การพัฒนาโปรแกรมประยุกต์บนระบบแอนดรอยด์ เพื่อการเข้ารหัสรูปภาพดิจิตอลด้วยสัญญาณอลวน

The Development of Android Application Software for Digital Image Encryption using Chaotic Signals

ศิวพงษ์ นิลวงษ์ 54113025-8

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีไทย-ญี่ปุ่น
ปีการศึกษา 2557

หัวข้อปริญญานิพนธ์	การพัฒนาโปรแกรมประยุกต์บนระบบแอนดรอยด์เพื่อการเข้ารหัสรูปภาพดิจิตอลด้วยสัญญาณอลวน
โดย	ศิวพงษ์ นิลวงษ์ 54113025-8
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาปริญญานิพนธ์	ผู้ช่วยศาสตราจารย์ ดร.วิมล แสนอุ้ม

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีไทย-ญี่ปุ่น อนุมัติให้นับปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์
(ผู้ช่วยศาสตราจารย์ ดร.เลอเกียรติ์ วงศ์สารพิกูล)
วันที่.....เดือน.....พ.ศ.....

คณะกรรมการสอบปริญญานิพนธ์

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

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

อาจารย์ที่ปรึกษาปริญญานิพนธ์

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

ลิขสิทธิ์ของสถาบันเทคโนโลยีไทย-ญี่ปุ่น

การพัฒนาโปรแกรมประยุกต์บนระบบแอนดรอยด์ เพื่อการเข้ารหัสรูปภาพดิจิตอล ด้วยสัญญาณอลวน

นายศิวพงษ์ นิลวงษ์ 54113025-8

อาจารย์ที่ปรึกษาปริญญานิพนธ์ : ผศ.ดร.วิมล แสนอุ้ม

โครงงานนี้เป็นการศึกษาและพัฒนาโปรแกรมประยุกต์ (แอปพลิเคชัน) บนระบบแอนดรอยด์ เพื่อใช้ในการเข้ารหัส และถอดรหัสรูปภาพดิจิตอล โดยสามารถรับรูปภาพจากผู้ใช้งานด้วยการเลือกรูปภาพที่มีอยู่ในอุปกรณ์ที่ใช้ระบบแอนดรอยด์ของผู้ใช้ และสามารถเลือกที่จะเข้ารหัสหรือถอดรหัสรูปภาพที่ต้องการด้วยรหัสตัวเลขทศนิยมที่ผู้ใช้กำหนด โดยมีการพัฒนาเป็น 3 ขั้นตอนคือ การทดสอบระบบอลวนบน MATLAB เพื่อศึกษาการทำงานของระบบอลวน, การทดสอบระบบอลวนบนแอนดรอยด์, และการพัฒนาแอปพลิเคชันสำหรับเข้ารหัสและถอดรหัสรูปภาพ โดยประยุกต์ระบบอลวนในการสร้างสัญญาณอลวนสำหรับการเข้าและถอดรหัสรูปภาพ แอปพลิเคชันบนระบบแอนดรอยด์ที่พัฒนาขึ้น สามารถเข้ารหัสและถอดรหัสรูปภาพได้โดยสมบูรณ์ และสามารถนำรูปภาพผลลัพธ์ออกมาเป็นไฟล์รูปภาพนามสกุล .PNG ได้อีกด้วย

คำสำคัญ : โปรแกรมประยุกต์บนระบบแอนดรอยด์ / Chaotic map / การเข้ารหัสรูปภาพ

The Development of Android Application Software for Digital Image Encryption using Chaotic Signals

Sivapong Nilwong 54113025-8

Academic Advisor : Asst. Prof. Dr. Wimol San-Um

This project is the study and the development of the Android application software (Application) which can encrypt and decrypt the desired digital image through the desired password which are numbers with floating points. The development process consists of 3 processes. The first process is the selected chaotic system tested on MATLAB to study characteristics of the selected chaotic system. The second process is the implementation of the selected chaotic system on an Android as an Android application. Finally, the third process is the development of an Android application which can encrypt and decrypt digital images using the chaotic signal generated from the selected chaotic system. The developed Android application can encrypt and decrypt the digital image which is used in experiment successfully. Moreover, the developed Android application can also export the result from the application as a .PNG image file.

Keywords : Android application software / Chaotic map / Image encryption

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จได้ ด้วยความกรุณาของ ผู้ช่วยศาสตราจารย์ ดร.วิมล แสนอุ้ม อาจารย์ที่ปรึกษาปริญญานิพนธ์ ซึ่งได้ให้คำปรึกษา ข้อชี้แนะ และความช่วยเหลือในทุกด้านตลอดช่วงการจัดทำปริญญานิพนธ์ฉบับนี้จนกระทั่งสำเร็จลุล่วงไปได้ด้วยดี

ขอขอบพระคุณผู้ช่วยศาสตราจารย์ ดร.เลอเกียรติ์ วงศ์สารพิกูล คณบดีคณะวิศวกรรมศาสตร์ที่ได้อนุมัติให้ปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของ การศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต และขอขอบคุณ อาจารย์ รักษิต ชุติภักดีวงศ์ อาจารย์ประจำภาควิชาวิศวกรรมศาสตร์คอมพิวเตอร์ ที่ได้ให้คำแนะนำปริญญานิพนธ์ฉบับนี้ รวมทั้ง อาจารย์ ดร.กรกฎ เหมสถาปัตย์ ประธานสอบปริญญานิพนธ์ และผู้ช่วยศาสตราจารย์ ดร. วรากร ศรีเชวงทรัพย์ กรรมการสอบปริญญานิพนธ์และอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ ที่ให้คำแนะนำ และเสนอข้อคิดเห็นที่เป็นประโยชน์ต่อการปรับปรุงปริญญานิพนธ์ อีกทั้ง ขอกราบขอบพระคุณ คณาจารย์สถาบันเทคโนโลยีไทย-ญี่ปุ่นทุกท่าน ที่ให้ความรู้และคำแนะนำตลอดการศึกษาที่ผ่านมา

สุดท้ายนี้ กราบขอบพระคุณ มารดา ผู้ให้กำลังใจ ให้โอกาสในการศึกษาและทุนสนับสนุนในการทำปริญญานิพนธ์ จนกระทั่งเสร็จสมบูรณ์มา ณ ที่นี้ด้วย

ศิวพงษ์ นิลวงษ์

13 มีนาคม 2558

สารบัญ

บทที่		หน้า
	บทคัดย่อภาษาไทย	ค
	บทคัดย่อภาษาอังกฤษ	ง
	กิตติกรรมประกาศ	จ
	สารบัญ	ฉ
	สารบัญรูปภาพ	ซ
	สารบัญตาราง	ญ
1	บทนำ	1
	1.1 ความเป็นมาและความสำคัญของปัญหา	1
	1.2 วัตถุประสงค์ของโครงงาน	2
	1.3 ขอบเขตของการศึกษา	2
	1.4 ประโยชน์ที่คาดว่าจะได้รับ	2
	1.5 แผนงานและระยะเวลาในการดำเนินงาน	3
2	หลักการพื้นฐานและทฤษฎีที่เกี่ยวข้อง	4
	2.1 ระบบอลวน	4
	2.2 Chaotic map	4
	2.3 Android	6
	2.4 Java	7
	2.5 OpenCV	9
	2.6 Histogram (Image)	9
	2.7 Literature Review	10

สารบัญ (ต่อ)

3	ขั้นตอนการดำเนินงาน	13
	3.1 อุปกรณ์ที่ใช้ในการดำเนินงาน	13
	3.2 การทดลอง Chaotic map บน MATLAB	13
	3.3 การทดลอง Chaotic map บน Android	16
	3.4 การประยุกต์ Chaotic map กับการเข้ารหัสรูปภาพบน Android	19
	3.5 แอปพลิเคชัน Android ที่ใช้ในการเข้ารหัสภาพ	21
4	ผลการดำเนินงาน	27
	4.1 การทำงานของแอปพลิเคชันเข้ารหัส และถอดรหัสรูปภาพ	27
	4.2 วิเคราะห์รูปภาพผลลัพธ์ที่ได้จากการเข้ารหัสรูปภาพ	31
5	สรุปผลและวิเคราะห์ปัญหา	34
	5.1 สรุปผลการดำเนินงาน	34
	5.2 ปัญหาและอุปสรรค	34
	5.3 แนวทางการแก้ปัญหา	35
	5.4 ข้อเสนอแนะ และการพัฒนาในอนาคต	36
	บรรณานุกรม	37
	ภาคผนวก	38
	ก. Code ส่วนการเข้ารหัส และถอดรหัสรูปภาพ	39
	ข. Code ส่วนของ Chaotic map ที่ใช้ค่าไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์, การสร้างกุญแจเข้ารหัสรูปภาพ, และการสลับตำแหน่งพิกเซลของรูปภาพ	41
	ค. Code ส่วนการ XOR รูปภาพโดยใช้ Library OpenCV และส่วนการส่งออกผลลัพธ์เป็นรูปภาพ	44

สารบัญรูปภาพ

ภาพที่		หน้า
2.1	Bifurcation diagram ของ Logistic map	5
2.2	ตัวอย่างผลการใช้งาน OpenCV ในการหาคุณลักษณะของภาพ	9
2.3	ตัวอย่าง Histogram ของภาพ Grayscale	10
2.4	Chaotic map ที่ใช้ค่าความไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์ทั้ง 4 กรณี	11
2.5	ชุดสมการ Henon map	11
2.6	ผลที่ได้จากการเข้ารหัสและถอดรหัสรูปภาพในงานวิจัยก่อนหน้า	12
3.1	Chaotic waveforms ที่ได้จาก MATLAB ของสมการ (3.1)	14
3.2	Bifurcation Diagram ที่ได้จาก MATLAB ของสมการ (3.1)	15
3.3	LE Spectrum ที่ได้จาก MATLAB ของสมการ (3.1)	16
3.4	Chaotic waveforms ที่ได้จากแอปพลิเคชัน Android ของสมการ (3.1)	17
3.5	Bifurcation Diagram ที่ได้จากแอปพลิเคชัน Android ของสมการ (3.1)	18
3.6	LE Spectrum ที่ได้จากแอปพลิเคชัน Android ของสมการ (3.1)	18
3.7	แผนภาพขั้นตอนการสร้างกุญแจเข้ารหัสถาพ	19
3.8	ตัวอย่างกุญแจเข้ารหัสภาพ	20
3.9	แผนภาพขั้นตอนการสลับตำแหน่งพิกเซลของรูปภาพ	20
3.10	Interface ของแอปพลิเคชัน	21
3.11	Flow chart แสดงการทำงานของแอปพลิเคชัน	24
3.12	แผนผังการทำงานของส่วนการเข้ารหัส (a) และส่วนการถอดรหัส (b)	25
4.1	หน้าต่างของแอปพลิเคชัน หลังจากผู้ใช้เลือกรูปภาพที่ต้องการ	27
4.2	หน้าต่างของแอปพลิเคชัน หลังการเข้ารหัสรูปภาพเสร็จสิ้น	28
4.3	หน้าต่างของแอปพลิเคชัน หลังการเข้ารหัสรูปภาพล้มเหลว	29
4.4	หน้าต่างของแอปพลิเคชัน หลังการถอดรหัสรูปภาพเสร็จสิ้น และได้ภาพต้นฉบับ	30

สารบัญรูปภาพ (ต่อ)

4.5	หน้าต่างของแอปพลิเคชัน หลังการถอดรหัสล้มเหลว และไม่ได้ภาพต้นฉบับ	**30**
4.6	ตัวอย่างของรูปที่ถูกส่งออกมาจาก แอปพลิเคชันเข้ารหัสและถอดรหัสรูปภาพ	31
4.7	ภาพต้นฉบับที่ใช้ในการทดสอบแอปพลิเคชัน	31
4.8	ผลลัพธ์ที่ได้จากการเข้ารหัสรูปภาพ	32
4.9	Histogram ของภาพต้นฉบับ โดยที่ (a), (b), และ (c) คือ Histogram ของโทนสีแดง, เขียว, และน้ำเงิน ตามลำดับ	32
4.10	Histogram ของภาพที่ถูกเข้ารหัสแล้ว โดยที่ (a), (b), และ (c) คือ Histogram ของโทนสีแดง, เขียว, และน้ำเงิน ตามลำดับ	33
ก.1	ส่วนการเข้ารหัสรูปภาพ	40
ก.2	ส่วนการถอดรหัสรูปภาพ	40
ข.1	ส่วนของ Chaotic map ที่ใช้ค่าไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์	42
ข.2	ส่วนการสร้างกุญแจเข้ารหัสรูปภาพ	42
ข.3	ส่วนการสลับตำแหน่งพิกเซลของรูปภาพ	43
ค.1	ส่วนการ XOR รูปภาพด้วย Library OpenCV	45
ค.2	ส่วนการส่งออกผลลัพธ์เป็นรูปภาพ	45

สารบัญตาราง

ตาราง		หน้า
1.1	แผนและระยะเวลาในการดำเนินงาน	3
3.1	การตั้งค่าของ Android Virtual Device	23

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เนื่องจากปัจจุบันเป็นยุคของการสื่อสารข้อมูล ข้อมูลที่ถูกส่งในเครือข่ายต่างๆ โดยเฉพาะอินเทอร์เน็ต ซึ่งมีผู้ใช้งานจำนวนมาก และเกิดเหตุการณ์โจมตีทางข้อมูลบ่อยครั้ง ตั้งแต่อดีตจนถึงปัจจุบันมีวิธีการเข้ารหัสและถอดรหัสข้อมูล เพื่อรักษาความลับของข้อมูลหลายวิธี เช่น การเข้ารหัสแบบ Symmetric Key และ Asymmetric Key เป็นต้น

ทว่า ระบบการเข้ารหัสที่มีใช้อยู่ในปัจจุบัน มีโอกาสที่จะถูกดัก หรือโจรกรรมข้อมูลจากผู้ไม่ประสงค์ดี ที่ต้องการเข้าถึงข้อมูลที่เป็นความลับของเจ้าของข้อมูลนั้นๆ จึงควรมีวิธีการเข้ารหัสที่หลากหลายมากขึ้น เพื่อให้ผู้ใช้ หรือเจ้าของข้อมูลมีทางเลือกด้านความปลอดภัยที่มากขึ้นสำหรับข้อมูลที่ต้องการรักษาความลับ

