การเข้ารหัสสื่อประสมโดยใช้เกออสในวงจรกรองสัญญาณดิจิตอล

MULTIMEDIA CONTENT ENCRYPTION USING IN DIGITAL FILTER

นครินทร์ รณรงค์ฤทธิ์

NAKARIN RONNARONGLIT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2559

KMITL-2016-EN-M-010-150

การเข้ารหัสสื่อประสมโดยใช้เคออสในวงจรกรองสัญญาณดิจิตอล

MULTIMEDIA CONTENT ENCRYPTION USING IN DIGITAL FILTER

นครินทร์ รณรงค์ฤทธิ์

NAKARIN RONNARONGLIT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ.2559

KMITL-2016-EN-M-010-150

MULTIMEDIA CONTENT ENCRYPTION USING IN DIGITAL FILTER

NAKARIN RONNARONGLIT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN TELECOMMUNICATIONS ENGINEERING

FACULTY OF ENGINEERING

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2016

KMITL-2016-EN-M-010-150

คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การเข้ารหัสสื่อประสมโดยใช้เคออสในวงจรกรองสัญญาณดิจิตอล
Thesis Title Multimedia Content Encryption using Chaos in Digital Filter
นักศึกษา นายนครินทร์ รณรงค์ฤทธิ์
รหัสประจำตัว 55611915
ปริญญา วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา วิศวกรรมโทรคมนาคม
อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผศ.ดร.ศรวัฒน์ ชิวปรีชา
หมายเลขวิทยานิพนธ์ KMITL-2016-EN-M-010-150

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
รศ.ดร.ยุทธพงษ์	รังสรรค์เสรี	
ผศ.ดร.ณัฐกานต์	พุทธรักษ์	
ศ.ดร.โกสินทร์	จำนงไทย	
ผศ.ดร.พิชญ	สุพรรณกูล	
ผศ.ดร.ศรวัฒน์	ชิวปรีชา	

วัน / เดือน/ ปี ที่สอบ วันพุธที่ 6 กรกฎาคม พ.ศ. 2559 เวลา 09.00-11.00 น.
สถานที่สอบ ณ อาคารเฉลิมพระเกียรติ ห้อง HM-302

คณะวิศวกรรมศาสตร์ รับรองแล้ว

(รองศาสตราจารย์ ดร. คมสัน มาลีสี)

คณบดี คณะวิศวกรรมศาสตร์

วันที่ 6 กรกฎาคม พ.ศ. 2559

หัวข้อวิทยานิพนธ์	การเข้ารหัสสื่อประสมโดยใช้เคออสในวงจรกรองสัญญาณดิจิตอล
นักศึกษา	นายนครินทร์ รณรงค์ฤทธิ์
รหัสประจำตัว	55611915
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมโทรคมนาคม
พ.ศ.	2559
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ผศ.ดร.ศรวัฒน์ ชิวปรีชา

บทคัดย่อ

วิทยานิพนธ์ฉบับนี้นำเสนอการเข้ารหัสลับเนื้อหาสื่อประสมที่ประกอบไปด้วยข้อมูลรูปภาพ ข้อมูลเสียง และข้อความ ในรูปแบบดิจิตอล เป็นการเข้ารหัสลับชนิดบล็อคร่วมกับกุญแจสมมาตร โดยอาศัยเคออสในวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง มาสร้างกุญแจลับ กุญแจลับเกิดจากการกำหนดรหัสผ่านอักขระจำนวน 16 อักขระ เพื่อสร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล 2 ตัว และบังคับให้ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลอย่างน้อย 1 ตัวอยู่นอกสามเหลี่ยมเสถียรภาพ ตามเงื่อนไขการเกิดเคออส คือวงจรกรองสัญญาณนั้นต้องมีความไร้เสถียรภาพและไม่เป็นเชิงเส้น หลังจากนั้นนำระนาบบิตของกุญแจและข้อมูลต้นฉบับทั้ง 8 ระนาบบิตมาดำเนินการทางลอจิกด้วย XOR (Exclusive or) จะทำให้ได้ระนาบบิตของข้อมูลลับทั้งหมด 8 ระนาบบิต สุดท้ายรวมทุกระนาบบิตเป็นข้อมูลลับออกมา การวัดประสิทธิภาพจะประกอบไปด้วย ความไวของกุญแจความไวของข้อมูลต้นฉบับ อัตราสัญญาณต่อสัญญาณรบกวน ค่าเอนโทรปีข้อมูล ค่าสหสัมพันธ์ และการรับรู้คุณภาพข้อมูลลับด้วยการมอง เปรียบเทียบกับผลลัพธ์ที่ได้จากงานวิจัยอื่น และโครงสร้างเข้ารหัสลับที่นำเสนอสามารถใช้กับข้อมูลเสียง และข้อความ 1 มิติได้เป็นอย่างดี

Thesis Title	Multimedia Content Encryption using Chaos in Digital Filter
Student	Mr. Nakarin Ronnaronglit
Student ID.	55611915
Degree	Master of Engineering
Program	Telecommunications Engineering
Year	2016
Thesis Advisor	Asst.Prof.Dr. Sorawat Chivapreecha

ABSTRACT

This thesis presents multimedia content encryption consisting of digital image audio and text using block encryption with symmetry key based on chaos in 2nd order IIR digital filter to generate the secret key. The designed secret key takes 16 characters to generate the filter coefficients and takes 1 filter coefficient out of stability triangle followed the Chaos theory with to unstable and non-linearity digital filter. Then, XOR (Exclusive or) is performed between bit-planes of plaintext and bit-planes of the secret key. The output is bit-planes of ciphertext 8 bit-planes and then all bit-planes is combined to make the cipher. The performance is measured by key sensitivity, plaintext sensitivity, correlation coefficients, PSNR, entropy and perceptual security compared with the previous research works. The proposed cryptosystem can be applied to audio and text 1 dimension as well.

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จได้ด้วยความกรุณาจากอาจารย์ที่ปรึกษา ผศ.ดร.ศรวัฒน์ ชิวปรีชา ที่ให้ความช่วยเหลือ ให้คำชี้แนะช่วยแก้ปัญหาตลอดจนให้ความรู้และประการณ์ที่ดีแก่ข้าพเจ้า

ขอขอบคุณผู้สนับสนุนในการทำงานวิจัย ทั้งเพื่อน พี่ น้อง ทุกคนที่ได้เกี่ยวข้องซึ่งได้ชี้แนะและให้คำปรึกษารวมถึงให้กำลังใจในการทำงานวิจัย

ข้าพเจ้าขอขอบพระคุณ คณะกรรมการสอบวิทยานิพนธ์ รศ.ดร.ยุทธพงษ์ รังสรรค์เสรี, ผศ.ดร.ณัฐกานต์ พุทธรักษ์, ศ.ดร.โกสินทร์ จำนงไทย, และ ผศ.ดร.พิชญ สุพรรณกูล ที่ได้ให้ข้อเสนอแนะคำแนะนำในงานวิจัยข้าพเจ้าอย่างมาก

สำหรับคุณงามความดีอันใดที่เกิดจากวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดา มารดา ซึ่งเป็นที่รักและเคารพยิ่ง ตลอดจนครูอาจารย์ที่เคารพทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

นครินทร์ รณรงค์ฤทธิ์

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

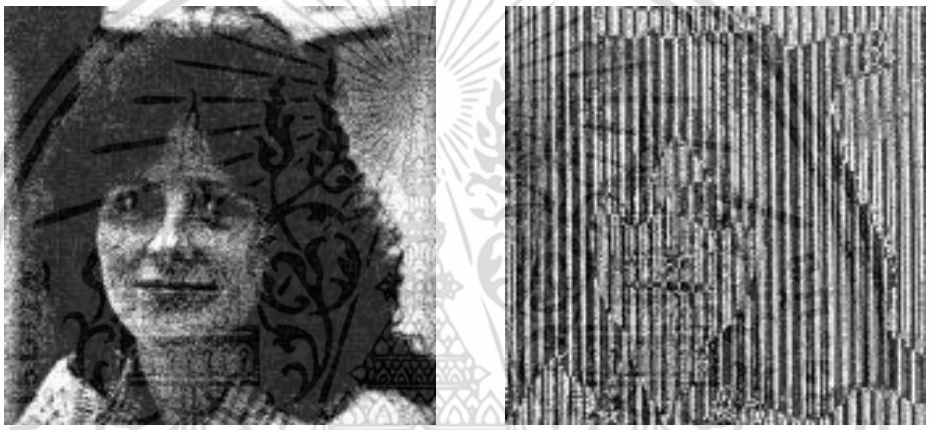
การเข้ารหัสลับสามารถจำแนกได้เป็น 2 แบบคือการเข้ารหัสแบบบล็อคและการเข้ารหัสแบบสตรีม ทุกวันนี้จะใช้การเข้ารหัสลับข้อมูลที่ต้องส่งผ่านเครือข่ายสื่อสารต่างๆ โดยข้อมูลนั้นเป็นข้อมูลที่มีขนาดไม่ใหญ่มาก และส่งเป็นบางครั้งไม่ได้ส่งตลอดเวลา เป็นผลทำให้การเข้ารหัสลับแบบบล็อคเป็นที่นิยมอย่างมาก ยกตัวอย่างเช่น อัลกอริทึม DES (Data Encryption Standard) ที่ออกแบบโดย Horst Feisel ผู้ซึ่งเคยปฏิบัติงานอยู่บริษัท IBM และอัลกอริทึมนี้ได้รับเลือกเข้าเป็นอัลกอริทึมมาตรฐานสำหรับรัฐบาลกลางสหรัฐอเมริกา นับตั้งแต่ปี 1977 โดยออกแบบให้เข้ารหัสด้วยกุญแจขนาด 56 บิต แต่มีแฮกเกอร์สามารถเดาสุ่มกุญแจเพื่อหากุญแจที่ถูกต้องในการถอดรหัสได้

กุญแจ 56 บิต ในปี 1977 เป็นกุญแจที่ใหญ่มาก แต่ในยุคปัจจุบันนี้คอมพิวเตอร์สามารถทำงานได้เร็วมากยิ่งขึ้น ทำให้การเดาสุ่มกุญแจที่มีขนาด 56 บิต ใช้เวลาเพียง 1 วันเท่านั้น จึงทำให้อัลกอริทึมนี้ไม่ปลอดภัยอีกต่อไป กลายเป็นเพียงอัลกอริทึมที่เคยมีความปลอดภัยและในการศึกษาเท่านั้น และได้มีการคิดค้นเพิ่มขนาดกุญแจของ DES ให้มากขึ้นด้วยการประมวลผล 3 รอบ เรียกว่า 3 DES (TDEA or Triple DEA) ในระหว่างที่อัลกอริทึม DES ถูกค้นพบช่องโหว่ทำให้รัฐบาลกลางสหรัฐ (National Institute of Standards and Technology – NIST) จัดประกวดอัลกอริทึมเข้ารหัสลับใหม่เพื่อมาเป็นมาตรฐานการเข้ารหัสลับแทน DES นักคณิตศาสตร์ชาวเบลเยียม Joan Daemen และ Vincent Rijmen ก็ชนะการประกวดด้วยอัลกอริทึมของพวกเขาเองที่ชื่อว่า Rijndael การเข้ารหัสของ Rijndael ถูกพัฒนาและบรรจุไปในมาตรฐานการเข้ารหัสลับเรียกว่า อัลกอริทึม AES (Advanced Encryption Standard) และได้รับความนิยมอย่างมาก ได้ถูกบรรจุลงไปในมาตรฐานไอทีหลายโปรโตคอลเช่น SSL (Secure Sockets Layer) WPA (Wi-Fi Protected Access) เป็นต้น อัลกอริทึม AES สามารถรองรับกุญแจได้ 3 ขนาด คือ 128 บิต 192 บิต และ 256 บิต ซึ่งเพียงพอต่อการใช้งานไปอีกนาน [1]

ในขณะเดียวกันสื่อประสมโดยเฉพาะรูปภาพได้รับความนิยมเป็นอย่างมากในการใช้งานอินเตอร์เน็ต เช่น ทางการแพทย์ อุตสาหกรรม และการทหาร ดังนั้นความปลอดภัยของสื่อประสมจึงมีความสำคัญอย่างมาก จะต้องป้องกันให้เป็นความลับและเป็นส่วนตัว เพราะปัจจุบันนี้มีแฮกเกอร์โจมตีขโมยข้อมูล เช่น การปลอมไอพี (IP Spoofing) การทำให้บริการเกิดความผิดปกติ (Denial of Service) การปลอมตัวเป็นคนกลาง (Man-in-the-Middle) ดังนั้นการเข้ารหัสจากปลายทางถึงปลายทาง (End-to- End Encryption) จึงเป็นวิธีการแก้ปัญหาที่อาจจะเกิดขึ้นได้ เพราะจะทำให้แฮกเกอร์ได้ข้อมูลลับไปแทนข้อมูลต้นฉบับจะต้องใช้เทคนิคและความสามารถในการถอดข้อความลับ

นั้นอีกด้วย กระบวนการเข้ารหัสจากปลายทางถึงปลายทางมีการใช้งานหลากหลาย เช่น PGP (Pretty Good Privacy) ที่ผู้ใช้ทุกคนต้องสร้างกุญแจสาธารณะขึ้นมาด้วยตนเองทั้งผู้ส่งและผู้รับ จากนั้นเมื่อต้องการส่งอีเมล แทนที่จะส่งอีเมลเป็นเนื้อความธรรมดา ก็เปลี่ยนเป็นอีเมลที่เข้ารหัสด้วยกุญแจสาธารณะของผู้รับ ทำให้ผู้ที่สามารถอ่านอีเมลได้คือผู้ที่ถือกุญแจลับที่เข้าคู่กับกุญแจสาธารณะที่เราส่งไปหาเท่านั้น วิธีการเช่นนี้เป็นที่ได้รับความนิยมเพราะถึงแม้แฮกเกอร์สามารถโจรกรรมข้อมูลได้แต่ก็ยังไม่สามารถเข้าใจข้อมูลนั้นได้

แต่การใช้อัลกอริทึมมาตรฐานดังที่กล่าวมานั้นมีข้อเสียสำหรับการเข้ารหัสลับเนื้อหาสื่อประสม [2] โดยเฉพาะรูปภาพดิจิตอลคือทำให้ข้อมูลรูปภาพดิจิตอลลับมีลักษณะที่ยังคงเหมือนข้อมูลต้นฉบับอยู่เช่น รูปที่ 1.1

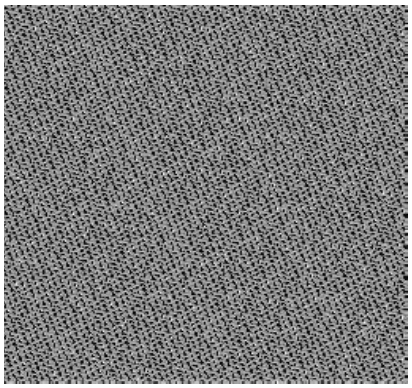


(ก) (ข)

รูปที่ 1.1 รูปภาพดิจิตอลต้นฉบับและรูปภาพดิจิตอลลับที่เข้ารหัสลับด้วย AES [3] (ก) รูปภาพดิจิตอลต้นฉบับ (ข) รูปภาพดิจิตอลลับ

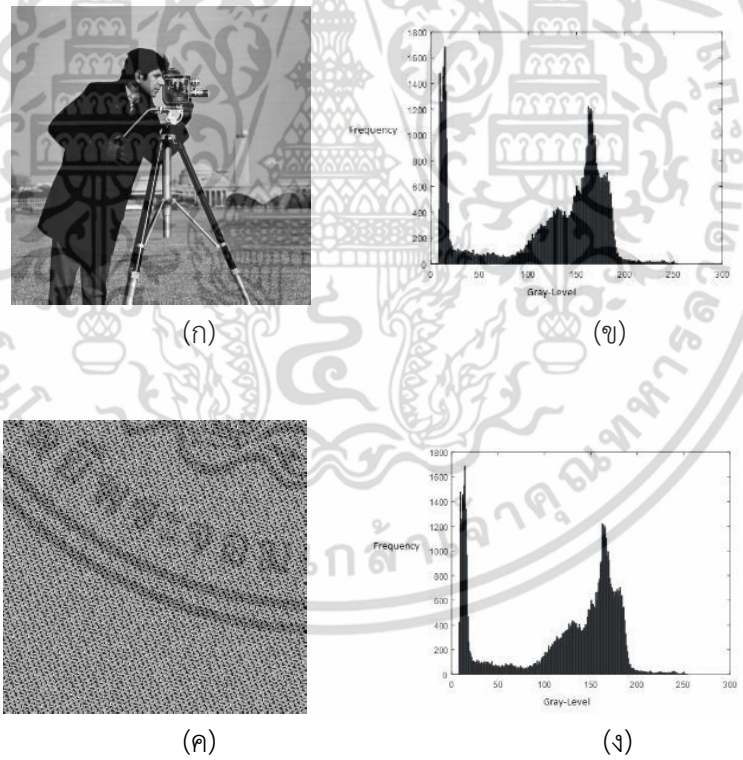
จากรูปที่ 1.1 (ก) เป็นรูปภาพดิจิตอลต้นฉบับที่ต้องการเข้ารหัสลับ และเมื่อผ่านกระบวนการเข้ารหัสลับโดยอัลกอริทึม AES จะทำให้ได้รูปดิจิตอลลับที่ยังคงเหลือเนื้อหาที่สอดคล้องถึงรูปภาพดิจิตอลต้นฉบับอยู่ ดังรูปที่ 1.1 (ข)

ทำให้ปัจจุบันนี้มีงานวิจัยจำนวนมากได้นำเสนออัลกอริทึมใหม่เพื่อนำมาใช้เข้ารหัสลับรูปภาพดิจิตอล เช่น ใช้เคออติกแมพเข้ารหัสลับรูปภาพดิจิตอลด้วยการสลับค่าตามสมการเคออติก หรือที่เรียกว่า เคออติกแมพ ผลลัพธ์ที่ได้เป็นที่น่าพอใจเพราะรูปภาพลับมีเนื้อหาที่ไม่คล้ายคลึงกับรูปภาพต้นฉบับแม้แต่น้อย ดังรูปที่ 1.2



รูปที่ 1.2 รูปภาพดิจิตอลที่เข้ารหัสลับด้วยแคทแมพ (Cat map)

จากรูปที่ 1.2 เป็นรูปภาพดิจิตอลที่เข้ารหัสลับด้วยเคออติกแมพที่มีชื่อว่า แคทแมพ (Cat map) แต่กระนั้นพบว่าค่าฮีสโทแกรมของรูปภาพลับที่ได้จากการเข้ารหัสลับด้วยอัลกอริทึมนี้ เหมือนกับรูปภาพดิจิตอลต้นฉบับทุกประการ [4-6] ดังรูปที่ 1.3

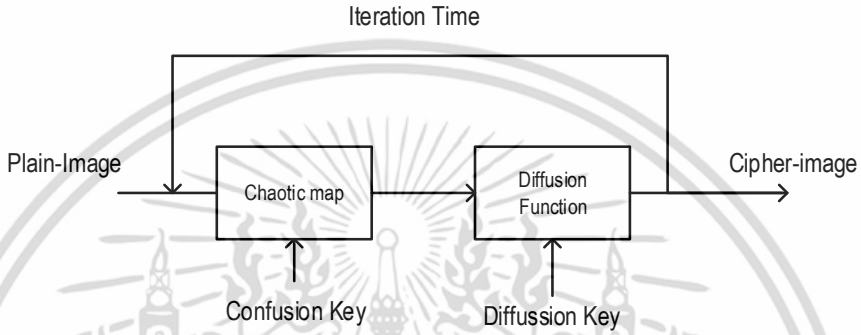


(ก) (ข)

(ค) (ง)

รูปที่ 1.3 ฮีสโทแกรมของรูปภาพต้นฉบับและรูปภาพที่เข้ารหัสลับด้วยแคทแมพ (ก) รูปภาพดิจิตอลต้นฉบับ (ข) ฮีสโทแกรมของรูปภาพต้นฉบับ (ค) รูปภาพดิจิตอลลับ (ง) ฮีสโทแกรมของรูปภาพลับ

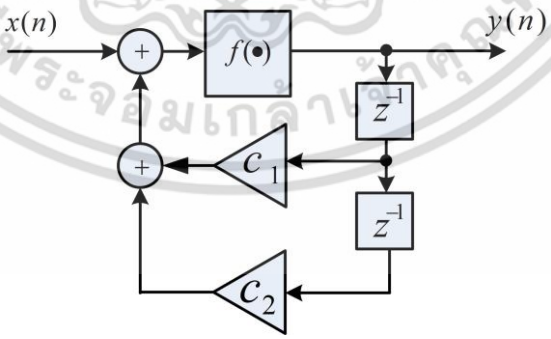
จากรูปที่ 1.3 (ก) คือรูปภาพดิจิตอลต้นฉบับ รูปที่ 1.3 (ข) คือฮีสโทแกรมของรูปภาพดิจิตอลต้นฉบับ และ เมื่อเข้ารหัสลับแล้วจะได้ดังรูปที่ 1.3 (ค) และฮีสโทแกรมได้ดังรูปที่ 1.3 (ง) ทำให้มีงานวิจัยออกแบบระบบเข้ารหัสลับรูปภาพดิจิตอลที่ทำให้ค่าฮีสโทแกรมของรูปภาพลับนั้นเปลี่ยนแปลงไป คือระบบที่ปรับปรุงการเข้ารหัสลับใช้เคออติกแมพด้วยการเพิ่มฟังก์ชั่นการแปลงค่าเข้าไปด้วย ที่เรียกว่า การเข้ารหัสลับแบบสลับและแปลงค่า (Confusion and Diffusion) แสดงได้ดังรูปที่ 1.4 [7-9]



รูปที่ 1.4 ระบบเข้ารหัสลับแบบสลับและแปลงค่าโดยใช้เคออติกแมพ

แต่ระบบเข้ารหัสลับนี้มีข้อเสียคือมีความไวต่อกุญแจต่ำ จะอธิบายรายละเอียดในการเปรียบเทียบผลการทดลองในบทที่ 4

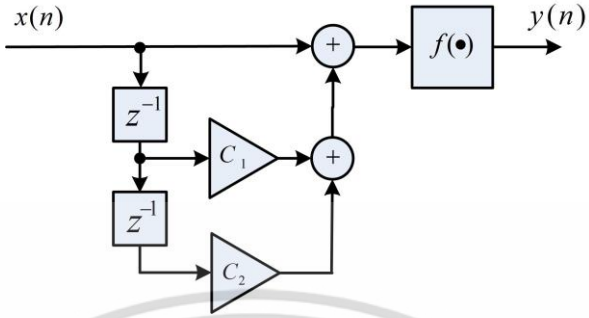
อีกงานวิจัยที่เกี่ยวข้องกับการเข้ารหัสลับคือการเข้ารหัสลับโดยอาศัยปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล (Chaos in digital filter) แสดงระบบได้ดังรูปที่ 1.5 [10-11]



รูปที่ 1.5 ระบบเข้ารหัสลับโดยใช้ปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล [11]

จากรูปที่ 1.5 การเข้ารหัสลับโดยใช้ปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล IIR (Infinite impulse response) อันดับที่สอง ค่าสัมประสิทธิ์เปรียบเสมือนกุญแจลับของวิทยาการ

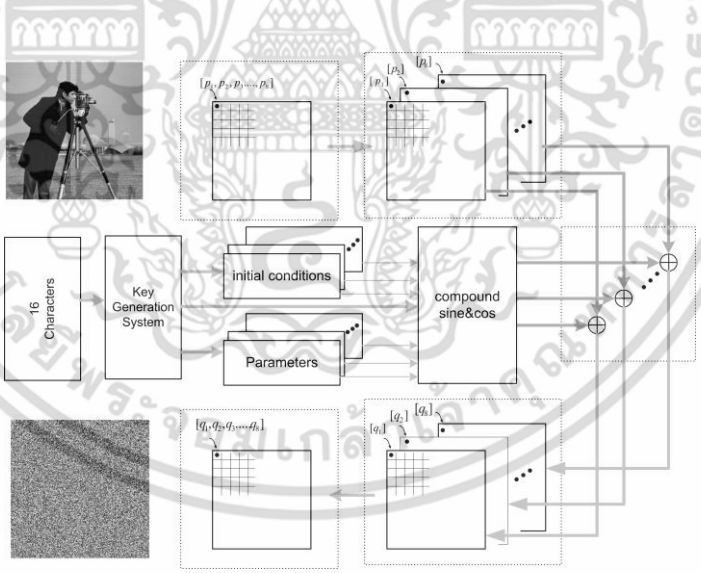
เข้ารหัสลับ โดยในส่วนถอดรหัสลับจะใช้วงจรกรองสัญญาณดิจิตอล FIR (Finite impulse response) อันดับที่สอง แสดงระบบได้ดังรูปที่ 1.6



รูปที่ 1.6 ระบบถอดรหัสลับโดยใช้ปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล [11]

จากรูปที่ 1.6 แสดงการถอดรหัสลับโดยใช้ปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล FIR อันดับที่สอง ซึ่งวิธีการนี้มีข้อเสียคือมีความไวต่อกุญแจต่ำ

และล่าสุดมีงานวิจัยเกี่ยวกับการสร้างสัญญาณเคออติกจากการรวมกันของ Sine และ Cosine เพื่อสร้างเคออติกแมพ เข้ารหัสลับรูปภาพดิจิตอล แสดงระบบเข้ารหัสลับได้ดังรูปที่ 1.7 [12]



รูปที่ 1.7 ระบบเข้ารหัสลับโดยการสร้างสัญญาณเคออติกจากการรวมกันของ Sine และ Cosine

จากรูปที่ 1.7 จะเห็นได้ว่ากระบวนการเข้ารหัสลับอาศัยการดำเนินการทางลอจิกด้วย XOR (Exclusive OR) โดยในส่วนกุญแจเกิดจากการสร้างสัญญาณเคออสจากเคออติกแมพของการรวมกัน Sine และ Cosine ข้อเสียคือ ทำให้ได้รูปภาพลับที่แต่ละพิกเซลยังมีคงความสัมพันธ์ระหว่างพิกเซลใกล้เคียงกันอยู่

ดังนั้นงานวิจัยนี้ได้ออกแบบระบบเข้ารหัสลับเนื้อหาสื่อประสม ที่มีทั้ง รูปภาพดิจิตอล ข้อความ และเสียง (Multimedia content) โดยจะเน้นเนื้อหาของรูปภาพดิจิตอลเป็นหลัก โดยระบบเข้ารหัสลับใช้กุญแจส่วนตัวขนาด 128 บิต เพื่อสร้างระนาบบิต 8 ระนาบบิตในการ XOR กับข้อมูลต้นฉบับในแต่ละระนาบบิต ซึ่งในส่วนสร้างระนาบบิตของกุญแจลับจะอาศัยการเกิดปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล IIR ลำดับที่ 2 ที่มีความไร้เสถียรภาพ (Unstable) รวมทั้งเป็นระบบที่มีความไม่เป็นเชิงเส้น (Nonlinear) ส่วนผลการทดลองงานวิจัยนี้ได้วัดประสิทธิภาพของระบบเข้ารหัสลับในพารามิเตอร์ต่างๆ ให้เป็นไปตามมาตรฐานการออกแบบการเข้ารหัสลับและได้เปรียบเทียบกับโครงสร้างเข้ารหัสลับแบบอื่นๆ ที่ผ่านมา

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1) นำเสนอการเกิดปรากฏการ์เคออสในวงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 เพื่อนำไปสร้างกุญแจลับสำหรับระบบเข้ารหัสลับ

2) นำเสนอการเกิดปรากฏการ์เคออส ด้วยเคออติกแมพชนิดต่างๆ

3) เพื่อการศึกษาวิทยาการเข้ารหัสลับเนื้อหาสื่อประสม รูปภาพดิจิตอล ข้อความ เสียง (multimedia content)

4) เพื่อการศึกษาการออกแบบการประยุกต์ใช้งานระบบเข้ารหัสลับที่นำเสนอ

1.3 รายละเอียดวิทยานิพนธ์

วิทยานิพนธ์นี้ได้แบ่งออกเป็น 5 บทด้วยกัน คือ

บทที่ 1 บทนำ กล่าวถึงความเป็นมาและความสำคัญของปัญหาที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งการเข้ารหัสลับเนื้อหาสื่อประสม และงานวิจัยที่เกี่ยวข้อง พร้อมทั้งกล่าวถึงความมุ่งหมายและวัตถุประสงค์ของการศึกษา

บทที่ 2 กล่าวถึงวิทยาการเข้ารหัสลับ ประเภทของระบบเข้ารหัสลับการโจมตีระบบรหัสลับ ทฤษฎีเคออส ทฤษฎีพื้นฐานของวงจรกรองสัญญาณดิจิตอล และการเกิดปรากฏการณ์เคออสบนวงจรกรองสัญญาณดิจิตอล

บทที่ 3 กล่าวถึงการออกแบบและการคำนวณ การออกแบบโครงสร้างเข้ารหัสลับ การออกแบบส่วนกุญแจลับ และการวัดประสิทธิภาพของระบบเข้ารหัสลับ

บทที่ 4 กล่าวถึงผลการทดลองและทดสอบการทำงาน ข้อมูลต้นฉบับที่นำมาใช้ในการทดลอง รูปภาพดิจิตอล ข้อความ เสียง และไฟล์คอมพิวเตอร์ ผลลัพธ์การสร้างกุญแจลับ ผลวัดประสิทธิภาพของระบบเข้ารหัสลับและการออกแบบการประยุกต์ใช้งาน

บทที่ 5 กล่าวถึงข้อสรุปเนื้อหาวิทยานิพนธ์ ข้อเสนอแนะและแนวทางพัฒนาต่อไป

บทที่ 2
ความรู้พื้นฐานและทฤษฎีที่เกี่ยวข้อง

สำหรับบทนี้จะกล่าวถึงหลักการและทฤษฎีที่เกี่ยวข้องกับวิทยาการเข้ารหัสลับ โดยเฉพาะอย่างยิ่งการเข้ารหัสลับเนื้อหาสื่อประสมที่ประกอบไปด้วยรูปภาพดิจิตอล ข้อความ และเสียง (multimedia content) ทฤษฎีและหลักการเกิดปรากฏการณ์เคออสที่เกี่ยวข้องกับวิทยาการเข้ารหัสลับ รวมถึงการอธิบายการเกิดปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล การวัดประสิทธิภาพของระบบเข้ารหัสลับ

2.1 วิทยาการเข้ารหัสลับ

วิทยาการเข้ารหัสลับ [13] คือการปกปิดรักษาข้อมูลต้นฉบับ (Plaintext) เป็นความลับ โดยประกอบด้วยส่วนเข้ารหัสลับ (Encryption) และกุญแจลับ (Secret-Key) มาประมวลผลร่วมกับข้อมูลต้นฉบับ ข้อมูลต้นฉบับเมื่อผ่านการประมวลผลแล้วจะได้สัญญาณขาออกเป็น ข้อมูลลับ (Ciphertext) มาใช้ในระบบสื่อสาร ในส่วนสุดท้ายคือส่วนถอดรหัสลับ (Decryption) ในส่วนนี้จะต้องการข้อมูลลับและกุญแจลับ มาประมวลผลให้ได้กลับมาซึ่งข้อมูลต้นฉบับ โดยสามารถอธิบายระบบเข้ารหัสลับได้ดังสมการที่ (2.1) และ (2.2)

$$P = D(C, K) \tag{2.1}$$

$$C = E(P, K) \tag{2.2}$$

P คือ เซตของข้อมูลต้นฉบับที่เป็นไปได้ทั้งหมด

C คือ เซตของข้อมูลลับที่เป็นไปได้ทั้งหมด

K คือ เซตของกุญแจลับที่เป็นไปได้ทั้งหมด

E คือ การเข้ารหัสลับ

D คือ การถอดรหัสลับ

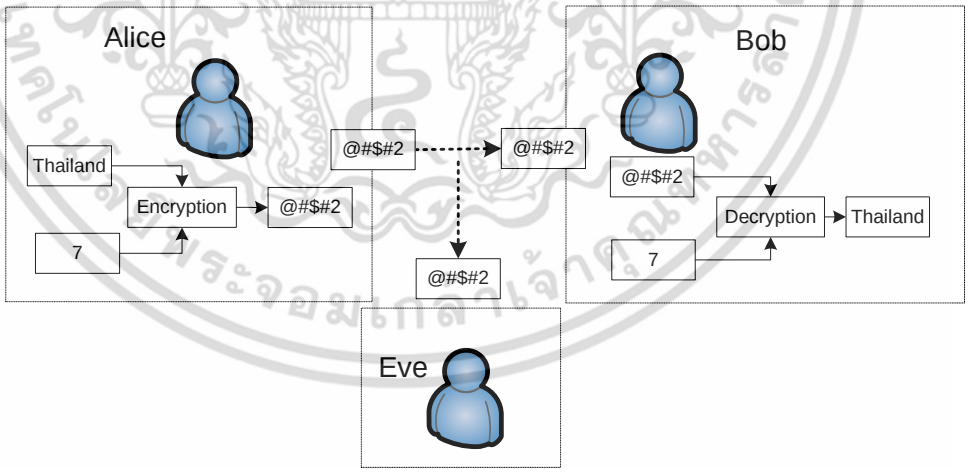
โดยที่ $D(E(X)) = X$ เป็นจริง สำหรับข้อมูลต้นฉบับทุกรูปแบบที่ $X \in P$ ซึ่งหมายความว่า ถ้าเข้ารหัสลับด้วยข้อความต้นฉบับ X โดยผ่านฟังก์ชัน E จะได้ ข้อความลับ C ออกมาและเมื่อถอดรหัสข้อมูลลับ โดยผ่านฟังก์ชัน D จะต้องได้ข้อความต้นฉบับกลับคืนมาเสมอ

