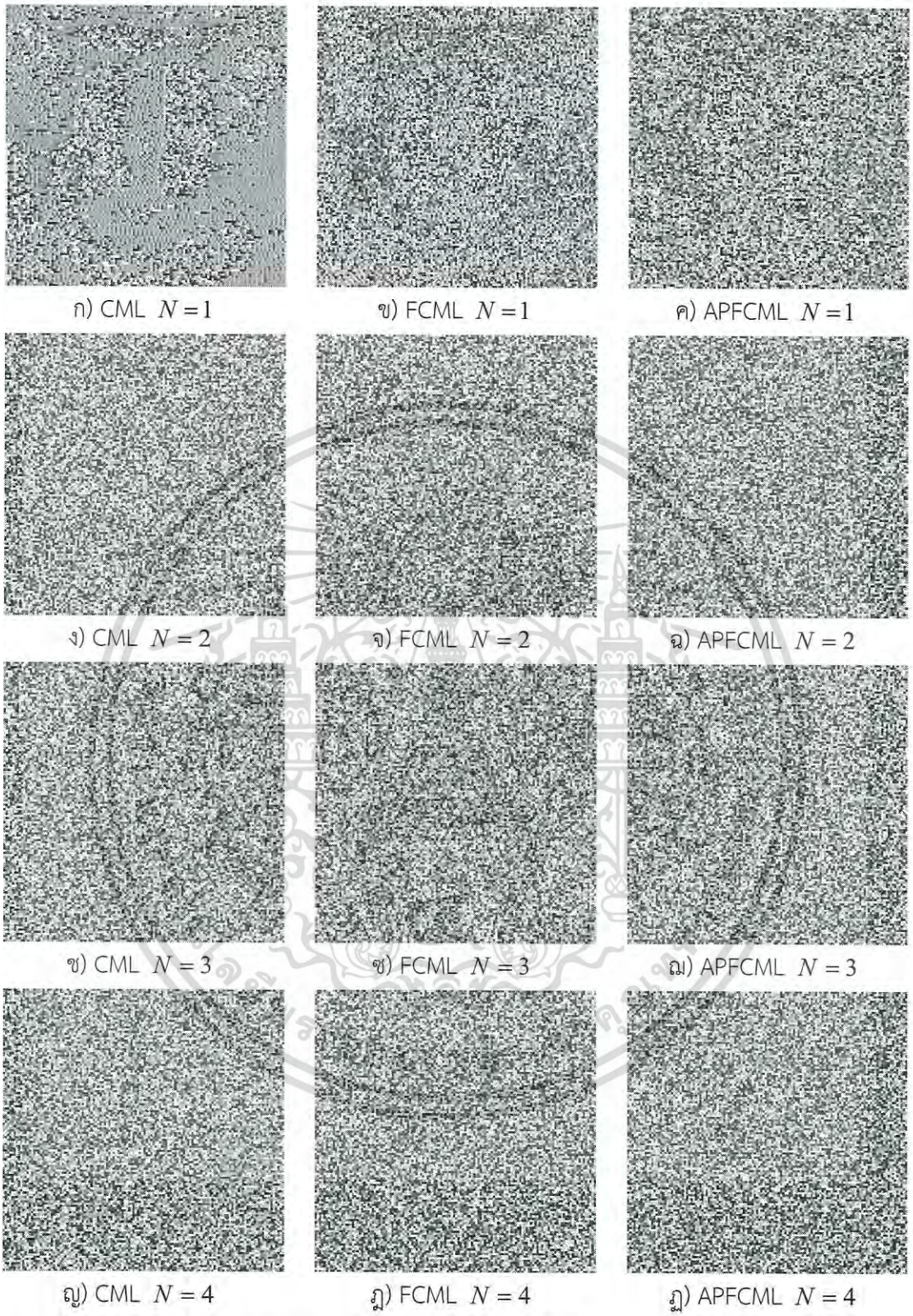


ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$



ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.15 การเข้ารหัสภาพ Mandril ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=2$



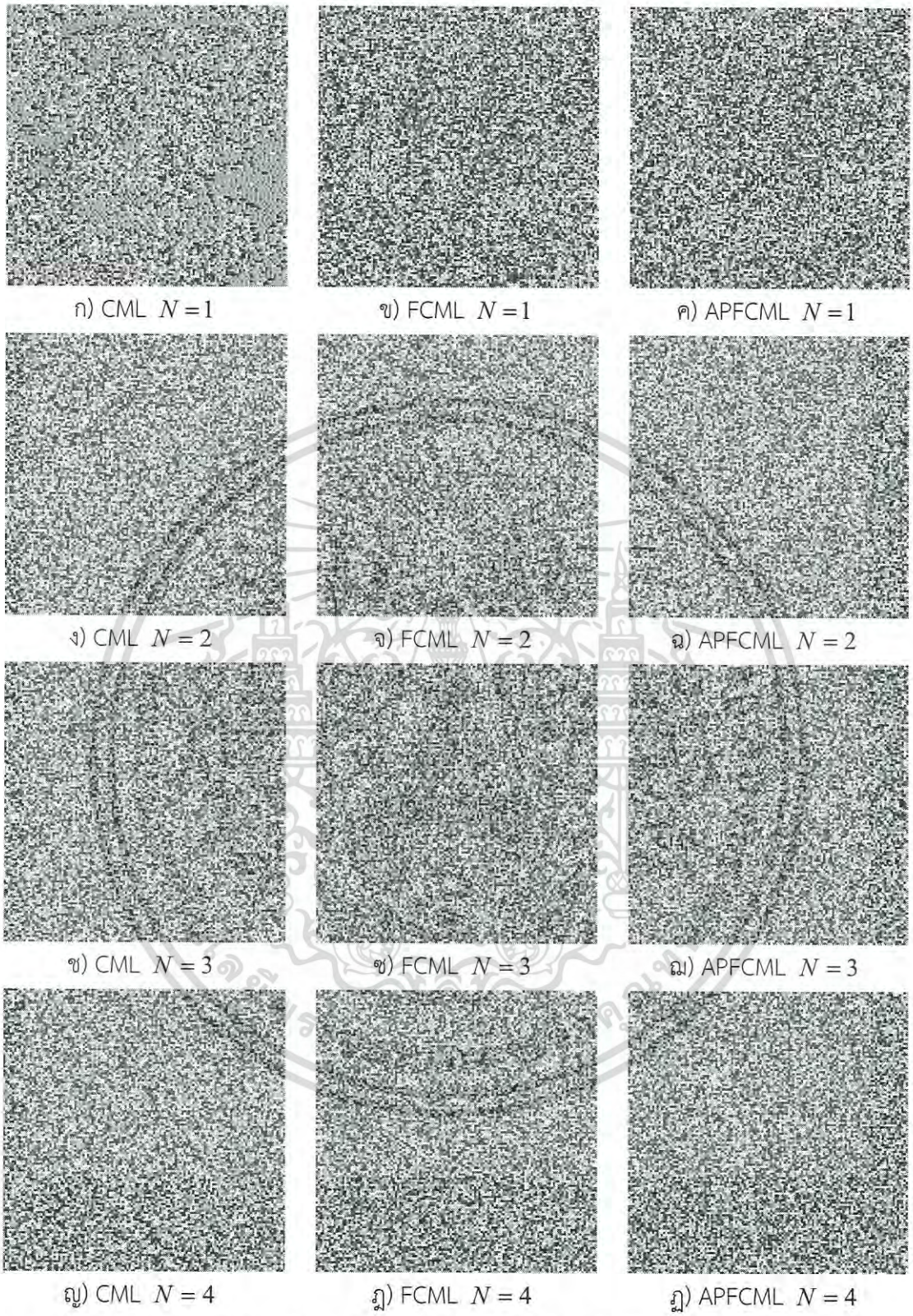
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.16 การเข้ารหัสภาพ Mandril ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=3$



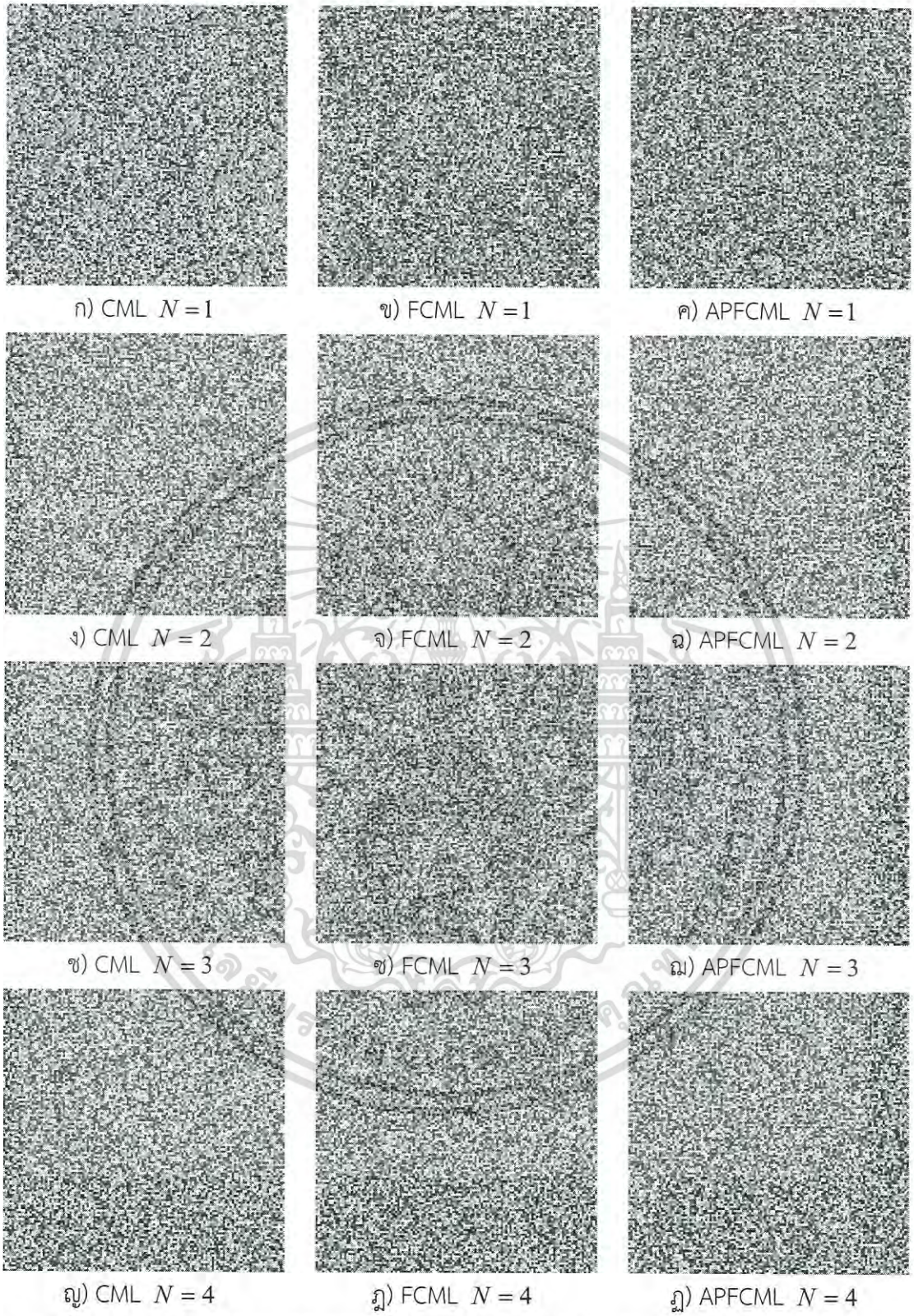
ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.17 การเข้ารหัสภาพ Mandril ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=4$



ก) CML $N=1$ ข) FCML $N=1$ ค) APFCML $N=1$

ง) CML $N=2$ จ) FCML $N=2$ ฉ) APFCML $N=2$

ช) CML $N=3$ ซ) FCML $N=3$ ฌ) APFCML $N=3$

ญ) CML $N=4$ ฎ) FCML $N=4$ ฏ) APFCML $N=4$

ภาพที่ 4.18 การเข้ารหัสภาพ Mandril ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=5$

ผลจากการเข้ารหัสผ่าน Cameraman ในภาพที่ 4.9 ถึงภาพที่ 4.13 และการเข้ารหัสภาพ Mandril ในภาพที่ 4.14 ถึงภาพที่ 4.18 มีแนวโน้มเช่นเดียวกับการเข้ารหัสภาพ Lena คือเมื่อกำหนดค่าจำนวนรอบในกระบวนการเข้ารหัส $J=1$ พบว่า การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ให้ผลการเข้ารหัสที่ด้อยกว่า การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) เนื่องจากยังคงมีรายละเอียดของภาพต้นฉบับปรากฏอยู่ และเมื่อกำหนดค่าจำนวนรอบในกระบวนการเข้ารหัส J มากขึ้น ผลจากการเข้ารหัสจะซ่อนภาพต้นฉบับได้มากขึ้น โดยเมื่อพิจารณาจากการใช้ค่าลำดับการวนซ้ำ N การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) จะซ่อนภาพได้ดีกว่าอีกสองวิธี

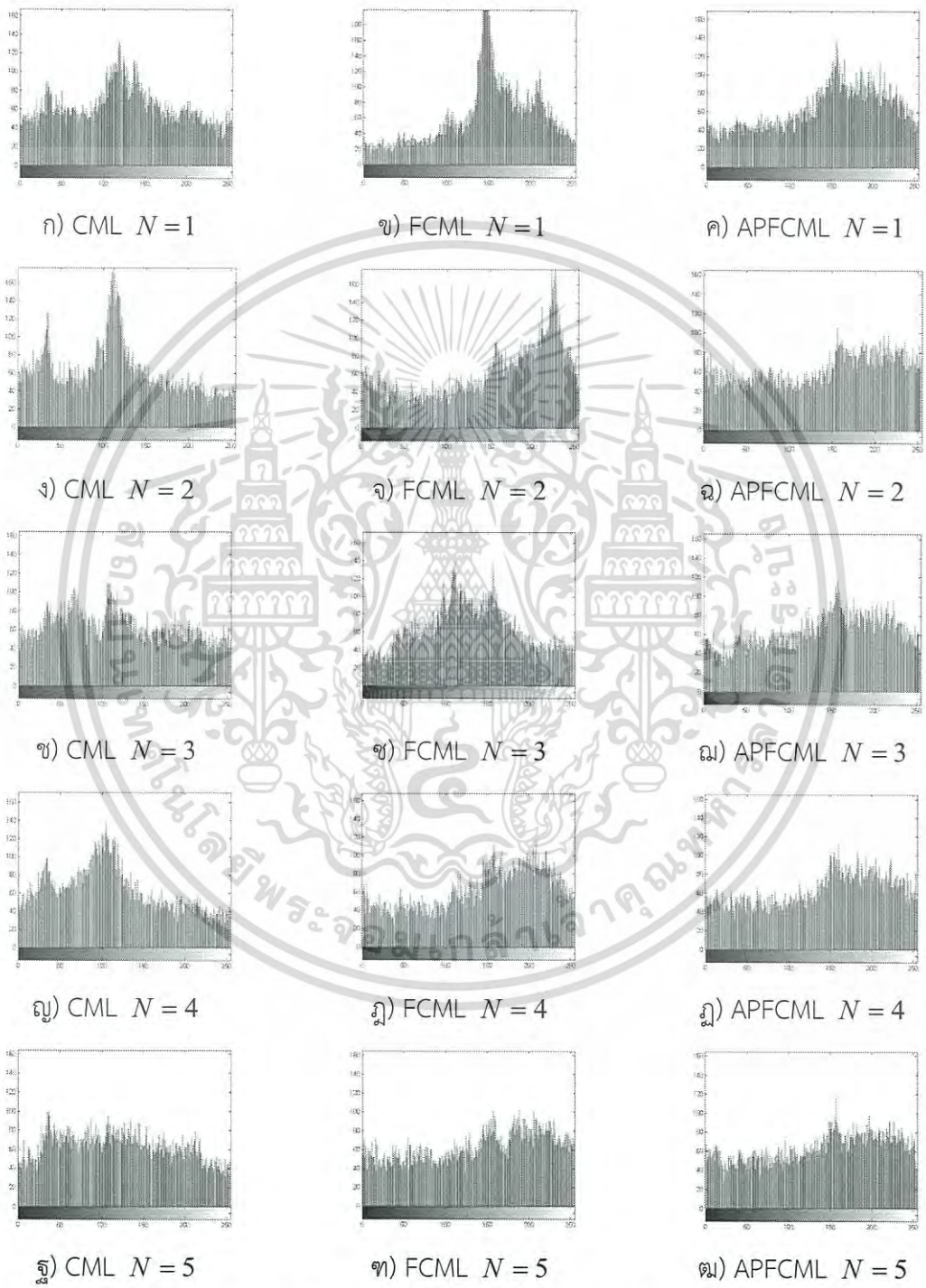
4.2 การวิเคราะห์ฮิสโตแกรม

ฮิสโทแกรมของภาพเป็นการแสดงการกระจายตัวของระดับความเข้มแสงภายในภาพ ซึ่งภาพที่ผ่านการเข้ารหัสควรมีการกระจายตัวเป็นแบบเอกรูป (Uniform Distribution) เพื่อความปลอดภัยจากการโจมตีโดยอาศัยการวิเคราะห์ข้อมูลทางสถิติในภาพ การทดสอบนี้แสดงฮิสโทแกรมของภาพ Lena ที่ผ่านการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ด้วยกุญแจลับตามตารางที่ 4.1 โดยทดลองเปลี่ยนค่ากุญแจลับเฉพาะจำนวนรอบในกระบวนการเข้ารหัส $J=1$ กับ 2 ค่าลำดับการวนซ้ำ N ตั้งแต่ 1 ถึง 5 ดังภาพที่ 4.19 และ ภาพที่ 4.20

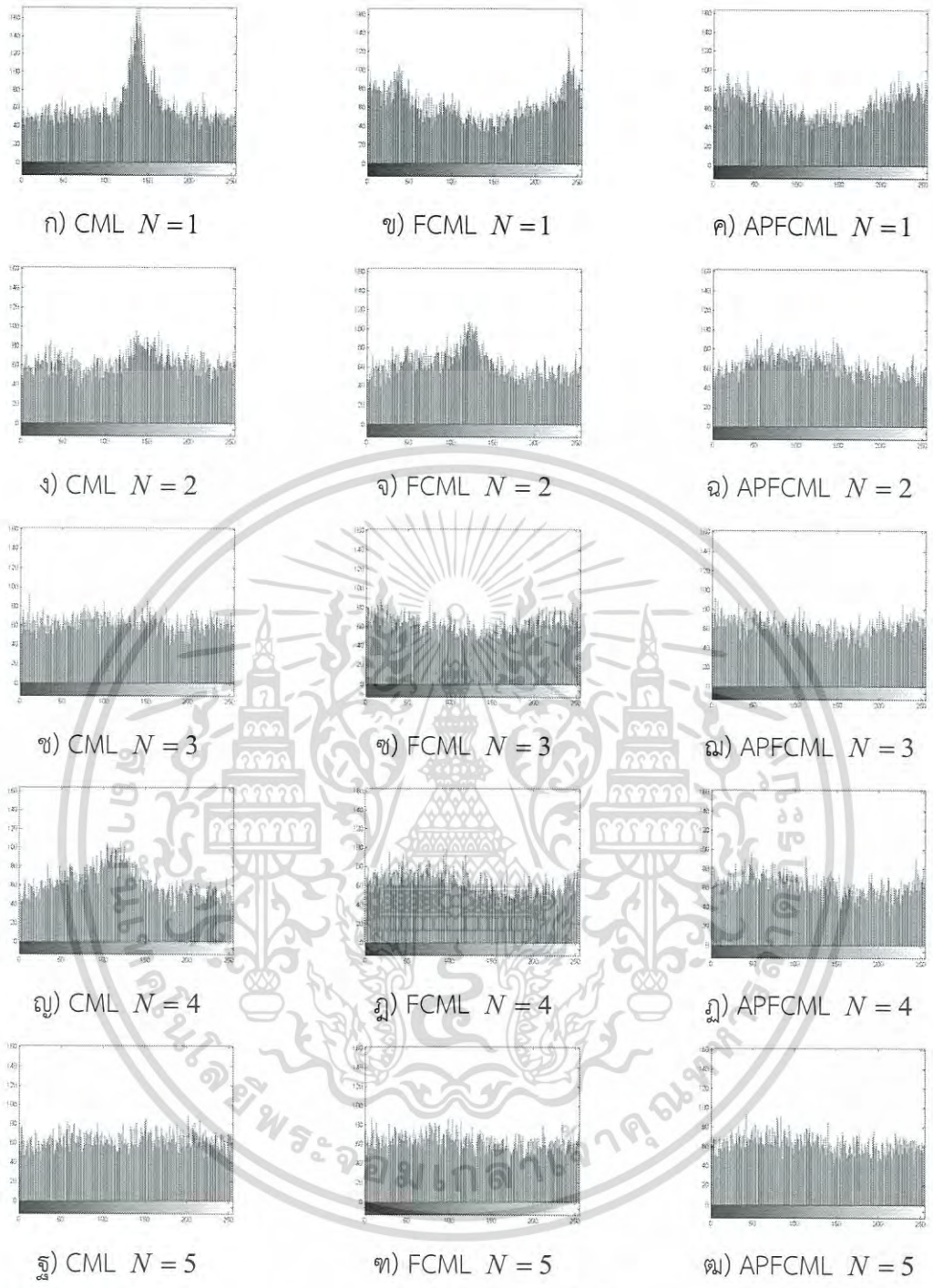
เมื่อพิจารณาฮิสโทแกรมของภาพที่เข้ารหัส โดยใช้จำนวนรอบในกระบวนการเข้ารหัส $J=1$ พบว่าการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีการกระจายตัวใกล้เคียงกับแบบเอกรูปมากกว่าการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ดังภาพที่ 4.19

และเมื่อใช้จำนวนรอบในกระบวนการเข้ารหัส $J=2$ การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) มีแนวโน้มการกระจายตัวเป็นแบบเอกรูป เมื่อค่าลำดับการวนซ้ำ N เพิ่มขึ้น โดยที่การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีการกระจายตัวเป็นแบบเอกรูปเริ่มตั้งแต่ ค่าลำดับการวนซ้ำ $N=2$ ดังภาพที่ 4.20

จากผลฮิสโทแกรมที่ได้สรุปได้ว่า การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) สามารถเริ่มใช้งานได้ตั้งแต่ใช้จำนวนรอบในกระบวนการเข้ารหัส (J) ตั้งแต่ 2 ขึ้นไป



ภาพที่ 4.19 ฮิสโทแกรมของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=1$



ภาพที่ 4.20 ฮิสโทแกรมของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J=2$

4.3 การวิเคราะห์ข้อมูลเอนโทรปี

ผลการทดสอบการเข้ารหัสภาพ แสดงถึงความสามารถในการซ่อนข้อมูลภาพต้นฉบับของการเข้ารหัสภาพ และการแสดงการกระจายตัวเป็นแบบเอกรูปของภาพที่ผ่านการเข้ารหัส สามารถแสดงความปลอดภัยจากการโจมตีโดยอาศัยการวิเคราะห์ข้อมูลทางสถิติ ทว่ายังต้องอาศัยการสังเกตซึ่งขึ้นอยู่กับบุคคลที่พิจารณาผลลัพธ์ ดังนั้นจึงนำข้อมูลเอนโทรปีซึ่งเป็นข้อมูลทฤษฎีทางคณิตศาสตร์ ซึ่งบ่งบอกความไม่เป็นระเบียบของข้อมูลได้ด้วยตัวเลข เมื่อข้อมูลเอนโทรปีมีค่าสูงแสดงถึงความปลอดภัยในข้อมูลภาพที่ผ่านกระบวนการเข้ารหัสมีมากขึ้น เนื่องจากเกิดความกระจายตัว หรือความไม่เป็นระบียบมากขึ้น โดยคำนวณค่าข้อมูลเอนโทรปี ได้จากสมการ (4.1)

$$H(m)=\sum_{i=0}^{2^N-1} p(m_i)\times \log_2 \frac{1}{p(m_i)} \tag{4.1}$$

เมื่อ $H(m)$ คือ เอนโทรปีของข้อมูล m ทั้งหมด

$p(m_i)$ คือ ความน่าจะเป็นที่เกิดค่าระดับความเข้มสี m_i

m_i คือ ระดับความเข้มสีของจุดภาพ

เมื่อทำการคำนวณหาข้อมูลเอนโทรปีของภาพ Lena ที่ผ่านการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ด้วยกุญแจลับตามตารางที่ 4.1 ได้ผลดังตารางที่ 4.2 ถึงตารางที่ 4.4

ตารางที่ 4.2 ข้อมูลเอนโทรปีของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	*7.9404*	*7.9067*	*7.9330*	*7.9653*	7.9840	7.9873	7.9876	7.9852	7.9887	7.9869
N=2	*7.8709*	*7.9782*	7.9889	7.9892	7.9863	7.9870	7.9880	7.9866	7.9896	7.9857
N=3	*7.9613*	7.9871	7.9865	7.9877	7.9871	7.9863	7.9884	7.9859	7.9885	7.9853
N=4	*7.9022*	*7.9615*	*7.9800*	7.9882	7.9883	7.9883	7.9882	7.9870	7.9875	7.9871
N=5	*7.9644*	7.9863	7.9876	7.9880	7.9866	7.9880	7.9889	7.9881	7.9886	7.9857
N=6	*7.9549*	7.9866	7.9874	7.9878	7.9868	7.9878	7.9872	7.9865	7.9881	7.9885
N=7	*7.9569*	7.9876	7.9864	7.9854	7.9870	7.9872	7.9879	7.9866	7.9863	7.9881
N=8	*7.9657*	7.9859	7.9883	7.9882	7.9874	7.9856	7.9882	7.9865	7.9877	7.9870
N=9	*7.9493*	7.9844	7.9879	7.9854	7.9883	7.9868	7.9880	7.9877	7.9884	7.9881
N=10	*7.9604*	7.9862	7.9883	7.9854	7.9875	7.9857	7.9860	7.9885	7.9859	7.9889

