วิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งโดยใช้การแยกระนาบบิตและเคโอติกแม็ปหลายชนิด

นางสาววิภาวดี อวยพร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2557

A ROBUST IMAGE ENCRYPTION METHOD BASED ON BIT PLANE DECOMPOSITION AND MULTIPLE CHAOTIC MAPS

Miss Wipawadee Auyporn

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering Program in Computer Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2014

หัวข้อวิทยานิพนธ์	วิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งโดยใช้การแยกระนาบบิตและเคโอติกแม็ปหลายชนิด
โดย	นางสาววิภาวดี อวยพร
สาขาวิชา	วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร. สาธิต วงศ์ประทีป

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร. บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร. สมชาย ประสิทธิ์จูตระกูล)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์ ดร. สาธิต วงศ์ประทีป)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร. อาทิตย์ ทองทักษ์)

.....กรรมการภายนอกมหาวิทยาลัย

(ดร. มหศักดิ์ เกตุฉ่ำ)

วิภาวดี อวยพร : วิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งโดยใช้การแยกระนาบบิตและเคโอติกแม็ปหลายชนิด (A ROBUST IMAGE ENCRYPTION METHOD BASED ON BIT PLANE DECOMPOSITION AND MULTIPLE CHAOTIC MAPS) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร. สาธิต วงศ์ประทีป, 104 หน้า.

การรักษาความปลอดภัยของสื่อมัลติมีเดียเป็นสิ่งสำคัญมากสำหรับการสื่อสารมัลติมีเดียผ่านเครือข่ายเปิด สำหรับบางโปรแกรมประยุกต์นั้นมีความจำเป็นต้องใช้วิธีการเข้ารหัสภาพที่ประสิทธิภาพด้านความปลอดภัยสูง งานวิจัยนี้มีวัตถุประสงค์เพื่อออกแบบวิธีการเข้ารหัสภาพให้มีความปลอดภัยสูง เนื่องจากวิธีการเข้ารหัสแบบเดิมเช่น DES, AES และ RSA ไม่เหมาะที่จะใช้กับข้อมูลภาพเพราะภาพโดยทั่วไปมีค่าสหสัมพันธ์และความซ้ำซ้อนระหว่างจุดภาพในระดับสูง โดยการประยุกต์ใช้สองแนวคิด อันได้แก่ การแยกระนาบบิตและเคโอติกแม็ปหลายชนิด วิธีการเข้ารหัสที่นำเสนอมีความแข็งแกร่งมากขึ้น เหมาะที่จะนำไปใช้กับข้อมูลภาพ โดยในขั้นตอนการสร้างความสับสนในหมู่จุดภาพของการเข้ารหัส ข้อมูลภาพจะถูกแบ่งแยกออกเป็น 8 ระนาบบิต จากนั้นแต่ละระนาบบิตจะถูกเรียงสับเปลี่ยนตามเคโอติกแม็ปต่างชนิดกัน แล้วระนาบบิตทั้งหมดจะถูกประกอบกลับเข้ามาใหม่ และถูกดำเนินการ XOR กับเมทริกซ์บิตแบบสุ่มเพื่อปรับเปลี่ยนค่าของจุดภาพทั้งหมดอย่างสมบูรณ์ ในขั้นตอนการแพร่นั้นข้อมูลภาพจะถูกแพร่ตามลำดับที่สร้างขึ้นใหม่อีกลำดับหนึ่งและดำเนินการ XOR อีกครั้งกับเมทริกซ์บิตแบบสุ่มอีกอันก่อนที่จะวนซ้ำ การวัดประสิทธิภาพการทำงานของวิธีที่นำเสนอนั้นจะใช้การวิเคราะห์ทางสถิติ การวิเคราะห์ขนาดของกุญแจ และการวิเคราะห์ความไวต่อการเปลี่ยนแปลงค่าเริ่มต้น ผลที่ได้รับแสดงให้เห็นว่าวิธีการเข้ารหัสภาพที่นำเสนอเป็นวิธีที่มีความปลอดภัยสูงและทนทานต่อการโจมตีแบบต่างๆ

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2557

5570563321 : MAJOR COMPUTER ENGINEERING
KEYWORDS: IMAGE ENCRYPTION / CHAOTIC MAPS / CONFUSION-DIFFUSION PROPERTIES

WIPAWADEE AUYPORN: A ROBUST IMAGE ENCRYPTION METHOD BASED ON BIT PLANE DECOMPOSITION AND MULTIPLE CHAOTIC MAPS. ADVISOR: ASSOC. PROF. SARTID VONGPRADHIP, Ph.D., 104 pp.

Multimedia security is very important for multimedia communications over open network. For some applications, the highly robust image encryption approach is needed. This project aims to design a high security image encryption method, since the conventional encryption methods such as DES, AES, and RSA do not suit for image data because there are high correlations and redundancy among pixels in natural images. By using two concepts; bit plane decomposition and multiple chaotic maps, the proposed encryption scheme offers more robust encryption method that is suitable for image data. In the confusion stage of the encryption, the image data is decomposed into eight bit planes, and then each bit plane is permuted separately based on different chaotic map. After that, eight bit planes are recomposed and performed XOR operation with a generated random bit matrix in order to alter all pixel values completely. In diffusion stage, the image is diffused based on a new generated sequence, and performed XOR operation again with another random bit matrix before iterating the diffusion process. The performance of the proposed method is evaluated by using statistical, key space, and key sensitivity analysis. The results show that the proposed image encryption method is very secure and robust against different attacks.

Department:	Computer Engineering	Student's Signature	.....
Field of Study:	Computer Engineering	Advisor's Signature	.....
Academic Year:	2014		

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี ขอกราบขอบพระคุณรองศาสตราจารย์ ดร. สาธิต วงศ์ประทีป ซึ่งเป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ท่านได้กรุณาสละเวลา ให้คำปรึกษา คำแนะนำเกี่ยวกับการทำวิจัย และให้การสนับสนุนเป็นอย่างดีจนทำให้งานวิจัยในครั้งนี้ประสบความสำเร็จ

ขอกราบขอบพระคุณคณะกรรมการสอบวิทยานิพนธ์ทุกท่านเป็นอย่างสูง ได้แก่ รองศาสตราจารย์ ดร. สมชาย ประสิทธิ์จูตระกูล ผู้ช่วยศาสตราจารย์อาทิตย์ ทองเพิ่ม และอาจารย์ ดร.มหศักดิ์ เกตุฉ่ำ ได้ให้ข้อคิด คำแนะนำ ที่เป็นประโยชน์อย่างยิ่งในการตรวจแก้วิทยานิพนธ์

ขอขอบพระคุณอาจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ จุฬาลงกรณ์มหาวิทยาลัยทุกท่านเป็นอย่างสูงที่ให้ข้อคิดและแนวทางในการทำวิจัย ขอขอบคุณเจ้าหน้าที่ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ทุกท่าน รวมถึงเพื่อนๆในหลักสูตร วศ.ม.ก2 และเพื่อนๆพี่น้องทุกคนในห้องวิจัย DSEL ที่ได้ให้การช่วยเหลือ คำแนะนำ และกำลังใจตลอดมาในการทำวิจัย

ท้ายที่สุดขอกราบขอบพระคุณนาวาอากาศตรีสุพจน์ อวยพรและนางวิจิตรา อวยพร รวมถึงร้อยเอกวีระพงษ์ อวยพร บิดามารดาและพี่ชายของผู้วิจัยซึ่งให้การสนับสนุน คอยเป็นห่วงเป็นใย และให้กำลังใจแก่ผู้วิจัยเสมอมา นอกจากนี้ผู้วิจัยขอขอบคุณท่านอื่นๆที่ไม่ได้กล่าวชื่อไว้ ณ ที่นี้ที่มีส่วนช่วยเหลือทำให้วิทยานิพนธ์ฉบับนี้สำเร็จเรียบร้อยลงได้ด้วยดีทุกประการ

สารบัญ

หน้า

หน้า

หน้า

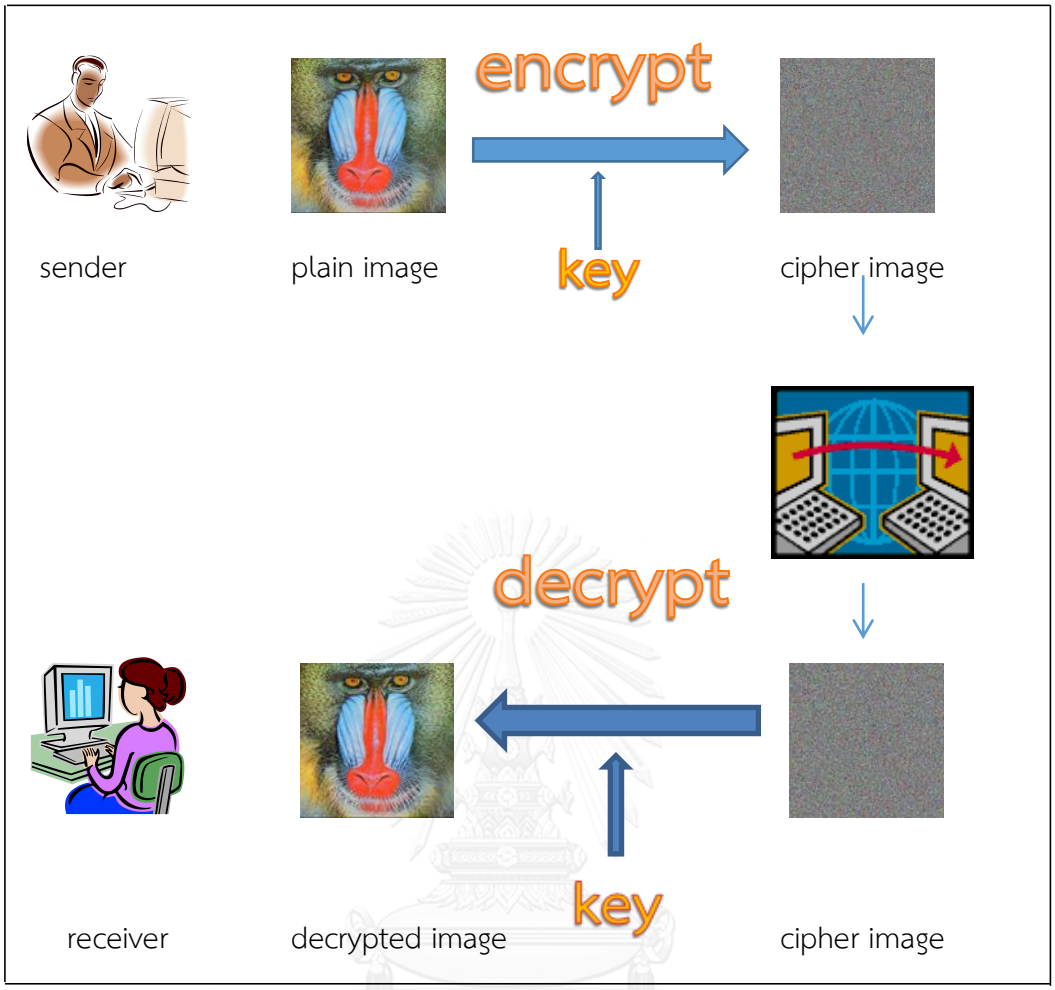
สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

เนื่องจากในยุคปัจจุบันมีข้อมูลมัลติมีเดียประเภทต่างๆ ถูกส่งทางอินเตอร์เน็ตอย่างแพร่หลาย อาทิเช่น ข้อมูลที่เป็นข้อความ ข้อมูลที่เป็นไฟล์ภาพ ข้อมูลที่เป็นไฟล์เสียง หรือ ข้อมูลที่เป็นไฟล์วีดีโอ เป็นต้น ซึ่งข้อมูลเหล่านี้อาจถูกเข้าถึงโดยบุคคลผู้ไม่พึงประสงค์ได้ และข้อมูลบางอย่างถือเป็นความลับที่ไม่สามารถแพร่งพรายออกสู่ภายนอก เช่น ภาพถ่ายส่วนตัว ภาพถ่ายทางการแพทย์ หรือภาพถ่ายทางการทหาร เป็นต้น วิทยาการเข้ารหัสลับ (Cryptography) [1] จึงเป็นศาสตร์ที่มีความจำเป็นอย่างยิ่งที่จะนำมาช่วยรักษาความลับของข้อมูล (Confidentiality) ในการสื่อสารข้อมูลระหว่างกันเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลสามารถเข้าถึงข้อมูลได้ นอกจากนั้นการเข้ารหัสข้อมูลยังช่วยให้ข้อมูลสามารถตรวจสอบความสมบูรณ์ได้ (Integrity) กล่าวคือ ผู้รับจะสามารถตรวจสอบได้ว่าข้อมูลที่ได้รับมานั้นถูกต้องตามที่ผู้ส่งส่งมาให้โดยข้อมูลไม่มีการสูญหายหรือถูกเปลี่ยนแปลงแก้ไขใดๆ และยังทำให้สามารถพิสูจน์ตัวตนของผู้ส่งข้อมูลได้ (Authentication) เพื่อให้ทราบว่าใครคือผู้ส่งข้อมูลตัวจริงซึ่งเป็นการป้องกันการแอบอ้างได้ และโดยพื้นฐานแล้วกระบวนการในการเข้ารหัสข้อมูลจะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์ที่ใช้แปรเปลี่ยนข้อมูลตั้งต้นไปสู่ข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้โดยใครก็ตามที่ไม่มีกุญแจ (key) สำหรับเปิดดูข้อมูลนั้น เราเรียกกระบวนการในการแปรรูปข้อมูลตั้งต้นว่า การเข้ารหัสข้อมูล (Encryption) [2] ส่วนกระบวนการในการแปลงข้อมูลที่เข้ารหัสไว้คืนสู่สภาพเดิมก่อนการเข้ารหัสเรียกว่า การถอดรหัสข้อมูล (Decryption) ซึ่งในงานวิจัยนี้เราสนใจศึกษาวิธีการเข้ารหัสข้อมูลที่เป็นไฟล์ภาพ (Image Encryption)



ภาพที่ 1-1 การเข้ารหัสข้อมูลภาพและการถอดรหัสข้อมูลภาพแบบสมมาตร

ในปัจจุบันมีงานวิจัยเกี่ยวกับวิธีการเข้ารหัสข้อมูลภาพค่อนข้างมาก ซึ่งในแต่ละงานวิจัยก็มุ่งเน้นที่การออกแบบวิธีการเข้ารหัสข้อมูลภาพเพื่อรักษาความลับของข้อมูลที่ระดับความปลอดภัยต่างๆกัน เนื่องจากในแต่ละงานประยุกต์นั้นต้องการใช้วิธีการเข้ารหัสที่แตกต่างกันตามความจำเป็นของงานประยุกต์นั้นๆ [3] เช่น ข้อมูลภาพบางประเภทต้องการเพียงระดับความปลอดภัยปานกลางเพื่อแลกกับการประมวลผลแบบทันกาล (Real-time) [4] ข้อมูลภาพบางประเภทต้องการระดับความปลอดภัยสูงโดยยอมให้เวลาในการประมวลผลมากขึ้นนิดหน่อยได้ และข้อมูลภาพบางประเภทต้องการระดับความปลอดภัยสูง [5] คือไม่ต้องการให้บุคคลที่สามสามารถโจมตีการเข้ารหัสได้ไม่ว่ากรณีใดๆก็ตาม และในงานวิจัยนี้เราสนใจศึกษาและออกแบบวิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งและทนทานต่อการโจมตีในรูปแบบต่างๆที่หลากหลาย เพื่อนำไปใช้ประโยชน์ในงานประยุกต์ที่ต้องการวิธีการเข้ารหัสภาพที่มีความปลอดภัยสูง

วิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งนั้นมีความซับซ้อนกว่าวิธีการเข้ารหัสข้อมูลที่เป็นข้อความธรรมดา เนื่องจากข้อมูลภาพเป็นข้อมูลที่มีลักษณะพิเศษ คือ เป็นข้อมูลชนิดสองมิติที่จุดภาพ (pixel) ที่อยู่ติดกันนั้นมีความสัมพันธ์กันสูง (High Correlations) และค่าสีระหว่างจุดภาพที่ใกล้ๆกันก็ยังมีโอกาสซ้ำซ้อนกันสูง (High Redundancy) ตามธรรมชาติของภาพโดยทั่วไป[6] ซึ่งถ้าใช้วิธีการเข้ารหัสแบบธรรมดา เช่น DES, triple DES, AES, RSA algorithm กับข้อมูลภาพอาจจะทำให้ข้อมูลถูกโจมตีได้ง่าย[7] ดังนั้นจึงได้มีผู้เสนอวิธีการในการเข้ารหัสข้อมูลภาพเพื่อแก้ปัญหานี้หลายวิธีการ โดยวิธีการในกลุ่มที่เราสนใจคือการนำเคโอติกแม็ป (Chaotic maps)[7-11] มาประยุกต์ใช้ในขั้นตอนการสร้างความไร้ระเบียบ (Confusion stage) ให้แก่ข้อมูลตั้งต้น เนื่องจากเคโอติกแม็ปมีคุณสมบัติทางคณิตศาสตร์หลายประการที่สามารถเทียบเคียงกับสิ่งที่วิธีการเข้ารหัสข้อมูลที่ดีจำต้องมีด้วย [12] เช่น เคโอติกแม็ปมีพารามิเตอร์ที่กำหนดได้ (Parameter) ส่วนวิธีการเข้ารหัสข้อมูลต้องมีกุญแจ (Key) ด้วยเช่นกัน เคโอติกแม็ปมีความไวต่อสถานะเริ่มต้นและปัจจัยควบคุม (Sensitivity to initial conditions and control parameters) ส่วนวิธีการเข้ารหัสจำเป็นต้องมีคุณสมบัติการแพร่กระจาย (Diffusion property) หรือ butterfly effect ด้วยเป็นต้น จะเห็นได้ว่าระหว่างเคโอติกแม็ปกับการเข้ารหัสข้อมูลนั้นมีคุณสมบัติหลายประการที่สามารถเทียบเคียงกันได้ จึงน่าสนใจเป็นอย่างยิ่งที่จะนำเคโอติกแม็ปมาประยุกต์ใช้ในการเข้ารหัสข้อมูล

โดยจุดมุ่งหมายของงานวิจัยนี้คือเพื่อศึกษาออกแบบและพัฒนาวิธีการเข้ารหัสข้อมูลรูปภาพให้มีความปลอดภัยมากขึ้น ซึ่งนอกจากเราจะพิจารณาใช้เคโอติกแม็ปแล้วเรายังจะทดลองใช้การแยกระนาบบิตของข้อมูลภาพก่อนด้วย (Bit Plane Decomposition) คือนำแต่ละระนาบบิตไปเรียงสับเปลี่ยนใหม่ (Permutation) โดยใช้เคโอติกแม็ปที่แตกต่างกันออกไป ทั้งนี้เพื่อให้การสลับสับเปลี่ยนของจุดภาพมีความซับซ้อนมากขึ้น ด้วยสมมติฐานที่ว่าสิ่งนี้จะสามารถเพิ่มความไร้ระเบียบของข้อมูล (Entropy) ให้แก่ข้อมูลภาพที่ถูกเข้ารหัส เนื่องด้วยวิธีการนี้ค่าสีของแต่ละจุดภาพจะถูกเปลี่ยนแปลงไปโดยสิ้นเชิงและยังถูกสลับตำแหน่งด้วยตั้งแต่ขั้นตอนนี้ ทำให้สามารถสลัดคุณลักษณะของความเป็นภาพต้นฉบับทิ้งได้อย่างสมบูรณ์และมีประสิทธิภาพยิ่งขึ้น ซึ่งการนำวิธีการแยกระนาบบิต (Bit plane decomposition) และเคโอติกแม็ปหลายๆชนิด (Multiple Chaotic Maps) มารวมกันในลักษณะนี้เป็นวิธีการเข้ารหัสข้อมูลที่เราพัฒนาขึ้นใหม่เพื่อให้มีความซับซ้อนมากกว่าวิธีการในปัจจุบัน และผลลัพธ์ที่คาดว่าจะได้รับคือเราจะได้วิธีการที่มีความแข็งแกร่งและมีความทนทานสูงมากขึ้นต่อการโจมตีที่หลากหลาย โดยแลกกับเวลาในการประมวลผลที่เพิ่มขึ้นเล็กน้อยและอยู่ในระดับที่ยอมรับได้และนำไปใช้ได้จริง เพื่อที่เราจะได้วิธีการที่เหมาะที่จะนำไปใช้กับข้อมูลภาพที่ต้องการวิธีการเข้ารหัสที่ระดับความปลอดภัยสูง ทั้งนี้เราจะวัดประสิทธิภาพโดย 1. การวิเคราะห์เอนโทรปีหรือความไร้ระเบียบของข้อมูล (Entropy Analysis) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Entropy Attack หรือไม่ 2. การวิเคราะห์ค่าทางสถิติของข้อมูลภาพ (Statistical Analysis) เช่น ฮิสโทแกรมของภาพ (Image Histogram) และ ค่าสัมประสิทธิ์ของความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficients) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Statistical Attack

หรือไม่ 3. การวิเคราะห์ขนาดของกุญแจ (Key Space Analysis) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Brute force หรือไม่ และ 4. การวิเคราะห์คุณสมบัติการแพร่กระจายของจุดภาพ (Diffusion Analysis/Sensitivity Analysis) เช่น วัดค่า NPCR และค่า UACI เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Differential Attack หรือไม่ [13-17]

1.2 วัตถุประสงค์ของการวิจัย

เพื่อศึกษาออกแบบและพัฒนาวิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งขึ้น โดยใช้เทคนิคการแบ่งข้อมูลภาพออกเป็นระนาบบิตต่างๆก่อนและประยุกต์ใช้เคโอติกแม็ปต่างชนิดกัน ได้แก่ Discretized Standard Map, Logistic Map และ Tinkerbell Map ในการเรียงสับเปลี่ยนบิตในแต่ละระนาบบิตอย่างสุ่มเทียมและเป็นอิสระต่อกัน เพื่อให้ภาพที่ถูกเข้ารหัสมีคุณสมบัติความไร้ระเบียบและการแพร่ (Confusion and Diffusion Properties) ที่ดีขึ้น และทำให้วิธีการมีความทนทานมากขึ้นต่อการโจมตีแบบเอนโทรปี การโจมตีแบบสถิติ การโจมตีแบบตะลุย และการโจมตีแบบใช้ความต่างด้วย

1.3 ขอบเขตของการวิจัย

1. เป็นวิธีการเข้ารหัสข้อมูลรูปภาพสี (Color Image Encryption) และใช้กับภาพระดับเทาได้ โดยไม่รวม Metadata

2. เป็นวิธีการเข้ารหัสแบบสมมาตร นั่นคือ ใช้กุญแจเดียวกันในการเข้ารหัสและถอดรหัส (Symmetric Key Encryption)

3. เป็นวิธีการเข้ารหัสข้อมูลภาพที่ใช้เคโอติกแม็ปเข้ามามีส่วนช่วย (Chaos-Based Image Encryption)

4. มีการประยุกต์ใช้เทคนิคการแยกระนาบบิต (Bit-Plane Decomposition) และการเรียงสับเปลี่ยนในระดับบิต (Bit-Level Permutation) ด้วย

5. ไม่ได้เป็นการการเข้ารหัสและการถอดรหัสแบบทันกาล (Real Time)

6. ไม่สามารถกู้คืนข้อมูลได้หากได้รับข้อมูลภาพที่เข้ารหัสที่ผิดเพี้ยนไป (ไม่ทนทานต่อ Data Loss Attack และ Noise Attack) เนื่องจากไม่มี Error Correction

7. เกณฑ์การวัดประสิทธิภาพมี 4 แบบด้วยกัน คือ

   a. การวิเคราะห์เอนโทรปีหรือความไร้ระเบียบของข้อมูล (Entropy Analysis)

b. การวิเคราะห์ค่าทางสถิติของข้อมูลภาพ (Statistical Analysis) เช่น ฮิสโทแกรมของภาพ (Image Histogram) และ ค่าสัมประสิทธิ์ของความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficients)

c. การวิเคราะห์ขนาดของกุญแจ (Key Space Analysis)

d. การวิเคราะห์คุณสมบัติการแพร่กระจายของจุดภาพ (Diffusion Analysis/Sensitivity Analysis) เช่น วัดค่า NPCR และค่า UACI

8. ใช้เกณฑ์การทดสอบประสิทธิภาพตามข้อ 7 วัดความทนทานต่อการโจมตีรูปแบบต่างๆตามลำดับ ดังต่อไปนี้

a. การโจมตีแบบเอนโทรปี (Entropy Attack)

b. การโจมตีแบบสถิติ (Statistical Attack)

c. การโจมตีแบบตะลุย (Brute Force Attack) หรือ การโจมตีโดยใช้เวลา (Timing Attack)

d. การโจมตีแบบใช้ผลต่าง (Differential Attack) หรือ การโจมตีโดยใช้การแพร่ (Diffusion Attack) เช่น

- Known Plain Text/Image Attack
- Known Cipher Text/Image Attack
- Chosen Plain Text/Image Attack
- Chosen Cipher Text/Image Attack

9. วัดเวลาที่ใช้ในการเข้ารหัสภาพและการถอดรหัสภาพจากโปรแกรมMatlab r2012a ที่ใช้ทดลอง เพื่อให้ทราบว่างานวิจัยนี้สามารถนำไปใช้ได้จริง

10. มีการเปรียบเทียบประสิทธิภาพของวิธีการที่นำเสนอกับวิธีการใกล้เคียงที่มีอยู่ในปัจจุบัน

1.4 ข้อตกลงเบื้องต้น

1. ภาพต้นฉบับ (Original Image หรือ Plain Image) หมายถึง ภาพหลักที่มีความสมบูรณ์สกุล TIFF, PNG หรือ JPG

2. ภาพที่ถูกเข้ารหัส (Encrypted Image หรือ Cipher Image) หมายถึง ภาพต้นฉบับที่ผ่านกระบวนการเข้ารหัสและใส่กุญแจลับเพื่อแปลงเปลี่ยนเป็นภาพที่อ่านความไม่ได้ ด้วยเหตุผลทางด้านความปลอดภัย

3. ภาพที่ถูกถอดรหัส (Decrypted Image) หมายถึง ภาพที่ถูกเข้ารหัสที่ผ่านกระบวนการถอดรหัสและใส่กุญแจลับเพื่อให้ได้มาซึ่งภาพต้นฉบับที่อ่านได้

4. เวลาที่ใช้ในการเข้ารหัสภาพ (Image Encryption Time) หมายถึง ระยะเวลาตั้งแต่นำภาพต้นฉบับเข้าสู่กระบวนการเข้ารหัสจนได้ภาพที่ถูกเข้ารหัส

5. เวลาที่ใช้ในการถอดรหัสภาพ (Image Decryption Time) หมายถึง ระยะเวลาตั้งแต่นำภาพที่ถูกเข้ารหัสเข้าสู่กระบวนการถอดรหัสจนได้ภาพที่ถูกถอดรหัส

6. คุณสมบัติความไร้ระเบียบ (Confusion Property) หมายถึง การที่ข้อมูลหรือข้อมูลภาพที่ถูกเข้ารหัส (Cipher-text /Cipher-image) ไม่สัมพันธ์กับกุญแจ (key) ในทางใดทางหนึ่ง (Shannon, 1949)

7. คุณสมบัติการแพร่ (Diffusion Property) หมายถึง การที่เปลี่ยนข้อมูลหรือข้อมูลภาพต้นฉบับ (Plain-text/Plain-image) เพียงเล็กน้อยกระทบต่อข้อมูลหรือข้อมูลภาพที่ถูกเข้ารหัส (Cipher-text /Cipher-image) ทั้งหมด หรือที่รู้จักกันดีในชื่อปรากฏการณ์ผีเสื้อขยับปีก (Butterfly Effect) (Shannon, 1949)

8. สภาพไร้ระเบียบ (Chaos) หมายถึง สภาพไร้เสถียรภาพ (unstable) มีความอ่อนไหวสูงยิ่ง หรือมีความเปราะบาง เมื่อมีการกระทบเพียงเล็กน้อยก็ทำให้เกิดความเปลี่ยนแปลงไปอย่างไม่เป็นเส้นตรง แต่เป็นทางที่คดเคี้ยว กวัดแกว่ง และบางครั้งก้าวกระโดด เกิดตรงจุดนั้นบ้าง จุดนี้บ้าง ทำให้ยากที่จะทำนายผลลัพธ์ได้ เพราะมีสิ่งอื่น ๆ ที่มาเป็นองค์ประกอบหลาย ๆ ประการที่ส่งผลต่อระบบใหญ่