2.1.1 ประเภทของระบบเข้ารหัสลับ

ระบบเข้ารหัสลับสามารถจำแนกได้หลากหลายรูปแบบตามเกณฑ์ที่ใช้ในการแบ่ง คือจำแนกแยกประเภทด้วยชนิดกุญแจลับได้แก่ กุญแจสมมาตร และกุญแจอสมมาตร จำแนกแยกประเภทด้วยวิธีการเข้ารหัสลับซึ่งแบ่งเป็น เข้ารหัสลับแบบบล็อค และเข้ารหัสลับแบบสตรีม และจำแนกแบ่งตามความปลอดภัยได้แก่ ระบบที่ปลอดภัยโดยไร้เงื่อนไข และระบบที่ปลอดภัยเชิงคำนวณ มีรายละเอียดดังหัวข้อต่อไปนี้

2.1.1.1 การเข้ารหัสลับแบบกุญแจสมมาตรและกุญแจอสมมาตร

สำหรับการเข้ารหัสลับด้วยกุญแจสมมาตร (Symmetric cipher) หรือเรียกว่า กุญแจส่วนตัว (Private key) กุญแจที่เข้ารหัสลับและกุญแจที่ถอดรหัสลับ เป็นกุญแจเดียวกัน ดังนั้นผู้ส่งข้อมูลลับและผู้รับข้อมูลลับเท่านั้นจะต้องเก็บกุญแจไว้ส่วนตัวไม่สามารถเปิดเผยให้บุคคลที่สามรับรู้ ในกรณีที่แฮกเกอร์สามารถขโมยข้อมูลได้ระหว่างเส้นทางการสื่อสารก็ไม่สามารถเข้าใจความหมายได้ ยกตัวอย่างเช่น Alice ต้องการส่งข้อมูลข้อความไปหา Bob ดังรูปที่ 2.1



รูปที่ 2.1 การส่งข้อมูลลับโดยใช้กุญแจสมมาตร

จากรูปที่ 2.1 ส่วนของผู้ส่ง Alice ส่งข้อมูลข้อความคำว่า “Thailand” เข้ารหัสลับด้วยกุญแจของตัวเองที่มีอยู่แล้วคือ “7” ผ่านกระบวนการเข้ารหัสลับได้ข้อมูลลับคือ “@#$#2” ทำให้ตลอดเส้นทางการสื่อสารระหว่าง Alice ไปยัง Bob เป็นข้อมูลลับที่เข้ารหัสลับแล้ว โดยมี Eve เป็นแฮก

เกอร์ขโมยข้อมูลในเส้นทางการสื่อสาร แต่ Eve ไม่สามารถเข้าใจได้ แต่เมื่อ Bob ได้รับข้อมูลลับก็สามารถถอดรหัสลับด้วยกุญแจของตัวเองที่มีอยู่แล้ว ซึ่งเป็นกุญแจที่เหมือนกับ Alice ทุกประการ ก็จะทำให้ Bob สามารถเข้าใจเนื้อหาข้อมูลจาก Alice ได้

สำหรับการเข้ารหัสด้วยกุญแจที่ไม่สมมาตร (Asymmetric cipher) หรือที่เรียกว่า กุญแจสาธารณะ (Public key) กุญแจที่ใช้ถอดรหัสลับจะแตกต่างจากกุญแจที่ใช้เข้ารหัสลับ ผู้ส่งข้อความลับจะส่งกุญแจออกด้วย ในกรณีที่ Eve ขโมยข้อมูลไปได้ก็ไม่สามารถใช้กุญแจนั้นถอดได้อยู่ดี เพราะข้อมูลลับนั้นไม่สามารถถอดได้ด้วยกุญแจที่ส่งมาด้วยกันได้ โดยที่ผู้รับข้อความลับจะเก็บกุญแจส่วนตัวไว้ เมื่อได้กุญแจมาจากผู้ส่งก็สามารถคำนวณร่วมกับกุญแจที่มีอยู่ ให้ได้กุญแจมาถอดรหัสได้ กระบวนการดังกล่าวเรียกว่ากระบวนการแลกกุญแจ มีหลายแบบด้วยกัน ยกตัวอย่างเช่น แบบ Diffie-Hellman คือ ต้องมีกุญแจส่วนตัวของผู้ส่ง และผู้รับซึ่งเป็นกุญแจที่แตกต่างกันก็ได้ โดยกุญแจทั้ง 2 ตัวจะต้องมาคำนวณหากุญแจที่แท้จริงเพื่อใช้ในระบบรหัสลับ

2.1.1.2 การเข้ารหัสลับแบบบล็อคและแบบสตรีม

สำหรับการเข้ารหัสแบบบล็อค (Block cipher) คือ การแบ่งข้อมูลต้นฉบับจะทำการแบ่งออกเป็นส่วนๆ โดยแต่ละส่วนเรียกว่าบล็อคจากนั้นเข้ารหัสทีละบล็อค แสดงได้ดังสมการที่ (2.3) และ (2.4)

$$C_i = E(P_i, K) \tag{2.3}$$

$$P_i = D(C_i, K) \tag{2.4}$$

เมื่อ $i = 0, 1, ..., (N/n) - 1$

N คือ จำนวนบิตข้อมูลต้นฉบับ

n คือ จำนวนของบล็อค

C คือ ข้อมูลลับแบบบล็อค

P คือ ข้อมูลต้นฉบับแบบบล็อค

K คือ กุญแจเข้ารหัสลับแบบบล็อค

สำหรับการเข้ารหัสลับแบบสตรีม (Stream cipher) คือ การเข้ารหัสข้อมูลต้นฉบับจะดำเนินการทีละบิต แสดงได้ดังสมการที่ (2.5) ยกตัวอย่างการเข้ารหัสลับแบบสตรีมเช่น Rivest Cipher 4 (RC4) และ SNOW เป็นต้น

$$c_i = E(c_i, k_i) \quad (2.5)$$

$$p_i = D(c_i, k_i) \quad (2.6)$$

เมื่อ $i = 0, 1, ..., N-1$

c คือ ข้อมูลลับแบบสตรีม

p คือ ข้อมูลต้นฉบับแบบสตรีม

k คือ กุญแจเข้ารหัสลับแบบสตรีม

2.1.1.3 การเข้ารหัสลับแบบปลอดภัยโดยไร้เงื่อนไขและปลอดภัยเชิงคำนวณ

การเข้ารหัสลับสามารถแบ่งตามความปลอดภัยได้ 2 แบบ คือ แบบที่ปลอดภัยโดยไร้เงื่อนไข (Unconditionally secure algorithm) เป็นระบบที่มีความปลอดภัยสูง เนื่องจากผู้โจมตีไม่สามารถวิเคราะห์ข้อความลับกลับมาเป็นข้อความต้นฉบับได้ ไม่ว่าจะมีเวลาและทรัพยากรในการประมาลผลมากเท่าใดก็ตาม เพราะระบบนี้จะใช้กุญแจเพียงครั้งเดียวแล้วทิ้ง (one-time-pad) ข้อเสียของระบบนี้คือมีการบำรุงรักษาสูงและแพงเนื่องจากกุญแจจำเป็นต้องสร้างใหม่อยู่ตลอดเวลา ปัจจุบันนี้ส่วนมากจะใช้ในระบบการเงินของธนาคาร แบบต่อมาคือ แบบที่ปลอดภัยเชิงคำนวณ (Computationally secure algorithm) เป็นระบบที่ผู้โจมตีต้องใช้เวลาในการโจมตีวิเคราะห์ระบบเข้ารหัสลับ ซึ่งระบบชนิดนี้มีความปลอดภัยเพียงพอต่อการใช้งาน เพราะผู้เข้ารหัสลับสามารถทำให้ข้อความลับเป็นความลับได้ยาวนานตราบใดที่กุญแจยังคงเก็บไว้เป็นความลับ

อีกหนึ่งกระบวนการที่สำคัญของวิทยาการเข้ารหัสคือการวิเคราะห์รหัสลับ Cryptanalysis) ซึ่งผู้วิเคราะห์รหัสลับ (Cryptanalyst) จะต้องมีความรู้ในทางคณิตศาสตร์เป็นอย่างดี เช่น Alan Turing ผู้วิเคราะห์โครงสร้าง อินิกม่า (Enigma) ของเยอรมันในสงครามโลกครั้งที่ 2 ซึ่งกระบวนการวิเคราะห์รหัสลับเป็นส่วนหนึ่งของการโจมตีระบบรหัสลับดังจะกล่าวรายละเอียดในหัวข้อต่อไป

2.1.2 การโจมตีระบบเข้ารหัสลับ

การโจมตีระบบรหัสลับ สามารถแบ่งออกได้เป็น 2 วิธี คือ การวิเคราะห์รหัสลับและการโจมตีแบบตะลุย สามารถอธิบายได้ดังนี้

2.1.2.1 การวิเคราะห์รหัสลับ

โดยทั่วไปในการศึกษาถึงการวิเคราะห์รหัสลับ (Cryptanalysis) จะมีข้อกำหนดสมมุติฐานพื้นฐานว่า แฮกเกอร์สามารถทราบถึงโครงสร้างของระบบเข้ารหัสลับที่ใช้งานเป็นอย่างดี โดยสามารถแบ่งเป็นขีดความสามารถของผู้เจาะรหัสลับได้ดังนี้

1. รับรู้ข้อความลับอย่างเดียว (Ciphertext-only) คือ ผู้เจาะรหัสลับสามารถเข้าถึงข้อความลับได้และต้องการหาข้อความต้นฉบับหรือกุญแจ วิธีการนี้เป็นวิธีการที่ฝ่ายตรงข้ามมีข้อมูลน้อยที่สุด

2. ทราบข้อความต้นฉบับ (Known plaintext) ผู้เจาะรหัสลับสามารถเข้าถึงข้อความต้นฉบับและข้อความลับได้ ทำให้สามารถวิเคราะห์หาความสัมพันธ์ระหว่างข้อความต้นฉบับและข้อความลับเพื่อหากุญแจได้

3. เลือกข้อความต้นฉบับ (Chosen plaintext) ผู้เจาะรหัสลับสามารถเข้าถึงและใช้เครื่องเข้ารหัสได้ชั่วคราว ทำให้สามารถเลือกใช้ข้อความต้นฉบับได้เองตามปรารถนา จึงได้ข้อความลับที่เป็นของคู่กัน วิธีการนี้ทำให้ผู้เจาะรหัสลับสามารถวิเคราะห์หาความสัมพันธ์ระหว่างข้อความต้นฉบับและข้อความลับเพื่อหากุญแจได้

4. เลือกข้อความลับ (Chosen ciphertext) วิธีการนี้เป็นวิธีการที่คล้ายคลึงกับเลือกข้อความต้นฉบับ แต่ผู้เจาะรหัสลับสามารถใช้เครื่องถอดรหัสลับได้ชั่วคราว จึงสามารถกำหนดข้อความลับได้ตามปรารถณาเพื่อวิเคราะห์หาความสัมพันธ์ระหว่างข้อความลับและข้อความต้นฉบับเพื่อหากุญแจได้

5. การวิเคราะห์หาส่วนแตกต่าง (Differential Cryptanalysis) วิธีนี้คือการวิเคราะห์หาส่วนแตกต่างสัญญาณมาเปรียบเทียบกัน

2.1.2.2 การโจมตีแบบตะลุย

การโจมตีแบบตะลุย (Brute-Force) เป็นการโจมตีโดยเดาค่ากุญแจทุกค่าที่สามารถเป็นไปได้ และนำค่ากุญแจนั้นมาถอดรหัสข้อความลับที่มีอยู่ จนกว่าได้ข้อความต้นฉบับที่ต้องการ การโจมตีแบบนี้ไม่สามารถป้องกันได้ ทั้งนี้เนื่องจากผู้โจมตีเพียงแค่เอากุญแจแต่ละค่ามาถอดรหัสข้อความลับตรง ๆ อย่างไรก็ตามผู้เข้ารหัสลับสามารถทำให้ผู้โจมตีต้องประสบกับความยากลำบากหรือประสบกับความยุ่งยากในการโจมตีได้ ทั้งนี้ทั้งนั้นความแข็งแกร่งของระบบเข้ารหัสลับยังคงต้องขึ้นอยู่กับส่วนอื่นอีก

ถ้ากุญแจในระบบเข้ารหัสลับของเรามีจำนวนบิตสูง หรือกุญแจมีขนาดใหญ่ จะมีผลทำให้จำนวนกุญแจทั้งหมดที่สามารถเป็นได้สูงตามไปด้วย ตารางที่ 2.1 คือจำนวนกุญแจทั้งหมดของขนาดกุญแจต่างๆ และเวลาที่ใช้ในการถอดรหัสของกุญแจแต่ละขนาดในกรณีที่รู้อัลกอริทึม

ตารางที่ 2.1 จำนวนกุญแจทั้งหมดของขนาดกุญแจต่างๆ และเวลาที่ใช้ในการถอดรหัสของกุญแจแต่ละขนาด 1 ล้านล้านครั้งต่อวินาที [24]

ขนาดกุญแจ (บิต)	อัลกอริทึม	ค่าที่เป็นไปได้	ระยะเวลาการโจมตีตะลุย (1 ล้านล้านครั้งต่อวินาที)
32	Blowfish-32	4.3×10^{9}	1.25 มิลลิวินาที
56	DES	7.2×10^{16}	10 ชั่วโมง
128	AES-128 , วิธีที่นำเสนอ	3.4×10^{38}	5.4×10^{18} ปี
168	3-DES	3.7×10^{50}	5.9×10^{30} ปี
192	AES-192	6.2×10^{57}	1.8×10^{57} ปี

จากตารางจะเห็นว่า ถ้ากุญแจที่ขนาดกุญแจ 32 บิต สามารถคำนวณออกมาโดยใช้เวลาไม่มากด้วยเทคโนโลยีซุปเปอร์คอมพิวเตอร์ (Super computer) แต่ถ้ากุญแจมีขนาดเพิ่มขึ้นเช่น ที่ 128 บิต หรือ 256 บิต จะต้องใช้เวลานานมหาศาล ดังนั้นระบบเข้ารหัสลับที่ดีควรจะต้องใช้ขนาดของกุญแจลับอย่างน้อย 128 บิต เพื่อป้องกันการโจมตีแบบตะลุยได้อีกทางหนึ่ง

2.2 ทฤษฎีเคออส

2.2.1 ลักษณะพฤติกรรมเคออส

คือระบบพลวัตที่มีการเปลี่ยนแปลงตามเวลา โดยลักษณะการเปลี่ยนแปลงของระบบ เคออสนี้จะมีลักษณะที่ปั่นป่วนจนดูเหมือนเป็นการสุ่มไร้ระเบียบ แต่จริงแล้วระบบเคออสเป็นระบบที่เป็นระเบียบ ซึ่งในทางคณิตศาสตร์และฟิสิกส์ให้คำจำกัดความของระบบเคออสว่าคือระบบที่ไม่เป็นเชิงเส้น (non-linear system) ระบบเคออสไม่จำเป็นต้องแตกต่างกันในแง่ของขนาดของผลลัพธ์เสมอไป แต่อาจแตกต่างกันในแง่ของพฤติกรรมการเปลี่ยนแปลงก็ได้ ตัวอย่างเช่น ถ้ามีระบบอยู่สองระบบแล้วกำหนดให้ค่าเงื่อนไขเริ่มต้นต่างกันเพียงเล็กน้อย การเปลี่ยนแปลงของระบบทั้งสองนั้นจะมีลักษณะที่คล้ายคลึงกันมากในขณะเริ่มต้น แต่เมื่อเวลาผ่านไปการเปลี่ยนแปลงนั้นแทบจะไม่มีอะไรที่เหมือนกันเลย

2.2.2 คุณสมบัติของเคออส

1. เคออสเป็นระบบพลวัต (Dynamical system) คือ ระบบที่มีสถานะของระบบมีการเปลี่ยนแปลงตามเวลา และสามารถอธิบายด้วยสมการคณิตศาสตร์ อาจเป็นการนำเอาปรากฏการณ์ในธรรมชาติมาเขียนเป็นสมการตามหลักฟิสิกส์ หรือสร้างสมการขึ้นมาเองตามเหตุผลและการคาดคะเน

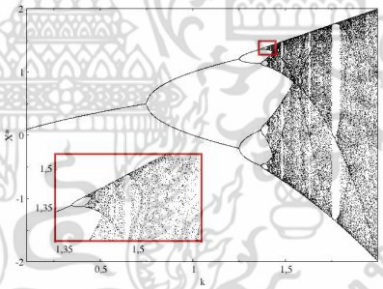
2. เคออสเป็นระบบไม่เป็นเชิงเส้น (non-linear system) คือ ผลลัพธ์ทั้งหมดของระบบ ไม่เท่ากับ ผลรวมของผลลัพธ์ที่เกิดจากส่วนย่อย ๆ ของระบบรวมกัน

3. เคออสไวต่อค่าเริ่มต้น (sensitive dependence on initial conditions) คือ ถ้าระบบใดๆ ที่เริ่มต้นจากสภาวะที่แตกต่างกันเพียงเล็กน้อย เมื่อระบบได้มีการเปลี่ยนแปลงไปสักระยะหนึ่ง สภาวะของระบบทั้งสองนั้นจะแตกต่างกันอย่างเห็นได้ชัด

4. เคออสไม่สามารถทำนายล่วงหน้าในระยะยาว (long-term prediction is impossible) เพราะไม่สามารถรู้ได้ว่าจะมีเหตุปัจจัยใดที่กระทบ ส่งผลให้เกิดการเปลี่ยนแปลง

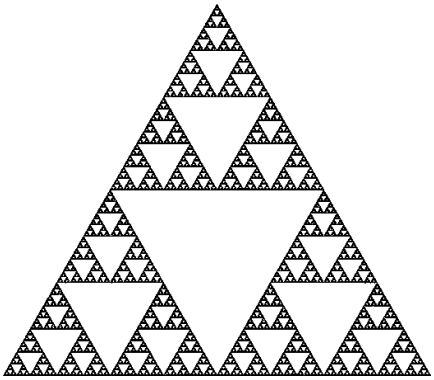
2.2.3 ค่าตัวชี้วัดความเป็นเคออส

ทางสองแพร่ง (Bifurcation) หรือทางแพร่ง มีลักษณะเหมือนตัววาย (Y) เกิดขึ้นเมื่อความไร้ระเบียบได้พัฒนาตัวเองออกไปจากจุดสมดุลจนสุดขอบเขต ทำให้ระบบมีความยุ่งเหยิงซับซ้อนที่สุด ณ จุดที่ไกลจากสมดุลที่สุดนี้ ตัวควบคุมหรือตัวดึงดูด (Attractor) จะเปลี่ยนสภาพโดยสิ้นเชิงไปสู่ตัวควบคุมตัวใหม่ที่จะทำหน้าที่กำหนดและควบคุมระบบที่ปรากฏขึ้นใหม่หลังทางแพร่งนี้ที่ไม่เหมือนเดิมและซับซ้อนยิ่งกว่าเดิม แต่จะคงสาระและคุณสมบัติเดิมเป็นเนื้อในอยู่ในระบบใหม่นั้น ตัวอย่างเช่น ลอจิสติกแมพ ดังรูปที่ 2.2



รูปที่ 2.2 ลักษณะของทางสองแพร่ง (Bifurcation)

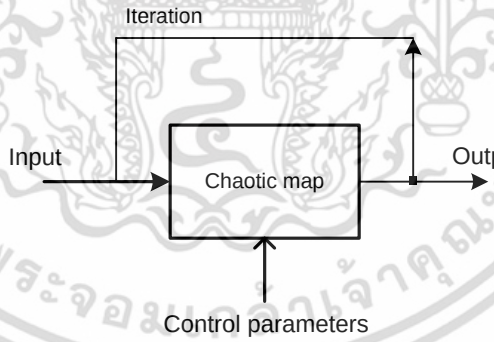
แฟรกทัล (Fractal) เป็นระบบรูปร่างเรขาคณิตชนิดหนึ่ง ที่อาจมีเกณฑ์ในการประกอบรูปร่างที่ไม่ซับซ้อน แต่เกณฑ์เหล่านั้นจะก่อให้เกิดแบบภาพในลักษณะภาพใหญ่และภาพย่อยที่ลักษณะเหมือนกันหรือคล้ายกันมาก หรือที่เรียกว่า ความคล้ายตัวเอง (Self-similarity) ระบบเคออสทุกระบบไม่จำเป็นต้องมีคุณลักษณะนี้ แต่ส่วนมากมักจะเกิดร่วมกับระบบเคออส ดังรูปที่ 2.3



รูปที่ 2.3 ลักษณะของแฟรกทัล (Fractal)

2.2.4 เคออติกแมพ (Chaotic map)

เคออติกแมพ (Chaotic map) เป็นระบบพลวัตที่สามารถเขียนเป็นสมการทางคณิตศาสตร์ได้ โดยทั่วไปสำหรับเคออติกแมพ จะประกอบไปด้วยค่าเงื่อนไขเริ่มต้น (Initial condition) และตัวแปรควบคุม (Control parameter) จำนวนรอบ (Iteration) แสดงได้ดังรูปที่ 2.4 โดยสัญญาณขาเข้าเปรียบเสมือนข้อมูลต้นฉบับ จำนวนรอบและค่าเริ่มต้นเปรียบเสมือนกุญแจลับ และสุดท้ายสัญญาณขาออกเปรียบเสมือนข้อมูลลับ



รูปที่ 2.4 ระบบเคออติกแมพ

ปัจจุบันมีเคออติกแมพจำนวนมากที่ได้นำมาประยุกต์ใช้กับวิทยาการเข้ารหัสลับในส่วนการสลับตำแหน่งของข้อมูลต้นฉบับ เช่น ลอจิสติกแมพ (Logistic map) แคทแมพ (Cat map) และสแตนดาร์ดแมพ (Standard map) ซึ่งมีรายละเอียดดังนี้

2.2.4.1 ลอจิสติกแมพ (Logistic map)

ระบบพลวัตไม่เป็นเชิงเส้นอย่างง่ายที่สามารถแสดงพฤติกรรมเคออสได้ ลอจิสติกแมพนี้เริ่มเป็นที่รู้จักกว้างขวางจากผลงานตีพิมพ์ของนักชีววิทยา Robert May แรกเริ่มนั้นลอจิสติกแมพนี้ถูกสร้างขึ้นโดย Pierre François Verhulst เพื่อเป็นแบบจำลองการกระจายปริมาณประชากรมนุษย์ ต่อมาถูกนำไปใช้สำหรับการเพิ่มปริมาณประชากรของสปีชีส์อื่นๆ ภายใต้สภาวะแวดล้อมจำกัด เช่น อาหาร โรค และ อื่นๆ อีกมากมายซึ่งแบบจำลองจะมีพฤติกรรมจากผลของค่าเริ่มต้น ซึ่งสามารถเขียนในรูปสมการทางคณิตศาสตร์ดังสมการที่ (2.7)

$$X_{n+1} = rX_n(1 - X_n) \tag{2.7}$$

r คือ ค่าคงที่เริ่มต้น (Initial value)

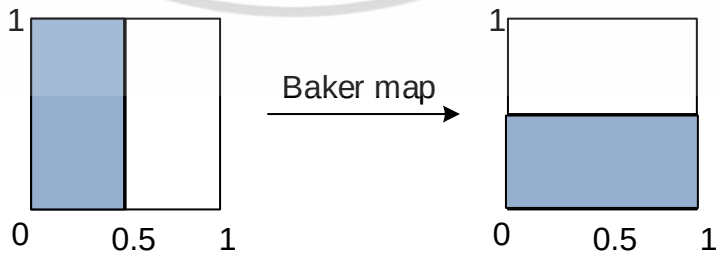
n คือ จำนวนรอบ (Iteration)

2.2.4.2 เบเกอร์แมพ (Baker map)

เบเกอร์แมพ (Baker map) เป็นระบบพลวัตไม่เป็นเชิงเส้น 2 มิติ แสดงได้ดังสมการที่ (2.8) และรูปที่ 2.5

$$(X_{n+1}, Y_{n-1}) = \begin{cases} (2X_n, Y_n/2) & ; \ 0 \le X_n < 1/2 \\ (2X_n - 1, Y_k/2 + 1/2) & ; \ 1/2 \le X_n \le 1 \end{cases} \tag{2.8}$$

เมื่อ n คือ จำนวนรอบ (Iteration)



(ก) (ข)

รูปที่ 2.5 ลักษณะของเบเกอร์แมพ (Baker map) (ก) ข้อมูลต้นฉบับแบ่งออกเป็นสองส่วน (ข) ข้อมูลเมื่อผ่านเบเกอร์แมพ 1 รอบ (n=1)

จากรูปที่ 2.5 (ก) ตำแหน่งข้อมูลต้นฉบับแบ่งออกเป็นสองส่วน เมื่อผ่านเบเกอร์แมพรอบที่ 1 จะได้ตำแหน่งใหม่ดังรูปที่ 2.5 (ข)

2.2.4.3 แคทแมพ (Cat map)

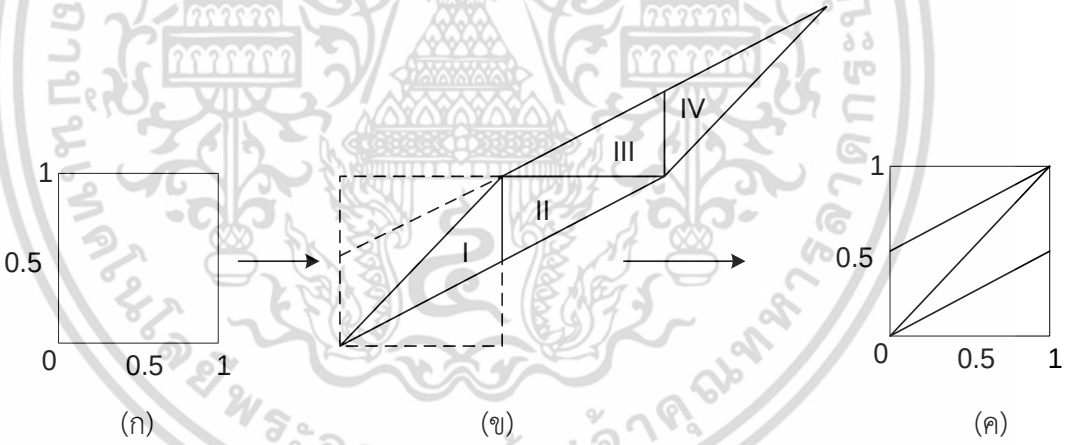
แคทแมพ (Cat map) ผู้สร้างคือ Vladimir Arnold โดยใช้รูปภาพแมวเป็นตัวทดลองจึงได้ตั้งชื่อว่า แคทแมพ เป็นระบบ 2 มิติ ดังสมการคณิตศาสตร์ที่ (2.9) และสมการที่ (2.10) และรูปที่ 2.6

$$X_{n+1} = (X + aY) \bmod N \tag{2.9}$$

$$Y_{n+1} = (bX + (ab+1)Y) \bmod N \tag{2.10}$$

a, b คือ ค่าคงที่เริ่มต้น (Initial value)

n คือ จำนวนรอบ (Iteration)



รูปที่ 2.6 ลักษณะของแคทแมพ (Cat map) (ก) ข้อมูลต้นฉบับ (ข) การสลับตำแหน่งในรอบที่ 1 (ค) ข้อมูลเมื่อผ่าน 1 รอบ (n=1)

จากรูปที่ 2.6 (ก) เป็นข้อมูลต้นฉบับ ผ่านแคทแมพตามรูปที่ 2.6 (ข) จะทำให้ได้ข้อมูลใหม่ดังรูปที่ 2.6 (ค) ซึ่งเป็นรูปที่เกิดจากการสลับค่าผ่านเคออติกแคทแมพ 1 รอบ

2.2.4.4 สแตนดาร์ดแมพ (Standard map)

สแตนดาร์ดแมพ (Standard map) หรือชื่อเดิมคือ Chirikov standard map คิดค้นโดย Boris Chirikov สามารถอธิบายด้วยสมการที่ (2.11)

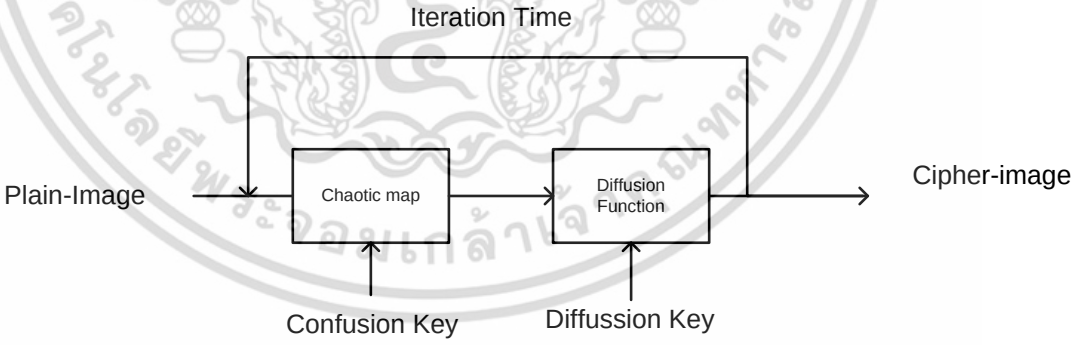
$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} X_n + Y_n \bmod 2\pi \\ Y_n - q\sin(X_n + Y_n) \bmod 2\pi \end{bmatrix} \quad (2.11)$$

n คือ จำนวนรอบ (Iteration)

q คือ ค่าคงที่เริ่มต้น (Initial value)

2.2.4.5 ระบบเข้ารหัสลับแบบสลับและแปลงค่า (Confusion and Diffusion)

ระบบเข้ารหัสลับแบบสลับและแปลงค่า (Confusion and Diffusion) ถูกนำเสนอโดย Shanon และได้นำมาใช้ออกแบบระบบเข้ารหัสลับแบบบล็อคเพื่อเพิ่มความแข็งแกร่ง เช่น DES และ AES ซึ่งระบบเข้ารหัสทั้ง 2 แบบนี้เหมาะสำหรับข้อมูลขนาดเล็ก ไม่เหมาะกับข้อมูลสื่อประสมเนื่องจากมีขนาดใหญ่และมีความเสมือนกันระหว่างตำแหน่งใกล้เคียงสูง ดังนั้นจึงเกิดระบบเข้ารหัสที่ได้ออกแบบโดยใช้เคออติกแมพเพื่อสลับค่า ถูกนำเสนอโดย เฟรดดริก (Fridrich) [7] ดังรูปที่ 2.7



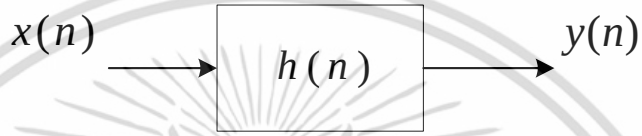
รูปที่ 2.7 ระบบเข้ารหัสลับแบบสลับและแปลงค่าโดยใช้เคออติกแมพ

ในส่วนการสลับค่า (Confusion) จะใช้เคออติกแมพมาใช้ในการปรับสลับค่า ซึ่งมีหลากหลายวิธีดังที่อธิบายในหัวข้อก่อนหน้านี้ แต่สัญญาณขาออกที่ได้จะถูกพิจารณาเป็นสัญญาณขาเข้าให้กับส่วนแปลงค่า (Diffusion) ตามลำดับ

2.3 ทฤษฎีพื้นฐานของวงจรกรองสัญญาณดิจิตอล

2.3.1 ความหมายของวงจรกรองสัญญาณดิจิตอล

วงจรกรองสัญญาณดิจิตอล (Digital filter) คือ กระบวนการเชิงเลข (Numerical procedure) ซึ่งเปลี่ยนลำดับของจำนวนๆ หนึ่งเข้าไปอีกลำดับหนึ่งที่มีคุณสมบัติตามที่ต้องการ หรือระบบที่รับสัญญาณแบบดิจิตอล เพื่อสร้างสัญญาณขาออกให้มีลักษณะตามต้องการที่ได้ทำการออกแบบระบบ ดังรูปที่ 2.8

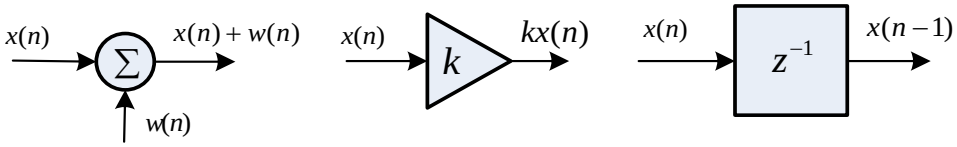


รูปที่ 2.8 วงจรกรองสัญญาณดิจิตอล

สัญญาณขาเข้า $x(n)$ เป็นสัญญาณดิจิตอล โดยมีระบบ $h(n)$ เป็นผลการตอบสนองอิมพัลส์ของวงจรกรองสัญญาณดิจิตอล สามารถประยุกต์ใช้งานได้มากมายเช่น ทางด้านระบบอิเล็กทรอนิกส์ ระบบสื่อสาร ระบบควบคุม และวิทยาการเข้ารหัสลับ จากรูปที่ 2.8 สามารถเขียนเป็นสมการได้ดังสมการที่ (2.12)

$$y(n) = x(n) * h(n) \tag{2.12}$$

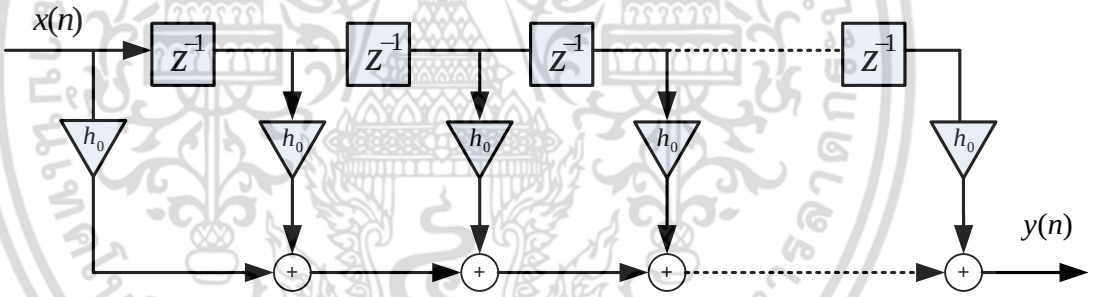
โดยทั่วไปการใช้วงจรกรองสัญญาณดิจิตอลจำเป็นต้องมีการแปลงสัญญาณขาเข้าให้อยู่ในรูปแบบดิจิตอล หลักจากนั้นสัญญาณจะถูกประมวลผลทางตัวเลข ซึ่งจะอาศัยวงจรที่ใช้ในระบบคอมพิวเตอร์ ได้แก่ ตัวบวก ตัวคูณ ตัวหน่วงเวลา และอุปกรณ์หน่วยความจำต่างๆ วงจรกรองสัญญาณดิจิตอล ประกอบไปด้วย 3 ส่วนสำคัญคือ ส่วนตัวบวก (Adder) ตัวคูณ (multiplier) และตัวหน่วงเวลา (unit delay) ดังแสดงในรูปที่ 2.9