ตารางที่ 4.3 ข้อมูลเอนโทรปีของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	*7.6842*	*7.9430*	*7.9562*	*7.9774*	7.9831	7.9871	7.9870	7.9863	7.9858	7.9880
N=2	*7.8553*	*7.9656*	*7.9800*	7.9854	7.9859	7.9857	7.9874	7.9858	7.9886	7.9870
N=3	*7.8918*	7.9829	7.9856	7.9878	7.9872	7.9885	7.9862	7.9886	7.9856	7.9876
N=4	*7.9219*	*7.9753*	7.9878	7.9862	7.9868	7.9864	7.9894	7.9867	7.9879	7.9891
N=5	*7.9599*	7.9847	7.9857	7.9858	7.9856	7.9872	7.9869	7.9878	7.9865	7.9846
N=6	*7.9414*	*7.9799*	7.9857	7.9877	7.9876	7.9860	7.9864	7.9875	7.9869	7.9891
N=7	*7.9500*	7.9863	7.9898	7.9863	7.9872	7.9875	7.9878	7.9876	7.9866	7.9880
N=8	*7.9493*	7.9837	7.9890	7.9901	7.9856	7.9886	7.9883	7.9885	7.9884	7.9871
N=9	*7.9485*	7.9840	7.9877	7.9871	7.9889	7.9872	7.9857	7.9891	7.9882	7.9891
N=10	*7.9563*	7.9844	7.9885	7.9886	7.9875	7.9891	7.9886	7.9883	7.9868	7.9888

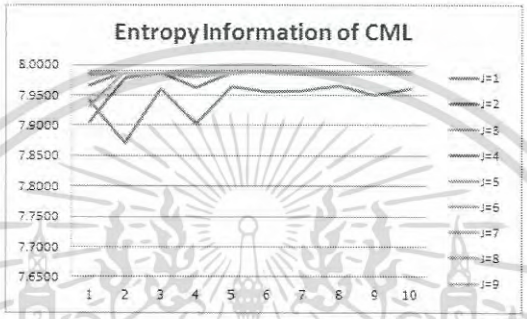
ตารางที่ 4.4 ข้อมูลเอนโทรปีของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	*7.9147*	*7.9643*	*7.9792*	7.9833	7.9855	7.9891	7.9874	7.9879	7.9888	7.9871
N=2	*7.9585*	*7.9790*	7.9854	7.9873	7.9868	7.9886	7.9877	7.9886	7.9859	7.9862
N=3	*7.9495*	7.9822	7.9880	7.9866	7.9864	7.9863	7.9888	7.9888	7.9894	7.9872
N=4	*7.9516*	*7.9795*	7.9854	7.9866	7.9877	7.9883	7.9878	7.9870	7.9875	7.9904
N=5	*7.9646*	7.9850	7.9893	7.9889	7.9871	7.9889	7.9888	7.9851	7.9876	7.9868
N=6	*7.9466*	7.9814	7.9853	7.9855	7.9866	7.9885	7.9869	7.9879	7.9890	7.9882
N=7	*7.9556*	7.9856	7.9875	7.9878	7.9871	7.9886	7.9863	7.9889	7.9872	7.9890
N=8	*7.9544*	7.9830	7.9859	7.9873	7.9886	7.9884	7.9860	7.9868	7.9880	7.9844
N=9	*7.9529*	7.9842	7.9859	7.9899	7.9859	7.9879	7.9883	7.9872	7.9881	7.9882
N=10	*7.9555*	7.9848	7.9861	7.9877	7.9868	7.9877	7.9876	7.9867	7.9892	7.9854

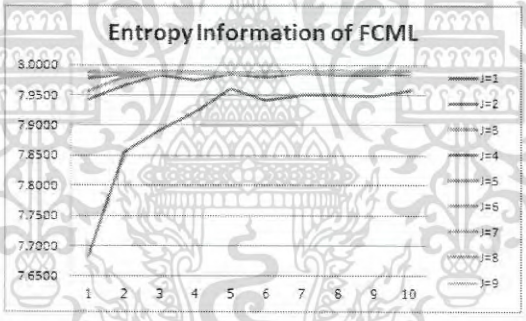
จากตารางที่ 4.2 ถึงตารางที่ 4.4 เป็นข้อมูลเอนโทรปีของภาพ Lena ที่เข้ารหัสด้วยวิธีต่าง ๆ โดยข้อมูลเอนโทรปีที่มีค่ามากแสดงถึงการกระจายตัวของข้อมูลภาพที่มากขึ้น ซึ่งแสดงถึงผลการเข้ารหัสที่ดีขึ้น (สำหรับข้อมูลข้อมูลเอนโทรที่เป็นตัวเอียง และขีดเส้นใต้แสดงถึงข้อมูลเอนโทรที่น้อยเกินค่าเฉลี่ยทั้งหมด) สามารถนำข้อมูลเอนโทรปีมาสรุปเป็นแผนภูมิได้ดังภาพที่ 4.21

เมื่อพิจาณาแผนภูมิจากภาพที่ 4.21 เมื่อ $J=1$ พบว่าข้อมูลเอนโทรปีของภาพที่เกิดจากการเข้ารหัสภาพด้วย วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ที่ $N=1$

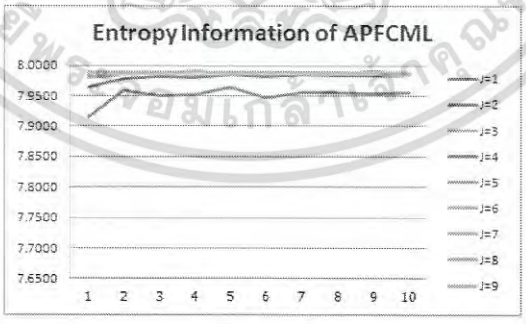
ถึง 3 มีค่าเอนโทรปีน้อยกว่าวิธีการอื่น ซึ่งสอดคล้องกับผลการเข้ารหัสภาพ Lena ดังภาพที่ 4.4 คือมีรายละเอียดของภาพต้นฉบับอยู่มากกว่าค่า N อื่น ๆ และเมื่อพิจารณาที่ค่า $J = 2$ ค่าเอนโทรปีของภาพที่เกิดจากการเข้ารหัสภาพด้วย วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีค่าเอนโทรปีมากกว่าวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ซึ่งสอดคล้องกับผลการเข้ารหัสภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแต่ละวิธี เมื่อ $J = 2$ ดังภาพที่ 4.5



ก)



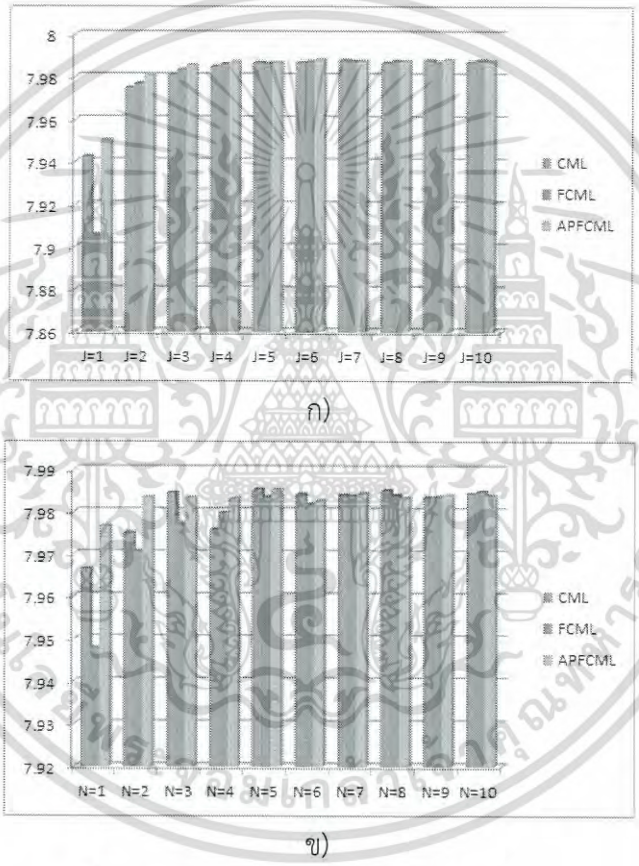
ข)



ค)

ภาพที่ 4.21 แผนภูมิข้อมูลเอนโทรปีของภาพ Lena ที่ผ่านการเข้ารหัสภาพแต่ละวิธี
ก) วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)
ข) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)
ค) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

จากแผนภูมิข้อมูลเอนโทรปีภาพ Lena ที่ผ่านการเข้ารหัสภาพแต่ละวิธี ในภาพที่ 4.21 เมื่อนำมาวิเคราะห์โดยพิจารณาค่าเฉลี่ยข้อมูลเอนโทรปีที่ค่า J และ N แต่ละค่าของทั้ง 3 วิธีการเข้ารหัสภาพได้ผลดังแผนภูมิในภาพที่ 4.22 โดยค่าเฉลี่ยข้อมูลเอนโทรปีทั้งหมดของการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) มีค่าเป็น 7.98078805 ค่าเฉลี่ยข้อมูลเอนโทรปีทั้งหมดของการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) มีค่าเป็น 7.97765078 และ ค่าเฉลี่ยข้อมูลเอนโทรปีทั้งหมดของการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีค่าเป็น 7.98296514



ภาพที่ 4.22 แผนภูมิค่าเฉลี่ยข้อมูลเอนโทรปี

ก) พิจารณาจากค่าจำนวนรอบในกระบวนการเข้ารหัส (J) เมื่อใช้ $N = 1$ ถึง 10

ข) พิจารณาจากค่าลำดับการวนซ้ำ (N) เมื่อใช้ $J = 1$ ถึง 10

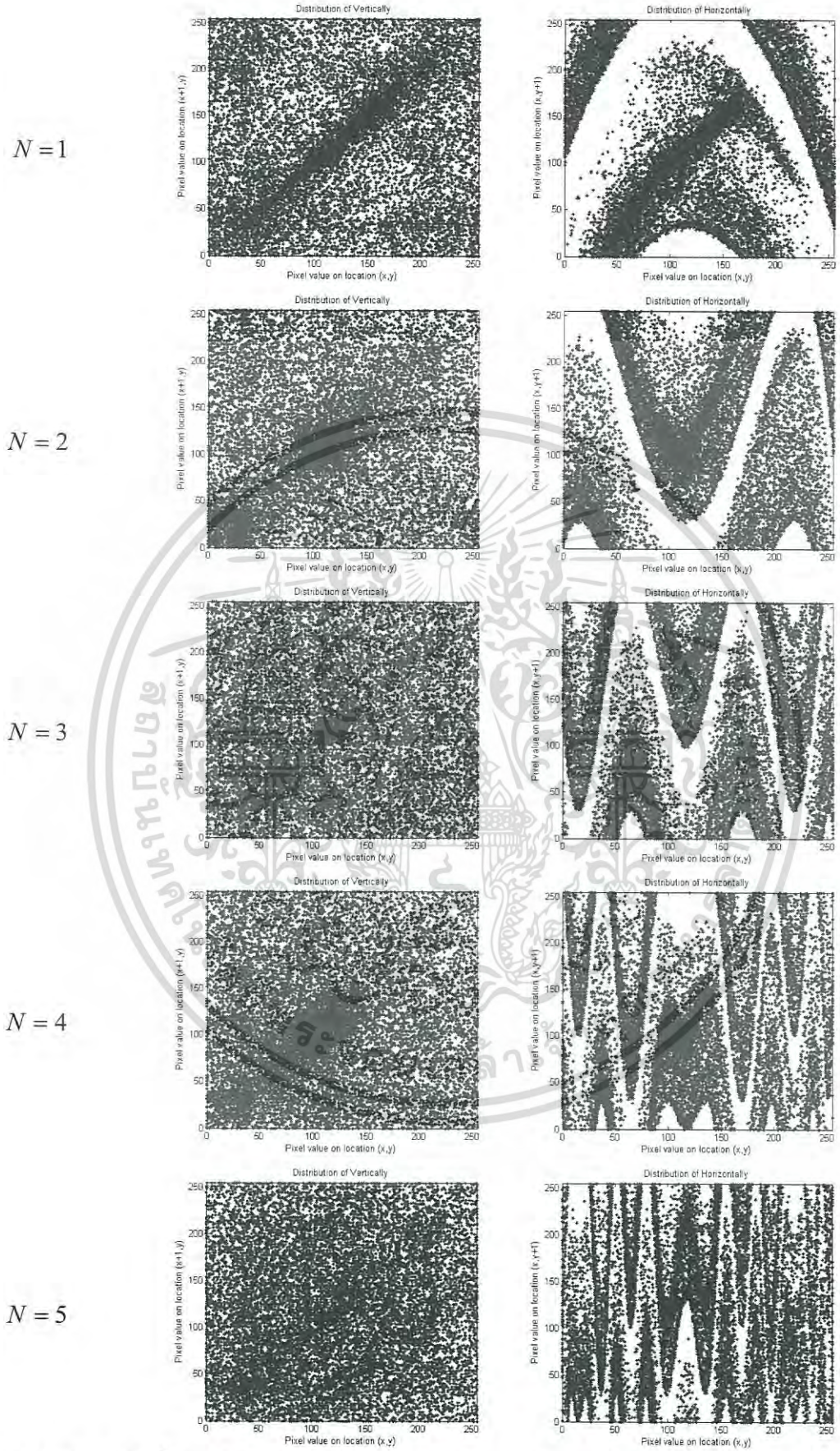
เมื่อพิจารณาการเข้ารหัสภาพ แผนภูมิข้อมูลเอนโทรปีของภาพ Lena ที่ผ่านการเข้ารหัสภาพและ ค่าเฉลี่ยข้อมูลเอนโทรปี สามารถใช้ค่าเฉลี่ยข้อมูลเอนโทรปีทั้งหมดของการเข้ารหัสภาพทั้ง 3 วิธี ซึ่งมีค่าเป็น 7.98046799 เป็นตัววัดผลการเข้ารหัสที่ดีได้ หากวิเคราะห์ค่าเอนโทรปีแต่ละชุดกุญแจลัพธ์ที่ใช้เข้ารหัสภาพ ชุดกุญแจ J และ N ที่ทดลองแล้วให้ค่าเอนโทรปีมากกว่าหรือเท่ากับ

7.98046799 สำหรับวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) มี 84 ค่า สำหรับวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) มี 83 ค่า และ สำหรับวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มี 86 ค่า โดยค่าเอนโทรปีที่น้อยกว่า 7.98046799 จะขีดเส้นและทำตัวเอียงไว้ในตารางที่ 4.2 ถึง ตารางที่ 4.4

เมื่อพิจารณาเฉพาะค่าเฉลี่ยข้อมูลเอนโทรปีที่ค่า J แต่ละค่าของทั้ง 3 วิธี จากภาพที่ 4.22 ก) พบว่าวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) มีค่าเอนโทรปีมากกว่าหรือเท่ากับ 7.98046799 เมื่อใช้ J มากกว่า 2 ส่วนวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ค่าเอนโทรปีมากกว่าหรือเท่ากับ 7.98046799 เมื่อใช้ J มากกว่า 1 ซึ่งสรุปได้ว่า การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) สามารถใช้จำนวนกุญแจในส่วนของ ลำดับการวนซ้ำ (N) และ จำนวนรอบในกระบวนการเข้ารหัส (J) ได้มากกว่าอีกสองวิธี

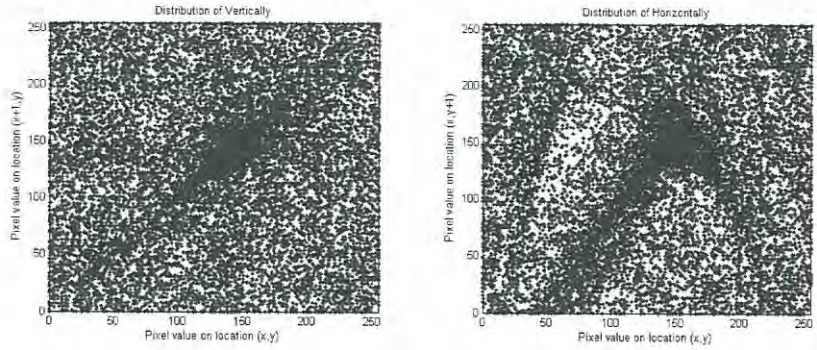
4.4 การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์

การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์เป็นหนึ่งในเครื่องมือสำหรับใช้วิเคราะห์ทางสถิติ โดยคำนวณความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอน และความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งในภาพ [28-29] เนื่องจากในข้อมูลภาพทั่วไปนั้น จุดภาพที่อยู่ติดกันนั้นจะมีความต่อเนื่องกันหรือมีค่าระดับความเข้มที่ใกล้เคียงกัน เช่นสัมประสิทธิ์ความสัมพันธ์ของจุดภาพที่ติดกันในแนวแกนตั้ง และในแนวแกนนอน ของภาพต้นฉบับในภาพที่ 4.1 ถึง ภาพที่ 4.3 จะมีการเกาะกลุ่มกัน ดังนั้นภาพที่เข้ารหัสที่ดีควรจะมีการกระจายตัวของจุดภาพหรือมีความสัมพันธ์กันน้อย การทดสอบส่วนนี้แสดงความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอน และแนวแกนตั้ง ของภาพ Lena ที่ผ่านการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ด้วยกุญแจลับตามตารางที่ 4.1 โดยเปลี่ยนกุญแจลับเฉพาะจำนวนรอบในกระบวนการเข้ารหัส $J=1$ กับ 2 ค่าลำดับการวนซ้ำ N ตั้งแต่ 1 ถึง 5

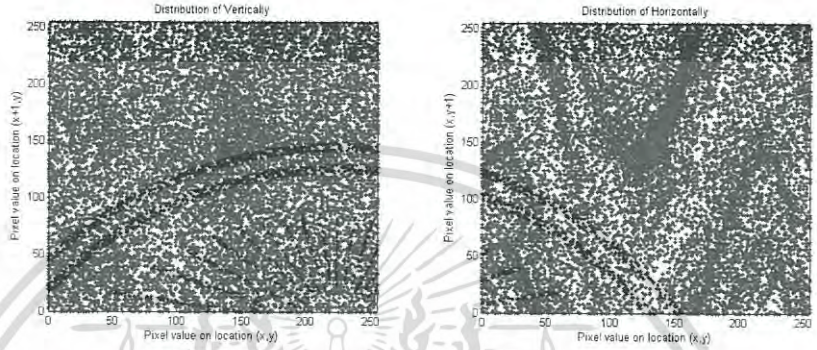


ภาพที่ 4.23 สัมประสิทธิ์ความสัมพันธ์ของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแบบ CML เมื่อ $J=1$