9. ปรากฏการณ์ผีเสื้อขยับปีก (Butterfly Effect) หมายถึง เรื่องเล็กๆเช่นการที่ผีเสื้อกระพือปีกสามารถก่อให้เกิดเรื่องใหญ่ๆที่ไม่คาดคิดในระยะทางไกลๆได้

10. การเบรก (break) หมายถึง การถอดรหัสข้อมูลออกมาได้ ถึงแม้จะไม่ทราบวิธีการเข้ารหัสและไม่มีกุญแจที่ใช้ถอดรหัสก็ตาม

11. การโจมตีแบบเอนโทรปี (Entropy Attack) หมายถึง การโจมตีโดยการวิเคราะห์ความไร้ระเบียบของข้อมูล (หาได้จากการวัดค่าเอนโทรปี) ตัวอย่างง่ายๆ เช่น การโจมตีโดยดูจากความถี่ของข้อมูล นำไปเทียบความความรู้ที่มีอยู่ก่อนหน้าและหาอัลกอริทึมในการเข้ารหัส

12. การโจมตีแบบสถิติ (Statistical Attack) หมายถึง การโจมตีโดยการนำข้อมูลทางสถิติของข้อมูลหรือข้อมูลภาพที่ถูกเข้ารหัส (Cipher-text/Cipher-image) ไปวิเคราะห์เพื่อหาคุณลักษณะของข้อมูลต้นฉบับ ข้อมูลทางสถิติของรูปภาพ เช่น

- ฮิสโทแกรม (Histogram)

- ค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficients)

13. การโจมตีแบบตะลุย (Brute Force Attack) หรือ การโจมตีโดยใช้เวลา (Timing Attack) หมายถึง การโจมตีด้วยการลองถอดรหัสลับด้วยกุญแจทุกๆรูปแบบที่เป็นไปได้ ซึ่งการโจมตีลักษณะนี้ฟังก์ชันการทำงานที่ใช้ในการถอดรหัสลับจะมีค่าเพิ่มขึ้นแบบ exponential ตามขนาดของกุญแจ

14. การโจมตีแบบใช้ผลต่าง (Differential Attack) หมายถึง การโจมตีด้วยข้อมูลภาพที่ทราบและทดสอบโดยอาศัยผลต่างทีละเล็กทีละน้อยไปเรื่อยๆ จนสามารถหากุญแจลับได้

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1. ทำให้ได้วิธีการเข้ารหัสข้อมูลภาพที่มีความแข็งแกร่งและทนทานมากขึ้นต่อการโจมตีที่หลากหลาย

2. สามารถนำวิธีการเข้ารหัสข้อมูลภาพที่ได้พัฒนาขึ้นนี้ไปใช้งานได้จริงในงานประยุกต์ที่ต้องการความปลอดภัยสูง

3. ทำให้เกิดแนวทางการวิจัยด้านการเพิ่มความปลอดภัยในการพัฒนาระบบการเข้ารหัสข้อมูลภาพ

1.6 ลำดับขั้นตอนในการเสนอผลการวิจัย

1. ศึกษาทฤษฎี หลักการพื้นฐานที่ใช้ในการวิจัย และงานวิจัยที่เกี่ยวข้อง

2. ศึกษาเทคนิคต่างๆ ที่มีอยู่ก่อนหน้า รวมถึงแนวคิด หลักการ ข้อดี ข้อเสียของแต่ละเทคนิค

3. กำหนดวัตถุประสงค์ และตั้งสมมติฐาน
4. ออกแบบแนวทางการวิจัยทดลอง
5. ทดสอบและปรับปรุงวิธีการที่นำเสนอ
6. วิเคราะห์ผลการทดลอง
7. สรุปผลและเรียบเรียงวิทยานิพนธ์และนำเสนอผลงานวิจัย

1.7 งานวิจัยที่ได้รับการตีพิมพ์

W. Auyporn and S. Vongpradtip, A Robust Image Encryption Method Based On Bit Plane Decomposition and Multiple Chaotic Maps, 2014 IACSIT International Conference on Communication and Signal Processing (ICCSP2014), Bangkok, Thailand, 10-12 October 2014, pp. 70-76.

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในส่วนนี้เป็นทฤษฎีที่เกี่ยวข้องกับวิทยาการเข้ารหัสลับ (Cryptography) [1, 2] และงานวิจัยที่เกี่ยวข้องกับการเข้ารหัสภาพ (Image Encryption) [4], [7], [18-32] ซึ่งในส่วนของทฤษฎีนั้นจะกล่าวถึงการเข้ารหัสข้อมูลตั้งแต่ยุคเริ่มต้น จนไปถึงการเข้ารหัสข้อมูลภาพในยุคปัจจุบัน

2.1 ความรู้เบื้องต้นเกี่ยวกับการเข้ารหัสข้อมูลและคำศัพท์ต่างๆที่เกี่ยวข้อง

Crypto แปลว่า "การซ่อน" ส่วน Graph แปลว่า "การเขียน" Cryptography จึงมีความหมายว่า “การเขียนเพื่อซ่อนข้อมูล” Cryptography เป็นระบบการรักษาความปลอดภัยที่ประกอบด้วยการเข้ารหัสข้อมูล (Encryption) และการถอดรหัสข้อมูล (Decryption) โดยมีจุดประสงค์เพื่อป้องกันไม่ให้ผู้อื่นสามารถอ่านข้อมูลได้ ยกเว้นผู้ที่เราต้องการให้อ่านได้เท่านั้น ซึ่งผู้ที่เราต้องการให้อ่านได้จะต้องทราบวิธีการถอดรหัสข้อมูลที่ซ่อนไว้ได้ เพราะฉะนั้นประโยชน์ของ Cryptography คือการรักษาความลับของข้อมูล

Encryption หมายถึง กระบวนการหรือขั้นตอนในการเข้ารหัสข้อมูลที่เปลี่ยนแปลงไปจากเดิม

Decryption หมายถึง กระบวนการหรือขั้นตอนในการถอดรหัสข้อมูล เพื่อให้ข้อมูลที่เข้ารหัสไว้คืนสู่สภาพเดิมก่อนเข้ารหัส

Plain Text/Image หมายถึง ข้อความหรือข้อมูล/ข้อมูลภาพต่างๆที่ยังไม่ผ่านกรรมวิธีการเข้ารหัส

Cipher Text/Image หมายถึง ข้อความหรือข้อมูล/ข้อมูลภาพต่างๆที่ผ่านการเข้ารหัสแล้วและทำให้รูปแบบของข้อมูลเปลี่ยนแปลงไป

Secret Key หมายถึง กุญแจลับที่ใช้ร่วมกับอัลกอริทึมในการเข้ารหัสและถอดรหัส

2.2 ประวัติความเป็นมาเกี่ยวกับวิธีการเข้ารหัสข้อมูลตามยุคสมัย

Cryptography สามารถแบ่งตามยุคสมัยได้เป็น 2 ยุคคือ

1.ยุคประวัติศาสตร์ (หรือที่เรียกว่ายุค Classic)

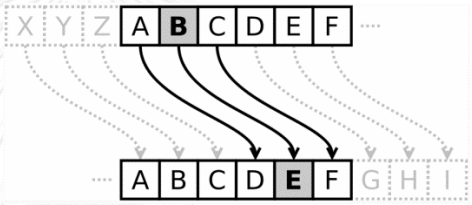
2.ยุคปัจจุบัน (Modern)

2.2.1 การเข้ารหัสในยุคประวัติศาสตร์ (หรือยุค Classic)

2.2.1.1 Caesar cipher

การเข้ารหัสข้อมูลแบบ Caesar cipher มีขึ้นในราว 50-70 ปีก่อนคริสตกาล สร้างโดยกษัตริย์ Julius Caesar แห่งโรมัน เพื่อใช้เข้ารหัสข้อความในสารที่ส่งในระหว่างการทำศึกสงคราม เพื่อป้องกันไม่ให้ศัตรูสามารถอ่านข้อความในสารนั้นได้หากสารนั้นถูกแย่งชิงไป การเข้ารหัสแบบ Caesar cipher จะใช้วิธีการแทนที่ตัวอักษรต้นฉบับด้วยตัวอักษรที่อยู่ห่างออกไปข้างหน้าสามตัวเช่น แทนที่ตัว A ด้วยตัว D และแทนที่ตัว B ด้วยตัว E เป็นต้น ดังนั้นการเข้ารหัสแบบ Caesar cipher จึงเป็นการเลื่อนตัวอักษรโดยจำนวนครั้งของการเลื่อนเท่ากับสาม (Shiftment, n = 3)

การแม็ปของตัวอักษรในการเข้ารหัสแบบ Caesar cipher สามารถเขียนได้ดังนี้



ภาพที่ 2-1 วิธีการเข้ารหัสแบบ Ceasar cipher

การแม็ปของตัวอักษรในการเข้ารหัสแบบ Caesar cipher สามารถเขียนได้ดังนี้

Plain: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Cipher: DEFGHIJKLMNOPQRSTUVWXYZABC

หากใช้การเข้ารหัสข้อมูลแบบ Caesar cipher เข้ารหัส Fox code จะได้ดังนี้

Plaintext: the quick brown fox jumps over the lazy dog

Ciphertext: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

ต่อมา Augustus (ผู้เป็น Caesar องค์ที่สองจากทั้งหมด 12 Caesars) ซึ่งเป็นหลานของ Julius Caesar ได้เปลี่ยนสูตรให้แทนที่ตัว A ด้วยตัว C และแทนที่ตัว B ด้วยตัว D ดังนั้นจึงกลายเป็นการเลื่อนตัวอักษรที่มีจำนวนครั้งของการเลื่อนเท่ากับสอง (Shiftment, n = 2)

การเข้ารหัสทั้งสองวิธีนี้สามารถถูกเบรค (Break) ได้โดยง่าย (การเบรคในที่นี้หมายถึงการถอดรหัสข้อมูลออกมาได้ ถึงแม้จะไม่ทราบวิธีการเข้ารหัสและไม่มีกุญแจที่ใช้ถอดรหัสก็ตาม) การเบรคการเข้ารหัสข้อมูลแบบ Caesar cipher ทำได้โดยการทดลองทำการเลื่อนตัวอักษรทุกตัว โดยทดลองเลื่อนด้วยจำนวน Shiftment ที่ต่างกันคือ n=1, n=2, n=3, ... ไปจนถึง n=26 ซึ่งจะใช้การจำนวนครั้งในการทดสอบสูงสุดเพียง 26 ครั้ง (สำหรับภาษาอังกฤษซึ่งมีเพียง 26 ตัวอักษร) ก็จะสามารถทำการเบรคได้ในที่สุด

2.2.1.2 Mono-alphabetic ciphers

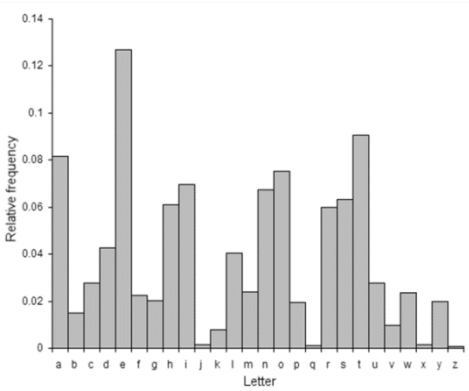
การเข้ารหัสข้อมูลแบบ Mono-alphabetic Cipher (หรือเรียกว่า Mono-alphabetic substitution ciphers) คิดค้นโดยชาวอาหรับ โดยใช้วิธีการแทนที่ตัวอักษรแบบ 1 ต่อ 1 (ไม่ใช่การเลื่อน) ตัวอย่างของ Mono-alphabetic ciphers ในยุคแรก ๆ คือการเข้ารหัสข้อมูลแบบ Atbash ใช้การแทนที่ตัว A ด้วยตัว Z แทนที่ตัว B ด้วยตัว Y และแทนที่ตัว C ด้วยตัว X เป็นต้น

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

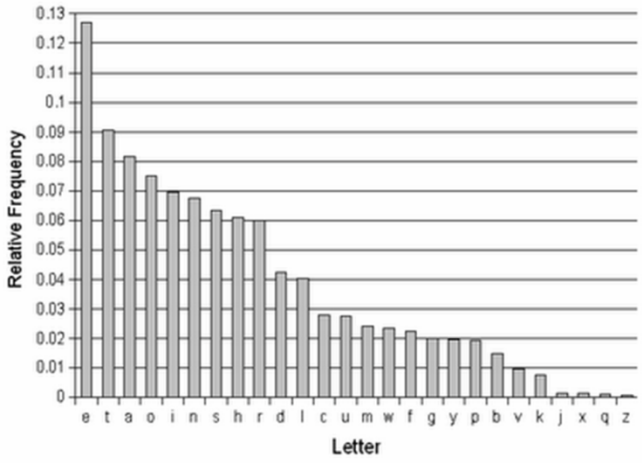
การเบรค Monoalphabetic ciphers จะทำได้ยากกว่าการเบรค Caesar cipher เนื่องจากมีคู่ที่เป็นไปได้อยู่ 26 ยกกำลัง 26 คู่ การเบรคจะต้องใช้การสุ่มไปเรื่อย ๆ จนกว่าจะสำเร็จ ซึ่งจะต้องใช้จำนวนครั้งในการคำนวณการคำนวณถึง 26! ครั้ง (26! = 26 x 25 x 24 x 23 x ... x 1)

การเบรค Mono-alphabetic ciphers สามารถทำได้อีกวิธีหนึ่งคือการวิเคราะห์ความถี่ของตัวอักษรที่ปรากฏ (frequency analysis) ตัวอย่างเช่นตัวอักษร e กับ t จะเกิดบ่อยที่สุดในข้อความภาษาอังกฤษ โดยอักษร e มีอัตราการเกิดบ่อยถึง 13% ส่วนอักษร t มีอัตราการเกิดบ่อยถึง 9%



ภาพที่ 2-2 ความถี่ของตัวอักษรที่ปรากฏ

ตัวอักษรที่พบได้บ่อยมากได้แก่ e, t, a, i, o, n, s, h, y, d และ l ตามลำดับ หากนำมาเรียงตามลำดับจากพบได้มากไปจนถึงพบได้น้อยการนำตัวอักษรที่ใช้บ่อยไปใช้เพื่อถอดรหัสแบบ Monoalphabetic ciphers จะสามารถทำให้เดาและถอดรหัสได้เร็วขึ้น เช่นหากพิจารณาข้อมูลที่เข้ารหัสด้วย Monoalphabetic ciphers แล้วพบว่ามีตัวอักษรตัวหนึ่งที่พบได้บ่อยที่สุด ก็อาจจะสันนิษฐานได้ว่าเป็นตัวอักษรนั้นเป็นตัวอักษรสามารถถอดรหัสกลับได้เป็นตัว e เป็นต้น



ภาพที่ 2-3 ความถี่ของตัวอักษรที่ปรากฏ (เรียงตามความถี่มากไปน้อย)

2.2.1.3 Poly-alphabetic Encryption

Poly-alphabetic Encryption คิดค้นโดย Blaise De Vignere ชาวฝรั่งเศส เมื่อประมาณ 500 ปีที่แล้ว อัลกอริทึมนี้ใช้เทคนิคที่ประกอบไปด้วย Multiple Mono-alpha Cipher คือมี Mono-alphabetic ciphers หลาย ๆ ตัวประกอบกัน ซึ่งจะมีการกำหนดระยะห่างให้กับตัวอักษรก่อนโดยระยะห่างในแต่ละช่วงจะไม่

เท่ากันตัวอย่างเช่น n = 7 ให้เป็น C1 และ n = 15 ให้เป็น C2 หลังจากนั้นกำหนดรูปแบบ (Pattern) ในการใส่ข้อมูล เช่น C1, C2, C2, C1, C2 เป็นต้น

เทคนิคนี้จะใช้ในช่วงสงครามโลกครั้งที่ 1 และยากที่จะถอดรหัสด้วยมือเปล่า แต่ถ้าใช้คอมพิวเตอร์จะสามารถถอดรหัสได้ง่าย นอกจากนั้นหากต้องการจะเบรคโดยใช้คอมพิวเตอร์ก็จะทำการเบรคได้ง่ายเช่นกัน ผู้ที่เบรค Polyalphabetic Encryption ได้เป็นชาวรัสเซียชื่อ Friedrich Kasiski เบรคได้ในปี 1863 โดยให้ข้อสังเกตว่าถ้าได้ Cipher Text ที่มีความยาวมากพอ Pattern จะเริ่มซ้ำ และสามารถที่จะเห็นความเหมือนของ Cipher text โดยดูที่ Frequency Analysis ตัวอักษรแต่ละตัวปรากฏบ่อยแค่ไหน

2.2.1.4 One-Time Pad

One-Time Pad คิดค้นโดย Gilbert Vernam ชาวอังกฤษในช่วงสงครามโลกครั้งที่ 1 เป็นวิธีการเพิ่มความสามารถในการเข้ารหัสให้กับ Polyalphabetic Encryption โดยใช้การแม็ปจาก 1 ตัวอักษรให้เป็นไปได้หลายตัวอักษร ซึ่งมีวิธีการดังนี้ใช้ Key ที่มีขนาดเท่ากันกับ Plain Text

Cipher Text ที่เป็นคำนวณออกมาได้จะมีขนาดเท่ากันกับขนาดของ Plain Text ตัวอักษรทุกตัวจะต้องมีการเปลี่ยนหมดเช่นหาก L ตัวแรกแม็ปได้เป็น N (สมมุติ) แล้ว L ตัวที่สองจะต้องแม็ปได้เป็นตัวอื่นเช่นตัว V เป็นต้น

ใช้ Operation ง่าย ๆ เช่น + เพื่อเข้ารหัสและ - เพื่อถอดรหัส หรือใช้ XOR สำหรับทั้งการเข้ารหัสและถอดรหัส

Plain Text :	**H**	**E**	**L**	**L**	**O**
Key :	**X**	**M**	**C**	**K**	**L**
Cipher Text :	**E**	**Q**	**N**	**V**	**Z**

การเข้ารหัสแบบ One-Time Pad นี้ Cipher Text จะมีความเป็น Random มากหรือน้อยขึ้นอยู่กับความเป็น Random ของ Key ตัวอย่างการเข้ารหัสด้วยวิธี One-Time Pad แสดงดังนี้ (จะเห็นได้ว่า L ตัวแรกแม็ปได้เป็น N ส่วน L ตัวที่สองแม็ปได้เป็น V ขึ้นอยู่กับคีย์

แต่อย่างไรก็ตาม One-Time Pad ก็ยังมีปัญหาอยู่เช่น Key ที่ใหญ่เท่ากับ Plain Text จะต้องใช้พื้นที่มากสำหรับเก็บ Key นอกจากนั้น Key ที่ใหญ่ก็ทำให้ใช้งานได้อย่างลำบาก (หากเทียบกับการใช้ Key ที่มีขนาดเล็ก) นอกจากนั้นผู้ส่ง

ข้อความจะต้องมีการส่ง Key ไปยังปลายทางเพื่อใช้ในการถอดรหัส ซึ่งอาจจะทำให้ Key ถูกขโมยได้ในระหว่างขั้นตอนการส่งคีย์

2.2.1.5 Playfair cipher

Playfair cipher เป็น Block Cipher ตัวแรกเกิดขึ้นในปี ค.ศ. 1854 โดย Sir Charles Wheatstone ซึ่งเล่าให้ Baron Playfair ฟัง แล้วจากนั้นก็ถูกเล่าต่อให้ Albert และ Load Palmerston ฟังบนโต๊ะอาหารเย็น Playfair cipher ถูกใช้ในกองกำลังทางประเทศสหราชอาณาจักรในสงครามโลกครั้งที่ 1 มีขบวนการทำงานของอัลกอริทึมดังนี้

(1) สร้างตาราง Key ขนาด 5 x 5 = 25 แบบสุ่มโดยตัดตัว Q ออก

ตัวย่าง Key ขนาด 5x5

P L A Y F
I R E X M
B C D G H
J K N O S
T U V W Z

(2) แบ่งตัวอักษร Plain Text ต้นฉบับออกมาเป็นคู่ ๆ หากมีตัวอักษรที่ติดกันให้เอา X คั่นกลาง และหากตัวสุดท้ายไม่ครบคู่ให้ใส่ Z เข้าไปแทนเช่น ต้องการเข้ารหัสข้อความว่า "Hide the gold in the tree stump" ก็สามารถจัดตัวอักษรเป็นคู่ ๆ ได้ดังนี้

HI DE TH EG OL DI NT HE TR EX ES TU MP
^

ใส่ X เข้าไปเนื่องจากมีตัว E สองตัวติดกัน

(3) ถ้าไม่อยู่ในแถวและ Column เดียวกัน ให้แทนที่ตัวอักษรแบบไขว้กัน เช่น HI ในข้อความต้นฉบับ (H ไม่ได้อยู่แถวเดียวกันกับ I และ H ก็ไม่ได้อยู่ใน Column เดียวกันกับ I) จะกลายเป็น BM (H กลายเป็น I และ B กลายเป็น M)

(4) ถ้า 2 ตัวอักษรอยู่ Column เดียวกัน ให้เอาตัวอักษรที่อยู่ข้างล่างติดกันมาแทนที่ โดยทำทีละตัว (หากตัวอักษรนั้นอยู่ล่างสุดให้เอาตัวบนสุดมาแทนที่) เช่น DE ในข้อความต้นฉบับ จะกลายเป็น ND เนื่องจาก D ถูกแทนที่ด้วย N ส่วน E ถูกแทนที่ด้วย D

(5) ถ้า 2 ตัวอักษรอยู่แถวเดียวกัน ให้เอาตัวอักษรที่อยู่ขวามือมาแทนที่ โดยทำทีละตัว (หากตัวอักษรนั้นอยู่ขวาสุดให้เอาตัวซ้ายสุดมาแทนที่) เช่น TU ในข้อความต้นฉบับ จะกลายเป็น UV เนื่องจาก T ถูกแทนที่ด้วย U ส่วน U ถูกแทนที่ด้วย V หากทำการเข้ารหัสแล้วจะได้ดังนี้

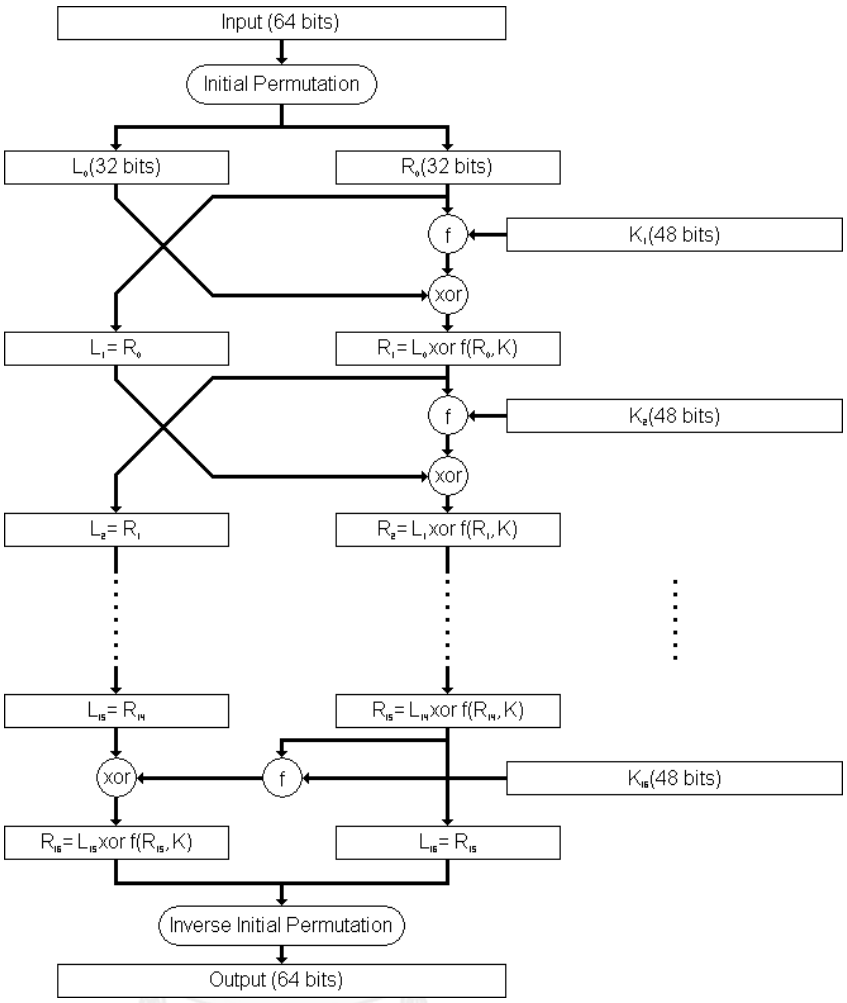
Plain Text: HI DE TH EG OL DI NT HE TR EX ES TU MP
Cipher Text: BM ND ZB XD KY BE JV DM UI XM MN UV IF

2.2.2 การเข้ารหัสในยุค Modern

2.2.2.1 DES (Data Encryption Standard)

DES เป็นการเข้ารหัสแบบ Block cipher ที่พัฒนามาจากอัลกอริทึม Lucifer ของ IBM โดย Lucifer ได้รับการพัฒนาเพิ่มความสามารถและเปลี่ยนชื่อเป็น DES แล้วได้รับการนำเสนอต่อ US NIST (US National Institute of Standards and Technology) ให้กลายเป็นมาตรฐานของการเข้ารหัส

การเข้ารหัสข้อมูลแบบ DES เป็นการเข้ารหัสโดยกระทำกับกลุ่มของข้อมูลขนาด 64 บิต ลำดับแรกข้อมูล 64 บิตนี้จะถูกสลับตำแหน่ง (สลับบิต) จากนั้นจะถูกแบ่งเป็น 2 ส่วนได้แก่ส่วนทางซ้ายและส่วนทางขวา (ส่วนละ 32 บิต) ขั้นตอนต่อไปจะใช้ฟังก์ชั่นทางคณิตศาสตร์ (ฟังก์ชั่น f) ข้อมูลจากส่วนซ้ายหรือขวาจะถูกนำมารวมกันกับ Key โดยจะทำซ้ำกันอย่างนี้เป็นจำนวนทั้งสิ้น 16 รอบ เมื่อเสร็จสิ้นขั้นตอนนี้ (รอบที่ 16) ผลลัพธ์ที่ได้จากทั้งส่วนทางซ้ายและขวาก็จะถูกนำมารวมกันเป็นข้อมูลขนาด 64 บิตอีกครั้งหนึ่ง และนำไปสลับตำแหน่งในขั้นตอนสุดท้าย



ภาพที่ 2-4 กระบวนการทำงานของ DES

การทำงานของฟังก์ชั่น f ในแต่ละรอบ จะเป็นการเลื่อนบิตของ Key ซึ่งจะเลือกใช้เพียง 48 บิตจากทั้งสิ้น 56 บิต ข้อมูลในส่วนทางขวา (32 บิต) จะถูกขยายให้กลายเป็นข้อมูลขนาด48 บิต จากนั้นจะนำมารวมกับกุญแจขนาด 48 บิต (ที่เลือกมา) การรวมกันในขั้นตอนนี้จะใช้การ XOR ผลลัพธ์ขนาด 48 บิตที่ได้จะถูกนำไปทำการแทนที่อีก 8 ครั้ง ผลลัพธ์จากการแทนที่จะเหลือข้อมูลเพียง 32 บิตเท่านั้น หลังจากนั้นก็จะต้องทำการสลับตำแหน่งกันอีกครั้ง