(ก) (ข) (ค)

รูปที่ 2.9 องค์ประกอบพื้นฐานที่ใช้เป็นส่วนประกอบของวงจรกรองสัญญาณดิจิตอล (ก) ตัวบวก (ข) ตัวคูณ (ค) ตัวหน่วงเวลา

จากรูปที่ 2.9 (ก) ตัวบวก (Adder) คือการรวมกันของสัญญาณ รูปที่ 2.9 (ข) ตัวคูณ (Multiplier) และ รูปที่ 2.9 (ค) ตัวหน่วงเวลาหนึ่งหน่วย (Unit delay) เป็นอุปกรณ์เข้าถึงค่าในอดีตของลำดับข้อมูล วงจรกรองสัญญาณดิจิตอลสามารถจำแนกตามลักษณะของผลตอบสนองอิมพัลส์ คือ วงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์จำกัด (FIR) และวงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์ไม่จำกัด (IIR) แสดงโครงสร้างของวงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์จำกัด (FIR) ได้ดังรูปที่ 2.10

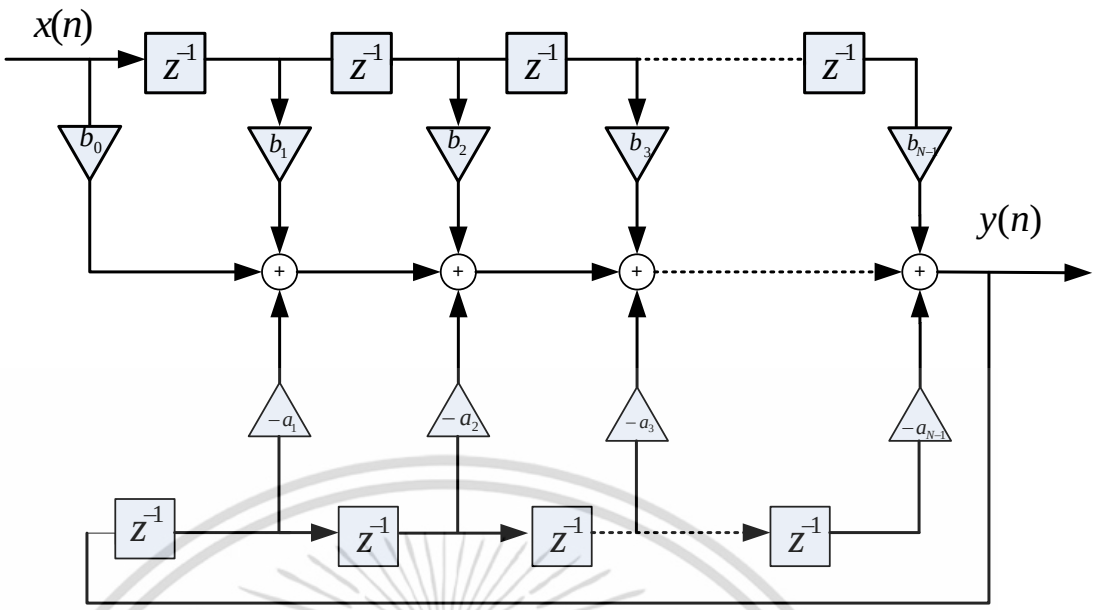


รูปที่ 2.10 โครงสร้างของวงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์จำกัด (FIR)

จากรูปที่ 2.10 วงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์จำกัด (FIR) เป็นวงจรกรองสัญญาณที่ไม่มีการป้อนกลับ สามารถแสดงฟังก์ชันถ่ายโอนได้ดังสมการที่ (2.13)

$$H(z) = \sum_{n=0}^{N+1} h(n) z^{-1} \tag{2.13}$$

และโครงสร้างของวงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์ไม่จำกัด (IIR) แสดงได้ดังรูปที่ 2.11



รูปที่ 2.11 โครงสร้างของวงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์ไม่จำกัด (IIR)

จากรูปที่ 2.11 วงจรกรองสัญญาณดิจิตอลแบบผลตอบสนองอิมพัลส์ไม่จำกัด (IIR) เป็นวงจรที่มีการป้อนกลับ หรือที่เรียกว่าวงจรกรองสัญญาณแบบป้อนกลับ (Recursive filter) เพราะสัญญาณขาออกจะขึ้นอยู่กับค่าสัญญาณขาเข้าที่ป้อนเข้ามาและสัญญาณขาออกในอดีตสามารถแสดงฟังก์ชันถ่ายโอนได้ดังสมการที่ (2.14)

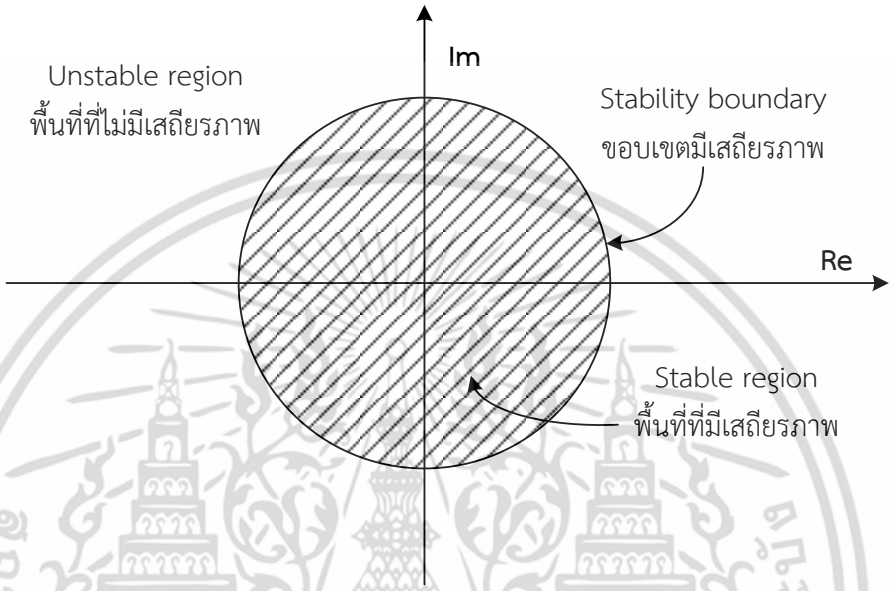
$$H(z) = \frac{Y(z)}{X(z)} = \frac{\sum_{k=0}^{M} b_k z^{-k}}{1 + \sum_{k=0}^{N} a_k z^{-k}} \qquad (2.14)$$

2.3.2 การเกิดปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล

วงจรกรองสัญญาณดิจิตอล (Digital filter) สามารถกำหนดค่าของระบบเพื่อให้ได้ข้อมูลที่มีลักษณะพฤติกรรมเคออสได้ด้วยวงจรกรองสัญญาณดิจิตอลแบบ IIR โดยมีเงื่อนไข 2 ข้อ คือ ความไร้เสถียรภาพของระบบ และ ความไม่เป็นเชิงเส้นของระบบ สามารถอธิบายได้ดังนี้

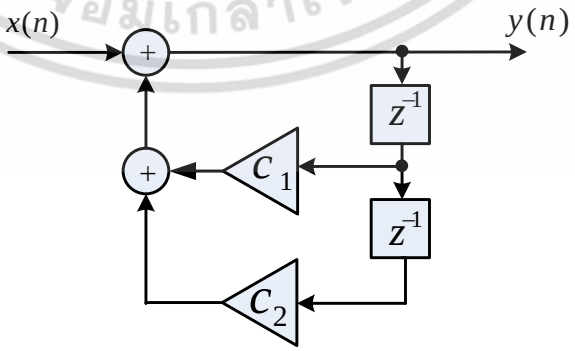
2.3.2.1 ความไร้เสถียรภาพของระบบ

ระบบที่มีเสถียรภาพมีเงื่อนไขว่า สัญญาณขาเข้าที่มีขอบเขตของขนาดจำกัด จะทำให้เกิดสัญญาณขาออกที่มีขอบเขตจำกัด โดยสามารถตรวจสอบได้จากระนาบ z-plane สำหรับการพิจารณาดิจิตอลโดเมนดังรูปที่ 2.12 จากการคำนวณตำแหน่งของโพลจากฟังก์ชันถ่ายโอน



รูปที่ 2.12 พื้นที่ที่มีเสถียรภาพบน z-plane

จากรูปที่ 2.12 ระบบมีเสถียรภาพเมื่อตำแหน่งของโพลทุกตัวมีขนาดน้อยกว่าหนึ่ง หรืออยู่ภายในวงกลมหนึ่งหน่วย (Unit circle) ยกตัวอย่างเช่นวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สองที่มีโครงสร้างแบบโดยตรง (Direct form II) ดังรูปที่ 2.13



รูปที่ 2.13 วงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง

จากรูปที่ 2.13 โครงสร้างวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง สามารถพิจารณาเป็นสมการผลต่างสืบเนื่องได้ดังสมการที่ (2.15)

$$y(n) = x(n) + c_1 y(n-1) + c_2 y(n-2) \tag{2.15}$$

และจากสมการผลต่างสืบเนื่องสามารถเขียนเป็นฟังก์ชันถ่ายโอนได้ดังสมการที่ (2.16) ถึงสมการที่ (2.18)

$$Y(z) = X(z) + c_1 Y(z) z^{-1} + c_2 Y(z) z^{-2} \tag{2.16}$$

$$Y(z)(1 - c_1 z^{-1} - c_2 z^{-2}) = X(z) \tag{2.17}$$

$$H(z) = \frac{Y(z)}{X(z)} = \frac{1}{(1 - c_1 z^{-1} - c_2 z^{-2})} \tag{2.18}$$

จากฟังก์ชันถ่ายโอนของวงจรกรองสัญญาณลำดับที่สอง สามารถหาตำแหน่งของโพลได้ 2 ตัวดังสมการที่ (2.19) และ สมการที่ (2.20)

$$p_1 = \frac{c_1 + \sqrt{c_1^{\,2} + 4c_2}}{2} \tag{2.19}$$

$$p_2 = \frac{c_1 - \sqrt{c_1^{\,2} - 4c_2}}{2} \tag{2.20}$$

จากสมการที่ (2.19) แสดงถึงตำแหน่งโพลตัวที่หนึ่ง และสมการที่ (2.20) แสดงถึงตำแหน่งโพลตัวที่สอง ของวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง

ยกตัวอย่างวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง ที่มีค่าดังนี้

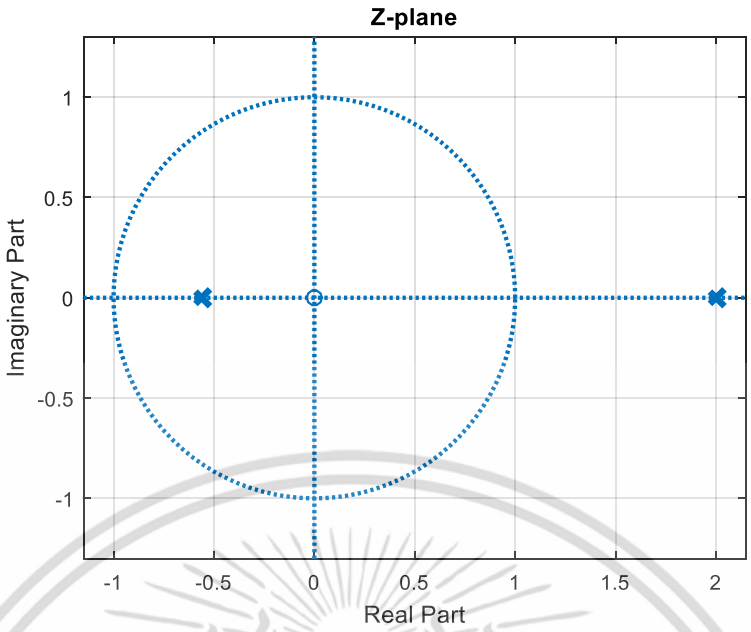
สัญญาณขาเข้า $x(n) = 0.5$

ค่าสัมประสิทธิ์วงจรกรองสัญญาณ $C_1 = 3$ และ $C_2 = -2$

ค่าเริ่มต้น $y(1) = 0$ และ $y(2) = 0$

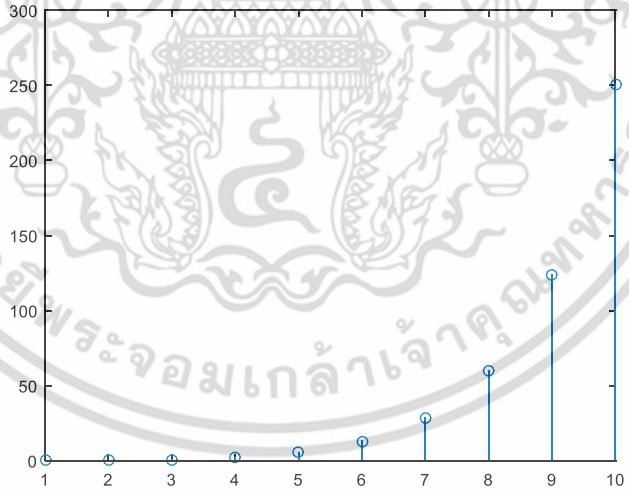
คำนวณหาตำแหน่งโพลได้ดังนี้ $p_1 = \frac{3 + \sqrt{3^2 + 4(-2)}}{2} = 2$ และ $p_2 = \frac{3 - \sqrt{3^2 - 4(-2)}}{2} =$ -0.5616

สามารถแสดงตำแหน่งโพลทั้งสองบนระนาบ z-plane ได้ดังรูปที่ 2.14



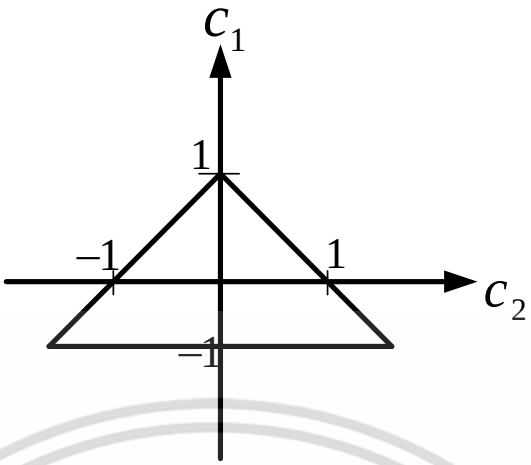
รูปที่ 2.14 ตำแหน่งของโพลบนระนาบ z-plane

จากรูปที่ 2.14 ตำแหน่งของโพลบนระนาบ z-plane ตำแหน่งของโพลตัวที่หนึ่ง คือ 2 ตำแหน่งของโพลตัวที่สอง คือ -0.5616 และแสดงสัญญาณขาออก $y(n)$ ได้ดังรูปที่ 2.15



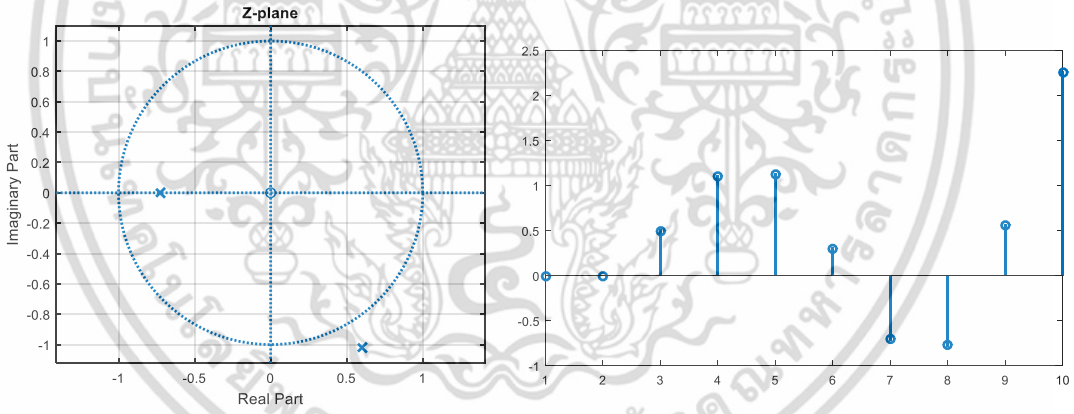
รูปที่ 2.15 สัญญาณขาออกของระบบที่ไร้เสถียรภาพ

จากรูปที่ 2.15 สัญญาณขาออกของระบบที่ไร้เสถียรภาพในกรณีที่ ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง มีค่าเป็น $C_1 = 3$ และ $C_2 = -2$ แสดงให้ว่าระบบมีความไร้เสถียรภาพ จากเงื่อนไขการเกิดความไร้เสถียรภาพนี้ ค่าสัมประสิทธิ์วงจรกรองสัญญาณจะต้องมีอย่างน้อยหนึ่งตัวอยู่ภายนอกสามเหลี่ยมเสถียรภาพดังรูปที่ 2.16



รูปที่ 2.16 สามเหลี่ยมเสถียรภาพ

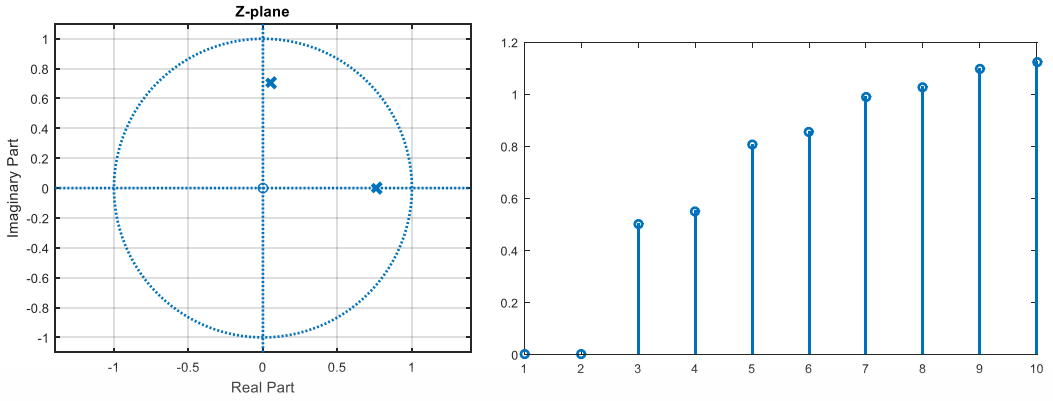
ยกตัวอย่างเช่น กรณีที่ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล มีค่าที่อยู่นอกสามเหลี่ยมเสถียรภาพทั้ง 2 ตัว $C_1 = 1.2$ และ $C_2 = -1.4$ แสดงได้ดังรูปที่ 2.17



(ก) (ข)

รูปที่ 2.17 ตำแหน่งของโพลบนระนาบ z-plane และสัญญาณขาออกของระบบกรณีที่ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล มีค่าที่อยู่นอกสามเหลี่ยมเสถียรภาพทั้ง 2 ตัว (ก) ตำแหน่งของโพลบนระนาบ z-plane (ข) สัญญาณขาออกของระบบที่ไร้เสถียรภาพ

กรณีที่ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล มีค่าที่อยู่ในสามเหลี่ยมเสถียรภาพทั้ง 2 ตัว $C_1 = 0.1$ และ $C_2 = 0.5$ แสดงได้ดังรูปที่ 2.18



(ก) (ข)

รูปที่ 2.18 ตำแหน่งของโพลบนระนาบ z-plane และสัญญาณขาออกของระบบกรณีที่ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล มีค่าที่อยู่ในสามเหลี่ยมเสถียรภาพทั้ง 2 ตัว (ก) ตำแหน่งของโพลบนระนาบ z-plane (ข) สัญญาณขาออกของระบบที่มีเสถียรภาพ

2.3.2.2 ความไม่เป็นเชิงเส้นของระบบ

ความไม่เป็นเชิงเส้นสามารถเกิดขึ้นจากความคลาดเคลื่อนจากการล้นในการคำนวณ การล้นในการคำนวณ (Overflow) คือ เหตุการณ์ที่ผลลัพธ์ของการประมวลผลมีค่าเกินช่วงที่จะสามารถแทนค่าได้ ที่เกิดจากผลลัพธ์ของการบวกของระบบตัวเลขที่มีตำแหน่งจุดทศนิยมคงที่ (Fixed Point) ในระบบจำนวนโดยตรง จุดทวินิยมเลขฐานสอง (Binary point) ที่แบ่งระหว่างจำนวนเต็ม (integer) และจำนวนทศนิยม (fraction) จะถูกจำกัดให้คงที่ โดยบิตแรกจะเรียกว่า (sign bit) ใช้ในการแสดงเครื่องหมายของตัวเลขโดยถ้าเป็นเครื่องหมายบวกจะแทนด้วย 0 และถ้าเป็นเครื่องหมายลบจะแทนด้วย 1 ซึ่งขนาดของตัวเลขจะแสดงในรูปแบบเลขยกกำลังของเลข 2 โดยหน้าจุดทศนิยมจะมีกำลังเป็นบวกรวมกำลัง 0 ด้วย และหลังจุดทศนิยมจะมีกำลังเป็นลบดังตัวอย่างการหาค่าจำนวนเต็มของเลขฐานสอง 01.101_2 ดังสมการที่ (2.21)

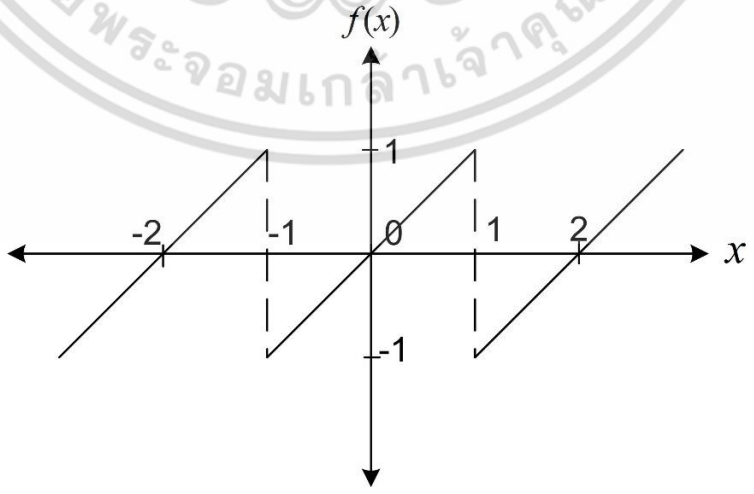
$$01.101_2 = (0\times 2^1)+(1\times 2^0)+(1\times 2^{-1})+(0\times 2^{-2})+(1\times 2^{-3}) = 1.625_{10} \qquad (2.21)$$

ความเที่ยงตรงของระบบตัวเลขจะถูกกำหนดโดยบิตที่อยู่ขวาสุดหรือบิตนัยสำคัญต่ำสุด (Least significant bit) ส่วนขอบเขต (Range) ของระบบตัวเลขจะนิยามโดยช่วงระหว่างจำนวนลบมากที่สุดที่สามารถแสดงได้ ซึ่งจุดทศนิยมจะเป็นตัวกำหนดความเที่ยงตรงและขอบเขตของระบบตัวเลข เมื่อกำหนดจุดทศนิยมให้อยู่ทางขวาสุดรูปแบบบิตจะมีเพียงเลขจำนวนเต็มและไม่มีเลขทศนิยม อีกรูปแบบที่แสดงตัวเลขของระบบจำนวนโดยตรง คือส่วนเติมเต็มสอง (2's Complement)

เมื่อนำระบบจำนวนโดยตรงมาใช้แทนค่าสัญญาณหรือนำมาประมวลผลของวงจรกรองสัญญาณดิจิตอลจะมีความคลาดเคลื่อนเกิดขึ้น โดยจะยกตัวอย่างเช่นการแปลงเลขฐานสิบไปเป็นเลขฐานสองของจำนวนลบมาอธิบาย ซึ่งเลขจำนวนลบที่จะทำการแปลงได้แก่ -6.86_{10} เมื่อทำการแปลงขนาดของเลขฐานสิบไปเป็นเลขฐานสองได้คือ $-6.86_{10} = 0110.1110_2$ (เท่ากับ -6.875_{10}) ซึ่งจะเห็นได้ว่าค่าที่ได้ออกมานั้นมีความคลาดเคลื่อนจากเดิม โดยความคลาดเคลื่อนที่เกิดขึ้นอาจเกิดจากความผิดพลาดจากการจัดระดับสัญญาณ (Quantization error) หรือความคลาดเคลื่อนที่เกิดจากการล้น (Overflow)

ความคลาดเคลื่อนจากการล้น หมายถึงผลลัพธ์ที่ได้จากการประมวลผล ที่มีค่ามากเกินกว่าขอบเขตที่สามารถแทนค่าในระบบจำนวนตรงได้ การล้นที่เกิดจากการบวกโดยจะพิจารณาการล้นที่เกิดกับผลลัพธ์ของการบวกเลขในส่วนเติมเต็มสอง ซึ่งตัวอย่างของการเกิดการล้นมีดังนี้ ให้ตัวตั้งเป็น 0100 (เท่ากับ 4) และตัวบวก 0100 เช่นกัน ซึ่งเมื่อบวกกันควรได้ผลลัพธ์เป็น 8 จึงจะถูกต้องแต่ผลลัพธ์ที่ได้ไม่สามารถแทนค่าได้ในขอบเขตระหว่าง -8 ถึง 7 ดังนั้นการล้นจึงเกิดขึ้น ซึ่งผลลัพธ์ที่ได้จากการเกิดการล้น คือ 1000 ซึ่งมีค่าเท่ากับ -8

จากการเกิดการล้นแบบส่วนเติมเต็มสอง สามารถนำมาพล็อตเป็นกราฟได้ดังรูปที่ 2.19 ซึ่งเป็นกราฟแสดงค่าที่เกิดจากการบวกเลขฐานสอง 8 บิต โดยแกนนอนแสดงค่าที่ถูกต้องที่เกิดจากการบวก ส่วนแกนตั้งแสดงค่าที่เกิดจากการล้น ซึ่งทั้งสองแกนได้แปลงเป็นเลขฐานสิบ จากกราฟจะเห็นได้ว่าการล้นแบบส่วนเติมเต็มสองจะทำให้ผลลัพธ์ที่ได้เปลี่ยนไปมากดังนั้นเมื่อเกิดการล้นจากวงจรกรองสัญญาณดิจิตอลจะได้ผลลัพธ์ที่ผิดไปอย่างมาก



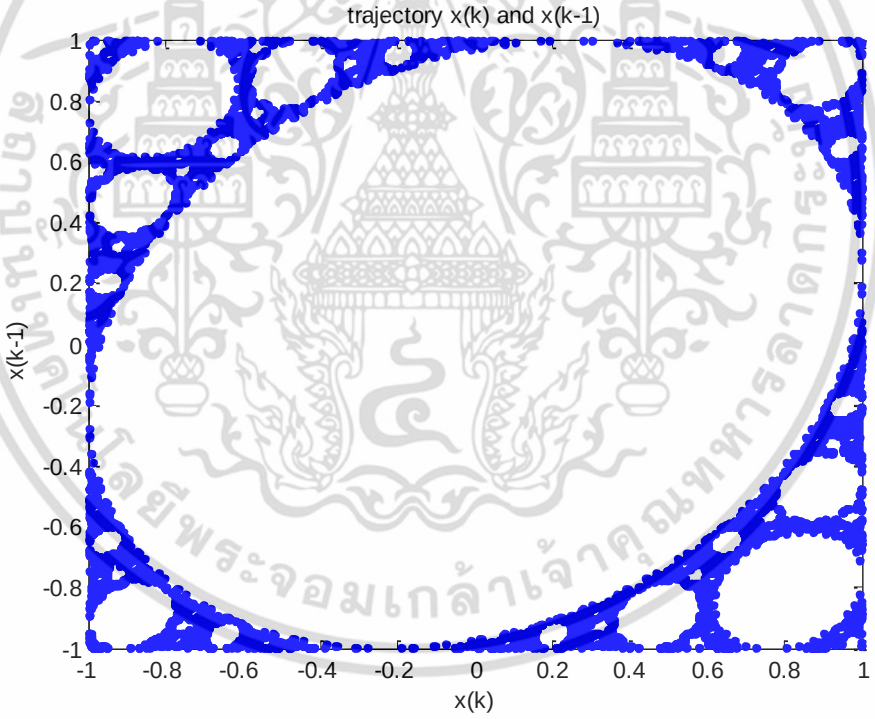
รูปที่ 2.19 การล้นของการบวกเลขส่วนเติมเต็มสอง

จากรูปที่ 2.19 จะเห็นได้ว่าเคออสนั้นเป็นระบบที่ไม่เป็นเชิงเส้น ซึ่งในการจำลองการล้นของระบบบนโปรแกรม MATLAB สามารถทำได้ด้วยการใช้ฟังก์ชันมอดูโลดังสมการที่ (2.22)

$$f(x) = ((x+1) \bmod 2) - 1 \tag{2.22}$$

2.3.3 พฤติกรรมเคออสในวงจรกรองสัญญาณดิจิตอล

พฤติกรรมเคออสในวงจรกรองสัญญาณดิจิตอล สามารถแสดงได้จากเส้นทางการเคลื่อนที่ (Trajectory) โดยการพล็อตค่า สัญญาณขาออกอันดับที่หนึ่ง (Output feedback first order) ของวงจรกรองสัญญาณ เทียบกับค่า สัญญาณขาออกอันดับที่สอง (Output feedback second order) ของวงจรเดียวกัน ซึ่งได้ดังรูปที่ 2.20



รูปที่ 2.20 เส้นทางเคลื่อนที่ 1000 จุด

จากรูปที่ 2.20 เส้นทางเคลื่อนที่ 1000 จุดเกิดแบบภาพในลักษณะภาพใหญ่และภาพย่อยที่ลักษณะเหมือนกันหรือคล้ายกันมาก หรือที่เรียกว่า ความคล้ายตัวเอง (Self-similarity) ซึ่งเป็นพฤติกรรมของเคออส

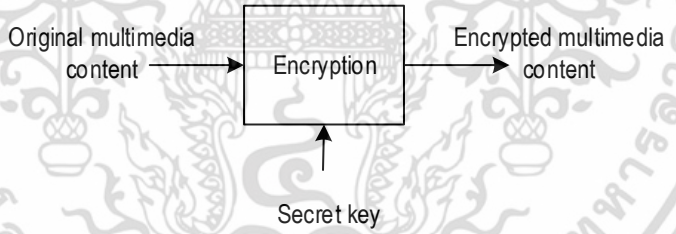
บทที่ 3

การออกแบบและการคำนวณ

ในบทนี้จะกล่าวถึงการออกแบบโครงสร้างระบบเข้ารหัสลับเนื้อหาสื่อประสมทั้งรูปภาพดิจิตอล เสียง และข้อความ (Multimedia content encryption) โดยจะสร้างกุญแจลับจากการเกิดปรากฏการณ์เคออสในวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง (Chaos in digital) รวมถึงการวัดประสิทธิภาพของระบบเข้ารหัสลับในรูปแบบต่างๆ ที่มีผลต่อประสิทธิภาพระบบเข้ารหัสลับ

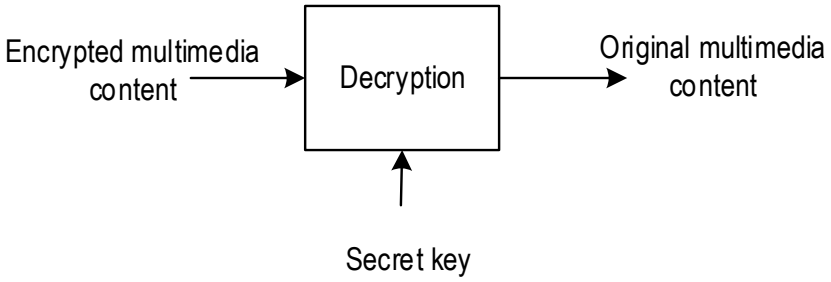
3.1 การออกแบบโครงสร้างเข้ารหัสลับและถอดรหัสลับสื่อประสม

โครงสร้างการเข้ารหัสลับสื่อประสม จะมีลักษณะดังรูปที่ 3.1 โดยข้อมูลต้นฉบับ (Plaintext) จะเป็นข้อมูลสื่อประสม เช่น ข้อความ รูปภาพดิจิตอล และเสียง โดยที่ข้อมูลลับที่ได้จากกระบวนการเข้ารหัสลับหรือที่เรียกว่าข้อมูลลับ (Cipher) ยังคงเป็นไฟล์คอมพิวเตอร์สื่อประสมชนิดเดียวกันกับต้นฉบับจะแตกต่างเฉพาะเนื้อหาสื่อประสมเท่านั้น