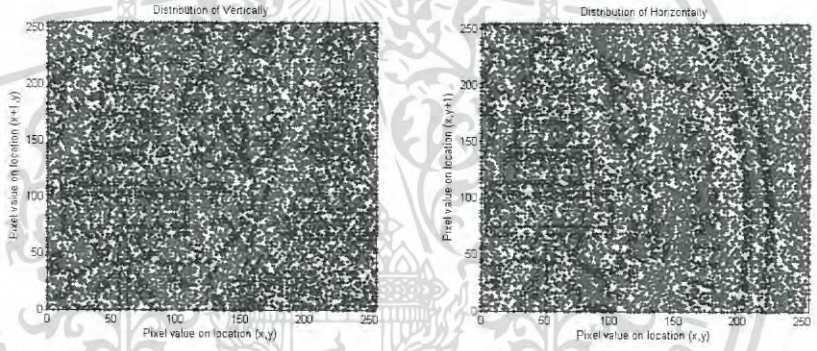
$N=1$



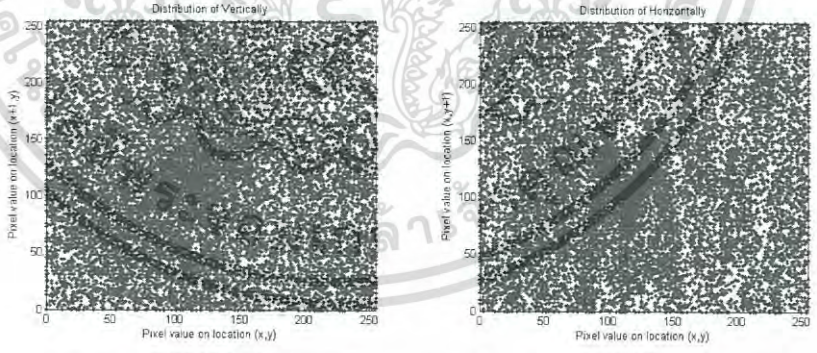
$N=2$



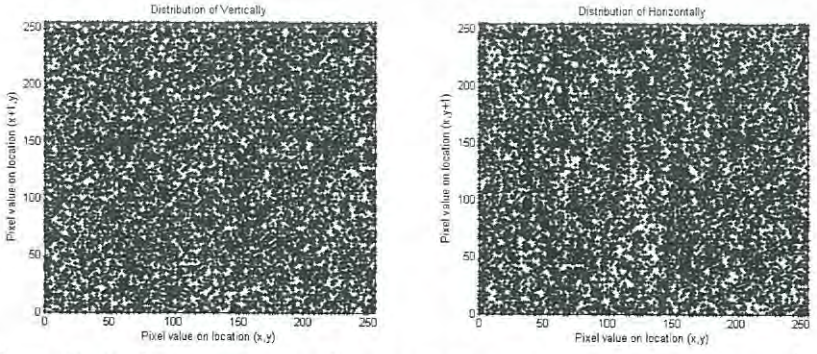
$N=3$



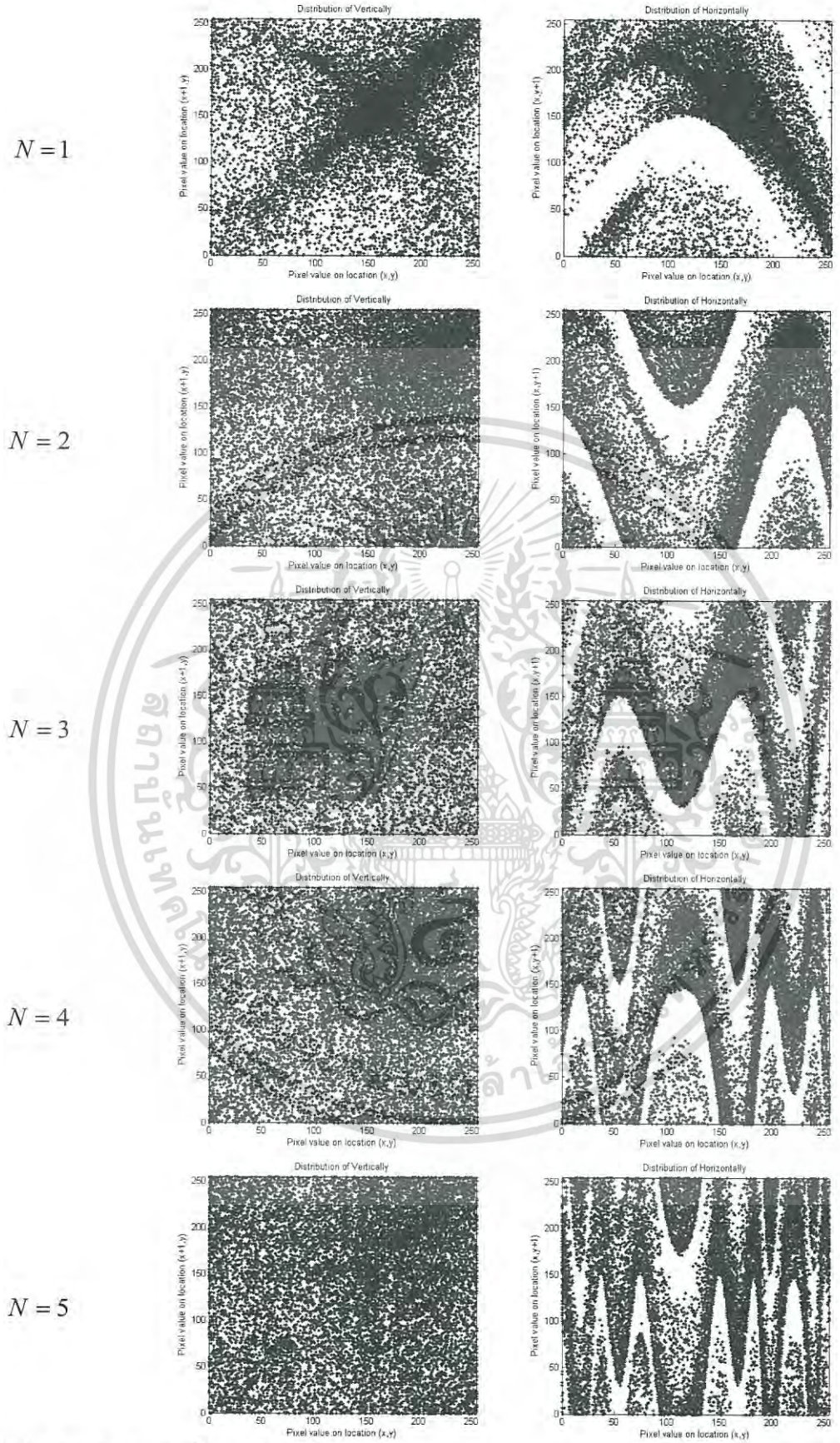
$N=4$



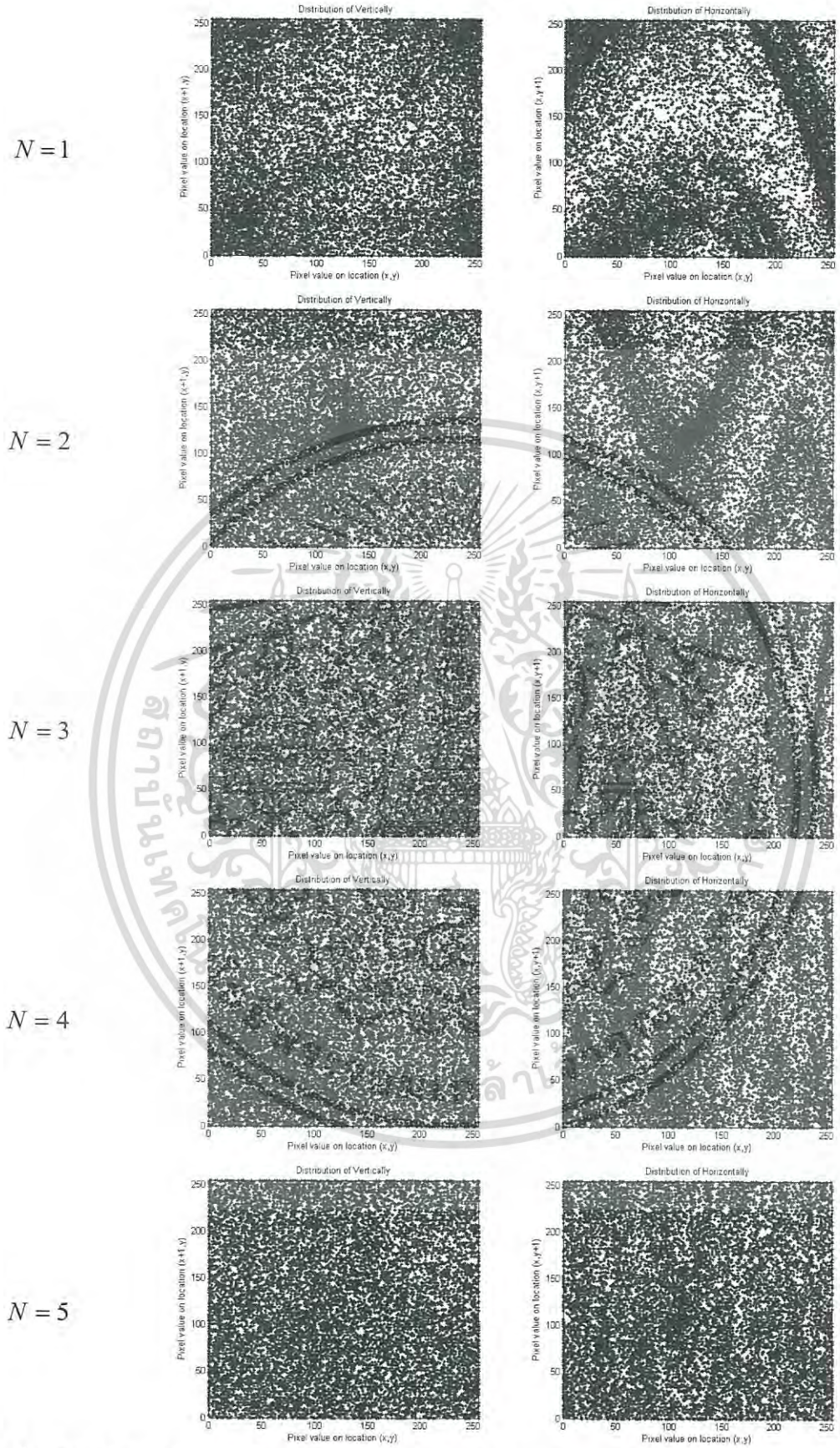
$N=5$



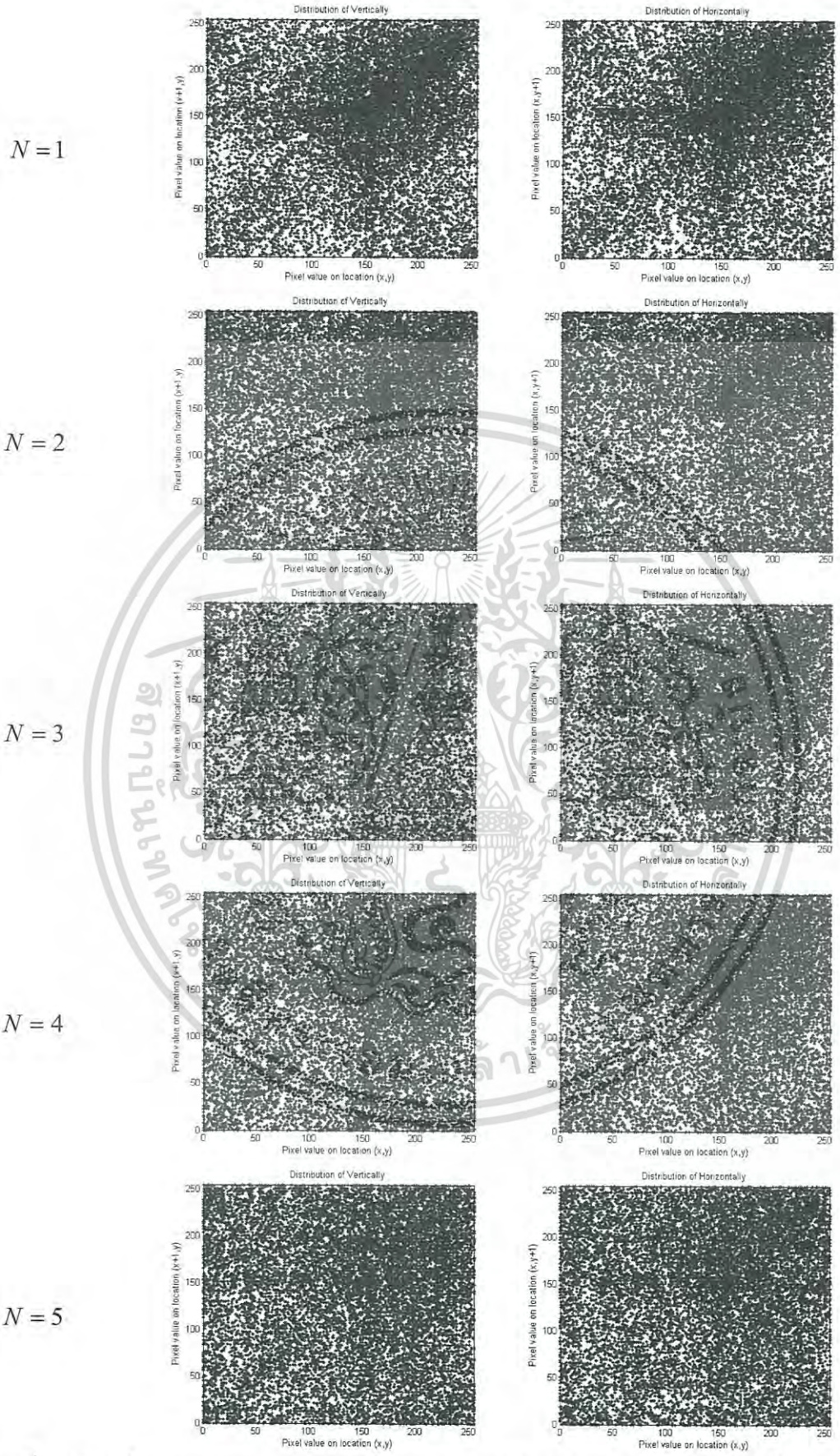
ภาพที่ 4.24 สัมประสิทธิ์ความสัมพันธ์ของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแบบ CML เมื่อ $J=2$



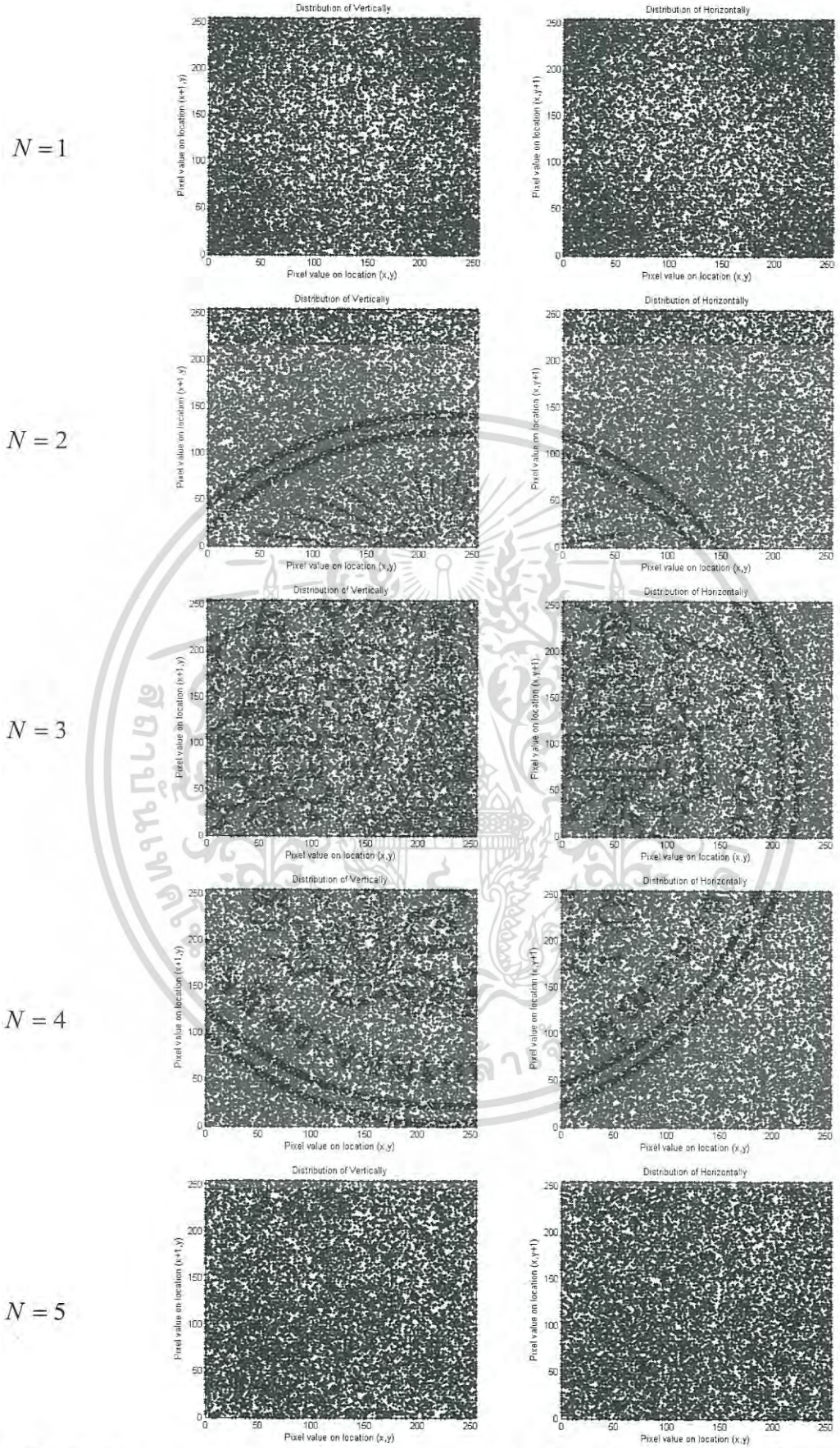
ภาพที่ 4.25 สัมประสิทธิ์ความสัมพันธ์ของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแบบ FCML เมื่อ $J=1$



ภาพที่ 4.26 สัมประสิทธิ์ความสัมพันธ์ของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแบบ FCML เมื่อ $J = 2$



ภาพที่ 4.27 ฮิสโทแกรมของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแบบ APFCML เมื่อ $J=1$



ภาพที่ 4.28 ฮิสโทแกรมของภาพ Lena ด้วยกระบวนการเข้ารหัสภาพแบบ APFCML เมื่อ $J = 2$

โดยภาพที่ 4.23 และภาพที่ 4.24 แสดงความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้ง (ภาพด้านซ้าย) และความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอน (ภาพด้านขวา) ของภาพ Lena ที่ผ่านการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ภาพที่ 4.25 กับ ภาพที่ 4.26 ความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันของภาพ Lena ที่ผ่านการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันของภาพ Lena ที่ผ่านการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) แสดงในภาพที่ 4.27 กับ ภาพที่ 4.28

เมื่อพิจารณาผลลัพธ์การกระจายตัวของความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันของภาพ Lena ที่ผ่านการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) เมื่อใช้จำนวนรอบในกระบวนการเข้ารหัส $J=1$ จากภาพที่ 4.23 พบว่าการกระจายตัวของความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งมีส่วนที่เกาะกลุ่ม และเมื่อเพิ่มค่าจำนวนรอบในกระบวนการเข้ารหัส $J=2$ จากภาพที่ 4.24 พบว่าการกระจายตัวของความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งมีการกระจายตัวดีขึ้น ซึ่งผลจากภาพที่ 4.25 กับภาพที่ 4.26 แสดงให้เห็นว่าการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) มีแนวโน้มใกล้เคียงกับการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

จาก ภาพที่ 4.27 ซึ่งแสดงการกระจายตัวของความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันของการเข้ารหัสภาพ Lena ด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) พบว่ามีการประจายตัวที่ดีเริ่มตั้งแต่ใช้จำนวนรอบในกระบวนการเข้ารหัส $J=1$ สรุปได้ว่ามีการกระจายตัวที่ดีกว่าอีกสองวิธีที่ผ่านมา

จากผลการทดลองในภาพรวม เมื่อทำการเพิ่มจำนวนลำดับการวนซ้ำ (N) จำนวนรอบในกระบวนการเข้ารหัส (J) ในกระบวนการเข้ารหัส จะทำให้ภาพมีการกระจายตัวมากขึ้น และ การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) จะมีการกระจายตัวของความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอน และความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งที่ดีกว่า

4.5 การวิเคราะห์ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์

ค่าสัมประสิทธิ์ความสัมพันธ์ สามารถแสดงความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอน และความสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งในภาพ ซึ่งช่วยในการวิเคราะห์ประสิทธิผลของการเข้ารหัส แต่ยังต้องอาศัยการสังเกต ดังนั้นเพื่อให้สามารถ

วัดประสิทธิภาพในเชิงตัวเลข สามารถใช้ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์เป็นตัววัดเชิงตัวเลขได้ และคำนวณได้ดังสมการ (4.2) [28-29]

$$C_r = \frac{N\sum_{j=1}^{N}\left(x_j \times y_j\right) - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \tag{4.2}$$

เมื่อทำการคำนวณหาค่าสัมประสิทธิ์ความสัมพันธ์ระหว่าง 2 จุดที่อยู่ติดกัน ภาพ Lena ที่ผ่านการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ด้วยกุญแจลับตามตารางที่ 4.1 ได้ผลดังตารางที่ 4.5 ถึงตารางที่ 4.10

ตารางที่ 4.5 ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	0.1421	0.1656	0.0696	0.0714	0.0976	0.0467	0.0718	0.0659	0.0713	0.0638
N=2	0.0766	0.0482	0.0428	0.0226	0.0185	0.0182	0.0316	0.0306	0.0237	0.0180
N=3	0.0641	0.0276	0.0250	0.0299	0.0209	0.0141	0.0207	0.0268	0.0153	0.0196
N=4	0.0441	0.0193	0.0218	0.0127	0.0324	0.0260	0.0147	0.0210	0.0303	0.0194
N=5	0.0495	0.0227	0.0260	0.0196	0.0221	0.0331	0.0227	0.0377	0.0262	0.0325
N=6	0.0220	0.0209	0.0207	0.0235	0.0079	0.0236	0.0207	0.0146	0.0197	0.0233
N=7	0.0075	0.0329	0.0163	0.0154	0.0109	0.0196	0.0177	0.0262	0.0322	0.0288
N=8	0.0317	0.0179	0.0222	0.0236	0.0134	0.0219	0.0387	0.0233	0.0317	0.0147
N=9	0.0283	0.0302	0.0240	0.0180	0.0221	0.0247	0.0204	0.0324	0.0262	0.0178
N=10	0.0272	0.0166	0.0334	0.0177	0.0299	0.0272	0.0290	0.0049	0.0149	0.0200

ตารางที่ 4.6 ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอนของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	0.0659	0.2009	0.0479	0.0387	0.0874	0.0559	0.0568	0.0670	0.0561	0.0733
N=2	0.0471	0.0450	0.0064	0.0325	0.0353	0.0244	0.0287	0.0175	0.0156	0.0332
N=3	0.0169	0.0313	0.0165	0.0124	0.0226	0.0209	0.0271	0.0305	0.0179	0.0299
N=4	0.0011	0.0265	0.0241	0.0245	0.0260	0.0185	0.0237	0.0299	0.0212	0.0190
N=5	0.0136	0.0261	0.0121	0.0206	0.0271	0.0281	0.0025	0.0284	0.0146	0.0336
N=6	0.0046	0.0205	0.0191	0.0174	0.0277	0.0261	0.0178	0.0359	0.0369	0.0346
N=7	0.0321	0.0103	0.0278	0.0201	0.0270	0.0323	0.0179	0.0250	0.0250	0.0102
N=8	0.0324	0.0217	0.0398	0.0288	0.0114	0.0139	0.0259	0.0072	0.0262	0.0275
N=9	0.0207	0.0308	0.0187	0.0242	0.0185	0.0186	0.0305	0.0287	0.0257	0.0204
N=10	0.0259	0.0177	0.0265	0.0198	0.0193	0.0102	0.0285	0.0291	0.0311	0.0247

ตารางที่ 4.7 ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	0.2245	0.1574	0.1165	0.1018	0.0695	0.0858	0.0850	0.0814	0.0660	0.0892
N=2	0.0538	0.0413	0.0177	0.0361	0.0199	0.0215	0.0133	0.0230	0.0219	0.0242
N=3	0.0509	0.0348	0.0243	0.0268	0.0154	0.0360	0.0275	0.0275	0.0190	0.0147
N=4	0.0350	0.0195	0.0255	0.0253	0.0284	0.0192	0.0071	0.0037	0.0309	0.0063
N=5	0.0335	0.0194	0.0329	0.0215	0.0278	0.0209	0.0118	0.0305	0.0286	0.0142
N=6	0.0174	0.0204	0.0305	0.0090	0.0175	0.0206	0.0210	0.0204	0.0105	0.0251
N=7	0.0142	0.0294	0.0146	0.0113	0.0204	0.0104	0.0204	0.0117	0.0123	0.0211
N=8	0.0161	0.0259	0.0210	0.0228	0.0227	0.0198	0.0246	0.0175	0.0396	0.0237
N=9	0.0183	0.0132	0.0294	0.0254	0.0163	0.0307	0.0237	0.0245	0.0402	0.0283
N=10	0.0173	0.0199	0.0196	0.0298	0.0396	0.0268	0.0233	0.0185	0.0284	0.0356

ตารางที่ 4.8 ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอนของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	-0.2527	0.2027	0.1328	0.0549	0.1098	0.0251	0.1046	0.0762	0.0690	0.0779
N=2	-0.0438	0.0289	0.0234	0.0373	0.0134	0.0292	0.0101	0.0232	0.0244	0.0083
N=3	0.0370	0.0266	0.0275	0.0202	0.0088	0.0137	0.0316	0.0310	0.0294	0.0222
N=4	-0.0447	0.0196	0.0228	0.0280	0.0360	0.0270	0.0187	0.0271	0.0280	0.0229
N=5	0.0671	0.0144	0.0206	0.0277	0.0278	0.0165	0.0268	0.0348	0.0239	0.0301
N=6	0.0191	0.0227	0.0187	0.0189	0.0139	0.0239	0.0290	0.0215	0.0247	0.0390
N=7	0.0230	0.0100	0.0069	0.0057	0.0196	0.0260	0.0209	0.0213	0.0192	0.0233
N=8	0.0355	0.0129	0.0224	0.0295	0.0236	0.0267	0.0229	0.0071	0.0173	0.0254
N=9	0.0233	0.0321	0.0319	0.0398	0.0191	0.0290	0.0170	0.0262	0.0278	0.0277
N=10	0.0151	0.0222	0.0192	0.0300	0.0350	0.0146	0.0315	0.0189	0.0139	0.0263

ตารางที่ 4.9 ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	0.1508	0.0587	0.0688	0.0896	0.0610	0.0784	0.0633	0.0817	0.0847	0.0739
N=2	0.0495	0.0380	0.0384	0.0356	0.0310	0.0260	0.0319	0.0206	0.0208	0.0329
N=3	0.0464	0.0058	0.0244	0.0225	0.0306	0.0215	0.0187	0.0294	0.0296	0.0104
N=4	0.0314	0.0167	0.0194	0.0217	0.0192	0.0223	0.0285	0.0375	0.0305	0.0222
N=5	0.0170	0.0141	0.0187	0.0280	0.0149	0.0166	0.0270	0.0350	0.0404	0.0257
N=6	0.0378	0.0359	0.0154	0.0217	0.0165	0.0255	0.0246	0.0253	0.0228	0.0221
N=7	0.0251	0.0145	0.0256	0.0167	0.0170	0.0298	0.0228	0.0167	0.0225	0.0192
N=8	0.0198	0.0268	0.0119	0.0188	0.0328	0.0200	0.0243	0.0098	0.0177	0.0195
N=9	0.0209	0.0078	0.0111	0.0358	0.0166	0.0268	0.0217	0.0228	0.0156	0.0277
N=10	0.0352	0.0234	0.0239	0.0291	0.0250	0.0196	0.0215	0.0277	0.0419	0.0315

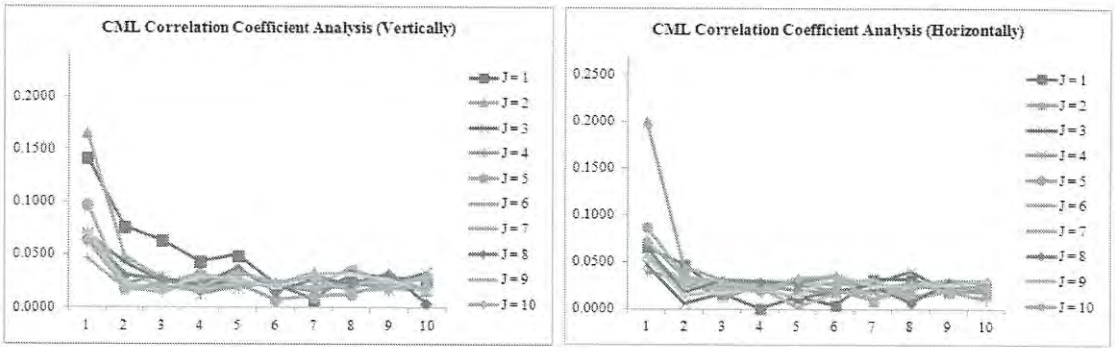
ตารางที่ 4.10 ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอนของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	0.1580	0.0568	0.0773	0.0883	0.0593	0.0917	0.0631	0.0808	0.0721	0.0833
N=2	0.0434	0.0324	0.0235	0.0223	0.0237	0.0099	0.0117	0.0263	0.0088	0.0180
N=3	0.0478	0.0174	0.0255	0.0174	0.0275	0.0276	0.0193	0.0282	0.0283	0.0291
N=4	0.0317	0.0213	0.0158	0.0155	0.0128	0.0249	0.0131	0.0220	0.0201	0.0151
N=5	0.0309	0.0256	0.0294	0.0237	0.0314	0.0187	0.0198	0.0158	0.0228	0.0193
N=6	0.0258	0.0292	0.0259	0.0217	0.0159	0.0354	0.0191	0.0239	0.0224	0.0372
N=7	0.0285	0.0276	0.0293	0.0240	0.0178	0.0252	0.0287	0.0291	0.0193	0.0328
N=8	0.0201	0.0275	0.0246	0.0249	0.0254	0.0407	0.0184	0.0179	0.0279	0.0274
N=9	0.0211	0.0272	0.0222	0.0286	0.0279	0.0298	0.0233	0.0242	0.0212	0.0354
N=10	0.0281	0.0159	0.0153	0.0320	0.0326	0.0096	0.0254	0.0219	0.0112	0.0204

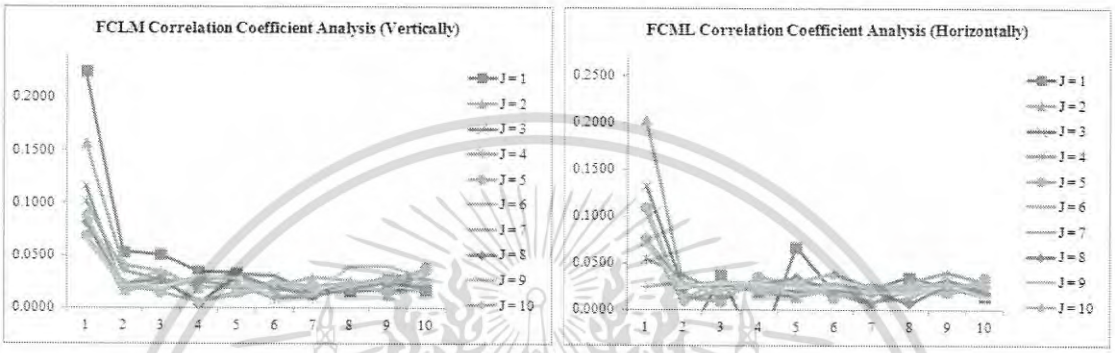
จากตารางที่ 4.2 ถึงตารางที่ 4.7 เป็นการหาค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนนอนของภาพ Lena สามารถนำมาสรุปเป็นแผนภูมิได้ดังภาพที่ 4.29

เมื่อพิจารณาภาพที่ 4.29 ก) เมื่อ $J=1$ พบว่าภาพรวมของค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันในแนวแกนตั้งจะมากกว่าเมื่อใช้ค่า $J=2$ ถึง 10 ซึ่งสัมพันธ์กับภาพที่ 4.23 ถึง ภาพที่ 4.28 แสดงถึงผลการเข้ารหัสภาพเมื่อใช้ค่า $J=1$ ได้ผลแย่กว่าการใช้ค่าอื่น ๆ และเมื่อเปรียบเทียบกับผลการเข้ารหัสภาพสามารถสรุปได้ว่าเมื่อค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ของการเข้ารหัสภาพที่มีค่าน้อยจะให้ผลการเข้ารหัสที่ดี หรือค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ของการเข้ารหัสภาพแปรผกผันกับผลการเข้ารหัสภาพ ซึ่งเมื่อเปรียบเทียบในภาพรวมการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ระหว่างจุดภาพสองจุดภาพที่อยู่ติดกันน้อยกว่าอีกสองวิธี

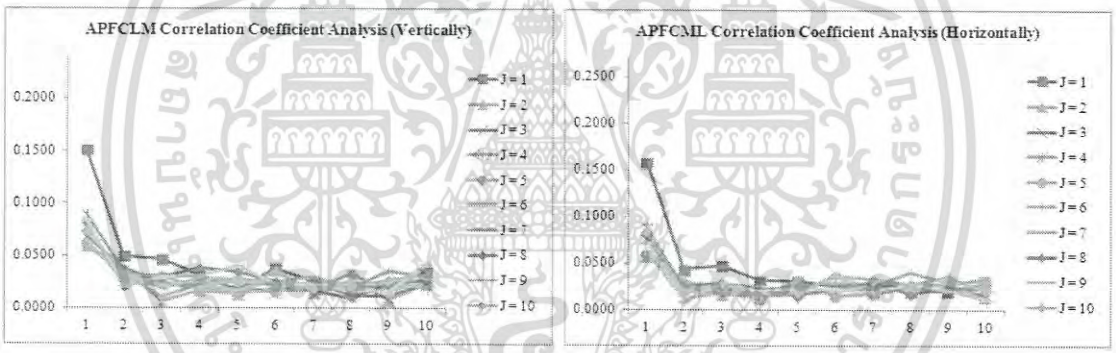
เมื่อเทียบกับการทดสอบประสิทธิผลของการเข้ารหัสภาพด้วยวิธีที่ผ่านมาพบว่าค่าที่แนะนำในการเข้ารหัสคือค่าที่น้อยว่า 0.1 สามารถสรุปได้ว่าการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ให้ผลการเข้ารหัสภาพที่ดีกว่าอีกสองวิธี