จากการที่มีวิธีในการเข้ารหัสข้อมูล และอุปกรณ์สำหรับการเข้ารหัสที่หลากหลาย ในปัจจุบัน แนวทางหนึ่งที่น่าสนใจคือ ระบบอลวน (Chaos) ซึ่งให้ผลลัพธ์ออกมาในแบบสุ่มที่มีความยากต่อการคาดเดาผลลัพธ์ โดยระบบอลวนมีความไวต่อค่าสถานะเริ่มต้นของระบบ และตัวแปรควบคุมของระบบอย่างมาก เมื่อค่าเหล่านี้มีการเปลี่ยนแปลงแม้เพียงเล็กน้อย เช่น ทศนิยมในตำแหน่งที่ 7 หรือทศนิยมในตำแหน่งที่ 11 ที่มีความสำคัญน้อยมากกับข้อมูล จะส่งผลให้ผลลัพธ์สุดท้ายที่ต่างออกไป

โครงงานนี้ได้นำเสนอการเข้ารหัสรูปภาพ ซึ่งเป็นข้อมูลที่มีขนาดใหญ่ และมักมีปัญหาด้านความปลอดภัยของข้อมูลอยู่เสมอ ดังเหตุภาพหลุดดารา หรือบุคคลสำคัญ หรือแม้แต่เอกสารลับที่หลุดสู่สายตาสาธารณชนโดยไม่ได้รับอนุญาตจากเจ้าของภาพ และกลายเป็นเหตุวุ่นวายหลายครั้ง ในรูปแบบแอปพลิเคชันบนระบบ Android ซึ่งเป็นหนึ่งในระบบปฏิบัติการของอุปกรณ์เคลื่อนที่ที่ถูกใช้งานมากที่สุด เพื่อแสดงการเข้ารหัสรูปภาพบนอุปกรณ์ใกล้ตัวที่ถูกใช้งานบ่อยในชีวิตประจำวัน

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อศึกษาการใช้งานระบบอลวนบนระบบ Android

1.2.2 เพื่อศึกษาการนำระบบอลวน มาประยุกต์กับการเข้ารหัสภาพ

1.3 ขอบเขตของการศึกษา

1.3.1 ศึกษาการทำงานของระบบอลวนบนระบบ Android

1.3.2 ศึกษาและทดลองแนวคิด สมการ บน MATLAB

1.3.3 ใช้ Eclipse ที่เสริม ADT เป็นเครื่องมือในการเขียนแอปพลิเคชัน

1.3.4 ใช้โทรศัพท์ระบบปฏิบัติการ Android จริง เป็นอุปกรณ์ในการทดลองแอปพลิเคชัน

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 เข้าใจการทำงานของระบบอลวนบนระบบ Android

1.4.2 สามารถนำระบบอลวนมาประยุกต์กับการเข้ารหัสภาพบนระบบ Android ได้

1.5 แผนงานและระยะเวลาในการดำเนินงาน

ตาราง 1.1 แผนและระยะเวลาในการดำเนินงาน

ขั้นตอนการดำเนินงาน	พ.ศ. 2557							พ.ศ. 2558	
	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.
1. ศึกษาทฤษฎีที่เกี่ยวข้อง และ Chaotic map ที่ใช้									
3. ทดสอบ Chaotic map บน MATLAB									
4. แปลง Chaotic map เป็น Code Android และทดสอบ									
5. พัฒนาแอปพลิเคชันเข้ารหัสรูปภาพและถอดรหัสรูปภาพ									
6. เขียนรายงานความก้าวหน้า									
7. นำเสนอผลงาน									

TNI
THAI - NICHI INSTITUTE OF TECHNOLOGY

บทที่ 2

หลักการพื้นฐานและทฤษฎีที่เกี่ยวข้อง

2.1 ระบบอลวน

ระบบอลวน หรือ Chaotic system เป็นระบบที่มีความเป็นพลวัต โดยทั่วไปเป็นที่รู้จักในคุณสมบัติที่ว่า อ่อนไหวต่อสถานะเริ่มต้นของระบบ และตัวแปรควบคุมของระบบอย่างมาก ซึ่งทั้งค่าของสถานะเริ่มต้นของระบบ และตัวแปรควบคุมของระบบ ถ้ามีการเปลี่ยนแปลงแม้เพียงเล็กน้อยจากเดิม จะทำให้ระบบให้ผลลัพธ์ออกมาต่างจากเดิมอย่างมาก ทำให้คาดเดา หรือประมาณค่าของระบบหรือผลที่ได้จากระบบได้ยาก

คำว่า Chaos ใช้ในการระบุพฤติกรรมของระบบในช่วงที่ระบบนั้นเกิดความเป็น aperiodic หรือมีความไม่ซ้ำตัวเอง และมักจะปรากฏในลักษณะของการสุ่ม หรือเหมือน Noise (สัญญาณรบกวน) โดย Chaos เกิดได้จากระบบที่มีความไม่เป็นเชิงเส้น (Nonlinear system) ซึ่งเป็นระบบที่มีสมการในเชิงเวลาที่มีความไม่เป็นเชิงเส้น กล่าวคือตัวแปรที่ระบุสถานะของระบบ เช่น ความเร็ว, ความดัน, ตำแหน่ง, หรือความเร่ง ปรากฏอยู่ในสมการในรูปแบบที่ไม่เป็นเชิงเส้น

2.2 Chaotic map

Chaotic map เป็นหนึ่งในรูปแบบของระบบอลวนที่เกิดจากการใช้สมการวนซ้ำตัวเองในแกนของเวลา แบบ discrete-time หรือในช่วงเวลาหนึ่งที่สนใจ ใช้ค่าสถานะของระบบ ณ เวลาปัจจุบัน ในการคำนวณค่าสถานะของระบบในเวลาถัดไป และสามารถเกิดรูปแบบความอลวนขึ้นได้ โดยทั่วไป Chaotic map มักมาในรูปแบบของสมการที่มีการกระทำวนซ้ำตัวเอง และมีความง่ายในการคำนวณ ดังสมการ

$$x_{n+1} = f(x_n) \tag{2.1}$$

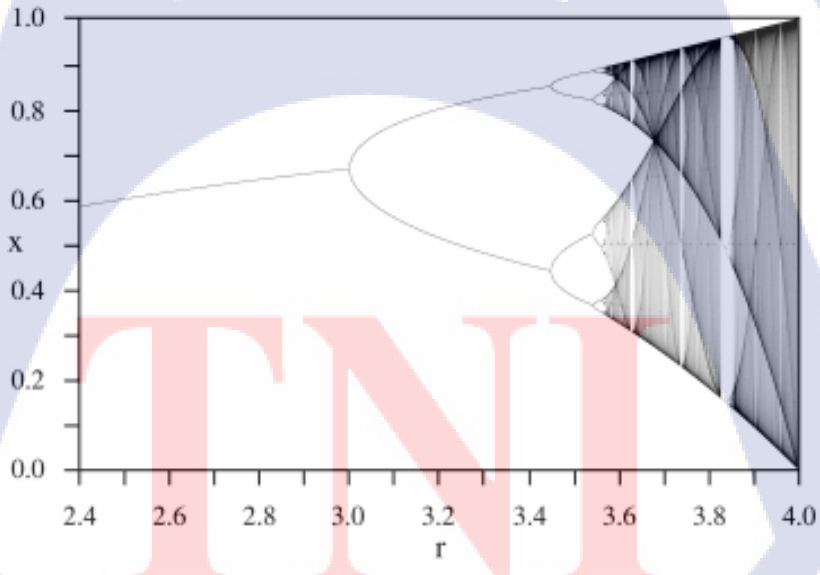
ในปริญญานิพนธ์นี้จะยกตัวอย่างหนึ่งใน Chaotic map ที่ถูกยกมาใช้เป็นตัวอย่างบ่อยที่สุดและง่ายต่อการคำนวณมากที่สุดคือ Logistic map ซึ่งมีสมการดังนี้

$$x_{n+1} = rx_n(1 - x_n) \tag{2.2}$$

โดยที่ r คือตัวแปรควบคุม และมีค่าอยู่ในช่วง [0, 4] และ x_n คือตัวแปรสถานะของระบบ ตามปกติแล้ว การวิเคราะห์ Chaotic map สามารถทำได้ 2 วิธี คือ วิเคราะห์เชิงคุณภาพ และวิเคราะห์เชิงปริมาณ

2.2.1 การวิเคราะห์ Chaotic map เชิงคุณภาพ

การวิเคราะห์ Chaotic map เชิงคุณภาพสามารถทำได้โดยการใช้ Bifurcation diagram ซึ่งเป็นการหาจุดวกกลับของกราฟของค่าผลลัพธ์ที่ได้จาก Chaotic map ในแกนเวลา แล้วนำจุดวกกกลับเหล่านั้น มาสร้างเป็น Bifurcation diagram ตัวอย่างเช่น Bifurcation Diagram ของ Logistic map ดังภาพที่ 2.1 จะเห็นได้ว่า ระบบมีความอลวนในช่วงค่าของตัวแปรควบคุม r ตั้งแต่ประมาณ 3.6 จนถึง 4 โดยสังเกตจากความหนาของจำนวนจุดวกกลับที่ถูกจุดไว้ใน Bifurcation diagram



ภาพที่ 2.1 Bifurcation diagram ของ Logistic map

ทั้งนี้ คำว่า Bifurcation ใช้ในการอธิบายการเปลี่ยนแปลงแบบฉับพลันในพลวัต (Dynamic) ของระบบ เช่น การเปลี่ยนแปลงพฤติกรรมของ fixed point เมื่อมีตัวแปรเปลี่ยนค่า เป็นต้น

2.2.2 การวิเคราะห์ Chaotic map เชิงปริมาณ

การวิเคราะห์ Chaotic map เชิงปริมาณสามารถทำได้โดยการใช้ Lyapunov Exponent (LE) spectrum ซึ่งเป็นการวัดอัตราการกระจายตัว และความไม่เสถียรของระบบ ซึ่งค่า LE ใช้ในการระบุอัตราการเปลี่ยนแปลงทิศทางของค่าของชุดข้อมูล เมื่อค่าเริ่มต้นของชุดข้อมูลมีความใกล้เคียงกับค่าเริ่มต้นของชุดข้อมูลอ้างอิงอย่างมาก โดยใช้สมการ

$$\lambda = \lim_{n \to \infty} \left(\frac{1}{N}\right) \sum_{n=1}^{N} \ln f'(x_n) \qquad (2.3)$$

โดยที่ N คือจำนวนข้อมูลในชุดข้อมูล x_n (ในที่นี้ได้มาจาก Chaotic map) λ คือค่า LE และ f'(x) คืออนุพนัธ์อันดับหนึ่งของระบบ โดยระบบจะมีความอลวนเมื่อค่า LE มากกว่า 0

2.3 Android

Android เป็นหนึ่งในระบบปฏิบัติการสำหรับอุปกรณ์พกพา หรืออุปกรณ์เคลื่อนที่ (Mobile) ที่ถูกใช้งานมากที่สุดในปัจจุบัน มีพื้นฐานมาจาก Linux และได้ถูกใช้บนอุปกรณ์เช่น Smartphone, Tablet, และ e-Reader เป็นต้น Android ยังมีคุณสมบัติในการทำ Multi-threading และ Multi-processing หรือการทำงานหลาย Thread และหลาย Process ในเวลาเดียวกัน

Android ยังเอื้อต่อนักพัมนาแอปพลิเคชัน ทั้งการให้เครื่องมือสำหรับการสร้างแอปพลิเคชันที่มีความสามารถที่หลากหลาย รวมทั้งการพัฒนา การทดสอบแอปพลิเคชัน และการจำลองอุปกรณ์ที่ใช้งานระบบปฏิบัติการ Android และยังมีตลาดที่เปิดกว้างที่เอื้อต่อการนำแอปพลิเคชันที่ผู้พัฒนาได้พัฒนาเสร็จแล้ว นำไปวางขายได้อย่างอิสระ

การพัฒนาแอปพลิเคชันบนระบบ Android ผู้พัฒนาสามารถเลือกเครื่องมือในการพัฒนาได้อย่างอิสระ ซึ่งเครื่องมือในปัจจุบันที่ได้รับการแนะนำจากเว็บไซต์ผู้พัฒนาหลักของ Android คือ Android Studio ซึ่งเป็นโปรแกรมสำหรับพัฒนาแอปพลิเคชันบนระบบ Android โดยเฉพาะ จากเดิมคือ ADT (Android Developer Tools) Bundle ที่เป็นส่วนเสริมของ Eclipse ที่เป็นเครื่องมือสำหรับพัฒนาแอปพลิเคชัน Java เป็นหลัก ให้สามารถนำมาใช้พัฒนาแอปพลิชันของระบบ Android ได้

สำหรับ ADT Bundle นั้น เป็นชุดของอุปกรณ์พัฒนาแอปพลิเคชัน Android ในอดีตมาพร้อมกับ Eclipse IDE (Integrated Development Environment) ที่มีการเสริม ADT ที่มี Android SDK

(Software Development Kit) เข้าไป ทำให้สามารถใช้ Eclipse ในการพัฒนาแอปพลิเคชัน Android ได้ นอกเหนือจากการพัฒนาโปรแกรมภาษา Java เพียงอย่างเดียว

โดยทั่วไปแล้วขั้นตอนพื้นฐานของการพัฒนาแอปพลิเคชันบนระบบ Android ไม่ว่าจะด้วยเครื่องมือใดก็ตาม มีขั้นตอนดังนี้

1. Setup : ขั้นตอนนี้เป็นการติดตั้ง IDE (Integrated Development Environment) ซึ่งเป็นเครื่องมือในการพัฒนาแอปพลิเคชัน และ AVD (Android Virtual Devices) ซึ่งเป็นอุปกรณ์จำลองอุปกรณ์จริงที่ใช้ระบบปฏิบัติการ Android ในรุ่นต่างๆตามแต่ผู้พัฒนาแอปพลิเคชันจะเลือกใช้บนคอมพิวเตอร์ เพื่อเตรียมสำหรับการทดสอบแอปพลิเคชัน

2. Development : เป็นขั้นตอนพัฒนาแอปพลิเคชันตามที่ต้องการ โดยเป็นการเขียนชุดประโยคคำสั่ง หรือ Code ให้แอปพลิเคชันทำงานตามการทำงานที่เขียนไว้

3. Debugging and Testing : เป็นช่วงที่ Build ตัวแอปพลิเคชันที่พัฒนาให้กลายเป็นไฟล์ .apk ที่สามารถทำการ Debug ได้ โดยทุกครั้งที่มีการ Build สำเร็จ ระบบจะสร้างไฟล์ .apk ใหม่ทุกครั้ง ซึ่งไฟล์ .apk ที่ถูกสร้างสามารถนำไปติดตั้งบนอุปกรณ์จริงที่ใช้ระบบปฏิบัติการ Android หรืออุปกรณ์จำลองดังที่ติดตั้งไว้ข้างต้น เพื่อทดสอบและแก้ไขข้อผิดพลาดที่อาจเกิดขึ้น

4. Publish : เป็นช่วงที่ปล่อยให้ใช้งานได้จริง โดยอาจนำไปวางไว้ใน Play Store ของ Google หรือปล่อยไฟล์ .apk ให้ผู้ใช้งานหรือผู้สนใจติดตั้งได้ด้วยตนเอง