รูปที่ 3.1 โครงสร้างการเข้ารหัสลับสื่อประสม

จากรูปที่ 3.1 โครงสร้างการเข้ารหัสลับสื่อประสม จะประกอบไปด้วยเนื้อหาต้นฉบับ (Original multimedia content) เป็นข้อมูลขาเข้าของระบบเข้ารหัสลับซึ่งในระบบจะถูกออกแบบตามอัลกอริทึมที่ผู้ออกแบบได้ออกแบบไว้ (Encryption algorithm) และกุญแจลับ (Secret key) โดยข้อมูลขาออกของระบบเข้ารหัสลับจะเป็นเนื้อหาสื่อประสมที่เข้ารหัสลับแล้ว (Encrypted multimedia content) หรือที่เรียกว่า ข้อมูลลับ (cipher)

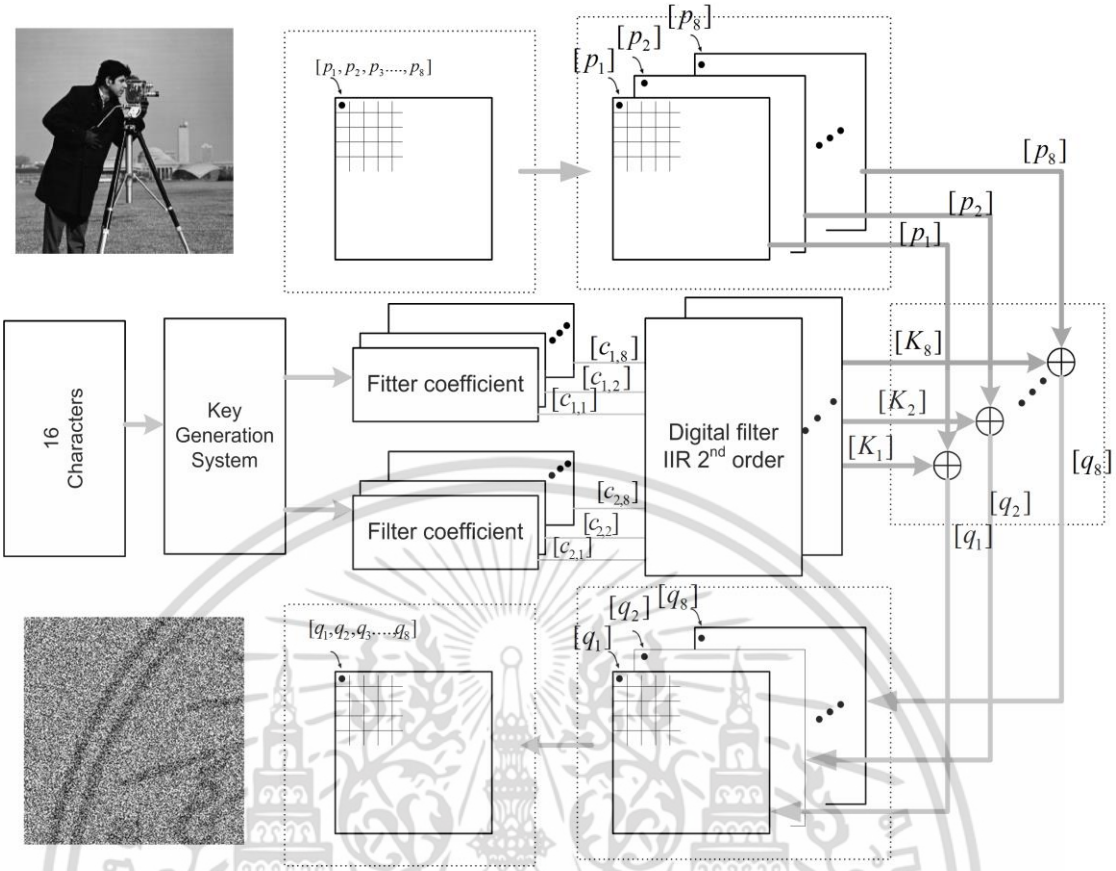


รูปที่ 3.2 โครงสร้างการถอดรหัสลับสื่อประสม

จากรูป 3.2 แสดงโครงสร้างการถอดรหัสลับสื่อประสม จะเห็นได้ว่าส่วนเข้ารหัสลับและถอดรหัสลับจะต้องมีกุญแจลับที่เหมือนกันตามหลักการเข้ารหัสแบบกุญแจส่วนตัวใช้ในการเข้ารหัสลับและถอดรหัสลับ ข้อมูลขาเข้าของระบบถอดรหัสลับจะเป็นข้อมูลลับ และข้อมูลขาออกของระบบถอดรหัสลับจะเป็นเนื้อหาสื่อประสมต้นฉบับ

ในงานวิจัยนี้ได้ออกแบบโครงสร้างระบบเข้ารหัสลับเป็นโครงสร้างเข้ารหัสลับแบบบล็อคร่วมกับกุญแจสมมาตร โครงสร้างภายในของระบบเข้ารหัสลับและถอดรหัสลับเหมือนกัน ในการส่งข้อมูลสื่อประสมผ่านช่องสัญญาณสื่อสารต่างๆ ให้ผู้รับข้อมูลปลายทางจะต้องมีกุญแจที่เหมือนกับผู้ส่งข้อมูลลับเพื่อใช้ในการถอดรหัสลับให้สามารถได้ข้อมูลต้นฉบับกลับคืนมา

ในการออกแบบและคำนวณจะใช้ข้อมูลต้นฉบับสื่อประสม สามชนิดข้อมูลคือ ข้อความ รูปภาพดิจิตอล และเสียง ทั้งสามชนิดข้อมูลนี้ รูปภาพดิจิตอลมีความทนทานต่อการโจมตีน้อยที่สุด เพราะค่าพิกเซลของรูปภาพดิจิตอลในบริเวณใกล้เคียง (Neighbors of Pixel) มีค่าใกล้เคียงกันมาก ทำให้ในบางกรณีที่รูปภาพดิจิตอลถูกโจรกรรมแล้วพยายามถอดรหัสโดยแฮกเกอร์ทำได้ง่ายขึ้น โครงสร้างการออกแบบเข้ารหัสลับรูปภาพดิจิตอลแสดงได้ดังรูปที่ 3.3 และโครงสร้างการออกแบบเข้ารหัสลับข้อความและเสียงแสดงได้ดังรูปที่ 3.4



รูปที่ 3.3 โครงสร้างระบบเข้ารหัสลับรูปภาพดิจิตอลที่นำเสนอ

p_i คือ ข้อมูลรูปภาพดิจิตอลต้นฉบับ

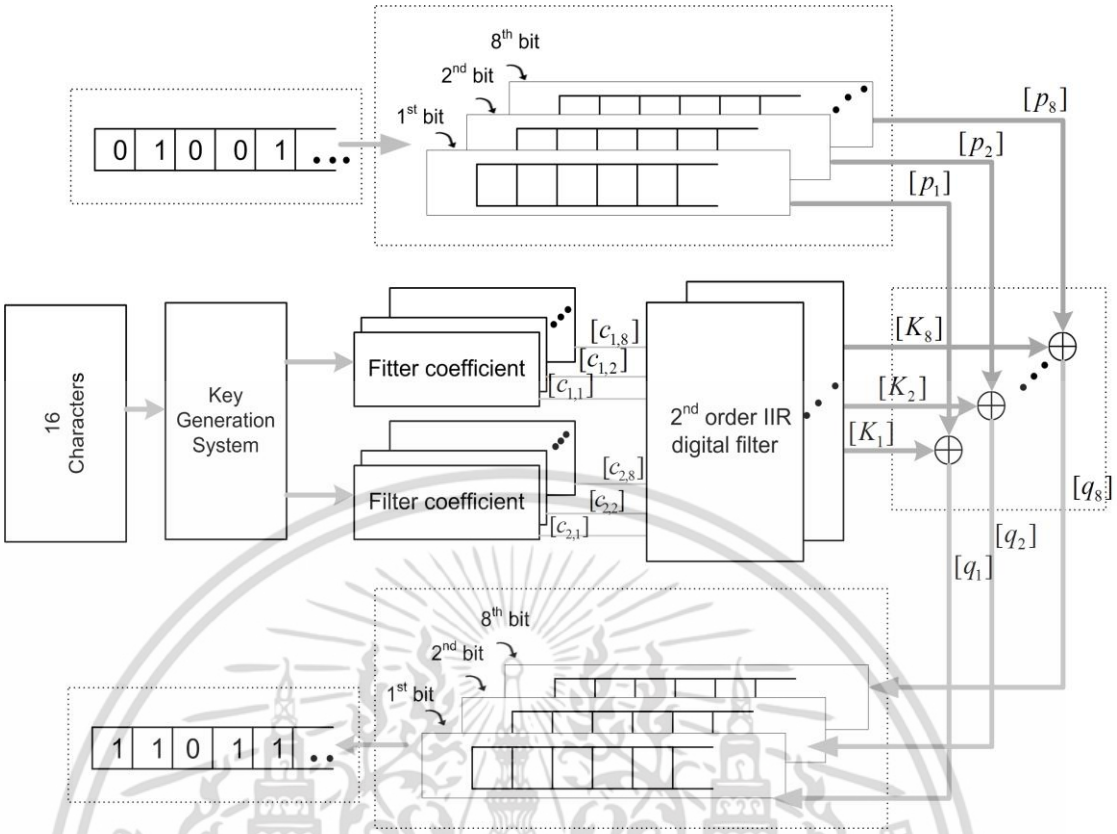
q_i คือ ข้อมูลรูปภาพดิจิตอลต้นลับ

K_i คือ กุญแจลับ

$C_{1,i}$ คือ ค่าสัมประสิทธิ์ของวงจรกรองสัญญาณดิจิตอลตัวที่ 1

$C_{2,i}$ คือ ค่าสัมประสิทธิ์ของวงจรกรองสัญญาณดิจิตอลตัวที่ 2

$i = 1,2,3,...8$

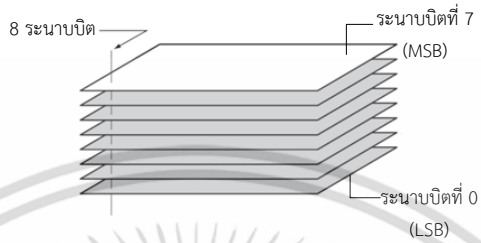


รูปที่ 3.4 โครงสร้างการออกแบบเข้ารหัสข้อความและเสียงที่นำเสนอ

จากรูปที่ 3.4 ซึ่งเป็นระบบเข้ารหัสลับเนื้อหาสื่อประสมชนิด 1 มิติ ได้แก่ข้อความและเสียง จะเห็นได้ว่าการเข้ารหัสลับเนื้อหาสื่อประสมทั้งรูปภาพดิจิตอล ข้อความ และเสียง จะประกอบด้วยส่วนของการเตรียมข้อมูลต้นฉบับอยู่ในระนาบบิต p_i ต่อมาคือกระบวนการสร้างกุญแจลับให้อยู่ในระนาบบิต K_i และสุดท้ายกระบวนการสร้างข้อมูลลับด้วยการดำเนินการทางลอจิกด้วย XOR ระหว่างระนาบบิตข้อมูลต้นฉบับกับระนาบบิตกุญแจลับ q_i แล้วรวมกันทุกระนาบบิตให้ได้ข้อมูลลับออกมา

3.2 ประเภทของข้อมูลต้นฉบับ

ในการออกแบบและคำนวณจะใช้ข้อมูลต้นฉบับสื่อประสมทั้งสามชนิดข้อมูลคือ ข้อความ รูปภาพดิจิตอล และเสียง (Original multimedia content) โดยส่วนการออกแบบให้ข้อมูลต้นฉบับอยู่ในระนาบบิตทั้งหมด 8 ระนาบบิต (bit-plane slicing) ดังรูปที่ 3.5



รูปที่ 3.5 การแยกระนาบบิต 8 ระนาบบิต

จากรูปที่ 3.5 เป็นการแยกระนาบบิต 8 บิต ออกมาได้ทั้งหมด 8 ระนาบบิต ระนาบที่ 7 เป็นระนาบที่มีนัยสำคัญสุด และระนาบที่ 0 เป็นระนาบที่มีนัยสำคัญน้อยสุด ระนาบบิตของข้อมูลรูปภาพเป็น 2 มิติ ส่วนเสียงและข้อความเป็น 1 มิติ ได้อธิบายดังต่อไปนี้

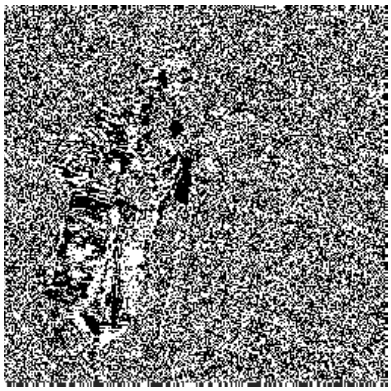
3.2.1 ข้อมูลชนิดรูปภาพดิจิตอล

ข้อมูลชนิดรูปภาพดิจิตอลได้เลือกใช้รูปภาพดิจิตอลสีเทา (gray scale) ขนาด 256x256 พิกเซล เพื่อใช้ในการทดสอบระบบเข้ารหัสลับที่นำเสนอ แสดงรูปภาพดิจิตอลต้นฉบับดังรูปที่ 3.6

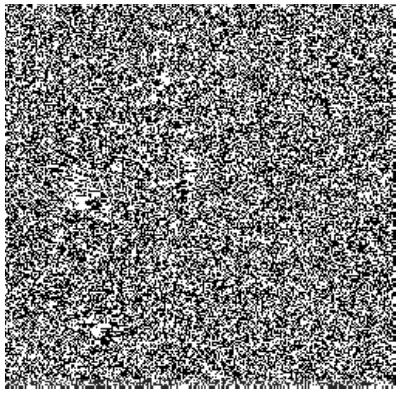
รูปที่ 3.6 ข้อมูลชนิดรูปภาพดิจิตอล Cameraman

จากรูปที่ 3.6 เป็นรูปภาพดิจิตอลที่ใช้ในการออกแบบและคำนวณเป็นชนิดสีเทา 8 บิต สามารถทำให้อยู่ในระนาบบิต เพื่อเตรียมข้อมูลต้นฉบับในรูปแบบระนาบบิตได้ดังรูปที่ 3.7 จะได้ทั้งหมด 8 ระนาบบิต

รูปที่ 3.7 ระนาบบิตของรูปภาพต้นฉบับทั้ง 8 ระนาบบิต



(ช)



(ซ)

รูปที่ 3.7 (ต่อ) ระนาบบิตของรูปภาพต้นฉบับทั้ง 8 ระนาบบิต (ก) ระนาบบิตที่ 7 (ข) ระนาบบิตที่ 6 (ค) ระนาบบิตที่ 5 (ง) ระนาบบิตที่ 4 (จ) ระนาบบิตที่ 3 (ฉ) ระนาบบิตที่ 2 (ช) ระนาบบิตที่ 1 (ซ) ระนาบบิตที่ 0

ข้อมูลต้นฉบับรูปภาพดิจิตอลเป็นข้อมูลต้นฉบับที่ใช้ในการทดลองเป็นรูปภาพดิจิตอลสีเทา Cameraman ขนาด 256x256 พิกเซล จากรูปที่ 3.7 เป็นระนาบบิตที่เกิดจากรูปภาพดิจิตอลสีเทาทั้งหมด 8 ระนาบบิต 1 บิต ต่อ 1 พิกเซล

3.2.2 ข้อความ

ข้อมูลชนิดข้อความจะมีเนื้อหาอักขระข้อความที่สามารถเข้าใจได้ โดยอักขระข้อความที่ใช้ในการทดลองจะอยู่ภายใต้มาตรฐานผลิตภัณฑ์อุตสาหกรรม 620-2533 หรือที่รู้จักกันทั่วไปว่า TIS-620 เป็นชุดอักขระมาตรฐานอุตสาหกรรมของไทย มีชื่อเต็มว่า รหัสสำหรับอักขระไทยที่ใช้กับคอมพิวเตอร์ ยกตัวอย่างเช่นอักษระคำว่า “ทดสอบ” แสดงค่าในมุมมองเลขฐานสิบหก เลขฐานสิบ และเลขฐานสองดังตารางที่ 3.1

ตารางที่ 3.1 ตัวอย่างการแปลงค่าอักขระเป็นเลขฐานสิบหก เลขฐานสิบ และเลขฐานสอง โดยใช้รหัสสำหรับอักขระไทยที่ใช้กับคอมพิวเตอร์ (TIS-620)

มุมมอง	ท	ด	ส	อ	บ
เลขฐานสิบหก	0xB8	0xB4	0xCA	0xCD	0xBB
เลขฐานสิบ	184	180	202	205	187
เลขฐานสอง	10111000	10110100	11001010	11001101	10111011

จากตารางที่ 3.1 แสดงตัวอย่างการแปลงค่าอักขระเป็นเลขฐานสิบหก เลขฐานสิบ และเลขฐานสอง โดยใช้รหัสสำหรับอักขระไทยที่ใช้กับคอมพิวเตอร์ (TIS-620) หนึ่งอักขระ แทนได้ 8 บิต ดังนั้นสามารถสร้างข้อมูลมาได้ 8 ชุด โดยแต่ละชุดเกิดจากการรวมกันของบิต แสดงได้ดังตาราง 3.2

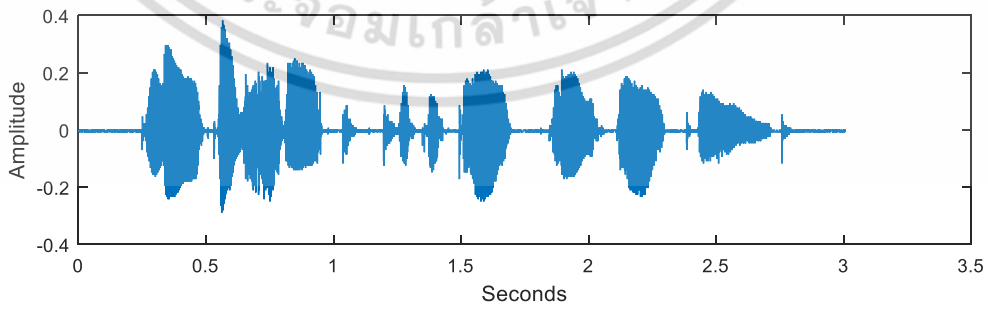
ตารางที่ 3.2 ข้อมูลต้นฉบับข้อความ คำว่า “ทดสอบ” ในระนาบบิตทั้งหมด 8 ระนาบบิต

อันดับของระนาบบิต	ค่าประจำตำแหน่งบิต				
	1	2	3	4	5
ข้อมูลต้นฉบับระนาบที่ 1	1	1	1	1	1
ข้อมูลต้นฉบับระนาบที่ 2	0	0	1	1	0
ข้อมูลต้นฉบับระนาบที่ 3	1	1	0	0	1
ข้อมูลต้นฉบับระนาบที่ 4	1	1	0	0	1
ข้อมูลต้นฉบับระนาบที่ 5	1	0	1	1	1
ข้อมูลต้นฉบับระนาบที่ 6	0	1	0	1	0
ข้อมูลต้นฉบับระนาบที่ 7	0	0	1	0	1
ข้อมูลต้นฉบับระนาบที่ 8	0	0	0	1	1

จากตารางที่ 3.2 แสดงให้เห็นถึงค่าของ คำว่า “ทดสอบ” มีการจัดเรียงข้อมูลต้นฉบับทั้งหมด 8 ระนาบบิต แต่ละระนาบมีขนาด 1 มิติ

3.2.3 ข้อมูลชนิดเสียง

ข้อมูลชนิดเสียงที่ใช้ในทดลองเป็นไฟล์เสียงชนิด WAVE (.wav) ขนาดความยาวประมาณสามนาที ไม่มีการบีบอัด แสดงขนาดแอมพลิจูดได้ดังรูปที่ 3.8

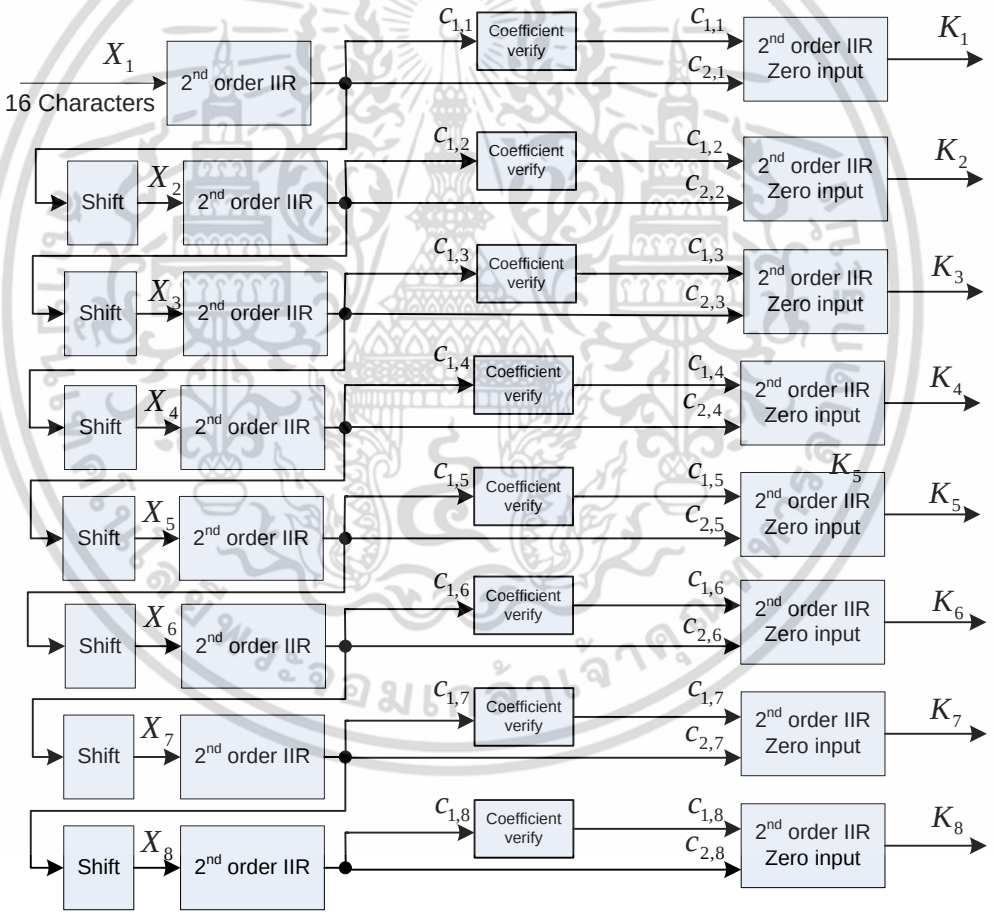


รูปที่ 3.8 ขนาดแอมพลิจูดข้อมูลต้นฉบับชนิดเสียง

จากรูปที่ 3.8 แสดงขนาดแอมพลิจูดข้อมูลต้นฉบับข้อมูลชนิดเสียง ข้อมูลต้นฉบับเสียงนี้มีจำนวนบิตต่อแซมเปิ้ลคือ 8 ไฟล์เสียงชนิด WAVE (.wav) ดังนั้นสามารถแบ่งเป็นระนาบบิตได้ทั้งหมด 8 ระนาบบิตเช่นเดียวกับข้อมูลข้อความ

3.3 การออกแบบส่วนกุญแจลับ

ในส่วนการออกแบบกุญแจลับ กุญแจลับเป็นแบบสมมาตรตามที่กล่าวมาก่อนหน้านี้คือกุญแจลับของระบบเข้ารหัสลับและถอดรหัสลับเป็นดอกเดียวกันเหมือนกันทุกประการ หรือที่เรียกว่ากุญแจส่วนตัว ในระบบที่นำเสนอนี้ได้ออกแบบส่วนกุญแจลับโดยจะสร้างกุญแจมาทั้งหมด 8 ระนาบบิตซึ่งจะสอดคล้องกับข้อมูลต้นฉบับที่มี 8 ระนาบบิตเช่นเดียวกัน โดยแสดงโครงสร้างกระบวนการสร้างกุญแจลับดังรูปที่ 3.9

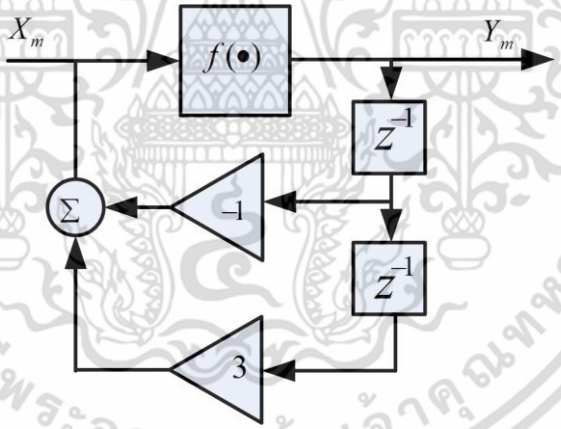


รูปที่ 3.9 โครงสร้างกระบวนการสร้างกุญแจลับจากอักขระ 16 ตัว

จากรูปที่ 3.9 จะประกอบด้วย 3 ส่วนย่อย โดยส่วนที่ 1 คือ ส่วนสร้างกุญแจจากอักขระ (Key generation system) แทนค่าด้วย $X_1, X_2, X_3, ..., X_8$ คือสัญญาณขาเข้าของวงจรกรองสัญญาณดิจิตอล เพื่อสร้างสัญญาณขาออก c_1 และ c_2 ส่วนต่อมาคือส่วนตรวจสอบและแก้ไขค่าสัมประสิทธิ์ (Filter coefficient verification) จะตรวจสอบ c_1 ให้อยู่ในเงื่อนไขที่จะทำให้วงจรเกิดความไร้เสถียรภาพ และส่วนสุดท้ายคือ สร้างระนาบบิตจากวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สอง (Key plane generation) แทนค่าด้วย $K_1, K_2, K_3, ..., K_8$ ในแต่ละขั้นตอนได้อธิบายรายละเอียดดังต่อไปนี้

3.3.1 สร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณ (Filter coefficient generation system)

ข้อมูลขาเข้า 16 ตัวอักขระ (ASCII) แปลงค่าให้รูปในรูปแบบจำนวนเต็มคงที่ (fixed point) 8 บิต แทนค่าด้วย X_m โดยที่ แทนค่าด้วย $m = 1,2,3,...8$ นำมาผ่านวงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 ที่มีค่าสัมประสิทธิ์วงจรกรองสัญญาณคือ -1 และ 3 ดังรูปที่ 3.10



รูปที่ 3.10 วงจรสร้างค่าสัมประสิทธิ์ให้วงจรกรองสัญญาณดิจิตอล IIR ลำดับที่สอง

จากรูปที่ 3.10 สัญญาณขาออก จะมีลักษณะเป็นเคออสตามทฤษฎีการเกิดเคออสในวงจรกรองสัญญาณดิจิตอลที เพราะมีค่าสัมประสิทธิ์อย่างน้อย 1 ตัวอยู่นอกสามเหลี่ยมเสถียรภาพ และเกิดการล้นการบวกของเลขเติมเต็มสอง ในการทดลองผ่านโปแกรม MATLAB ความคลาดเคลื่อนของการล้นจะไม่เกิดขึ้นจึงต้องใช้ $f(\bullet)$ ในการสร้างความผิดพลาดที่เกิดจากการล้น สัญญาณขาออกจะมีจำนวน 16 ตัว แทนด้วย $Y_1, Y_2, Y_3, ..., Y_{16}$ และพิจารณากำหนดให้ Y_{15} เป็น $c_{1,1}$ และ กำหนดให้ Y_{16} เป็น $c_{2,1}$ พร้อมทั้งยังนำข้อมูลขาออกทั้งหมดมาทำการเลื่อนตำแหน่ง 3 ตำแหน่งจากเดิม คือ $Y_1, Y_2, Y_3, ..., Y_{16}$ เป็น $Y_{14}, Y_{15}, Y_{16}, Y_1, Y_2, ..., Y_{13}$ เพื่อสร้างสัญญาณขาเข้าให้ระนาบบิตต่อไปทำซ้ำ

ทั้งหมด 8 ครั้งจะทำให้ได้ c_1 และ c_2 อย่างละ 8 ค่า ยกตัวอย่างเช่น 16 ตัวอักขระ (ASCII) มีค่า “ThasFD123%da@3fl” จะได้ค่า c_1 และ c_2 ดังตารางที่ 3.3

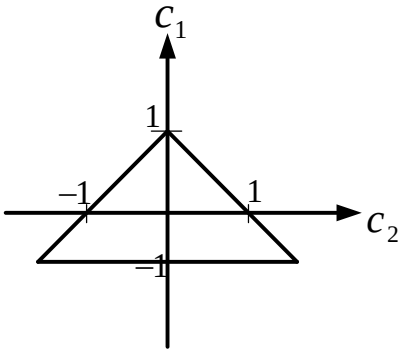
ตารางที่ 3.3 ผลลัพธ์การสร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2

อันดับระนาบบิต (m)	ค่าสัมประสิทธิ์วงจรกรองสัญญาณ $C_{1,m}$ โดยที่ $m = 1,2,3,...,8$	ค่าสัมประสิทธิ์วงจรกรองสัญญาณ $C_{2,m}$ โดยที่ $m = 1,2,3,...,8$
1	0.940937500012521	-0.603750000005443
2	-0.759375409300840	0.791875177911401
3	-0.849432613520205	-0.208940855152278
4	-0.410512175165469	-0.333814867709504
5	0.156795578691087	0.714520396338911
6	0.756845665768234	-0.892492958366694
7	0.127126532699603	0.345213875925721
8	-0.054168174082059	-0.456798520138300

จากตารางที่ 3.3 ผลลัพธ์การสร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล 16 ตัวอักขระ (ASCII) ที่มีค่า “ThasFD123%da@3fl” สามารถสร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล ได้ทั้งหมด 8 ชุด โดย 1 ชุดจะมี 2 ตัวแปร คือ c_1 และ c_2 เพื่อใช้ในวงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 ที่ประกอบไปด้วยค่าสัมประสิทธิ์ 2 ตัว จะเห็นได้ว่าค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลจะทำให้ระบบมีเสถียรภาพดังนั้นจึงต้องแก้ไขค่าสัมประสิทธิ์ให้อย่างน้อย 1 ตัวอยู่นอกสามเหลี่ยมเสถียรภาพ

3.3.2 ตรวจสอบและแก้ไขค่าสัมประสิทธิ์ (Filter coefficient verification)

หลังจากสร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 เรียบร้อยแล้วต่อมาคือการตรวจสอบและแก้ไขค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลนั้นให้เกิดความไม่มีเสถียรภาพ โดยการกำหนดให้ค่าสัมประสิทธิ์อย่างน้อยหนึ่งตัวอยู่ภายนอกสามเหลี่ยมเสถียรภาพดังรูปที่ 3.11



รูปที่ 3.11 สามเหลี่ยมเสถียรภาพ

จากรูปที่ 3.11 C_1 คือค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลตัวแรก และ C_2 คือค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลตัวที่ 2 โดยออกแบบฟังก์ชันการตรวจสอบค่า C_1 ถ้าในกรณีที่มีค่าอยู่ในช่วง -1 ถึง 1 จะเปลี่ยนเป็นค่าใหม่คือ $c_1^{-1} \times 10$ ซึ่งจะทำให้ C_1 มีค่าที่ไม่อยู่ในช่วง -1 ถึง 1 ส่วน C_2 จะไม่มีกระบวนการตรวจสอบค่า ดังนั้นจากผลลัพธ์ตารางที่ 3.3 สามารถหาค่า C_1 ใหม่ได้ดังตารางที่ 3.4

ตารางที่ 3.4 ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 โดยที่มี 1 ตัวอยู่ภายนอกสามเหลี่ยมเสถียรภาพ

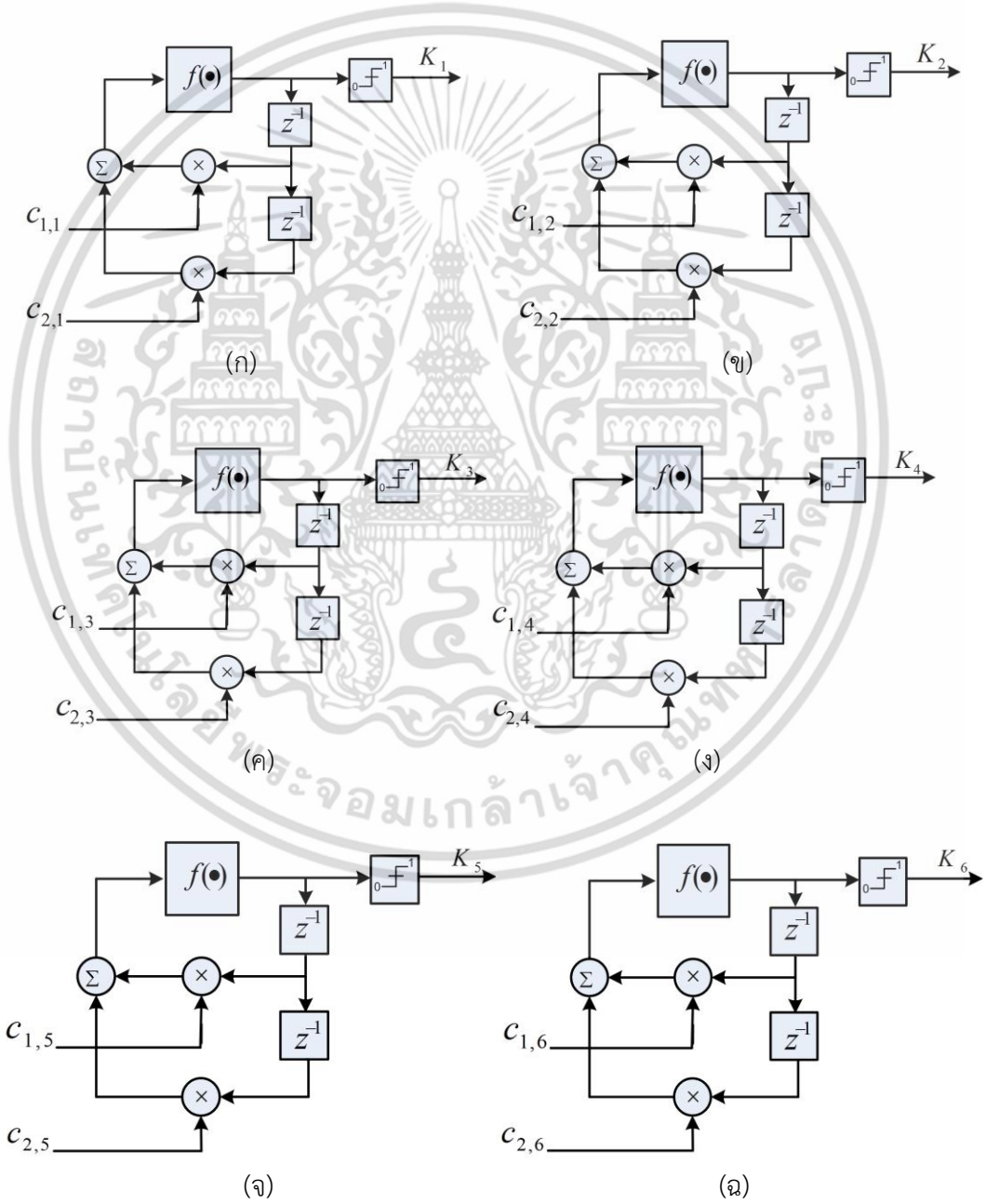
อันดับระนาบบิต (m)	ค่าสัมประสิทธิ์วงจรกรองสัญญาณ $C_{1,m}$ โดยที่ $m = 1,2,3,\ldots,8$	ค่าสัมประสิทธิ์วงจรกรองสัญญาณ $C_{2,m}$ โดยที่ $m = 1,2,3,\ldots,8$
1	10.627698438915374	-0.603750000005443
2	13.168717181936458	0.791875177911401
3	-11.772564227971134	-0.208940855152278
4	-24.3598134354217	-0.333814867709504
5	63.7773085407059	0.714520396338911
6	13.2127333910931	-0.892492958366694
7	78.6617851336336	0.345213875925721
8	-184.610247058559	-0.456798520138300