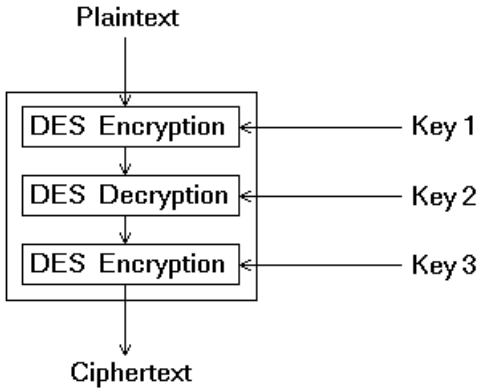
หนึ่งรอบของการทำฟังก์ชั่น f จะประกอบด้วยขบวนการข้างต้น 4 ครั้ง ข้อมูลในส่วนทางซ้ายจะต้องผ่านขบวนการเดียวกัน ผลลัพธ์ที่ได้จากทั้งส่วนทางซ้ายและขวาจะถูกนำมารวมกันแบบ XOR เมื่อเสร็จสิ้นขั้นตอนนี้แล้ว ผลลัพธ์ที่ได้จะถูกใช้เป็นข้อมูลส่วนทางขวาของรอบใหม่ และข้อมูลของส่วนทางขวาเดิมก็จะกลายเป็นข้อมูลส่วนซ้ายของวงรอบใหม่

บริษัทแห่งหนึ่งต้องการเบรค DES เพื่อสร้างความแข็งแกร่งให้กับ RSA จึงจัดให้มีการประกวดการเบรคขึ้นโดยให้รางวัล 10,000 US$ สำหรับผู้ชนะในแต่ละรอบ บริษัท Distribution.net ใช้เวลา 41 วันก็ทำการเบรค DES ได้สำเร็จ บริษัท EFF สามารถ เบรค ได้ภายในเวลา 56 ชั่วโมง Distribution.net และบริษัท EFF ก็จับมือกันและใช้คอมพิวเตอร์กว่า 100,000 เครื่องทั่วโลกมาแคร็ก DES ซึ่งก็สามารถทำได้ ในเวลา 22 ชั่วโมง 15 นาที จึงเป็นต้นเหตุทำให้มีการขยาย Key ของ DES จาก 64 Bit ให้เป็น 128 Bit เพื่อจะได้ใช้เวลาในการแคร็ก (crack) นานขึ้น

ปัจจุบัน DES แบ่งออกเป็น DES 64 Bit และ DES 128 Bit แต่ถึงแม้ว่าจะใช้ 128 bit ก็ตาม DES ก็ยังสามารถถูกแคร็กได้ จึงได้มีการพัฒนาให้มี Tripple-DES (3DES) ที่มีความปลอดภัยสูงขึ้น

2.2.2.2 Tripple-DES (3DES)

Triple-DES เป็นการเข้ารหัสที่ถูกสร้างมาเพื่อแก้ปัญหาความอ่อนแอของ DES โดย Triple-DES จะช่วยเสริมความปลอดภัยให้การเข้ารหัสมีปลอดภัยมากขึ้น โดยการใช้อัลกอริทึม DES เป็นจำนวนสามครั้งเพื่อทำการเข้ารหัส โดยในแต่ละครั้งจะใช้กุญแจในการเข้ารหัสที่แตกต่างกันออกไป ดังนั้นจำนวนกุญแจที่ใช้ใน Triple-DES จึงมีทั้งสิ้น 3 ดอก (ความยาวดอกละ 56 บิต) ด้วยความแข็งแกร่งนี้จึงทำให้ Triple-DES เป็นอีกหนึ่งในมาตรฐานในการเข้ารหัสในปัจจุบัน



ภาพที่ 2-5 กระบวนการทำงานของ triple-DES

2.2.2.3 AES (Advance Encryption Standard)

AES (Advance Encryption Standard) เป็นการเข้ารหัสที่พัฒนาขึ้นมาเพื่อใช้ทดแทน DES หลังจากที่ DES ถูกเบรคได้โครงการพัฒนา AES ได้เริ่มต้นเมื่อปี 1997 โดย NIST หลังจากนั้น (ในปี 1998) NIST ก็ให้นักวิทยาการหัสลับทั่วโลกส่งอัลกอริทึมเข้ามาเพื่อคัดเลือกโดยกำหนดให้ 128 Bit เป็นมาตรฐานของ และ 256 Bit

อัลกอริทึมต่าง ๆ ถูกคัดเลือกเข้ามาทั้งสิ้น 15 อัลกอริทึม และมีอยู่ 5 อัลกอริทึมที่ผ่านเข้ารอบชิง จนผลสุดท้ายอัลกอริทึมของ Rijndeal ได้รับการตัดสินให้ชนะเพราะเร็วกว่าและใช้อัลกอริทึมที่ธรรมดากว่า แต่ได้ความปลอดภัยเท่ากัน จากนั้นจึงได้กลายเป็น RFC 3826 เมื่อปี 2004 ข้อกำหนดในมาตรฐานล่าสุดอนุญาตให้ใช้ AES เข้ารหัสข้อมูลโดยใช้ Key ที่มีขนาดต่าง ๆ ได้ ซึ่งได้แก่ 128 Bit, 192 Bit และ 256 Bit

วงรอบการทำงานของ AES แบ่งเป็น 3 ส่วนหลัก ๆ ได้แก่ Initial Round, Rounds และ Final Round และในแต่ละส่วนก็มีกระบวนการย่อยต่าง ๆ ดังนี้

(1) Initial Round

- AddRoundKey

(2) Rounds

- SubBytes: เป็น non-linear substitution ซึ่งแต่ละไบต์จะถูกแทนที่ด้วยไบต์ที่ได้จาก lookup table (รูปที่ 7)

- ShiftRows: เป็นการเลื่อนไบต์ในแต่ละแถว ซึ่งจะทำเฉพาะแถวที่ 2, 3 และ 4

- MixColumns: เป็นการผสมรวม 4 ไบต์ภายในคอลัมน์

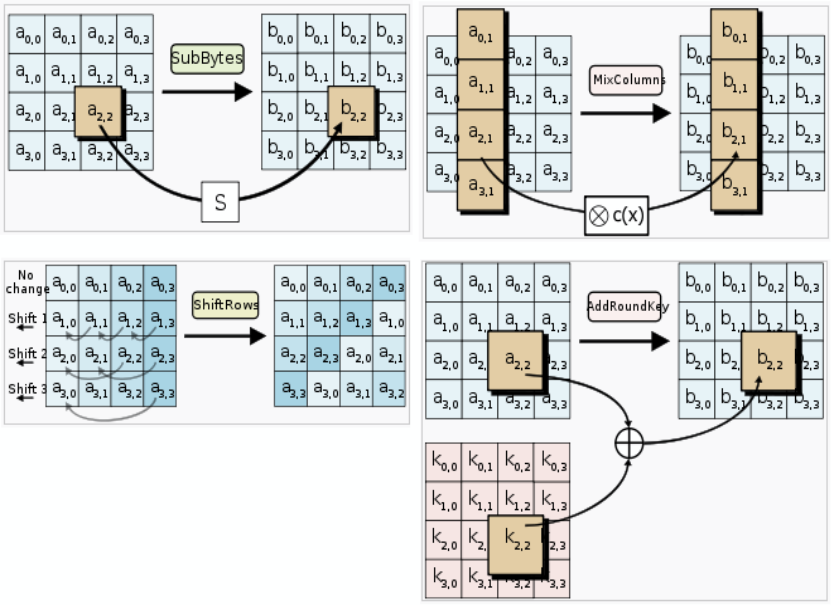
- AddRoundKey เป็นการนำ Cipher Text และ Key (ที่มาจาก key schedule) ผสมรวมกลายเป็น Cipher Text ใหม่

(3) Final Round (no MixColumns)

- SubBytes

- ShiftRows

- AddRoundKey



ภาพที่ 2-6 กระบวนการ SubBytes, ShiftRows, MixColumns และ AddRoundKey

2.2.3 การเข้ารหัสแบบสมมาตร (Symmetric Key Cryptography)

การเข้ารหัสโดยใช้กุญแจดอกเดียวเรียกว่า "การเข้ารหัสแบบสมมาตร" (Symmetric Key Cryptography) เนื่องจากใช้ Key ตัวเดียวกันในการเข้ารหัสและถอดรหัส นอกจาก DES และ AES แล้วอัลกอริทึมในการเข้ารหัสแบบสมมาตรอย่างอื่นก็มีเช่น Blowfish และ IDEA แต่อาจจะไม่เป็นที่นิยมมากนัก การเข้ารหัสแบบสมมาตรถึงแม้จะใช้อัลกอริทึมที่แข็งแกร่งอย่าง AES และใช้ Key ที่มีความยาวตั้งแต่128 bit ขึ้นไปแล้วก็ยังมีข้อด้อยอยู่ตัวอย่างเช่น

- การส่ง Key ไปยังผู้รับเพื่อใช้ในการถอดรหัส หาก Key ถูกดักจับได้แล้วการเข้ารหัสก็จะไม่มีความหมายอะไรเลยเพราะผู้ดักฟังที่ดักจับได้ Key ไป ก็สามารถที่จะดักจับ Cipher Text แล้วถอดรหัสได้

- หากมีจำนวนผู้ใช้มากขึ้น ซึ่งผู้ใช้แต่ละคู่จะต้องใช้คีย์ที่แตกต่างจากคู่สื่อสารอื่น จะทำให้จำนวนคีย์ที่ต้องใช้ทั้งหมดมีจำนวนมากเช่น ผู้ใช้ N คนจะต้องใช้คีย์ทั้งหมดเท่ากับ N x (N-1) / 2

ด้วยข้อจำกัดเกี่ยวกับเรื่องการบริหารจัดการคีย์นี้ จึงได้มีมีการคิดค้น "การเข้ารหัสแบบอสมมาตร" ขึ้นมาซึ่งภาษาอังกฤษเรียกว่า Asymmetric Key Cryptography

2.2.4 การเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography)

การเข้ารหัสแบบอสมมาตร (Asymmetric Key Cryptography) บางตำราอาจใช้คำว่า Asymmetric Key Encryption หรือ Public Key Encryption หรือใช้คำว่า Public Key Infrastructure (PKI) หรือ Public-Key Cryptography

การเข้ารหัสแบบนี้ถูกคิดค้นโดย Whit Diffie และ Marty Hellman ตั้งแต่ปี1976 โดยถูกสร้างมาเพื่อเป็นทางเลือกในการส่งข้อมูลที่เป็นความลับ เพราะการเข้ารหัสแบบสมมาตร (ใช้กุญแจดอกเดียว) จะมีปัญหาเรื่องการถูกดักจับ Key และปัญหาเกี่ยวกับการจัดการ Key ที่มีอยู่เป็นจำนวนมากเมื่อใช้ในระบบใหญ่ การเข้ารหัสแบบอสมมาตรจะใช้ Key สองอัน โดยหากเราเข้ารหัสด้วย Key อันหนึ่งจะต้องทำการถอดรหัสด้วย Key อีกอันหนึ่งที่เหลือ

ตัวอย่างเช่น

- หากเข้ารหัสด้วย Key1 จะต้องถอดรหัสด้วย Key2 เท่านั้น
- หากเข้ารหัสด้วย Key2 จะต้องถอดรหัสด้วย Key1 เท่านั้น
- หากเข้ารหัสด้วย Key1 แล้วถอดรหัสด้วย Key1 จะไม่สามารถถอดรหัสได้
- หากเข้ารหัสด้วย Key2 แล้วถอดรหัสด้วย Key2 จะไม่สามารถถอดรหัสได้

การประยุกต์ใช้งานทำได้โดย เก็บ Key อันหนึ่งไว้กับตัวเองเรียกว่า Private Key ส่วนอีก Key หนึ่งสามารถที่จะแจกจ่ายให้ผู้อื่นได้ดังนั้น Key นี้จึงถูกเรียกว่า Public Key เมื่อผู้อื่นต้องการที่จะส่งข้อมูลที่เป็นความลับมายังเจ้าของ Private Key จะต้องทำการเข้ารหัสข้อมูลนั้นด้วย Public Key ของผู้รับ ดังนั้นจึงทำให้ผู้ที่มี Private Key เท่านั้นที่จะถอดรหัสข้อมูลได้ ส่วนการส่งข้อมูลที่เข้ารหัสด้วย Private Key ไปยังผู้อื่น ผู้ใดก็ตามที่มี Public Key (ซึ่งมีอยู่หลายคน) จะสามารถถอดรหัสข้อมูลได้

2.2.4.1 RSA

RSA เป็นอัลกอริทึมในการเข้ารหัสแบบอสมมาตร ถูกสร้างขึ้นมาเมื่อปี1978 โดย Ron Rivest, Adi Shamir และ Leonard Adleman ตั้งแต่คิดค้นมายังไม่มีใครสามารถเบรคอัลกอริทึมนี้ได้ และ RSA ได้ถูกนำมาใช้อย่างแพร่หลายในด้าน e-commerce

กระบวนการทำงานของ RSA

(1) เลือก p และ q ซึ่งเป็นจำนวนเฉพาะที่มีค่าต่างกัน

(2) ให้ n = pq

(3) ให้ m = (p-1)(q-1)

(4) เลือกค่า e ที่ 1 < e < m ซึ่งหารร่วมมากของ m กับ e มีค่าเป็น 1 (สามารถหาค่า e ได้โดยการสุ่มค่าจำนวนเต็มบวกพร้อมกับทดสอบว่าหารร่วมมากของ m กับ e มีค่าเป็น 1)

(5) หาค่า d ที่ทำให้ ed mod m = 1

(6) Public key คือ (e,n)

(7) Private key คือ (d,n)

(8) ให้ M คือข้อความที่ยังไม่ถูกเข้ารหัส (ในรูปแบบของตัวเลข) M < n

(9) การเข้ารหัส => C = M^e mod n

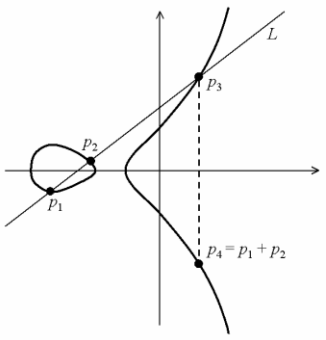
(10) การถอดรหัส => M = C^d mod n

สาเหตุที่ทำให้ RSA ยากที่จะทำการเบรคได้คือ แม้จะทราบ Public Key (e,n) ทราบค่า Message (M) และทราบค่า Cipher (C) ก็ตาม แต่ก็ยากที่จะทำการคำนวณย้อนกลับเพื่อหาค่าของ Private Key (d) ได้

2.2.4.2 ECC

ECC ย่อมาจาก Elliptic Curves Cryptography ได้รับการนำเสนอโดย Neal Koblitz และ Victor S. Miller ในปี 1985 โดยอัลกอริทึมการเข้ารหัส ECC นี้ได้รับการพัฒนาจากสมการของเส้นโค้งของวงรี

$$y^2 = x^3 + ax + b$$



ภาพที่ 2-7 กราฟแสดงความสัมพันธ์ของสมการ Elliptic Curves

ECC มีข้อดีที่เหนือกว่า RSA คือจะใช้คีย์ที่สั้นกว่าแต่สามารถให้ความปลอดภัยเท่ากับ RSA ได้ หรือหากใช้คีย์ที่ยาวเท่ากับคีย์ของ RSA จะมีความปลอดภัยสูงกว่า คือหากต้องการที่จะเบรคจะใช้เวลาในการ Brute Force นานกว่า RSA

เนื่องจาก ECC ใช้ Key ที่มีขนาดเล็กกว่า RSA มาก และมีความสามารถในการคำนวณที่รวดเร็ว ใช้พลังงานต่ำและใช้หน่วยความจำน้อย ดังนั้น ECC จึงเหมาะสำหรับการใช้งานในอุปกรณ์เคลื่อนที่ขนาดเล็กอย่างเช่น โทรศัพท์มือถือ Pocket PC และ PDA เป็นต้น

กล่าวโดยสรุปแล้ว วิธีการเข้ารหัสข้อมูลแบบต่างๆมีข้อดีข้อเสียและที่มาต่างกัน ซึ่งวิธีการเหล่านี้ถูกพัฒนาขึ้นมาตามยุคสมัยและตามชนิดของข้อมูลในยุคสมัยนั้นๆ และงานแต่ละประเภทหรือชนิดข้อมูลแต่ละชนิดก็ต้องการระดับความปลอดภัยต่างๆกัน เราจึงควรเลือกใช้วิธีการเข้ารหัสที่เหมาะสมกับงานที่จะนำไปใช้ ในลำดับต่อไปจะพูดถึงเทคนิคหรือวิธีการเข้ารหัสข้อมูลภาพที่ใช้กันในปัจจุบัน

2.3 วิธีการเข้ารหัสข้อมูลภาพ

การเข้ารหัสข้อมูลภาพมีบทบาทสำคัญในการช่วยรักษาความลับของข้อมูลภาพที่ถูกส่งผ่านเครือข่ายอินเตอร์เน็ต วิธีการเข้ารหัสภาพถูกแบ่งย่อยได้หลายประเภท ถ้าเราพิจารณาถึงปัญหาและความท้าทายในเรื่องเวลาหรือความรวดเร็วในการเข้ารหัสข้อมูลภาพ เราจะสามารถแบ่งวิธีการเข้ารหัสข้อมูลภาพได้ 2 แบบ [18] ดังนี้

1. Partial encryption (Selective encryption) คือ วิธีการเข้ารหัสข้อมูลที่เลือกข้อมูลเป็นส่วนๆเพื่อมาทำการเข้ารหัส วิธีการประเภทนี้จึงประมวลผลได้เร็ว เหมาะที่จะไปใช้กับงานประยุกต์แบบทันกาล (real time)

2. Full encryption คือ วิธีการเข้ารหัสฉบับเต็ม อาจจะมีข้อเสียทางด้านเวลาในการประมวลผลเพราะใช้ข้อมูลทั้งหมดมาเข้ารหัส แต่สามารถรับประกันความปลอดภัยได้มากกว่าวิธีการเข้ารหัสแบบ partial encryption

และหากพิจารณาตามโดเมน (domain) แล้ว วิธีการเข้ารหัสข้อมูลรูปภาพสามารถแบ่งแยกได้เป็น 3 โดเมนด้วยกัน [18] คือ

1. Spatial domain หรือ โดเมนพื้นที่

2. Frequency domain หรือ โดเมนความถี่

3. Hybrid domain หรือ การรวมระหว่างโดเมนพื้นที่ (Spatial domain) และโดเมนความถี่ (Frequency domain)

2.3.1 Chaos-Based Image Encryption

ในงานวิจัยนี้เราสนใจวิธีการเข้ารหัสข้อมูลภาพในกลุ่ม Chaos-based และการเข้ารหัสแบบ full encryption ในโดเมนพื้นที่ (spatial domain) ซึ่งมี chaos-based encryption algorithm มีโครงสร้าง (architecture) โดยทั่วๆไป ประกอบด้วย 2 ขั้นตอนหลัก ดังต่อไปนี้

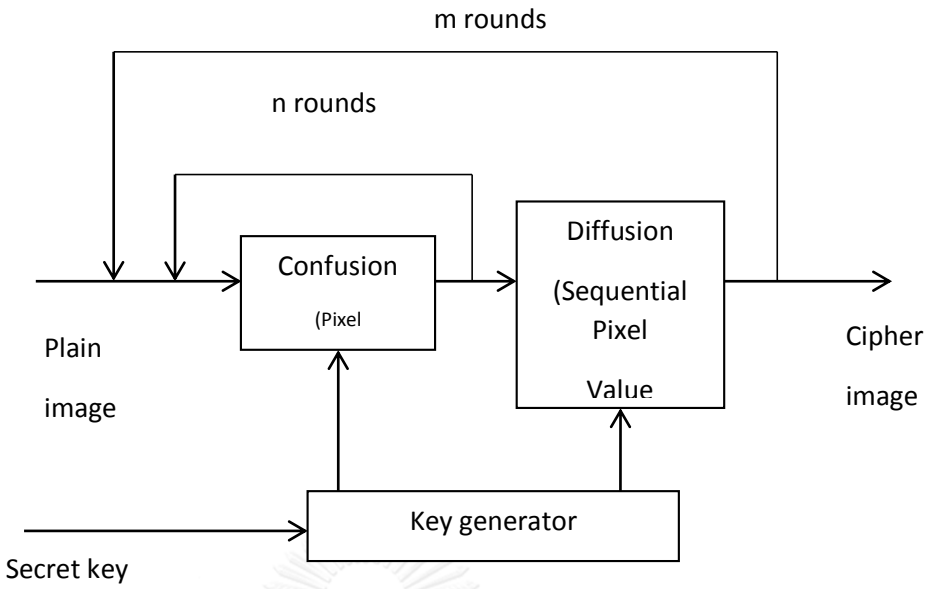
1. ขั้นตอนการสร้างความไร้ระเบียบ (Confusion stage)

ในขั้นตอนนี้จะทำการเรียงสับเปลี่ยนจุดภาพใหม่โดยไม่เปลี่ยนแปลงค่าสีของจุดภาพ และกุญแจลับ (secret key) จะถูกแปลงมาเป็นพารามิเตอร์ควบคุม (control parameter) ที่นำไปสร้าง key sequence ฟังก์ชั่นที่นำมาใช้ก็ฟังก์ชั่นในกลุ่มเคโอติก (Chaotic functions) เช่น Lorenz map, Henon map, Logistic map, Arnold cat map, Chirikov map และ Chebyshev map เป็นต้น

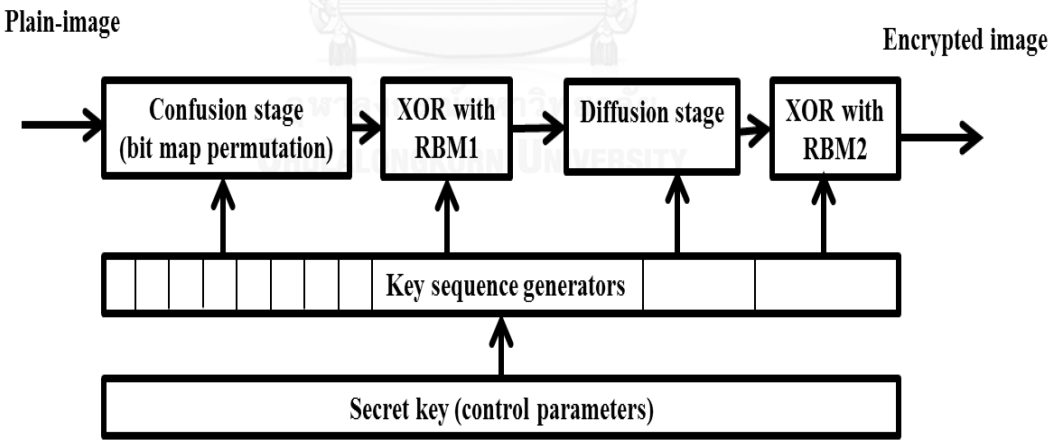
2. ขั้นตอนการแพร่ (Diffusion stage)

ในขั้นตอนนี้นับเป็นขั้นตอนที่สำคัญที่ช่วยเพิ่มความปลอดภัย เพราะหากมีแต่ขั้นตอนการสร้างความไร้ระเบียบ(Confusion stage) วิธีการอาจจะถูกโจมตีได้ง่าย เนื่องจากค่าสีของแต่ละจุดภาพยังไม่เปลี่ยน ในขั้นตอนนี้จึงเปลี่ยนค่าสีของแต่ละจุดภาพโดยอาศัยฟังก์ชั่นเคโอติกอีกเช่นกัน

สุดท้ายทั้งสองขั้นตอนนี้ถูกวนซ้ำหลายๆรอบ (looping) เพื่อให้ได้ระดับความปลอดภัยที่ต้องการ และด้วยคุณสมบัติความไร้ระเบียบของฟังก์ชั่นเคโอติกทำให้ chaos-based method เหมาะสำหรับนำไปใช้กับวิธีการเข้ารหัสข้อมูลภาพเพื่อให้มีคุณสมบัติความไร้ระเบียบ (confusion property) ด้วย



ภาพที่ 2-8 แสดงโครงสร้างของ chaos-based image cryptosystem โดยทั่วๆไป



ภาพที่ 2-9 โครงสร้างของวิธีการเข้ารหัสข้อมูลภาพที่เสนอ (proposed image encryption scheme)

2.4 เคโอติกแม็ป (Chaotic maps)

ในงานวิจัยนี้เราได้เลือกใช้เคโอติกแม็ป 3 ชนิด ดังต่อไปนี้

1. Standard Chaotic Map
2. Logistic Chaotic Map
3. Tinkerbell Chaotic Map

2.4.1 Standard Chaotic Map

สมการคณิตศาสตร์ของ Standard Chaotic Map มีดังต่อไปนี้

$$a_{i+1} = (a_i + b_i) \bmod 2p,$$
$$b_{i+1} = (b_i + k\sin(a_i + b_i)) \bmod 2p,$$

โดยที่ $k, k > 0$ เป็นพารามิเตอร์ควบคุม และ (a_i, b_i)เป็นลำดับที่ i โดยจะเป็นค่าจำนวนจริงระหว่าง $[0, 2p)$ สำหรับทุกๆ i

เนื่องจากสมการต้องนำไป mod กับค่า 2π ซึ่งเป็น floating point ในคอมพิวเตอร์จึงมีอีกเวอร์ชั่นของ Standard Chaotic Map ซึ่งคือ Discretized Standard Map ซึ่งเราจะนำมาใช้ในงานวิจัยนี้ สมการของ Discretized Standard Map มีดังต่อไปนี้

$$x_{i+1} = (x_i + y_i) \bmod N,$$
$$y_{i+1} = (y_i + K\sin(\frac{2px_{i+1}}{N})) \bmod N,$$

โดยที่ N คือความกว้างหรือความยาวของภาพ และ K เป็นกุญแจลับ (Secret key) ที่ทำหน้าที่เป็นพารามิเตอร์ควบคุม (control parameter) ในสมการนี้

2.4.2 Logistic Chaotic Map

สมการคณิตศาสตร์ของ Logistic Chaotic Map มีดังต่อไปนี้

$$x_{i+1} = rx_i(1 - x_i),$$

โดยที่ x_0คือค่าเริ่มต้น และ r คือพารามิเตอร์ควบคุม โดยที่มีค่าระหว่าง 3.57 กับ 4

2.4.3 Tinkerbell Chaotic Map

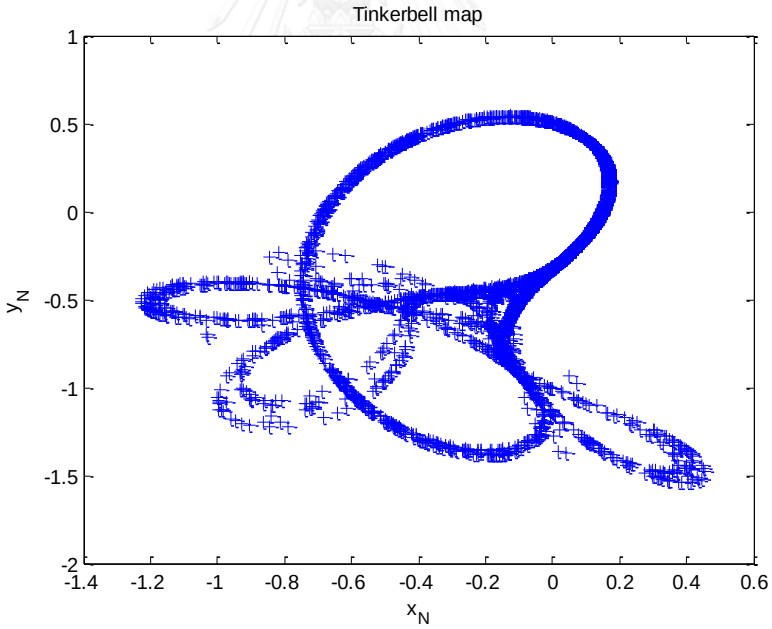
เป็นเคโอติกแม็ปอีกหนึ่งชนิดที่เราเลือกใช้ เนื่องจากว่ายังไม่พบงานวิจัยใดเลือกใช้เคโอติกแม็ปชนิดนี้ และเราเห็นว่ารูปแบบของเคโอติกแม็ปมีความน่าสนใจและมีรูปแบบแตกต่างจากเคโอติกแม็ปแบบอื่น จึงน่าจะนำมาประยุกต์ใช้ได้ เพื่อให้เกิดความหลากหลาย

Tinkerbell Chaotic Map มีสมการทางคณิตศาสตร์ ดังต่อไปนี้

$$x_{i+1} = x_i^2 - y_i^2 + ax_i + by_i,$$
$$y_{i+1} = 2x_iy_i + cx_i + dy_i,$$

โดยที่ where x_0 และ y_0 เป็นค่าเริ่มต้น และ a, b, c, and d เป็นพารามิเตอร์ควบคุม (control parameters)