2.4 Java

Java เป็นภาษาสำหรับเขียนโปรแกรมที่สามารถใช้งานได้หลากหลาย ทำงานหลายงานได้พร้อมกัน มีความเป็นคลาส และเป็นภาษาเชิงวัตถุ (Object Oriented) ถูกออกแบบมาให้ง่ายพอให้โปรแกรมเมอร์จำนวนมากสามารถเรียนรู้และฝึกฝนการใช้งานจนชำนาญได้ โดย Java มีความคล้ายกับภาษา C หรือ C++ แต่มีการจัดการที่แตกต่างกัน นอกจากนี้ Java ยังถูกออกแบบให้มีขนาดเล็กและเคลื่อนย้ายได้ง่าย กล่าวคือ สามารถใช้งานได้บนทุกระบบปฏิบัติการ

การที่ Java เป็นอิสระจากทุกแพล็ตฟอร์มและระบบปฏิบัติการนี้ เป็นหนึ่งในข้อดีที่สำคัญที่สุดของ Java เหนือภาษาอื่นส่วนใหญ่ ตามปกติภาษาการเขียนโปรแกรมทั่วไปเช่น C หรือ C++ ต้อง

เปลี่ยนจากภาษาระดับสูงให้เป็นภาษาเครื่องก่อนจึงสามารถใช้งานได้ ด้วยการใช้ Compiler โดยนำโปรแกรมที่ยังอยู่ภาษาระดับสูงมาแปลงให้เป็นภาษาระดับเครื่องทั้งโปรแกรม โปรแกรมที่เกิดขึ้นจากกระบวนการนี้สามารถนำไปใช้งานได้ไม่จำกัดจำนวนครั้ง แต่เมื่อจะนำไปใช้ในคอมพิวเตอร์เครื่องอื่นที่ใช้ระบบไม่เหมือนกัน จะต้องคอมไพล์อีกครั้งด้วยคอมไพเลอร์ตัวอื่น อีกวิธีคือ การใช้ Interpreter ซึ่งจะแปลคำสั่งทีละคำสั่งในวงรอบแบบ รับและทำงาน เพื่อให้โปรแกรมสามารถทำงานได้ครบถ้วนจะต้องเกิดวงรอบนี้ซ้ำจนกว่าจะจบคำสั่งทั้งหมด

สำหรับ Java นักออกแบบได้ทำให้ Java มีทั้ง 2 คุณสมบัติข้างต้น โดยโปรแกรมที่เขียนด้วยภาษา Java จะถูก Compile เป็นภาษาของเครื่องเสมือน หรือ Virtual machine ที่เรียกว่า Java Virtual Machine (JVM) สำหรับภาษาเครื่องที่ใช้ทำงานบนเครื่อง JVM นี้เรียกว่า Java bytecode ซึ่งแน่นอนว่า Java bytecode นี้ ไม่สามารถใช้งานกับคอมพิวเตอร์จริงอื่นได้นอกจาก JVM ซึ่งการใช้งาน JVM นี้เองเป็นหนึ่งในจุดขายของ Java และทำให้ Java เป็นอิสระจากทุกแพล็ตฟอร์มและระบบปฏิบัติการ

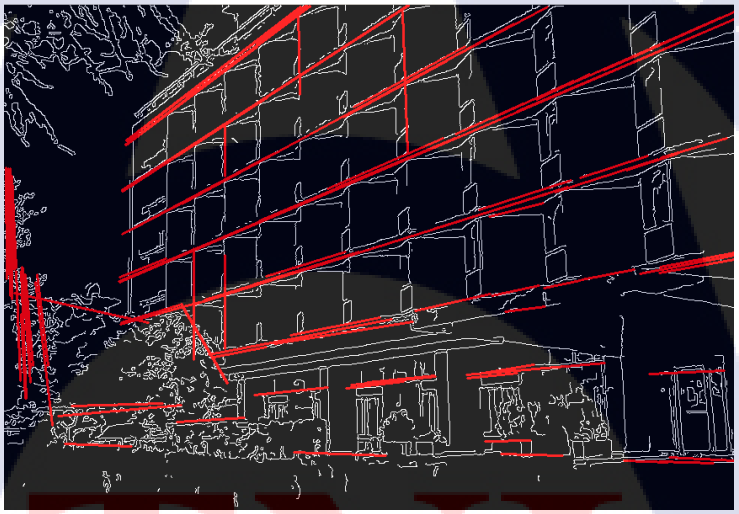
Java ยังมีลักษณะของการเป็นภาษาเชิงวัตถุ หรือ Object-oriented ที่มีแนวคิดคือ มององค์ประกอบภายในโปรแกรมเป็นวัตถุที่มีข้อมูล และองค์ประกอบย่อยภายในวัตถุที่หลากหลาย ในบางครั้งการมองวัตถุ อาจเป็นการมองในแง่การตอบสนองต่อข้อความที่เข้ามาสู่โปรแกรม ซึ่งวัตถุที่แตกต่างกันอาจตอบสนองต่อข้อความเดียวกันที่เข้ามาไม่เหมือนกัน หรือการมองในแบบครอบครัว กล่าวคือ การที่วัตถุที่ต่างกัน แต่อาจมีข้อมูลภายในที่เหมือนกันในการตอบสนองข้อความเดียวกันที่เข้ามา หรือเรียกได้ว่าอยู่ใน Class เดียวกัน แต่เป็นไปได้เช่นกันที่วัตถุที่มีคุณลักษณะที่คล้ายกันอาจจะอยู่ใน Class ที่ต่างกัน

Class เป็นรูปแบบสำหรับวัตถุที่มีคุณสมบัติคล้ายกัน มีคุณสมบัติทั้งหมดที่ชุดของวัตถุนั้นจะมีได้ Class สามารถถูกสืบทอดได้ หรือเรียกว่าการ Inherit โดย Class ลูกที่สืบทอดมาจากคลาสเดิมจะถูกเรียกว่า Subclass ซึ่งจะได้รับสิ่งที่มีอยู่ใน Class เดิมที่ถูกสืบทอดทั้งหมด และยังสามารถ Override หรือเปลี่ยนแปลงส่วนที่สืบทอดมาได้อีกด้วย

2.5 OpenCV

OpenCV เป็น Library สำหรับช่วยในการพัฒนาซอฟต์แวร์สำหรับงานด้าน Computer Vision และ Machine Learning ที่เป็น Library แบบ Open Source โดยรองรับภาษาสำหรับการเขียนโปรแกรมไม่ว่าจะเป็น C, C++, Java, Python, และรวมถึง MATLAB อีกด้วย อีกทั้งรองรับหลายระบบปฏิบัติการ ที่ครอบคลุมทั้ง Windows, Android, Linux, และ Mac OS

สำหรับตัว OpenCV นั้น ประกอบไปด้วยอัลกอริธึมกว่า 2500 รูปแบบที่เกี่ยวกับการทำงานด้าน Computer Vision และ Machine Learning จำนวนมาก เช่น อัลกอริธึมรู้จำใบหน้า, อัลกอริธึมตรวจจับวัตถุ, อัลกอริธึมตรวจจับการเคลื่อนไหวของมนุษย์ เป็นต้น โดยในปริญญานิพนธ์นี้ จะใช้เพียงแค่อัลกอริธึมในส่วนของการ XOR รูปภาพ 2 รูป โดยหนึ่งในตัวอย่างของการใช้งาน OpenCV คือการหาคุณลักษณะของรูปภาพ โดยใช้ OpenCV ให้ผลเป็นดังภาพที่ 2.x

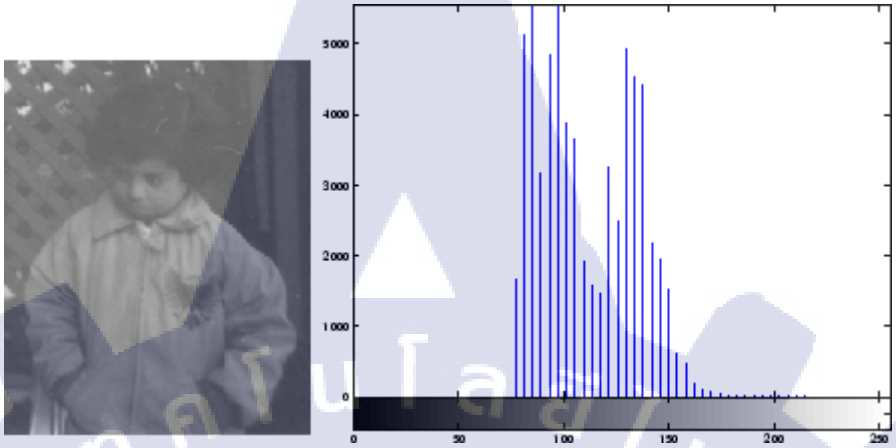


ภาพที่ 2.2 ตัวอย่างผลการใช้งาน OpenCV ในการหาคุณลักษณะของภาพ

2.6 Histogram (Image)

Histogram คือกราฟแท่งที่สามารถบรรยายการกระจายของข้อมูลในชุดข้อมูลที่สนใจ ในกรณีของรูปภาพดิจิตอลคือ ระดับสีในแต่ละโทนสี ที่ประกอบรวมเข้ากันเป็นรูปภาพดิจิตอล หนึ่งในตัวอย่างพื้นฐานคือ รูป Grayscale (ขาว-เทา-ดำ) แบบ 8 บิทต่อพิกเซล จะได้ 256 ระดับสีในโทนสี

เทา โดยที่สีดำสนิทอยู่ที่ระดับค่าสีที่ 0 และสีขาวอยู่ในระดับสีที่ 255 โดยในแกน x แทนด้วยระดับสีในโทนสีที่สนใจ และแกน y แทนด้วยจำนวนของพิกเซลที่อยู่ในระดับสีนั้นๆ ดังตัวอย่างดังภาพที่ 2.3



ภาพที่ 2.3 ตัวอย่าง Histogram ของภาพ Grayscale

2.7 Literature reviews

ระบบอวลวน (Chaos) และ Chaotic map ได้ถูกประยุกต์ใช้ในหลายด้าน เช่น ด้านความปลอดภัยของข้อมูล, การสร้างข้อมูลแบบสุ่ม เป็นต้น จากงานวิจัยที่ผ่านมา มีรูปแบบใหม่ๆของ Chaotic map และการประยุกต์ใช้ ถูกนำเสนอในหลายงานวิจัย โดยในปริญญานิพนธ์นี้ได้ยกมา 2 งานวิจัย คือ

2.7.1 The Generalization of Mathematically Simple and Robust Chaotic Maps with Absolute Value Nonlinearity

งานวิจัยของ ผศ.ดร.วิมล แสนอุ้ม และนายปฏิญญา เกตุทอง ได้นำเสนอ Chaotic map ที่ใช้ค่าความไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์ ทั้งหมด 4 กรณี ดังภาพที่ 2.4 โดย Chaotic map ที่ถูกนำเสนอทั้ง 4 กรณีนี้ ได้ถูกทดสอบด้วยแบบทดสอบ NIST Statistic test และผ่านทุกการทดสอบในทุกกรณี

Cases	Equations	Fixed Points	Jacobians
M_1	$x_{n+1} = \lvert 1 - ax_n \rvert$	$x = \frac{1}{a \pm 1}$	$\lvert -a \operatorname{sign}(1 - ax) \rvert$
M_2	$x_{n+1} = \lvert -1 + ax_n \rvert$	$x = \frac{1}{a \pm 1}$	$\lvert a \operatorname{sign}(1 + ax) \rvert$
M_3	$x_{n+1} = 1 - a\lvert x_n \rvert$	$x = \frac{1}{\pm a + 1}$	$\lvert -a \operatorname{sign}(x) \rvert$
M_4	$x_{n+1} = -1 + a\lvert x_n \rvert$	$x = \frac{1}{\pm a - 1}$	$\lvert a \operatorname{sign}(x) \rvert$

ภาพที่ 2.4 Chaotic map ที่ใช้ค่าความไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์ทั้ง 4 กรณี

ทั้งนี้ในปริญญานิพนธ์นี้ ได้นำกรณีหนึ่งจากงานวิจัยนี้ มาพัฒนาแอปพลิเคชันเข้ารหัสภาพต่อ นอกจากนี้ จะเห็นได้ว่าทุกรณีของ Chaotic map ที่ถูกนำเสนอดังภาพที่ 2.4 ยังเป็นสมการที่ง่ายต่อการคำนวณ และการประยุกต์ใช้งานต่ออีกด้วย

$$x_{n+1} = y_{n+1} - ax_n^2,$$

$$y_{n+1} = b\, x_n$$

ภาพที่ 2.5 ชุดสมการ Henon map

2.7.2 Android Application for Secret Image Transmission and Reception Using Chaotic Steganography

อีกหนึ่งงานวิจัยคืองานวิจัยของ G. Savithri และ K.L.Sudha ได้นำ Henon map ซึ่งเป็นหนึ่งใน Chaotic map มีลักษณะเป็นกลุ่มของสมการดังภาพที่ 2.5 มาใช้ในการเข้ารหัสรูปภาพในรูปแบบแอปพลิเคชันบนระบบ Android โดยใช้ค่าที่ได้จาก Henon map รวมทั้งยังมีการทดสอบโดยการทดลองเข้ารหัสและถอดรหัส ด้วยค่าเริ่มต้นของระบบที่เหมือนกัน แต่ตัวแปรควบคุมที่ต่างกัน ได้ผลดัง

ภาพที่ 2.6 จะเห็นได้ว่า เมื่อใช้ค่าเริ่มต้นของระบบในการถอดรหัสที่ต่างกันแม้เพียงทศนิยมในตำแหน่งที่ 5 ผลที่ได้จากการถอดรหัสจะต่างออกไปอย่างสิ้นเชิง

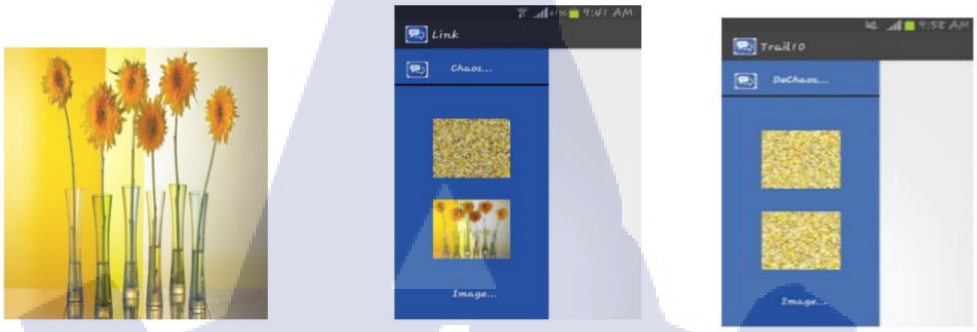


Figure 7a.Original image b. Decryption with original key a=1.80000 c. Decryption with a=1.80001