จากตารางที่ 3.4 จะเห็นได้ว่ามีค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 โดยมี 1 ตัวออกนอกสามเหลี่ยมเสถียรภาพนั่นคือ C_1 ไม่ได้อยู่ช่วง -1 ถึง 1 ซึ่งถ้านำค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลที่ได้จากตารางนี้ไปใช้ในวงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 จะทำให้

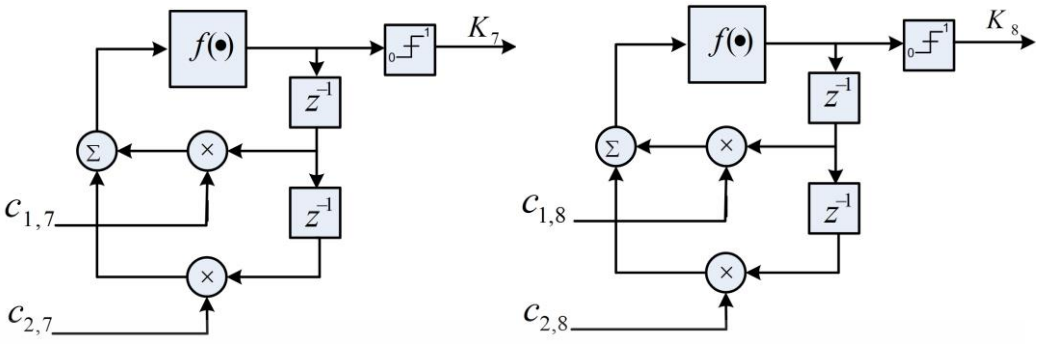
วงจรนั้นมีความไร้เสถียรภาพทันที ซึ่งได้นำไปใช้ในการสร้างระนาบบิตของกุญแจลับซึ่งจะอธิบายในหัวข้อถัดไป

3.3.3 สร้างระนาบบิตของกุญแจลับทั้งหมด 8 ระนาบบิต

ในส่วนนี้เป็นการสร้างระนาบบิตของกุญแจลับทั้งหมด 8 ระนาบ โดยใช้วงจรกรองสัญญาณดิจิตอล IIR อันดับที่ 2 เช่นเดียวกัน แต่จะมีคุณสมบัติของระบบคือไม่มีสัญญาณขาเข้า ส่วนสัญญาณขาออก มีค่าเป็นเลขฐานสอง ซึ่งจะใช้ทั้งหมด 8 วงจรกรองสัญญาณที่มีค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลแตกต่างกันตามที่ได้สร้างมาในส่วนก่อนหน้านี้ดังรูปที่ 3.12



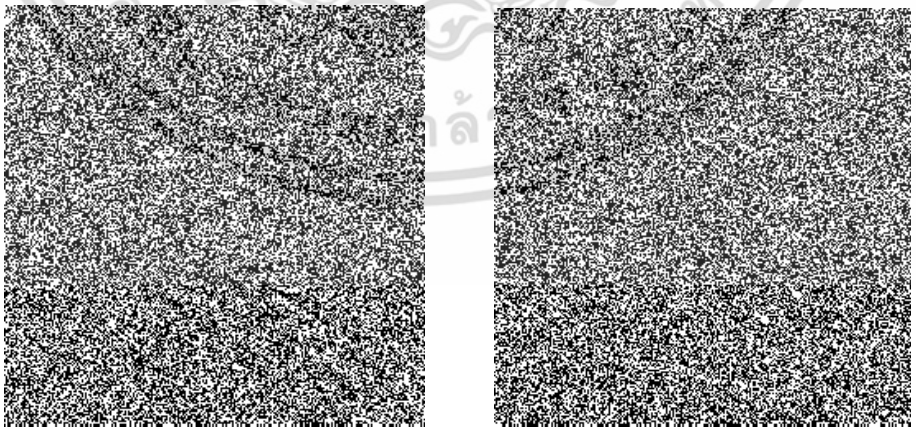
รูปที่ 3.12 วงจรกรองสัญญาณดิจิตอล IIR อันดับที่สองเพื่อสร้างกุญแจระนาบบิต



(ช) (ซ)

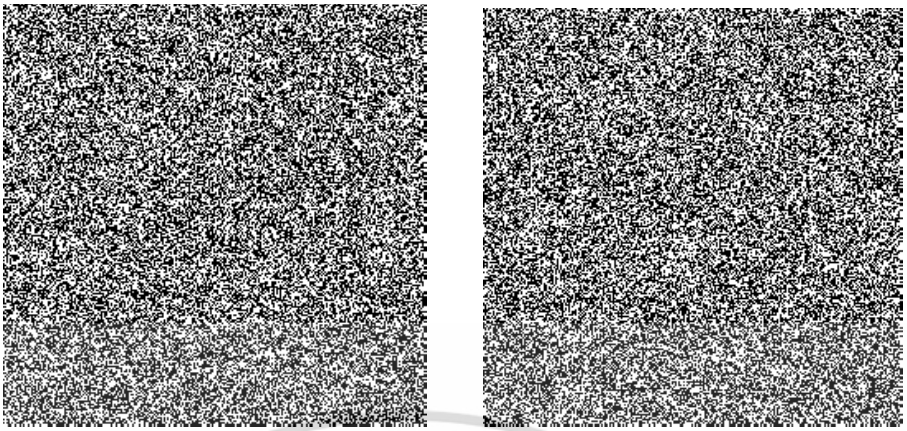
รูปที่ 3.12 (ต่อ) วงจรกรองสัญญาณดิจิตอล IIR อันดับที่สองเพื่อสร้างกุญแจระนาบบิต (ก) วงจรสร้างกุญแจระนาบบิตที่ 1 (ข) วงจรสร้างกุญแจระนาบบิตที่ 2 (ค) วงจรสร้างกุญแจระนาบบิตที่ 3 (ง) วงจรสร้างกุญแจระนาบบิตที่ 4 (จ) วงจรสร้างกุญแจระนาบบิตที่ 5 (ฉ) วงจรสร้างกุญแจระนาบบิตที่ 6 (ช) วงจรสร้างกุญแจระนาบบิตที่ 7 (ซ) วงจรสร้างกุญแจระนาบบิตที่ 8

จากรูปที่ 3.12 สัญญาณขาออกจากวงจรกรองสัญญาณที่ได้ออกแบบมานั้นผ่านกระบวนการปรับค่าให้เป็น 0 หรือ 1 เลขฐานสอง หรือเรียกว่ากุญแจระนาบบิต (Key plane) ซึ่งจะมีทั้งหมด 8 ระนาบบิตคือ $K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8$ โดยแต่ละระนาบบิตขึ้นอยู่กับค่าสัมประสิทธิ์วงจรกรองสัญญาณ C_1 และ C_2 กุญแจระนาบบิตของข้อมูลต้นฉบับรูปภาพดิจิตอลแสดงดังรูปที่ 3.13

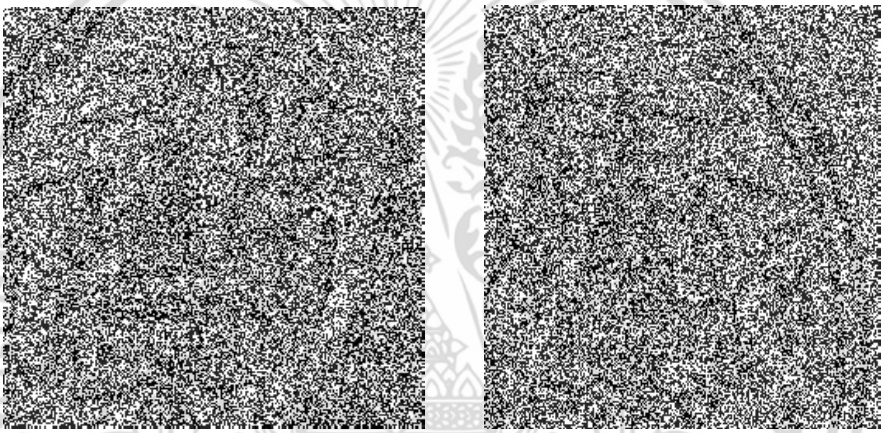


(ก) (ข)

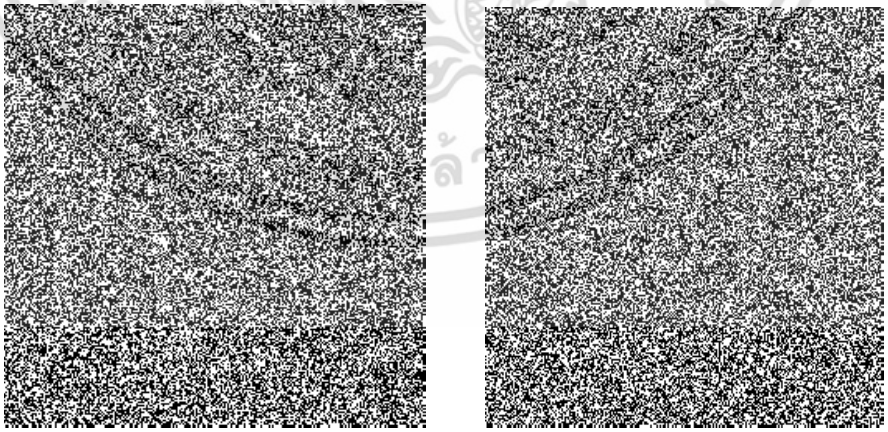
รูปที่ 3.13 กุญแจระนาบบิตทั้ง 8 ระนาบบิต



(ค) (ง)



(จ) (ฉ)



(ช) (ซ)

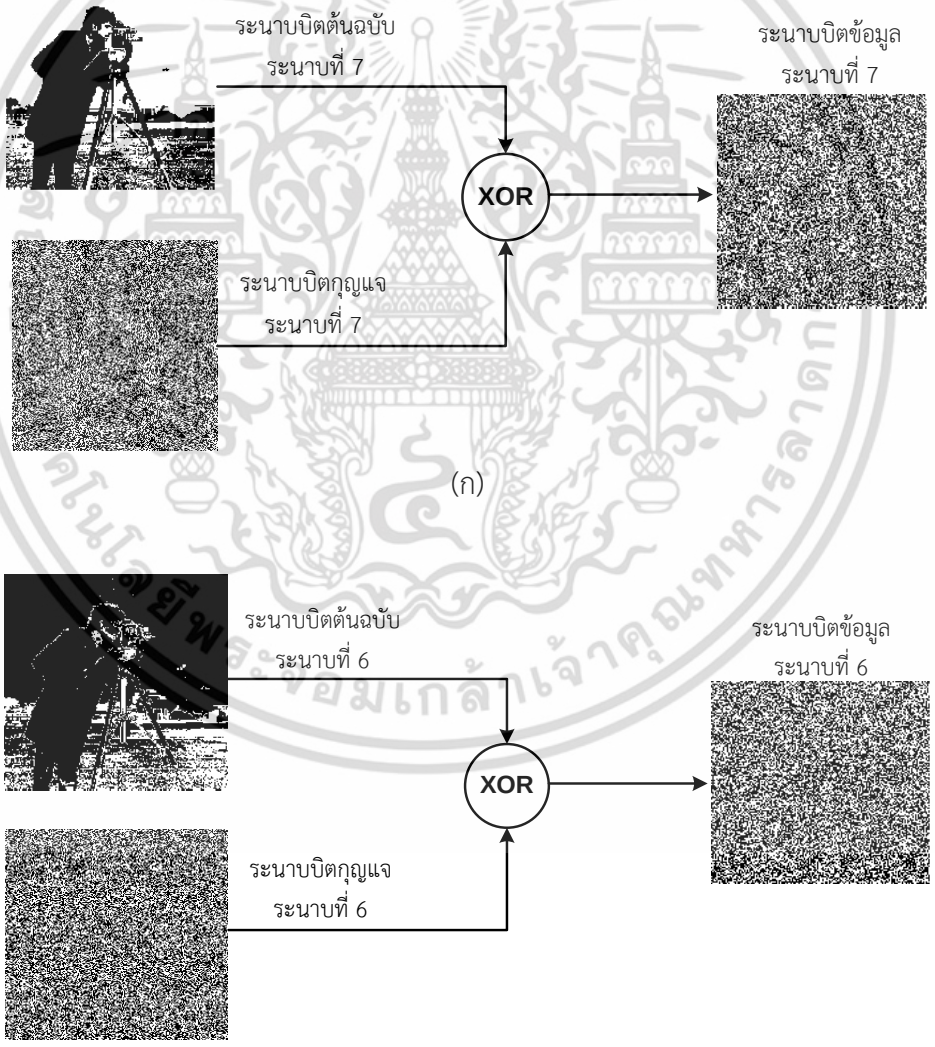
รูปที่ 3.13 (ต่อ) กุญแจระนาบบิตทั้ง 8 ระนาบบิต (ก) กุญแจระนาบบิตที่ 7 (ข) กุญแจระนาบบิตที่ 6 (ค) กุญแจระนาบบิตที่ 5 (ง) กุญแจระนาบบิตที่ 4 (จ) กุญแจระนาบบิตที่ 3 (ฉ) กุญแจระนาบบิตที่ 2 (ช) กุญแจระนาบบิตที่ 1 (ซ) กุญแจระนาบบิตที่ 0

จากรูปที่ 3.13 ได้แสดงถึงระนาบบิตของกุญแจข้อมูลรูปภาพดิจิตอลทั้งหมด 8 ระนาบบิต ซึ่งเป็นระนาบ 2 มิติ ที่เกิดจากระบบเข้ารหัสลับที่ได้นำเสนอ 1 พิกเซลมีค่า 1 บิต

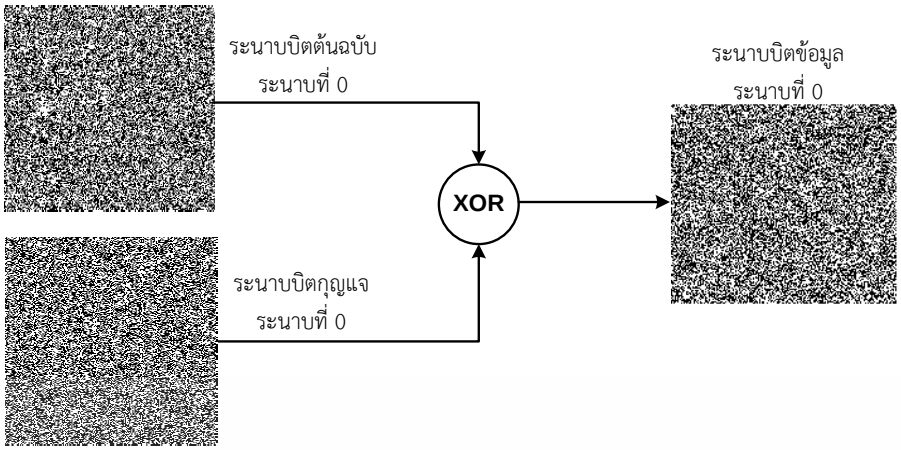
ส่วนระนาบกุญแจของข้อมูลข้อความ ก็จะมีทั้งหมด 8 ระนาบบิตเช่นเดียวกันแต่จะมีขนาด 1 มิติ มีความยาวเท่ากับจำนวนข้อความ

และระนาบกุญแจของข้อมูลเสียง จะมีทั้งหมด 8 ระนาบบิตเช่นเดียวกับข้อมูลรูปภาพดิจิตอลและมีขนาด 1 มิติ เหมือนข้อมูลข้อความ

หลังจากนั้นนำระนาบข้อมูลต้นฉบับและระนาบกุญแจทั้ง 8 ระนาบบิตมาดำเนินการทางลอจิกด้วย XOR เพื่อให้ได้อีกระนาบบิตคือ ระนาบบิตข้อมูลลับ (Cipher plane) ยกตัวอย่างเช่น ข้อมูลรูปภาพดิจิตอล ดังรูปที่ 3.14



รูปที่ 3.14 ขั้นตอนการดำเนินการทางลอจิกด้วย XOR



(ค)

รูปที่ 3.14 ขั้นตอนการดำเนินการทางลอจิกด้วย XOR (ก) ดำเนินการทางลอจิกด้วย XOR ระนาบบิตที่ 7 (ข) ดำเนินการทางลอจิกด้วย XOR ระนาบบิตที่ 6 (ค) ดำเนินการทางลอจิกด้วย XOR ระนาบบิตที่ 0

3.4 การวัดประสิทธิภาพของระบบเข้ารหัสลับ

การออกแบบระบบเข้ารหัสลับนั้นจำเป็นต้องมีการวัดประสิทธิภาพของระบบเข้ารหัสลับเพื่อให้ได้ระบบตามที่ต้องการ ในการออกแบบระบบเข้ารหัสลับใดก็ตาม จำเป็นต้องคำนึงถึงประสิทธิภาพของระบบด้วย ในงานวิจัยทางวิชาการมากมายได้สร้างตัวแปรขึ้นเพื่อใช้ในการออกแบบระบบเข้ารหัสลับ โดยได้เลือกใช้เนื้อหาสื่อประสมรูปภาพดิจิตอลเป็นหลักเนื่องจากสามารถบ่งชี้ประสิทธิภาพได้ชัดเจน อธิบายตัวแปรดังหัวข้อตามต่อไปนี้

3.4.1 ความไวของกุญแจ (Key Sensitivity)

ความไวของกุญแจ (Key Sensitivity) [14] คือ การเปลี่ยนแปลงของกุญแจเพียงเล็กน้อยมีผลทำให้ข้อมูลลับเปลี่ยนแปลงตาม ซึ่งคำนวณได้ดังสมการที่ (3.1)

$$KS = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} C_0(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} C_1(i,j)}{2 \times M \times N} \times 100\% \tag{3.1}$$

$$C_0 = E(P, K_0) \tag{3.2}$$

$$C_1 = E(P, K_1) \tag{3.3}$$

P คือ ข้อมูลต้นฉบับ

C_0 คือ ข้อมูลเข้ารหัสแล้วด้วยกุญแจแรก

C_1 คือ ข้อมูลที่เข้ารหัสแล้วด้วยกุญแจที่สอง

K_0 คือ กุญแจแรก

K_1 คือ กุญแจที่สอง

$E(\bullet)$ คือ ฟังก์ชันเข้ารหัสลับ

โดยให้ K_0 ต่างกับ K_1 เพียง 1 บิต ระบบเข้ารหัสข้อมูลลับที่ดีต้องมีค่า Key Sensitivity (KS) มากกว่า 50 เปอร์เซ็นต์

3.4.2 ความไวของข้อมูลต้นฉบับ (Plaintext Sensitivity)

ในการสร้างระบบเข้ารหัสลับให้มีความปลอดภัยอีกตัวแปรหนึ่งที่มีความสำคัญคือ ความไวของข้อมูลต้นฉบับซึ่งในการเข้ารหัสลับสื่อประสมแบบรูปภาพดิจิตอลสามารถวัดได้จาก 2 ตัวแปรคือ จำนวนอัตราการเปลี่ยนแปลงของพิกเซล (NPCR : number of pixel change rate) และ ค่าเฉลี่ยความเป็นปึกแผ่นของรูปภาพ (UACI : unified average changing intensity) [15] โดยทั่วไปแล้วทั้งสองค่านี้จะแสดงเป็นเปอร์เซ็นต์ ค่า NPCR สามารถหาได้จากสมการที่ (3.4) และค่า UACI สามารถหาได้จากสมการที่ (3.6)

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i, j)}{M \times N} \times 100\% \tag{3.4}$$

$$D(i, j) = \begin{cases} 0 & if \quad P_1(i, j) = P_2(i, j) \\ 1 & if \quad P_1(i, j) \neq P_2(i, j) \end{cases} \tag{3.5}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|P_1(i, j) - P_2(i, j)|}{L - 1}\right] \times 100\% \tag{3.6}$$

M คือ ขนาดความกว้างของรูปภาพดิจิตอล

N คือ ขนาดความยาวของรูปภาพดิจิตอล

P_1 คือ ข้อความลับที่เข้ารหัสด้วยรูปภาพต้นฉบับ

P_2 คือ ข้อความลับที่เข้ารหัสด้วยรูปภาพต้นฉบับที่เปลี่ยนแปลงเพียง 1 พิกเซล

L คือ ค่าความเข้มของพิกเซลสูงสุด

จากผลการวิจัยระบบเข้ารหัสลับที่ดี ควรจะมีค่า NPCR มากกว่า 90 เปอร์เซ็นต์ และค่า UCAI น้อยกว่า 30 เปอร์เซ็นต์ เพราะสามารถป้องกันการวิเคราะห์ ระบบรหัสลับแบบหาส่วนแตกต่าง (differential attacks) จากงานวิจัยของ Eli Biham และ Adi Shamir ที่วิเคราะห์การเข้ารหัสลับแบบ ดีอีเอส (DES : Data Encryption Standard) [16]

3.4.3 อัตราสัญญาณต่อสัญญาณรบกวน (Peak Signal-to-Noise Ratio)

ค่าอัตราสัญญาณต่อสัญญาณรบกวน เป็นตัวแปรส่วนหนึ่งในการวัดประเมินคุณภาพข้อมูลสื่อประสมที่ผ่านกระบวนการประมวลผล เช่น การบีบอัดข้อมูล โดยกระบวนการบีบอัดข้อมูลนั้นจำเป็นจะต้องมีค่า PSNR ที่สูง ซึ่งสามารถคำนวณได้จาก สมการที่ (3.7)

$$PSNR = 20\log_{10}\left(\frac{L}{\sqrt{MSE}}\right) \tag{3.7}$$

$$MSE = \frac{1}{M \times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[c(i,j) - p(i,j)]^2 \tag{3.8}$$

M คือ ขนาดความกว้างของรูปภาพดิจิตอล

N คือ ขนาดความยาวของรูปภาพดิจิตอล

c คือ ข้อความลับที่เข้ารหัสด้วยรูปภาพต้นฉบับ

p คือ ข้อความต้นฉบับ

L คือ ค่าความเข้มของพิกเซลสูงสุด

โดยทั่วไปในระบบเข้ารหัสลับข้อมูลจะต้องมีค่าอัตราสัญญาณต่อสัญญาณรบกวนที่ต่ำกว่า 30 dB จะเห็นได้ว่า ผู้ออกแบบระบบเข้ารหัสลับจะต้องออกแบบให้ได้ค่าที่ตรงข้ามกัน นั่นคือค่าจะต้องต่ำกว่า 30 dB [17]

3.4.4 ค่าเอนโทรปี (Information Entropy)

ค่าเอนโทรปี คือ ปริมาณที่บอกถึงความไม่เป็นระเบียบของระบบ ยิ่งระบบมีความไม่เป็นระเบียบสูง เอนโทรปีก็จะยิ่งมีค่าสูง แต่ถ้าระบบมีความไม่เป็นระเบียบน้อย เอนโทรปีก็จะยิ่งมีค่าต่ำใน

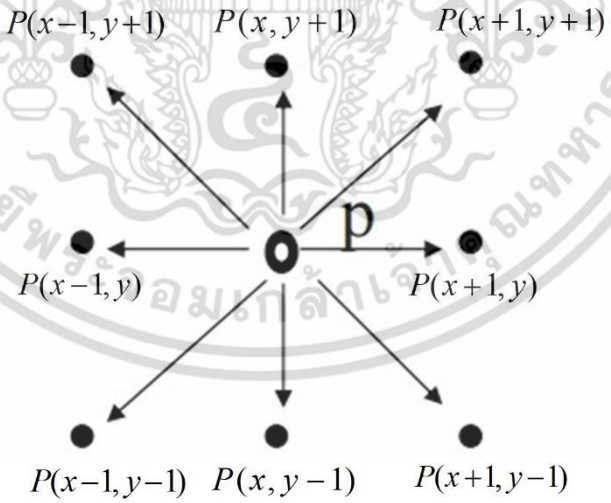
ทฤษฎีของแชลนอล [18] ได้ระบุค่าเอนโทรปีไว้ว่า ระบบเข้ารหัสลับที่ดีค่าเอนโทรปีก็จะต้องมีค่าสูง เพื่อป้องกันการโจมตีแบบวิเคราะห์ค่าทางสถิติ สามารถคำนวณได้จากสมการที่ (3.9)

$$H(s) = \sum_{i=1}^{2^M - 1} P(S_i) \log_2 \frac{1}{P(S_i)} \tag{3.9}$$

ในกรณีที่เข้ารหัสลับรูปด้วยดิจิตอลสีเทา (Gray scale) นั้น ค่าที่มากที่สุดจะมีค่าเท่ากับ 8 และค่าที่น้อยที่สุดคือ 0 เนื่องจาก 1 พิกเซลประกอบด้วย 8 บิต ในงานวิจัยส่วนมากได้ใช้ค่าเอนโทรปีในการออกแบบหรือวิเคราะห์ระบบเข้ารหัสลับ จะเห็นได้ว่าค่าที่ได้ส่วนมากจะมีค่า 7.00 ถึง 7.99 ดังนั้นการออกแบบระบบเข้ารหัสลับจะต้องทำให้ค่าเอนโทรปีมีค่าอย่างน้อย 7 สำหรับรูปภาพดิจิตอล 8 บิต

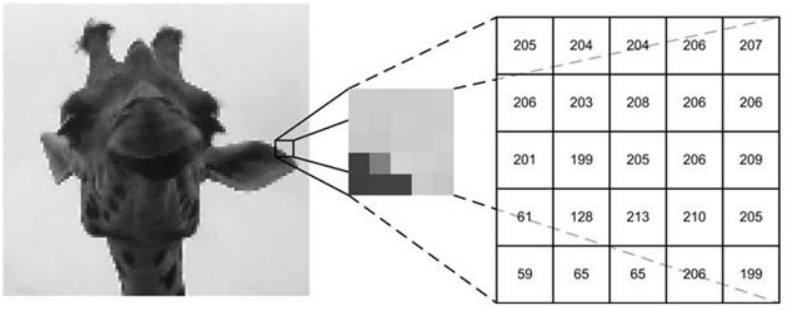
3.4.5 ค่าสหสัมพันธ์ (Correlation Coefficient)

ข้อมูลรูปภาพดิจิตอลแต่ละพิกเซลจะมีพิกเซลใกล้เคียง เช่น $P(x, y)$ จะมีพิกเซลใกล้เคียงทั้งทางแนวนอนและแนวตั้ง คือ $P(x+1, y)$, $P(x, y+1)$, $P(x-1, y)$, $P(x, y-1)$ และมีอีก 4 ตำแหน่งในแนวทแยง คือ $P(x+1, y+1)$, $P(x-1, y+1)$, $P(x+1, y-1)$, $P(x-1, y-1)$ สามารถแสดงตำแหน่งได้ดังรูปที่ 3.15



รูปที่ 3.15 ความสัมพันธ์ของพิกเซลใกล้เคียง

จากรูปที่ 3.15 จะเห็นได้ว่า1 พิกเซลจะมีพิกเซลใกล้เคียงทั้งหมด 8 ทิศทาง แสดงตัวอย่างได้ดังรูปที่ 3.16



รูปที่ 3.16 ตัวอย่างพิกเซลใกล้เคียง

ยกตัวอย่างรูปภาพดิจิตอลรูปที่ 3.16 จะมีความสัมพันธ์กันในพิกเซลที่ใกล้เคียงกัน (Neighborhood pixel) ที่ตำแหน่ง $P(2,2) = 203$

$$P(3,2) = 208 \quad P(3,3) = 205$$
$$P(1,2) = 206 \quad P(3,1) = 204$$
$$P(2,3) = 199 \quad P(1,3) = 201$$
$$P(2,1) = 204 \quad P(1,1) = 205$$

ในการหาค่าความสัมพันธ์สามารถหาค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สันได้ ดังสมการที่ (3.10)

$$r_{xy} = \frac{N\sum XY - (\sum X)(\sum Y)}{\sqrt{\left[N\sum X^2 - \left(\sum X\right)^2\right]\left[N\sum Y^2 - \left(\sum Y\right)^2\right]}} \tag{3.10}$$

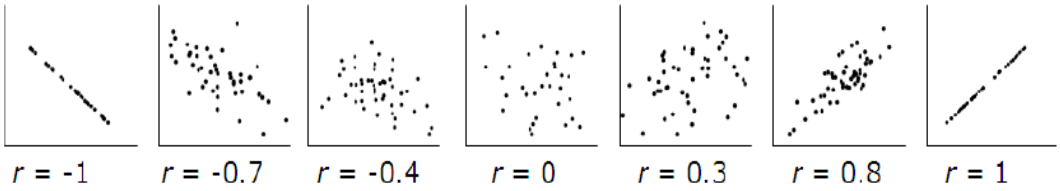
r_{xy} คือ ค่าสัมประสิทธิ์สหสัมพันธ์แบบเพียร์สัน

X คือ ข้อมูลที่วัดได้จากตัวแปรที่ 1

Y คือ ข้อมูลที่วัดได้จากตัวแปรที่ 2

N คือ ขนาดกลุ่มตัวอย่าง

ในการตีความหมายของค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สันเป็นความสัมพันธ์เชิงเส้น (r) ได้ดังรูปที่ 3.17



รูปที่ 3.17 ความสัมพันธ์เชิงเส้น (r)

จากรูปที่ 3.17 ได้แสดงการพล็อตกระจายค่าพิกเซล 2 ตำแหน่งและค่าสัมประสิทธิ์สหสัมพันธ์เพียร์สัน ดังนั้นระบบเข้ารหัสลับที่ดีจะต้องทำให้พิกเซลใกล้เคียงไม่มีความสัมพันธ์กันนั้น คือ ทำให้ค่าสัมประสิทธิ์เข้าใกล้ 0 ให้ได้มากที่สุด [20]

3.4.6 การรับรู้ข้อมูลลับ (Perceptual Security)

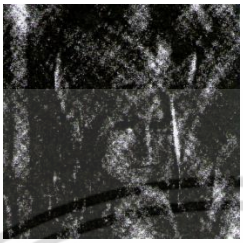
การเข้ารหัสลับโดยเฉพาะการเข้ารหัสสื่อประสม [3] มีลักษณะที่แตกต่างจากการเข้ารหัสไฟล์ คือข้อมูลต้นฉบับสื่อประสมมีความสัมพันธ์กันสูง ซึ่งทำให้ข้อมูลลับมีลักษณะที่ยังสามารถเข้าใจได้ ซึ่งสามารถแบ่งระดับการรับรู้ได้ดังตารางที่ 3.5

ตารางที่ 3.5 ระดับการรับรู้คุณภาพของข้อมูลลับ (Perceptual Security) [3]

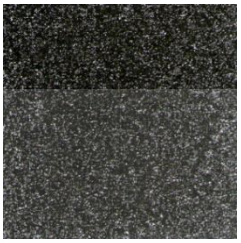
ระดับคุณภาพของรูปดิจิตอล (Quality Level)	ความหมายแต่ละระดับคุณภาพของรูปดิจิตอลลับ (Corresponding Quality of Ciphertext)
QL0	สามารถรับรู้ถึงข้อมูลต้นฉบับได้เป็นอย่างดี (Completely understandable)
QL1	ยังสามารถรับรู้ข้อมูลต้นฉบับได้ (Understandable)
QL2	ไม่สามารถรับรู้ได้ (Not understandable)

จากตารางที่ 3.5 แบ่งระดับการรับรู้ได้ 3 แบบ QL0 คือ แบบยังสามารถรับรู้ถึงข้อมูลต้นฉบับได้เป็นอย่างดี QL1 คือ แบบที่ยังสามารถรับรู้ข้อมูลต้นฉบับได้ QL2 คือแบบที่ไม่สามารถรับรู้ได้เลย ยกตัวอย่างทั้ง 3 ระดับ ได้ดังรูปที่ 3.18