ซึ่งจะเห็นได้ว่า Tinkerbell Chaotic Map ใช้พารามิเตอร์ควบคุมหลายตัว สิ่งนี้ทำให้เราเพิ่มขนาด key space ให้ใหญ่ขึ้นได้ และพฤติกรรมหรือรูปแบบของ Tinkerbell Chaotic System ดังปรากฏในภาพนี้



ภาพที่ 2-10 Tinkerbell Chaotic Map โดยที่ $a = 0.9, b = -0.6013, c = 2, d = 0.5,$ และค่าเริ่มต้น $x_0 = -0.72, y_0 = -0.64$

2.5 งานวิจัยต่างๆที่เกี่ยวข้อง

จากการศึกษาเกี่ยวกับ Image Encryption พบว่ามีงานวิจัยทางด้านนี้อยู่มากมาย โดยในงานวิจัยนี้เราสนใจที่จะศึกษาวิจัยและออกแบบวิธีการเข้ารหัสภาพให้มีความแข็งแกร่งมากขึ้นและยากต่อการโจมตีโดยวิธีต่างๆ ซึ่งงานวิจัยที่เกี่ยวข้องมีดังต่อไปนี้

ผลงานวิจัยของ N.K. Pareek, Vinod Ptidar และ K.K. Sud [7] ได้นำเสนออัลกอริทึ่มที่ใช้ Logistic maps จำนวน 2 ชุด และ external key จำนวน 80 บิตในการเข้ารหัสข้อมูลภาพโดยใช้ operations ต่างๆจำนวน 8 ชนิด

งานวิจัยของ H. Gao, Y. Zhang, S. Liang, D. Li [19] ได้นำเสนอวิธีการในการเข้ารหัสข้อมูลภาพโดยใช้ระบบเคโอติก (Chaotic system) ใช้ power และ tangent function แทนที่จะใช้ linear function โดยสร้าง chaotic sequence จาก NCA map โดยเข้ารหัสได้โดยทำการ XOR ตัวภาพตั้งต้นกับลำดับจำนวนเต็ม

งานวิจัยของ H. Yu และ Z. Zhu [20] ได้นำเสนอวิธีการที่มีประสิทธิภาพในการเข้ารหัสภาพโดยใช้ image reconstruction ด้วยการที่จุดภาพในระดับบิต (bit level) มีลักษณะที่แตกต่างกันออกไป วิธีการนี้นำบิตต่างๆกันนี้มาจัดการเรียงในระดับบิตใหม่ ผลลัพธ์คือได้คือวิธีการมีประสิทธิภาพมากขึ้นและมีระดับความปลอดภัยสูงขึ้น

งานวิจัยของ K.C. Ravishankar, M.G. Venkateshmurthy [21] ได้นำเสนอวิธีการเข้ารหัสรูปภาพแบบ Region-based โดยเทคนิคคือจะทำการแบ่งส่วน (segment) ภาพให้เป็นส่วนต่างๆตามขนาดที่กำหนดไว้ก่อน และทำการเข้ารหัสภาพที่ถูกตัดส่วนเหล่านี้ด้วยวิธีการที่เป็นอิสระต่อกัน ผลลัพธ์คือเวลาในการเข้ารหัสลดลงไปมาก

งานวิจัยของ S.H. Kamali, R. Shakerian [22] ได้นำเสนอรูปแบบการเข้ารหัสที่มีการปรับเปลี่ยนมาจากอัลกอริทึ่ม AES โดยใช้ ShiftRow transformation ถ้าค่าในแถวแรกและคอลัมน์แรกเป็นเลขคู่ แถวที่ 1 และแถวที่ 4 จะไม่เปลี่ยนแปลง และแถวที่ 2 กับแถวที่ 3 จะถูกขยับวนตามเข็มนาฬิกา แต่ถ้าเป็นเลขคี่ แถวที่ 1 และแถวที่ 3 จะไม่เปลี่ยนแปลง และแถวที่ 2 กับแถวที่ 4 จะถูกขยับวนทวนเข็มนาฬิกา ผลลัพธ์ที่ได้คือวิธีการนี้มีความทนทานต่อ statistical attack และมีประสิทธิภาพมากกว่าอัลกอริทึ่ม AES

งานวิจัยของ K. Sakthidasan Sankaran และ B.V. Santhosh Krishna [23] ได้นำเสนอระบบการเข้ารหัสข้อมูลที่ประกอบด้วย 2 ขั้นตอน คือ ขั้นตอน Confusion และขั้นตอน Diffusion ในขั้นตอน Confusion จะทำการเรียงสับเปลี่ยนตำแหน่งของจุดภาพโดยใช้ระบบเคโอติกแบบสามมิติระบบหนึ่ง จากนั้นในขั้นตอน Diffusion จุดภาพจะถูกทำการแพร่กระจายโดยระบบเค-โอติกอีกระบบหนึ่ง ซึ่งเงื่อนไขเริ่มต้นและพารามิเตอร์ควบคุม (initial conditions and control parameters) ที่ใช้ในทั้งสองขั้นตอนถูกกำหนดโดยกุญแจลับ (secret key)

งานวิจัยของ Hazem Mohammad Al-Najjar และ Asem Mohammad AL-Najjar [24] ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพโดยประยุกต์ใช้ Logistic chaotic map โดยแบ่งระบบเป็น 2 ขั้นตอน คือ การแทนที่จุดภาพ (pixel replacement) และการสลับจุดภาพ (pixel scrambling) ในส่วนของขั้นตอนของการทำ pixel replacement หรือการแทนที่จุดภาพนั้น คือเปลี่ยนค่าสีโดยไม่เปลี่ยนตำแหน่งของจุดภาพ ส่วนแบบที่สอง pixel scrambling นั้นคือการเปลี่ยนตำแหน่งของจุดภาพโดยไม่ได้เปลี่ยนค่าสี ในขั้นตอนของการทำ pixel replacement สามารถทำได้ 2 แบบคือ แบบแรกทำได้โดยใช้ตารางการแม็ปจุดภาพ (pixel mapping tables : PMT) และแบบที่สองนำจุดภาพไปทำ XOR operation กับ random vector ที่ถูกสร้างโดย Logistic map

ผลงานวิจัยของ Mrinal Kanti Mandal, Gourab Dutta Banik, Debasish Chattopadhyay และ Debashis Nandi ได้ใช้เทคนิคนี้ในการเข้ารหัสภาพระดับเทาโดยใช้ XOR operation และการเรียงสับเปลี่ยนจุดภาพทำให้เกิดคุณสมบัติความไร้ระเบียบและการแพร่ (confusion and diffusion properties)

งานวิจัยของ Somaya, Al-Maadeed, Afnan Al-Ali และ Turki Abdalla [25] ได้นำเสนอวิธีการเข้ารหัสภาพที่ประกอบ 2 หน่วยคือ หน่วย pixel shuffler และหน่วย stream cipher ซึ่งหน่วยการสับเปลี่ยนจุดภาพ (pixel shuffler) นั้นมีประโยชน์ 2 ทางคือนอกจากจะมีการจัดเรียงตำแหน่งของจุดภาพใหม่ (Diffusion) ก็ยังมีการเปลี่ยนแปลงค่าสีของจุดภาพ (Confusion) ด้วย ซึ่งขั้นตอน Confusion ถูกรับผิดชอบโดยหน่วยที่สองคือหน่วย stream cipher โดยใช้ non-linear function operation และหน่วย pixel shuffler นั้นจะนำเคโอติกแม็ปมาประยุกต์ใช้ในสองทิศทาง คือ แนวตั้งและแนวนอนเพื่อลดความสัมพันธ์ (correlations) ระหว่างจุดภาพที่อยู่ติดกัน โดยใช้ 2D Henon map ในการสร้างตัวเลขแบบสุ่มเทียม (pseudorandom number) เพื่อที่จะนำไปสร้าง permutation matrix หลังจากนั้นจะใช้อัลกอริทึ่ม W7 ในการสร้าง key steam และค่าของจุดภาพจะถูกเปลี่ยนแปลงโดยการใช้ XOR operation ระหว่างจุดภาพที่ถูกเรียงสับเปลี่ยนแล้วกับ key stream

งานวิจัยของ Kamlesh Gupta และ Sanjay Silakari [4] ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพที่แบ่งแยกภาพเป็นภาพสีแดง ภาพสีเขียว และภาพสีน้ำเงินก่อน (red, green, blue channel) แล้วนำภาพสีแดงและภาพสีเขียวไปแปลงหรือเรียงใหม่โดยเป็นระนาบแนวตั้งและแนวนอนตามลำดับ ส่วนภาพสีน้ำเงินยังคงเดิม จากนั้นนำภาพไปทำขั้นตอน Confusion โดยใช้ 2D Cat map ตามด้วย Standard map สุดท้ายขั้น Diffusion คือการทำ XOR operation ระหว่างภาพที่ถูกเรียงสับเปลี่ยนมากับภาพที่ได้จากขั้นตอน Confusion

งานวิจัยของ Chong Fu, Jun-jie Chen, Hao Zou, Wei-hong Meng, Yong-feng

Zhan, และ Ya-wen [26] ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพที่ปรับปรุงขั้นตอน Diffusion เพิ่มเติม เพื่อให้การประมวลผลในขั้นตอนนี้รวดเร็วขึ้น โดยใช้การแพร่กระจายแบบสองทิศทาง ในขั้นตอนแรก ความแตกต่างจะถูกกระจายออกไปทุกจุดภาพโดยการปรับเปลี่ยนค่าสีของจุดภาพซ้ายไปทางขวา และด้านบนลงด้านล่างตามลำดับ ในขั้นตอนที่สองจากขวาไปซ้ายและด้านล่างขึ้นไปด้านบน วิธีการนี้ทำให้ไม่ต้องเริ่มรอบ permutation-diffusion อีกครั้ง ดังนั้นรอบของการเข้ารหัสโดยรวมจะลดลง โดยไม่ต้องปรับลดระดับความปลอดภัย

งานวิจัยของ Shima Ramesh Maniyath และ Supriya M [27] ได้นำเสนอวิธีการเข้ารหัสภาพและวิธีการเข้ารหัสไฟล์วีดีโอโดยประยุกต์มาจากเรื่องลำดับ DNA จุดมุ่งหมายคือต้องการลดทอนเวลาในการเข้ารหัสภาพขนาดใหญ่ โดยใน confusion stage จะนำภาพต้นฉบับไปทำการ XOR กับ DNA template ที่เตรียมไว้จากการใช้ Arnold cat map และในแต่ละค่าสีจะแบ่งเป็นฐาน 4 แทนได้แก่ ค่า 00 แทนด้วย ‘A’ ค่า 01 แทนด้วย ‘T’ ค่า 10 แทนด้วย ‘C’ และค่า 11 แทนด้วย ‘G’

งานวิจัยของ Paul A.J P. M. K. Paulose Jacob [28] ได้นำเสนอขั้นตอนการเข้ารหัสสำหรับการเข้ารหัสภาพที่มีประสิทธิภาพมากขึ้น ในงานวิจัยนี้นำเสนอวิธีการเข้ารหัสแบบสมมาตร (symmetric key encryption) โดยใช้ matrix array symmetric key ทำให้แปลงรูปต้นฉบับเป็นรูปที่ถูกเข้ารหัสได้อย่างรวดเร็ว รูปแบบคือใช้ block cipher ขนาด 128 บิต และใช้ขนาดของกุญแจ 128 บิต ผลลัพธ์ที่ได้เทียบเคียงกับอัลกอริทึ่ม AES และเหมาะกับการเข้ารหัสแบบเร็ว (fast encryption)

งานวิจัยของ A.Gautam, M. Panwar และ Dr.P.R Gupta [4] ได้นำเสนอวิธีการเข้ารหัสที่ใช้การแบ่งรูปภาพเป็นบล็อกต่างๆก่อนที่จะเข้ากระบวนการเข้ารหัส (Block cipher) และใช้อัลกอริทึ่ม blowfish ข้อดีของวิธีการนี้คือสามารถป้องกันการสูญหายของข้อมูลได้

งานวิจัยของ X. F.Guo และ X.cong [29] ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพโดยใช้สองกระบวนการหลักคือ กระบวนการสลับจุดภาพ (scrambling) และกระบวนการแทนที่ค่าสี (substitution) จากระบบเคโอติกที่ผสมกัน (hybrid chaotic system) คือเริ่มแรกใช้ Logistic chaotic map กับ Chua’s system ในการสลับตำแหน่งจุดภาพ และจากนั้นใช้การแทนที่จุดภาพโดย chaotic sequence อีกอันหนึ่งที่สร้างโดย optimized Chua’s system เพื่อให้ได้ภาพใหม่ ผลที่ได้คือวิธีการนี้มีคุณสมบัติของความไร้ระเบียบและการแพร่กระจายที่ดี (Confusion-Diffusion properties) ขนาดของกุญแจใหญ่ และอัลกอริทึ่มมีความไวต่อสถานะเริ่มต้นด้วย

งานวิจัยของ Ruisong Ye Haiying Zhao [30] ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพที่มีประสิทธิภาพโดยใช้ Affine Modular Maps โดยในขั้นตอนการสร้างความไร้ระเบียบให้ข้อมูลภาพ (Confusion stage) ได้เรียงสับเปลี่ยนข้อมูลภาพต้นฉบับอย่างมีประสิทธิภาพ และกระบวนการแพร่ (Diffusion stage) จะใช้กระบวนการแพร่แบบสองทิศทางเพื่อทำให้เปลี่ยนค่าสีของแต่ละจุดภาพของทั้งภาพ ผลการทดลองแสดงให้เห็นว่ารูปแบบการเข้ารหัสแบบนี้มีความปลอดภัยสูง และภาพที่ถูก

เข้ารหัสมีความอ่อนไหวต่อทั้งกุญแจและรูปต้นฉบับ ซึ่งเป็นข้อดีของวิธีการเข้ารหัส นอกจากนั้นยังสามารถใช้กับภาพที่มีความกว้างไม่เท่ากับความสูงได้เป็นอย่างดีด้วย

งานวิจัยของ R. liu และ X. tian [31] ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพสีโดยใช้เคโอติกแม็ปและการสับเปลี่ยนจุดภาพในระดับบิตในโดเมนพื้นที่ โดยขั้นแรกใช้ Logistic chaotic sequence เพื่อเรียงสับเปลี่ยนตำแหน่งของจุดภาพและจากนั้นเปลี่ยนภาพเป็น binary matrix และเรียงสับเปลี่ยนบิตใหม่โดยใช้ Logistic sequence อีกอันหนึ่ง ผลที่ได้คือวิธีการนี้มีประสิทธิภาพสูงและสามารถประมวลผลได้เร็ว เหมาะที่จะนำไปใช้ในแอ็พพลิเคชั่นในพวกโทรศัพท์มือถือ

งานวิจัยของ A. Anto Steffi และ Dipesh Sharma [32] ได้นำเสนออัลกอริทึ่มที่แก้ไขปรับปรุงวิธีการเข้ารหัสและการถอดรหัสภาพโดยใช้เคโอติกแม็ป 2 ระบบ โดยเลือกที่จะใช้ Lorenz map และ Baker map โดยผู้วิจัยยังคงใช้ขั้นตอน Confusion และขั้นตอน Diffusion แต่ในแต่ละขั้นจะใช้กุญแจลับที่ต่างกัน (separate key)

กล่าวโดยสรุปแล้วในแต่ละวิธีการมีข้อดีข้อเสียที่แตกต่างกัน ทั้งนี้ขึ้นอยู่กับเทคนิคที่ถูกนำมาใช้ และเราจึงควรเลือกเทคนิคหรือวิธีการที่เหมาะสมกับโปรแกรมประยุกต์ต่างๆตามความต้องการของโปรแกรมประยุกต์นั้นๆ เนื่องจากวิธีการบางส่วนถูกปรับปรุงขึ้นเพื่อเพิ่มความเร็วในการประมวลผล เช่นวิธีการในกลุ่ม partial encryption ก็เหมาะสำหรับใช้ในโปรแกรมประยุกต์แบบทันกาล (real-time) และวิธีการบางกลุ่มก็ถูกปรับกลไกต่างๆเพื่อเพิ่มระดับความปลอดภัย (full encryption) ซึ่งในงานวิจัยนี้เราสนใจพัฒนาและออกแบบวิธีการเข้ารหัสที่มีความแข็งแกร่งขึ้นเพื่อนำไปใช้กับโปรแกรมประยุกต์ที่ต้องการระดับความปลอดภัยสูง ดังนั้นในงานวิจัยนี้เราจึงเลือกใช้วิธีการ full encryption แบบ chaos-based และเลือกใช้การทำ bit-plane decomposition ในโดเมนพื้นที่ (spatial domain) และนำสองแนวคิดนี้มาประกอบกันโดยใช้การแยกระนาบบิตก่อนและประยุกต์ใช้เคโอติกแม็ปหลายๆชนิด อันได้แก่ Logistic map, Standard map และ Tinkerbell map ที่ไม่เคยปรากฏในงานวิจัยประเภท image encryption มาประยุกต์ใช้ด้วย เพื่อสร้าง random bit matrix ที่หลากหลายสำหรับนำไปใช้ในขั้นตอนการสร้างความไร้ระเบียบ (confusion stage) และขั้นตอนการแพร่ (diffusion stage) เราคาดหวังว่านี่จะเป็นทางเลือกใหม่ในการเข้ารหัสข้อมูลภาพให้มีความปลอดภัยสูงขึ้น

บทที่ 3
แนวคิดและวิธีดำเนินการวิจัย

ในบทนี้จะกล่าวถึงแนวคิดและวิธีการดำเนินการวิจัย ซึ่งแนวคิดของงานวิจัยนี้คือการที่นำเค-โอติกแม็ปหลายชนิด (Multiple Chaotic Maps) มาประยุกต์ใช้ร่วมกัน เพื่อช่วยเพิ่มความซับซ้อนของลำดับที่ถูกสร้างขึ้นเพื่อนำไปเข้ารหัส และการประยุกต์ใช้เทคนิคการแยกระนาบบิต (Bit Plane Decomposition) ร่วมกันในลักษณะที่บิตที่มีนัยยะสำคัญต่างกันทั้ง 8 บิตนั้นถูกจัดเรียงไปคนละแบบ เพื่อช่วยเพิ่มคุณสมบัติความไร้ระเบียบและการแพร่ให้แก่ภาพที่ถูกเข้ารหัสได้ โดยคาดหวังว่าจะทำให้วิธีการเข้ารหัสรูปภาพที่เสนอนี้มีความทนทานมากขึ้นต่อการโจมตีในรูปแบบต่างๆ อันได้แก่ การโจมตีแบบเอนโทรปี (Entropy Attack), การโจมตีทางสถิติ (Statistical Attack), การโจมตีแบบตะลุย (Brute Force Attack) และ การโจมตีแบบใช้ความต่าง (Differential/Sensitivity Attack) ด้วยสมมติฐานที่ว่าเทคนิคนี้จะทำให้เราได้วิธีการเข้ารหัสข้อมูลภาพที่มีระดับความปลอดภัยสูงขึ้น โดยเราจะมีเกณฑ์การวัดประสิทธิภาพด้านความปลอดภัย 4 แบบด้วยกัน ได้แก่

a. การวิเคราะห์เอนโทรปีหรือความไร้ระเบียบของข้อมูล (Entropy Analysis)

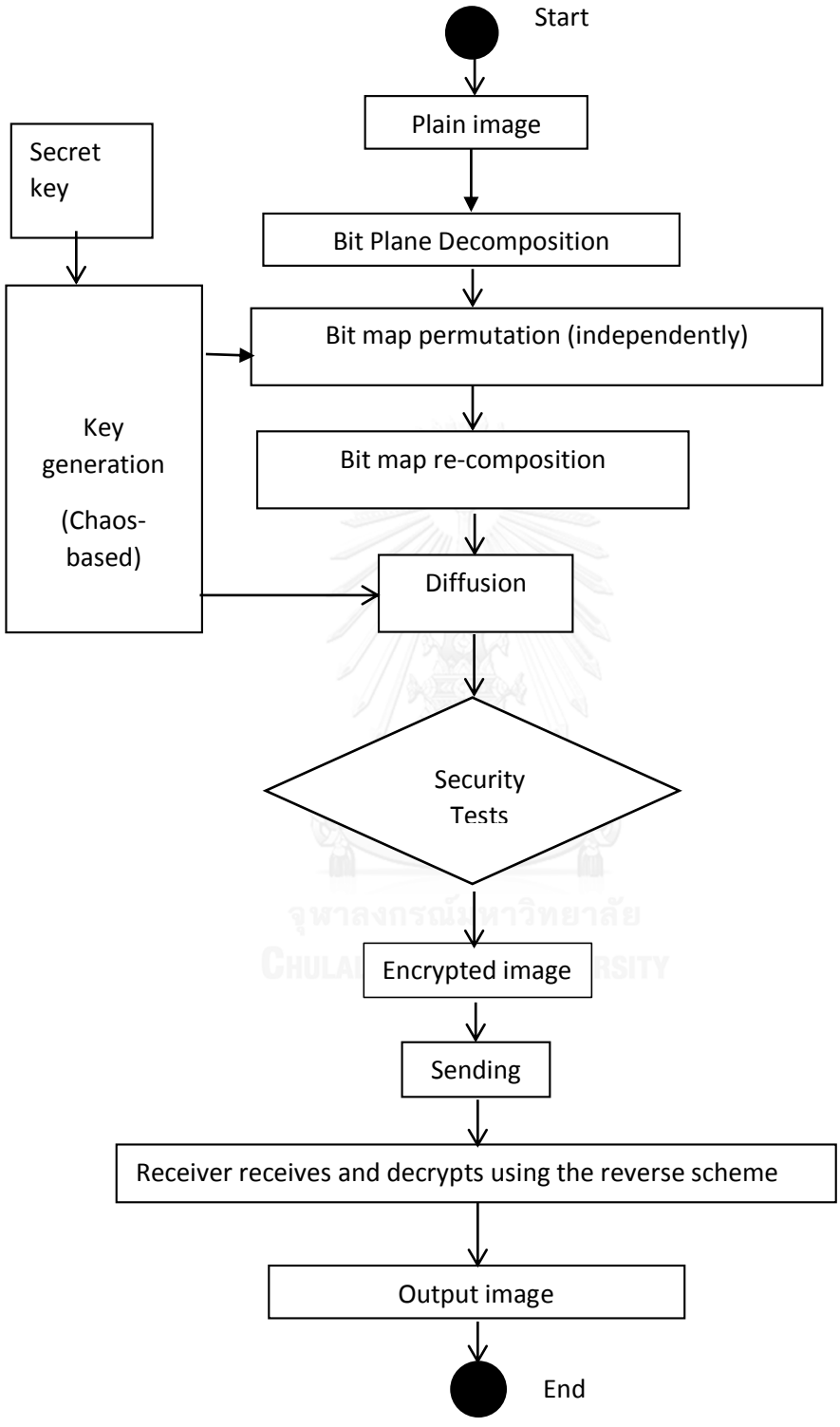
b. การวิเคราะห์ค่าทางสถิติของข้อมูลภาพ (Statistical Analysis) เช่น ฮิสโทแกรมของภาพ (Image Histogram) และ ค่าสัมประสิทธิ์ของความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficients)

c. การวิเคราะห์ขนาดของกุญแจ (Key Space Analysis)

d. การวิเคราะห์คุณสมบัติการแพร่กระจายของจุดภาพ (Diffusion Analysis / Sensitivity Analysis) เช่น วัดค่า NPCR (Number of Pixels Change Rate) และค่า UACI (Unified Average Changing Intensity)

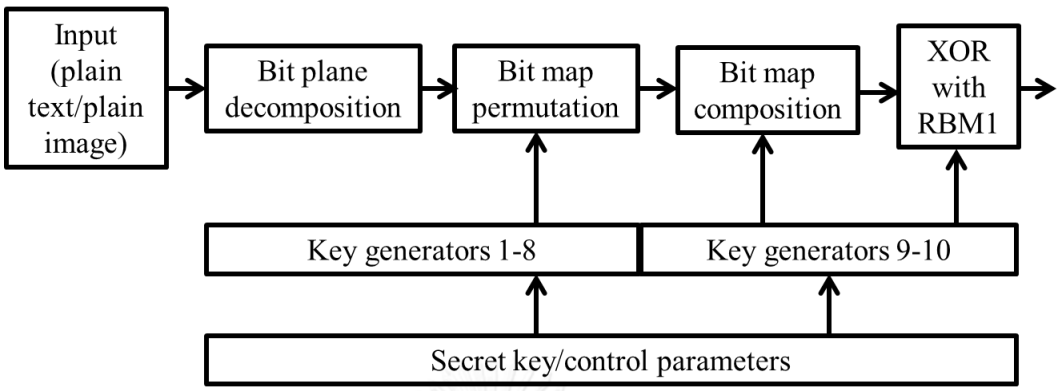
และในลำดับต่อไปจะกล่าวถึงภาพรวมทั้งหมดของงานวิจัยนี้

3.1 ภาพรวมทั้งหมดของงานวิจัย



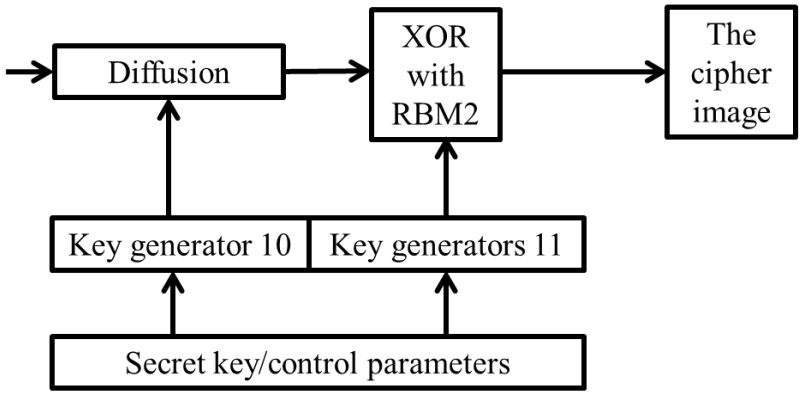
ภาพที่ 3-1 ภาพรวมทั้งหมดของงานวิจัย

สำหรับภาพรวมทั้งหมดของงานวิจัย ในงานวิจัยนี้สามารถแบ่งการทำงานออกได้เป็น 2 ขั้นตอนหลัก คือ ขั้นตอนการสร้างความไร้ระเบียบให้ข้อมูล (Confusion stage) และขั้นตอนการแพร่ (Diffusion stage)



ภาพที่ 3-2 ขั้นตอนการสร้างความไร้ระเบียบให้ข้อมูล (Confusion stage)

ในส่วนแรก ขั้นตอนการสร้างความไร้ระเบียบให้ข้อมูล (Confusion Stage) เรามีแนวคิดคือ จะทำการแยกระนาบบิตออกเป็น 8 ระนาบบิตก่อน (Bit Plane Decomposition) จากนั้นนำแต่ละระนาบบิตไปเรียงสับเปลี่ยนใหม่โดยเคโอติกแม็ปชนิดต่างๆที่ใช้พารามิเตอร์ควบคุมต่างๆกัน ซึ่งพารามิเตอร์ควบคุมนี้เราจะแบ่งมาจากกุญแจลับ (secret key) บรรยายให้เห็นภาพ คือ เมื่อเรามี 8 ระนาบบิต อาจจะใช้ Discretized Standard Map กับ 3 ระนาบบิต Logistic Chaotic Map กับ 3 ระนาบบิต และใช้ Tinkerbell Chaotic Map กับ 2 ระนาบบิต เป็นต้น และเรียงสับเปลี่ยนบิตในแต่ละระนาบบิตใหม่โดยเป็นอิสระต่อกัน หลังจากนั้นจึงนำทั้ง 8 ระนาบบิตมารวมเป็นภาพใหม่และส่งต่อไปยังขั้นตอนต่อไปหรือขั้นตอนการแพร่ (Diffusion Stage) นั่นเอง



ภาพที่ 3-3 ขั้นตอนการแพร่ (Diffusion stage)

ในส่วนที่สองหรือขั้นตอนการแพร่ (Diffusion Stage) เราจะใช้ประโยชน์จากเคโอติกแม็ปด้วยเช่นกัน คือ ใช้เคโอติกแม็ปต่างๆในการสร้างลำดับแบบสุ่มเทียม (random bit sequences) และนำลำดับนั้นๆมาเรียงใหม่เพื่อหาลำดับหรือทิศทางของการแพร่ จากนั้นนำข้อมูลภาพมาเรียงเป็นเวคเตอร์ และเปลี่ยนค่าสีของแต่ละจุดภาพโดยใช้ลำดับนั้นอ้างอิง