ภาพที่ 2.6 ผลที่ได้จากการเข้ารหัสและถอดรหัสรูปภาพในงานวิจัยก่อนหน้า

TNI
THAI - NICHI INSTITUTE OF TECHNOLOGY

บทที่ 3

ขั้นตอนการดำเนินงาน

3.1 อุปกรณ์ที่ใช้ในการดำเนินงาน

3.1.1 Hardware

- Computer
  - Manufacturer: Dell
  - Model: Vostro 5460 (Year 2013)
  - Processor: Intel® Core i5-3230M (2.6 GHz up to 3. GHz)
  - RAM: 4 GB DDR3 RAM
  - VGA: NVIDIA GeForce GT 630M
  - OS: Windows 8.1 Pro 64 bit
- Smartphone: Sony Xperia M2

3.1.2 Software

- ADT Bundle
  - Android SDK
  - Eclipse IDE

3.2 การทดลอง Chaotic map บน MATLAB

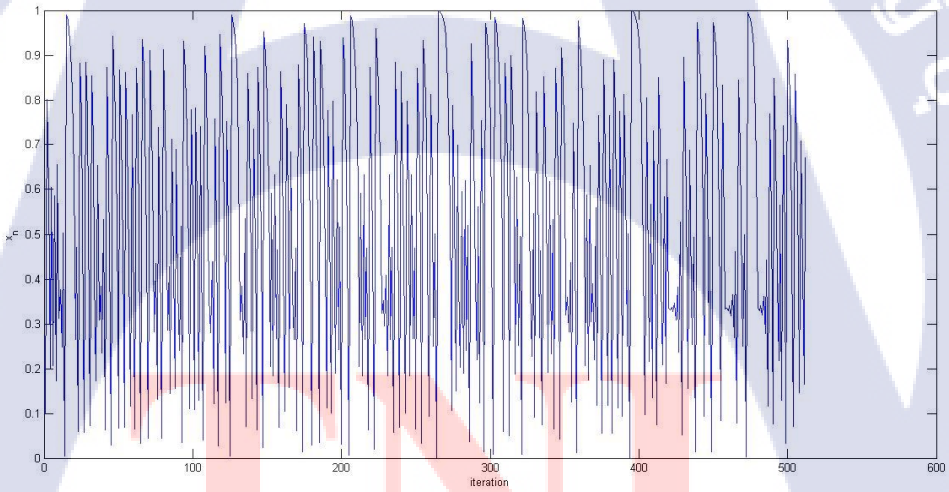
ก่อนนำ Chaotic map ไปใช้บน Android ควรมีการทดลอง Chaotic map บน MATLAB เสียก่อน เพื่อให้เกิดความง่ายต่อการใช้งาน และดัดแปลง Chaotic map เป็นภาษาสำหรับการเขียน

โปรแกรมที่ต้องการใช้งาน (ในที่นี้ภาษาที่ใช้ในการเขียนแอปพลิเคชันของ Android คือ Java) ในปริญญานิพนธ์นี้ เลือกใช้ Chaotic map ที่ใช้ค่าความไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์ ในกรณีแรกสุด ซึ่งมีสมการดังต่อไปนี้

$$x_{n+1} = |1 - ax_n| \tag{3.1}$$

โดยที่ x คือสถานะของระบบในแต่ละรอบของการประมวลผลของ Chaotic map ที่ n และ a คือตัวแปรควบคุมของระบบ และได้ทำการทดลองดังนี้

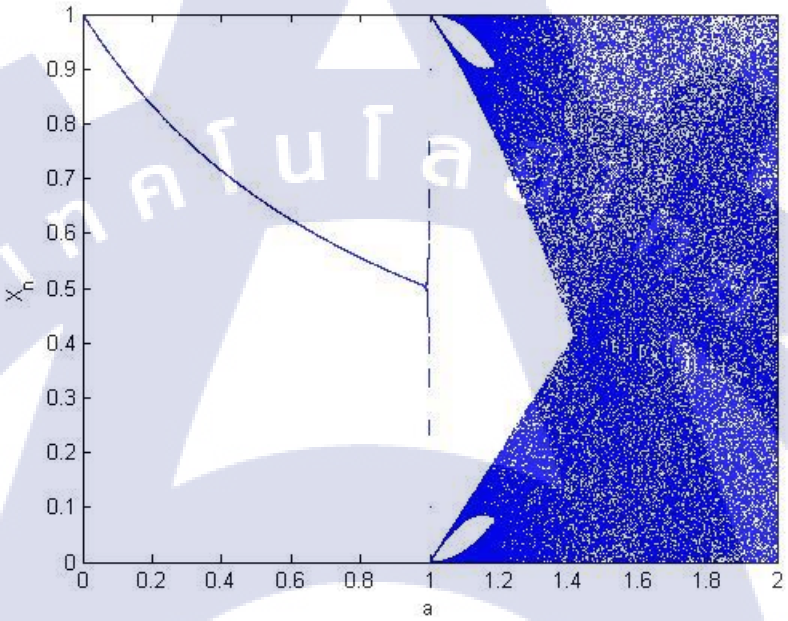
3.2.1 การทดลองให้ Chaotic map ประมวลผลข้อมูล Chaotic waveforms ในเชิงเวลา โดยนำ Chaotic map มาคำนวณซ้ำจนกว่าจะถึงรอบที่กำหนด ในที่นี้คือการคำนวณค่า x ของสมการ (3.1) โดยกำหนดตัวแปรควบคุม a ให้มีค่า 1.999 และสถานะเริ่มต้นของ x มีค่าเป็น 0.1 หลังจากการประมวลผลเสร็จสิ้น นำค่า x มาสร้างเป็น Chaotic waveforms ดังภาพที่ 3.1



ภาพที่ 3.1 Chaotic waveforms ที่ได้จาก MATLAB ของสมการ (3.1)

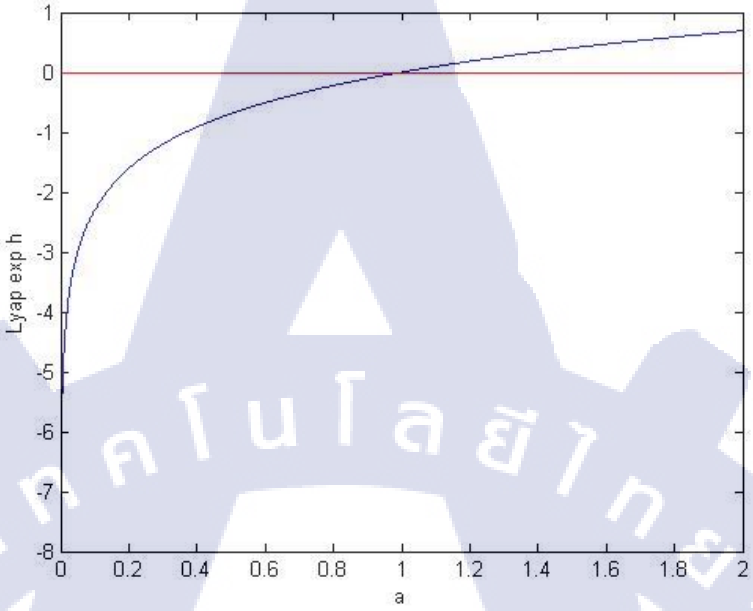
3.2.2 การประมวลผล Bifurcation diagram ซึ่งเป็นวิธีการประเมิน Chaotic map ในเชิงคุณภาพเพื่อดูว่า Chaotic map นั้นๆ มีความอลวนมากเพียงใด และมีช่วงของความอลวนอยู่ในช่วงใดของตัวแปรควบคุม a โดยนำค่าของตัวแปรสถานะ ในที่นี้คือตัวแปร x ในแกนของเวลา ที่ผ่านการคำนวณจากสมการ Chaotic map เป็นจำนวนรอบที่กำหนด มาหาจุดวกกลับของกราฟในแต่ละค่าของตัวแปรควบคุม

a โดยChaotic map ที่เป็นสมการ (3.1) เริ่มจากค่าต่ำสุดของ a ที่ 0 และ สิ้นสุดที่ค่าสูงสุดของ a ที่ 2 เมื่อประมวลผลเสร็จแล้ว จะได้ผลดังภาพที่ 3.2 จะพบว่า ระบบ ซึ่งในที่นี้คือ Chaotic map มีจำนวนจุดวกกลับมากจนเกินกว่าจะนับได้ หรือกล่าวคือ มีพฤติกรรมความอลวน (Chaos) เมื่อค่าของตัวแปรควบคุม a อยู่ในช่วง [1, 2]



ภาพที่ 3.2 Bifurcation Diagram ที่ได้จาก MATLAB ของสมการ (3.1)

3.2.3 การประมวลผล LE Spectrum ซึ่งเป็นวิธีการประเมิน Chaotic map ในเชิงปริมาณ เพื่อดูว่า Chaotic map นั้นๆ มีความอลวนมากเพียงใด และมีช่วงของความอลวนอยู่ในช่วงใดของตัวแปรควบคุม a โดยนำค่าของตัวแปรสถานะ ในที่นี้คือตัวแปร x ในแกนของเวลา ที่ผ่านการคำนวณจากสมการ Chaotic map เป็นจำนวนรอบที่กำหนด มาเข้าสมการคำนวณค่า LE ดังสมการ (2.3) ในแต่ละค่าของตัวแปรควบคุม a โดยChaotic map ที่เป็นสมการ (3.1) เริ่มจากค่าต่ำสุดของ a ที่ 0 และ สิ้นสุดที่ค่าสูงสุดของ a ที่ 2 เมื่อประมวลผลเสร็จแล้วนำค่าที่ได้จากสมการมาแสดงผลเป็นกราฟ จะได้กราฟดังภาพที่ 3.3 จากกราฟจะเห็นได้ว่าค่าของ LE มีค่ามากกว่า 0 เมื่อค่าของตัวแปรควบคุมอยู่ในช่วง [1, 2] ซึ่งเป็นช่วงของค่าตัวแปรควบคุม a ช่วงเดียวกันกับที่ Bifurcation diagram ระบุว่า ระบบมีความเป็น Chaos

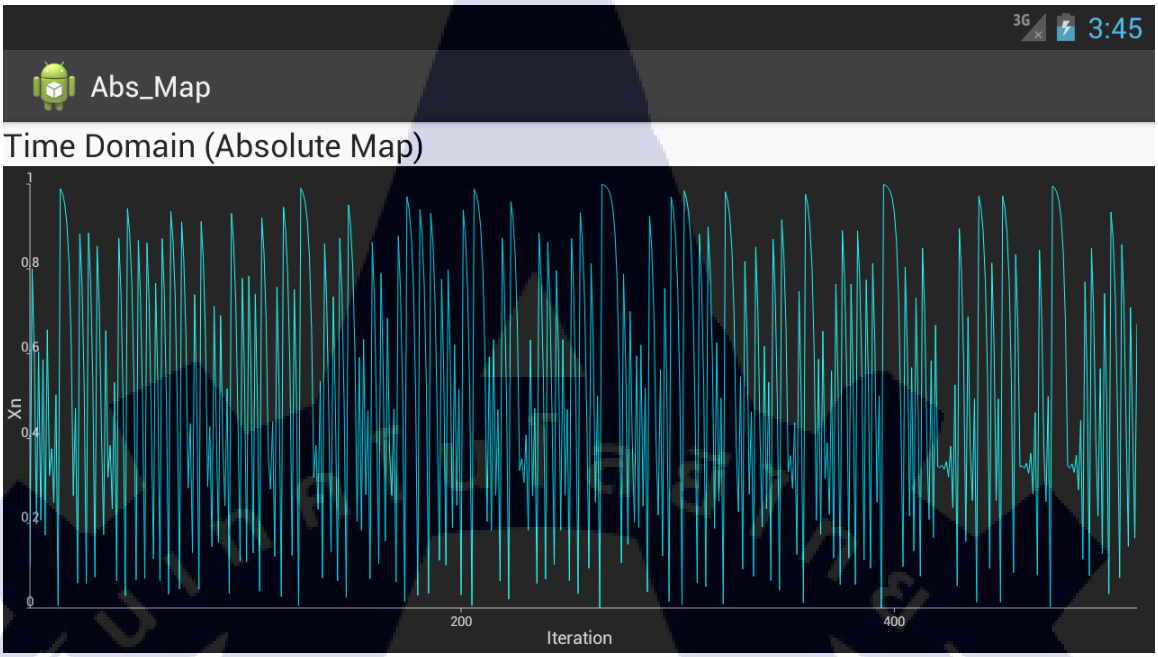


ภาพที่ 3.3 LE Spectrum ที่ได้จาก MATLAB ของสมการ (3.1)

3.3 การทดลอง Chaotic map บน Android

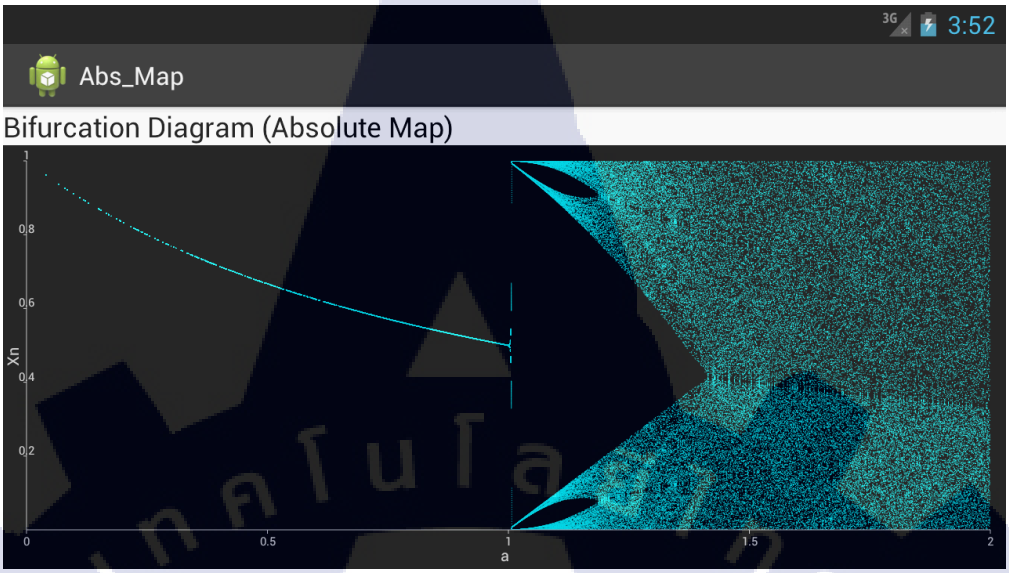
คล้ายกับการทดลองบน MATLAB แต่เป็นการนำแนวคิดที่ได้ มาเปลี่ยนให้เป็นแอปพลิเคชันที่สามารถใช้ได้บน Android โดยใช้ภาษา Java และใช้ Eclipse IDE ที่เสริม ADT เป็นเครื่องมือในการพัฒนาแอปพลิเคชัน ทั้งนี้แอปพลิเคชันสำหรับทดสอบ Chaotic map ได้มีการใช้ Library achartengine ช่วยในการสร้างกราฟ ซึ่งการทำงานของแอปพลิเคชันมีดังนี้