QL0



QL1



QL2

รูปที่ 3.18 ระดับการรับรู้คุณภาพของข้อมูลลับ 3 ระดับ

จากรูปที่ 3.18 จะเห็นได้ว่า QL0 มีความเหมือนกับรูปต้นฉบับเป็นอย่างมากจึงทำให้สามารถรับรู้และเข้าใจเป็นอย่างดี QL1 มีความคล้ายคลึงกับต้นฉบับบางส่วน และ QL2 ไม่มีความคล้ายคลึงต้นฉบับแม้แต่น้อยทั้งยังไม่สามารถสื่อสารได้เลย การออกแบบจึงจำเป็นต้องให้ข้อมูลลับอยู่ในระดับ QL2

บทที่ 4
ผลการออกแบบและทดสอบการทำงาน

ในบทนี้จะกล่าวถึงผลลัพธ์การออกแบบระบบเข้ารหัสลับเนื้อหาสื่อประสม ทั้งรูปภาพ ข้อความ และเสียง ในรูปแบบดิจิตอล และผลลัพธ์การวัดประสิทธิภาพของระบบเข้ารหัสลับตามที่ได้ออกแบบมาในหัวข้อก่อนหน้านี้เปรียบเทียบระหว่างระบบเข้ารหัสลับที่ถูกนำเสนอที่ผ่านมา และสุดท้ายได้ยกตัวอย่างการประยุกต์ใช้งานโครงสร้างที่นำเสนอกับการรับส่งข้อความสั้นบนสมาร์ทโฟน และไฟล์ข้อมูลบนเครื่องคอมพิวเตอร์

4.1 ผลลัพธ์ของการเข้ารหัสลับเนื้อหาสื่อประสม

ผลลัพธ์ของการสร้างกุญแจลับจากรหัสผ่าน (password) เป็นอักขระ 16 ตัว กำหนดเป็นสัญญาณขาเข้าของระบบ เพื่อสร้างสัญญาณขาออกที่เป็นกุญแจระนาบบิต ยกตัวอย่างการใช้งานโดยกำหนดค่าพารามิเตอร์ดังนี้

รหัสผ่าน (password) - “Kio@398$gRu2ga!4”

ข้อมูลต้นฉบับ (Plaintext) - รูปภาพดิจิตอล ข้อความ และเสียง

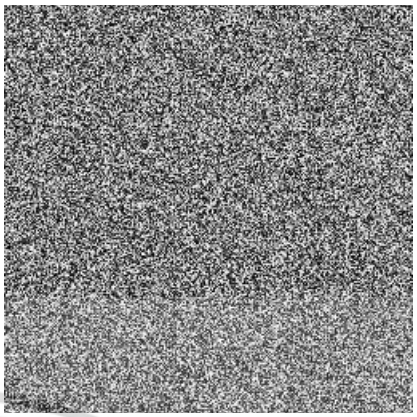
4.1.1 ข้อมูลลับรูปภาพดิจิตอล

ข้อมูลลับรูปภาพดิจิตอลทดลองเข้ารหัสลับรูปภาพดิจิตอลทั้งหมด 5 รูปภาพด้วยรหัสผ่านเดียวกัน แสดงรูปภาพดิจิตอลต้นฉบับและรูปภาพลับได้ดังรูปที่ 4.1

(ก) (ข)

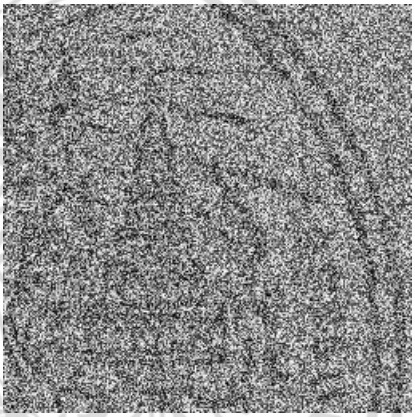
รูปที่ 4.1 ข้อมูลรูปภาพดิจิตอลต้นฉบับและรูปภาพที่เข้ารหัสลับ 5 รูป

(ค)

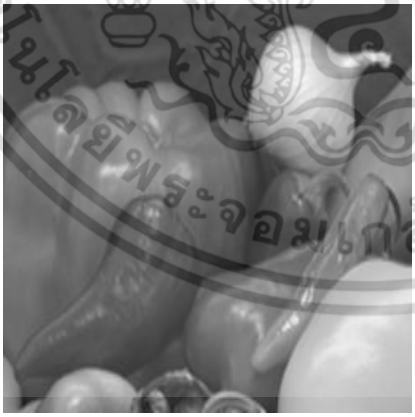


(ง)

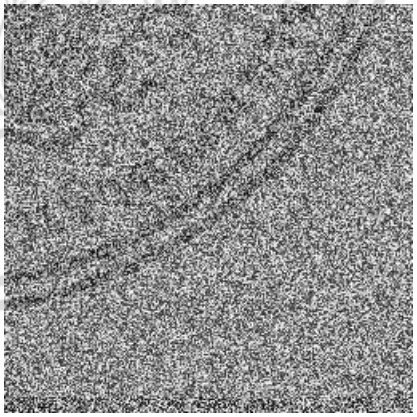
(จ)



(ฉ)



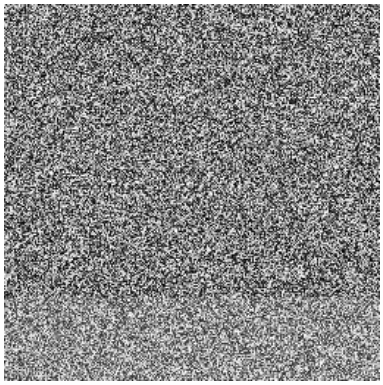
(ช)



(ซ)

รูปที่ 4.1 (ต่อ) ข้อมูลรูปภาพดิจิตอลต้นฉบับและรูปภาพที่เข้ารหัสลับ 5 รูป

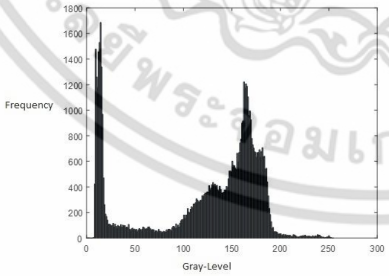
(ฌ)



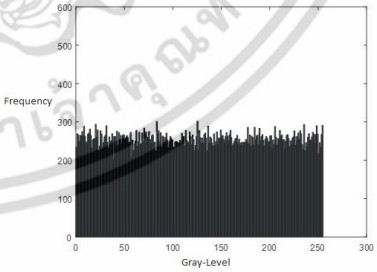
(ญ)

รูปที่ 4.1 (ต่อ) ข้อมูลรูปภาพดิจิตอลต้นฉบับและรูปภาพที่เข้ารหัสลับ 5 รูป (ก) รูปภาพต้นฉบับ Cameraman (ข) รูปภาพเข้ารหัสลับ Cameraman (ค) รูปภาพต้นฉบับ Map (ง) รูปภาพเข้ารหัสลับ Map (จ) รูปภาพต้นฉบับ Football (ฉ) รูปภาพเข้ารหัสลับ Football (ช) รูปภาพต้นฉบับ Onion (ซ) รูปภาพเข้ารหัสลับ Onion (ฌ) รูปภาพต้นฉบับ Autumn (ญ) รูปภาพเข้ารหัสลับ Autumn

จากรูปที่ 4.1 แสดงรูปที่ใช้ในการทดสอบ 5 รูป คือ 1) Cameraman 2) Map 3) Football 4) Onion และ 5) Autumn เห็นได้ชัดเจนว่ารูปภาพลับทั้ง 5 รูป ไม่มีความคล้ายกับรูปภาพต้นฉบับเลย แม้แต่น้อย ส่วนผลของฮีสโทแกรมของรูปภาพดิจิตอล เปรียบเทียบระหว่างรูปภาพต้นฉบับและรูปภาพที่เข้ารหัสแล้ว แสดงได้ดังรูปที่ 4.2 และ 4.3 รูปภาพต้นฉบับคือ Cameraman



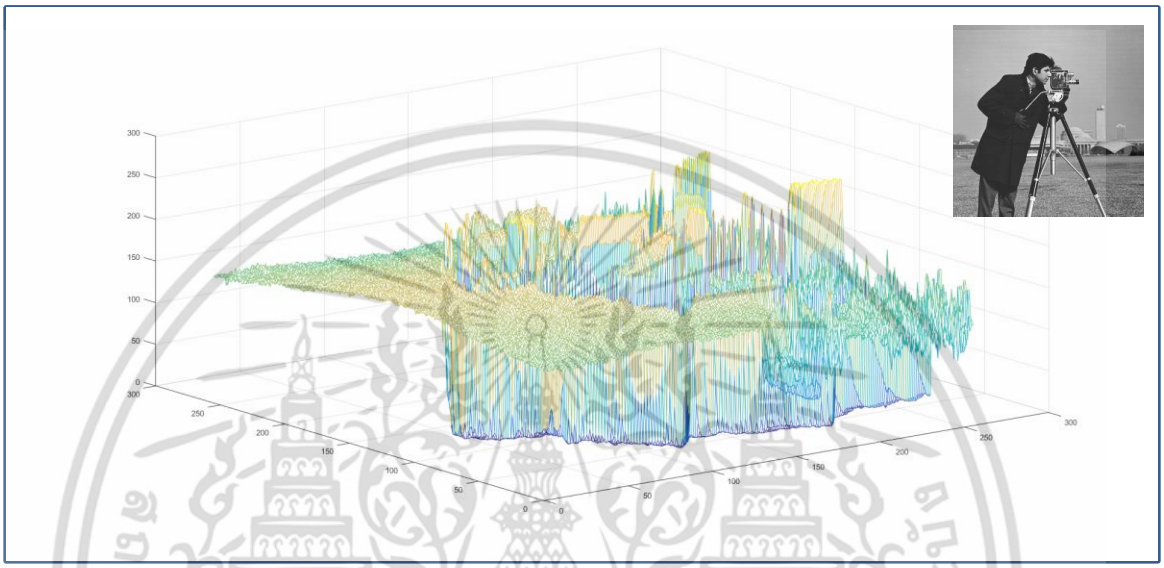
(ก)



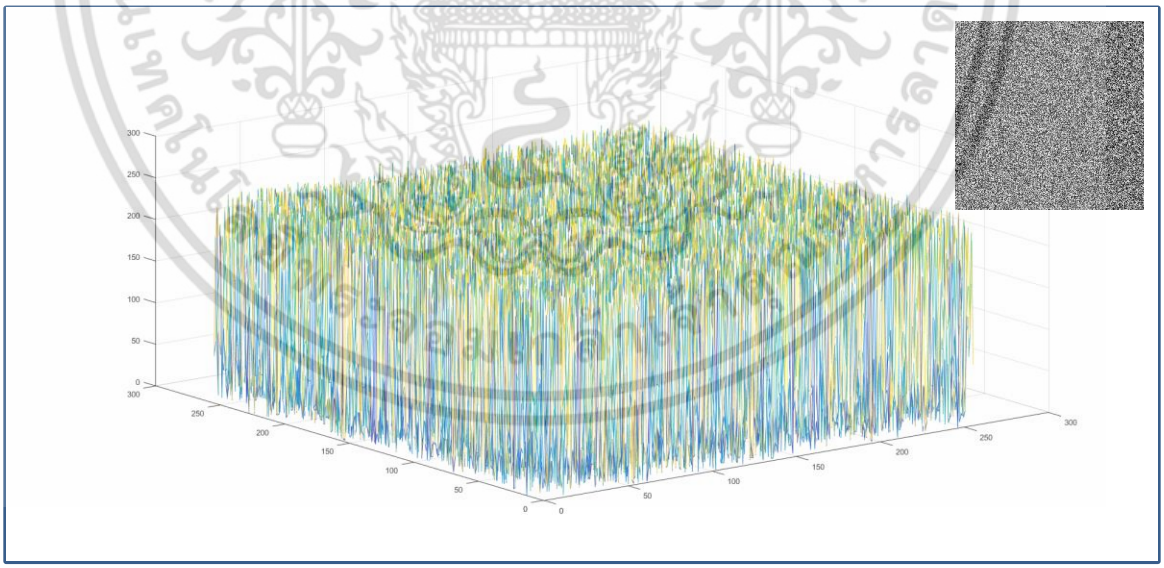
(ข)

รูปที่ 4.2 ฮีสโทแกรมของรูปภาพต้นฉบับและรูปภาพลับ (ก) ฮีสโทแกรมรูปภาพต้นฉบับ (ข) ฮีสโทแกรมรูปภาพลับ

จากรูปที่ 4.2 ฮีสโทแกรมของรูปภาพต้นฉบับและรูปภาพลับ รูปที่ 4.2 (ก) เป็นฮีสโทแกรมของรูปภาพดิจิตอลต้นฉบับ และรูปที่ 4.2 (ข) คือฮีสโทแกรมของรูปภาพลับ และแสดงสเปกตรัม 2 มิติได้ดังรูปที่ 4.3

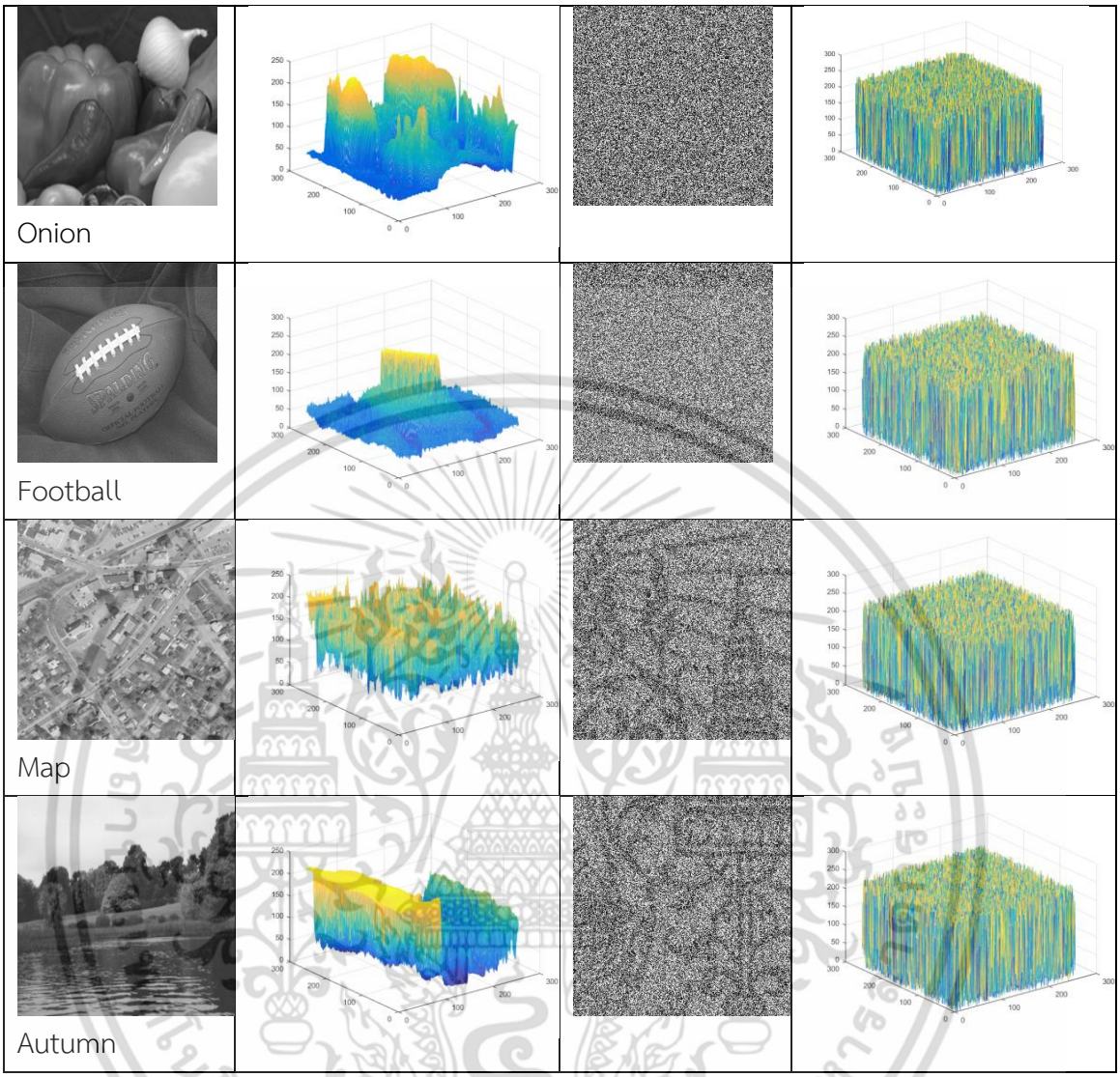


(ก)



(ข)

รูปที่ 4.3 สเปกตรัม 2 มิติของรูปภาพต้นฉบับและรูปภาพลับ Cameraman (ก) สเปกตรัม 2 มิติ รูปภาพต้นฉบับ Cameraman (ข) สเปกตรัม 2 มิติ รูปภาพลับ Cameraman



รูปที่ 4.4 สเปกตรัม 2 มิติของรูปภาพต้นฉบับและรูปภาพลับ (Onion, Football, Map, Autumn)

จากรูปที่ 4.3 และ 4.4 จะเห็นได้ว่าค่าสเปกตรัมของรูปภาพลับมีความแตกต่างอย่างมากกับรูปภาพต้นฉบับ โดยสเปกตรัมของรูปภาพลับนั้นมีลักษณะเหมือนสัญญาณรบกวนมาก ซึ่งเป็นผลที่ดีสำหรับการเข้ารหัสลับ

4.1.2 ข้อความลับ

ข้อความจะทดลองข้อความอักขระภาษาไทย ทั้งหมด 3 ข้อความ และอังกฤษอีก 3 ข้อความ เข้ารหัสลับด้วยกุญแจเดียวกันคือ “Kio@398$gRu2ga!4” แสดงผลการทดลองได้ดังตารางที่ 4.1 และ 4.2

ตารางที่ 4.1 ผลลัพธ์การเข้ารหัสลับข้อความภาษาไทย

ข้อมูลข้อความต้นฉบับ		ข้อมูลข้อความลับ	
อักขระ	เลขฐานสิบหก	เลขฐานสิบหก	อักขระ
ความลับสุดยอด	A4C7D2C1C5D1BACA D8B4C2CDB4	8409F366CB9F52BB 1BEC028F56	O&?ญ ศ
กรุงเทพมหานคร	A1C3D8A7E0B7BEC1 CBD2B9A4C3	810DF900EEF956B0 088A79E621	K,Y ป |ณ้w
ด่วนที่สุด	B4E8C7B9B7D5E8CA D8B4	9426E61EB99B00BB 1BEC	V* ศ\X

จากตารางที่ 4.1 แสดงผลลัพธ์การเข้ารหัสลับข้อความภาษาไทย ตามมาตรฐาน TIS-602 ในรูปแบบเลขฐานสิบหกจะเห็นได้ว่าข้อความลับมีความไม่เหมือนกับข้อความต้นฉบับ

ตารางที่ 4.2 ผลลัพธ์การเข้ารหัสลับข้อความภาษาอังกฤษ

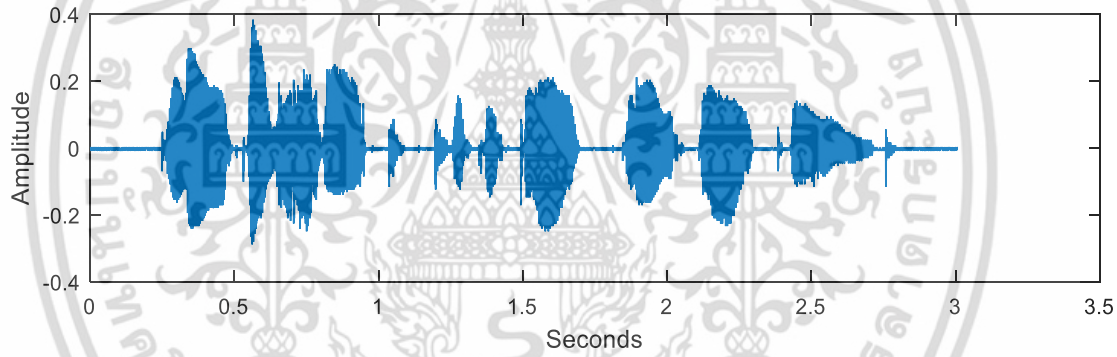
ข้อมูลข้อความต้นฉบับ		ข้อมูลข้อความลับ	
อักขระ	เลขฐานสิบหก	เลขฐานสิบหก	อักขระ
7.30 PM	372E333020504D	17E012972E1EA5	"- `ญw
Thailand	546861696C616E64	74A640CE622F8615	bKMF๑ fฎ
Secret	536563726574	73AB42D56B3A	d=Ѣ

จากตารางที่ 4.2 แสดงผลลัพธ์การเข้ารหัสลับขข้อความภาษาอังกฤษ ในรูปแบบเลขฐานสิบหก จะเห็นได้ว่าข้อความลับมีความไม่เหมือนกับข้อความต้นฉบับ ข้อมูลต่อไปที่ทดสอบคือ ข้อมูลชนิดเสียง

4.1.3 ข้อมูลลับเสียง

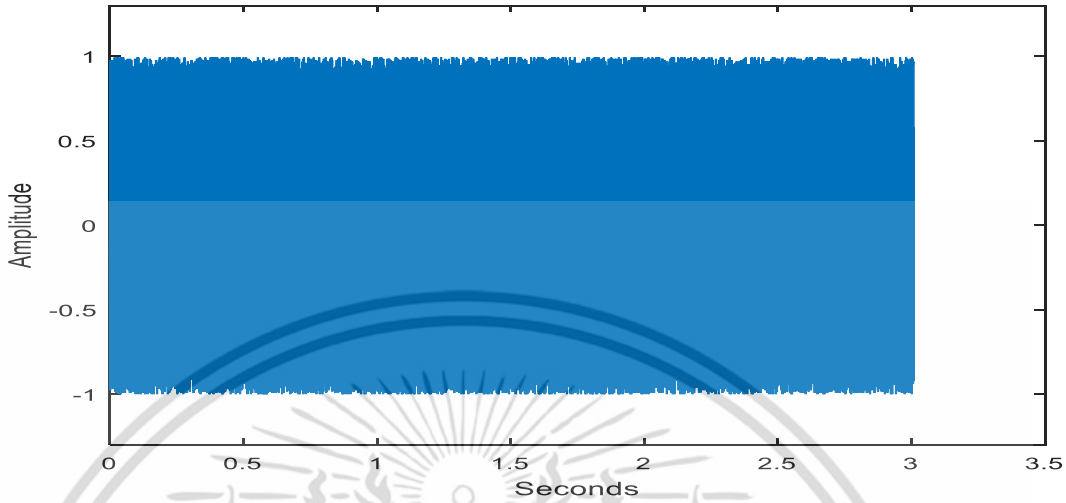
ข้อมูลชนิดเสียงที่ใช้ในทดลองเป็นไฟล์เสียงชนิด WAVE (.wav) ขนาดความยาวประมาณสามนาที ไม่มีการบีบอัด แสดงข้อมูลไฟล์และขนาดแอมพลิจูดได้ดังรูปที่ 4.5

```
info =

            Filename: 'C:\Users\Nakarin\Desktop\FileM-May\1127\chaos_soundWdf\PlainAudio.wav'
    CompressionMethod: 'Uncompressed'
          NumChannels: 1
           SampleRate: 16000
         TotalSamples: 48136
             Duration: 3.0085
                Title: 'KMITL-2016.'
              Comment: 'This is my Plain-audio file.'
               Artist: 'Nakarin'
        BitsPerSample: 8

>>
```

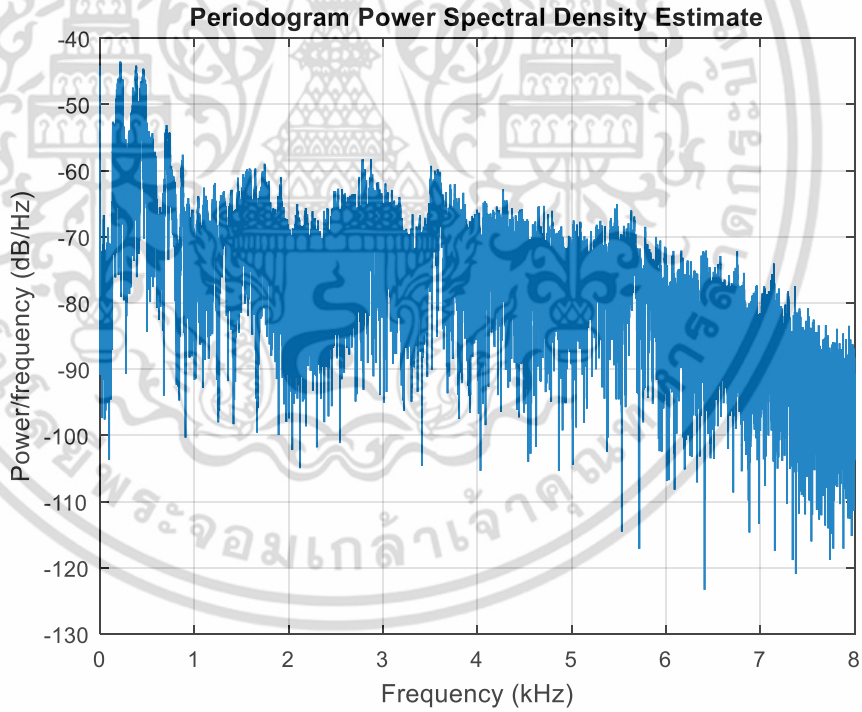


รูปที่ 4.5 แอมพลิจูดของข้อมูลเสียงต้นฉบับ

ทดสอบใช้รหัสลับ “Kio@398$gRu2ga!4” แสดงผลลัพธ์ข้อมูลเสียงลับได้ดังรูปที่ 4.6

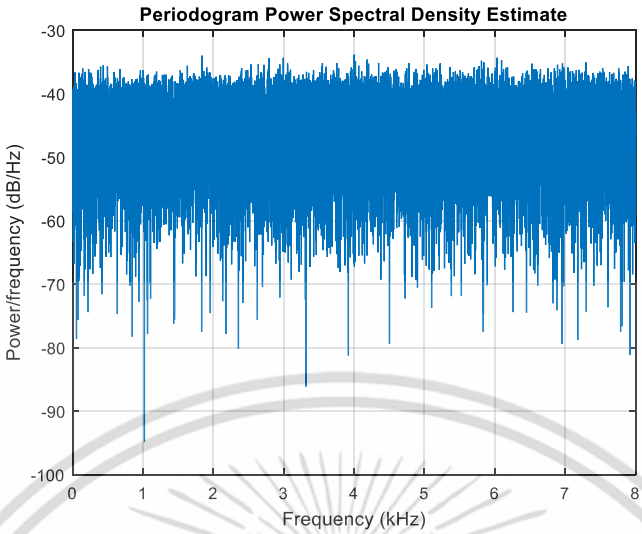


รูปที่ 4.6 แสดงแอมพลิจูดของข้อมูลเสียงลับ



(ก)

รูปที่ 4.7 ความหนาแน่นสเปกตรัมของ (PSD) ของข้อมูลเสียง



(ข)

รูปที่ 4.7 (ต่อ) ความหนาแน่นสเปกตรัมของ (PSD) ของข้อมูลเสียง (ก) ความหนาแน่นสเปกตรัมของ (PSD) ข้อมูลเสียงต้นฉบับ (ข) ความหนาแน่นสเปกตรัมของ (PSD) ของข้อมูลเสียงลับ

จากรูปที่ 4.6 และ 4.7 จะเห็นได้ว่าข้อมูลเสียงลับมีขนาดแอมพลิจูดและความหนาแน่นสเปกตรัมมีลักษณะเหมือนกับสัญญาณรบกวนที่มีกำลังงานเท่ากันตลอดในทุกย่านความถี่

4.2 ผลลัพธ์การวัดประสิทธิภาพของระบบเข้ารหัสลับ

ในการวัดประสิทธิภาพการระบบเข้ารหัสลับเนื้อหาสื่อประสม โดยทั่วไปจะอ้างอิงจากการเข้ารหัสรูปภาพดิจิตอล เนื่องจากเนื้อหารูปภาพดิจิตอลมีส่วนที่มีความสัมพันธ์ระหว่างพิกเซลใกล้เคียงกันสูงมาก ทำให้บางโครงสร้างเข้ารหัสลับรูปภาพดิจิตอลแล้วยังมีลักษณะเหมือนข้อมูลต้นฉบับดังที่ได้กล่าวไปในหัวข้อก่อนหน้านี้ ดังนั้นผลที่ได้จากการวัดรูปภาพดิจิตอลมีค่าที่ดี จะทำให้ข้อมูลข้อความและเสียงดีตามไปด้วย ประสิทธิภาพของระบบเข้ารหัสลับที่นำเสนอนี้ได้แสดงผลลัพธ์การวัดประสิทธิภาพระบบเข้ารหัสลับได้ตามหัวข้อดังต่อไปนี้

4.2.1 ขนาดกุญแจและความไวกุญแจ

ผลลัพธ์จากการวัดประสิทธิภาพขนาดกุญแจแสดงได้ดังตารางที่ 4.3 เปรียบเทียบขนาดกุญแจต่างๆ ที่ใช้ในระบบเข้ารหัส และจำนวนกุญแจที่เป็นไปได้ รวมถึงการเดาสุ่มกุญแจด้วยซุปเปอร์คอมพิวเตอร์ (Super computer)

ตารางที่ 4.3 ผลลัพธ์ขนาดกุญแจและระยะเวลาที่ใช้เดากุญแจลับเทียบอัลกอริทึมอื่น

ขนาดกุญแจ	อัลกอริทึม	จำนวนกุญแจที่เป็นไปได้	ระยะเวลาที่ใช้เดา Brute-force (1 ล้านล้านครั้งต่อวินาที) [24]
32	Blowfish-32	4.3×10^{9}	1.25 ms
56	DES	7.2×10^{16}	10 hrs
128	AES-128, ระบบที่นำเสนอ	3.4×10^{16}	5.4×10^{18}
168	3-DES	3.7×10^{50}	5.9×10^{30}
192	AES-192	6.2×10^{57}	1.8×10^{57}

ตารางที่ 4.4 ผลลัพธ์ความไวของกุญแจ (Key Sensitivity)

ขนาดกุญแจ	Key Sensitivity (%)
KOPyhtg7$%rtgyho	96.278
1236814657824694	96.240
HELLOTHAILANDAAB	95.094
^74/$@$^&*#4%^&3	96.224
g3$Hf43!Kop09@88	96.129

จากตารางที่ 4.4 ได้ทดสอบกุญแจทั้ง 5 ตัว จะเห็นได้ว่าค่าความไวของกุญแจ (Key Sensitivity) ที่แสดงผลออกมาเป็นเปอร์เซ็นต์ มีค่ามากกว่า 50 เปอร์เซ็นต์ เข้าใกล้ 100 เปอร์เซ็นต์ ซึ่งถือว่าการออกแบบในส่วนของกุญแจลับมีความแข็งแรงโดยทำให้การเดาสุ่มกุญแจใช้ระยะเวลายาวนานขึ้น

4.2.2 ความไวของข้อมูลต้นฉบับ

ผลการทดลองความไวของข้อมูลต้นฉบับสามารถวัดได้จากค่า NPCR และ UACI ซึ่งแสดงผลลัพธ์ได้ดังตารางที่ 4.5

ตารางที่ 4.5 ผลลัพธ์ความไวของข้อมูลต้นฉบับรูปภาพดิจิตอล

ชื่อรูปภาพต้นฉบับ	NPCR (เปอร์เซ็นต์)	UACI (เปอร์เซ็นต์)
Cameraman	99.6048	31.036
Onion	99.6185	30.3122
Map	99.619	27.107
Autumn	99.619	34.984
Football	99.619	31.506

จากตารางที่ 4.5 จะเห็นได้ว่าระบบที่นำเสนอมีค่าความไวของข้อมูลต้นฉบับที่ได้มาตรฐานการออกแบบระบบเข้ารหัสลับ คือค่าที่ดีต้อง มีค่า NCPR มากกว่า 90 เปอร์เซ็นต์ และ UACI ไม่เกิน 33 เปอร์เซ็นต์ จากผลการทดลองนี้แสดงให้เห็นว่าระบบที่นำเสนอมีความแข็งแรงผ่านมาตรฐานการออกแบบวงจรเข้ารหัสลับในมุมมองของความไวของข้อมูลต้นฉบับ

4.2.3 อัตราสัญญาณต่อสัญญาณรบกวน และค่าเอนโทรปีข้อมูล

ผลลัพธ์อัตราสัญญาณต่อสัญญาณรบกวน (PSNR) และ ค่าเอนโทรปีข้อมูล (Information Entropy) แสดงได้ดังตารางที่ 4.6

ตารางที่ 4.6 ผลลัพธ์อัตราสัญญาณต่อสัญญาณรบกวน (PSNR) และค่าเอนโทรปีข้อมูล (Entropy)

ชื่อรูปภาพต้นฉบับ	PSNR	Entropy
Cameraman	8.41435	7.99693
Onion	8.64603	7.99762
Map	9.8109	7.9969
Autumn	7.3668	7.9972
Football	8.283	7.9975

จากตารางที่ 4.6 จะเห็นได้ว่าผลลัพธ์อัตราสัญญาณต่อสัญญาณรบกวน (PSNR) และ ค่าเอนโทรปีข้อมูล (Entropy) มีค่าที่ผ่านมาตรฐานการออกแบบระบบเข้ารหัสลับในมุมมองทั้งสองตัวแปรนี้ คืออัตราสัญญาณต่อสัญญาณรบกวน จะต้องต่ำกว่า 30dB