กำหนดให้ภาพมีขนาด $\mathrm{M} \times \mathrm{N}$

เรียงภาพใหม่เป็นเวคเตอร์ $J(i)$ โดยที่ $\mathrm{i} = 1,2,3,\ldots,\mathrm{M} \times \mathrm{N}$ จากนั้นเรียงภาพใหม่โดยใช้ลำดับการแพร่ที่ได้มาจากเคโอติกแม็ป เราจะทำการ BITXOR สองจุดภาพที่มีลำดับก่อนหน้าเพื่อเปลี่ยนค่าสีของจุดภาพหลังจากจุดก่อนหน้าไปเรื่อยๆตามลำดับที่ได้ และทำซ้ำจนครบ 1 รอบ (1 รอบการทำงาน คือ ขนาดของภาพ $\mathrm{M} \times \mathrm{N}$ ทั้งนี้เพื่อให้แต่ละจุดภาพสามารถเชื่อมโยงและส่งผลกระทบต่อการเปลี่ยนแปลงของอีกจุดภาพใดๆในภาพก็ได้)

$$J'(k) = J'(k-1) \bigoplus J'(k), \text{โดยที่ } \mathrm{k} = 1,2,3,\ldots,\mathrm{M} \times \mathrm{N}$$

ด้วยขั้นตอนการแพร่นี้ จะทำให้ภาพที่ถูกเข้ารหัสมีคุณสมบัติ butterfly effect คือถ้าค่าใดค่าหนึ่งเปลี่ยนแปลงไปเล็กน้อย จะส่งผลทำให้เกิดความแตกต่างอย่างมหาศาลกับจุดภาพที่เหลือ และภาพที่เข้ารหัสจะเกิดความแตกต่างกันแม้ภาพต้นฉบับแตกต่างกับเพียงจุดภาพเดียว ประโยชน์ของกระบวนการแพร่นี้คือทำให้วิธีการมีความทนทานต่อการโจมตีแบบรู้ภาพต้นฉบับล่วงหน้า หรือ known-plain image attack นั่นเอง

3.2 วิธีการเข้ารหัสข้อมูลภาพที่นำเสนอ (Proposed Image Encryption Method)

- เตรียมชุดภาพทดลอง เป็น test image ใน CV database

  1. ภาพ Lena test image ขนาด 128 X 128, 256 X 256, 512 X 512

  2. ภาพ Baboon test image ขนาด 128 X 128, 256 X 256, 512 X 512

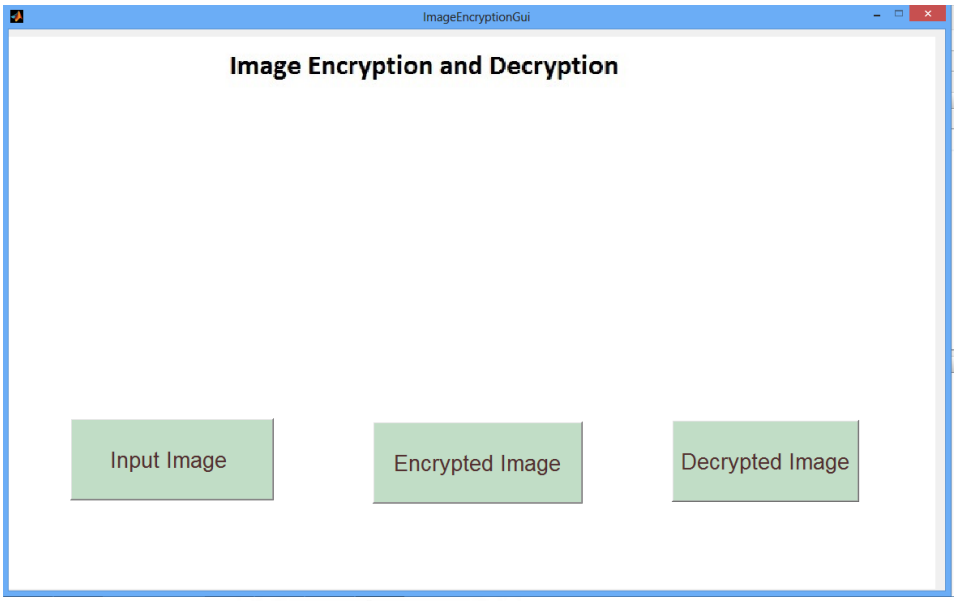
  3. ภาพ Airplane test image ขนาด 128 X 128, 256 X 256, 512 X 512

  และภาพที่จะใช้ทดลองเพิ่มเติม ได้แก่ ภาพสีดำล้วน ภาพสีขาวล้วน ภาพ Fruits ภาพ Peppers, ภาพ Barbara, ภาพ Goldhill, ภาพ Boat และภาพ Zelda

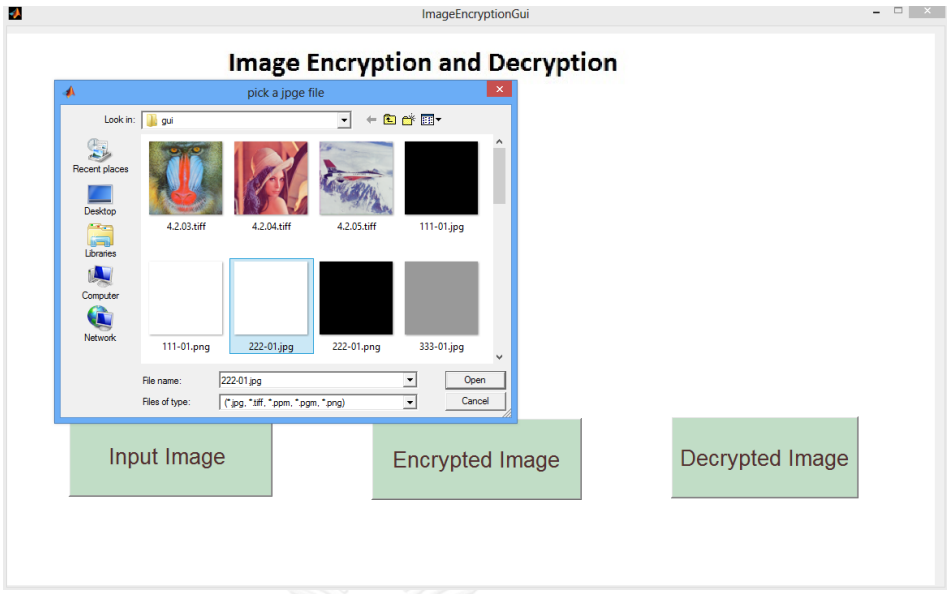
- เขียนโปรแกรมสำหรับการเข้ารหัสข้อมูลภาพ ในที่นี้ ใช้โปรแกรม MATLAB r2012a ในส่วนของโปรแกรมจะประกอบด้วย function ต่างๆดังต่อไปนี้

3.2.1 Image Encryption GUI

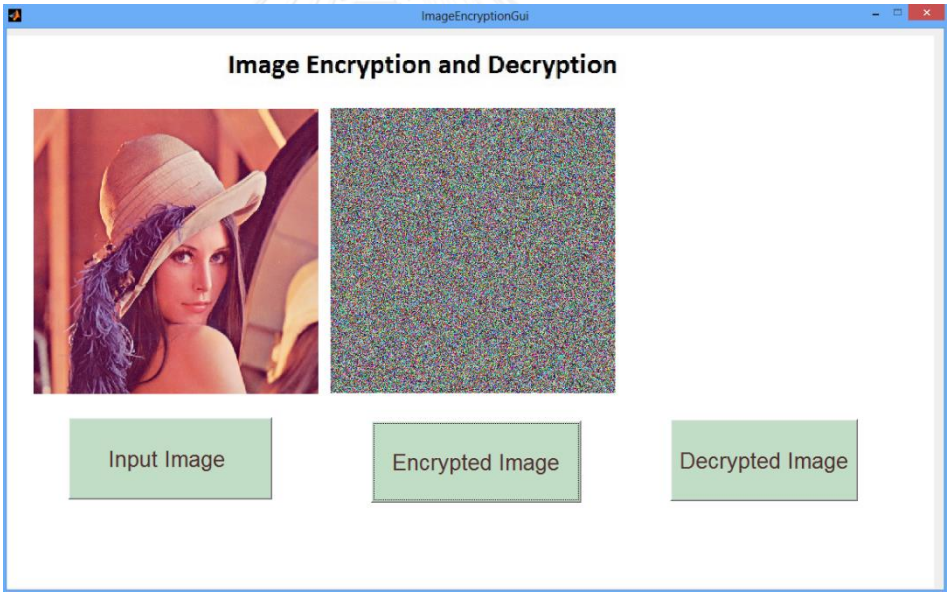
ออกแบบ Graphic User Interface ให้เหมาะกับการใช้งาน ในที่นี้ให้ผู้ใช้สามารถ browse เลือกรูปที่จะนำมาเข้ารหัสได้ และสามารถกด “encrypted image” เพื่อเข้ารหัสภาพตามวิธีการที่นำเสนอ และมีการบันทึกข้อมูลภาพที่ถูกเข้ารหัสลงบนคอมพิวเตอร์ด้วย และผู้ใช้ยังสามารถตรวจสอบได้อีกว่าด้วยวิธีการนี้สามารถถอดรหัสข้อมูลภาพออกมาได้ถูกต้องเหมือนกับภาพต้นฉบับหรือไม่ โดยการกด “decrypted image” และภาพที่ถูกถอดรหัสมาได้ก็จะถูกบันทึกไว้อัตโนมัติเช่นกัน



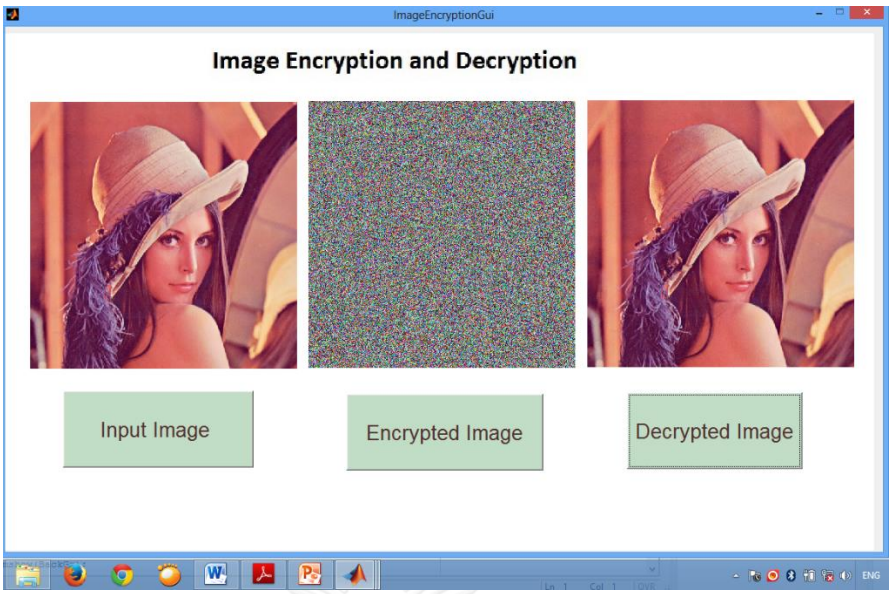
ภาพที่ 3-4 Graphic User Interface สำหรับที่จะใช้ในการเข้ารหัสและถอดรหัสข้อมูลภาพ



ภาพที่ 3-5 หน้าต่างเลือกรูปภาพที่จะนำมาเข้ารหัส



ภาพที่ 3-6 แสดงการใช้งานหลังจากกด “Encrypted Image”



ภาพที่ 3-7 ตัวอย่างภาพ Image Encryption GUI แสดงภาพ lena ต้นฉบับ ภาพ Lena ที่ถูกเข้ารหัส และภาพ Lena ที่ถูกถอดรหัสตามลำดับ

3.2.2 Converse Key to Parameter

ในส่วนนี้จะเป็นฟังก์ชั่นที่ใช้สำหรับแปลงค่ากุญแจลับหรือ secret key เป็นค่าพารามิเตอร์ต่างๆที่จะนำไปควบคุมค่าตัวแปรเริ่มต้นของเคโอติกแม็ปต่างๆในการสร้างลำดับ key sequence

3.2.3 Image Encrypt

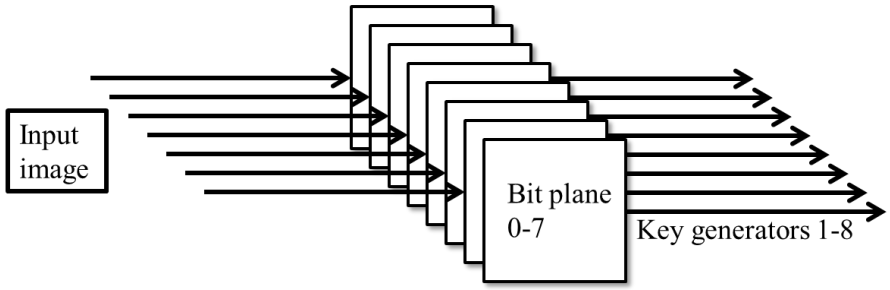
ฟังก์ชั่นเพื่อเข้ารหัสข้อมูลภาพ มีขั้นตอนวิธีการทำงานดังต่อไปนี้

Input: Plain-image + key

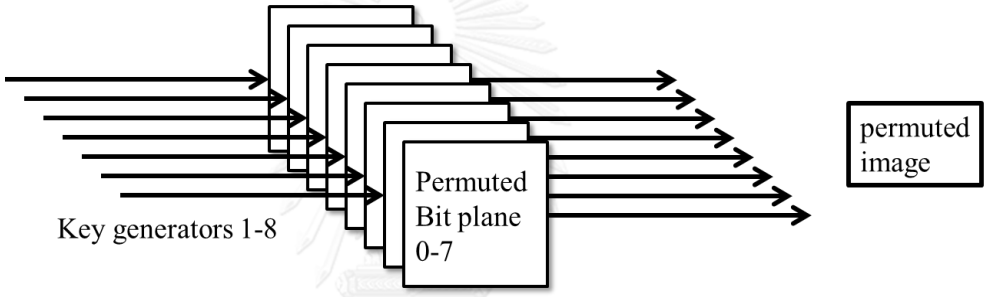
Output: Encrypted image

Algorithm:

โดยเริ่มแรกในส่วนของ Confusion stage จะมีการแยกระนาบบิตออกเป็น 8 ระนาบบิตด้วยกัน จากนั้นนำแต่ละระนาบบิตไปเรียงสับเปลี่ยนบิตใหม่โดยขึ้นอยู่กับกุญแจลับ (secret key) ที่ได้รับมาและนำกุญแจลับไปแปลงเป็นพารามิเตอร์ควบคุมในเคโอติกแม็ปจากนั้นสร้างเป็น random bit sequence ทั้ง 8 ที่เป็นอิสระต่อกัน และนำบิตมาทำการ permutation ตามลำดับเหล่านั้น หลังจากนั้นค่อยนำระนาบบิตทั้ง 8 มารวมกันใหม่และส่งต่อไปยัง diffusion stage



ภาพที่ 3-8 การแยกระนาบบิต (Bit plane decomposition)



ภาพที่ 3-9 การรวมระนาบบิต (Bit plane composition)

ข้อเสนอแนะในขั้นตอนนี้ คือเนื่องจากแต่ละระนาบบิตถูกเรียงสลับบิตใหม่โดยไม่ขึ้นต่อกัน เราสามารถแยกคิดแบบ parallel computing ก็ได้ ทำให้เวลาในการประมวลผลเร็วขึ้น

นำภาพที่ได้จาก confusion stage ไปสร้างคุณสมบัติของการแพร่ โดยใช้ประโยชน์จากเคโอติกแม็ปเช่นกัน แต่เป็นอันที่ใช้พารามิเตอร์ควบคุมคนละค่ากัน เมื่อได้ลำดับการแพร่ก็นำภาพมาเรียงเป็นเวคเตอร์และจัดการเปลี่ยนค่าสีของแต่ละจุดภาพตามลำดับนั้นไปเรื่อยจนจบ

$$J'(k) = J'(k-1) \oplus J'(k), \text{โดยที่ } \mathrm{k} = 1,2,3,\ldots,\mathrm{M} \times \mathrm{N}$$

สุดท้ายมีการวนซ้ำ ยิ่งจำนวนรอบมาก ความไร้ระเบียบของภาพที่ถูกเข้ารหัสก็จะเพิ่มขึ้น แต่แลกกับเวลาในการประมวลผลที่เพิ่มขึ้นนั้นเอง ในงานวิจัยนี้ใช้การวนในส่วนของ

การแพร่เท่ากับขนาดของภาพ นั่นคือ ถ้าหากในแต่ละจุดภาพเกิดการเปลี่ยนแปลงนั้น สามารถส่งผลกระทบถึงจุดภาพใดๆในภาพก็ได้

3.2.4 Image Decrypt

ฟังก์ชั่นเพื่อถอดรหัสข้อมูลภาพ

Input: Encrypted image + key

Output: Decrypted image

Algorithm:

โดยในส่วนนี้จะทำย้อนกลับจากขั้นตอนวิธีการเข้ารหัสข้อมูลภาพ กล่าวคือ เริ่มจากขั้นตอนการแพร่ (Diffusion stage) ย้อนไปสู่ขั้นตอนการสร้างความไร้ระเบียบ (Diffusion stage) ซึ่งในส่วนของขั้นตอนการแพร่นั้น จะใช้สมการเดิมและจำนวนรอบเท่าเดิมในการทำให้จุดภาพกลับคืนสู่ตำแหน่งที่ถูกต้องก่อนการแพร่

$$J'(k) = J'(k-1) \bigoplus J'(k), \text{โดยที่ } \mathrm{k} = 1,2,3,\ldots,\mathrm{M} \times \mathrm{N}$$

จากนั้นในส่วนของขั้นตอนการสร้างความไร้ระเบียบนั้นจะทำให้บิตทั้งหมดกลับคืนสู่ค่าเดิมและตำแหน่งเดิมโดยการนำไปดำเนินการ XOR กับเมทริกซ์บิตแบบสุ่มเทียมเหมือนกันกับในขั้นตอนการเข้ารหัส และจากนั้นเรียงสับเปลี่ยนระนาบบิตทั้ง 8 กลับคืนสู่ตำแหน่งเดิมโดยใช้วิธีการเดียวกันกับขั้นตอนใน 3.2.3 และนำระนาบบิตทั้ง 8 มารวมเป็นภาพอีกครั้ง ก็จะได้ภาพที่ถูกรหัสซึ่งเหมือนกับภาพต้นฉบับทุกประการ

3.2.5 Key Generators

ฟังก์ชั่นเพื่อสร้างลำดับโดยใช้เคโอติกแม็ป ดังต่อไปนี้

- Discretized Standard Map
- Logistic Chaotic Map
- Tinkerbell Chaotic Map

โดยจะทำการ implement ตามสมการเคโอติปแม็ปที่ได้กล่าวในหัวข้อ 2.4

3.2.6 Bit Permutation by Key

ฟังก์ชั่นที่ใช้ในการเรียงสับเปลี่ยนบิตโดยใช้ลำดับที่ถูกสร้างจาก 3.2.5

3.2.7 Image Diffusion by Key

ฟังก์ชั่นที่ใช้ในการเป็นทิศทางการแพร่โดยใช้ลำดับที่ถูกสร้างตามวิธี 3.2.5 เช่นกัน

3.2.8 Security Test

ฟังก์ชั่นที่ใช้ในการคำนวณค่าหรือกราฟต่างๆ ดังต่อไปนี้

- Entropy
- Histogram
- Correlation Coefficients
- Plots between adjacent pixels
- NPCR
- UACI

ซึ่งรายละเอียดการคำนวณจะกล่าวถึงต่อไปในหัวข้อ 3.4

3.3 การถอดรหัสข้อมูลภาพ (Image Decryption)

ในส่วนของการถอดรหัสภาพนั้น เราจะใช้วิธีการเดียวกันกับที่การเข้ารหัสภาพ เพียงแต่ขั้นตอนจะถูกทำย้อนกลับจากท้ายสุดไปแรกสุดเท่านั้น(reverse order) สามารถดูได้จากหัวข้อ 3.2.4

3.4 เกณฑ์การวัดประสิทธิภาพ

เราจะวัดประสิทธิภาพด้านความปลอดภัย 4 แบบด้วยกัน [13-17] ได้แก่

1. Entropy Analysis
2. Statistical Analysis
3. Key Space Analysis
4. Diffusion Analysis (Sensitivity Analysis)

3.4.1 Entropy Analysis

การวิเคราะห์เอนโทรปีหรือความไร้ระเบียบของข้อมูล (Entropy Analysis) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ entropy attack หรือไม่

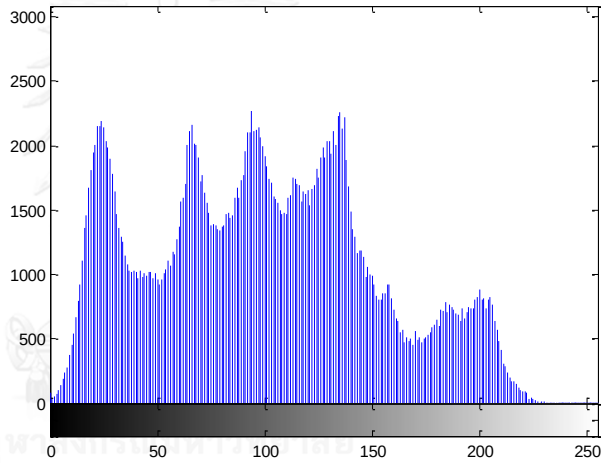
วิธีการคำนวณค่าเอนโทรปี (Entropy)

$$H(x) = -\sum_{i=1}^{N} p(x_i) log_2(p(x_i))$$

เนื่องจากเป็นภาพสีมีค่าสีอยู่ระหว่าง 0 ถึง 255 ค่าเอนโทรปีสูงสุดจะคือ 8 ถ้าหากได้ค่าเอน-โทรปีของ cipher image เข้าใกล้ 8 แสดงได้ว่าวิธีการเข้ารหัสนี้มีความทนทานต่อ entropy attack มาก

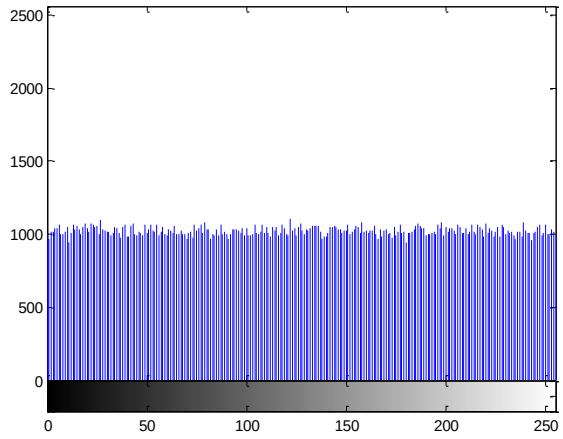
3.4.2 Statistical Analysis

การวิเคราะห์ค่าทางสถิติของข้อมูลภาพ (Statistical Analysis) เช่น ฮิสโทแกรมของภาพ (Histogram) และ ค่าสัมประสิทธิ์ของความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficient) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Statistical attack หรือไม่



ภาพที่ 3-10 แสดงตัวอย่างฮิสโทแกรมของภาพ

ถ้าหากฮิสโทแกรมแบบรูป uniform distribution แสดงว่าค่าสีของภาพเฉลี่ยไปเท่ากันๆในทุกๆค่าสี หมายถึงเป็นวิธีการเข้ารหัสข้อมูลที่ดี สามารถปกปิดคุณลักษณะของข้อมูลภาพต้นฉบับได้อย่างดีเยี่ยม



ภาพที่ 3-11 แสดงตัวอย่างฮิสโทแกรมของภาพ แบบ Uniform Distribution

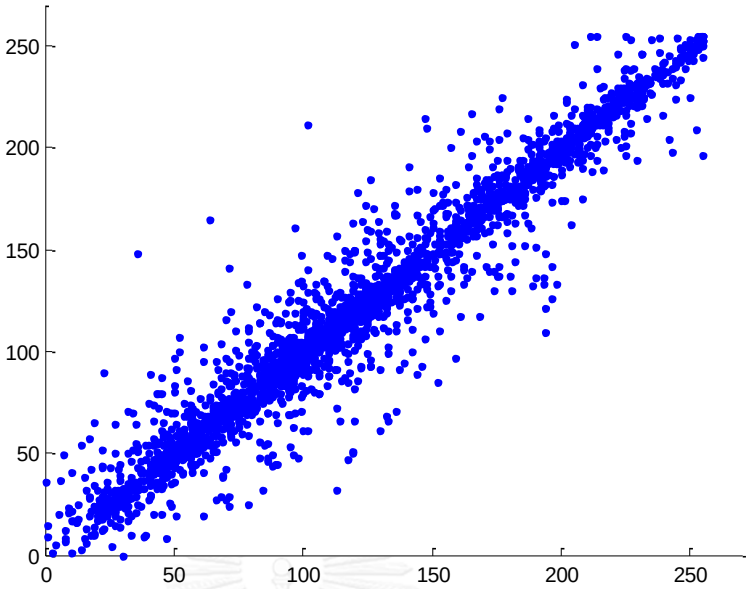
ส่วนค่าสัมประสิทธ์ความสัมพันธ์ระหว่างจุดภาพในแนวต่างๆ (Correlation Coefficient)สามารถคำนวณได้ดังนี้

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2)(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2)}}$$

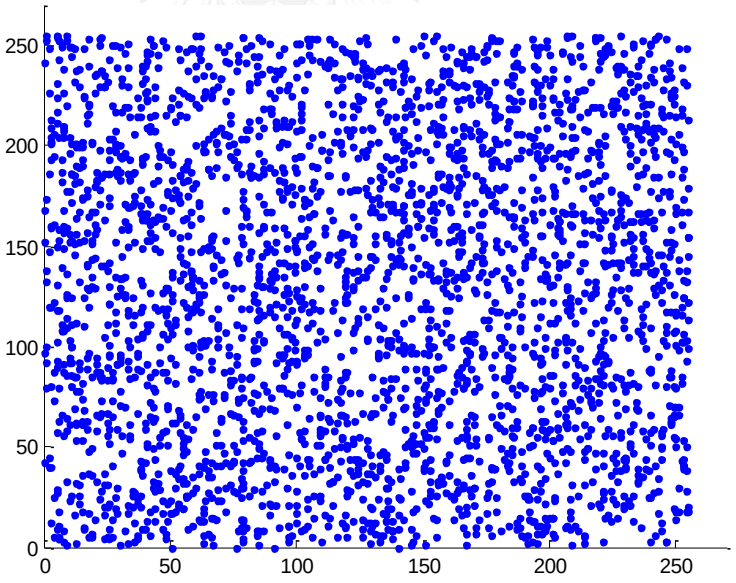
$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

r_{xy} จะมีค่าอยู่ระหว่าง -1 กับ 1 การวิเคราะห์คือ ถ้าหากค่า r_{xy} เข้าใกล้ศูนย์จะแสดงว่ามี correlation ต่ำ ถ้าหากค่าห่างจากศูนย์ไปแสดงว่า correlation สูง วิธีการเข้ารหัสข้อมูลภาพที่ดีควรจะให้ค่า correlation ของภาพที่ถูกเข้ารหัสที่ต่ำ เข้าใกล้ศูนย์ นอกจากนั้นเรายังสามารถนำค่าของจุดภาพที่อยู่ติดกัน (จะเป็นในแนวแกนนอน แกนตั้ง หรือ แกนทแยงก็ได้) มาพล็อตกราฟ เพื่อดูความสัมพันธ์ระหว่างจุดภาพได้อีกด้วย



ภาพที่ 3-12 ตัวอย่างภาพที่จุดภาพที่อยู่ใกล้กันมีความคล้ายคลึงกันสูง



ภาพที่ 3-13 ตัวอย่างภาพที่จุดภาพที่อยู่ใกล้กันมีความเป็นอิสระต่อกัน

3.4.3 Key Space Analysis

การวิเคราะห์ขนาดของกุญแจ (Key Space Analysis) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Brute force หรือไม่ เราใช้การคำนวณหาขนาดของ key ที่เราใช้