3.3.1 การประมวลผล Chaotic waveforms ในเชิงเวลา โดยขั้นตอนและกระบวนการ คล้ายกับช่วงที่ทดลองบน MATLAB โดยสิ่งที่เปลี่ยนไปคือภาษาที่ใช้ในการทำงานของแอปพลิเคชันเปลี่ยนเป็นภาษา Java ได้ผลจากแอปพลิเคชันทดสอบ เป็นดังภาพที่ 3.4 ซึ่งมีความคล้ายกับผลที่ได้จาก MATLAB ดังแสดงในภาพที่ 3.1



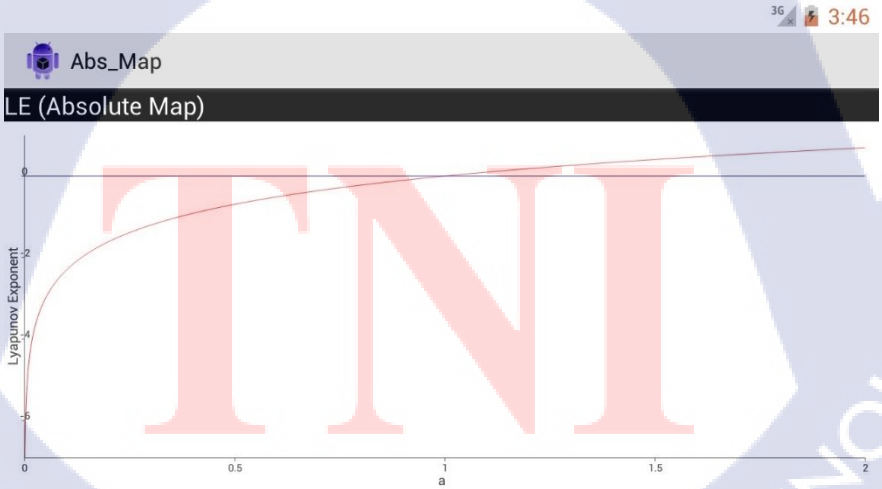
ภาพที่ 3.4 Chaotic waveforms ที่ได้จากแอปพลิเคชัน Android ของสมการ (3.1)

3.3.2 การประมวลผล Bifurcation diagram คล้ายกับช่วงที่ทดลองบน MATLAB เช่นกัน โดยสิ่งที่เปลี่ยนไป นอกจากภาษาที่ใช้ในการทำงานแล้ว อีกสิ่งหนึ่งที่เปลี่ยนไปคือ แนวคิดที่ใช้ในการหาจุดวกกลับของกราฟจะเปลี่ยนเป็นการหาจุดยอด (Peak) ของกราฟแทน โดยเทียบค่าของ x ณ จุดนั้นๆว่ามากกว่าค่าที่ใกล้เคียง ทั้งก่อนหน้า และค่าถัดไปหรือไม่ และเทียบว่าค่าที่จุด x นั้นๆ ว่าค่าน้อยกว่าค่าใกล้เคียงหรือไม่ ถ้าเงื่อนไขใดเงื่อนไขหนึ่งถูกต้อง ให้นำจุด x นั้นๆ มาเตรียมใส่ใน Bifurcation diagram ผลที่ได้จากแอปพลิเคชันทดสอบ เป็นดังภาพที่ 3.5 ซึ่งมีความใกล้เคียงกับผลที่ได้จาก MATLAB ดังภาพที่ 3.2 จำนวนจุดวกกลับมากจนเกินกว่าจะนับได้ หรือกล่าวคือ มีพฤติกรรมความอลวน (Chaos) เมื่อค่าของตัวแปรควบคุม a อยู่ในช่วง [1, 2] เช่นเดียวกับผลจาก MATLAB



ภาพที่ 3.5 Bifurcation Diagram ที่ได้จากแอปพลิเคชัน Android ของสมการ (3.1)

3.3.3 การประมวลผล LE Spectrum คล้ายกับช่วงที่ทดลองบน MATLAB เกือบทุกประการ เปลี่ยนเพียงภาษาที่ใช้ในการทำงานของแอปพลิเคชันเป็นภาษา Java โดยผลที่ได้จากแอปพลิเคชันทดสอบเป็นดังภาพที่ 3.6 ซึ่งมีความใกล้เคียงกับผลที่ได้จาก MATLAB ดังภาพที่ 3.3 จะเห็นได้จากผลว่าค่าของ LE มากกว่า 0 ในช่วงของค่าตัวแปรควบคุม a อยู่ในช่วง [1, 2] เช่นกัน



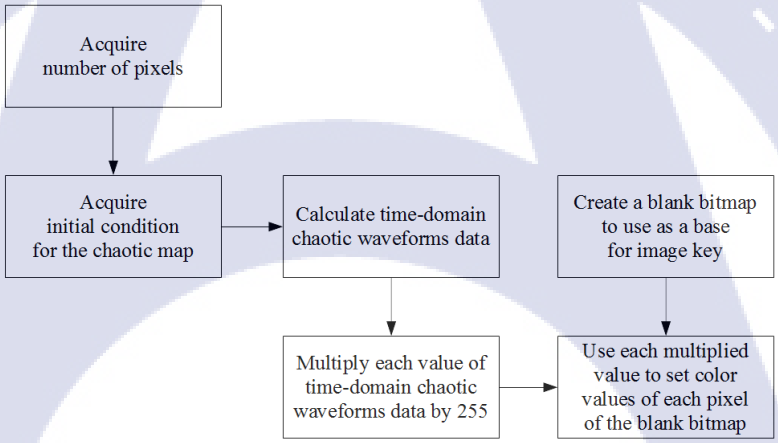
ภาพที่ 3.6 LE Spectrum ที่ได้จากแอปพลิเคชัน Android ของสมการ (3.1)

3.4 การประยุกต์ Chaotic map กับการเข้ารหัสรูปภาพบน Android

ในส่วนของการประยุกต์ Chaotic map มาใช้ในการเข้ารหัสภาพนั้น ดังที่ได้ทดลองกับส่วนของการทดลอง Chaotic map บน Android พบว่า Chaotic map ที่ใช้ค่าความไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์ในกรณีแรก หรือสมการ (3.1) สามารถใช้งานได้บน Android ดังนั้น Chaotic map ดังสมการ (3.1) จะเป็นตัวที่ถูกนำมาใช้ในการเข้ารหัสภาพด้วย

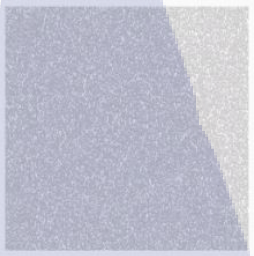
3.4.1 การสร้างกุญแจ

การสร้างกุญแจสำหรับเข้ารหัส ดังแสดงในแผนผังดังภาพที่ 3.7 คือ นำ Chaotic map มาใช้เป็นส่วนสร้างกุญแจสำหรับการเข้ารหัส (Key) ซึ่งเป็นข้อมูลภาพ Bitmap ดังเช่นภาพที่ 3.8



ภาพที่ 3.7 แผนภาพขั้นตอนการสร้างกุญแจเข้ารหัสถาพ

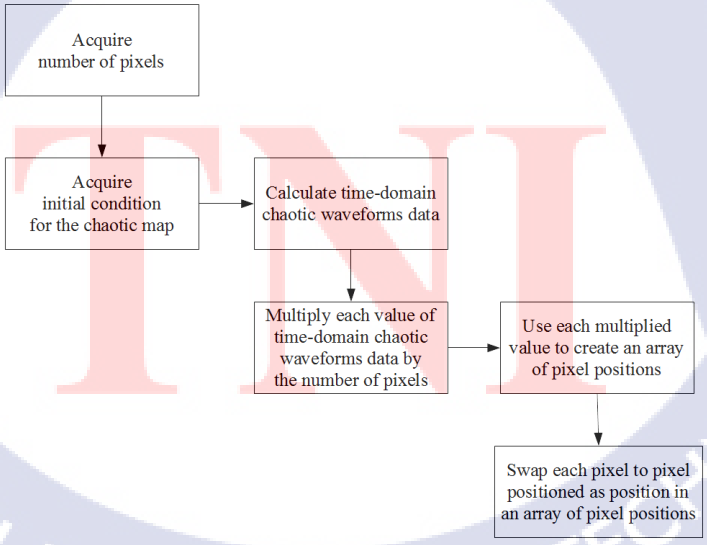
กุญแจสามารถสร้างได้โดยนำ Chaotic map ตามสมการ (3.1) มาประมวลผลในเชิงเวลา เป็นจำนวนรอบเท่ากับจำนวนพิกเซลของรูปภาพ โดยใช้ตัวแปรควบคุม a มีค่าเป็น 1.999 และค่าสถานะเริ่มต้นตามที่ได้รับมาจากผู้ใช้ แล้วนำค่าสถานะของระบบ (ค่า x ของสมการ (3.1)) ในแต่ละรอบของการทำงาน มากำหนดเป็นอาเรย์ของค่าของพิกเซล โดยคูณแต่ละค่าที่ได้จาก Chaotic map ด้วย 255 แล้วปัดเศษทศนิยมขึ้น (ถ้ามี) แล้วนำค่าของพิกเซลซึ่งอยู่ในอาเรย์ของค่าของพิกเซล มากำหนดเป็นค่า RGB ของพิกเซลของรูปที่จะเป็น Key ซึ่งมีขนาดความกว้างและความยาวเท่ากับภาพที่จะนำมาเข้ารหัส



ภาพที่ 3.8 ตัวอย่างกุญแจเข้ารหัสภาพ

3.4.2 การสลับตำแหน่งพิกเซลในรูปภาพ (Scramble Image)

การสลับตำแหน่งพิกเซลในรูปภาพ ดังแสดงในแผนภาพดังภาพที่ 3.9 ในช่วงแรกคล้ายกับในส่วนของการสร้างกุญแจ กล่าวคือ นำ Chaotic map ตามสมการ (3.1) มาประมวลผลในเชิงเวลาด้วยตัวแปรควบคุม a มีค่าเป็น 1.999 และค่าสถานะเริ่มต้นของระบบตามที่ได้รับมาจากผู้ใช้ เป็นจำนวนรอบเท่ากับจำนวนพิกเซล แล้วนำค่าสถานะของระบบในแต่ละรอบการทำงาน มากำหนดเป็นอาเรย์ของตำแหน่งของพิกเซลที่จะสลับไปหา โดยคูณค่าที่ได้จาก Chaotic map ด้วยจำนวนพิกเซล แล้วปัดเศษทศนิยมขึ้น (ถ้ามี) จากนั้นสลับตำแหน่งของพิกเซล เริ่มจากพิกเซลแรกสุดของภาพทางด้านซ้ายบนสุดของรูปภาพ สลับกับพิกเซลในตำแหน่งที่จะสลับไปหา ซึ่งอยู่ในอาเรย์ของตำแหน่งของพิกเซลที่จะสลับไปหา โดยสลับตำแหน่งไปจนถึงพิกเซลสุดท้ายทางด้านมุมขวาล่างของรูปภาพ



ภาพที่ 3.9 แผนภาพขั้นตอนการสลับตำแหน่งพิกเซลของรูปภาพ

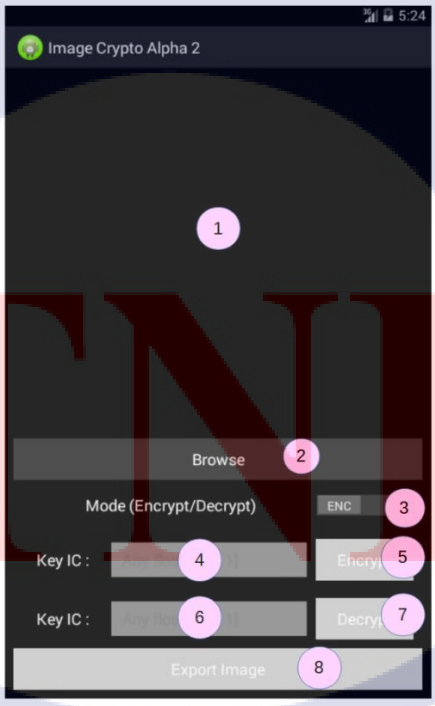
สำหรับการสลับตำแหน่งของพิกเซลกลับตำแหน่งเดิม สามารถทำได้โดยสลับตำแหน่งพิกเซลเริ่มต้นจากพิกเซลสุดท้ายทางด้านมุมขวาล่างของรูปภาพ ย้อนกลับไปหาพิกเซลแรกสุดที่มุมบนซ้ายสุดของรูปภาพแทน ทั้งนี้การสลับตำแหน่งของพิกเซลกลับให้มีประสิทธิภาพสูงสุด ควรใช้อาเรย์ของตำแหน่งของพิกเซลที่จะสลับไปหาที่มีค่าเดียวกัน เพื่อให้สลับแล้วพิกเซลทุกพิกเซลกลับเข้าตำแหน่งเดิม

3.5 แอปพลิเคชัน Android ที่ใช้ในการเข้ารหัสภาพ

แอปพลิเคชันที่ใช้ในการเข้ารหัสภาพที่นำเสนอในปริญญานิพนธ์นี้ มีรูปลักษณ์ และการทำงานดังที่จะอธิบายต่อไปนี้

3.5.1 การออกแบบ User Interface

User Interface เป็นส่วนที่ใช้ในการติดต่อกับผู้ใช้แอปพลิเคชัน ซึ่งมีลักษณะดังภาพที่ 3.10 โดยส่วนประกอบของ User Interface ตามตัวเลขที่ระบุในภาพที่ 3.10 มีดังนี้



ภาพที่ 3.10 Interface ของแอปพลิเคชัน

1. พื้นที่แสดงผล ส่วนนี้จะเป็นส่วนแสดงผลของแอปพลิเคชัน ทั้งรูปภาพที่จะนำมาเข้ารหัส, รูปภาพที่เข้ารหัสแล้ว, และรูปภาพที่ถอดรหัสแล้ว โดยปกติถ้าไม่มีรูปภาพใดๆ จะเป็นพื้นที่ว่าง