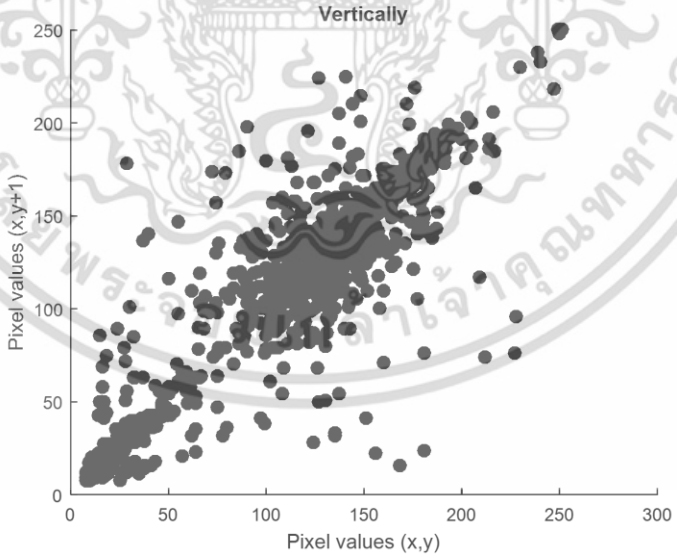
4.2.4 ค่าสัมประสิทธิ์สหสัมพันธ์ของรูปภาพดิจิตอล

สำหรับผลการทดลองค่าสัมประสิทธิ์สหสัมพันธ์ของรูปภาพดิจิตอล จะแสดงออกออกมาทั้งหมด 3 ความสัมพันธ์ คือ ความสัมพันธ์ในแนวนอน แนวตั้ง และแนวทแยง

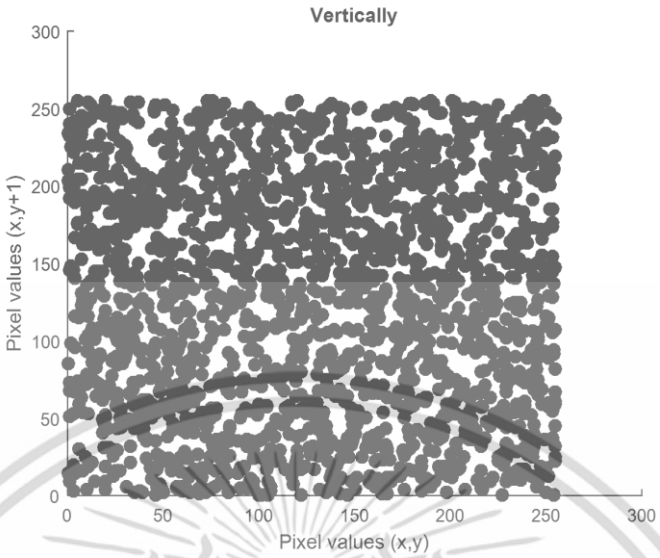
ตารางที่ 4.7 ผลลัพธ์ค่าสัมประสิทธิ์สหสัมพันธ์ (Correlation coefficient) ของรูปภาพดิจิตอล

ชื่อรูปภาพต้นฉบับ	แนวนอน (Horizontal๗	แนวตั้ง (Vertical)	แนวทแยง (Diagonal)
Cameraman	-0.0014	-0.0003	-0.0026
Onion	-0.00067	-0.0047	-0.00346
Map	-0.0039	-0.0076	0.007
Autumn	-0.0033	-0.0055	-0.0022
Football	-0.0026	-0.0073	-0.0055

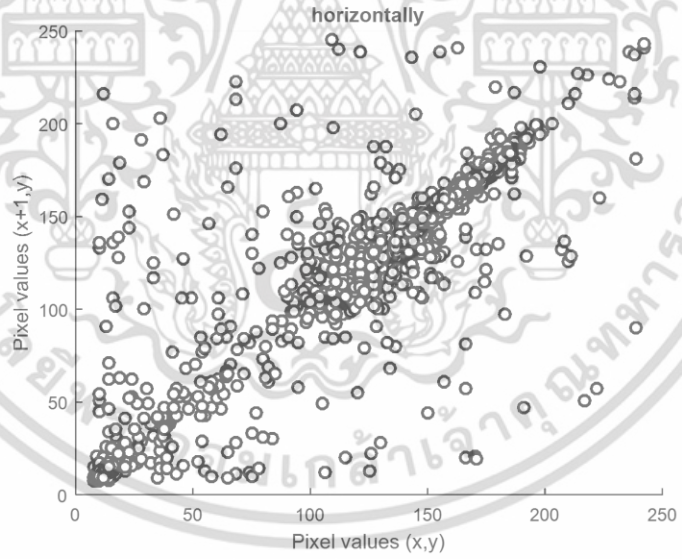
จากตารางที่ 4.7 จะเห็นได้ว่าค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างพิกเซลใกล้เคียงมีค่าที่แตกต่างกันมากทั้ง 3 แบบความสัมพันธ์ และทดสอบพล็อตจุดแสดงความสัมพันธ์ระหว่างพิกเซลใกล้เคียง ทั้ง 3 แบบ ได้ดังรูปที่ 4.8 ถึง รูปที่ 4.10



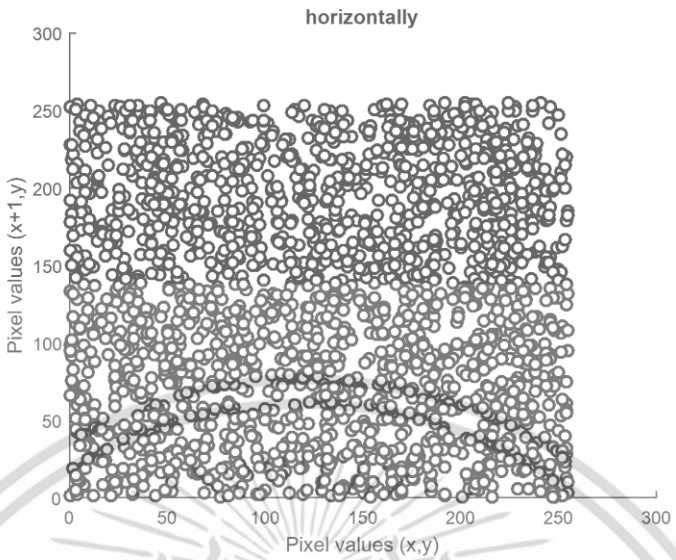
รูปที่ 4.8 การพล็อตจุดระหว่างพิกเซลใกล้เคียงแนวตั้งของรูปภาพดิจิตอลต้นฉบับ



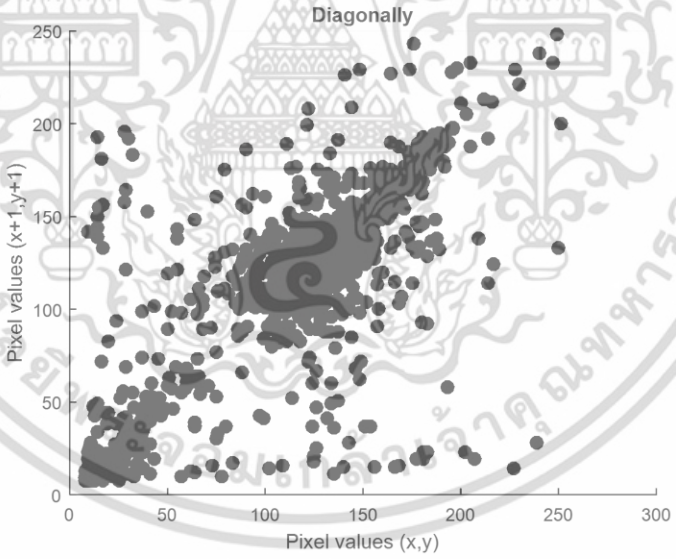
รูปที่ 4.9 การพล็อตจุดระหว่างพิกเซลใกล้เคียงแนวตั้งของรูปภาพดิจิตอลลับ



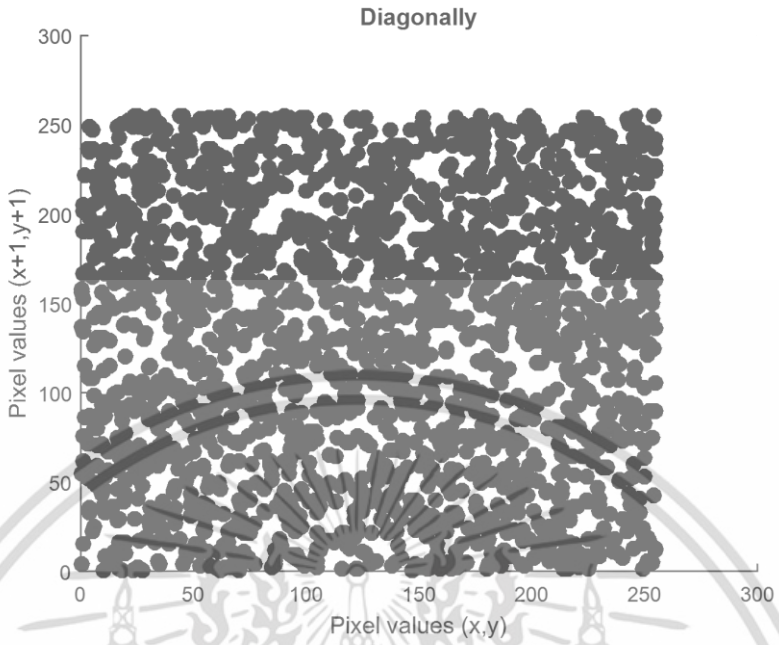
รูปที่ 4.10 การพล็อตจุดระหว่างพิกเซลใกล้เคียงแนวนอนของรูปภาพดิจิตอลต้นฉบับ



รูปที่ 4.11 การพล็อตจุดระหว่างพิกเซลใกล้เคียงแนวนอนของรูปภาพดิจิตอลลับ



รูปที่ 4.12 การพล็อตจุดระหว่างพิกเซลใกล้เคียงแนวทแยงของรูปภาพดิจิตอลต้นฉบับ



รูปที่ 4.13 การพล็อตจุดระหว่างพิกเซลใกล้เคียงแนวทแยงของรูปภาพดิจิตอลลับ

จากรูปที่ 4.8-4.13 ลักษณะการพล็อตของแต่ละจุดกระจายรูปภาพ cameraman แสดงให้เห็นว่าข้อมูลรูปภาพลับมีเนื้อหาพิกเซลที่ไม่มีความสัมพันธ์กับพิกเซลบริเวณใกล้เคียงเลยทุกกรณี ซึ่งถือว่าเป็นข้อมูลรูปภาพลับที่ดี

4.3 เปรียบเทียบประสิทธิภาพกับระบบเข้ารหัสลับโครงสร้างอื่น

ทดลองเข้ารหัสรูปภาพดิจิตอลตามงานวิจัยก่อนหน้านี้ 4 โครงสร้างเข้ารหัสลับ โดยใช้ข้อมูลต้นฉบับรูปภาพดิจิตอล 5 รูปภาพ คือ 1) Cameraman แสดงได้ดังตารางที่ 4.8 2) Onion แสดงได้ดังตารางที่ 4.9 3) Map แสดงได้ดังตารางที่ 4.10 4) Autumn แสดงได้ดังตารางที่ 4.11 และ 5) Football แสดงได้ดังตารางที่ 4.12

ตารางที่ 4.8 เปรียบเทียบประสิทธิภาพระบบเข้ารหัสลับรูปภาพ Cameraman กับระบบเข้ารหัสลับโครงสร้างที่นำเสนอก่อนหน้า

โครงสร้างเข้ารหัสลับ	Correlation coefficient			PSNR	NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal				
โครงสร้างที่ 1 [4]	-0.1963	-0.1407	-0.0488	9.21544	98.9304	26.5356	7.00972
โครงสร้างที่ 2 [9]	0.00054	-0.0019	0.00096	8.46314	99.2767	30.2259	7.99473
โครงสร้างที่ 3 [11]	-0.0036	0.0022	0.00582	8.38196	99.5834	31.1812	7.99578
โครงสร้างที่ 4 [12]	0.06616	-0.0155	-0.0014	8.38435	99.6063	31.1803	7.99712
โครงสร้างที่นำเสนอ	-0.0014	-0.0003	-0.0026	8.41435	99.6048	31.036	7.99693

ตารางที่ 4.9 เปรียบเทียบประสิทธิภาพระบบเข้ารหัสลับรูปภาพ Onion กับระบบเข้ารหัสลับโครงสร้างที่นำเสนอก่อนหน้า

โครงสร้างเข้ารหัสลับ	Correlation coefficient			PSNR	NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal				
โครงสร้างที่ 1 [4]	0.16632	-0.20536	-0.11335	10.8297	99.0448	22.4611	7.33253
โครงสร้างที่ 2 [9]	-0.05	-0.0043	-0.06698	8.30329	99.6338	32.005	7.92879
โครงสร้างที่ 3 [11]	-0.00526	-0.00038	0.00417	8.65853	99.6002	30.3138	7.99574
โครงสร้างที่ 4 [12]	0.49745	-0.0201	-0.27442	8.6573	99.617	30.3052	7.99762
โครงสร้างที่นำเสนอ	-0.00067	-0.0047	-0.00346	8.64603	99.6185	30.3122	7.99762

ตารางที่ 4.10 เปรียบเทียบประสิทธิภาพระบบเข้ารหัสลับรูปภาพ Map กับระบบเข้ารหัสลับโครงสร้างที่นำเสนอก่อนหน้า

โครงสร้างเข้ารหัสลับ	Correlation coefficient			PSNR	NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal				
โครงสร้างที่ 1 [4]	0.0828	0.024	0.0366	14.329	99.094	15.476	7.1199
โครงสร้างที่ 2 [9]	-0.0182	-0.0027	-0.0067	9.6137	99.648	27.957	7.9712
โครงสร้างที่ 3 [11]	-0.003	0.0132	-0.0025	9.771	99.59	27.246	7.9953
โครงสร้างที่ 4 [12]	0.3954	-0.0339	-0.1969	9.7891	99.617	27.195	7.9975
โครงสร้างที่นำเสนอ	-0.0039	-0.0076	0.007	9.8109	99.619	27.107	7.9969

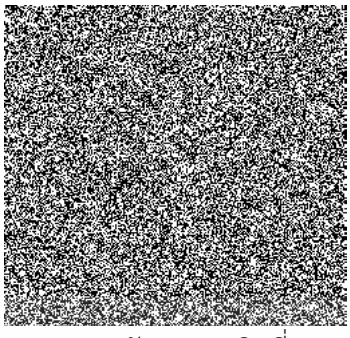
ตารางที่ 4.11 เปรียบเทียบประสิทธิภาพระบบเข้ารหัสลับรูปภาพ Autumn กับระบบเข้ารหัสลับโครงสร้างที่นำเสนอก่อนหน้า

โครงสร้างเข้ารหัสลับ	Correlation coefficient			PSNR	NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal				
โครงสร้างที่ 1 [4]	0.5742	0.5042	0.3155	7.2096	98.915	33.537	7.0197
โครงสร้างที่ 2 [9]	-0.0243	0.1982	0.0598	7.2413	99.677	35.87	7.914
โครงสร้างที่ 3 [11]	-0.0013	-0.0065	0.0006	7.3895	99.634	34.916	7.9952
โครงสร้างที่ 4 [12]	0.506	-0.0419	-0.2644	7.3759	99.617	34.942	7.9972
โครงสร้างที่นำเสนอ	-0.0033	-0.0055	-0.0022	7.3668	99.619	34.984	7.9972

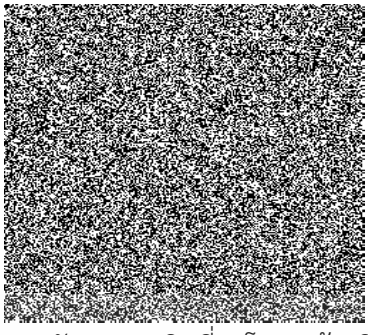
ตารางที่ 4.12 เปรียบเทียบประสิทธิภาพระบบเข้ารหัสลับรูปภาพ Football กับระบบเข้ารหัสลับโครงสร้างที่นำเสนอก่อนหน้า

โครงสร้างเข้ารหัสลับ	Correlation coefficient			PSNR	NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal				
โครงสร้างที่ 1 [4]	0.3235	-0.2208	0.0742	13.805	98.616	13.963	6.6982
โครงสร้างที่ 2 [9]	-0.2605	0.149	-0.2386	7.4333	99.725	36.238	7.8822
โครงสร้างที่ 3 [11]	-0.007	0.0085	0.0023	8.2788	99.577	31.585	7.9963
โครงสร้างที่ 4 [12]	0.4874	-0.0469	-0.2725	8.2876	99.617	31.507	7.9974
โครงสร้างที่นำเสนอ	-0.0026	-0.0073	-0.0055	8.283	99.619	31.506	7.9975

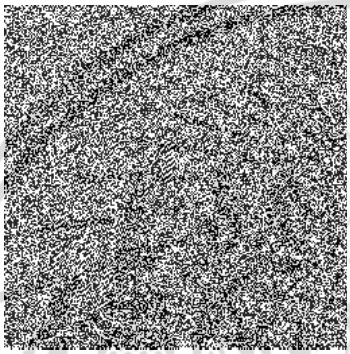
จากตารางที่ 4.9 ถึงตารางที่ 4.12 โครงสร้างที่ 1 [4] เป็นโครงสร้างที่ใช้เคออติกแบบแคทแมพ โครงสร้างที่ 2 [7] เป็นโครงสร้างที่เพิ่ม diffusion โครงสร้างที่ 3 [12] เป็นโครงสร้างที่ใช้เคออติกแมพแบบการรวมกันของ Sine และ Cosine โครงสร้างที่ 4 [11] เป็นโครงสร้างที่ใช้วงจรกรองสัญญาณดิจิตอล IIR ลำดับที่สอง และโครงสร้างสุดท้ายเป็นโครงสร้างที่นำเสนอ จะเห็นได้ว่ามีค่าสหสัมพันธ์ (Correlation coefficient) ที่ดีที่สุดคือมีค่าเข้าใกล้ 0 มากที่สุด ค่า NPCR และ UACI ก็มีค่าที่ได้มาตรฐานการออกแบบคือ NPCR สูงกว่า 90 เปอร์เซ็นต์ และ UACI ต่ำกว่า 33 เปอร์เซ็นต์ และมีค่า PSNR และ Entropy ได้มาตรฐานการออกแบบระบบเข้ารหัสลับ และได้เปรียบเทียบระนาบบิตของรูปภาพดิจิตอลลับระหว่างโครงสร้างที่ 4 [12] ดังรูปที่ 4.14



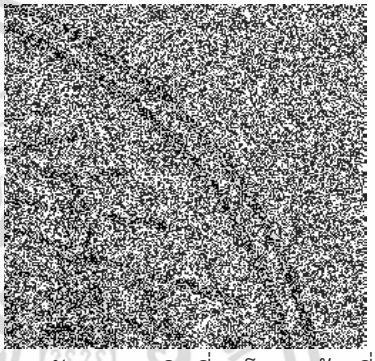
(ก) รูปภาพลับระนาบบิตที่ 0 [12]



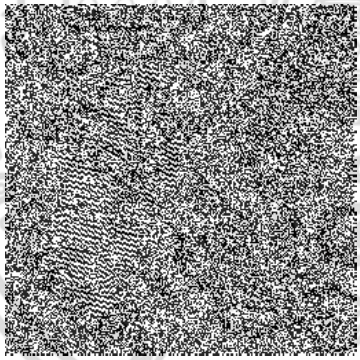
(ข) รูปภาพลับระนาบบิตที่ 0 โครงสร้างที่นำเสนอ



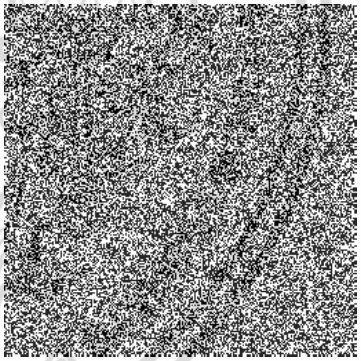
(ค) รูปภาพลับระนาบบิตที่ 1 [12]



(ง) รูปภาพลับระนาบบิตที่ 1 โครงสร้างที่นำเสนอ

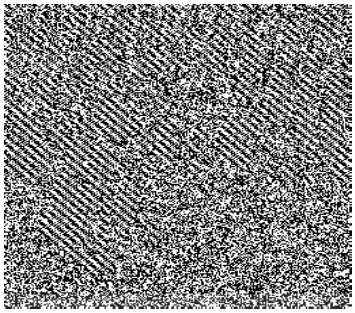


(จ) รูปภาพลับระนาบบิตที่ 2 [12]

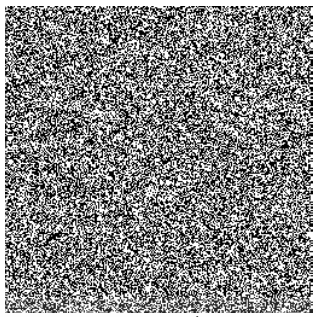


(ฉ) รูปภาพลับระนาบบิตที่ 2 โครงสร้างที่นำเสนอ

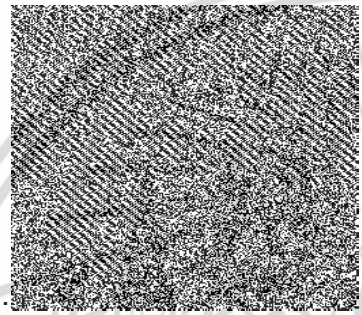
รูปที่ 4.14 ระนาบบิตรูปภาพลับแต่ละระนาบเปรียบเทียบโครงสร้างที่ 4 [12]



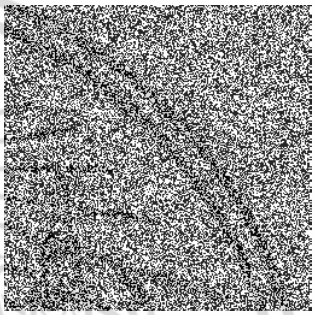
(ช) รูปภาพลับระนาบบิตที่ 3 [12]



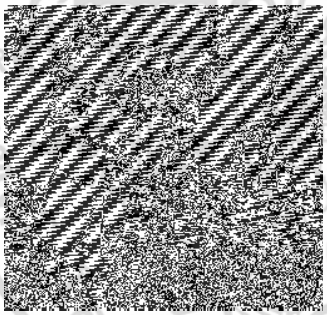
(ซ) รูปภาพลับระนาบบิตที่ 3 โครงสร้างที่นำเสนอ



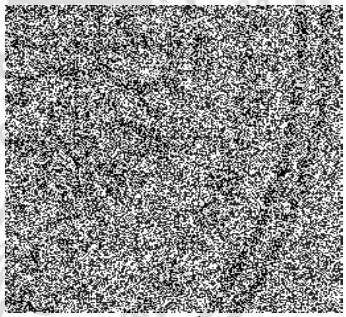
(ฌ) รูปภาพลับระนาบบิตที่ 4 [12]



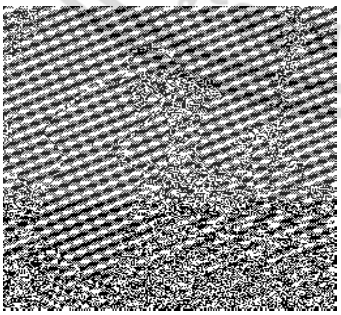
(ญ) รูปภาพลับระนาบบิตที่ 4 โครงสร้างที่นำเสนอ



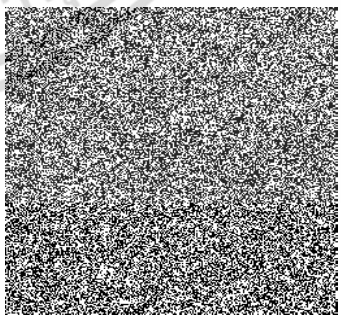
(ฐ) รูปภาพลับระนาบบิตที่ 5 [12]



(ฑ) รูปภาพลับระนาบบิตที่ 5 โครงสร้างที่นำเสนอ

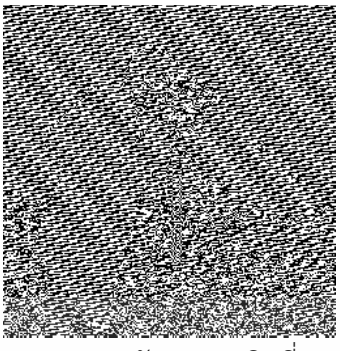


(ฒ) รูปภาพลับระนาบบิตที่ 6 [12]

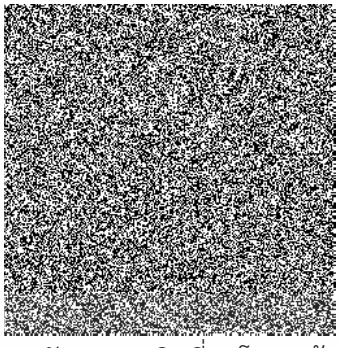


(ณ) รูปภาพลับระนาบบิตที่ 6 โครงสร้างที่นำเสนอ

รูปที่ 4.14 (ต่อ) ระนาบบิตรูปภาพลับแต่ละระนาบเปรียบเทียบโครงสร้างที่ 4 [12]



(ด) รูปภาพลับระนาบบิตที่ 7 [12]



(ต) รูปภาพลับระนาบบิตที่ 7 โครงสร้างที่นำเสนอ

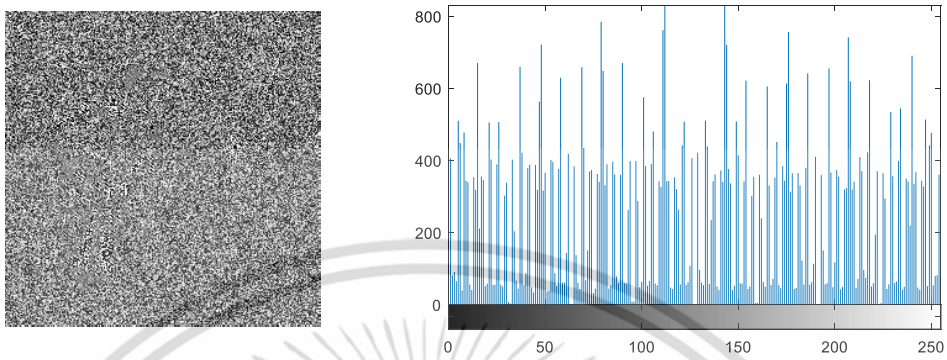
รูปที่ 4.14 (ต่อ) ระนาบบิตรูปภาพลับแต่ละระนาบเปรียบเทียบโครงสร้างที่ 4 [12]

จากรูปที่ 4.14 สามารถแสดงความสัมพันธ์พิกเซลใกล้เคียงแนวนอนของแต่ละระนาบบิตเปรียบเทียบกันได้ดังตารางที่ 4.13

ตารางที่ 4.13 ผลลัพธ์การเปรียบเทียบความสัมพันธ์พิกเซลใกล้เคียงแนวนอนของแต่ละระนาบบิตของโครงสร้างที่นำเสนอกับโครงสร้าง [12]

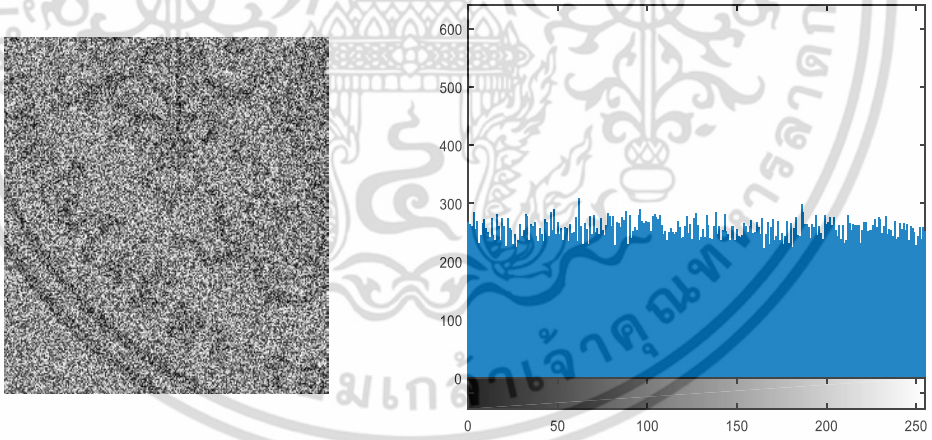
อันดับระนาบบิต	โครงสร้างที่ 4 [12]	โครงสร้างที่นำเสนอ
ระนาบบิตที่ 1	0.003056	-0.00922
ระนาบบิตที่ 2	0.051814	0.006432
ระนาบบิตที่ 3	0.159043	-0.00149
ระนาบบิตที่ 4	0.218385	0.002906
ระนาบบิตที่ 5	0.069204	-0.000683
ระนาบบิตที่ 6	-0.0106	-0.00646
ระนาบบิตที่ 7	-0.0129	0.003329
ระนาบบิตที่ 8	0.106336	-0.000582

จากผลลัพธ์ตารางที่ 4.13 จะเห็นได้ว่า โครงสร้างที่นำเสนอได้สร้างระนาบบิตกุญแจที่มีความซับซ้อนกว่าโครงสร้างที่ 4 [12] เพราะมีค่าที่เข้าใกล้ 0 มากกว่า นอกจากนี้ได้ทดสอบกุญแจด้วยกุญแจที่เป็นอักขระเดียวกันหมดทั้ง 16 ตัว คือ “AAAAAAAAAAAAAAAA” โดยโครงสร้างที่ 4 [12] มีค่าฮีสโทแกรมที่มีค่าที่แตกต่างจากสัญญาณรบกวนดังรูปที่ 4.15



รูปที่ 4.15 ข้อมูลลับเมื่อใช้กุญแจลับด้วยค่าเดียวกันทั้งหมด 16 อักขระ “AAAAAAAAAAAAAAAA” ของโครงสร้างที่ 4 [12]

จากรูปที่ 4.15 จะเห็นได้ว่าฮีสโทแกรมมีลักษณะที่สามารถวิเคราะห์ทางสถิติได้ซึ่งถือว่าเป็นข้อมูลลับที่ไม่ดีพอต่อการใช้งาน ส่วนโครงสร้างที่นำเสนอนั้นมีข้อมูลลับที่แตกต่างดังรูปที่ 4.16



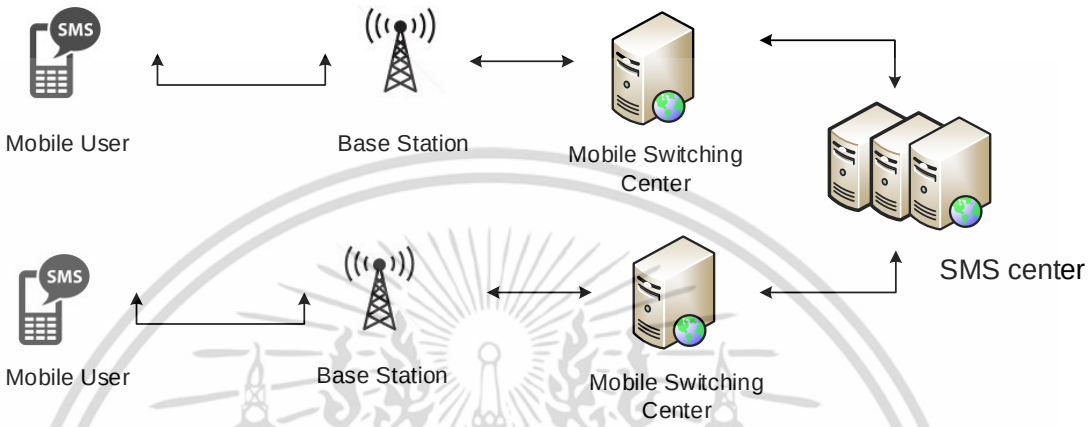
รูปที่ 4.16 ข้อมูลลับเมื่อใช้กุญแจลับด้วยค่าเดียวกันทั้งหมด 16 อักขระ “AAAAAAAAAAAAAAAA” ของโครงสร้างที่นำเสนอ

จากรูปที่ 4.16 จะเห็นว่าข้อมูลลับมีลักษณะที่ยังคงเหมือนสัญญาณรบกวนอยู่ ซึ่งถือว่ายังเป็นข้อมูลลับที่ดี

4.4 การประยุกต์ใช้งาน

4.4.1 การรับส่งข้อความสั้น

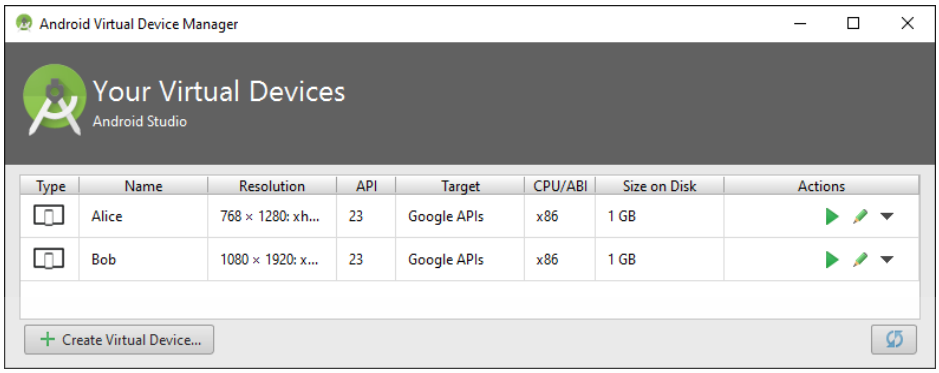
การรับส่งข้อความสั้นจะสื่อสารแบบไร้สารผ่านระบบ GSM มีโครงสร้างดังรูปที่ 4.17



รูปที่ 4.17 สถาปัตยกรรมการรับส่งข้อความสั้น (SMS)