ก)



ข)



ค)

ภาพที่ 4.29 แผนภูมิค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ของการเข้ารหัสภาพ Lena ด้วย
ก) วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)
ข) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)
ค) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

4.6 ค่าเฉลี่ยการเปลี่ยนระดับสีเทา (GAVE)

ข้อมูลในภาพที่มีการเข้ารหัสลับย่อมมีการเปลี่ยนแปลงจากภาพต้นฉบับ ในการแสดงผลภาพที่ทำการเข้ารหัสจะแสดงความแตกต่างระหว่างภาพต้นฉบับ และภาพที่มีการเข้ารหัสลับ ซึ่งค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาเป็นการเปรียบเทียบความแตกต่างระหว่างภาพต้นฉบับ และภาพที่ผ่านการเข้ารหัส ซึ่งเป็นเครื่องมือวัดอีกตัวที่แสดงตัวเลขผลลัพธ์สามารถนำมาวิเคราะห์เปรียบเทียบได้

ค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทา สามารถเรียกแทนด้วย GAVE คำนวณได้จากสมการ (4.3) โดยการกำหนด $G=\left(g_{ij}\right)_{M\times N}$ เป็นข้อมูลจากภาพต้นฉบับ และ $C=\left(g_{ij}\right)_{M\times N}$ เป็นข้อมูลจากภาพที่เข้ารหัส [30]

$$GAVE(G,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|g_{ij}-c_{ij}\right|}{MN} \tag{4.3}$$

เมื่อ $GAVE(G,C)$ คือ ค่าเฉลี่ยการเปลี่ยนระดับสีเทาระหว่างภาพต้นฉบับ และภาพที่มีการเข้ารหัสลับ

g_{ij} คือ ระดับความเข้มสีของจุดภาพของภาพต้นฉบับที่จุดภาพ i,j

c_{ij} คือ ระดับความเข้มสีของจุดภาพของภาพที่เข้ารหัสที่จุดภาพ i,j

M คือ ขนาดของภาพในแนวนอน

N คือ ขนาดของภาพในแนวตั้ง

โดยค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาของภาพ Lena ที่ผ่านการเข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) แสดงในตารางที่ 4.11 ถึง ตารางที่ 4.12

ตารางที่ 4.11 ค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	6.81	8.87	10.27	11.70	13.06	13.59	14.65	14.70	14.79	14.59
N=2	8.08	12.36	14.27	14.44	14.71	14.59	14.62	14.85	15.03	14.82
N=3	11.86	14.49	14.90	14.85	15.21	14.90	14.70	15.14	15.13	14.84
N=4	8.71	11.89	13.44	14.29	14.31	14.64	14.61	15.15	15.19	14.65
N=5	9.61	13.63	14.62	14.88	14.80	14.63	14.97	14.80	15.05	15.42
N=6	10.38	13.36	14.49	14.72	14.48	14.63	14.94	15.00	14.78	14.81
N=7	10.13	13.43	14.40	14.81	14.71	15.00	14.99	14.80	14.53	14.41
N=8	10.50	13.96	14.49	14.83	14.85	14.72	14.76	14.93	15.09	14.92
N=9	10.58	13.40	14.62	14.97	15.30	14.83	14.59	14.81	14.59	14.54
N=10	9.74	13.01	13.93	14.58	14.58	14.80	14.73	14.95	14.69	14.69

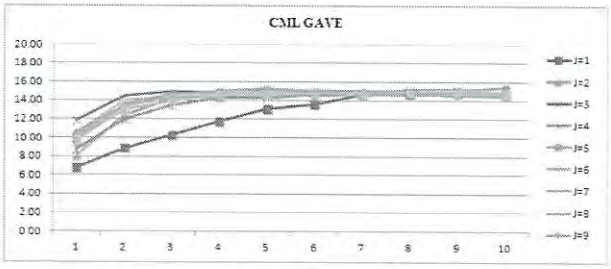
ตารางที่ 4.12 ค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	12.94	17.57	12.63	15.55	14.96	14.04	15.36	14.62	14.72	14.67
N=2	14.53	11.67	16.62	13.82	15.14	14.79	14.77	14.64	14.47	14.62
N=3	14.56	15.77	14.12	15.17	14.26	14.79	14.94	14.93	14.73	14.55
N=4	14.91	14.24	15.31	14.21	14.76	14.54	14.56	14.68	14.48	14.86
N=5	16.10	14.06	14.88	14.83	14.60	14.85	14.88	14.76	14.67	14.54
N=6	15.61	14.82	13.94	15.17	14.71	14.80	14.84	14.59	14.75	14.83
N=7	15.17	15.02	14.58	14.78	14.79	14.87	14.86	14.89	14.73	14.81
N=8	14.41	14.67	14.71	14.65	14.68	14.69	14.81	14.59	15.02	14.57
N=9	14.84	14.60	14.61	14.91	14.81	14.66	14.62	15.21	14.87	14.92
N=10	15.10	14.60	14.26	14.68	14.45	14.65	14.76	14.72	14.62	14.87

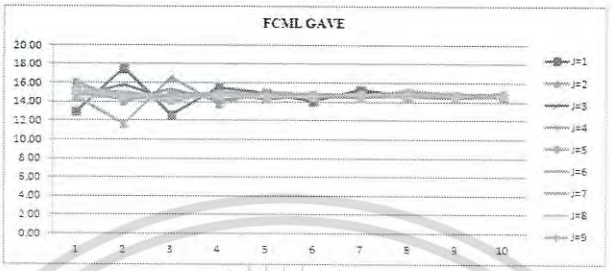
ตารางที่ 4.13 ค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาของภาพ Lena ที่เข้ารหัสด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

	J=1	J=2	J=3	J=4	J=5	J=6	J=7	J=8	J=9	J=10
N=1	14.32	18.49	12.11	15.72	15.00	14.33	15.20	15.03	14.59	14.79
N=2	16.81	12.09	15.99	13.85	15.49	14.46	15.03	14.67	15.13	14.49
N=3	14.10	15.45	14.12	15.13	14.23	14.91	14.83	14.49	14.77	15.02
N=4	15.79	13.70	14.95	14.91	14.71	14.58	14.37	15.03	14.51	15.13
N=5	15.97	13.75	15.10	14.74	14.98	14.66	14.86	14.79	14.92	14.67
N=6	15.53	14.89	14.42	14.66	14.54	14.60	15.10	14.38	14.79	14.56
N=7	15.33	15.08	14.57	14.99	14.37	15.04	14.74	14.56	14.84	14.97
N=8	14.34	15.00	14.74	14.77	14.69	14.45	15.31	14.53	14.85	14.97
N=9	15.27	14.72	14.26	14.93	14.77	15.36	14.62	15.21	14.82	14.86
N=10	15.50	14.60	14.76	14.60	14.57	14.84	14.63	14.89	15.00	15.14

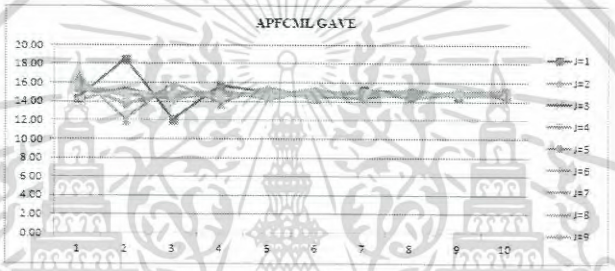
จากตารางที่ 4.11 ถึง ตารางที่ 4.13 ซึ่งเป็นค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาของภาพ Lena สามารถนำมาสรุปแผนภูมิได้ดังภาพที่ 4.29



ก)



ข)



ค)

ภาพที่ 4.30 แผนภูมิค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาของภาพ Lena ด้วย
ก) วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)
ข) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML)
ค) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML)

เมื่อพิจารณาการเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) จากภาพที่ 4.30 ก) เมื่อ $J=1$ พบว่าค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาจะน้อยกว่าที่ค่า $J=2$ และเมื่อเพิ่มจำนวน N ค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทาจะลดลง ซึ่งมีความสัมพันธ์กับการทดสอบประสิทธิผลของการเข้ารหัสภาพด้วยวิธีที่ผ่านมาทั้งการวิเคราะห์ผลการเข้ารหัสภาพ การวิเคราะห์ฮิสโตแกรม การวิเคราะห์ข้อมูลเอนโทรปี และ การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์ เมื่อเปรียบเทียบกับผลการเข้ารหัสภาพสามารถสรุปได้ว่า เมื่อค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทามากขึ้นจะให้ผลการเข้ารหัสที่ดี ซึ่งเมื่อเปรียบเทียบในภาพรวมโดยพิจารณาจากค่าเฉลี่ยการปรับเปลี่ยนระดับสีเทา เมื่อใช้ ค่า $J=2$ ถึง 10 สามารถสรุปได้ว่า การเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความ

ยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ให้ผลการเข้ารหัสภาพที่ดีกว่าการเข้ารหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML)

4.7 การวิเคราะห์ขนาดของกุญแจลับ (Key Space Analysis)

ขนาดของกุญแจลับ หมายถึง ความแตกต่างของกุญแจลับที่ใช้ในกระบวนการเข้ารหัส และถอดรหัส [31] ซึ่งหากขนาดของกุญแจลับมีขนาดมากเพียงพอจะทำให้การโจมตีด้วยวิธีการไล่สุ่มรหัสผ่าน (Brute Force Attack) ไม่มีผล กุญแจลับ

จากการทดสอบประสิทธิผลของการเข้ารหัสภาพด้วยวิธีที่ผ่านมาทั้งหมดเมื่อพิจาณาการใช้ค่า ลำดับการวนซ้ำ (N) และจำนวนรอบในกระบวนการเข้ารหัส (J) เป็นกุญแจ โดยภาพรวมแนะนำให้ใช้จำนวนรอบในกระบวนการเข้ารหัส $J >= 2$ และ $N >= 2$ ดังนั้นหากนับจำนวนกุญที่ใช้จาก ลำดับการวนซ้ำ (N) และจำนวนรอบในกระบวนการเข้ารหัส (J) มีจำนวน 72 ค่า

สำหรับการเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ใช้กุญแจลับ 3 ตัวในการเข้ารหัส และถอดรหัส ได้แก่ ค่าพารามิเตอร์ (r) ลำดับการวนซ้ำ (N) และ จำนวนรอบในกระบวนการเข้ารหัส (J) โดยค่าพารามิเตอร์ที่ใช้งานได้อยู่ในช่วง $3.57 < r < 4$ และค่าพารามิเตอร์ (r) ซึ่งเป็นจำนวนจริงที่ใช้ตามมาตฐาน IEEE 754 ซึ่งมีความแม่ยำถึง 10^{38} [37] เมื่อคำนวณขนาดของกุญแจลับ ของวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ได้ดังสมการ 4.4

$$\begin{aligned} |3.57-4| \times 10^{38} \times 72 &= 0.43 \times 10^{38} \times 72 \\ &= 3.096 \times 10^{39} \end{aligned} \tag{4.4}$$

สำหรับ การเข้ารหัส และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ใช้กุญแจลับ 4 ตัวในการเข้ารหัส และถอดรหัส ได้แก่ ลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) ค่าพารามิเตอร์ (r) ลำดับการวนซ้ำ (N) และ จำนวนรอบในกระบวนการเข้ารหัส (J) เมื่อพิจารณาค่าพารามิเตอร์ที่ใช้งานได้ขึ้นอยู่กับลำดับการอนุพันธ์ที่เป็นเศษส่วนค่าต่าง ๆ โดยงานวิจัยนี้ได้หาค่าพารามิเตอร์ที่ใช้ได้จากลำดับการอนุพันธ์ที่เป็นเศษส่วนจำนวน 9 ค่า ดังตารางที่ 2.3 เมื่อคำนวณขนาดของกุญแจลับ ของวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) สามารถได้ดังสมการ 4.5

$$\begin{bmatrix} |8.72-7.85|+|6.35-5.61|+|5.5-4.9|+ \\ |5.15-4.55|+|4.92-4.35|+|4.77-4.22|+ \\ |4.65-4.13|+|4.57-4.05|+|4.51-4.00| \end{bmatrix} \times 10^{38} \times 72 = 5.48 \times 10^{38} \times 72 \quad (4.5)$$
$$= 3.9456 \times 10^{40}$$

สำหรับการเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ใช้กุญแจลับ 5 ตัวในการเข้ารหัส และถอดรหัส ได้แก่ ลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) ค่าพารามิเตอร์ (r) ลำดับการวนซ้ำ (N) จำนวนรอบในกระบวนการเข้ารหัส (J) ค่าพารามิเตอร์ของพลวัตความยุ่งเหยิงใช้กำหนดลำดับจุดภาพในการเข้ารหัส (r_G) และ ค่าเงื่อนไขตั้งต้นของพลวัตความยุ่งเหยิงใช้กำหนดลำดับจุดภาพในการเข้ารหัส (x_{0G}) โดยเมื่อพิจารณาค่าพารามิเตอร์ที่ใช้งานได้ขึ้นอยู่กับลำดับการอนุพันธ์ที่เป็นเศษส่วนค่าต่าง ๆ โดยงานวิจัยนี้ได้หาค่าพารามิเตอร์ที่ใช้ได้จากลำดับการอนุพันธ์ที่เป็นเศษส่วนจำนวน 9 ค่า ดังตารางที่ 2.3 ค่าพารามิเตอร์ของพลวัตความยุ่งเหยิงใช้กำหนดลำดับจุดภาพในการเข้ารหัส $3.57 < r_G < 4$ และ ค่าเงื่อนไขตั้งต้นของพลวัตความยุ่งเหยิงใช้กำหนดลำดับจุดภาพในการเข้ารหัส $0 < x_{0G} < 1$ เมื่อคำนวณขนาดของกุญแจลับ ของวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) สามารถได้ดังสมการ 4.6

$$5.48 \times 10^{38} \times |3.57-4| \times 10^{38} \times |0-1| \times 10^{38} \times 72 = 5.48 \times 10^{38} \times 0.43 \times 10^{38} \times 10^{38} \times 72 \quad (4.6)$$
$$= 1.6966 \times 10^{116}$$

จากสมการที่ 4.6 พบว่าวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีขนาดของกุญแจลับมากกว่าอีก 2 วิธีอย่างมหาศาล ซึ่งยังสามารถขยายขนาดของกุญแจลับได้อีกโดยใช้ช่วงของ ค่าพารามิเตอร์ จากคู่ของ ลำดับการอนุพันธ์ที่เป็นเศษส่วนเพิ่มเติม

บทที่ 5
การวิเคราะห์ และบทสรุป

วิทยานิพนธ์นี้ได้ศึกษา การเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) โดยทดสอบประสิทธิผลของการเข้ารหัสด้วย การเข้ารหัสภาพ การวิเคราะห์ฮิสโตแกรม การวิเคราะห์ข้อมูลเอนโทรปี การวิเคราะห์ค่าสัมประสิทธิ์ความสัมพันธ์ การวิเคราะห์ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ ค่าเฉลี่ยการเปลี่ยนระดับสีเทา และ การวิเคราะห์ขนาดของกุญแจลับ

ข้อแตกต่างของการเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) คือ จำนวนของกุญแจลับที่นำมาใช้งาน โดยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ใช้กุญแจลับเพียง 3 ตัวในการเข้ารหัส และถอดรหัส ได้แก่ ค่าพารามิเตอร์ (r) ลำดับการวนซ้ำ (N) และ จำนวนรอบในกระบวนการเข้ารหัส (J) ส่วนวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ได้ใช้รูปแบบลอจิสติกแบบลำดับที่เป็นเศษส่วน แทนลอจิสติกแมพ ทำให้มีกุญแจลับใหม่ได้แก่ ลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) และเมื่อผสานคู่ของลำดับการอนุพันธ์ที่เป็นเศษส่วน (α) กับช่วงของพารามิเตอร์ (r) ที่เกิดความเป็นพลวัตความยุ่งเหยิง ทำให้มีจำนวนกุญแจลับที่ใช้อย่างมาก ในการทดสอบประสิทธิผลด้วยตัวชี้วัดต่าง ๆ พบว่าประสิทธิผลการเข้ารหัสภาพของทั้งสองวิธีไม่ต่างกันมาก เนื่องเป็นการเปลี่ยนเพียงพลวัตความยุ่งเหยิงที่ใช้ในการเข้ารหัสภาพซึ่งมีคุณสมบัติคล้ายกัน โดยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ให้ผลที่ดีกว่าเมื่อวิเคราะห์ด้วยข้อมูลเอนโทรปีทใช้จำนวนรอบในกระบวนการเข้ารหัส $J=1$ แต่เมื่อใช้ค่าจำนวนรอบในกระบวนการเข้ารหัส $J=2$ ถึง 10 วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ให้ผลที่ดีกว่าโดยเฉพาะเมื่อใช้ค่า ลำดับการวนซ้ำ $N=1$ เมื่อวิเคราะห์ด้วยค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ และ ค่าเฉลี่ยการเปลี่ยนระดับสีเทา วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) ได้ผลที่ดีกว่า และสำหรับขนาดของกุญแจลับของวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) มากกว่า วิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ถึง 14 เท่า

วิทยานิพนธ์นี้ได้นำเสนอการเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) ซึ่งพัฒนาการเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) โดยเปลี่ยนจากการเข้ารหัสจุดภาพที่เป็นลำดับต่อกัน เป็นการสลับลำดับในการเข้ารหัส

จุดภาพ ซึ่งส่วนที่กำหนดลำดับในการเข้ารหัสจุดภาพนั้น ได้ใช้พลวัตความยุ่งเหยิงอีกตัว นอกจากทำให้มีการใช้กุญแจลับเพิ่มขึ้นแล้ว ยังทำให้ประสิทธิผลการเข้ารหัสภาพดีกว่าการเข้ารหัสภาพ และถอดรหัสภาพด้วยวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) และ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) โดยเมื่อพิจารณาผลการเข้ารหัสภาพ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) สามารถซ่อนข้อมูลภาพต้นฉบับได้ดีตั้งแต่เริ่มใช้จำนวนรอบในกระบวนการเข้ารหัส $J = 2$ และ $N = 1$ ซึ่งอีก 2 วิธียังมีข้อมูลภาพต้นฉบับเหลืออยู่ และเมื่อใช้ฮิสโตแกรม ข้อมูลเอนโทรปี ค่าสัมประสิทธิ์ความสัมพันธ์ ค่าสัมประสิทธิ์ระหว่างสหสัมพันธ์ และ ค่าเฉลี่ยการเปลี่ยนระดับสีเทามาใช้ในการวิเคราะห์ ก็ยังให้ผลที่ดีกว่า สุดท้ายเมื่อพิจารณาขนาดของกุญแจลับ วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิงบนพื้นฐานการเลือกพิกเซลแบบปรับเปลี่ยนได้ (APFCML) มีขนาดของกุญแจลับมากกว่า วิธีโครงร่างแผนที่แบบพลวัตเชิงเศษส่วนของความยุ่งเหยิง (FCML) 4.3×10^{75} เท่า และมากกว่าวิธีโครงร่างแผนที่แบบพลวัตของความยุ่งเหยิง (CML) ถึง 5.48×10^{76} เท่า

เอกสารอ้างอิง

[1] Shujun, L. 2003. **Analyses and New Designs of Digital Chaotic Ciphers.** Xi'an : Xi'an Jiaotong University Press.

[2] Bishop, D. 2003. **Introduction to Cryptography with Java Applets.** Boston : Jones and Bartlett Publishers.

[3] Mendezes, A. J. Oorschot, P. C. V. and Vanstone, S. A. 1997. **Handbook of Applied Cryptography.** New York : CRC Press.

[4] Pecora, L. M. and Carroll, T. L. 1990. "Synchronization in chaotic systems." **Phys. Rev. Lett.** 64 : 821-824.

[5] Cuomo, K. M. and Oppenheim, A. V. 1993. "Circuit implementation of synchronized chaos with applications to communications." **Phys. Rev. Lett.** 71 : 65-68.

[6] Kocarev, L. and Parlitz, U. 1995. "General Approach for Chaotic Synchronization with Applications to Communication." **Phys. Rev. Lett.** 74 : 5028-5031

[7] Van Wiggeren, D. G. and Roy, R. 1998. "Communication with Chaotic Lasers." **Science.** 279 : 1198-1200.

[8] Boccaletti, S. Kurths, J. Osipov, G. Valladares, D. L. and Zhou, C. 2002. "The Synchronization of Chaotic Systems." **Phys. Rep.** 366 : 1-101.

[9] Perez, G. and Cerdeira, H. A. 1995. "Extracting Messages Masked by Chaos." **Phys. Rev. Lett.** 74 : 1970-1973.

[10] Short, K. M. and Parker, A. T. 1998. "Unmasking a hyper chaotic communication scheme." **Phys. Rev. E.** 58 : 1159-1162.

[11] Zhou, C. and Lai, C. H. 1999. "Extracting messages masked by chaotic signals of time-delay systems." **Phys. Rev. E.** 60 : 320-323.

[12] Wang, S. Kuang, J. Li, J. Luo, Y. Lu, H. and Hu, G. 2002. "Chaos-based secure communications in a large community." **Phys. Rev. E.** 66 : 065202(R).

[13] Pareek, N. K. Patidar, V. and Sud, K. K. 2003. "Discrete chaotic cryptography using external key." **Phys. Lett. A.** 309 : 75-82.

[14] Kocarev, L. Sterjev, M. Fekete, A. and Vattaym, G. 2004. "Public-key encryption with chaos." **Chaos.** 14 : 1078.

[15] Kotulski, Z. and Szczepanski, J. 1997. "Discrete Chaotic Cryptography." **Ann. Phys.** (Paris) 6 : 381-394.

[16] Baptista, M. S. 1998. "Cryptography with Chaos." **Phys. Lett. A** 240 : 50-54.

[17] Alvarez, E. Fernandez, A. Garcia, P. Jimenez, J. and Marcano, A. 1999. "New approach to chaotic encryption." **Phys. Lett. A** 263 : 373-375.

[18] Wong, K. W. Ho, S. W. and Yung, C. K. 2003. "A chaotic cryptography scheme for generating short ciphertext." **Phys. Lett. A** 310 : 67-73.

[19] Pareek, N. K. Patidar, V. and Sud, K. K. 2005. "Cryptography using multiple one-dimensional chaotic maps." **Communications in Nonlinear Science and Numerical Simulation.** 10 (7) : 715-723.

[20] Kaneko, K. and Tsuda, I. 2001. **Complex Systems: Chaos and Beyond.** A Constructive Approach with Applications in Life Sciences. Berlin : Springer-Verlag.

[21] Lu, H. Wang, S. Li, X. Tang, G. Kuang, J. Ye, W. and Hu, G. 2004. "A new spatiotemporally chaotic cryptosystem and its security and performance analyses." **Chaos 14(3)** 617-629

[22] Wang, S. Liu, W. Lu, H. Kuang, J. and Hu, G. 2004. "Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications." **Int. J. Mod. Phys. B.** 18 : 2617-2622. DOI: 10.1142/S0217979204025798

[23] Pisarchik, A.N. Flores-Carmona, N. J. and Carpio-Valadez, M. 2006. "Encryption and decryption of images with chaotic map lattices." **American Institute of Physics.** DOI: 10.1063/1.2242052

[24] Hosseinnia, H. Ghaderi, R. Ranjbar, A. N. Sadati, S. J. and Momani, S. 2012. "Synchronization of Fractional Chaotic Systems via Fractional-Order Adaptive Controller." **Applied Mechanics and Materials.** DOI: 10.4028/www.scientific.net/AMM.109.333

[25] Solak, E. and Çokal, C. 2008. "Comment on "Encryption and decryption of images with chaotic map lattices"." **American Institute of Physics.** DOI: 10.1063/1.2966114

[26] Sittigorn, J. and Paithoonwattanakij, K. 2015. "Adaptive Pixel-Selection Fractional Chaotic Map Lattices for image cryptography." **Scientific Research and Essays.** vol. 10(17) : 531-543. DOI: 10.5897/SRE2015.6248

[27] Shannon, C. E. 1949. "Communication theory of secrecy systems." **Bell System Technical Journal.** 28. pp. 656–715.

[28] Pareek, N. K. Patidar, V. and Sud, K.K. 2006. "Image encryption using chaotic logistic map." **Image and Vision Computing.** vol. 24 : 926–934.

[29] Liu, S. Sun, J. and Xu, Z. 2009. "An Improved Image Encryption Algorithm based on Chaotic System." **Journal Of Computers.** vol. 4, no. 11 : 1091-1100.

[30] Li, Q. and Wang, Y. 2011. "The Performance Analysis of Image Encryption Algorithm Based on Chaotic System." **International Conference on Electronic & Mechanical Engineering and Information Technology.** 978-l-61284-088-8/ll/ : 3492–3494.

[31] Fu, C. Chen, J. Zou,H. Meng,W. Zhan,Y. and Yu, Y. 2012. "A Chaos-based Digital Image Encryption Scheme with an improved Diffusion Strategy." **Journal Optic Express.** 2363, vol. 20. no. 3.

[32] Weisstein, Eric W. **Logistic Equation.** [Online]. Available : http://mathworld.wolfram.com/LogisticEquation.html.

[33] Podlubny, I. 1999. **Fractional Differential Equations.** Technical University of Kosice, Slovak Republic : Acadmic Press.

[34] Suansook, Y. and Paithoonwattanakij, K. 2009. "Chaos in Fractional Order Logistic Model." **International Conference on Signal Processing Systems.** : 297-301. DOI:10.1109/ICSPS.2009.60.

[35] Suansook, Y. and Paithoonwattanakij, K. 2009. "Dynamic of Logistic Model at Fractional order." **IEEE International Symposium on Industrial Electronics.** : 718-723. DOI:10.1109/ISIE.2009.5219765.

[36] Sittigorn, J. Paithoonwattanakij, K. and Surawatpunya, C. 2013. "Image Encryption and Decryption with a Selective Pixel Using Chaotic Map Lattices." **International Conference on Engineering, Applied Sciences, and Technology.** 37-42.