2. ปุ่ม Browse เป็นปุ่มที่ใช้ในการเรียกหารูปภาพที่ผู้ใช้ต้องการจะนำมาเข้ารหัส หรือถอดรหัสจากภายในอุปกรณ์ Android ของผู้ใช้งานแอปพลิเคชันนี้

3. สวิตช์สำหรับเลือกรูปแบบการทำงานของแอปพลิเคชัน โดยสามารถเปลี่ยนไปและกลับ ระหว่างการเข้ารหัส และการถอดรหัส รูปภาพ

4. ช่องว่างสำหรับใส่ค่าเริ่มต้นที่จะใช้ใน Chaotic map ในส่วนของการเข้ารหัสภาพ (Encryption) เป็นช่องว่างสำหรับใส่ตัวเลข โดยค่าของที่ผู้ใช้จะใส่ ควรเป็นทศนิยมที่อยู่ในช่วง [0, 1]

5. ปุ่ม Encrypt เป็นปุ่มที่ใช้สำหรับการเข้ารหัส เมื่อผู้ใช้กดปุ่มนี้ แอปพลิเคชันจะเข้ารหัสรูปภาพทันที ปุ่มนี้จะทำงานได้หลังจากที่มีการเลือกรูปภาพจากผู้ใช้ โดยการกดปุ่ม Browse แล้ว

6. ช่องว่างสำหรับใส่ค่าเริ่มต้นที่จะใช้ใน Chaotic map ในส่วนของการถอดรหัสภาพที่ถูกเข้ารหัสไว้ (Decryption) เป็นช่องว่างสำหรับใส่ตัวเลข โดยค่าของที่ผู้ใช้จะใส่ ควรเป็นทศนิยมที่อยู่ในช่วง [0, 1]

7. ปุ่ม Decrypt เป็นปุ่มที่ใช้สำหรับการถอดรหัส เมื่อผู้ใช้กดปุ่มนี้ แอปพลิเคชันจะถอดรหัสรูปภาพทันที ปุ่มนี้จะทำงานได้หลังจากที่มีการเลือกรูปภาพจากผู้ใช้ โดยการกดปุ่ม Browse แล้ว

8. ปุ่ม Export Image ใช้ในการนำผลที่ได้จากแอปพลิเคชันที่แสดงอยู่ที่พื้นที่แสดงผล ออกจากแอปพลิเคชันเป็นไฟล์รูปภาพ นามสกุล .PNG

3.5.2 การออกแบบ Android Virtual Device (AVD)

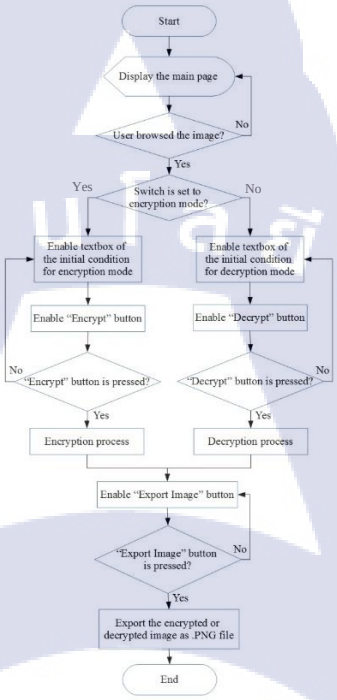
Android Virtual Device ซึ่งเป็นการตั้งค่าสำหรับอุปกรณ์จำลองของอุปกรณ์ที่ใช้ระบบ Android ที่จำลองอยู่บนคอมพิวเตอร์ โดยในปริญญานิพนธ์นี้ ได้ใช้การตั้งค่าของ AVD ดังนี้

ตาราง 3.1 การตั้งค่าของ Android Virtual Device

Configurations	Selected options/values
Device	5.1” WVGA(480 x 800 mdpi)
Target	Android 4.4.2 – API level 19
CPU/ABI	ARM (armeabi-v7a)
Skin	Skin with dynamic hardware controls
Back camera	None
RAM	512 MB
VM heap	64 MB
Internal storage	512 MB
SD card	512 MB

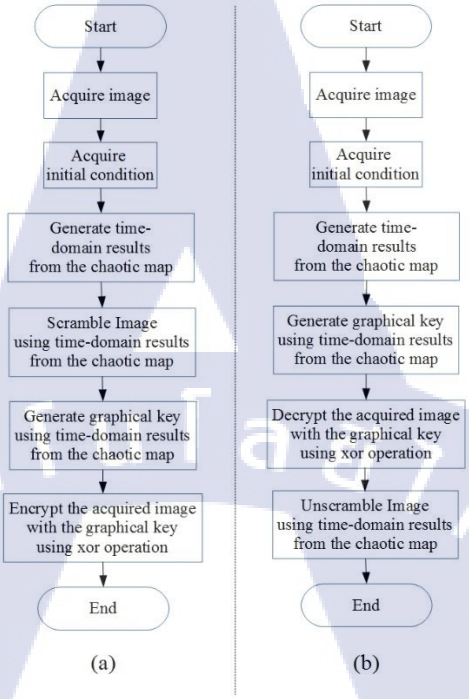
3.5.3 การออกแบบการทำงานของแอปพลิเคชัน

การทำงานของแอปพลิเคชัน ตามแผนภาพดังภาพที่ 3.11 แอปพลิเคชันมีขั้นตอนการทำงานตามที่ออกแบบ ดังนี้



ภาพที่ 3.11 Flow chart แสดงการทำงานของแอปพลิเคชัน

1. แสดงหน้าจอหลักของแอปพลิเคชัน หลังจากผู้ใช้เริ่มการทำงานของแอปพลิเคชัน
2. รอการเลือกภาพจากผู้ใช้ โดยผู้ใช้จะเลือกภาพด้วยการกดปุ่ม Browse บนจอ
3. แสดงภาพที่ผู้ใช้เลือกบนพื้นที่แสดงผลบนหน้าต่างของแอปพลิเคชัน และเปิดการทำงานของส่วนเข้ารหัส หรือถอดรหัส โดยตรวจสอบกับสวิตซ์เลือกรูปแบบการทำงานของแอปพลิเคชัน
4. รอการกดปุ่มเข้ารหัส หรือถอดรหัสรูปภาพ จากผู้ใช้งาน เมื่อปุ่มถูกกดจะเข้าสู่กระบวนการเข้ารหัส หรือถอดรหัสต่อไป (ขึ้นกับรูปแบบการทำงานของแอปพลิเคชันที่ถูกเลือก ณ เวลานั้น)
5. เข้าสู่การเข้ารหัส หรือถอดรหัส โดยมีรูปแบบการทำงานตามแผนภาพดังภาพที่ 3.12 รายละเอียดของการทำงานในส่วนของการเข้ารหัส และถอดรหัสรูปภาพมีดังนี้



ภาพที่ 3.12 แผนผังการทำงานของส่วนการเข้ารหัส (a) และส่วนการถอดรหัส (b)

5.1 การเข้ารหัสรูปภาพ (a) เป็นส่วนสำหรับเข้ารหัสรูปภาพ ซึ่งจะสามารถทำงานได้เมื่อสวิตซ์เลือกรูปแบบการทำงานของแอปพลิเคชันถูกปรับไปที่ Encryption มีการทำงานดังนี้

5.1.1 รับรูปภาพและ แปลงรูปภาพเป็น Bitmap ในช่วง Acquire Image

5.1.2 รับค่าเริ่มต้นที่จะใช้ใน Chaotic map จากช่องที่ผู้ใช้กรอก หรือสุ่มขึ้นมาถ้าไม่มีการกรอกจากผู้ใช้

5.1.3 สร้างชุดของผลลัพธ์ของสมการ (3.1) ในเชิงเวลา โดยจำนวนของผลลัพธ์มีเท่ากับจำนวนพิกเซลของรูปภาพ

5.1.4 ทำการสลับตำแหน่งของพิกเซลในรูปภาพทั้งหมด

5.1.5 สร้างกุญแจสำหรับการเข้ารหัส ดังที่อธิบายในหัวข้อ 3.4

5.1.6 เข้ารหัสรูปภาพด้วยการ XOR ระหว่างภาพต้นฉบับ และกุญแจเข้ารหัส โดยใช้เมธอด bitwise_xor() ซึ่งเป็นหนึ่งในเมธอดที่มีอยู่ใน Library OpenCV

5.2 การถอดรหัสรูปภาพ (b) เป็นส่วนสำหรับถอดรหัสรูปภาพ ซึ่งสามารถทำงานได้เมื่อสวิตซ์เลือกรูปแบบการทำงานของแอปพลิเคชันถูกปรับไปที่ Decryption มีการทำงานคล้ายกับส่วนเข้ารหัสรูปภาพ โดยมีการทำงานดังนี้

5.2.1 รับรูปภาพและ แปลงรูปภาพเป็น Bitmap ในช่วง Acquire Image

5.2.2 รับค่าเริ่มต้นที่จะใช้ใน Chaotic map จากช่องที่ผู้ใช้กรอก หรือสุ่มขึ้นมาถ้าไม่มีการกรอกจากผู้ใช้

5.2.3 สร้างชุดของผลลัพธ์ของสมการ (3.1) ในเชิงเวลา โดยจำนวนของผลลัพธ์มีเท่ากับจำนวนพิกเซลของรูปภาพ

5.2.4 สร้างกุญแจสำหรับการเข้ารหัส ดังที่อธิบายในหัวข้อ 3.4

5.2.5 ถอดรหัสรูปภาพด้วยการ XOR ระหว่างภาพต้นฉบับ และกุญแจถอดรหัส โดยใช้เมธอด bitwise_xor() ซึ่งเป็นหนึ่งในเมธอดที่มีอยู่ใน Library OpenCV

5.2.6 ทำการสลับตำแหน่งของพิกเซลในรูปภาพทั้งหมด กลับสู่ตำแหน่งดั้งเดิม (ถ้าเป็นไปได้)

6. หลังจากการทำงานของส่วนเข้ารหัส หรือถอดรหัสเสร็จสิ้น แอปพลิเคชันจะเปิดการทำงาน ให้ปุ่ม Export Image สามารถใช้งานได้ และรอการกดจากผู้ใช้ (ถ้ามี)

7. ทำการ Export รูปภาพที่ถูกเข้ารหัส หรือถอดรหัสแล้ว ไปเก็บไว้ยังหน่วยความจำภายในอุปกรณ์ Android ของผู้ใช้ หลังจากที่ผู้ใช้กดปุ่ม Export Image โดยไฟล์รูปภาพที่ถูก Export จะเป็นไฟล์รูปภาพนามสกุล .png

บทที่ 4

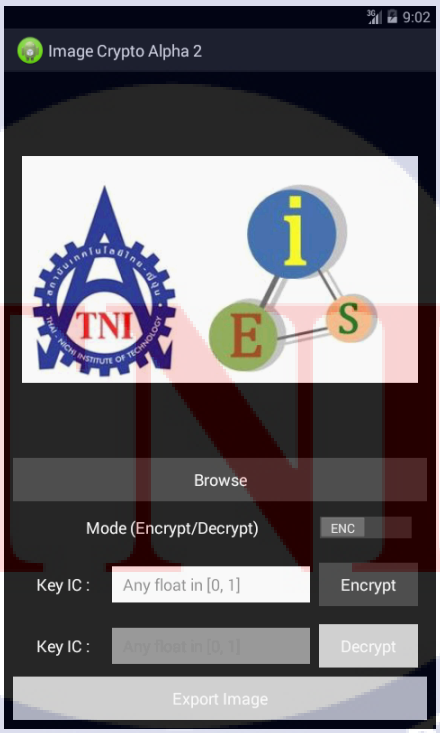
ผลการดำเนินงาน

4.1 การทำงานของแอปพลิเคชันเข้ารหัส และถอดรหัสรูปภาพ

แอปพลิเคชันที่เข้ารหัสภาพ และถอดรหัสภาพ สามารถทำการเข้ารหัส และถอดรหัสรูปภาพได้ รวมทั้งยังสามารถส่งภาพออกมาเป็นไฟล์รูปภาพนามสกุล .PNG เพื่อนำไปส่งต่อหรือเก็บรักษา ตามแต่วิจารณญาณของผู้ใช้งาน ซึ่งมีผลจะการทำงานขั้นตอนต่างๆดังนี้

4.1.1 การเลือกรูปภาพจากผู้ใช้

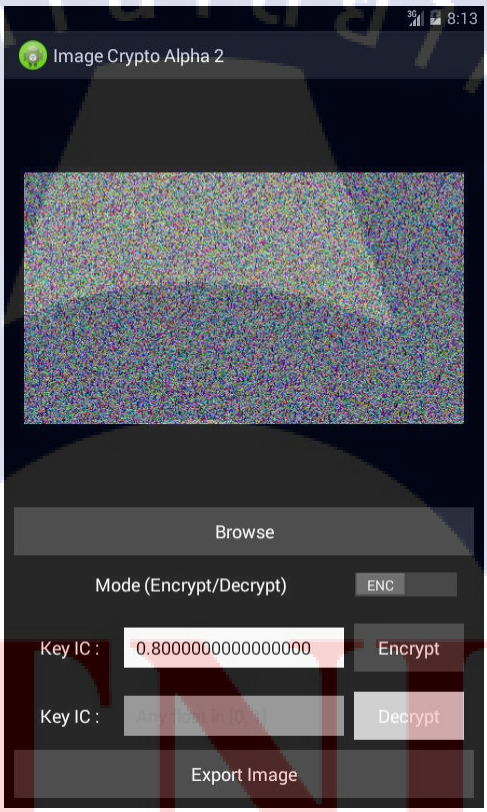
เมื่อผู้ใช้กด Browse ผู้ใช้จะสามารถเลือกรูปภาพจากภายในอุปกรณ์ Android ของผู้ใช้ได้ และรูปภาพที่ถูกเลือกจะถูกแสดงผลที่หน้าจอของผู้ใช้ ดังภาพที่ 4.1



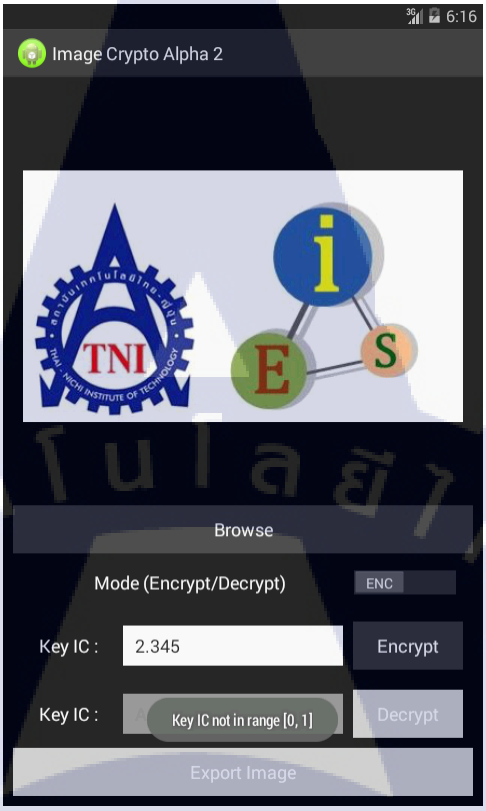
ภาพที่ 4.1 หน้าต่างของแอปพลิเคชัน หลังจากผู้ใช้เลือกรูปภาพที่ต้องการ