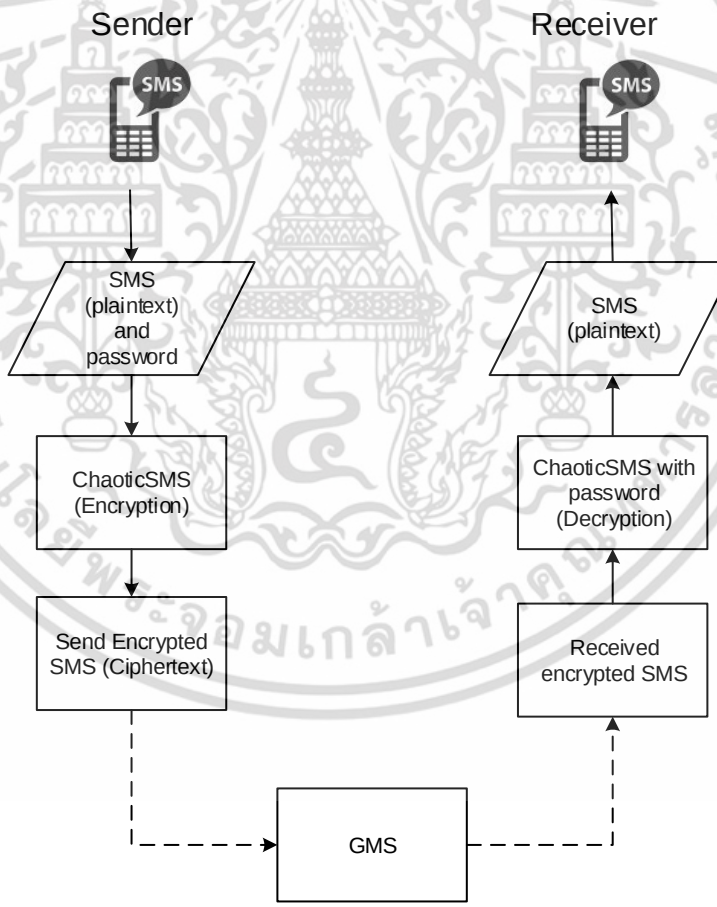
จากรูปที่ 4.17 เป็นการรับส่งข้อมูลระหว่าง 2 ผู้ใช้บริการ คือผู้ส่งข้อความสั้นและผู้รับข้อความสั้น โดยส่งผ่านสถานีส่ง ต่อด้วยตัวกระจายข้อมูล (MSC: Mobile Switching Center) และไปที่ศูนย์จัดการข้อความสั้น (SMS center) ในกรณีที่ ผู้รับข้อความสั้นปลายทางปิดโทรศัพท์เคลื่อนที่ไว้ ข้อความสั้นนั้นก็ยังจัดเก็บรักษาไว้ที่ ศูนย์จัดการข้อความสั้น (SMS center) จนกว่าปลายทางหรือผู้รับข้อความสั้นนั้นเปิดเครื่อง ข้อความสั้นที่เก็บไว้ที่ศูนย์กลางก็ถูกส่งไปยังเครื่องปลายทาง และลบข้อความสั้นนั้นทิ้ง

สำหรับการประยุกต์รับส่งข้อความสั้นนั้น ได้สร้างสมาร์ทโฟนจำลองเพื่อใช้รับและส่งข้อความลับ และมีงานวิจัยที่ได้ประยุกต์การเข้ารหัสกับการรับส่งข้อมูลความสั้น [21-23] สำหรับการประยุกต์โครงสร้างที่นำเสนอนี้จะสร้างแอปพลิเคชันผ่านโปรแกรม Android Studio ซึ่งเป็นโปรแกรมสำหรับนักพัฒนาแอปพลิเคชัน แสดงชื่อเครื่องได้ดังรูปที่ 4.18



รูปที่ 4.18 สมาร์ทโฟนที่จำลองเพื่อใช้ในการทดลอง

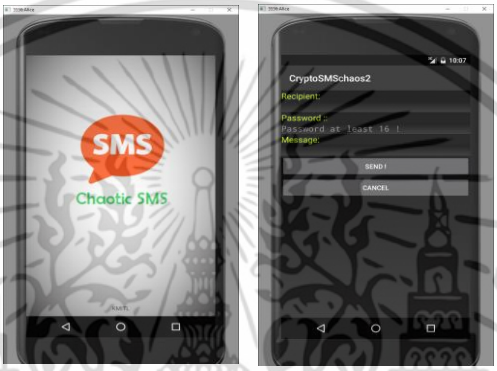
และการออกแบบแอปพลิเคชันเข้ารหัสลับข้อความสั้น ได้ดังรูปที่ 4.19



รูปที่ 4.19 ออกแบบแอปพลิเคชันเข้ารหัสลับข้อความสั้น

จากรูปที่ 4.19 ผู้ส่งข้อความลับ (Sender) เริ่มต้นพิมพ์ข้อความสั้นผ่านช่องรับข้อความของโปรแกรม พร้อมรหัสผ่าน 16 อักขระ หลังจากนั้นระบบได้ส่งข้อความสั้นที่ได้รับการเข้ารหัสผ่านเครือข่ายไปส่งปลายทาง โดยที่ตลอดการสื่อสาร ข้อความสั้นนั้นยังคงเข้ารหัสลับไว้อยู่ จนกระทั่งผู้รับข้อความสั้น (Receiver) ได้ใส่รหัสผ่านในแอปพลิเคชันเพื่อกู้ข้อความสั้นนั้นกลับคืนมา

ทดสอบจำลองสมาร์ทโฟนของ Alice และ Bob ทดลองส่งข้อความสั้นจาก Alice ไปหา Bob ได้ดังรูปที่ 4.20 โดยมีหน้าต่างแสดงผลดังรูปที่ 4.21

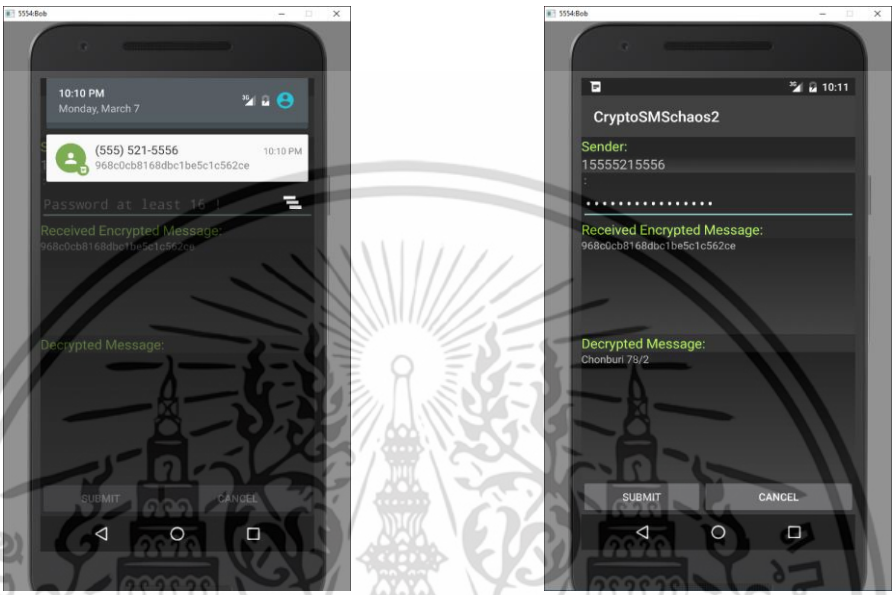


รูปที่ 4.20 หน้าต่างแสดงผลแอปพลิเคชันการรับส่งข้อความสั้น (Chaotic SMS)

รูปที่ 4.21 หน้าต่างผู้ใช้แสดงเพื่อใส่รายละเอียดการส่ง

จากรูปที่ 4.20 และ 4.21 ผู้ใช้สามารถกำหนดหมายเลขปลายได้ นั้นคือ ‘5554’ พร้อมกำหนดรหัสลับ 16 ตัวอักขระคือ ‘qwertyuiopasdfgh’ และเนื้อหาข้อความสั้นที่ต้องการส่ง ‘Chonburi 78/2’ และมีปุ่มกดรับคำสั่ง สองคำสั่งคือส่งและยกเลิก เมื่อกดส่งข้อความสั้นลับนั้นจะถูกส่งออกไปทันทีให้ปลายทาง ซึ่งในการใช้งานบนสมาร์ทโฟนจริง ข้อความสั้นจะถูกส่งไปยัง เครือข่ายผู้ให้บริการจัดเก็บไว้ที่

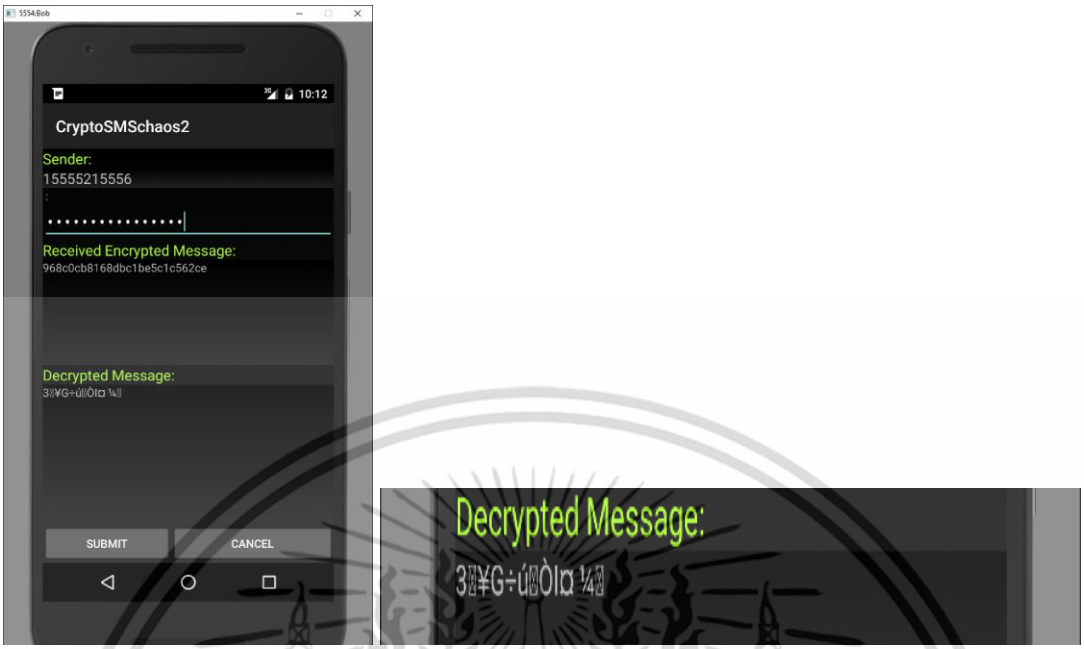
SMSC ก่อนเพื่อส่งต่อไปให้ปลายทาง ข้อความลับจะถูกเก็บไว้ยัง SMSC จนกว่าปลายทางจะเปิดใช้บริการเครือข่าย เมื่อข้อความลับย้ายจาก SMSC ไปยังเครื่องปลายทาง แอปพลิเคชันที่เครื่องปลายทางจะทำงานทันที ดังรูปที่ 4.22



(ก) (ข)

รูปที่ 4.22 ทดสอบการส่งข้อความสั้นผ่านแอปพลิเคชัน (ก) แอปพลิเคชันการรับข้อความสั้นพื้นฐาน (ข) แอปพลิเคชันการรับข้อความสั้นที่นำเสนอ

จากรูปที่ 4.22 (ก) เป็นแอปพลิเคชันพื้นฐานการรับส่งข้อความสั้น ซึ่งยังคงทำงานได้ตามปกติ ส่วนรูปที่ 4.22 (ข) เป็นแอปพลิเคชันที่ได้นำเสนอ โดยหน้าต่างแสดงข้อความลับนั้นจะประกอบไปด้วยหมายเลขต้นทางของผู้ส่งข้อความสั้น และช่องใส่รหัสผ่านจำนวน 16 อักขระ และช่องแสดงผลข้อความลับ ซึ่งยังไม่มีการแสดงผลใด เกิดขึ้นจนกว่าจะใส่รหัสลับทั้ง 16 ตัว แล้วกดยืนยัน (Submit) ทั้งนี้ทั้งนั้นได้ทำการทดลองโดยใส่รหัสลับที่ไม่ตรงลงไป แล้วถอดรหัสพบว่าข้อความลับนั้นไม่สามารถกู้คืนมาได้ดังเดิม ดังรูปที่ 4.23

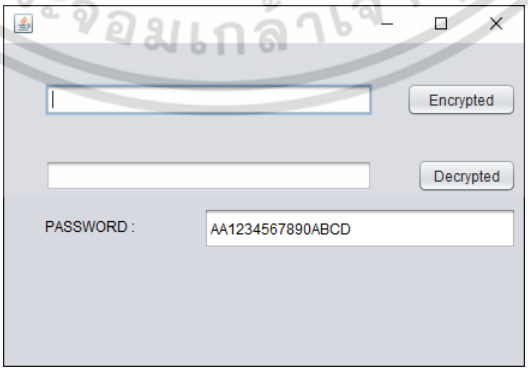


รูปที่ 4.23 หน้าต่างผู้ใช้แสดงการถอดรหัสด้วยกุญแจที่ผิด

จากรูปที่ 4.23 แสดงผลหน้าต่างผู้ใช้แสดงการถอดรหัสด้วยกุญแจที่ผิด คือส่งด้วยกุญแจ ‘qwertyuiopasdfgh’ แต่ถอดด้วย ‘qwertyuiopasdfgg’ ที่แตกต่างไป จึงถือเป็นผลที่น่าพอใจเป็นอย่างมาก

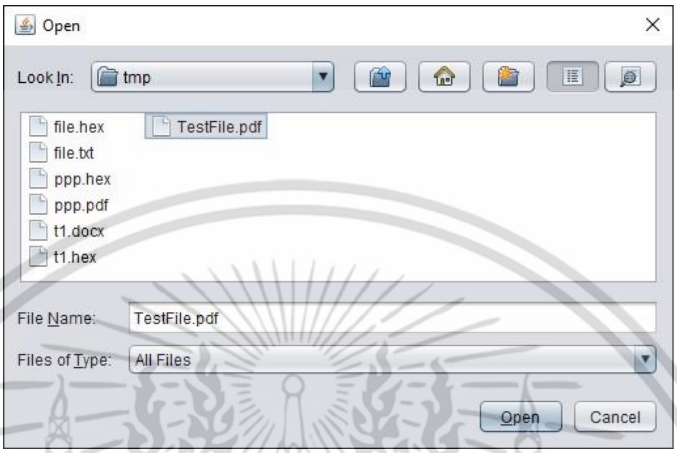
4.4.2 การเข้ารหัสลับไฟล์

ทดสอบบนคอมพิวเตอร์ระบบปฏิบัติการ Window10 สร้างแอปพลิเคชันจากภาษาจาวาโดยใช้โปรแกรม Netbean ออกแบบหน้าต่างที่ติดต่อผู้ใช้งาน โดยมีโครงสร้างหน้าต่างดังรูปที่ 4.24



รูปที่ 4.24 หน้าต่างหน้าโปรแกรมเข้ารหัสลับไฟล์คอมพิวเตอร์

หน้าต่างโปรแกรมประกอบไปด้วยส่วนเข้ารหัสลับไฟล์ ส่วนกำหนดรหัสลับ และส่วนถอดรหัสลับ ในส่วนเข้ารหัสลับสามารถเลือกไฟล์คอมพิวเตอร์ได้ทุกชนิดไฟล์หน้าต่างโปรแกรมแสดงดังรูปที่ 4.25



รูปที่ 4.25 หน้าต่างเลือกไฟล์คอมพิวเตอร์เพื่อเข้ารหัสลับ

สามารถเข้ารหัสไฟล์ใดก็ได้ ยกตัวอย่างเช่น ไฟล์ “TestFile.pdf” ในรูปที่ 4.26 ซึ่งเป็นไฟล์ชนิด PDF ที่มีขนาด 41KB มีค่าแต่ละไบต์ตามรูปที่ 4.27

รูปที่ 4.26 ไฟล์ชนิด PDF ที่ใช้ในการทดลอง

```
25 50 44 46 2D 31 2E 35 0D 0A 25 B5 B5 B5 B5 0D      %PDF-1.5..%µµµµ.
0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70      .1 0 obj..<</Typ
65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20      e/Catalog/Pages
32 20 30 20 52 2F 4C 61 6E 67 28 74 68 2D 54 48      2 0 R/Lang(th-TH
29 20 2F 53 74 72 75 63 74 54 72 65 65 52 6F 6F      ) /StructTreeRoo
74 20 31 31 20 30 20 52 2F 4D 61 72 6B 49 6E 66      t 11 0 R/MarkInf
6F 3C 3C 2F 4D 61 72 6B 65 64 20 74 72 75 65 3E      o<</Marked true>
3E 3E 3E 0D 0A 65 6E 64 6F 62 6A 0D 0A 32 20 30      >>>..endobj..2 0
```

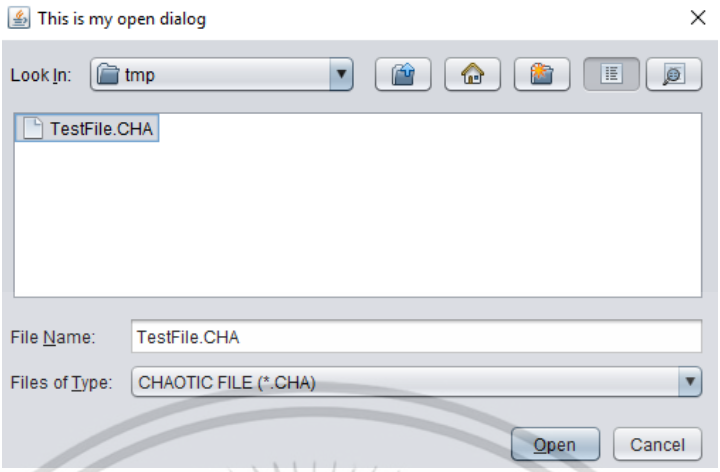
รูปที่ 4.27 ไฟล์ในรูปแบบเลขฐานสิบหก 256 ไบต์

รูปที่ 4.27 เป็นส่วน 256 ไบต์แรกของข้อมูลไฟล์ต้นฉบับ (TestFile.pdf) เมื่อเข้ารหัสลับร่วมกับเข้ารหัสลับกับกุญแจที่มีขนาด 128 บิต หรือ 16 อักขระ คือ ‘AA1234567890ABCD’ ทำให้ได้ไฟล์ลับออกมาเป็นไฟล์กำหนดนามสกุลคือ CHAOTIC FILE (.CHA) มีค่าแต่ละไบต์ตามรูปที่ 4.28

```
20 55 41 43 28 34 2B 30 08 0F 20 B0 B0 B0 B0 08       UAC(4+0.. °°°°.
0F 34 25 35 25 6A 67 6F 08 0F 39 39 2A 51 7C 75      .4%5%jgo..99*Q|u
60 2A 46 64 71 64 69 6A 62 2A 55 64 62 60 76 25      `*Fdqdijb*Udb`v%
37 25 35 25 57 2A 49 64 6B 62 2D 71 6D 28 51 4D      7%5%W*Idkb-qm(QM
2C 25 2A 56 71 77 70 66 71 51 77 60 60 57 6A 6A      ,%*VqwpfqQw``Wjj
71 25 34 34 25 35 25 57 2A 48 64 77 6E 4C 6B 63      q%44%5%W*HdwnLkc
6A 39 39 2A 48 64 77 6E 60 61 25 71 77 70 60 3B      j99*Hdwn`a%qwp`;
3B 3B 3B 08 0F 60 6B 61 6A 67 6F 08 0F 37 25 35      ;;;..`kajgo..7%5
```

รูปที่ 4.28 ไฟล์ลับในรูปแบบเลขฐานสิบหก 256 ไบต์

จากรูปที่ 4.28 ได้แสดงค่า 256 ไบต์ของข้อมูลไฟล์ลับออกมาในรูปแบบเลขฐานสิบหก ซึ่งแต่ละไบต์มีค่าแตกต่างจากข้อมูลไฟล์ต้นฉบับ ในส่วนการถอดรหัสลับไฟล์หรือการกู้ข้อมูลไฟล์กลับคืนมานั้น ก็เช่นเดียวกันนั่นคือเลือกไฟล์ลับที่ต้องการจะถอดรหัสลับกลับคืนมา จะต้องเลือกไฟล์นามสกุล CHAOTIC FILE (.CHA) เท่านั้น ดังรูปที่ 4.29



รูปที่ 4.29 หน้าต่างเลือกไฟล์ลับคอมพิวเตอร์เพื่อถอดรหัสลับ

เมื่อเลือกไฟล์คอมพิวเตอร์ลับที่ต้องการจะถอดรหัสลับหรือกู้คืนแล้วนั้น ต้องกำหนดรหัสผ่านให้ตรงกับรหัสผ่านที่ได้เข้ารหัสลับไว้ก่อนหน้านี้เท่านั้น ในกรณีที่รหัสผ่านไม่ตรงแม้แต่เพียงบิตเดียวก็ไม่สามารถถอดรหัสไฟล์ลับให้ได้ข้อมูลไฟล์ต้นฉบับกลับคืนมา สุดท้ายเมื่อได้ไฟล์ลับมาแล้วก็สามารถนำไฟล์นั้นไปจัดเก็บไว้ที่ไหนก็ได้ โดยเฉพาะอย่างยิ่งบนคลังเก็บข้อมูลสาธารณะ จากผลการประยุกต์ใช้งานจะเห็นได้ว่าโครงสร้างที่นำเสนอสามารนำมาประยุกต์ใช้งานได้อย่างมากมายและเหมาะสำหรับอุปกรณ์ทุกประเภท

บทที่ 5

สรุปผล

5.1 สรุปผลการทดลอง

งานวิจัยนี้นำเสนอการเข้ารหัสลับเนื้อหาสื่อประสมที่ประกอบไปด้วยข้อมูลรูปภาพดิจิตอล ข้อมูลเสียง และข้อความ เป็นการเข้ารหัสลับชนิดบล็อคร่วมกับกุญแจลับส่วนตัวหรือที่เรียกว่ากุญแจสมมาตร โดยใช้การเกิดเคออสในวงจรกรองสัญญาณดิจิตอล IIR อันดับที่สองมาสร้างกุญแจลับ ขั้นตอนในส่วนของการสร้างกุญแจลับเกิดจากการกำหนดรหัสผ่านอักขระจำนวน 16 อักขระ เพื่อสร้างค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอล 2 ตัว โดยค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลจะต้องทำให้วงจรกรองสัญญาณนั้นมีความไร้เสถียรภาพและไม่เป็นเชิงเส้น ความไร้เสถียรภาพสามารถทำได้โดยบังคับให้ค่าสัมประสิทธิ์วงจรกรองสัญญาณดิจิตอลอย่างน้อย 1 ตัวอยู่นอกสามเหลี่ยมเสถียรภาพ และความไม่เป็นเชิงเส้นสามารถเกิดขึ้นได้ด้วยความคลาดเคลื่อนการล้นของการบวกตัวเลขส่วนเติมเต็มสอง ค่าสัญญาณขาออกจากวงจรกรองสัญญาณจะถูกปรับค่าให้มีค่าเป็น 0 และ 1 เพื่อนำมาสร้างเป็นกุญแจระนาบบิตโดยจะมีวงจรกรองสัญญาณดิจิตอลทั้งหมด 8 ชุดเพื่อสร้างกุญแจระนาบบิตทั้งหมด 8 ระนาบบิต ให้กับระบบเข้ารหัสลับ ในส่วนของข้อมูลต้นฉบับจะทำการแยกระนาบบิตออกเป็น 8 ระนาบบิตเช่นกัน หลังจากนั้นนำระนาบบิตของกุญแจและข้อมูลต้นฉบับทั้ง 8 ระนาบบิตมาดำเนินการทางลอจิกด้วย XOR (Exclusive or) จะทำให้ได้ระนาบบิตของข้อมูลลับทั้งหมด 8 ระนาบบิต สุดท้ายนำระนาบบิตข้อมูลลับที่ได้แต่ละระนาบบิตมารวมกันเป็นข้อมูลลับที่ใช้ในการสื่อสาร

การทดลองได้ทดลองเนื้อหาสื่อประสมทั้งหมดสามชนิดข้อมูล คือ ข้อมูลชนิดรูปภาพดิจิตอล ข้อมูลชนิดเสียง และข้อมูลชนิดข้อความ มาเข้ารหัสลับ ในส่วนการวัดประสิทธิภาพของระบบเข้ารหัสลับนั้นได้เลือกวัดผลกับข้อมูลชนิดรูปภาพดิจิตอลเป็นหลักเพราะข้อมูลชนิดนี้มีความทนทานต่อการถอดรหัสลับจากการโจมตีแบบตะลุยของแฮกเกอร์ได้ง่ายที่สุดเพราะค่าพิกเซลใกล้เคียงมีค่าที่คล้ายกันมาก จึงทำให้โครงสร้างเข้ารหัสลับรูปภาพดิจิตอลที่มีประสิทธิภาพมาก จะส่งผลให้เข้ารหัสลับข้อความและเสียงมีประสิทธิภาพมากด้วยเช่นกัน ตัวแปรที่ใช้ในการวัดประสิทธิภาพจะประกอบไปด้วย ความไวของกุญแจ (Key Sensitivity) ความไวของข้อมูลต้นฉบับ (Plaintext Sensitivity) ในรูปแบบของค่า NPCR และ UACI อัตราสัญญาณต่อสัญญาณรบกวน (Peak Signal-to-Noise Ratio) ค่าเอนโทรปีข้อมูล (Information Entropy) ค่าสหสัมพันธ์ (Correlation Coefficient) วัดทั้ง 3 แนวของพิกเซลใกล้เคียงคือ แนวนอน แนวตั้ง และแนวทแยง และการรับรู้ข้อมูลลับด้วยการมอง (Perceptual Security)

จากผลลัพธ์การทดลองวัดประสิทธิภาพของระบบเข้ารหัสลับที่ได้นำเสนอเปรียบเทียบกับโครงสร้างเข้ารหัสลับแบบอื่น ทั้งหมด 4 โครงสร้าง คือ โครงสร้างที่เข้ารหัสลับโดยใช้เคออติกแมพแบบแคทเมพเท่านั้น [4] โครงสร้างที่เข้ารหัสลับแบบสลับค่าและแปลงค่าโดยใช้เคออติกแมพ [9] โครงสร้างที่เข้ารหัสลับโดยใช้เคออสในวงจรกรองสัญญาณดิจิตอล [11] และโครงสร้างที่เข้ารหัสลับด้วยการประมวลผล XOR ของแต่ละระนาบบิตข้อมูลและเพิ่มระบบสร้างกุญแจลับแบบ 16 อักขระมาสร้างกุญแจระนาบบิตที่เป็นเคออสจาก sine และ cosine แมพ ผลลัพธ์ที่ได้คือ ความไวของกุญแจและความไวของข้อมูลต้นฉบับ มีค่าที่สูงกว่าโครงสร้าง [4], [7] และ [11] และการรับรู้ของเนื้อหารูปภาพดิจิตอลลับแตกต่างจากข้อมูลต้นฉบับไปอย่างมากอยู่ในระดับ QL2 และที่สำคัญเมื่อเปรียบเทียบกับโครงสร้าง [12] ที่มีการสร้างกุญแจจากอักขระ 16 อักขระ จะเห็นได้ว่าข้อมูลลับที่ได้จากโครงสร้างที่นำเสนอมีค่า ฮีสโทแกรมที่ดีกว่า และค่าความสัมพันธ์ระหว่างพิกเซลใกล้เคียงของข้อมูลลับแต่ละระนาบบิตมีค่าความสัมพันธ์ที่ต่ำกว่าโครงสร้าง [12] ซึ่งถือว่าโครงสร้างการเข้ารหัสลับที่นำเสนอนี้เป็นระบบที่สามารถนำมาใช้ในการเข้ารหัสลับข้อมูลสื่อประสมได้เป็นอย่างดี นอกจากนี้แล้วยังได้แสดง การประยุกต์ใช้งาน คือ ประยุกต์ใช้งานบนสมาร์ทโฟนเพื่อเข้ารหัสลับข้อความสั้น (Chaotic SMS) และประยุต์ใช้งานบนคอมพิวเตอร์ด้วยภาษาจาวาเพื่อเข้ารหัสลับไฟล์คอมพิวเตอร์ได้ทุกชนิด เพื่อสามารถจัดเก็บไฟล์คอมพิวเตอร์นั้นไว้ได้อย่างปลอดภัย

5.2 ข้อเสนอแนะ

ระบบเข้ารหัสลับที่นำเสนอนี้สามารถเพิ่มการตรวจสอบความถูกต้องของข้อมูล (cryptography checksum) และนำไปประยุกต์ใช้งานได้อีกมากมาย อาทิเช่น การเข้ารหัสลับแบบสตรีมของระบบกล้องวงจรปิด การประชุมทางไกลผ่านระบบวีดีโอ การกระจายเสียงผ่านเครือข่ายสาธารณะ

เอกสารอ้างอิง

[1] National Institute of Standard and Technology (NIST), Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication (FIPS PUB) 140- 1.Gaithersburg, MD:NIST, 2001.

[2] B. Furht, Handbook of Internet and Multimedia System and Applications. Boca Raton, FL:CRC Press., 1999.

[3] S. Lian, MULTIMEDIA CONTENT ENCRYPTION Techniques and Application, Taylor & Francis Group 1-199, 2009.

[4] M. George, A. Ioannis, “Cryptography with chaos” Proceeding of 5th Chaotic Modeling and simulation International Conference, Athens Greece, 12-15 June 2012.

[5] J. C. Yen and J. I. Guo, "A new chaotic key-based design for image encryption and decryption", Proceedings of IEEE International Symposium on Circuits and Systems, vol. 4, pp. 49-52

[6] L. Zhang, X. Liao and X. Wang, "An image encryption approach based on chaotic maps", Chaos Solitons and Fractals, vol. 24, no. 3, pp. 759-765, 2005

[7] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps”, Int. J. Bifurcation Chaos, vol. 8, no. 6, pp. 1259-1284,1998.

[8] J. Chen,Z. liang,C. Fu, H. Yu, “An improved permutation diffusion type image cipher with chaotic orbit perturbing mechanism”, OPTIC EXPRESS 27873, Vol.21, No.23,Published:13 Nov 2013.

[9] S. Sukalyan, K. Atanu, “Confusion and diffusion of grayscale image using multiple chaotic maps”, National Conference on Computing and Communication System (NCCCS), 2012.

[10] L. O. Chua, T. Lin, "Chaos in digital filters," IEEE Trans. Circuits Systs., vol. 35, no. 6, pp. 648-658, June 1998.

[11] C. Roeksukrungrueang, X. Dittaphong, K. Khongsomboon, N. Panyanouyong, S. Chivapreecha, “Chaotic encoder-decoder on FPGA for crypto system”, Asia-Pacific Signal and Information Processing Association (APSIPA), P1-5, Dec2014.

เอกสารอ้างอิง (ต่อ)

[12] S.Maksuanpan,T. Veerawadtanapong, W.San-Um "Robust digital image cryptosystem based on nonlinear of compound sine and cosine chaotic maps for private data protection" ICACT Transactions on Advanced Communications Technology (TACT) Vol. 3, Issue 2, March 2014

[13] S.A. Vanstone A.J. Menezes, and P.C. Oorschor, Handbook of Applied Cryptography. Baca Raton, FL:CRC Press, 1996.

[14] S. Lian,J. Sun, Z. Wang, “Security analysis of A Chaos-based image encryption algorithm”, Phisica A Elsevier Science, 2005.

[15] Y. Wu, Joseph P. Noonan, S. Agaian, "NPCR and UACI randomness tests for image encryption", Department of Electrical and Computer Engineering Tufts University Medford, MA, USA, 2011.

[16] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", Proc. CRYPTO—Adv. Cryptol., vol. 537, pp. 2-21, 1990

[17] H. M. Al-Otum, "Qualitative and quantitative image quality assessment of vector quantization, JPEG, and JPEG2000 compressed images," Journal of Electronic Imaging, vol. 12, no. 3, pp. 511-521, 2003

[18] C. Shannon, Communication Theory of Secret System, Bell system Technical Journal 28:656-715.1949

[19] Brute Force Calculator, Open Security Research Sponsored by Found stone http://calc.opensecurityresearch.com/

[20] S. Liu, J. Sun, Z. Xu “An improved image encryption algorithm based on chaotic system”, Journal of Computers, vol. 4, no. 11, 2009, pp.1091-1100.

[21] M. patil, V. Sahu, A. Jain "SMS text compression and encryption on Android O.S", International Conference on Computer Communication and Informatics (ICCCI - 2014), Jan. 03 – 05, 2014, Coimbatore, INDIA

[22] M. Mishra, V.H. Mankar, "Message embedded cipher using 2-d chaotic map", International Journal of Chaos, Control, Modelling and Simulation (IJCCMS) Vol.1, No.1, July 2012

เอกสารอ้างอิง (ต่อ)

[23] S. Ariffin, R.Mahmod, R.Rahmat, N.A. Idris, "SMS encryption using 3D-AES block cipher on Android message application", International Conference on Advanced Computer Science Applications and Technologies,2013, pp.310-314.

[24] ลัญฉกร วุฒิสิทธิกุลกิจ, ธงชัย โรจน์กังสดาล, วรากร ศรีเชวงทรัพย์, นพดล พรมภักษร “วิทยาการเข้ารหัสลับเบื้องต้น Introduction to Cryptography” จุฬาลงกรณ์มหาวิทยาลัย, 2548.

ประวัติผู้เขียน

ชื่อ-นามสกุล นายนครินทร์ รณรงค์ฤทธิ์

วัน เดือน ปีเกิด 11 พฤศจิกายน 2530 ที่อุตรดิตถ์

ที่อยู่ 73/1 หมู่ที่ 1 ตำบลเด่นเหล็ก
อำเภอน้ำปาด จังหวัดอุตรดิตถ์

ประวัติการศึกษา

พ.ศ.2554 วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโทรคมนาคม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ประสบการณ์การทำงานและผลงานวิจัย

พ.ศ.2558 นำเสนอผลงาน “An Improved Digital Image Encryption Using Chaos in Digital Filter” ในการประชุมวิชาการ The 2015 International Symposium on Multimedia and Communication Technology (ISMAC 2015)