[37] The MathWorks, Inc. **Floating-Point Numbers.** [Online]. Available : http://www.mathworks.com/help/matlab/matlab_prog/floating-point-numbers.html

ประวัติผู้เขียน

ชื่อ-นามสกุล จิระศักดิ์ สิทธิกร

วัน เดือน ปีเกิด 19 มกราคม 2523 ที่สระบุรี

ที่อยู่ 154/5 หมู่ที่ 1 ตำบลพระพุทธบาท อำเภอพระพุทธบาท จังหวัดสระบุรี 18120

ประวัติการศึกษา 2544 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโทรคมนาคม มหาวิทยาลัยเทคโนโลยีสุรนารี

2547 วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมโทรคมนาคม สถาบันเทคโนโลยี พระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ความชำนาญเฉพาะด้าน 1.) การประมวลผลภาพ

2.) การออกแบบวงจรดิจิทัล

3.) เครือข่ายคอมพิวเตอร์ และการสื่อสารข้อมูล

ประสบการณ์การทำงานและผลงานวิจัย

พ.ศ.2546-2550 อาจารย์ (ลูกจ้างชั่วคราว) ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2550-ปัจจุบัน อาจารย์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ผลงานวิจัย และบทความที่ได้รับการตีพิมพ์

1 Sittigorn, J. Paithoonwattanakij, K. and Surawatpunya, C. 2013. "Image Encryption and Decryption with a Selective Pixel Using Chaotic Map Lattices." **International Conference on Engineering, Applied Sciences, and Technology.** : 37-42.

2 Sittigorn, J. Paithoonwattanakij, K. and Surawatpunya, C. 2013. "Adaptive pixel-selection using chaotic map lattices for image cryptography" **Fifth International Conference on Graphic and Image Processing.** vol. 9069 : 906915-1-6.

3 Sittigorn, J. and Paithoonwattanakij, K. 2015. "Adaptive Pixel-Selection Fractional Chaotic Map Lattices for image cryptography." **Scientific Research and Essays.** vol. 10(17) : 531-543. DOI: 10.5897/SRE2015.6248

Image Encryption and Decryption with a Selective Pixel Using Chaotic Map Lattices

Jirasak Sittigorn[1], Kitti Paithoonwattanakij[2], Charray Surawatpunya[3]
[1] Department of Computer Engineering [2] Department of Electronics [3] Department of Telecommunication Engineering
Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang,
Bangkok, 10520 Thailand
[1] jirasak@live.kmitl.ac.th, [2] kpkitti@kmitl.ac.th, [3] kscharra@kmitl.ac.th

Abstract— **Chaotic theory is widely used in cryptography application. Chaotic cryptography generates a sequence of data that is similar to pseudorandom number based on an adjusted initial condition and a parameter. The main contribution of this paper is to apply the Chaotic Map Lattices (CML) to an image cryptographic algorithm. The modified CML encrypts and decrypts some pixels in the images from the introduced pixels based on the selected range of pixel intensity. Median and standard deviation from each image are used for calculating the range of pixel intensity. The new transformation equation and inverse-transformation equation enable encrypt some pixels in the images. Therefore, a violator is unable to predict the exact location of the encrypted pixels. Visual testing, statistical analysis and gray modification average value are used as quality assessment for the experimental results. The results show that the exact locations of the encrypted pixels are well hidden from the violator.**

Keywords-component; Chaotic Map Lattices; Image encryption; Median; Standard Deviation

I. INTRODUCTION

Dynamic systems and chaotic theory are used in communication and cryptography [1-6]. Cryptography is the study and practice of techniques for security. The original message has been changed to an encrypted message by an encryption algorithm using a secret key. Normally, a decryption process secures the signal message with the secret keys [5]. Chaotic theory studies the behavior of the nonlinear dynamic systems that are highly sensitive to small variation of initial condition. Chaotic system uses an initial condition and a parameter to generate a sequence of non-periodical data that looks like random numbers.

Image encryption changes image data from the original image to the encrypted image. Peoples having no permission cannot view or use the encrypted while those having permission can recover the original image from encrypted image. Image encryption with Chaotic Map Lattices (CML) is based on the chaos theory that is highly sensitive to the initial condition. It is difficult to decipher since they do not know the secret keys used in generating CML such as initial condition, parameter, number of iterations and number of cycles in encryption and decryption processes [7].

The defect of using CML in encryption and decryption is inconvertible because some data change in some image decryptions [8]. Precision in chaotic decryption is highly sensitive. Errors in rounding function may lead to fault decryption. Therefore, rounding function in encryption process should be prohibited.

In this paper, we propose a modified CML with a selective encrypted pixel selection method using median and standard deviation of the original image. These parameters are used to calculate the range of pixel intensity. Only pixels that have value in the selected range are encrypted. The range of pixel values for encryption from each color component is the new secret keys in decryption algorithm and is unpredictable from the violators.

II. CHAOTIC SYSTEM

The logistic map is a polynomial mapping of degree two that is one of chaos systems known as,

$$x_{n+1} = a\, x_n \left(1 - x_n\right) \tag{1}$$

where x_n and a are the system variable and parameter, respectively, n is the number of iterations and x_0 is an initial condition. In equation (1), system variable and parameter influence chaos system when $0<x_n<1$ and $3.57<a<4$. In this paper, the parameter value is set to $a = 3.9$ while the system variable is between $x_{min} = 0.095062$ and $x_{max} = 0.975000$ as suggested in [7].

The idea of encryption is that the image can be represented as a lattice of pixels. The pixel color is the combination of the three components: red, green, and blue shown as $C = (C_r, C_g, C_b)$. Normally, value of each component is an integer between 0 and 255. CML has created x_c in parallel for each of color component as shown by variable $x_c = (x^r_c, x^g_c, x^b_c)$. CML use the following transformation [7],

$$x_c = x_{min} + \delta x\left(C / 255\right) \tag{2}$$

Where $\delta x = x_{max} - x_{min}$. To extract the value of the color component, CML applies the inverse function [7],

$$C = \text{round}[(x_c - x_{min})255/\delta x] \quad (3)$$

Equation (3) is the inverted function of (2). Both equations are applied to every pixel in an image. However, only selected range of color value is derived.

Transformation equation and inverse function from CML must encrypt every value in the image. We propose a selective encrypted pixel selection algorithm based on statistics of the original image. Modified transformation equation and inverse function can encrypt every value in the image. For encryption, we use median, standard deviation and constant values from each color components of the image for selecting the range of pixel values [$C_{S\text{-}max}$, $C_{S\text{-}min}$] as (4) and (5).

$$C_{S-\min} = MED[C] - r_1 SD[C] \quad ; for \ C_{S-\min} \geq 0 \quad (4)$$

$$C_{S-\max} = MED[C] - r_2 SD[C] \quad ; for \ C_{S-\max} \leq 255 \quad (5)$$

Where r_1 and r_2 are constant values.

The proposed modified CML adopted from (2) is shown in (6).

$$x_c = x_{min} + \delta x(C - C_{S-\min} + 1)/(\delta C_S + 2) \quad (6)$$

Where [$C_{S\text{-}max}$, $C_{S\text{-}min}$] is the selected range of pixel values for encryption and $\delta C_S = C_{S\text{-}max} - C_{S\text{-}min}$. The modified inverse-transformation equation adopted from (3) is illustrated in (7).

$$C = \text{round}[(x_n - x_{min})(\delta C_S + 2)/\delta x + C_{S-min} - 1] \quad (7)$$

III. Encryption and Decryption Algorithm

The modify CML encryption and decryption algorithm are as followed:

A. Encryption Algorithm

The revised encryption algorithm is shown in Fig.1 which composes of the following steps.

1) Define secret keys as parameter (a), number of iteration (N), number of cycle (J) and threshold (T).

2) Convert the image containing two dimensional ($Row \times Column = m$ pixels) in terms of variable C which sequence is $i = 1, 2, 3, \ldots, m$. Calculate median and standard deviation of each color components. Define the selected range of pixel values for encrypt using (4) and (5).

3) Check the percentile of encrypted images from step 2) by following steps.

a) Calculate cumulative histogram from each color components.

b) If the percentile of cumulative histogram at $C_{S\text{-}min}$ is greater than T, then define new value $C_{S\text{-}min}$ is 0.

c) If the percentile of cumulative histogram at $C_{S\text{-}max}$ is smaller than 1-T, then define new value $C_{S\text{-}max}$ is 255.

4) Calculate x_c using (6) from three color components of the image.

5) Calculate order of pixels for encryption from range of pixel values from step 2) and 3).

6) Obtain the value of the last order (x_c^{last}) in step 5) and used as the initial condition for the first order as variable x_0^{first}.

7) Iterate n time of the first order from (1). Obtain the map variable x_n^{first} and add to this value the color value of the pixel (x_c^{first}). The sum value is applied as the initial condition for the subsequent order. Sometime sum of value is over range of chaos system (x_{max}). We used the condition in (10) to solve the problem. Iterate all maps subsequently starting from the first order and going through encrypt image pixels, pixel by pixel, toward the last order. The new x_c is the latest result of this cycle.

8) Use the last order (x_c^{last}) of previous cycle in step 7) as an initial condition for the first order in the new cycle. Repeat steps 6) overall the number of cycle (J).

9) Convert the sequence of encrypted data x_c back to the image containing two dimensional.

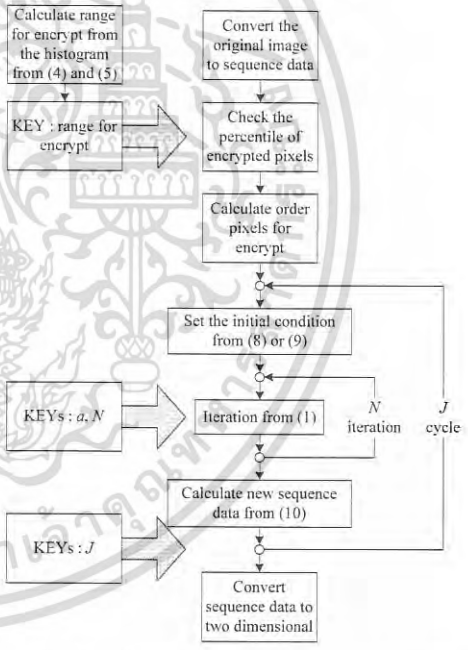


Figure 1. Block diagram of encryption algorithm.

The encryption algorithm can be summarized as follows (8)-(10).

$$x_0^i(j) = x_c^{last}(j-1) \quad ; if \ \ i = \text{first order} \quad (8)$$

$$x_0^i(j) = x_c^{i-1}(j) \quad ; if \ \ i \neq \text{first order} \quad (9)$$

$$x_c^i(j)=\begin{cases} x_n^i(j-1)+x_c^i(j-1) & \text{if } x_n^i(j-1)+x_c^i(j-1)\le x_{max} \\ x_n^i(j-1)+x_c^i(j-1)-\delta x & \text{if } x_{max}<x_n^i(j-1)+x_c^i(j-1)\le 2x_{max}-2x_{min} \\ x_n^i(j-1)+x_c^i(j-1)-2\delta x & \text{if } 2x_{max}-2<x_n^i(j-1)+x_c^i(j-1) \end{cases} \quad (10)$$

Where i is number of iteration and j is number of cycle.

B. *Decryption Algorithm*

The revised decryption algorithm is as followed.

1) Use secret keys from encryption algorithm as parameter, number of iteration, number of cycle and the selected range of pixels ($[C_{S\text{-}max}, C_{S\text{-}min}]$).

2) Convert the encrypted image containing two dimensional in terms of sequence encryted data x_c.

3) Calculate order of pixels for decryption from range of pixel values in step 1).

4) Recover the image of the j-1 cycle. Start decryption at the last order by using previous order pixels ($x_c^{i-1}(j)$) as initial condition $x_0^i(j-1)$. After n iterations from (1). Subtracting the last order $x_c^i(j-1)$ by $x_n^i(j)$. Continue decryption next step back to first order pixels.

5) Apply last order of j-1 cycle as the initial condition at the first order ($x_0^{first}(j-1)$). After n iterations from (1), we have $x_n^{first}(j-1)$. Subtract the first order $x_c^{first}(j)$ by $x_n^{first}(j-1)$. The subtraction value is used as the initial condition for the subsequent order. If the subtraction value is out of range of chaos system (x_{min}), (13) is applied.

6) Repeat steps 4) – 5) for the next cycles until cycle $j = 0$.

7) Convert the decryted data x_c back to the image containing two dimensional and then convert to the original image with (5).

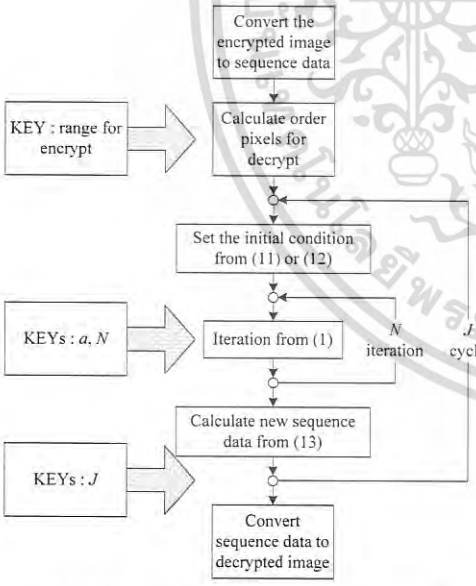


Figure 2. Block diagram of decryption algorithm.

Fig.2 shows the block diagram of the decryption process. The decryption algorithm can be summarized as follows:

$$x_0^i(j-1)=x_c^{i-1}(j) \quad ;if \quad i\neq \text{first order} \quad (11)$$

$$x_0^i(j-1)=x_c^{last}(j-1) \quad ;if \quad i=\text{first order} \quad (12)$$

$$x_c^i(j-1)=\begin{cases} x_c^i(j)-x_n^i(j-1) & \text{if } x_c^i(j)-x_n^i(j-1)\ge x_{min} \\ x_c^i(j)-x_n^i(j-1)+\delta x & \text{if } -x_{max}+2x_{min}<x_c^i(j)-x_n^i(j-1)\le x_{min} \\ x_c^i(j)-x_n^i(j-1)+2\delta x & \text{if } 2x_c^i(j)-x_n^i(j-1)<-x_{max}+2x_{min} \end{cases} \quad (13)$$

IV. Experiment and Results

In this section, we compare and discuss about the decrypted image from CML, CML without inverse function and CML with modify equations but without inverse function.

A. *The Decrypted Image from CML*

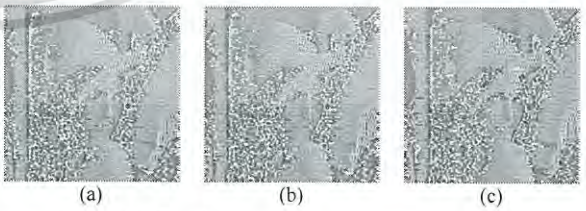
Some information in the decrypted image from CML will not be the same as in original image. Since the rounding function in encryption is not invertible when performing under finite precision [8]. The experimental results of encrypted image and decrypted image are shown in Fig.3 (a) and Fig.4 (a) with $N = 1$ and $J = 1$. The number of changed pixels between the original image and the decrypted image is 7,142 pixels as shown in Table I.

B. *The Decrypted Image from CML without Inverse Function*

When using CML without inverse function in the encryption process, the experimental results of the encrypted image and decrypted image are shown in Fig.3 (b) and Fig.4 (b). The decrypted image is perceptually similar to the original image even some pixels may be altered. In Table I, when using $N = 1$ and $J = 1$ the number of changed pixels between the original image and the decrypted image is 63 pixels.

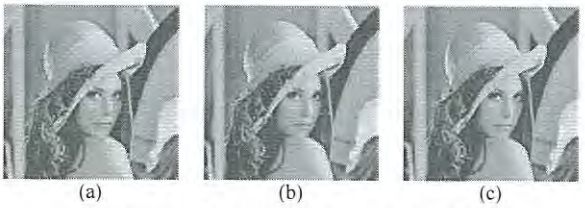
C. *The Decrypted Image from CML with the Proposed Modified CML without Inverse Function*

When using the proposed modified CML in (6) and (7) (by setting $C_{S\text{-}min} = 0$, $C_{S\text{-}max} = 255$) without inverse function in the encryption process, the experimental results of encrypted image and decrypted image are shown in Fig.3 (c) and Fig.4 (c). The decrypted image is the same as the original image. No pixel has been altered.



(a) (b) (c)

Figure 3. Result of encryption with $N = 1$ and $J = 1$.



(a) (b) (c)

Figure 4. Result of decryption with $N = 1$ and $J = 1$.

TABLE I. THE PIXEL CHANGED BETWEEN THE ORIGINAL IMAGE AND THE DECRYPTED IMAGE WITH 24-BIT COLOR AND RESOLUTION OF 125X125 PIXELS.

The number of iterations and number of cycles		Pixel Change
N, J	**Process**	**No. of Pixel**
$N = 1$ $J = 1$	CML	7,142
	CML (without inverse function)	63
	proposed modified CML (without inverse function)	0
$N = 5$ $J = 1$	CML	19,737
	CML (without inverse function)	55
	proposed modified CML (without inverse function)	0
$N = 1$ $J = 5$	CML	21,161
	CML (without inverse function)	96
	proposed modified CML (without inverse function)	0

V. ANALYSIS AND TEST RESULTS

In this section, we discuss about the range of pixel values or intensity selection in encryption process and also the performance of image encryption. The security analysis including visual testing, statistical analysis [9, 10] and gray modification average value [11].

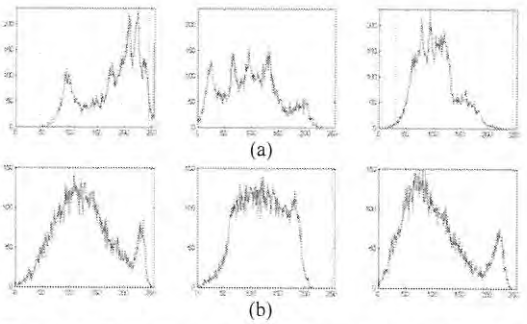
A. *The Selected Pixels for Encryption*

From each image, the range of pixel values for encryption is calculated from median and standard deviation from the image and the constant value r_1, r_2 from (4), (5). This calculated range value is adaptive to the image statistics. Two examples are shown in Fig.5, where each image is in 24-bit color with 125x125 pixels.

(a) (b)

Figure 5. Original Images of (a) Lena Color and (b) Mandril Color.

The range of pixel values for encryption are shown in Fig.6. These different ranges that give unpredictable position of the encrypted pixels are used in encryption, and shown in Table II. The selected pixels for encryption of each color component (red, green, blue) are shown in black color in the Fig.7.



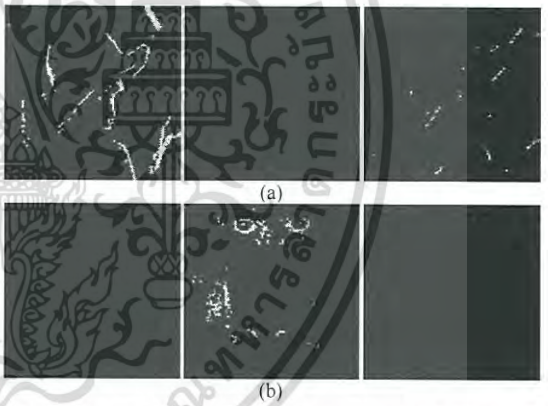
(a)

(b)

Figure 6. Histogram of (a) Lena Color and (b) Mandril Color.

TABLE II. THE RANGE OF PIXEL VALUES FOR ENCRYPTION WITH THRESHOLD $T = 0.03$.

The Original image		Static		Selected encryption range
Name	*Component*	*Median*	*Standard deviation*	*Range*
Lena color	Red	195	49.6624	[46.0128, 244.6624]
	Green	97	52.3535	[44.6465, 254.0605]
	Blue	102	35.8986	[30.2029, 245.5942]
Mandril color	Red	125	52.8001	[19.3997, 230.6003]
	Green	121	42.8364	[35.3271, 249.5093]
	Blue	93	56.6492	[36.3508, 206.2984]



(a)

(b)

Figure 7. Pixels encryption of each color component for (a) Lena color and (b) Mandril color.

B. *Visual Testing*

We choose 3 variations for experiment by varying number of iterations and number of cycles. In visual testing, the encrypted images still have acquired small detail from the original image because some information is not encrypted. Number of iterations and number of cycles for encrypting the image affect the encrypted result. It is seen that increasing the number of cycles give better encrypted results than increasing the number of iterations. The results are shown in Fig.8.

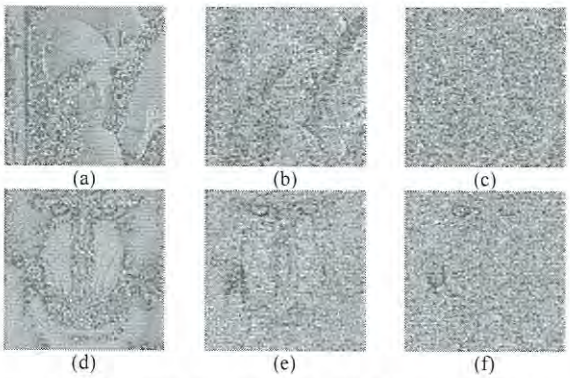


Figure 8. The encrypted image of the lena color with (a) N=1 J=1, (b) N=5 J=1, (c) N=1 J=5 and the encrypted image of the mandril color with (d) N=1 J=1, (e) N=5 J=1, (f) N=1 J=5.

C. *Statistical Analysis*

Image encryption has been successfully analyzed with the help of statistical analysis [9, 10]. Therefore, an ideal encryption should be robust against any statistical attack. We have provided statistical analysis by calculating the histogram and the correlations of two adjacent pixels in the encrypted images.

1) Histogram Analysis

The distribution of the image intensity is presented by the histograms' illustration. The encrypted image should generally have uniform distribution.

Fig.9 shows histogram of the original and the encrypted Lena color image for each color band red, green and blue using the parameter (N = 1, J = 1), (N = 5, J = 1) and (N = 1, J = 5), respectively. The comparison of using the parameter (N = 1, J = 5) and (N = 5, J = 1) is that using more number of cycles gain the better result, as shown in Fig.9 (c) and (d) respectively.

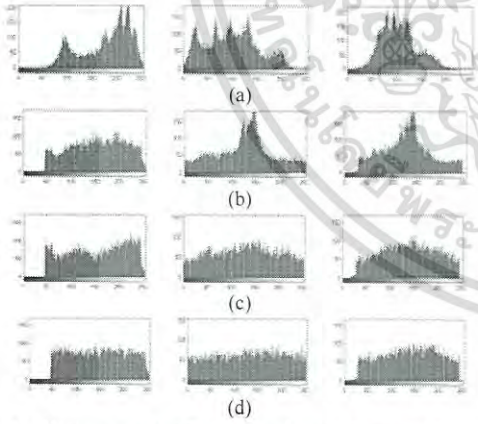


Figure 9. Histogram of (a) The Original Image Lena and (b)–(d) The Encrypted Image.

2) Correlation Coefficient Analysis

The correlation coefficient analysis is a statistical analysis, which calculated the statistical relationship between two horizontally adjacent pixels and two vertically adjacent pixels in encrypted image [9, 10]. Fig.10 frame (a) shows the distribution of two adjacent pixels of the original image Lena color for the distribution of two horizontally adjacent pixels (left) and the distribution of two vertically adjacent (right). Fig.10, (b)-(d) respectively, shows the distribution of two adjacent pixels of the encrypted image Lena color using the parameter (N = 1, J = 1), (N = 5, J = 1) and (N = 1, J = 5) for the distribution of two horizontally adjacent pixels (left) and the distribution of two vertically adjacent (right).

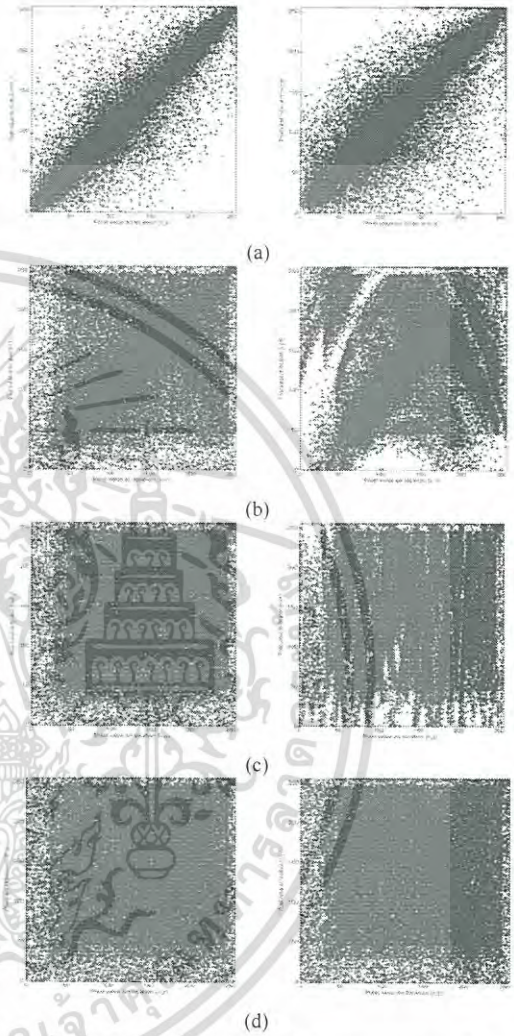


Figure 10. The distribution of two horizontally adjacent pixels (left) and two vertically adjacent (right) (a) the original image lena and (b)–(e) the encrypted image.

We also calculate the correlation between two vertically as well as horizontally adjacent pixels in the original and encrypted images. For this calculation, we use (14) [9, 10]. The result is shown in Table III. When number of iterations and number of cycles are increased, the correlation coefficients for two adjacent pixels are decreased.

$$C_r = \frac{N\sum_{j=1}^{N}\left(x_j \times y_j\right) - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \quad (14)$$

TABLE III. CORRELATION COEFFICIENTS FOR TWO ADJACENT PIXELS IN THE ORIGINAL AND ENCRYPTED IMAGES.

Image	Correlation coefficients				
	Adjacent	*Original Image*	*Encrypted Image*		
			N = 1, J = 1	*N = 5, J = 1*	*N = 1, J = 5*
Lena color	Hor.	0.9049	0.1174	0.1017	0.0564
	Ver.	0.9501	0.2672	0.1226	0.0669
Mandril color	Hor.	0.8605	0.0949	0.0636	0.0365
	Ver.	0.8601	0.2018	0.0718	0.0443

D. Gray Modification Average Value.

The values of pixels in the image encryption have been changed from the original image. Visual testing can show contrast between the original image and the image encryption. The percentage of unchanged point represents percentage of pixels difference. Gray modification average value, called *GAVE*, can measure the changed in value of image encryption. The higher the GAVE value, the better the encrypted image. *GAVE* is defined in (15), where $G = (g_{ij})_{M\times N}$ is the original image and $C = (c_{ij})_{M\times N}$ is the image encryption [11].

$$GAVE(G,C) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|g_{ij} - c_{ij}\right|}{MN} \quad (15)$$

GAVE of all pixels in the image and each color component are shown in Table IV. *GAVE* will increase as both the number of iterations and number of cycles increased.