4.1.2 การเข้ารหัสของภาพ และการถอดรหัสภาพ

4.1.2.1 การเข้ารหัสภาพ มีกรณีที่ต่างกันไปขึ้นกับการใช้งาน ถ้าการเข้ารหัสภาพมีการเข้ารหัสภาพโดยใส่ค่าเริ่มต้นของ Chaotic map ที่สามรถใช้งานได้ จะได้ผลดังภาพที่ 4.2 คือสามารถเข้ารหัสรูปภาพได้สมบูรณ์ และถ้าเข้ารหัสภาพโดยไม่ใส่ค่าเริ่มต้นให้กับ Chaotic map แอปพลิเคชันจะสุ่มค่าสถานะเริ่มต้นที่สามารถใช้งานได้ และได้ผลดังภาพที่ 4.2 เช่นกัน และสามารถเข้ารหัสรูปภาพได้สมบูรณ์เช่นกัน แต่ถ้าใส่ค่าสถานะเริ่มต้นให้กับ Chaotic map ที่ไม่สามารถใช้งานได้ จะไม่สามารถเข้ารหัสภาพได้ และจะได้ผลดังภาพที่ 4.3

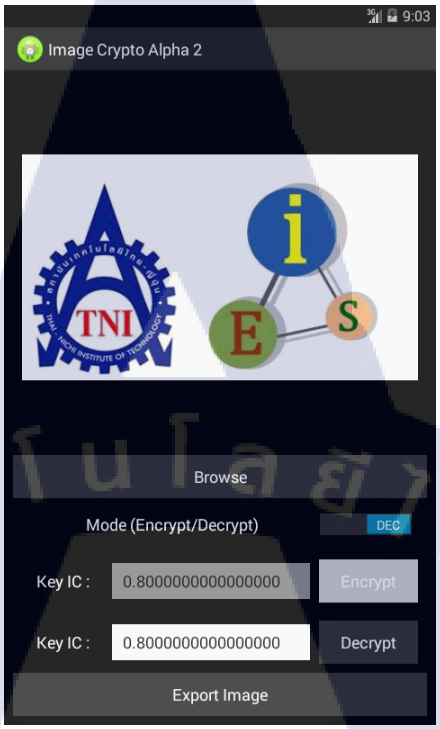


ภาพที่ 4.2 หน้าต่างของแอปพลิเคชัน หลังการเข้ารหัสรูปภาพเสร็จสิ้น

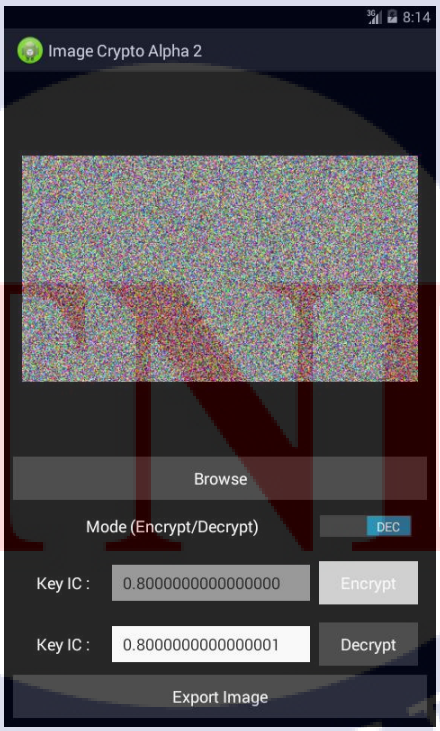


ภาพที่ 4.3 หน้าต่างของแอปพลิเคชัน หลังการเข้ารหัสรูปภาพล้มเหลว

4.1.2.2 การถอดรหัสภาพ คล้ายกับส่วนเข้ารหัสภาพคือมีกรณีที่ต่างกันไปขึ้นกับการใช้งาน ทั้งนี้ภาพที่ควรใช้ในการถอดรหัสควรเป็นภาพที่ถูกเข้ารหัสมาก่อนแล้ว เพื่อให้ได้ผลที่สมบูรณ์ในการตรวจสอบผลของการถอดรหัส โดยถ้าผู้ใช้กรอกค่าเริ่มต้นของ Chaotic map เดียวกันกับค่าเริ่มต้นที่ใช้ในการเข้ารหัส จะสามารถถอดรหัสได้เป็นภาพต้นฉบับก่อนการเข้ารหัส ดังภาพที่ 4.4 แต่ถ้าผู้ใช้กรอกค่าเริ่มต้นของ Chaotic map ที่ต่างกันกับช่วงที่เข้ารหัสภาพ การถอดรหัสจะได้ภาพที่ไม่สามารถระบุถึงภาพต้นฉบับได้เลย ดังภาพที่ 4.5 ทั้งนี้ความละเอียดของค่าเริ่มต้นของ Chaotic map จะส่งผล กับความแตกต่างของผลที่ได้จากการถอดรหัสรูปภาพ จนถึงความแตกต่างของค่าเริ่มต้นของ Chaotic map ในระดับความละเอียดที่ $1x10^{-16}$



ภาพที่ 4.4 หน้าต่างของแอปพลิเคชัน หลังการถอดรหัสรูปภาพเสร็จสิ้น และได้ภาพต้นฉบับ



ภาพที่ 4.5 หน้าต่างของแอปพลิเคชัน หลังการถอดรหัสล้มเหลว และไม่ได้ภาพต้นฉบับ

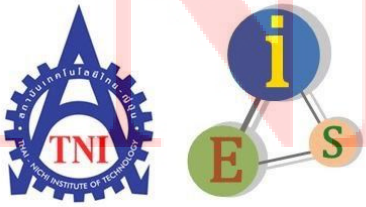
4.1.3 การส่งออกผลลัพธ์จากส่วนแสดงผลของแอปพลิเคชัน

แอปพลิเคชันสามารถส่งออกผลลัพธ์มาเป็นไฟล์รูปภาพ ซึ่งขั้นตอนนี้ทำงานก็ต่อเมื่อผู้ใช้กดปุ่ม Export Image ตัวอย่างผลที่ได้จากการส่งออกรูปภาพจากการเข้ารหัสภาพแสดงดังภาพที่ 4.6

ภาพที่ 4.6 ตัวอย่างของรูปที่ถูกส่งออกมาจาก แอปพลิเคชันเข้ารหัสและถอดรหัสรูปภาพ

4.2 วิเคราะห์รูปภาพผลลัพธ์ที่ได้จากการเข้ารหัสรูปภาพ

ในการวิเคราะห์ผลลัพธ์ที่ได้ จากการเข้ารหัสรูปภาพที่ได้มาจากแอปพลิเคชันเข้ารหัสภาพบนระบบ Android ที่นำเสนอในปริญญานิพนธ์นี้ สามารถวิเคราะห์ออกมาได้ในหลายรูปแบบ โดยในปริญญานิพนธ์นี้ ได้ทำการวิเคราะห์รูปภาพผลลัพธ์ใน 2 รูปแบบ ดังนี้



ภาพที่ 4.7 ภาพต้นฉบับที่ใช้ในการทดสอบแอปพลิเคชัน

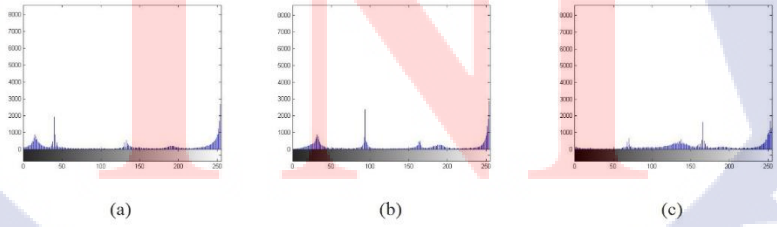
4.2.1 วิเคราะห์โดยการสังเกตรูปภาพ

ผลลัพธ์ที่ได้จากการเข้ารหัสรูปภาพดังภาพที่ 4.8 เมื่อเปรียบเทียบกับภาพต้นฉบับที่ใช้ในการทดลอง ดังภาพที่ 4.7 พบว่า เมื่อสังเกตในส่วนของการพิจารณารูปภาพ ผลลัพธ์ที่ได้จากการเข้ารหัสรูปภาพมีความแตกต่างกับภาพต้นฉบับโดยสิ้นเชิง ไม่สามารถเห็นส่วนใดส่วนหนึ่งของภาพต้นฉบับเลย

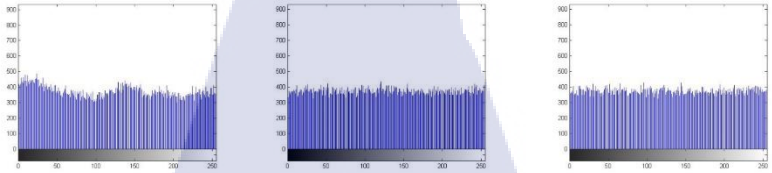
ภาพที่ 4.8 ผลลัพธ์ที่ได้จากการเข้ารหัสรูปภาพ

4.2.2 วิเคราะห์โดยการใช้ Histogram

สามารถทำได้โดยนำผลลัพธ์ที่ได้จากการเข้ารหัส และภาพต้นฉบับ มาหา Histogram ของรูปภาพ ด้วยโปรแกรม MATLAB ทั้งในช่วงโทนสี แดง, เขียว, และน้ำเงิน โดย Histogram ของภาพต้นฉบับในช่วงของโทนสี แดง, เขียว, และน้ำเงิน แสดงดังภาพที่ 4.9 ตามอักษรกำกับ a, b, และ c ตามลำดับ และ Histogram ของภาพที่ถูกเข้ารหัสในช่วงของโทนสี แดง, เขียว, และน้ำเงิน แสดงดังภาพที่ 4.10 ตามอักษรกำกับ a, b, และ c ตามลำดับ เมื่อวิเคราะห์ Histogram ของภาพต้นฉบับ และภาพที่ถูกเข้ารหัส ได้ผลดังนี้



ภาพที่ 4.9 Histogram ของภาพต้นฉบับ โดยที่ (a), (b), และ (c) คือ Histogram ของโทนสีแดง, เขียว, และน้ำเงิน ตามลำดับ



(a) (b) (c)

ภาพที่ 4.10 Histogram ของภาพที่ถูกเข้ารหัสแล้ว โดยที่ (a), (b), และ (c) คือ Histogram ของโทนสี แดง, เขียว, และน้ำเงิน ตามลำดับ

4.2.2.1 Histogram ของภาพต้นฉบับ โอนเอียงไปทางด้านขวา ทั้งในช่วงโทนสี แดง, เขียว, และน้ำเงิน ซึ่งอาจพอสรุปได้ว่า ลักษณะของพิกเซลส่วนใหญ่ โอนเอียงไปทางสีขาว

4.2.2.2 Histogram ของภาพที่ถูกเข้ารหัส มีการกระจายตัวอย่างสม่ำเสมอ ทั้งในช่วงโทนสี แดง, เขียว, และน้ำเงิน จากการที่มีการกระจายตัวอย่างสม่ำเสมอนี้ ไม่อาจสรุปได้ว่าพิกเซลส่วนใหญ่ของภาพ มีทิศทางของลักษณะไปในทิศทางใด

จากการเปรียบเทียบลักษณะของ Histogram ของรูปภาพทั้งสอง พบว่า Histogram ของทั้งสองภาพมีความแตกต่างกันโดยสิ้นเชิงเช่นกัน ไม่สามารถดูแนวโน้มลักษณะของพิกเซลของภาพต้นฉบับได้จาก Histogram ของภาพที่ถูกเข้ารหัส

บทที่ 5

สรุปผล และวิเคราะห์ปัญหา

5.1 สรุปผลการดำเนินงาน

การทำงานของแอปพลิเคชันเข้ารหัสและถอดรหัสภาพบนระบบ Android ที่นำเสนอในปริญญานิพนธ์นี้ สามารถทำงานได้ตามความต้องการของผู้จัดทำ โดยแบ่งส่วนการทำงานเป็น 2 ส่วนหลัก ดังนี้

5.1.1 ส่วนการเข้ารหัสภาพ สามารถทำการเข้ารหัสภาพได้โดยสมบูรณ์ โดยไม่คงเหลือเค้าเดิมของภาพต้นฉบับ ซึ่งสามารถตรวจสอบได้โดย Histogram ตามที่ระบุไว้ในบทที่ 4

5.1.2 ส่วนการถอดรหัสภาพ สามารถถอดรหัสภาพได้ภาพต้นฉบับ ถ้าผู้ใช้กรอกค่าสถานะเริ่มต้นของระบบถอดรหัส เป็นค่าเดียวกันกับ ค่าสถานะเริ่มต้นของระบบเข้ารหัส และจะไม่สามารถถอดรหัสได้ภาพต้นฉบับถ้าผู้ใช้กรอกค่าสถานะเริ่มต้นของระบบถอดรหัส ต่างกันกับค่าสถานะเริ่มต้นของระบบเข้ารหัส ซึ่งค่าความแตกต่างของสถานะเริ่มต้นของระบบเข้ารหัสและถอดรหัสภาพ มีความละเอียดถึงช่วง $1x10^{-16}$

นอกจากนี้ แอปพลิเคชันเข้ารหัสและถอดรหัสภาพบนระบบ Android ที่นำเสนอนี้ ยังสามารถส่งออกภาพผลลัพธ์ที่ได้จากแอปพลิเคชัน ออกเป็นรูปภาพขนาดเท่ากับภาพต้นฉบับได้อีกด้วย

5.2 ปัญหาและอุปสรรค

5.2.1 ข้อจำกัดของอุปกรณ์

5.2.1.1 อุปกรณ์ที่ใช้ระบบ Android ส่วนใหญ่มีข้อจำกัดด้านจำนวนจุดทศนิยม จากการที่ใช้ CPU ชนิดที่ต่างกันกับเครื่องคอมพิวเตอร์ส่วนบุคคล

5.2.1.2 อุปกรณ์ที่ใช้ระบบ Android หน่วยความจำภายใน (RAM) ที่จำกัด ทำให้การสร้าง Bitmap สำหรับใช้ในการสร้าง Key สำหรับการเข้ารหัส และการสร้าง Bitmap สำหรับไว้รองรับผลลัพธ์ไม่สามารถทำได้ในกรณีภาพมีขนาดใหญ่มาก (จำนวนพิกเซลของรูปภาพมากกว่า 2 ล้านพิกเซลขึ้นไป)