และวิเคราะห์เปรียบเทียบกับเกณฑ์มาตรฐานเรื่องขนาดของ key ขั้นต่ำในการเข้ารหัสให้ปลอดภัย ในกรณีนี้ไปเปรียบเทียบกับมาตรฐาน DES ซึ่งบอกว่า key space ควรมีขนาดไม่ต่ำกว่า 128 บิต

3.4.4 Diffusion Analysis (Sensitivity Analysis)

การวิเคราะห์คุณสมบัติการแพร่กระจายของจุดภาพ (Diffusion Analysis/Sensitivity Analysis) เช่น วัดค่า NPCR (Number of Pixels Change Rate) และค่า UACI (Unified Average Changing Intensity) เพื่อดูว่าวิธีการมีความทนทานต่อการโจมตีแบบ Differential attack หรือไม่

กำหนดให้ $c_1(i,j)$ และ $c_2(i,j)$ แทนภาพสองภาพ

ให้ $D(i,j)$ เป็นค่า 1 ถ้าค่า $c_1(i,j)$ และค่า $c_2(i,j)$ แตกต่างกัน และเป็นค่า 0 ถ้าเหมือนกัน

ค่า NPCR และ UACI สามารถคำนวณได้ดังนี้

$$NPCR = \sum_{i,j} \frac{D(i,j)}{(W \times H)} \times 100\%$$

$$UACI = \frac{1}{(W \times H)} \left[\sum_{i,j} \frac{c_1(i,j) - c_2(i,j)}{255} \right] \times 100\%$$

สำหรับค่า NPCR ไว้ใช้ทดลองเมื่อเราเปลี่ยนแปลง secret key เพียงเล็กน้อยแล้วดูว่าภาพที่ได้จากการเข้ารหัสแตกต่างไปจากเดิมมากหรือไม่ ถ้าเท่ากับ 100% แสดงว่าภาพสองภาพมีความแตกต่างกันทุกจุด วิธีการเข้ารหัสที่ดีจะให้ค่า NPCR เข้าใกล้ 100%

ส่วนค่า UACI ไว้ใช้ทดลองเมื่อเราเปลี่ยน plain image เพียงเล็กน้อยเช่น 1 จุดภาพ ภาพสองภาพที่ได้จากการเข้ารหัสด้วยวิธีเดียวกันควรมีความแตกต่างกัน โดยเฉลี่ยแล้วรูปภาพที่เป็น uniform distribution 2 ภาพจะมีค่าต่างกัน 33.33% ถ้าเป็นค่าระดับเทาจะมีความแตกต่างเฉลี่ยอยู่ประมาณ 255X33.33% = 85 นั่นเอง จึงสามารถใช้วัดระดับของความต่างของภาพ 2 ภาพได้

ทั้งสองค่านี้ก็จะทำให้เราสามารถประเมินได้ว่าคุณสมบัติการแพร่ (diffusion property) ของวิธีการเข้ารหัสดีหรือไม่

นอกจากนั้นเรายังจะนำค่าต่างๆเหล่านี้ไปเปรียบเทียบกับวิธีการเข้ารหัสภาพในกลุ่มเดียวกันเพื่อประเมินประสิทธิภาพของวิธีการของเราว่าดีเพียงพอหรือไม่ด้วย

บทที่ 4
การทดลองและผลการทดลอง

ในบทนี้จะกล่าวถึงเครื่องมือที่ใช้ในการทดลอง ผลการทดลองของการเข้ารหัสข้อมูลภาพและการถอดรหัสข้อมูลภาพด้วยวิธีการที่นำเสนอ และการทดสอบประสิทธิภาพด้านความปลอดภัย

4.1 เครื่องมือที่ใช้ในการทดลอง

4.1.1 ซอฟต์แวร์ที่ใช้ในการเขียนโปรแกรมคอมพิวเตอร์ คือ MATLAB r2012a

4.1.2 ฮาร์ดแวร์ที่ใช้ในการทดสอบคือ ซีพียู Intel® Core™i7-4500U CPU T7250 @ 1.80 GHz หน่วยความจำ 2.4 GB ฮาร์ดดิสก์ 150 GB บนระบบปฏิบัติการ Microsoft Window 8

4.1.3 รูปภาพที่ใช้ในการทดสอบ นามสกุล .png ได้แก่

1. ภาพ Lena test image ขนาด 128 X 128, 256 X 256, 512 X 512

2. ภาพ Baboon test image ขนาด 128 X 128, 256 X 256, 512 X 512

3. ภาพ Airplane test image ขนาด 128 X 128, 256 X 256, 512 X 512

และภาพที่จะใช้ทดลองเพิ่มเติม ได้แก่ ภาพสีดำล้วน ภาพสีขาวล้วน ภาพ Fruits ภาพ Peppers, ภาพ Barbara, ภาพ Goldhill, ภาพ Boat และภาพ Zelda

4.2 ผลการทดลอง

เราจะมุ่งเน้นที่การทดสอบประสิทธิภาพด้านความปลอดภัยเป็นหลัก โดยพิจารณาจากความสามารถในการที่วิธีการมีความทนทานต่อการโจมตีรูปแบบต่างๆ

โดยเราจะวัดประสิทธิภาพด้านความปลอดภัย 4 แบบด้วยกัน ได้แก่

A. Entropy Analysis

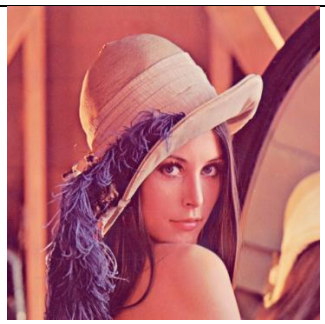
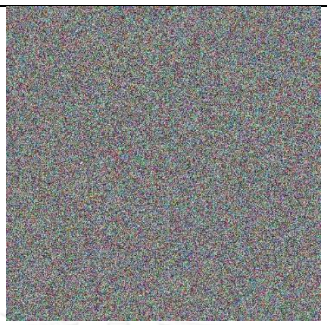
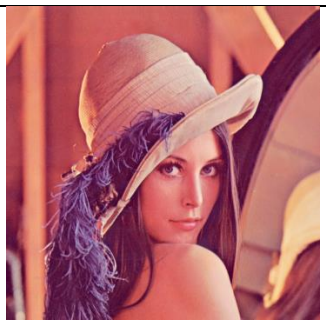
B. Statistical Analysis

C. Key Space Analysis

D. Diffusion Analysis (Sensitivity Analysis)

4.2.1 ภาพ Lena

ตารางที่ 4-1 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Lena)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ 4-1 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

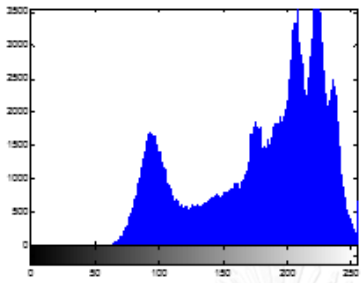
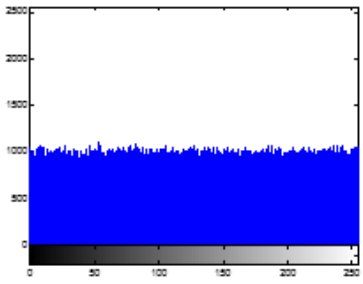
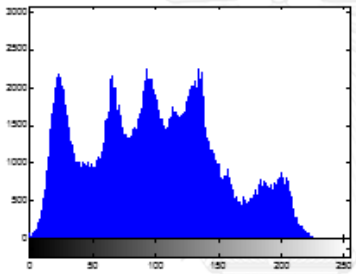
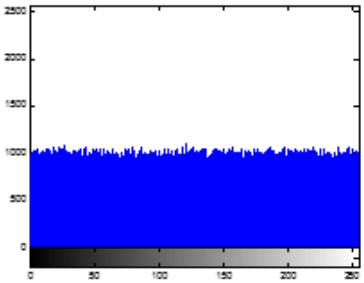
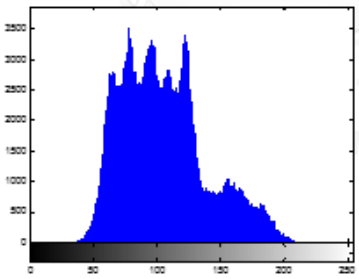
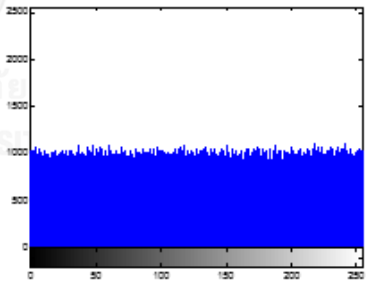
ตารางที่ 4-2 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Lena)

Entropy of Plain Image	Entropy of Encrypted Image
7.750197	7.999770

จากตารางที่ 4-2 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

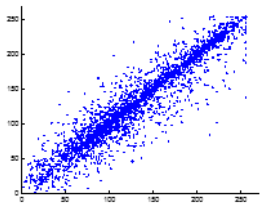
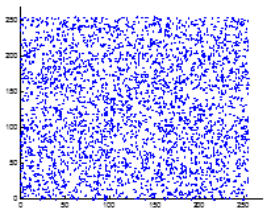
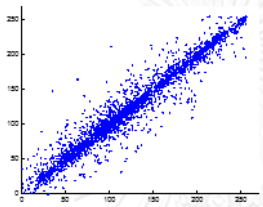
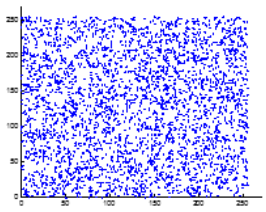
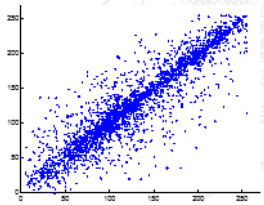
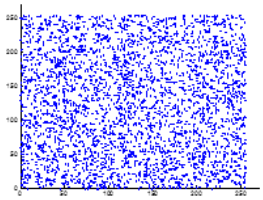
ตารางที่ 4-3 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Lena)

Channel	Histogram of Original Image	Histogram of Encrypted Image
Red		
Green		
Blue		

ตารางที่ 4-4 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Lena)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	R	0.9798	0.0024
	G	0.9691	-0.0013
	B	0.9327	0.0002
Vertical	R	0.9893	-0.0001
	G	0.9825	0.0032
	B	0.9576	-0.0036
Diagonal	R	0.9697	0.0022
	G	0.9555	-0.0004
	B	0.9183	0.0011

ตารางที่ 4-5 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Lena)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ 4-6 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard

	DES standard	Our proposed method
Key space	128 บิต	704 บิต

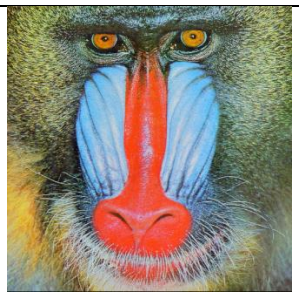
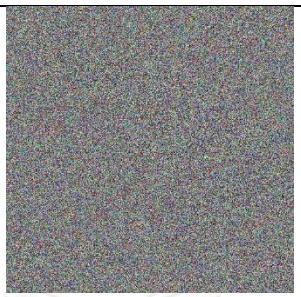
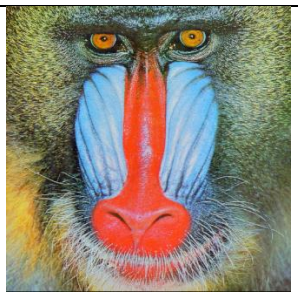
D. Diffusion Analysis

ตารางที่ 4-7 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Lena)

NPCR	99.25%
UACI	33.82%

4.2.2 ภาพ Baboon

ตารางที่ 4-8 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Baboon)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ 4-8 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

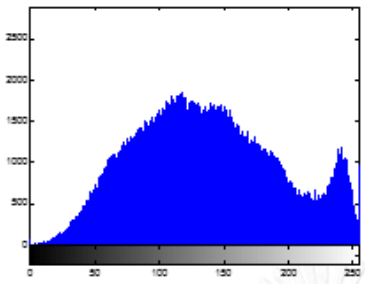
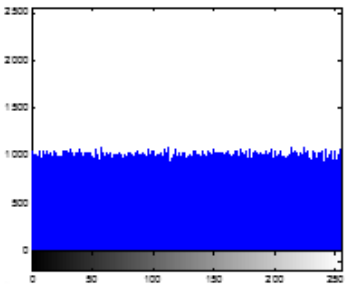
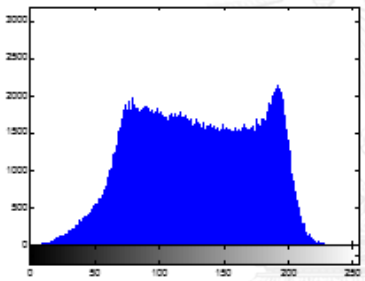
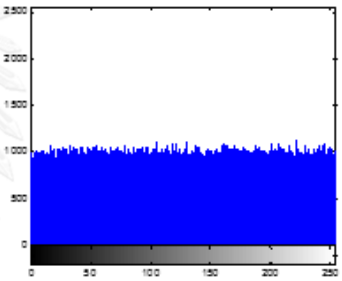
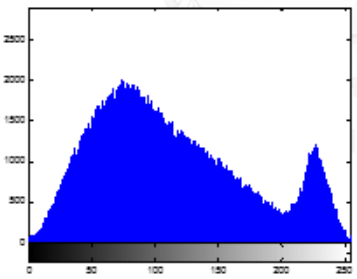
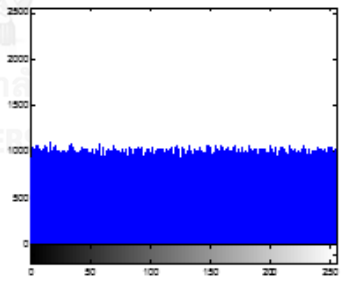
ตารางที่ 4-9 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Baboon)

Entropy of Plain Image	Entropy of Encrypted Image
7.762436	7.999761

จากตารางที่ 4-9 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

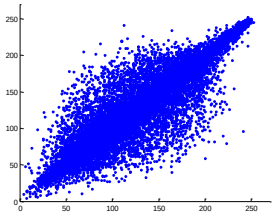
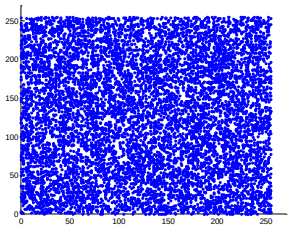
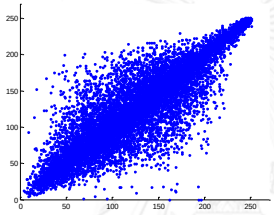
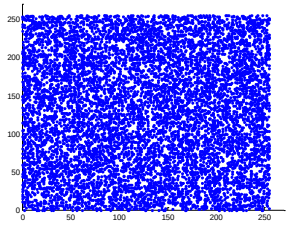
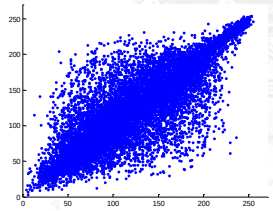
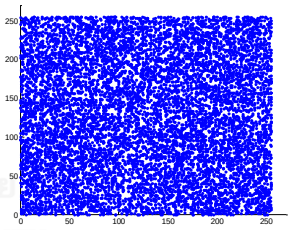
ตารางที่ 4-10 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Baboon)

Channel	Histogram of Original Image	Histogram of Encrypted Image
Red		
Green		
Blue		

ตารางที่ 4-11 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Baboon)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	R	0.9231	-0.0018
	G	0.8655	0.0016
	B	0.9073	-0.0017
Vertical	R	0.8660	0.0001
	G	0.7650	0.0025
	B	0.8809	-0.0015
Diagonal	R	0.8543	-0.0004
	G	0.7348	0.0030
	B	0.8399	-0.0034

ตารางที่ 4-12 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Baboon)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ 4-13 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard

	DES standard	Our proposed method
Key space	128 บิต	704 บิต

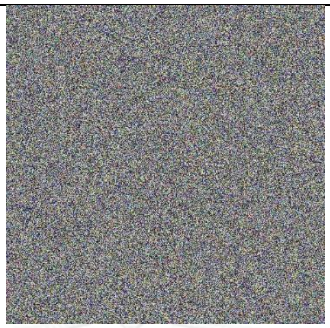
D. Diffusion Analysis

ตารางที่ 4-14 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Baboon)

NPCR	99.64%
UACI	33.79%

4.2.3 ภาพ Airplane

ตารางที่ 4-15 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Airplane)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ 4-15 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

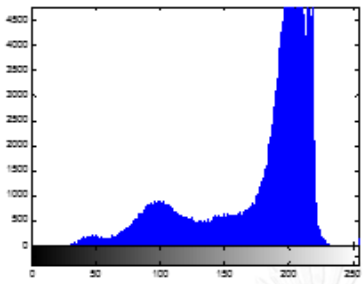
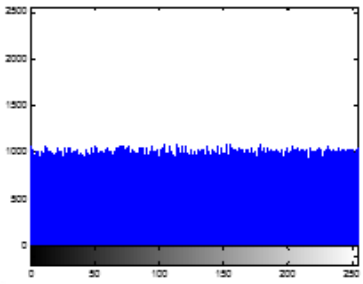
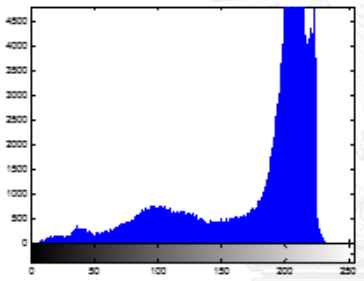
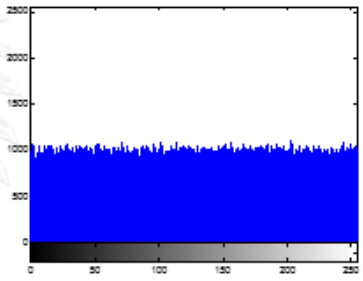
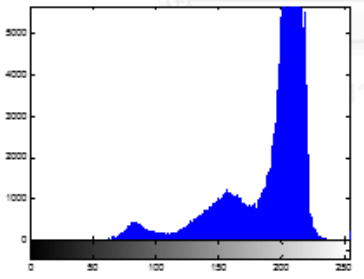
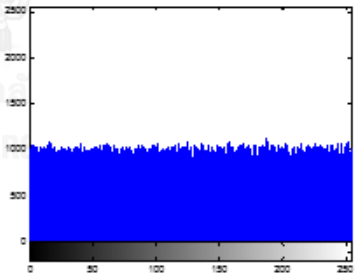
ตารางที่ 4-16 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Airplane)

Entropy of Plain Image	Entropy of Encrypted Image
6.663908	7.999757

จากตารางที่ 4-16 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

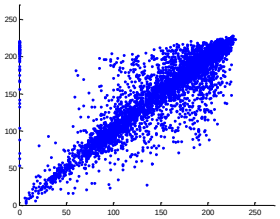
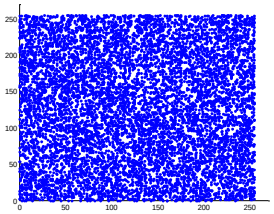
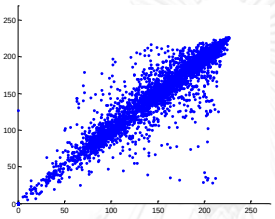
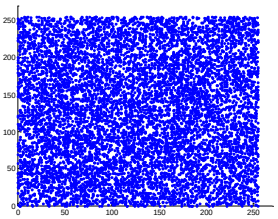
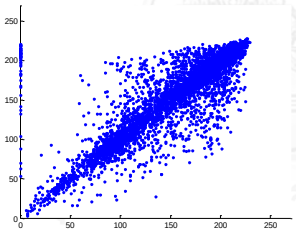
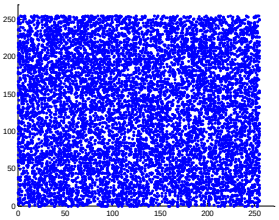
ตารางที่ 4-17 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Airplane)

Channel	Histogram of Original Image	Histogram of Encrypted Image
Red		
Green		
Blue		

ตารางที่ 4-18 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Airplane)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	R	0.9726	0.0016
	G	0.9578	0.0005
	B	0.9640	0.0005
Vertical	R	0.9568	0.0003
	G	0.9678	-0.0013
	B	0.9353	-0.0018
Diagonal	R	0.9343	-0.0004
	G	0.9326	-0.0045
	B	0.9146	-0.0004

ตารางที่ 4-19 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Airplane)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ 4-20 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard

	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ 4-21 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Airplane)

NPCR	99.88%
UACI	33.57%

ตารางที่ 4-22 ตารางแสดงเวลาที่ใช้ในการเข้ารหัสข้อมูลภาพและถอดรหัสข้อมูลภาพ

ชื่อภาพ	ขนาดภาพ	เวลาที่ใช้ในการเข้ารหัส (วินาที)	เวลาที่ใช้ในการถอดรหัส (วินาที)
Lena	128 X 128	0.69	0.62
	256 X 256	1.57	1.68
	512 X 512	3.08	3.12
Baboon	128 X 128	0.57	0.59
	256 X 256	1.25	1.32
	512 X 512	2.98	3.03
Airplane	128 X 128	0.65	0.64
	256 X 256	1.43	1.39
	512 X 512	3.31	3.30

จากตารางที่ 4-22 พบว่าวิธีการเข้ารหัสภาพที่นำเสนอสามารถนำไปประยุกต์ใช้งานได้จริง

ตารางที่ 4-23 ตารางเปรียบเทียบประสิทธิภาพของวิธีการที่นำเสนอกับวิธีการต่างๆใกล้เคียงที่มีอยู่ในปัจจุบัน (ภาพ Lena)

	A. Entropy Analysis	B. Statistical Analysis	3. Key Space Analysis	4. Sensitivity Analysis	
	Entropy	Correlation Coefficients	Key Space (bit)	NPCR (%)	UACI (%)
Liu H., 2011 [33]	7.9791	0.0578	380	99.56	33.4
Fu C., 2011 [26]	7.9880	0.0013	153	99.61	-
R. liu, 2012 [31]	7.9986	0.0142	-	-	-
Gururaj, 2014 [34]	7.996877	-0.005527	640	99.59	33.45
Our proposed method	7.999770	0.000411	704	99.25	33.82
Theoretical value	8	0	-	100	33.33

บทที่ 5
สรุปผลการวิจัย

ในบทนี้จะกล่าวถึงผลสรุปงานวิจัย ปัญหาที่พบ และขอเสนอแนะอันจะเป็นแนวทางการวิจัยด้านการเพิ่มความปลอดภัยในการพัฒนาระบบการเข้ารหัสข้อมูลภาพต่อไป

5.1 บทสรุป

วิทยานิพนธ์ฉบับนี้ได้นำเสนอวิธีการเข้ารหัสข้อมูลภาพ เพื่อพัฒนาวิธีการเข้ารหัสข้อมูลภาพให้มีความแข็งแกร่งขึ้น โดยใช้เทคนิคการแบ่งข้อมูลภาพออกเป็นระนาบบิตต่างๆก่อนและประยุกต์ใช้เค-โอติกแม็ปต่างชนิดกัน ได้แก่ Discretized Standard Map, Logistic Map และ Tinkerbell Map ในการเรียงสับเปลี่ยนบิตในแต่ละระนาบบิตอย่างสุ่มเทียมและเป็นอิสระต่อกัน ทำให้ภาพที่ถูกเข้ารหัสมีคุณสมบัติความไร้ระเบียบและการแพร่ที่ดีขึ้น และมีความทนทานมากขึ้นต่อการโจมตีรูปแบบต่างๆ

จากการทดลองด้วยรูปภาพทดลอง (test image) ต่างๆสามารถทดสอบประสิทธิภาพด้านความปลอดภัยของวิธีการที่นำเสนอด้วยการวิเคราะห์ 4 ด้านด้วยกัน [13-17] ได้แก่

A. Entropy Analysis

จากผลการคำนวณค่าเอนโทรปีหรือค่าความไร้ระเบียบของข้อมูลพบว่า ข้อมูลภาพที่ถูกเข้ารหัสมีค่าเอนโทรปีใกล้เคียงค่าเอนโทรปีที่เป็นไปได้มากสุดของภาพสี นั่นก็คือ 8 และมากกว่าค่าเอนโทรปีของภาพต้นฉบับอย่างมีนัยยะสำคัญ นั่นก็หมายความว่า ภาพที่ถูกเข้ารหัสมีการกระจายตัวของค่าสีของแต่ละจุดภาพดีกว่าภาพต้นฉบับนั่นเอง แสดงให้เห็นว่าวิธีการเข้ารหัสข้อมูลภาพที่นำเสนอมีประสิทธิภาพทำให้ข้อมูลมีความไร้ระเบียบมากขึ้นและมีความทนทานต่อการโจมตีแบบเอนโทรปี

B. Statistical Analysis

ในส่วนนี้เราจะพิจารณาดูข้อมูลทางสถิติ ในที่นี้เนื่องจากข้อมูลที่เราทดลองเป็นข้อมูลภาพ เราจะพิจารณาฮิสโทแกรม (Histogram) และค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficients)

- **ฮิสโทแกรม (Histogram)**

จากการพิจารณาฮิสโทแกรมของภาพแล้วพบว่าภาพที่ถูกเข้ารหัสด้วยวิธีการที่นำเสนอมีการกระจายของฮิสโทแกรมใกล้เคียงกับการ Uniform Distribution ส่วนฮิสโทแกรมของภาพต้นฉบับนั้นก็เป็นไปตามลักษณะของภาพนั้นๆซึ่งเป็นลักษณะเฉพาะตัวของภาพ เมื่อเราได้ฮิสโทแกรมของภาพที่

ถูกเข้ารหัสที่มีลักษณะใกล้เคียง Uniform Distribution จึงแสดงให้เห็นว่าวิธีการเข้ารหัสที่นำเสนอสามารถปกปิดคุณลักษณะของภาพต้นฉบับได้เป็นอย่างดี เนื่องจากหากดูจากฮิสโทแกรมประเภท Uniform Distribution ไม่สามารถสืบค้นได้ว่าเป็นฮิสโทแกรมนี้เป็นของภาพต้นฉบับภาพใด

- ค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพ (Correlation Coefficients)

จากการพิจารณาค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพเฉลี่ยทั้งภาพและทุกทิศทาง ได้แก่ ระหว่างจุดภาพทางแนวแกนนอน แกนตั้ง และแกนทแยง พบว่าค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพของภาพที่ถูกเข้ารหัสมีค่าใกล้เคียง 0 และค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพของภาพต้นฉบับใกล้เคียง 1 นั่นก็หมายความว่าจุดภาพที่อยู่ติดกันของภาพที่ถูกเข้ารหัสนั้นไม่มีความสัมพันธ์กันอย่างมีนัยยะสำคัญ หรือเรียกได้ว่าไม่มีความสัมพันธ์กันเลย ส่วนจุดภาพที่อยู่ติดกันของภาพต้นฉบับมีความสัมพันธ์กันในทางตรง แสดงให้เห็นว่าวิธีการเข้ารหัสข้อมูลภาพที่นำเสนอนั้นสามารถปกปิดคุณสมบัติเชิงสถิติของภาพต้นฉบับได้ดี ทำให้มีความแข็งแกร่งทนทานต่อการโจมตีแบบสถิติ

C. Key Space Analysis

จากการวิเคราะห์เรื่องขนาดของกุญแจ เนื่องจากวิธีการเข้ารหัสที่นำเสนอใช้เคโอติปแม็ปหลายชนิดทำให้มีตัวแปรควบคุมหรือพารามิเตอร์ในแต่ละสมการหลายตัว รวมทั้งสิ้น 11 ตัว และแต่ละค่าสามารถแทนด้วยจำนวนบิตในคอมพิวเตอร์ เท่ากับ 64 บิต นั่นก็หมายความว่าจำนวนบิตทั้งหมดสำหรับกุญแจของวิธีการนี้ คือ 11X64 = 704 บิต ซึ่งสามารถผ่านมาตรฐานของ DES ซึ่งระบุไว้ว่าขนาดของกุญแจที่ให้ระดับความปลอดภัยที่มั่นใจได้ คือ 128 บิตในปัจจุบัน ที่ไม่สามารถโจมตีแบบตะลุย (Brute Force Attack) ได้ในระยะเวลาอันสั้น