TABLE IV. GRAY MODIFICATION AVERAGE VALUE.

Image		Gray modification average value		
Name	Color	*N = 1, J = 1*	*N = 5, J = 1*	*N = 1, J = 5*
Lena color	All	17.3049	22.6418	28.3613
	Red	35.9718	40.8712	48.5924
	Green	9.38694	16.30.75	22.1478
	Blue	6.5559	10.7466	14.3436
Mand	All	13.3818	19.6350	25.1134
ril color	Red	16.3702	23.4894	29.4880
	Green	8.3791	15.1858	20.3469
	Blue	15.3962	20.2298	25.5053

VI. CONCLUSIONS

Chaotic Map Lattices is employed in the proposed image encryption and decryption algorithm. CML operates on a parameter, number of iterations and number of cycles as secret keys. We propose the modified CML that can encrypt unpredictable pixels in the images. These pixels are assigned with the intensity which are range of value of pixels selected from the combination between image statistics of median, standard deviation of color components, constants number r_1, r_2 and threshold (T). The range of pixel values for encryption from each color component is the new secret keys in decryption algorithm. From visualization results, we can still recognize scanty information from the original image since there are some unencrypted pixels. Although the proposed method encrypts some pixels in the image, but the location is difficult to guess and decrypted pixels are unpredictable from the violators.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett., vol. 64, pp. 821-824, 1990.

[2] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., vol. 71, pp. 65-68, 1993.

[3] L. Kocarev and U. Parlitz, "General Approach for Chaotic Synchronization with Applications to Communication," Phys. Rev. Lett., vol. 74, pp. 5028-5031, 1995.

[4] D. G. Van Wiggeren and R. Roy, "Communication with Chaotic Lasers," Science, vol. 279, pp. 1198-1200, 1998.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," Phys. Lett. A, vol. 309, pp. 75-82, 2003.

[6] L. Kocarev, M. Sterjev, A. Fekete, and G. Vattay, "Public-key encryption with chaos," Chaos, vol. 14, pp. 1078-1082, 2004.

[7] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," American Institute of Physics. DOI: 10.1063/1.2242052, 2006.

[8] E. Solak and C. Çokal, "Comment on "Encryption and decryption of images with chaotic map lattices"," American Institute of Physics. DOI: 10.1063/1.2966114, 2008.

[9] N. K. Pareek, V. Patidar and K.K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, pp. 926–934, 2006.

[10] S. Liu, J. Sun and Z. Xu, "An Improved Image Encryption Algorithm based on Chaotic System," Journal of Computers, vol. 4, no. 11, pp. 1091-1100, November 2009.

[11] Q. Li and Y. Wang, "The Performance Analysis of Image Encryption Algorithm Based on Chaotic System," International Conference on Electronic & Mechanical Engineering and Information Technology, 978-1-61284-088-8/11/, pp. 3492–3494, 2011.

Adaptive Pixel-Selection Using Chaotic Map Lattices for Image Cryptography

Jirasak Sittigorn[1], Kitti Paithoonwattanakij[2], and Charray Surawatpunya[3]
Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang,
Bangkok, 10520 Thailand
[1] jirasak@live.kmitl.ac.th, [2] kpkitti@kmitl.ac.th, [3] kscharra@kmitl.ac.th

ABSTRACT

Chaotic theory has been used in cryptography application for generating a sequence of data that is close to pseudorandom number based on an adjusted initial condition and a parameter. However, data recovery becomes a crucial problem due to the precision of the parameters. This difficulty leads to limited usage of Chaotic-based cryptography especially for error sensitive applications such as voice cryptography. In order to enhance the encryption security and overcome this limitation, an Adaptive Pixel-Selection using Chaotic Map Lattices (APCML) is proposed. In APCML, the encryption sequence has been adaptively selected based on chaos generator. Moreover, the chaotic transformation and normalization boundary have been revised to alleviate the rounding error and inappropriate normalization boundary problems. In the experiments, the measurement indices of originality preservation, visual inspection, and statistical analysis are used to evaluate the performance of the proposed APCML compared to that of the original CML. Consequently, the APCML algorithm offers greater performance with full recovery of the original message.

Keywords: Chaotic Map Lattices, Image cryptography, Adaptive Pixel-Selection.

1. INTRODUCTION

Secure communication is crucial for business communication especially when the communication is through the public network such as the Internet [1-6]. Personal internet banking and military communication are two sample applications that clearly require a secure communication. Typical method to protect data confidentiality is to use a cryptographic algorithm to hide the data called plain text. The cryptographic algorithm encrypts the plain text to a ciphered text using a key or keys, and it decrypts the ciphered text back to the plain text [5]. Symmetric cryptography used the same key or keys for encryption and decryption while asymmetric cryptography uses different keys for encryption and decryption. Since the symmetric cryptography shared keys when transforming a message back and forth, it becomes a target of attacking from an intruder. An attack can simply try different keys until the plain text is found.

Recently, chaotic theory is applied to the symmetric cryptography. The chaotic theory is a field of science that studies behavior of nonlinear dynamic systems that are highly sensitive to small variation of an initial condition. With small different initial conditions, output of a dynamic system is greatly deviated. Therefore, initial conditions and system parameters are used as keys for the chaotic cryptography. The nature of a chaotic system makes a dictionary attack impractical. Chaotic Map Lattices (CML) [7] is a cryptographic algorithm using the chaotic theory. Without knowledge of keys used in an encryption process, the decryption is difficult. The keys for the CML are parameters, number of iterations, and number of cycles. Precision of each value used in the process is crucial for cryptography accuracy. The need of high precision becomes a drawback in using the CML cryptography since the plain text may be irrecoverable due to the rounding function used in the process [8]. Therefore, it limits the use of CML cryptography to applications that are sensitive to small error such as an image, audio, or video cryptography. When CML is applied to image cryptography, it encrypts and decrypts every pixel of an image. The CML algorithm uses an initial condition from the previous pixel in sequence for the current encrypting pixel. As a result, it is possible to decrypt all the sequence of the encrypted pixels if the intruder can guess secret keys and the initial condition of the first pixel. In order to enhance the encryption security, an Adaptive Pixel-Selection using Chaotic Map Lattices (APCML) algorithm is proposed, where the encryption sequence has been adaptively selected. Even though the intruder can guess the secret keys and the initial condition of the first pixel, it is quite difficult to acquire the whole encryption sequence. Another limitation of the CML is its rounding error during chaotic transformation, which has been eliminated by removing the rounding process. The normalization

Fifth International Conference on Graphic and Image Processing (ICGIP 2013), edited by Yulin Wang, Xudong Jiang, Ming Yang, David Zhang, Xie Yi, Proc. of SPIE Vol. 9069, 906915 · © 2014 SPIE
CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2050858

boundary of CML also introduces errors during decryption. Therefore, the normalization boundary has been modified in APCML in order to fully recover the original message. The remainder of this paper is organized as follows. Section 2 describes the chaotic system and proposed modified chaotic map lattices while section 3 explains encryption and decryption algorithm using APCML. Section 4 illustrates results and analysis. Finally, the conclusions are discussed in section 5.

2. CHAOTIC SYSTEM

One of the well known chaotic systems is a logistic map, which is a polynomial mapping of degree two, and is given by:

$$x_{n+1} = a\, x_n \left(1 - x_n\right) \tag{1}$$

where x_n and a are the system variable and parameter, respectively. n is the number of iterations and x_0 is an initial condition. The system variable and parameter in (1) influence chaos system when $0 < x_n < 1$, $3.57 < a < 4$, $x_{\max} = a/4$ and $x_{\min} = a^2/4 \times (1 - a/4)\, x_{max}$.

The idea of encryption is that the image can be represented as a lattice of pixels. The pixel color is the combination of the three components: red, green, and blue shown as $C = (C_r, C_g, C_b)$. CML encryption creates x_c by processing each of color component in parallel $x_c = (x^r_c, x^g_c, x^b_c)$. Normally, value of each component is an integer between 0 and 255. This leads to the normalization parameter of 256 in the CML. However, using this normalization parameter causes errors during the decryption due to rounding errors. Therefore, the normalization boundary has been modified in APCML to the range of -1 to 255, which results in normalization parameter of 257 as shown in equation (2).

$$x_c = x_{min} + \delta x (C + 1)/(257) \tag{2}$$

where $\delta x = x_{\max} - x_{\min}$. To extract the value of color component, the inverse function is applied as the following:

$$C = \text{round}[(x_n - x_{min})(257)/\delta x - 1] \tag{3}$$

where round is rounding function that replaces a numerical value to integer. With the modified normalization boundary, it results in complete recovery of the original pixel values.

3. APCML ENCRYPTION AND DECRYPTION ALGORITHM

The proposed Adaptive Pixel-Selection using Chaotic Map Lattices (APCML) applies the CML and generates a sequence of pixels based on new keys in another chaotic process.

3.1 Encryption Algorithm

The revised encryption algorithm composes of the following steps as illustrated in Fig. 1 (a). The encryption algorithm can be summarized in the following equation (4)-(6).

$$x^i_0(j) = x^{last}_e(j-1) \quad ;if \quad i = 1^{st} \tag{4}$$

$$x^i_0(j) = x^{i-1}_e(j) \quad ;if \quad i \neq 1^{st} \tag{5}$$

$$x^i_s(j) = \begin{cases} x^i_n(j-1) + x^i_s(j-1) & if \;\; x^i_n(j-1) + x^i_s(j-1) \le x_{\max} \\ x^i_n(j-1) + x^i_s(j-1) - \delta x & if \;\; x_{\max} < x^i_n(j-1) + x^i_s(j-1) \le 2x_{\max} - 2x_{\min} \\ x^i_r(j-1) + x^i_s(j-1) - 2\delta x & if \;\; 2x_{\max} - 2x_{\min} < x^i_n(j-1) + x^i_s(j-1) \end{cases} \tag{6}$$

3.2 Decryption Algorithm

The revised decryption algorithm, Fig 1. (b), can expressed in the following equation (7)-(9).

$$x_0^i(j-1) = x_\varepsilon^{i-1}(j) \quad ;if \quad i \neq 1^{st} \tag{7}$$

$$x_0^i(j-1) = x_\varepsilon^{last}(j-1) \quad ;if \quad i = 1^{st} \tag{8}$$

$$x_\varepsilon^i(j-1) = \begin{cases} x_\varepsilon^i(j) - x_n^i(j-1) & if \;\; x_\varepsilon^i(j) - x_n^i(j-1) \geq x_{min} \\ x_\varepsilon^i(j) - x_n^i(j-1) + \delta x & if \;\; -x_{max} + 2x_{min} \leq x_\varepsilon^i(j) - x_n^i(j-1) < x_{min} \\ x_\varepsilon^i(j) - x_n^i(j-1) + 2\delta x & if \;\; 2x_\varepsilon^i(j) - x_n^i(j-1) < -x_{max} + 2x_{min} \end{cases} \tag{9}$$

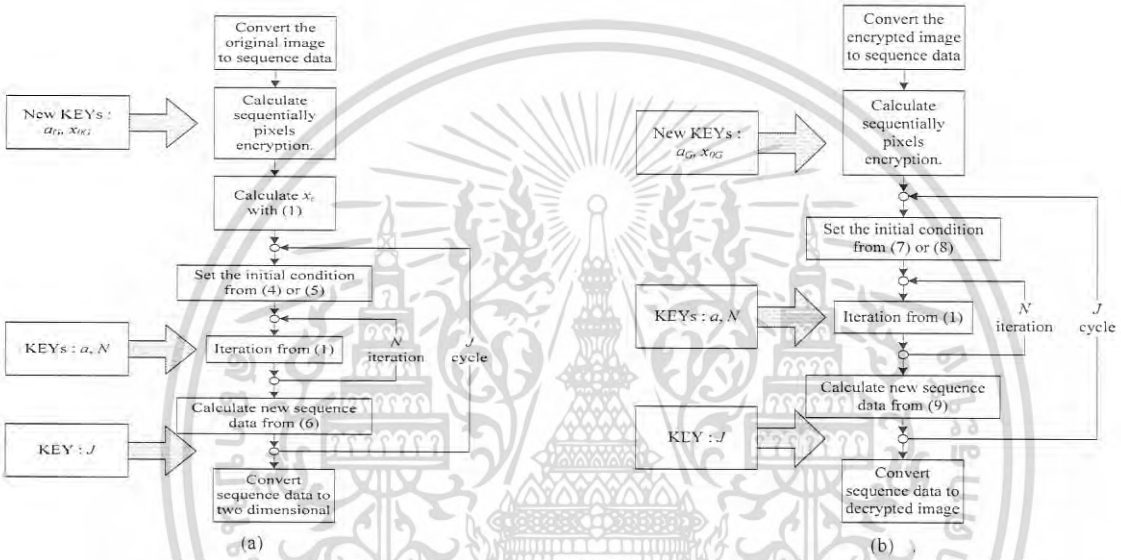


Figure 1. Block diagram for (a) encryption algorithm and (b) decryption algorithm.

4. ANALYSIS AND TEST RESULTS

In the experiments, Lena and Cameraman images with the size of 128 × 128 pixels are used for performance evaluation of the proposed APCML. The performance of the proposed APCML is compared to that of the original CML using measurement of originality preservation, visual inspection, and statistical analysis [9, 10]. The secret keys chosen for the experiments are the parameter $a = 3.9$, and the system variable is between $x_{min} = 0.095062$ and $x_{max} = 0.975000$ as suggested in [7]. The number of iterations and number of cycles as $N = 1$ to 7 and $J = 1$ to 7. The secret keys are defined in the encryption sequence for the gray image as $a_G = 3.9$ and $x_{0G} = 0.5$.

4.1 Originality Preservation

The efficient encryption and decryption algorithm should not alter the original message. In this experiment, we compare the results of decrypted images from the proposed APCML and the original CML in terms of the number of altered pixels and the mean square errors as shown in Table I. The decrypted images from both algorithms are illustrated in Fig. 2 (a)-(d). The white dots in Fig. 2 (e)-(f) represent the altered pixels from the CML algorithm. The limitations of rounding process and the normalization boundary in the CML result in large errors. However, with the proposed APCML, the problems have been solved thus the originality of the test images are completely preserved.

Figure 2. The decrypted image of lena color from (a) CML (J=1 N=1), (b) CML (J=7 N=7), (c) APCML (J=1 N=1) and (d) APCML (J=7 N=7). Show changed pixel of original for (e) CML (J=1 N=1) and (f) CML (J=7 N=7).

TABLE I. THE NUMBER OF CHANGED PIXELS AND MEAN SQUARED ERROR (MSE) BETWEEN THE ORIGINAL IMAGE AND THE DECRYPTED IMAGE.

The number of iterations and number of cycles		**No. of Pixel Change**	**MSE**
J, N	***Process***		
$J = 1$	original CML	2978	0.2147
$N = 1$	APCML	0	0.0000
$J = 7$	original CML	4487	60.8459
$N = 7$	APCML	0	0.0000

4.2 Visual Inspection

The encryption causes changes in pixel values. The larger the changes, the higher the encryption quality. Therefore, visual inspection can be used as another measurement index. The encrypted images should contain large changes thus less visual details of the original images. Fig. 3 shows the encrypted Lena and Cameraman images with four pairs of the number of iterations and number of cycles of $J = 1$ $N = 1$, $J = 1$ $N = 2$, and $J = 2$ $N = 1$. From Fig. 3, the results show that the CML and the proposed APCML deliver high encryption quality when the number of iteration and the number of cycle are greater than $N = 1$ and $J = 1$. We observe that with the correlation less than 0.05 the encrypted images could conceal most of the details of the original images, which indicates high encryption quality of the encryption algorithm.

Figure 3. The encrypted image. (a) Lena with CML encryption, (b) Cameraman with CML encryption, (c) Lena with APCML encryption, and (d) Cameraman with APCML encryption.

4.3 Statistical Analysis

The statistical analysis was diagnosed in image encryption [9, 10]. An encryption result should be robust against any statistical attack. The histograms of the test images and the correlations of two adjacent pixels in the encrypted images are simulated for statistical analysis.

4.4 Histogram Analysis

It is important to verify that there is no statistical similarities between the encrypted and original images in order to prevent the leakage of information to the attackers. The statistical similarity can be illustrated in term of histograms, which present the distribution of the pixel intensity in images. Histogram of the Lena original image is shown in Fig. 4 (a). Fig. 4 (b)-(e) shows histogram of the encrypted image using APCML. The histogram of original image contains large fluctuation while that of the encrypted image are close to uniform distribution. They are significantly different from original image. This shows that no statistical similarity appears between the encrypted and original images.

The histogram of the image using APCML is approximate to the uniform distribution. When the number of cycle are greater than one; *i.e.*, $J > 1$, the histograms of the encrypted image are uniformly distributed.

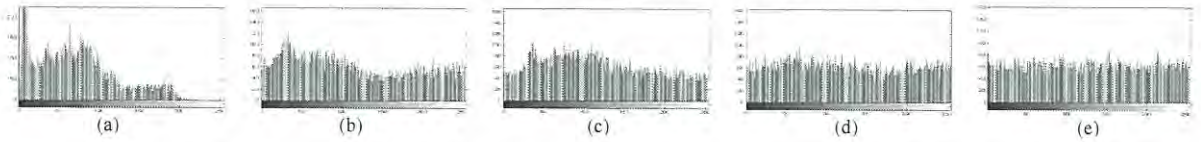


Figure 4. Histogram of (a) the original image and the encrypted image (b) APCML ($J = 1$ $N = 1$), (c) APCML ($J = 1$ $N = 2$) (d) APCML ($J = 2$ $N = 1$) and (e) APCML ($J = 7$ $N = 7$).

4.5 Correlation Coefficient Analysis

The correlation coefficient analysis is one of the important statistical analysis tools, which measures the statistical relationship between two horizontally adjacent pixels and two vertically adjacent pixels in encrypted image [9, 10]. For effective image cryptography, all the attributes of the original images should be concealed, and the encrypted images should be highly uncorrelated. If the original and encrypted images are uncorrelated or totally different, their correlation will be very low or close to zero. If they are identical, their corresponding correlation will be equal to one. Fig. 5 shows the distribution of two vertically adjacent pixels and two horizontally adjacent pixels. Fig. 5 (a) shows the distribution of the original Lena image. Fig. 5 (b-c) show the distribution of the encrypted Lena image from CML and APCML with $J = 1$ $N = 1$. The distribution of the encrypted Lena image from CML and APCML with $J = 3$ $N = 3$ are shown in Fig. 5 (d-e).

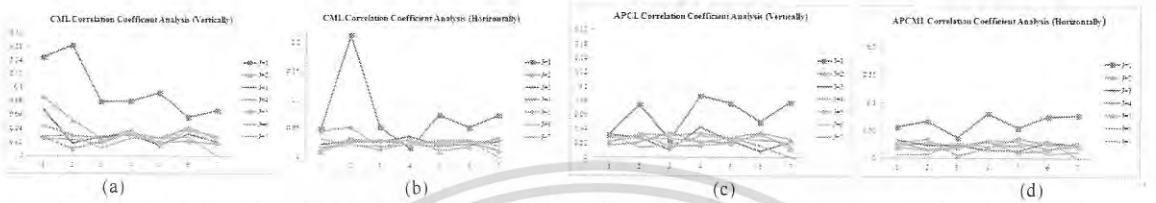
Figure 5. The distribution of two vertically adjacent pixels and two horizontally adjacent pixels of (a) the original and encrypted Lena image with (b) CML ($J = 1$ $N = 1$), (c) ACML ($J = 1$ $N = 1$), (d) CML ($J = 3$ $N = 3$) and (e) ACML ($J = 3$ $N = 3$).

4.6 Cross-correlation Equation

The cross-correlation technique is a method to get the displacement information of two consecutive images by comparing the similarity of a pair of image signals [6-8]. The cross-correlation between two vertically and two horizontally adjacent pixels in the original and encrypted images are calculated using (10) [9, 10]. Fig. 6 (a-b) demonstrates correlation coefficient analysis with CML encryption for vertical and horizontal directions with various combinations of N and J parameters. The correlation coefficient analysis with APCML encryption is shown in Fig. 6 (c-d). It can be seen that, to achieve the correlation less than 0.05 for all variations of N, it limits the values of J greater than 5 for the CML thus greater than 2 for the APCML. From the results, it demonstrates that the APCML permits larger variation of secret keys with higher encryption quality for all parameters.

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) \times \left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \quad (10)$$

where x_j is intensity of pixel at location (x, y), y_j is intensity of pixel at location $(x+1, y)$ for the cross-correlation of two vertically and y_j is intensity of pixel at location $(x, y+1)$ for the cross-correlation of two horizontally.



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

Figure 6. Correlation Coefficient Analysis for various combinations of J and N parameters (a) vertical directions of CML, (b) horizontal directions of CML, (c) vertical directions of APCML and (d) horizontal directions of APCML

5. CONCLUSION

This paper proposes an Adaptive Pixel-Selection using Chaotic Map Lattices (APCML) to enhance the encryption security and overcome the limitation of the original CML. In APCML, the encryption sequence has been adaptively selected based on chaos generator. Even though the intruder can guess the secret keys and the initial condition of the first pixel, it is quite difficult to acquire the whole encryption sequence. Moreover, the chaotic transformation and normalization boundary have been revised to alleviate the rounding error and inappropriate normalization boundary problems. In the experiments, the measurement indices of originality preservation, visual inspection, and statistical analysis are used to evaluate the performance of the proposed APCML compared to that of the original CML. The experimental results show the performance improvement of the APCML over that of the original CML with full recovery of the original message.

REFERENCES

[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett., 64, pp. 821-824, 1990.

[2] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., 71, pp. 65-68, 1993.

[3] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," Phys. Rev. Lett., 74, pp. 5028-5031, 1995.

[4] D. G. Van Wiggeren and R. Roy, "Communication with chaotic lasers," Science, 279, pp. 1198-1200, 1998.

[5] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," Phys. Lett. A, 309, pp. 75-82, 2003.

[6] L. Kocarev, M. Sterjev, A. Fekete, and G. Vattay, "Public-key encryption with chaos," Chaos, 14, pp. 1078-1082, 2004.

[7] A. N. Pisarchik, N. J. Flores-Carmona and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," American Institute of Physics. DOI: 10.1063/1.2242052, 2006.

[8] E. Solak and C. Çokal, "Comment on "Encryption and decryption of images with chaotic map lattices"," American Institute of Physics. DOI: 10.1063/1.2966114, 2008.

[9] N. K. Pareek, V. Patidar and K.K. Sud, "Image encryption using chaotic logistic map," Image and Vision Computing, vol. 24, pp. 926–934, 2006.

[10] S. Liu, J. Sun and Z. Xu, "An improved image encryption algorithm based on chaotic system," Journal Of Computers, vol. 4, no. 11, pp. 1091-1100, November 2009.

academicJournals

Vol. 10(17), pp. 531-543, 15 September, 2015
DOI: 10.5897/SRE2015.6248
Article Number: CD9CA3846875
ISSN 1992-2248

http://www.academicjournals.org/SRE

Scientific Research and Essays

Full Length Research Paper

Adaptive Pixel-Selection Fractional Chaotic Map Lattices for image cryptography

Jirasak Sittigorn* and Kitti Paithoonwattanakij

Faculty of Engineering, King Mongkut s Institute of Technology Ladkrabang, Chalongkrung Rd., Ladkrabang, Bangkok, 10520, Thailand.

Received 6 May, 2015 Accepted 20 July, 2015

Chaotic theory has been employed in cryptography application for establishing a sequence of data closest to pseudorandom number. Image cryptography with Chaotic Map Lattices (CML) uses the chaos parameters, the number of iterations and the number of cycles for encryption as secret keys. Amount of secret keys has a great impact on security in cryptography. Adaptive Pixel-Selection Fractional Chaotic Map Lattices (APFCML) enhances the encryption security by introducing a novel non-integer fractional order concept as secret keys. Fractional chaos is modified chaos with a fractional differential equation containing derivatives of non-integer order. A non-integer order has an effect on the range of chaos's parameter. Moreover, the encryption sequence has been adaptively selected based on another chaos generator. In the experiments, the measurement indices of originality preservation, visual inspection, and statistical analysis are used to evaluate the performance of the proposed APFCML compared to that of the original CML.

Key words: Chaotic, fractional logistic, image cryptography, Lyapunov exponent, bifurcation diagram.

INTRODUCTION

In the current trends, the communication is through the public network such as the Internet. The secure communication is crucial for business communication (Pecora and Carroll, 1990 Van Wiggeren and Roy, 1998). Electronic banking and military communication are two sample applications that clearly require a secure communication. The cryptographic algorithm is a method to protect plain text by changing it to data confidentiality. The cryptographic algorithm encrypts the plain text to a ciphered text using a key or keys, and it decrypts the ciphered text back to the plain text (Pareek et al., 2003).

Symmetric-key cryptography is algorithms for cryptography used the same keys for both encryption and decryption while asymmetric cryptography uses different keys for encryption and decryption. Since the symmetric-key cryptography shared keys when transforming a message back and forth, it becomes a target of attacking from an intruder. An attack can simply try different keys until the plain text is found.

The chaotic theory has been applied to the symmetric-key cryptography. It is a field of science that studies behavior of nonlinear dynamic systems that are highly

**Corresponding author. E-mail: jirasak@live.kmitl.ac.th.

sensitive to small variation of an initial condition. The output of a dynamic system is greatly deviated when initial conditions or parameters are changed. Therefore, initial conditions and system parameters are used as keys for the chaotic cryptography. The nature of a chaotic system makes a dictionary attack impractical. Chaotic Map Lattices (CML) (Pisarchik et al., 2006) is a cryptographic algorithm using the chaotic theory. Without knowledge of keys used in an encryption process, the decryption is practically difficult. The keys for the CML are chaotic parameters, number of iterations, and number of cycles. The parameters are variables in a logistic map that is well known chaotic systems. The limitation of a logistic map is the value of the parameter between 3.57 and 4. Therefore, a logistic map was chaos. When CML is applied to image cryptography, it encrypts and decrypts every pixel of an image. The CML algorithm uses an initial condition from the previous pixel in sequence for the current encrypting pixel. As a result, it is possible to decrypt all the sequence of the encrypted pixels if the intruder can guess secret keys and the initial condition of the first pixel. In order to enhance the encryption security, an Adaptive Pixel-Selection Fractional Chaotic Map Lattices (APFCML) algorithm is proposed, where the encryption sequence has been adaptively selected. Even though the intruder can guess the secret keys and the initial condition of the first pixel, it is quite difficult to acquire the whole encryption sequence. Another limitation of the CML algorithm is the amount of secret keys. The presented APFCML algorithm is based on fractional order and a parameter of fractional chaos with fractional-order as a new secret key. The fractional-order system is a dynamical system that can be modeled by a fractional differential equation containing derivatives of non-integer order (Mon e et al., 2010). Fractional chaos is the chaotic system when fractional-order and the selected parameters are appropriate. Each fractional-order offers difference boundary of parameter. The remainder of this paper is organi ed as follows. The methodology section describes the chaotic system, the fractional order logistic model, lyapunov exponent, bifurcation diagram, fractional chaotic system, and encryption and decryption algorithm using APFCML.