5.2.2 อุปสรรคระหว่างการพัฒนาแอปพลิเคชัน

5.2.2.1 เทคนิคการเข้ารหัสและถอดรหัสรูปภาพด้วยการ XOR รูปภาพหนึ่ง กับอีกรูปภาพหนึ่ง มีเครื่องมือ และชุดคำสั่งอยู่ภายในชุด SDK ของ Android แต่เครื่องมือและชุดคำสั่งนั้นมีความซับซ้อน อีกทั้งยังให้ผลไม่ดีเท่าที่ควร

5.2.2.2 การทำงานของ Code บน Emulator บนคอมพิวเตอร์ บางครั้งให้ผลในการทำงานที่แตกต่างกันกับการใช้งานบนอุปกรณ์ Android จริง ซึ่งเกิดจากการตั้งค่า Emulator ที่มีสมรรถนะสูงเกินกว่าอุปกรณ์ระบบ Android ทั่วไป

5.3 แนวทางการแก้ปัญหา

5.3.1 ปัญหาจากข้อจำกัดของอุปกรณ์

5.3.1.1 การแก้ปัญหาด้าน CPU ของอุปกรณ์ที่มีปัญหาเรื่องทศนิยมที่ไม่เท่ากันกับของอุปกรณ์ Android ทั่วไป สามารถแก้ได้โดยการตั้งค่า CPU ของอุปกรณ์ Android ใน Emulator ให้เป็น ARM ซึ่งเป็น CPU ที่ใช้ทั่วไปในอุปกรณ์ Android ส่วนใหญ่

5.3.1.2 การแก้ปัญหาด้าน RAM ของอุปกรณ์ที่ไม่เพียงพอกับการประมวลผลภาพขนาดใหญ่ สามารถแก้ได้โดยการย่อขนาดภาพที่จะใช้ในการเข้ารหัส ทว่าสำหรับภาพที่จะใช้ในการถอดรหัส ถ้ามีขนาดใหญ่อยู่ตั้งแต่ต้น จะไม่สามารถใช้วิธีการนี้ได้ เนื่องจากทำให้ค่าของพิกเซลเปลี่ยนไป ทำให้ไม่สามารถถอดรหัสได้รูปภาพที่เป็นต้นฉบับ

5.3.2 ปัญหาระหว่างการพัฒนา

5.3.2.1 สำหรับการแก้ปัญหาเครื่องมือในการประมวลผลภาพที่มีอยู่ภายใน SDK ของ Android มีความสามารถไม่เพียงพอกับการ XOR ภาพอย่างมีประสิทธิภาพ แก้ได้โดยการผนวก Library ภายนอกที่ชื่อว่า OpenCV ซึ่งเป็น Library ช่วยการประมวลผลภาพและวิดีโอ เข้ากับตัวโปรเจคต์ของแอปพลิเคชัน

5.3.2.2 สำหรับการแก้ปัญหา Code ทำงานไม่เหมือนกัน ระหว่างอุปกรณ์จริงและ Emulator ในช่วงของการทดสอบ สามารถแก้ได้โดยการตั้งค่าของ Emulator ให้คล้ายกับอุปกรณ์ทั่วไปในระดับล่างที่มีวางขายในปัจจุบัน ดังระบุไว้แล้วในตารางที่ 3.1

5.4 ข้อเสนอแนะ และการพัฒนาในอนาคต

5.4.1 การพัฒนาการเข้ารหัสและถอดรหัสรูปภาพจากแอปพลิเคชันนี้ ควรพัฒนาเพิ่มในส่วนรับค่าสถานะเริ่มต้นของระบบ ให้สามารถกรอกข้อความหรือตัวเลขที่เป็น Password แบบปกติทั่วไปได้

5.4.2 การพัฒนาแอปพลิเคชันสำหรับเข้ารหัสหรือถอดรหัสข้อมูล ควรมีการพัฒนาเพิ่มเติมในส่วนของการเข้ารหัสและถอดรหัสข้อมูลเสียง และวิดีโอเพิ่มเติม เพื่อความหลากหลายในการทำงาน

5.4.3 แอปพลิเคชัน Android ที่นำเสนอในปริญญานิพนธ์นี้ ควรมีการพัฒนาลงในระบบ iOS และ Windows phone ด้วย เพื่อเข้าถึงผู้ใช้งานที่หลากหลายมากขึ้น

5.4.4 ควรมีการพัฒนาหน้าต่างแสดงผล และหน้าต่างสำหรับใช้งานแอปพลิเคชัน ให้มีความสวยงามมากขึ้น และใช้งานได้ง่ายขึ้น

บรรณานุกรม

[1] Robert C. Hilborn, 2000, **Chaos and Nonlinear Dynamics**, Oxford University Press

[2] Google, **Android, The world's most popular mobile platform** [Online], Available: http://developer.android.com/about/index.html [2014, May 8]

[3] Google, **Workflow: Introduction** [Online], Available: http://developer.android.com/tools/workflow/index.html [2014, May 8]

[4] James Golsing, 2014, "Introduction", **The Java® Language Specification Java SE 8 Edition**

[5] OpenCV Developers Team, OpenCV > About [Online], Available: http://opencv.org/about.html [2015, Jan 1]

[6] Martin Evening, 2007, **Adobe Photoshop CS3 for Photographers: A Professional Image Editor's Guide**

[7] W. San-Um and P. Ketthong, 2014, "The Generalization of Mathematically Simple and Robust Chaotic Maps with Absolute Value Nonlinearity", **TENCON 2014**

[8] Savithri G. and K.L. Sudha, 2014, "Android Application for Secret Image Transmission and Reception Using Chaotic Steganography", **International Journal of Network Security & Its Applications (IJNSA)**, Vol.2, P.5107-5113

ภาคผนวก

ภาคผนวก ก.

Code ส่วนการเข้ารหัส และถอดรหัสรูปภาพ

```
@SuppressWarnings("deprecation")
public void encrypt()
{
    if(key_enc.getText().toString().equals(""))
    {
        key_enc.setText(String.valueOf(global_key));
    }
    double init_con = Double.parseDouble(key_enc.getText().toString());
    if(!(init_con>1||init_con<0))
    {
        long st_time = System.currentTimeMillis();
        Bitmap im_in = ((BitmapDrawable)imScr.getDrawable()).getBitmap();
        int no_pixels = countPixels(im_in);
        double[] x = abs_map_1(no_pixels, init_con, con_a);
        Bitmap imageKey = getKey_im(x, im_in);
        Bitmap scr = scrImage(im_in, x, 0);
        Bitmap res = xorBitmap(scr, imageKey);
        imScr.setImageBitmap(res);
        long fn_time = System.currentTimeMillis();
        Toast.makeText(this, String.valueOf(fn_time-st_time), Toast.LENGTH_SHORT).show();
        export.setClickable(true);
        if(sdk_level<android.os.Build.VERSION_CODES.JELLY_BEAN)
            export.setBackgroundDrawable(getResources().getDrawable(R.drawable.but_bg));
        else
            export.setBackground(getResources().getDrawable(R.drawable.but_bg));
    }
    else
    {
        Toast.makeText(this, "Key IC not in range [0, 1]", Toast.LENGTH_SHORT).show();
    }
}
```

ภาพที่ ก.1 ส่วนการเข้ารหัสรูปภาพ

```
@SuppressWarnings("deprecation")
public void decrypt()
{
    if(key_dec.getText().toString().equals(""))
    {
        key_dec.setText(String.valueOf(global_key));
    }
    double init_con = Double.parseDouble(key_dec.getText().toString());
    if(!(init_con>1||init_con<0))
    {
        long st_time = System.currentTimeMillis();
        Bitmap im_in = ((BitmapDrawable)imScr.getDrawable()).getBitmap();
        int no_pixels = countPixels(im_in);
        double[] x = abs_map_1(no_pixels, init_con, con_a);
        Bitmap imageKey = getKey_im(x, im_in);
        Bitmap xred = xorBitmap(im_in, imageKey);
        Bitmap res = scrImage(xred, x, 1);
        imScr.setImageBitmap(res);
        long fn_time = System.currentTimeMillis();
        Toast.makeText(this, String.valueOf(fn_time-st_time), Toast.LENGTH_SHORT).show();
        export.setClickable(true);
        if(sdk_level<android.os.Build.VERSION_CODES.JELLY_BEAN)
            export.setBackgroundDrawable(getResources().getDrawable(R.drawable.but_bg));
        else
            export.setBackground(getResources().getDrawable(R.drawable.but_bg));
    }
    else
    {
        Toast.makeText(this, "Key IC not in range [0, 1]", Toast.LENGTH_SHORT).show();
    }
}
```

ภาพที่ ก.2 ส่วนการถอดรหัสรูปภาพ

ภาคผนวก ข.

Code ส่วนของ Chaotic map ที่ใช้ค่าไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์, ส่วนการสร้างกุญแจเข้ารหัสรูปภาพ, และส่วนการสลับตำแหน่งพิกเซลของรูปภาพ

```
public double[] abs_map_1(int iter, double init, double a)
{
    double[] x = new double[iter];
    x[0] = init;
    for(int i=0;i<iter-1;++i)
    {
        x[i+1] = Math.abs(1-(a*x[i]));
    }
    return x;
}
```

ภาพที่ ข.1 ส่วนของ Chaotic map ที่ใช้ค่าไม่เป็นเชิงเส้นแบบค่าสัมบูรณ์

```
public Bitmap getKey_im(double[] x, Bitmap image)
{
    Bitmap key = Bitmap.createBitmap(image.getWidth(), image.getHeight(), Config.ARGB_8888);
    int[] xRGB = new int[x.length];
    int bit_asc = 0;
    int bit_dsc = xRGB.length-1;
    int bit_as2 = xRGB.length/2;
    for(int i=0;i<xRGB.length;++i)
        xRGB[i] = (int)Math.round(x[i]*255);
    for(int hor=0;hor<key.getWidth();++hor)
    {
        for(int ver=0;ver<key.getHeight();++ver)
        {
            key.setPixel(hor,ver,Color.argb(255, xRGB[bit_asc], xRGB[bit_dsc], xRGB[bit_as2]));
            ++bit_asc;
            --bit_dsc;
            ++bit_as2;
            if(bit_as2>xRGB.length-1)
            {
                bit_as2 = 0;
            }
        }
    }
    return key;
}
```

ภาพที่ ข.2 ส่วนการสร้างกุญแจเข้ารหัสรูปภาพ

```
public Bitmap scrImage(Bitmap image, double[] x, int mode)
{
    Bitmap target = image.copy(Config.ARGB_8888, true);
    int[] seq = new int[x.length];
    for(int i=0;i<seq.length;++i)
        seq[i] = (int)Math.round(x[i]*(x.length-1));
    int pos;
    if(mode==0)
    {
        pos = 0;
        for(int hor=0;hor<target.getWidth();++hor)
        {
            for(int ver=0;ver<target.getHeight();++ver)
            {
                int pix = target.getPixel(hor, ver);
                target.setPixel(hor, ver, target.getPixel((seq[pos]/target.getHeight()), (seq[pos]%target.getHeight())));
                target.setPixel(seq[pos]/target.getHeight(), seq[pos]%target.getHeight(), pix);
                ++pos;
            }
        }
    }
    else
    {
        pos = seq.length-1;
        for(int hor=target.getWidth()-1;hor>=0;--hor)
        {
            for(int ver=target.getHeight()-1;ver>=0;--ver)
            {
                int pix = target.getPixel(hor, ver);
                target.setPixel(hor, ver, target.getPixel((seq[pos]/target.getHeight()), (seq[pos]%target.getHeight())));
                target.setPixel(seq[pos]/target.getHeight(), seq[pos]%target.getHeight(), pix);
                --pos;
            }
        }
    }
    return target;
```

ภาพที่ ข.3 ส่วนการสลับตำแหน่งพิกเซลของรูปภาพ

ภาคผนวก ค.

Code ส่วนการ XOR รูปภาพโดยใช้ Library OpenCV

และส่วนการส่งออกผลลัพธ์เป็นรูปภาพ

```
public Bitmap xorBitmap(Bitmap im1, Bitmap im2)
{
    Bitmap res = Bitmap.createBitmap(im1.getWidth(), im1.getHeight(), Config.ARGB_8888);
    Mat mat_im_1 = new Mat(im1.getHeight(), im1.getWidth(), CvType.CV_8UC4);
    Mat mat_im_2 = new Mat(im2.getHeight(), im2.getWidth(), CvType.CV_8UC4);
    Mat mat_im_res = new Mat(im1.getHeight(), im1.getWidth(), CvType.CV_8UC4);
    List<Mat> planes1 = new ArrayList<Mat>(4);
    List<Mat> planes2 = new ArrayList<Mat>(4);
    List<Mat> planesR = new ArrayList<Mat>(4);
    Utils.bitmapToMat(im1, mat_im_1);
    Utils.bitmapToMat(im2, mat_im_2);
    Utils.bitmapToMat(res, mat_im_res);
    Core.split(mat_im_1, planes1);
    Core.split(mat_im_2, planes2);
    Core.split(mat_im_res, planesR);
    Core.bitwise_xor(planes1.get(0), planes2.get(0), planesR.get(0));
    Core.bitwise_xor(planes1.get(1), planes2.get(1), planesR.get(1));
    Core.bitwise_xor(planes1.get(2), planes2.get(2), planesR.get(2));
    planesR.set(3, planes1.get(3));
    Core.merge(planesR, mat_im_res);
    Utils.matToBitmap(mat_im_res, res);
    return res;
}
```

ภาพที่ ค.1 ส่วนการ XOR รูปภาพด้วย Library OpenCV

```
@SuppressLint("SimpleDateFormat") public void outBitmap()
{

    Bitmap outBmp = ((BitmapDrawable)imScr.getDrawable()).getBitmap();
    outBmp.setHasAlpha(true);
    OutputStream imOut = null;
    try
    {
        String f_path = Environment.getExternalStorageDirectory().getAbsolutePath()+"/CryptoRes";
        File fd_path = new File(f_path);
        if(!fd_path.exists())
        {
            fd_path.mkdir();
        }
        String t_st = new SimpleDateFormat("ddMMyyyy_HHmm").format(new Date());

        File im_file = new File(fd_path,"res"+t_st+".png");
        imOut = new FileOutputStream(im_file);
        outBmp.compress(Bitmap.CompressFormat.PNG, 100, imOut);
        imOut.flush();
        imOut.close();
        Toast.makeText(this, "Export completed", Toast.LENGTH_SHORT).show();
    }
    catch(Exception e)
    {
        Toast.makeText(this, "Error in file export", Toast.LENGTH_SHORT).show();
    }
}
```

ภาพที่ ค.2 ส่วนการส่งออกผลลัพธ์เป็นรูปภาพ