D. Diffusion Analysis หรือ Differential Analysis

จากการทดลองหาค่า NPCR (Number of Pixels Changing Rate) และค่า UACI (Unified Average Changing Intensity) เพื่อดูว่าวิธีการที่นำเสนอมีความไวต่อการเปลี่ยนแปลงค่าสถานะเริ่มต้นหรือมีคุณสมบัติของการแพร่หรือไม่ พบว่าค่า NPCR มีค่าโดยเฉลี่ย 99.6% และค่า UACI มีค่าโดยเฉลี่ย 33.42% จากการทดลองทั้ง 11 ภาพ ซึ่งใกล้เคียงกับค่าทางทฤษฎีนั่นคือ 100% และ 33.33%

ค่า NPCR สามารถบ่งบอกถึง ผลความแตกต่างจากการเปลี่ยนแปลงกุญแจลับ นั่นก็คือว่า ถ้าหากมีการเข้ารหัสด้วยกุญแจที่แตกต่างออกไปเล็กน้อย เช่น 1 บิต จะส่งผลให้ภาพที่ถูกเข้ารหัสมีความแตกต่างออกไปอย่างไร หากเท่ากับ 100% แสดงว่าภาพที่ถูกเข้ารหัสสองภาพแตกต่างกันโดยสิ้นเชิง ซึ่งจากผลการทดลองแสดงให้เห็นว่า ภาพที่ถูกเข้ารหัสด้วยกุญแจที่แตกต่างกันเล็กน้อยของวิธีการที่นำเสนอนี้มีความแตกต่างกันเกือบทุกจุดภาพ หรือประมาณ 99.6%

ส่วนค่า UACI สามารถวัดระดับความแตกต่างของภาพสองภาพ และเรานำไปใช้เพื่อวัดคุณสมบัติการแพร่ (Diffusion Property) นั่นคือ ถ้าหากค่าของจุดภาพในภาพต้นฉบับถูกเปลี่ยนแปลงไปเพียง 1 จุดภาพจะทำให้ภาพที่ถูกเข้ารหัส 2 ภาพ (ภาพหนึ่งจากภาพต้นฉบับดั้งเดิม อีกภาพจากภาพต้นฉบับที่มีเพียงค่าสีของบางจุดภาพเปลี่ยนแปลงไป) แตกต่างกัน ถ้าหากภาพที่ถูกเข้ารหัสทั้งสองภาพมีความแตกต่างกันประมาณ 33.33% นั่นหมายความว่าภาพที่ถูกเข้ารหัสทั้งสองเป็น uniform distribution ที่ต่างกัน ในทางทฤษฎีนั้นค่าเฉลี่ยความต่างของสองชุดตัวเลขแบบ uniformly distributed ระหว่าง 0 กับ 1 จะมีค่าเท่ากับ 1/3 นั่นคือ 33.33% ซึ่งจากผลการทดลองแสดงให้เห็นว่าค่า UACI โดยเฉลี่ยของวิธีการที่นำเสนอจากการทดลองด้วยภาพ 11 ภาพได้ผลลัพธ์คือ 33.42%

สรุปการวิเคราะห์โดยใช้ความต่างได้ว่าวิธีการที่นำเสนอสามารถเข้ารหัสข้อมูลภาพได้อย่างมีประสิทธิภาพและภาพที่ถูกเข้ารหัสมีความไวต่อการเปลี่ยนแปลงค่าเริ่มต้นเช่นกุญแจลับหรือข้อมูลภาพต้นฉบับ ซึ่งเป็นคุณสมบัติการแพร่ที่ดี

จากตาราง 4-23 เมื่อเปรียบเทียบผลการทดลองภาพ Lena กับวิธีการใกล้เคียงที่มีอยู่ในปัจจุบันแล้วพบว่าวิธีการที่นำเสนอได้ค่าเอนโทรปีที่ใกล้เคียงค่าเป็นไปได้มากสุดทางทฤษฎีมากกว่าวิธีการอื่นๆ และได้ค่าสัมประสิทธิ์ความสัมพันธ์ระหว่างจุดภาพที่อยู่ติดกันใกล้ค่า 0 มากกว่าวิธีการอื่น นั่นหมายถึงว่า มีความเป็นไปได้ว่าวิธีการที่นำเสนอนั้นมีความทนทานต่อการโจมตีแบบเอนโทรปีและทางสถิติมากกว่าวิธีการอื่นๆ และนอกจากนั้นวิธีการที่นำเสนอยังมีขนาดของกุญแจที่ใหญ่กว่าวิธีการอื่นทำให้มีความทนทานต่อการโจมตีแบบตะลุยมากกว่าด้วย ส่วนค่า NPCR และ UACI นั้นยังไม่สามารถสรุปได้ แต่ถือว่าวิธีการที่นำเสนอให้ผลลัพธ์ออกมาในเกณฑ์ดี

5.2 ข้อเสนอแนะ

เนื่องจากในงานวิจัยนี้เราใช้โปรแกรม Matlab ในการวิจัยเพื่อความสะดวกในการทดลองกับข้อมูลชนิดรูปภาพ การแสดงผลและกราฟต่างๆ ซึ่งอาจจะทำให้มีความช้าในการประมวลผล หากต้องการเพิ่มประสิทธิภาพความเร็วในการประมวลผล เราอาจจะพิจารณาใช้ภาษา C หรือภาษาอื่นๆ ในการเขียนโปรแกรม และนอกจากนั้นในส่วนของขั้นตอนการสร้างความไร้ระเบียบ (Confusion Stage) ตอนที่เราแยกระนาบบิตออกเป็น 8 ระนาบบิตและนำไปเรียงสับเปลี่ยนโดยใช้เคโอติกแม็ปต่างชนิดกันนั้น เนื่องจากการเรียงสับเปลี่ยนเป็นอิสระและไม่ขึ้นต่อกัน เราอาจจะพิจารณาใช้ parallel computing ในการช่วยคำนวณเพื่อย่นระยะเวลาในส่วนนี้ลง และจะทำให้วิธีการเข้ารหัสที่นำเสนอมีความรวดเร็วมากขึ้นกว่าเดิม

รายการอ้างอิง

1. Smart, N., *Cryptography: An Introduction*. 2004: McGraw-Hill.
2. Christof Paar, J.P., *Understanding Cryptography: A Textbook for Students and Practitioners*. 2010: Springer.
3. Rinki Pakshwar, V.K.T., Vineet Richhariya, *A Survey On Different Image Encryption and Decryption Techniques.* International Journal of Computer Science and Information Technologies, 2013. 4: p. 113-116.
4. Kamlesh Gupta, S.S., *New Approach for Fast Color Image Encryption Using Chaotic Map.* Journal of Information Security, 2011. 2: p. 139-150.
5. C. Fu, W.H.M., Y.F. Zhan, Z.L. Zhu, F.C.M. Lau, C.K. Tse, H.F. Ma, *An efficient and secure medical image protection scheme based on chaotic maps.* Computers in Biology and Medicine, September 2013. 43(8): p. 1000-1010.
6. K. Wang, W.P., et al, *On the security of 3D Cat map based on symmetric image encryption scheme.* Physics Letters A, August 2005. 343: p. 432-439.
7. N.K. Pareek, V.P., and K.K. Sud, *Image encryption using chaotic logistic map.* Image and Vision Computing, September 2006. 24: p. 926-934.
8. Li, X., *Image encryption scheme based on multiple chaotic maps*, in *IEEE International Conference on Emerging Intelligent Data and Web Technologies (EIDWT)*. September 2013: Xi'an, China.
9. A. Mousa, E.M.E.-R., et al, *Images cryptosystem based on chaotic maps for databases security*, in *IEEE 2nd International Japan-Egypt Conference on Electronics, Communications, and Computers*. December 2013.
10. C.K. Huang, H.H.N., *Multi chaotic systems based pixel shuffle for image encryption.* Optic Communications, June 2009. 282: p. 2123-2127.
11. F.Y. Sun, S.T.L., Z.Q. Li, Z.W. Lu, *A novel image encryption scheme based on spatial chaos map.* Chaos Solitions & Fractals, November 2008. 38(3): p. 631-640.
12. F. Chong, H.S., et al, *A chaos-based image encryption scheme with a*

plaintext related diffusion, in IEEE Int. Conf. on Information, Communications and Signal Processing. December 2013: Taiwan.

13. Z.L. Zhu, W.Z., et al, *A chaos-based symmetric image encryption scheme using a bit-level permutation.* Information sciences, March 2011. 181: p. 1171-1186.
14. G., Y., *Image scrambling encryption algorithm of pixel bit based on chaos map.* Pattern recognition letters, April 2010. 31: p. 347-354.
15. Fu C., L.B., Miao Y., Liu X., and Chen J., *A novel chaos-based bit-level permutation scheme for digital image encryption.* Optics communications, November 2011. 284: p. 5415-5423.
16. G.J Zhang, Q.L., *A novel image encryption method based on total shuffling scheme.* Optics Communications, June 2011. 284: p. 2775-2780.
17. H.T. Panduranga, S.K.N., et al, *Partial image encryption using blockwise shuffling and chaotic map*, in International Conference on Optical Imaging Sensor and Security. July 2013: India.
18. Sulong, L.M.J.a.G.B., *A Review Of Color Image Encryption Techniques.* IJCSI International Journal of Computer Science Issues, November 2013. 10(6): p. 266-275.
19. H.Gao, Y.Z., S. Liang, D.Li *A New Chaotic Image Encryption Algorithm*. Chaos, Solitons and Fractals 29. 2006.
20. H. Yu, Z.Z., *An Efficient Encryption Algorithm Based on Image Reconstruction*, in *International Workshop on Chaos-Fractals Theories and Applications.* 2009.
21. K.C. Ravishankar, M.G.V., *Region Based Selective Image Encryption*, in *Computing & Informatics,* 2006. *ICOCI '06. International Conference on* June 2006. p. 1-6.
22. S.H. Kamali, R.S., *A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption*, in *IEEE International Conference On Electronics and Information Engineering (ICEIE).* August 2010. p. 141-145.
23. Krishna, K.S.S.a.B.V.S., *A New Chaotic Algorithm for Image Encryption and*

Decryption of Digital Color Images. International Journal of information and Education Technology, June 2011. 1(2).

24. Hazem Mohammad Al-Najjar, A.M.A.-N., *Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table*. 2011.

25. Somaya Al-Maadeed, A.A.-A., and Turki Abdalla, *A New Chaos-Based Image-Encryption and Compression Algorithm.* Journal of Electrical and Computer Engineering, 2012.

26. Chong Fu, J.-j.C., Hao Zou, Wei-hong Meng, Yong-feng Zhan, and Ya-wen, *A chaos-based digital image encryption scheme with an improved diffusion strategy.* Optical Society of America, January 2012. 20(3): p. 2363-2378.

27. M, S.R.M.a.S. *An Uncompressed Image Encryption Algorithm Based on DNA Sequences*. in *Computer Science & Information Technology (CS & IT).* 2011.

28. Jacob, P.A.J.P.M.K.P., *Matrix based Cryptographic Procedure for Efficient Image Encryption*, in *IEEE Recent Advances in Intelligent Computational Systems (RAICS)*. September 2011. p. 173-177.

29. X.cong, X.F.G., *An Image Encryption Algorithm based on Scrambling and Substitution using Hybrid Chaotic Systems*, in Computational Intelligence and Security (CIS), *2011* Seventh International Conference *on* December 2011. p. 882-885.

30. Zhao, R.Y.H., *An Efficient Chaos-based Image Encryption Scheme Using Affine Modular Maps.* International Journal Computer Network and Information Security, 2012. 7: p. 41-50.

31. R. liu, X.t., *New algorithm for color image encryption using chaotic map and spatial bit level permutation.* Journal of Theoretical and Applied Information Technology, September 2012. 43(1).

32. A. Anto Steffi, D.S., *Modified Algorithm of Encryption and Decryption of Images using Chaotic Mapping.* International Journal of Science and Research (IJSR), February 2013. 2(2).

33. Liu H., W.X., *Color image encryption using spatial bit-level permutation and*

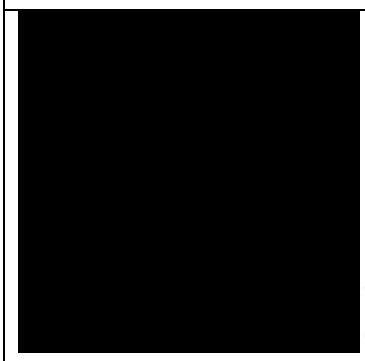
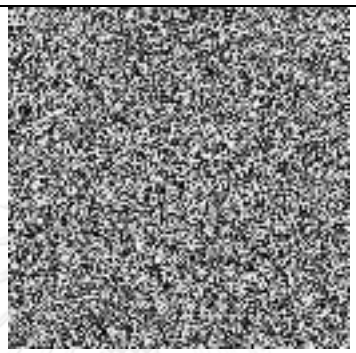
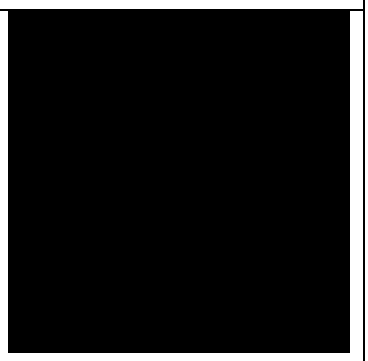
high-dimension chaotic system. Optics communications, August 2011. 284: p. 3895-3903.

34. G. Hanchinamani, L.K., *A Novel Approach for Image Encryption based on Parametric Mixing Chaotic System.* International Journal of Computer Applications, 2014. 96.

ภาคผนวก

ภาคผนวก ก
ผลการทดลองเพิ่มเติม

ตารางที่ ก-1 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพสีดำ)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-1 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

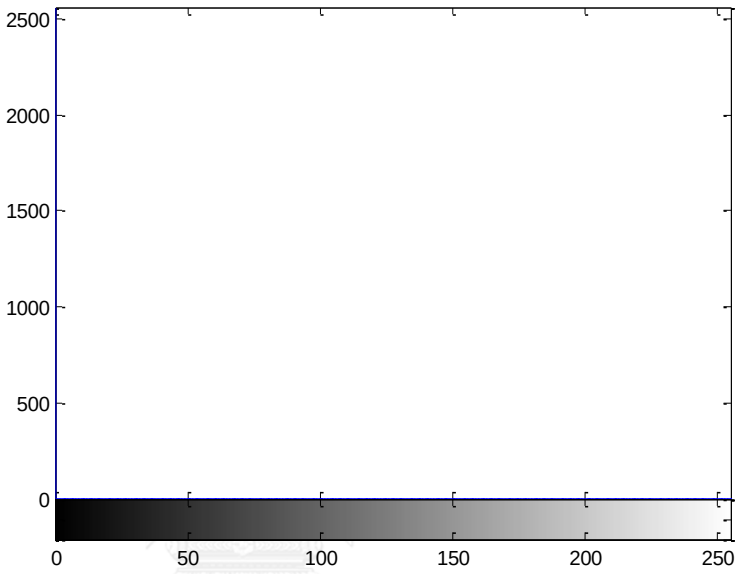
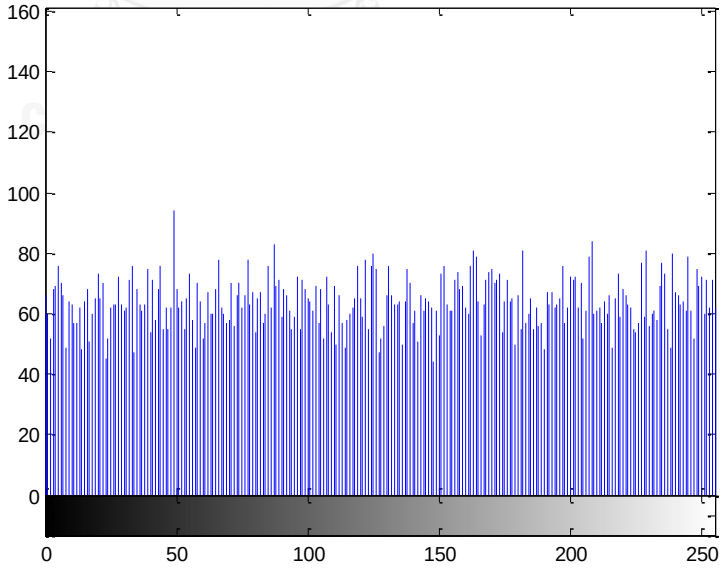
ตารางที่ ก-2 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส

Entropy of Plain Image	Entropy of Encrypted Image
0	7.988215

จากตารางที่ ก-2 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

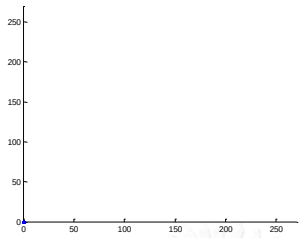
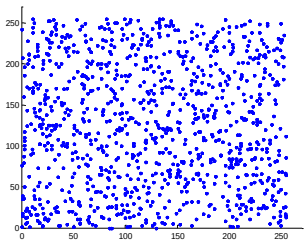
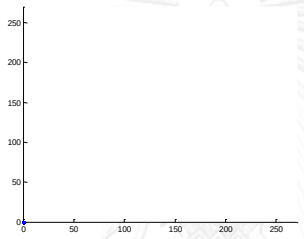
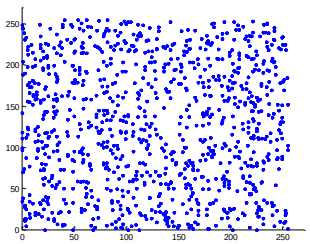
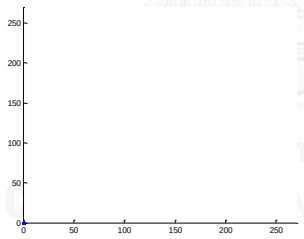
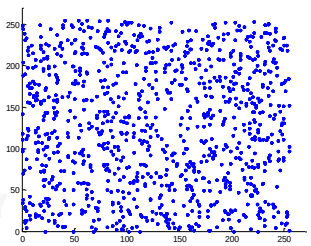
ตารางที่ ก-3 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพสีดำ)

	Gray Channel
Histogram of Original Image	
Histogram of Encrypted Image	

ตารางที่ ก-4 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพสีดำ)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	Gray	1	0.0035
	-	-	-
	-	-	-
Vertical	Gray	1	0.0038
	-	-	-
	-	-	-
Diagonal	Gray	1	-0.0087
	-	-	-
	-	-	-

ตารางที่ ก-5 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพสีดำ)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-6 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพสีดำ)

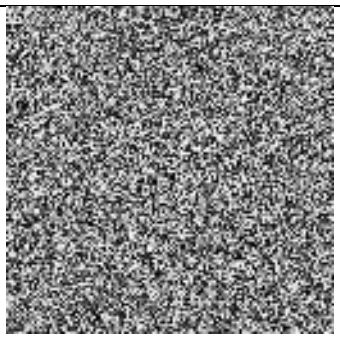
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-7 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพสีดำ)

NPCR	99.69%
UACI	33.31%

ตารางที่ ก-8 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพสีขาว)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-8 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

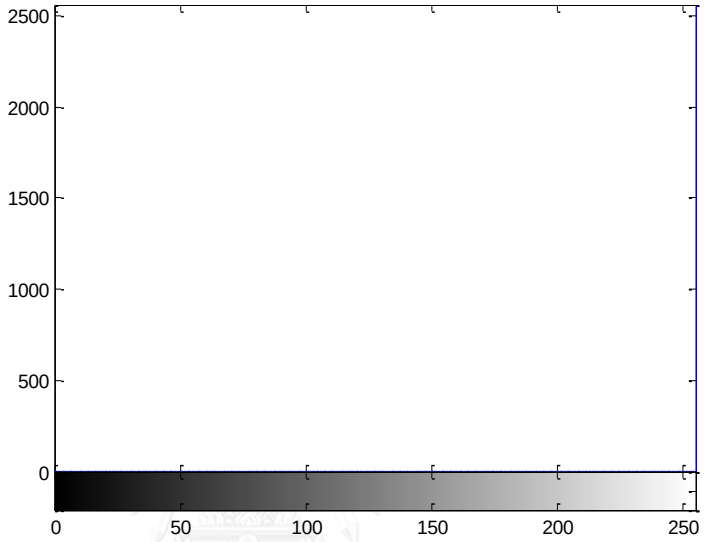
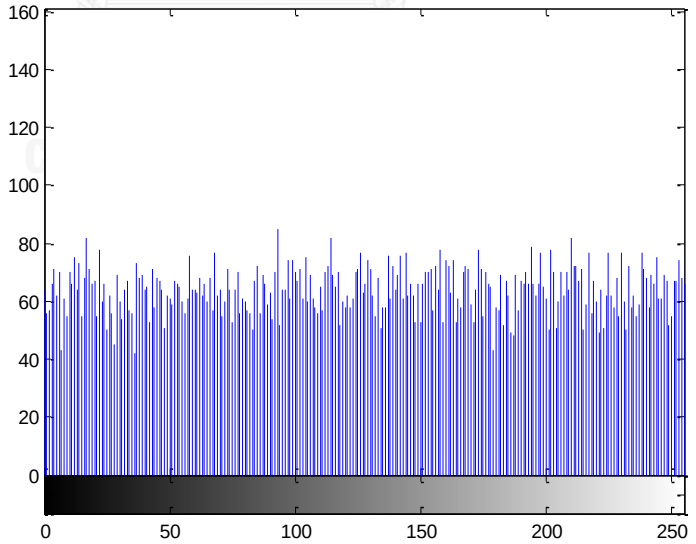
ตารางที่ ก-9 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพสีขาว)

Entropy of Plain Image	Entropy of Encrypted Image
0	7.988209

จากตารางที่ ก-9 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

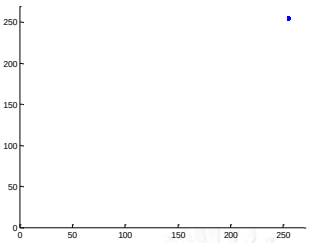
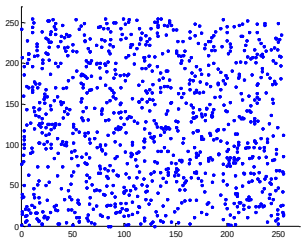
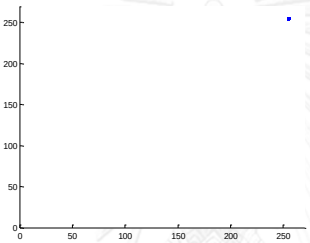
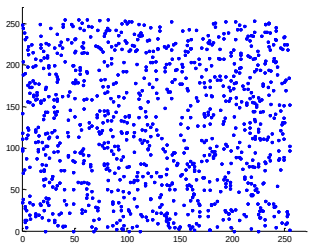
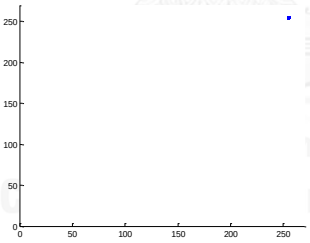
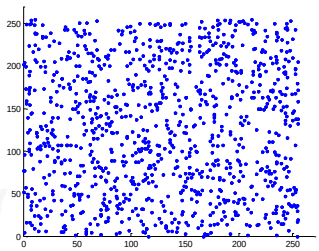
ตารางที่ ก-10 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพสีขาว)

	Gray Channel
Histogram of Original Image	
Histogram of Encrypted Image	

ตารางที่ ก-11 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพสีขาว)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	gray	1	0.0033
	-	-	-
	-	-	-
Vertical	gray	1	0.0040
	-	-	-
	-	-	-
Diagonal	gray	1	-0.0084
	-	-	-
	-	-	-

ตารางที่ ก-12 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพสีขาว)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-13 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพสีขาว)

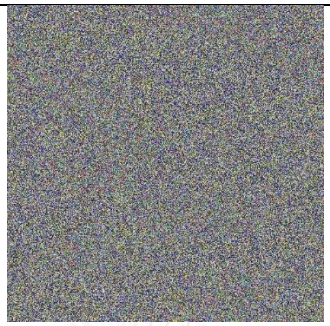
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-14 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพสีขาว)

NPCR	99.86%
UACI	33.32%

ตารางที่ ก-15 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Fruits)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-15 พบว่าภาพที่ถูกถอดรหัสมีความเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

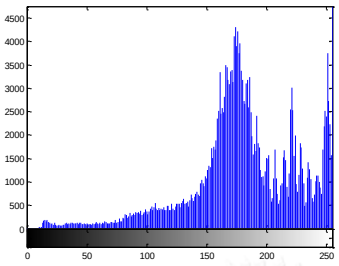
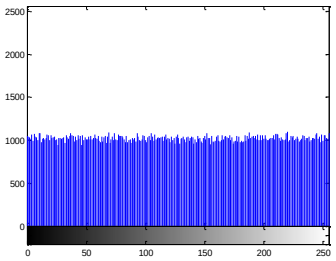
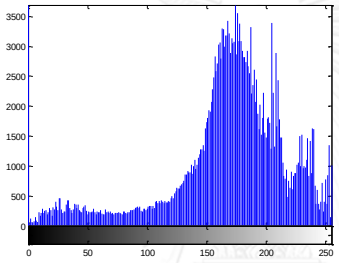
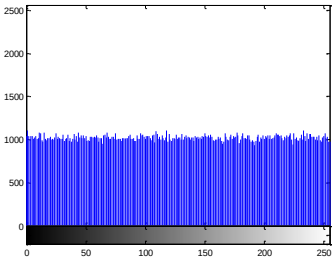
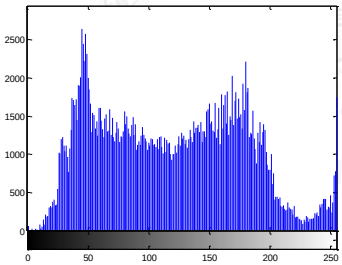
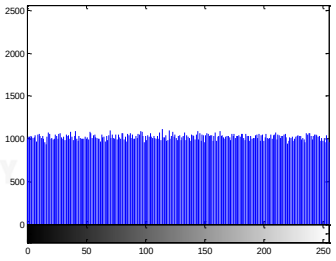
ตารางที่ ก-16 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Fruits)

Entropy of Plain Image	Entropy of Encrypted Image
7.631880	7.999782

จากตารางที่ ก-16 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

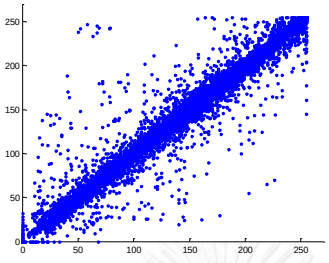
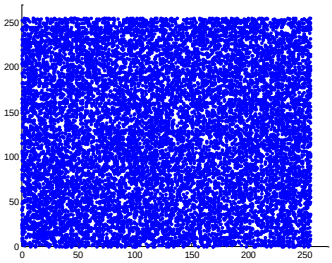
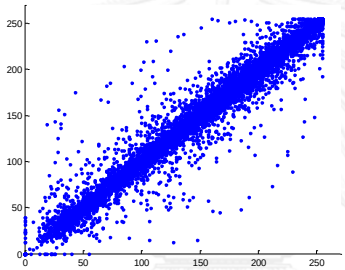
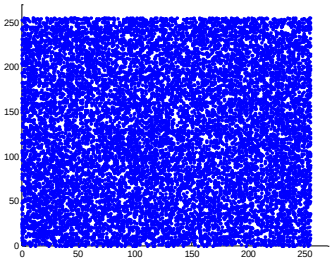
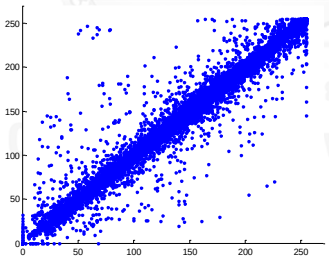
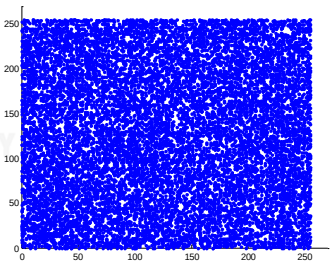
ตารางที่ ก-17 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Fruits)

Channel	Histogram of Original Image	Histogram of Encrypted Image
Red		
Green		
Blue		

ตารางที่ ก-18 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Fruits)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	R	0.9726	0.0029
	G	0.9774	0.0054
	B	0.9803	-6.5591×10^{-5}
Vertical	R	0.9728	4.1892×10^{-5}
	G	0.9778	-0.0016
	B	0.9807	0.0022
Diagonal	R	0.9523	-9.2030×10^{-5}
	G	0.9620	-0.0028
	B	0.9657	0.0011