METHODOLOGY

Chaotic system

A logistic map is the well known chaotic systems, which is a polynomial mapping of degree two, and is given by:

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

Where x_n is the system variable, r is the parameter, n is the number of iterations and x_0 is an initial condition. The system variable and parameter lead to chaotic system when $x_{\min}$ x_n $x_{\max}$, 3.57 r 4, $x_{\max} = \frac{r}{4}$ and $x_{\min} = \frac{r^2}{4}\left(1 - \frac{r}{4}\right)$.

Fractional order logistic model

The fractional order logistic model was the mathematical form accomplished by integral and derivative of fractional order (Podlubny, 1999). This mathematical field may be considered as old topic since it is been developed for more than a century (Podlubny, 1999). Recently, this mathematical theory has applied to many modem applications in physics and engineer (Petras, 2006 Sabatier et al., 2007). The fractional order logistic equation is obtained by apply the fractional operator to the logistic equation as follow:

$$\frac{d^n x^\mu}{dx^n} = \frac{\Gamma(\mu+1)}{\Gamma(\mu-n+1)} x^{\mu-n} \tag{2}$$

Where $\Gamma(\ )$ is the Gamma function. The Gamma function is defined as $n! = \Gamma(n+1)$.

The fractional order logistic model is operated by fractional derivative of logistic equation. The model is initially published by Pierre Verhulst (Pasti n, 2006). First order ordinary differential equation describes the continuous model. The discrete model discloses the chaotic property in certain regions (Alligood et al., 1996). The logistic Equation (1) is written as the sigmoid function as $f(x) = rx(1-x)$.

The fractional order logistic equation is obtained by applies the fractional operator to the logistic equation as follows:

$$D_x^\alpha f(x) = \frac{r x^{1-\alpha}}{\Gamma(\alpha+2)}\left(1 - \frac{2x}{\alpha+2}\right) \tag{3}$$

Where $D_x^\alpha f(x)$ is the α order derivative of a function $f(x)$, r is parameter, α is fractional order when $-\infty < \alpha < \infty$.

The result of the fractional logistic equation becomes chaotic system at some of parameter. Figures 1 and 2 illustrates the results with the number of iterations n 1-6. It can be seen that the chaotic behavior trends of fractional logistic equation arises at parameter $r = 6$ for order $\alpha = \frac{1}{2}$ and parameter $r = 5$ for order $\alpha = \frac{1}{4}$. The Lyapunov exponent and bifurcation diagram are tools for indicating chaos system.

Lyapunov exponent

In mathematics, the Lyapunov exponent is quantified the average stability for describing the discrete dynamical system which can compute from the result of numerical simulation or a physical experiment (Alligood et al., 1996 Moon, 2004). The characteristics of Lyapunov exponents are analy ed by the linear stability of non periodic system. An indicator is the typical rate of exponential divergence of nearby tra ectories (Alligood et al., 1996 Suansook and Paithoonwattanaki , 2014). This quantity is characteri es the rate of separation of nearby close tra ectories. The differences of initial condition and tra ectories are provided the different in rate of separation. The dynamic system predictability is determined by the largest Lyapunov exponent. The positive value of Lyapunov

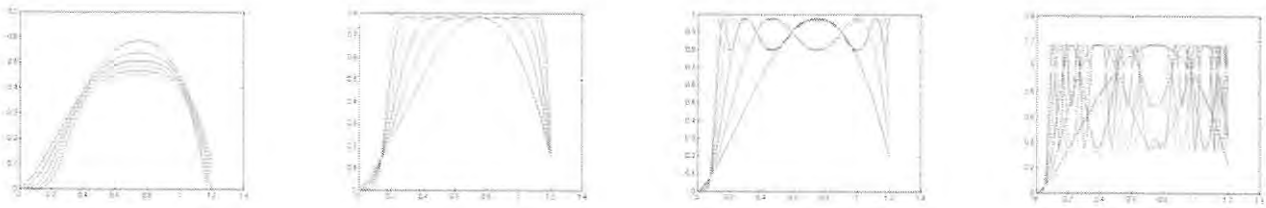


Figure 1. Result of fractional logistic equation for the number of iterations n 1-6 at order $\alpha = \frac{1}{2}$.

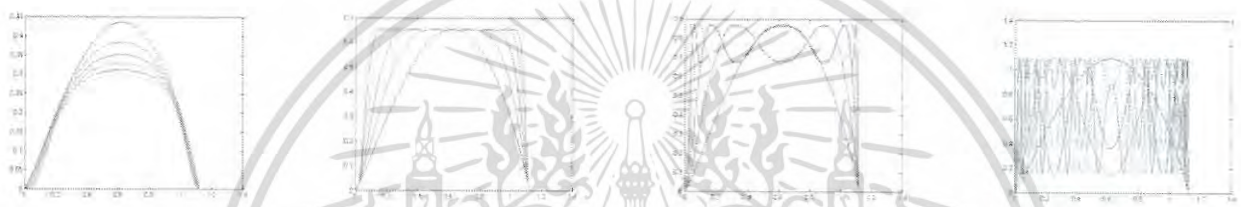


Figure 2. Result of fractional logistic equation for the number of iterations n 1-6 at order $\alpha = \frac{1}{4}$.

exponent is an indication that the system is chaotic (Alligood et al., 1996 Afraimovich and Hsu, 2002). The term Lyapunov exponent or exponential rate of divergence per iteration is defined as followed:

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \ln \left| \frac{df(x_i)}{dx} \right|_{x_i} \quad (4)$$

Where $\frac{df(x_i)}{dx}$ is the derivative of a function $f(x_i)$, λ is the Lyapunov exponent.

The Lyapunov exponent of fractional order logistic model can be calculated from the Equations (3) and (4). The numerical results of Lyapunov exponent of fractional logistic model for different order are shown in Figure 3.

Bifurcation diagram

Bifurcation theory was studies of changes in the qualitative of periodic point structure of dynamical systems, which is varying with time. The parameters are changed in a dynamical system, the stability of the balance points can change as well as the number of balance points. The values of parameters at which the qualitative or topological nature changes are known as critical or bifurcation values (Baker and Gollub, 1990). This occurs where a linear stability analysis yields an instability which characteri ed by a growth rate of a perturbation of the base solution. In dynamical system, a bifurcation diagram shows the possible long-term values either fixed points or periodic of a system as a function of a bifurcation parameter. In general, the bifurcation diagram represents stable solutions with solid line and unstable solutions with a dotted line. The theory of bifurcation is to study how the equilibrium points changes with the parameters (Suansook and Paithoonwattanaki, 2006). The bifurcation diagrams of the fractional order logistic equation for different order are illustrated in Figure 4.

Results of Lyapunov exponent and bifurcation diagram for each fractional order are used to describe the chaotic of fractional order logistic equation. The equation become chaotic when Lyapunov exponent value is greater than ero or Bifurcation Diagram are many values at the either fixed point (Table 1).

Image cryptography with regular CML considers the chaos parameters from a logistic map as one of secret keys. A logistic map becomes the chaotic system when the value of the parameter is between 3.57 and 4. However, in the proposed APFCML, the fractional logistic equation is chosen as additional secret keys. With dual sets of the secret keys, the encryption key length is extensive, thus the encryption security can be greatly intensifie.

The Lyapunov exponent and Bifurcation diagrams of fractional order logistic model are presented in Figures 3 and 4 respectively in order to illustrate the possibility of chaotic behavior in each fractional order. Even though the chaotic properties in fractional order logistic model depend on the same parameters as that of the logistic map, the order parameter is not restricted. Table 1 presents 10 samples of chaotic behavior cases with the order of fractional up to 9. With other fractional, the chaotic behavior can also be achieved. This leads to extensive selection of the fractional order parameters.

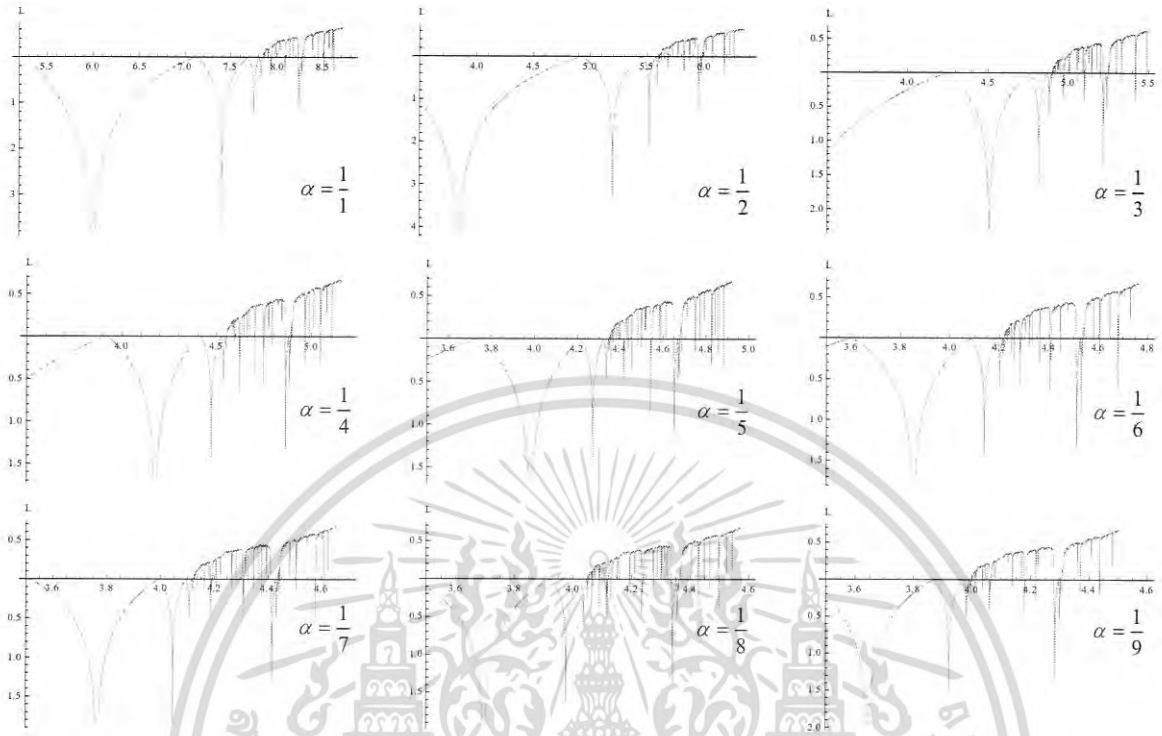


Figure 3. The Lyapunov exponent of fractional order logistic model at fractional order α.

Fractional chaotic system

The fractional logistic equation of order α in Equation (3) is rewritten in a logistic map as followed.

$$x_{n+1} = \frac{r x_n^{1+\alpha}}{\Gamma(\alpha+2)}\left(1-\frac{2x_n}{\alpha+2}\right) \tag{5}$$

Where x_n are the system variable, r is the parameter, n is the number of iterations x_0 is an initial condition and α is fractional order. For all $x \geq 0$ and $\alpha > 0$, $x_{\max}$ and $x_{\min}$ are as following.

$$x_{\max} = \frac{r(1+\alpha)^{1+\alpha}}{2^{1+\alpha}\Gamma(\alpha+2)}\left(1-\frac{\alpha+1}{\alpha+2}\right) \tag{6}$$

$$x_{\min} = \frac{r\left(\frac{r(1+\alpha)^{1+\alpha}}{2^{1+\alpha}\Gamma(\alpha+2)}\left(1-\frac{\alpha+1}{\alpha+2}\right)\right)^{1+\alpha}}{\Gamma(\alpha+2)}\left(1-\frac{2\left(\frac{r(1+\alpha)^{1+\alpha}}{2^{1+\alpha}\Gamma(\alpha+2)}\left(1-\frac{\alpha+1}{\alpha+2}\right)\right)}{\alpha+2}\right) \tag{7}$$

The image encryption, the image can be represented as a lattice of pixels. The color image is a combination of the three components: red, green, and blue shown as $C=(C_r, C_b, C_g)$. Encryption creates x_c by processing each of color component in parallel $x_c = (x_r, x_b, x_g)$. Normally, value of each component is an integer between 0 and 255. APFCML converts the integer value into the range of chaotic system variable by using the following transformation.

$$x_c = x_{min} + \delta x(C+1)/(257) \tag{8}$$

Where $\delta x = x_{\max} - x_{\min}$. To extract the value of color component, the inverse function is applied as followed:

$$C = \text{round}[(x_n - x_{min})(257)/\delta x - 1] \tag{9}$$

Where round is rounding function that replaces a numerical value to integer. With the modified normali ation boundary, it results in complete recovery of the original pixel values.

Encryption and decryption algorithm

The revised encryption algorithm composes of the following steps.

Encryption algorithm

(1) Define secret keys as number of iteration (N), number of cycle (J). Define the new secret keys as fractional order α, parameter of fractional order r, chaotic parameters r_G and initial condition x_{G0}.

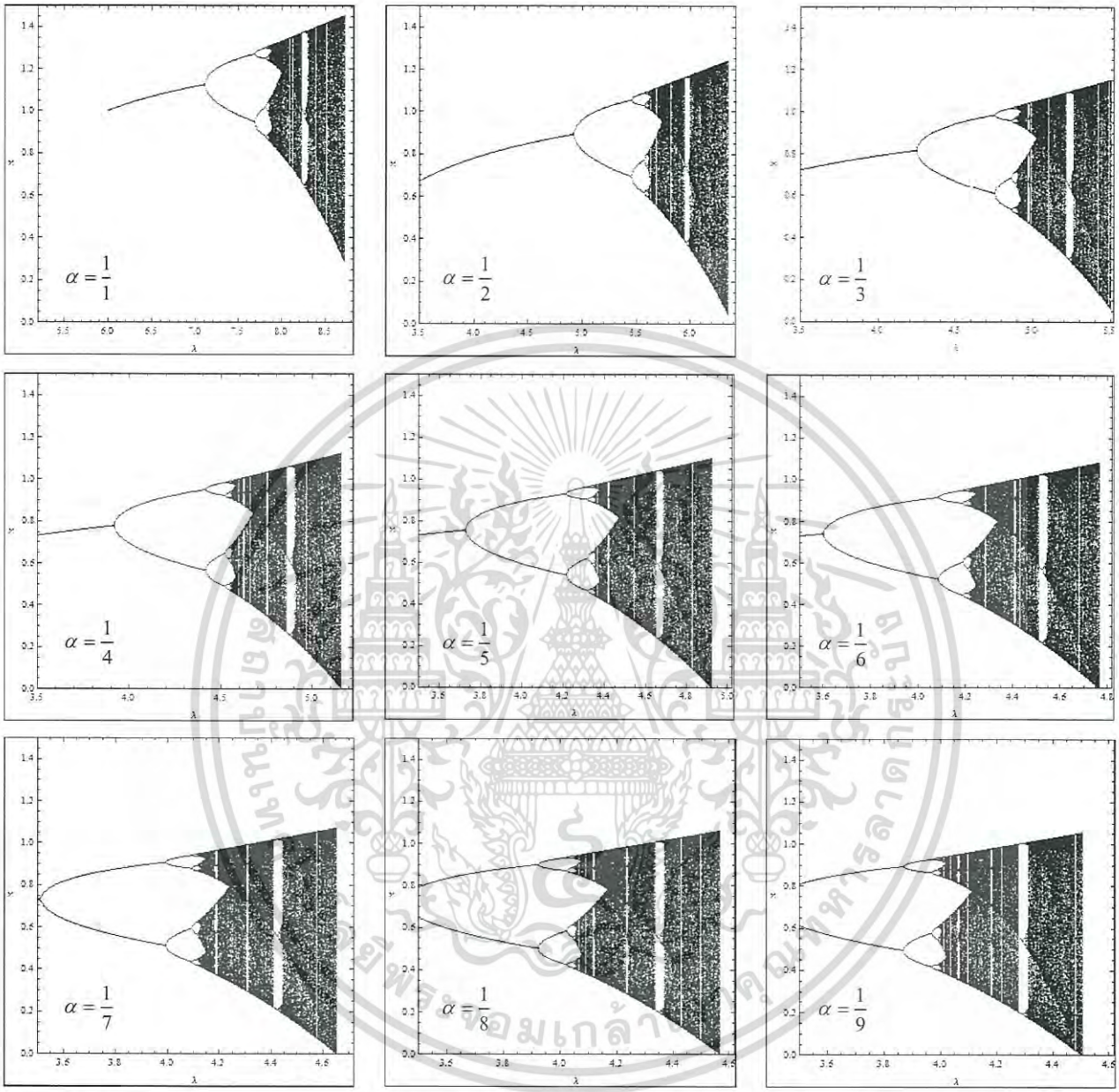


Figure 4. Bifurcation Diagram of fractional order logistic model at fractional order α .

(2) Convert two image containing two dimensional pixels (*Row Column* *m* pixels) into a sequential pixel of si e m (i 1, 2, 3, ..., *m*), which its value is calculated in terms of variable C .

(3) Calculate sequential data m from the equation (1) with new secret keys (r_G and x_{G0}) in step 1). Sort sequential data as sequential pixels for encryption.

(4) Calculate x_C with Equation (8) of pixel *I* with new secret keys (α and r).

(5) Use the value of the last first element in sequential pixel in step 4) (x_c^{last}) as the initial condition for the first element in sequential pixel (x_0^{first}).

(6) Obtain the mapping variable x_n^{first} by iterating *N* times of the first element in sequential pixel from Equation (10). Add the mapping variable x_n^{first} and the value of pixel (x_c^{first}). The sum of value is applied as the initial condition for the subsequent order. Sometime, sum of value is over range of chaos system (x_{max}). We used the condition in Equation (12) to solve the problem. Iterate all maps subsequently starting from the first element in sequential pixel and going through encrypt image pixels, pixel by pixel, toward the last element in sequential pixel. The new x_c is the latest result of this cycle.

Table 1. The rank of parameter for chaos system.

Fractional order	Parameter
1/1	7.85-8.72
1/2	5.61-6.35
1/3	4.90-5.5
1/4	4.55-5.15
1/5	4.35-4.92
1/6	4.22-4.77
1/7	4.13-4.65
1/8	4.05-4.57
1/9	4.00-4.51

(7) Use the last element in sequential pixel (x_c^{last}) of previous cycle in step 7) as an initial condition for the first element in sequential pixel in the new cycle. Repeat step 6) overall the number of cycles (J).

(8) Convert the sequence of encrypted data x_C back to the image containing two dimensional.

The encryption algorithm can be summari ed as following Equations (10) to (12).

$$x_0^i(j) = x_c^{last}(j-1) \quad ;if \quad i = 1^{st} \tag{10}$$

$$x_0^i(j) = x_c^{i-1}(j) \quad ;if \quad i \neq 1^{st} \tag{11}$$

$$x_e^i(j) = \begin{cases} x_n^i(j-1) + x_c^i(j-1) & if \ x_n^i(j-1) + x_c^i(j-1) \le x_{\max} \\ x_n^i(j-1) + x_c^i(j-1) - \delta x & if \ x_{\max} < x_n^i(j-1) + x_c^i(j-1) \le 2x_{\max} - 2x_{\min} \\ x_n^i(j-1) + x_c^i(j-1) - 2\delta x & if \ 2x_{\max} - 2x_{\min} < x_n^i(j-1) + x_c^i(j-1) \end{cases} \tag{12}$$

Decryption algorithm

The revised decryption algorithm is as followed.

(1) Use secret keys from Encryption Algorithm as parameter, number of iteration, number of cycle and the new secret keys in step 1).
(2) Convert the encrypted image containing two dimensional in terms of sequence encrypted data x_c.
(3) Calculate sequential data *m* from the Equation (1) with new secret keys in step 1). Sort sequential data as sequential pixel for decryption.
(4) Recover the image of the *j*-1 cycle. Start decryption at the last element in sequential pixel by using previous order pixels ($x_c^{i-1}(j)$) as initial condition $x_0^i(j-1)$. Calculate $x_n^i(j-1)$ at N iterations from the Equation (5). Subtract the last element in sequential pixel $x_c^i(j)$ by $x_n^i(j-1)$. Continue decryption process to the first element in sequential pixel.
(5) Apply the last element in sequential pixel of -1 cycle as the initial condition at the first element in sequential pixel ($x_0^{first}(j-1)$). After N iterations from (1) $x_n^{first}(j-1)$. Subtract the first order $x_c^{first}(j)$ by $x_n^{first}(j-1)$. The subtraction value is used as the initial condition for the next element in sequential pixel. Sometime, the subtraction of value is under range of chaos system (x_{min}). We propose the new condition in Equation (14).
(6) Repeat steps (4) to (5) for the next cycles until cycle *j* 0.
(7) Convert the decrypted data x_C back to the image containing two dimensional and then convert to the original image with formula (8) (Figure 5).

The decryption algorithm can be summari ed as follows in Equation (13) to (15)

$$x_0^i(j-1) = x_c^{i-1}(j) \quad ;if \quad i \neq 1^{st} \tag{13}$$

$$x_0^i(j-1) = x_c^{last}(j-1) \quad ;if \quad i = 1^{st} \tag{14}$$

$$x_c^i(j-1) = \begin{cases} x_c^i(j) - x_n^i(j-1) & if \ x_c^i(j) - x_n^i(j-1) \ge x_{\min} \\ x_c^i(j) - x_n^i(j-1) + \delta x & if \ -x_{\max} + 2x_{\min} \le x_c^i(j) - x_n^i(j-1) < x_{\min} \\ x_c^i(j) - x_n^i(j-1) + 2\delta x & if \ 2x_c^i(j) - x_n^i(j-1) < -x_{\max} + 2x_{\min} \end{cases} \tag{15}$$

ANALYSIS AND TEST RESULTS

Visual inspection

The encryption motivates the changes in pixel values without visual perception. Encryption quality is measured on how much changes can be introduced with minimum visual recognition. It can be measured as sub ective test or ob ective tests in terms of statistical analysis such as histogram analysis, correlation analysis, cross-correlation analysis, and Gray Modification Average Value. The employed secret keys for the CML based encryption are the logistic map parameters, the number of iterations, and the number of cycles while fractional order parameters of the logistic model are additionally introduced in the proposed APFCML based encryption. In order to illustrate the comparative encryption quality of both encryption systems, the examples of experimental results obtained from the CML based encryption with $r = 3.90$ and those obtained from the proposed APFCML based encryption with $\alpha = \frac{1}{2}, r = 5.90$ are presented in Figure 6. Both encryption systems are compared with the same number of iterations and the number of cycles. Figure 6 shows the encrypted Lena images with ten combination of the number of iterations and the number of cycles of J 1, N 1-5 and J 2, N 1-5.
From the results, it can be seen that the CML and the APFCML deliver high encryption quality when the number of cycles is greater than 1. Observing the encrypted images with number of cycles is 2 and the number of iterations is 1 that the CML have Lena image information more than the APFCML. The APFCML is more efficiency than the CML.

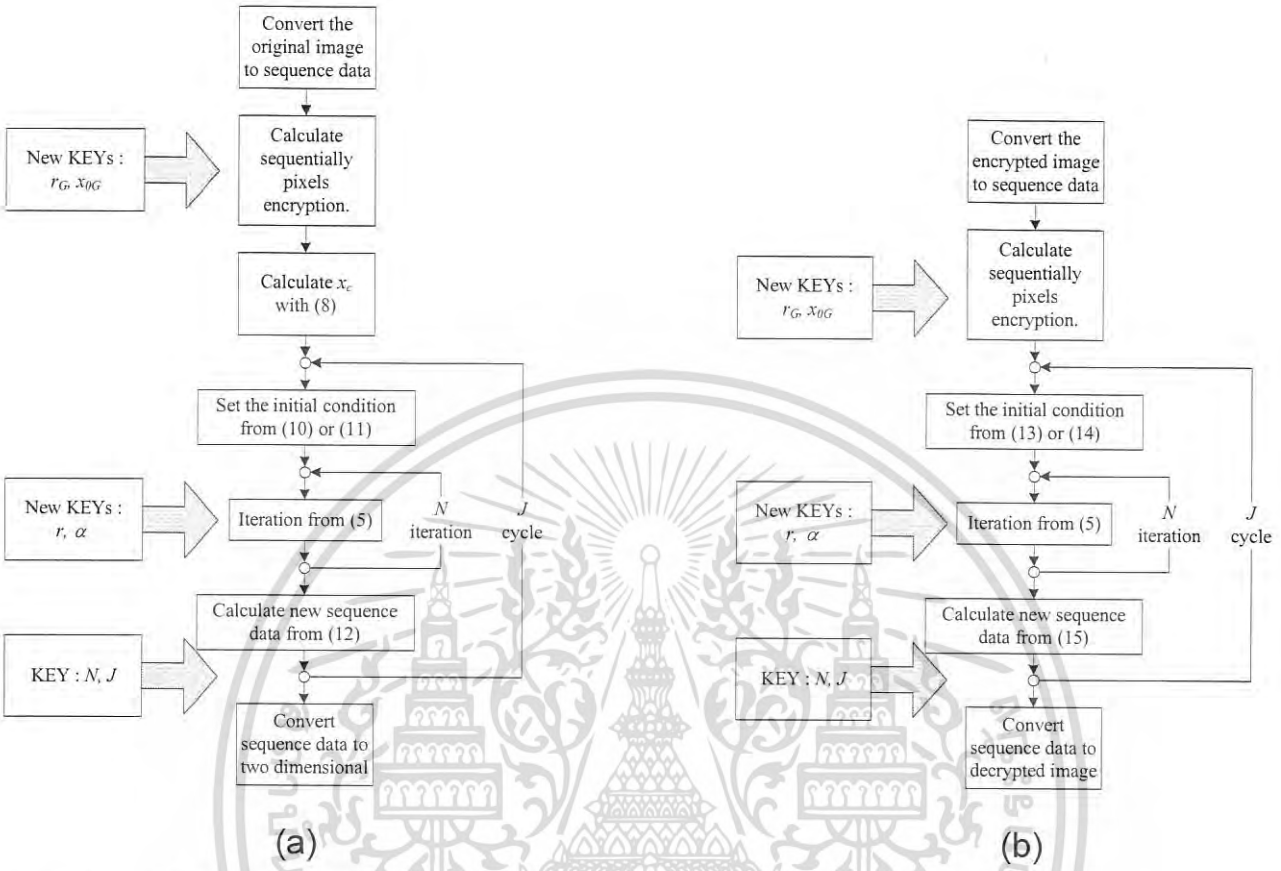


Figure 5. Block diagram for (a) encryption algorithm and (b) decryption algorithm.

Statistical analysis

The statistical analysis was analy ed in image encryption (Pareek et al., 2006 Liu et al., 2009). An encryption result should be robust against any statistical attack. The histograms of the test images and the correlations of two ad acent pixels in the encrypted images are simulated for statistical analysis.

Histogram analysis

It is important to verify that there is no statistical similarity between the encrypted and original images in order to prevent the leakage of information to the attackers. The statistical similarity can be illustrated in term of histograms, which present the distribution of the pixel intensity in images. Histogram of the Lena original image is shown in Figure 7a. Figure 7(b-f) shows histogram of the encrypted image using CML at $r = 3.90$. Figure 7(g- k) shows histogram of the encrypted image using APFCML when $\alpha = \frac{1}{2}, r = 5.90$. The histogram of original image contains large fluctuation while that of the encrypted image is close to the uniform distribution. It is significantly different from the original image. This shows that no statistical similarity appears between the encrypted and the original images.

From the results, the histogram distribution of the CML based encryption is close to the uniform distribution when J is greater than 1 and J is equal to N while that of the proposed APFCML based encryption can accomplish the goal with the J 1 N 2. It can be seen that the proposed APFCML based encryption can converge to the desired distribution with lower order of the secret key parameters, thus it can allow extensive range of the encryption parameters. This can guarantee that the encryption with the proposed APFCML based system can achieve greater encryption security than that of the CML based system.

Correlation coefficient analysis

The correlation coefficient analysis is one of the important statistical analysis tools, which measures the statistical

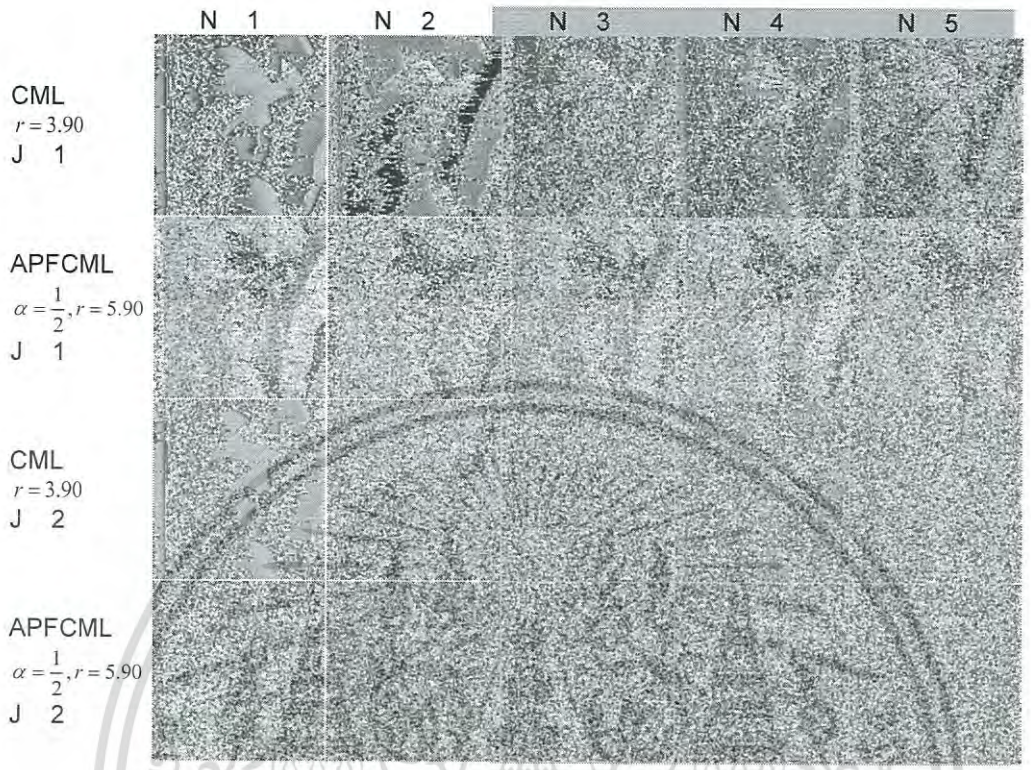


Figure 6. The encrypted Lena image with CML $r = 3.90$ and APFCML $\alpha = \frac{1}{2}, r = 5.90$.

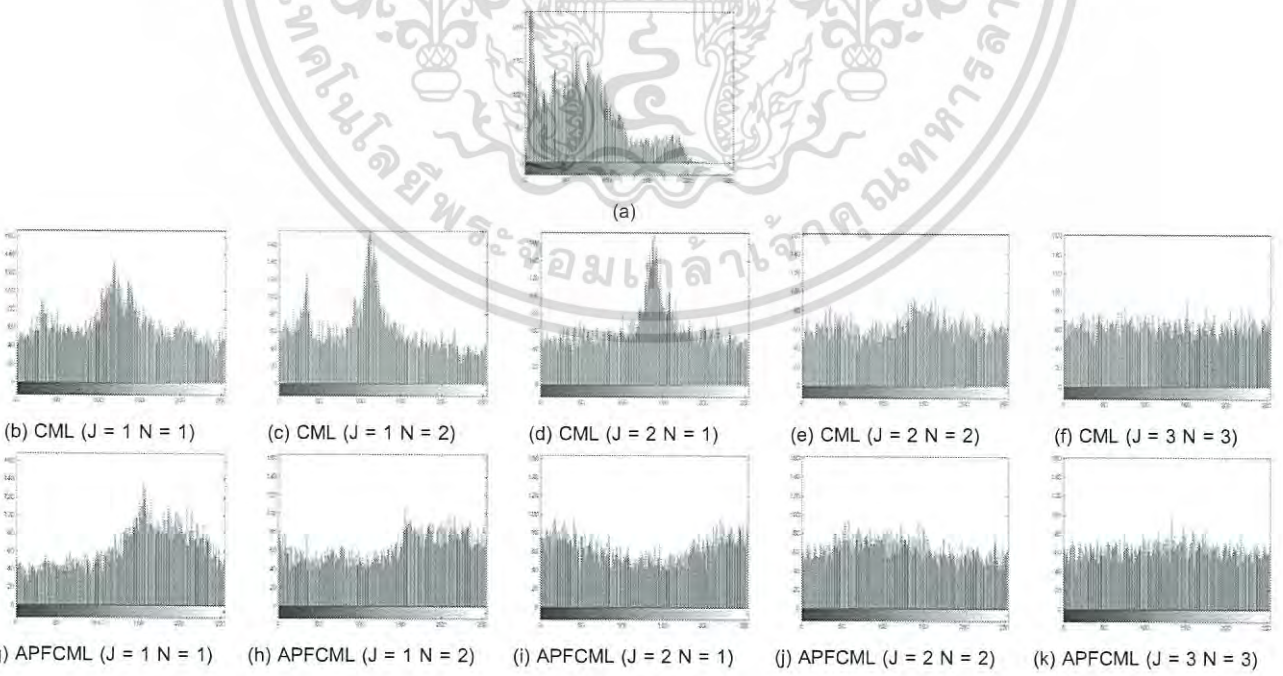


Figure 7. Histogram of (a) the original image and the encrypted image (b)-(f) CML $r = 3.90$ (g)-(k) APFCML $\alpha = \frac{1}{2}, r = 5.90$.

relationship between two hori ontally ad acent pixels and two vertically ad acent pixels in encrypted image (Pareek et al., 2006 Liu et al., 2009). For effective image cryptography, all the attributes of the original images should be concealed, and the encrypted images should be highly uncorrelated. If the original and encrypted images are uncorrelated or totally different, their correlation will be very low or close to ero. If they are identical, their corresponding correlation will be equal to one. Figure 8 shows the distribution of two vertically ad acent pixels and two hori ontally ad acent pixels. Figure 8(a) shows the distribution of the original Lena image. Figure 8 (b, d, f, h,) show the distribution of the encrypted Lena image from CML ($r=3.90$). The distributions of the encrypted Lena image from APFCML ($\alpha=\frac{1}{2}, r=5.90$) are shown in Figure 8(c, e, g, I ,k).

The determination of how well ad acent pixels are correlated is to consider the regression line representing the data. The hori ontally and vertically ad acent pixels are considered highly correlated if the regression line passes through points on the scatter plot. Otherwise, they are considered less correlated. The results show that the distributions obtained from the proposed APFCML based encryption are greatly dispersed from the scatter line for all Js and Ns while those of the CML based encryption are dispersed when J and N are greater than 2. This means that the APFCML encrypted pixels are greatly uncorrelated and it results in less visual perception and higher encryption quality.

Cross-correlation equation

The cross-correlation technique is a method to estimate the displacement information of two consecutive images by comparing the similarity of a pair of image signals (Kocarev et al., 2004 Solak and okal, 2008). The cross-correlation between two vertically and two hori ontally ad acent pixels in the original and encrypted images are calculated using Equation (10) (Pareek et al., 2006 Liu et al., 2009).

$$C_r=\frac{N\sum_{j=1}^{N}\left(x_j\times y_j\right)-\sum_{j=1}^{N}x_j\sum_{j=1}^{N}y_j}{\sqrt{\left(N\sum_{j=1}^{N}x_j^2-\left(\sum_{j=1}^{N}x_j\right)^2\right)\times\left(N\sum_{j=1}^{N}y_j^2-\left(\sum_{j=1}^{N}y_j\right)^2\right)}} \quad (16)$$

Where x_j is intensity of pixel at location $(x,\ y)$, y_j is intensity of pixel at location $(x+1,\ y)$ for the cross-correlation of two vertically and y_j is intensity of pixel at location $(x,\ y+1)$ for the cross-correlation of two hori ontally.

Figure 9(a) demonstrates correlation coefficient analysis with CML based encryption for vertical and hori ontal directions with various combinations of N and J parameters. The correlation coefficient analysis with APFCML based encryption is shown in Figure 9(b-d). It can be seen that, to achieve the correlation less than 0.05 for all variations of N, it limits the values of J greater than 5 for the CML thus greater than 3 for the APFCML. From the results, it demonstrates that the APFCML permits larger variation of secret keys with higher encryption quality for all parameters.

The results from Figure 9(a) and (b) show the correlation coefficient for the CML at J 1 N 1 more than the correlation coefficient for the APFCML that accords with the results of the visual inspection and the histogram analysis.

Gray modification average value

The values of pixels in the image encryption have been changed from the original image. Visual testing can show contrast between the original image and the image encryption. The percentage of unchanged point represents percentage of pixels difference. Gray modification average value, called GAVE, can measure the change in value of image encryption. The higher the GAVE value, the better the encrypted image. GAVE is defined in Equation (22), where $G=\left(g_{ij}\right)_{M\times N}$ is the original image and $C=\left(c_{ij}\right)_{M\times N}$ is the image encryption (Li and Wang, 2011).

$$GAVE(G,C)=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left|g_{ij}-c_{ij}\right|}{MN} \quad (17)$$

GAVE of all pixels in the image are shown in Figure 10. For the CML, GAVE will increase when number of cycle increases and number of iterations is greater than 7. At J 1, GAVE tends to converge slower. This is supported by the visual inspection results where the original information can still be perceived. For the APFCML, value of GAVE swing at number of cycleless than 3. Result shown GAVE value of APFCML more than CML.

Conclusion

This paper proposes an adaptive pixel-selection fractional chaotic map lattices for image cryptography to enhance the encryption security and overcome the limitation of the original CML. In the APFCML based encryption, the fractional logistic equation is applied in cryptography, which provides new secret keys as fractional order. In addition, the encryption sequence has been adaptively

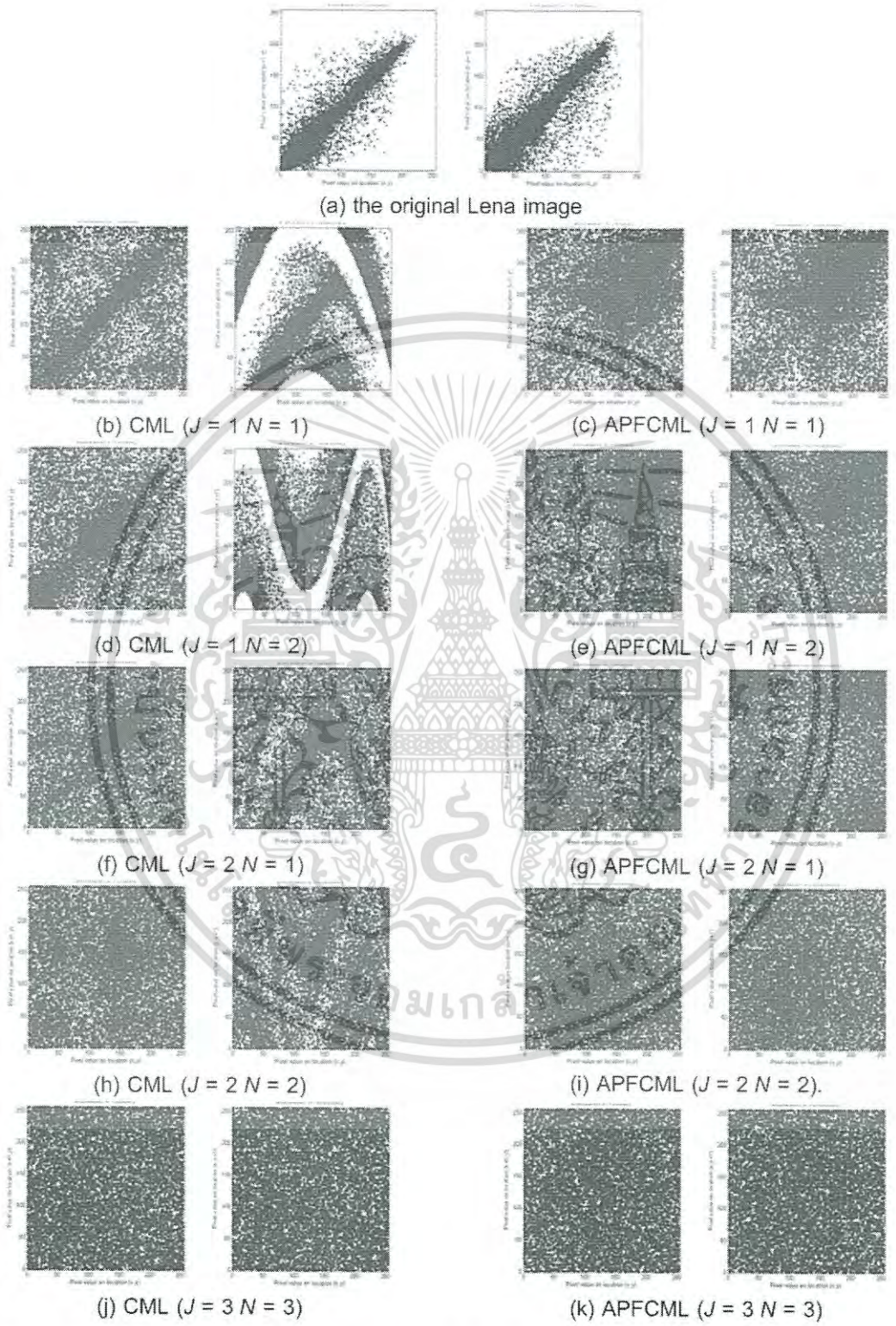


Figure 8. The distribution of two vertically ad acent pixels and two hori ontally ad acent pixels of the original and encrypted Lena image with CML $r = 3.90$ and APFCML $\alpha = \frac{1}{2}, r = 5.90$.

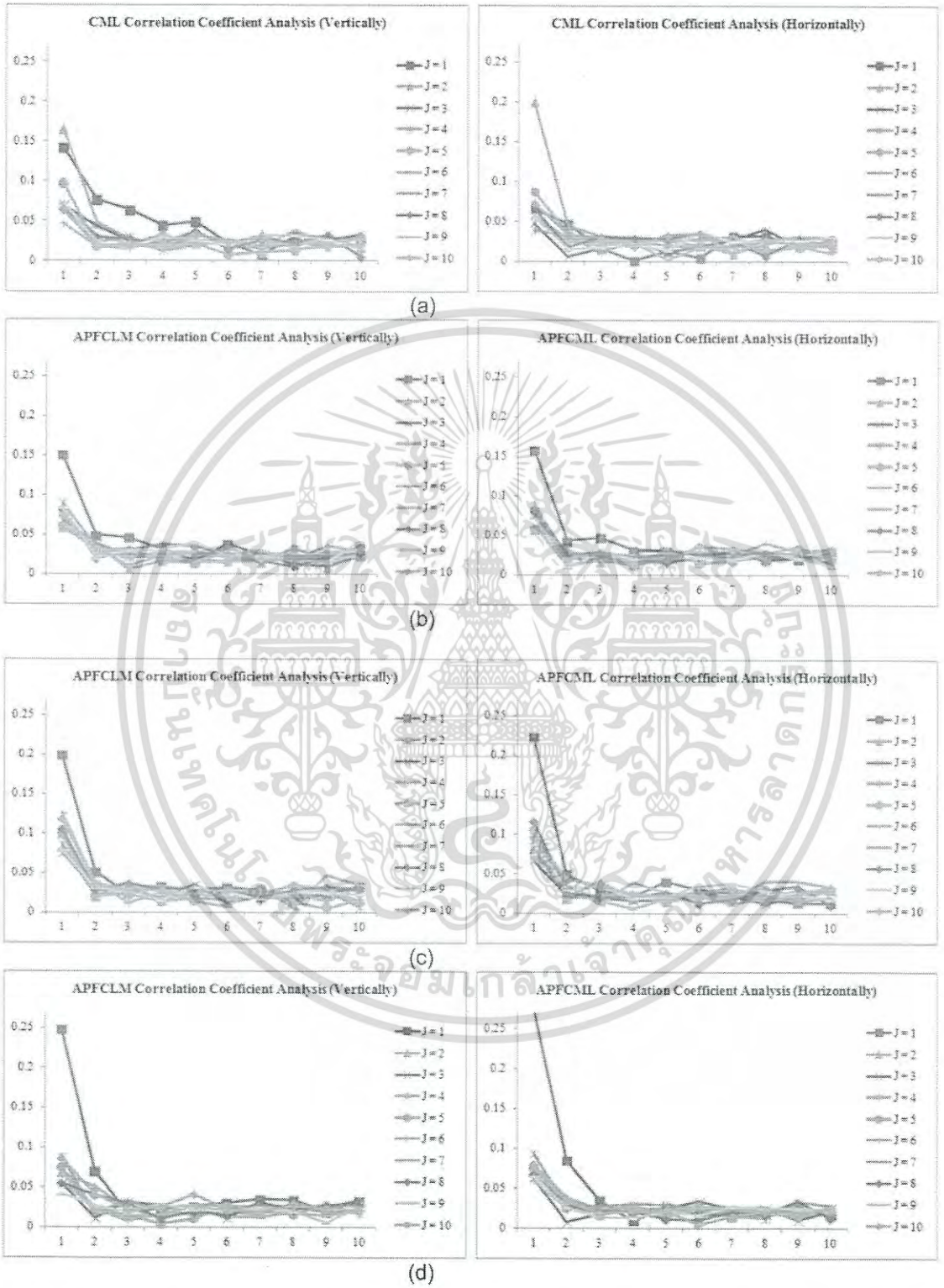


Figure 9. Correlation Coefficient Analysis for various combinations of *J* and *N* parameters of (a) CML $r = 3.90$ (b) APFCML $\alpha = \frac{1}{2}, r = 5.90$ (c) APFCML $\alpha = \frac{1}{2}, r = 5.97$ and (d) APFCML $\alpha = \frac{1}{4}, r = 4.85$.

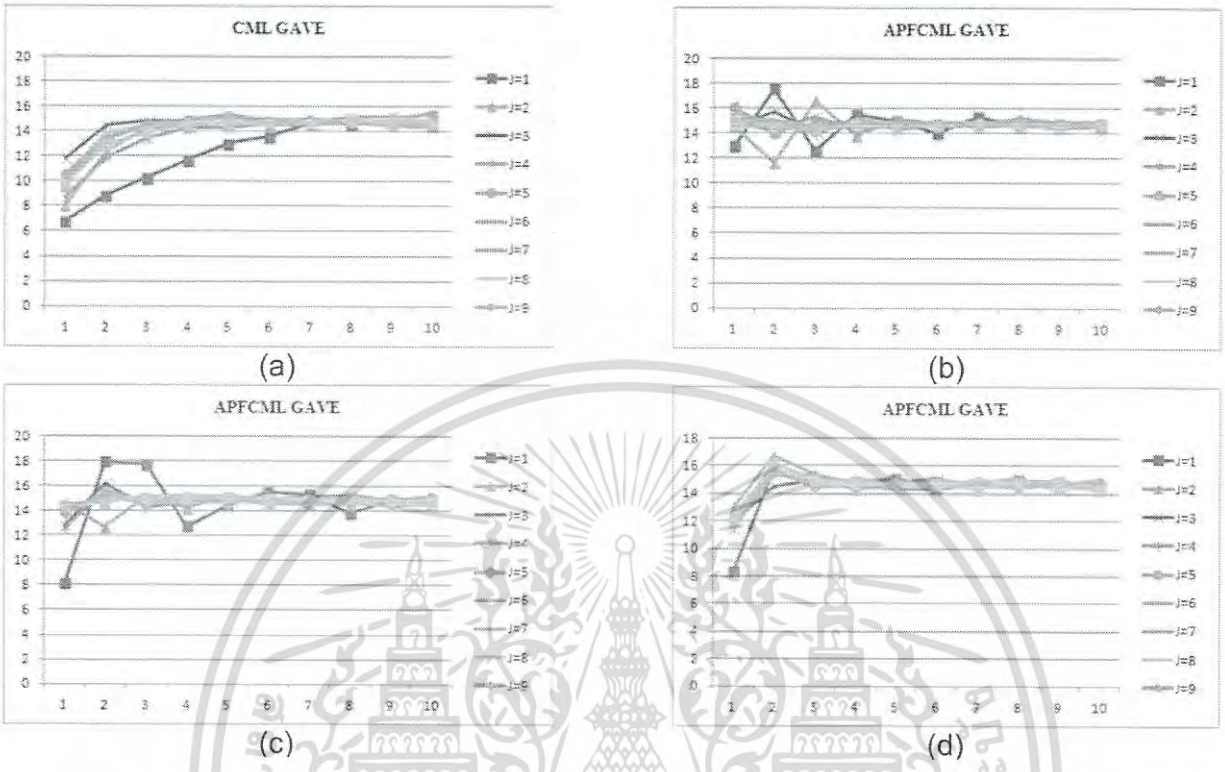


Figure 10. GAVE for various combinations of J and N parameters of (a) CML $r = 3.90$, (b) APFCML $\alpha = \frac{1}{2}, r = 5.90$, (c) APFCML $\alpha = \frac{1}{2}, r = 5.97$ and (d) APFCML $\alpha = \frac{1}{4}, r = 4.85$.

selected based on the chaos generator. Even though the intruder can guess the secret keys and the initial condition of the first pixel, it is quite difficult to acquire the whole encryption sequence. In the experiments, the measurement indices of originality preservation, visual inspection, and statistical analysis are used to evaluate the performance of the proposed APFCML compared to that of the original CML.

Conflict of Interest

The authors have not declared any conflict of interest.

REFERENCES

Afraimovich V, Hsu SB (2002). Lectures on Chaotic Dynamical Systems. American Mathematical Society. International Press.

Alligood KT, Sauer TD, Yorke JA (1996). An Introduction to Dynamical Systems. Springer.

Baker G L, Gollub J P (1990). Chaotic dynamics: an introduction. Cambridge University Press.

Kocarev L, Ster ev M, Fekete A, and Vattay G (2004). Public-key encryption with chaos. Chaos 14:1078-1082.

Li Q, Wang Y (2011). The Performance Analysis of Image Encryption Algorithm Based on Chaotic System. International Conference on Electronic Mechanical Engineering and Information Technology. 978-I-61284-088-8/II/, pp. 3492-3494.

Liu S, Sun J, Xu Z (2009). An improved image encryption algorithm based on chaotic system. J. Comput. 4(11):1091-1100.

Mon e CA, Chen Y, Vinagre BM, Xue D, Feliu-Batlle V (2010). Fractional-Order Systems and Controls: Fundamentals and Applications. Spinger. ISBN 9781849963350.

Moon FC (2004). Chaotic and Fractal Dynamics An Introduction for Applied Scientists and Engineers. Wiley-VCH Verlag GmbH and Co.

Pareek NK, Patidar V, Sud KK (2003). Discrete chaotic cryptography using external key. Phys. Lett. A. 309:75-82.

Pareek NK, Patidar V, Sud KK (2006). Image encryption using chaotic logistic map. Image Vision Comput. 24:926-934.

Pasti n H (2006). Chaotic Growth with the Logistic model of P.-F. Verhulst. Understanding Complex Systems, pp. 3-11.

Pecora LM, Carroll TL (1990). Synchroni ation in chaotic systems. Phys. Rev. Lett. 64:821-824.

Petras I (2006). Method for simulation of the fractional order chaotic systems. Acta Montanistica Slovaca. 11(4):273-277.

Pisarchik AN, Flores-Carmona NJ Carpio-Valade M (2006). Encryption and decryption of images with chaotic map lattices. American Institute of Physics.

Podlubny I (1999). Fractional Differential Equations. New York: Academic Press.

Sabatier J, Agrawal OP, Tenreiro Machado JA (2007). Advances in Fractional Calculus Theoretical Developments and Applications in Physics and Engineering. Springer.

Solak E and Çokal C (2008). Comment on "Encryption and decryption of images with chaotic map lattices". American Institute of Physics. DOI: 10.1063/1.2966114.

Suansook Y, Paithoonwattanaki K (2008). Bifurcation and Lyapunov Exponent in Orthogonal Frequency Division Multiplexing. IEEE 6th International Conference on Computational Cybernetics. Stara Lesn . Slovakia, pp. 107-112.

Suansook Y, Paithoonwattanaki K (2008). Chaos in Orthogonal Frequency Division Multiplexing Technique. International Conference on Advanced Computer Theory and Engineering, pp. 457-461.

Suansook Y, Paithoonwattanaki K (2014). Fractional order chaos in Josephson unction. Scientific Research and Essays. Vol.9(17):785-793.

Van Wiggeren DG, Roy R (1998). Communication with chaotic lasers. Science 279:1198-1200.