ตารางที่ ก-19 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Fruits)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-20 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพ Fruits)

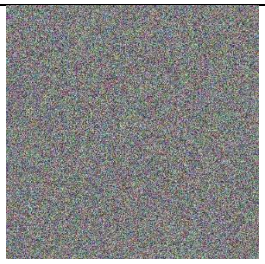
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-21 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Fruits)

NPCR	99.63%
UACI	33.12%

ตารางที่ ก-22 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Peppers)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-22 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

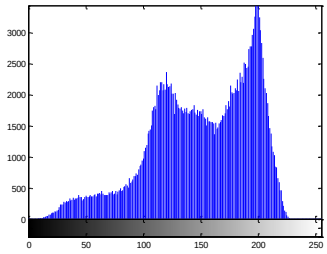
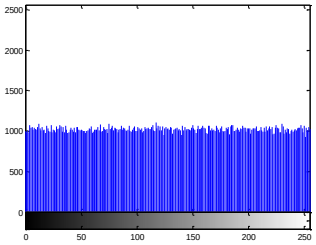
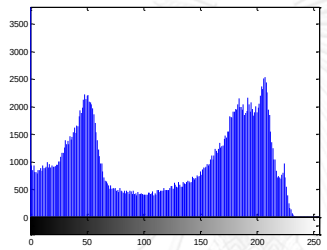
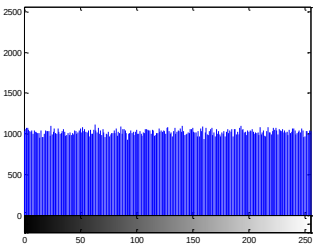
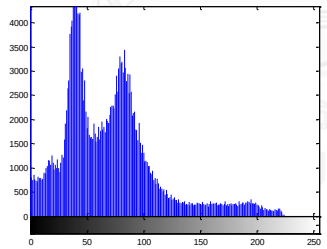
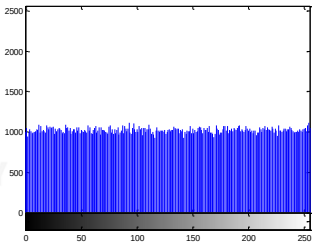
ตารางที่ ก-23 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Peppers)

Entropy of Plain Image	Entropy of Encrypted Image
7.669825	7.999756

จากตารางที่ ก-23 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

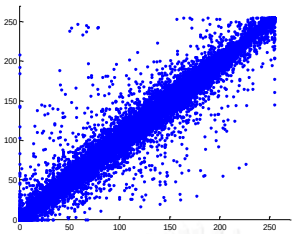
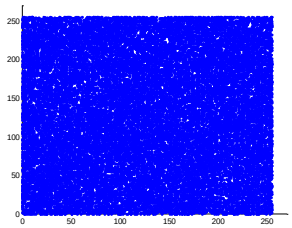
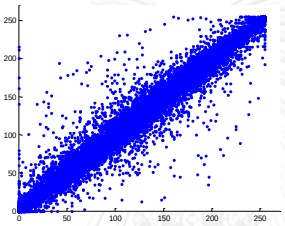
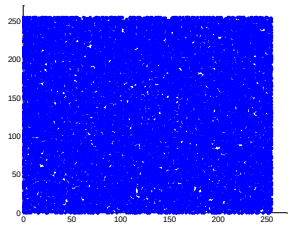
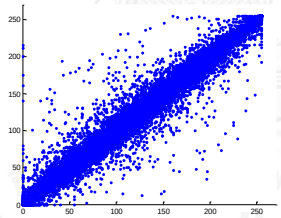
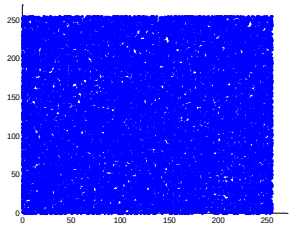
ตารางที่ ก-24 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Peppers)

Channel	Histogram of Original Image	Histogram of Encrypted Image
Red		
Green		
Blue		

ตารางที่ ก-25 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ(ภาพ Peppers)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	R	0.9635	-3.7457e-04
	G	0.9811	-2.7556e-04
	B	0.9665	0.0055
Vertical	R	0.9663	-0.0024
	G	0.9818	-3.5895e-04
	B	0.9664	0.0012
Diagonal	R	0.9564	-0.0035
	G	0.9687	-0.0012
	B	0.9478	0.0020

ตารางที่ ก-26 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Peppers)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-27 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพ Peppers)

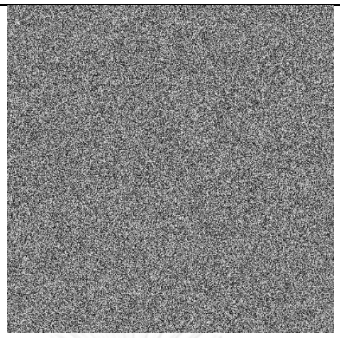
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-28 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Peppers)

NPCR	99.89%
UACI	33.23%

ตารางที่ ก-29 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Barbara)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-29 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

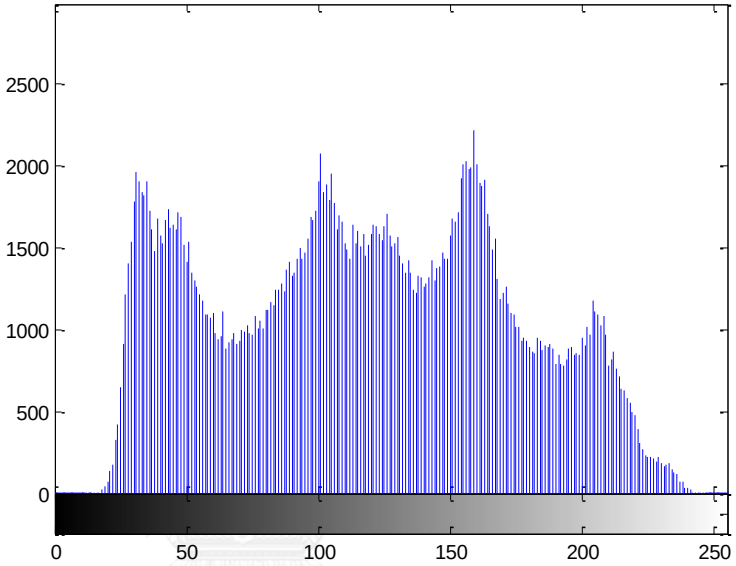
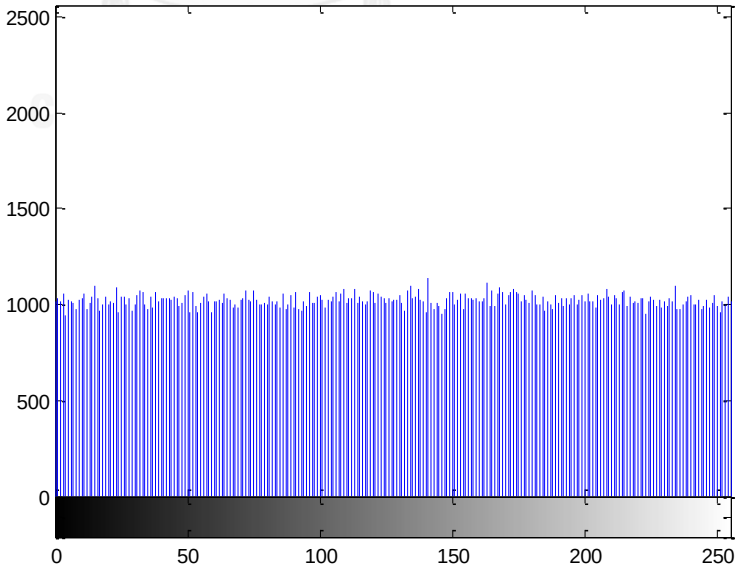
ตารางที่ ก-30 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Barbara)

Entropy of Plain Image	Entropy of Encrypted Image
7.632119	7.999275

จากตารางที่ ก-30 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

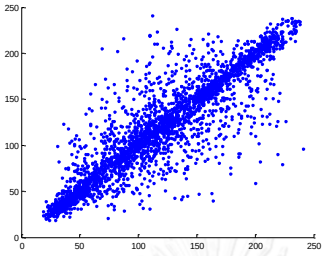
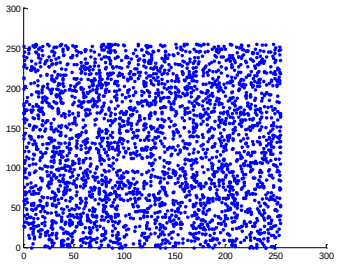
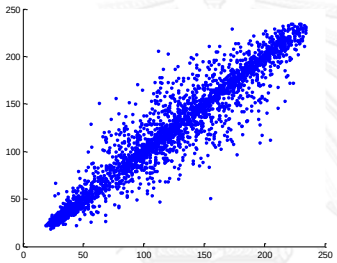
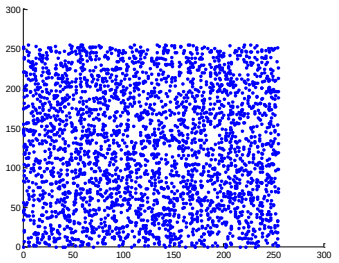
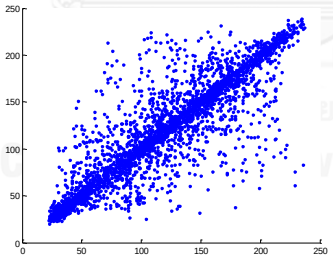
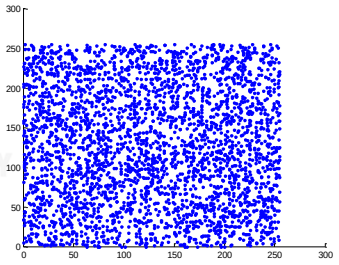
ตารางที่ ก-31 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Barbara)

	Gray Channel
Histogram of Original Image	
Histogram of Encrypted Image	

ตารางที่ ก-32 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Barbara)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	Gray	0.8954	4.0707×10^{-5}
	-	-	-
	-	-	-
Vertical	Gray	0.9589	0.0025
	-	-	-
	-	-	-
Diagonal	Gray	0.8830	-1.9577×10^{-5}
	-	-	-
	-	-	-

ตารางที่ ก-33 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Barbara)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-34 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพ Barbara)

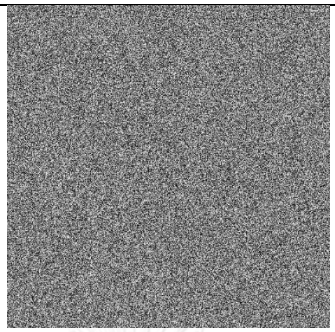
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-35 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Barbara)

NPCR	99.56%
UACI	33.35%

ตารางที่ ก-36 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Goldhill)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-36 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

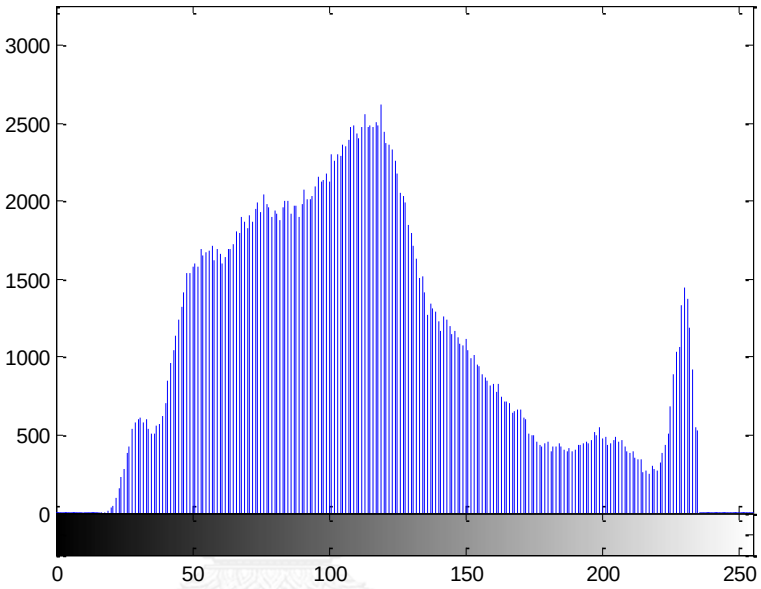
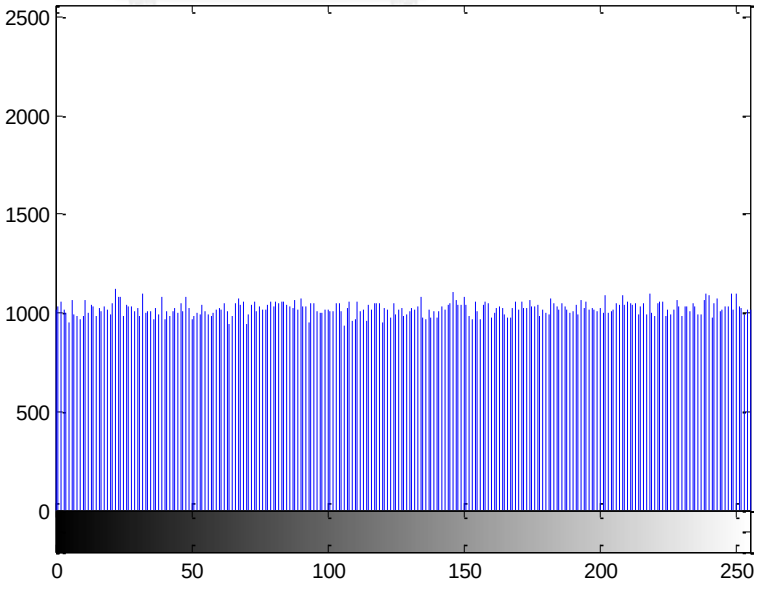
ตารางที่ ก-37 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Goldhill)

Entropy of Plain Image	Entropy of Encrypted Image
7.477819	7.999231

จากตารางที่ ก-37 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

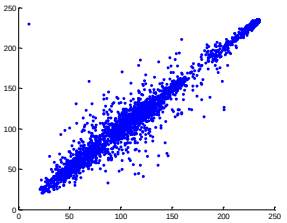
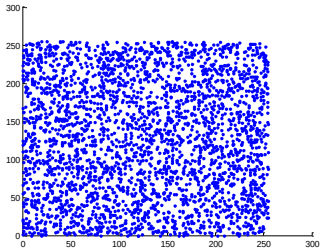
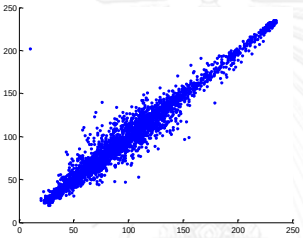
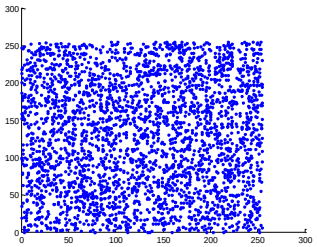
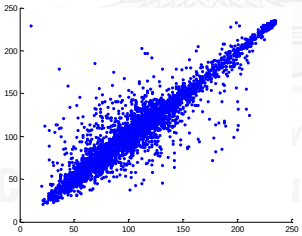
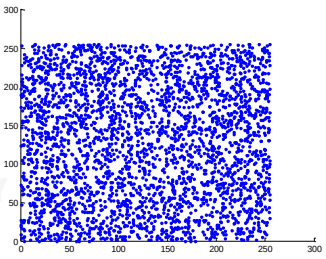
ตารางที่ ก-38 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Goldhill)

	Gray Channel
Histogram of Original Image	
Histogram of Encrypted Image	

ตารางที่ ก-39 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Goldhill)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	Gray	0.9704	-3.5968$\times 10^{-5}$
	-	-	-
	-	-	-
Vertical	Gray	0.9744	-0.0019
	-	-	-
	-	-	-
Diagonal	Gray	0.9522	-0.0036
	-	-	-
	-	-	-

ตารางที่ ก-40 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Goldhill)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-41 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพ Goldhill)

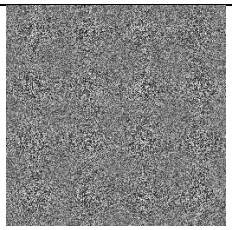
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-42 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Goldhill)

NPCR	99.41%
UACI	33.15%

ตารางที่ ก-43 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Boat)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-43 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

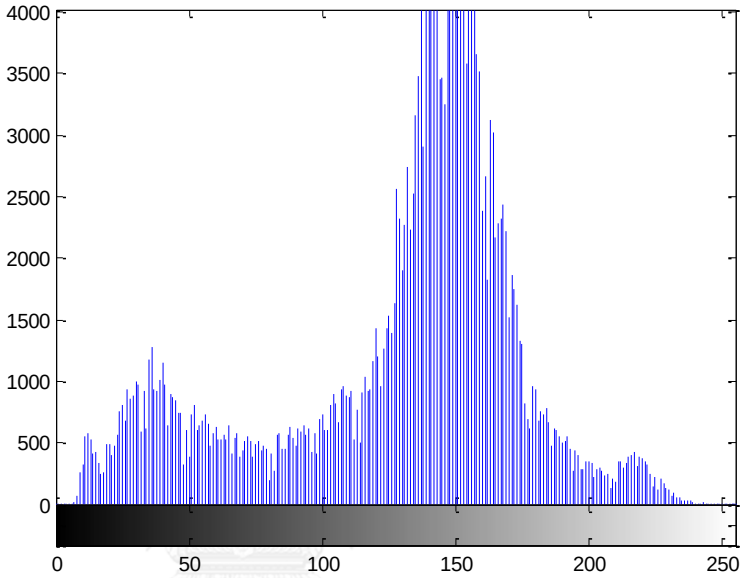
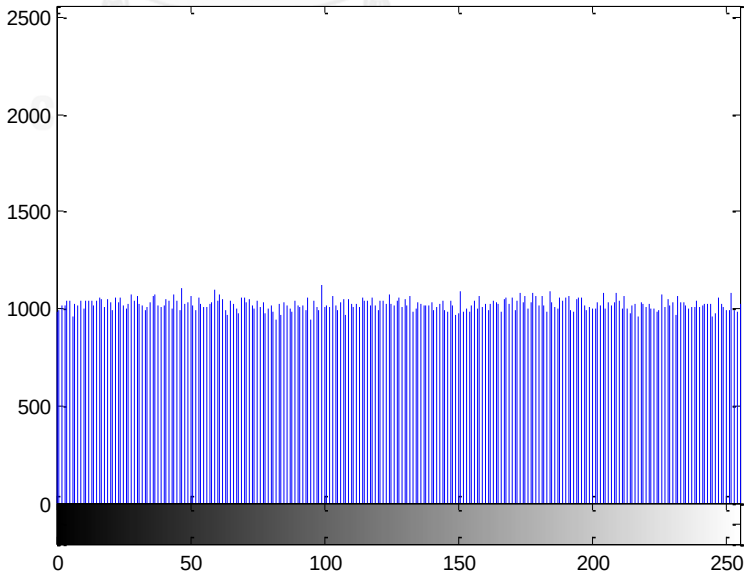
ตารางที่ ก-44 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Boat)

Entropy of Plain Image	Entropy of Encrypted Image
7.191370	7.999377

จากตารางที่ ก-44 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

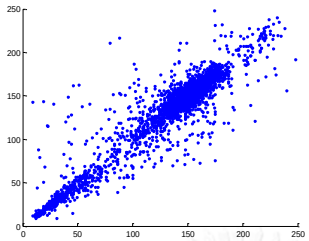
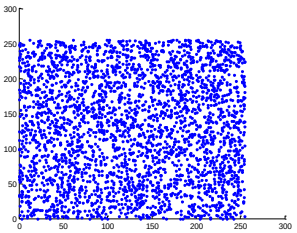
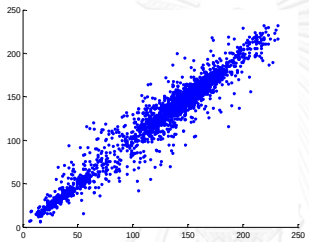
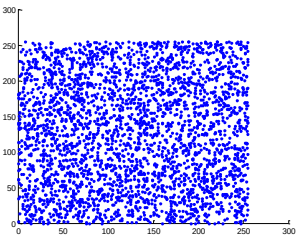
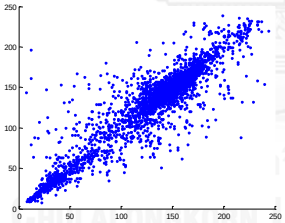
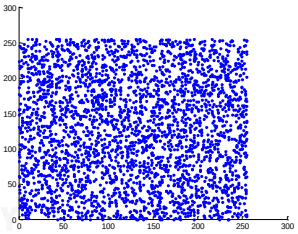
ตารางที่ ก-45 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Boat)

	Gray Channel
Histogram of Original Image	
Histogram of Encrypted Image	

ตารางที่ ก-46 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Boat)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	Gray	0.9381	-5.4266×10^{-5}
	-	-	-
	-	-	-
Vertical	Gray	0.9713	0.0040
	-	-	-
	-	-	-
Diagonal	Gray	0.9222	3.2017×10^{-5}
	-	-	-
	-	-	-

ตารางที่ ก-47 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Boat)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
diagonally		

C. Key Space Analysis

ตารางที่ ก-48 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพ Boat)

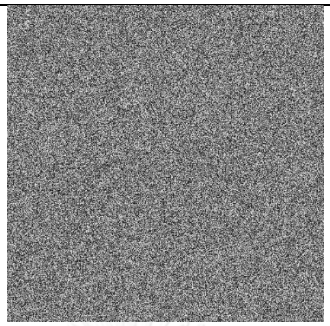
	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-49 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Boat)

NPCR	99.25%
UACI	33.54%

ตารางที่ ก-50 ตารางแสดงผลลัพธ์ ภาพต้นฉบับ ภาพที่ถูกเข้ารหัส และภาพที่ถูกถอดรหัส (ภาพ Zelda)

ภาพต้นฉบับ (Plain Image)	ภาพที่ถูกเข้ารหัส (Encrypted Image)	ภาพที่ถูกถอดรหัส (Decrypted Image)
		

จากตารางที่ ก-50 พบว่าภาพที่ถูกถอดรหัสเหมือนกันทุกประการกับภาพต้นฉบับ

A. Entropy Analysis

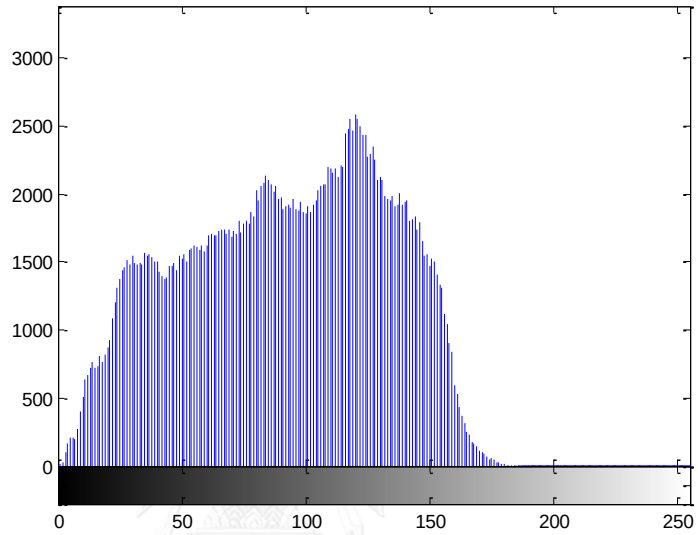
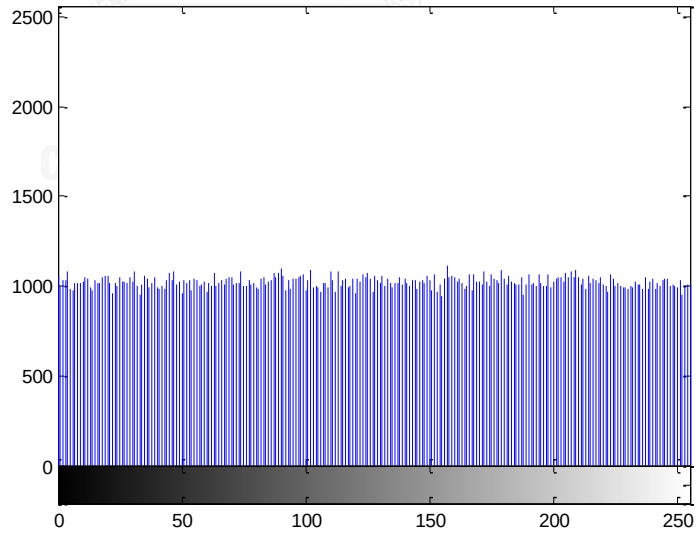
ตารางที่ ก-51 ตารางแสดงค่าเอนโทรปีของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Zelda)

Entropy of Plain Image	Entropy of Encrypted Image
7.266801	7.999352

จากตารางที่ ก-51 พบว่าค่าเอนโทรปีของภาพที่ถูกเข้ารหัสมากกว่าค่าเอนโทรปีของภาพต้นฉบับ และมีค่าใกล้เคียงค่าเอนโทรปีมากสุดทางทฤษฎี นั่นคือ 8

B. Statistical Analysis

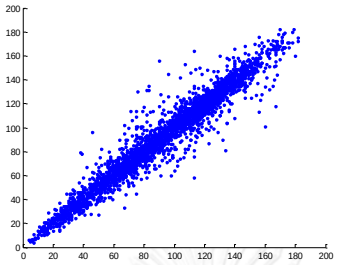
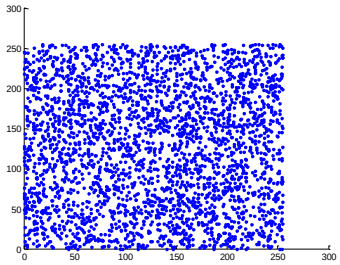
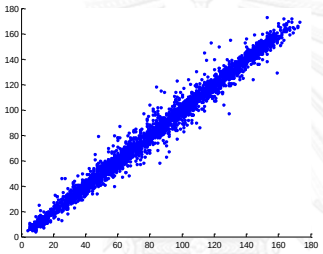
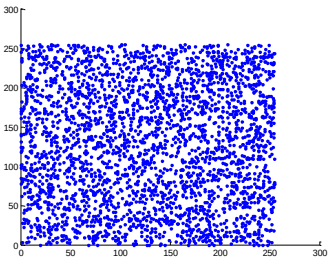
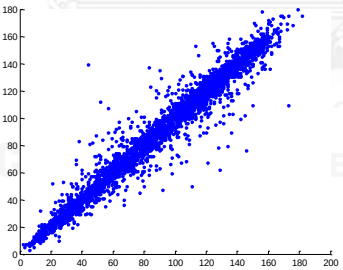
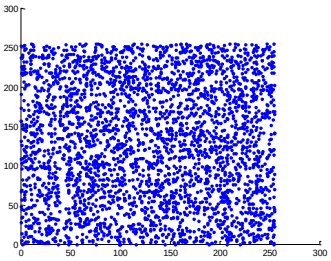
ตารางที่ ก-52 ตารางแสดงภาพฮิสโทแกรมของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีต่างๆ (ภาพ Zelda)

	Gray Channel
Histogram of Original Image	
Histogram of Encrypted Image	

ตารางที่ ก-53 ตารางแสดงค่าสหสัมพันธ์ของภาพต้นฉบับและภาพที่ถูกเข้ารหัสในช่องสีและทิศทางต่างๆ (ภาพ Zelda)

Direction	channel	Correlation Coefficients of	
		Original Image	Encrypted Image
Horizontal	Gray	0.9827	0.0043
	-	-	-
	-	-	-
Vertical	Gray	0.9916	-2.1517×10^{-5}
	-	-	-
	-	-	-
Diagonal	Gray	0.9780	8.5849×10^{-5}
	-	-	-
	-	-	-

ตารางที่ ก-54 ตารางแสดงกราฟระหว่างค่าของจุดภาพที่อยู่ติดกันในทิศทางต่างๆเปรียบเทียบระหว่างของภาพต้นฉบับและภาพที่ถูกเข้ารหัส (ภาพ Zelda)

Adjacent pixels	Plots of original image	Plots of Encrypted Image
Horizontally		
Vertically		
Diagonally		

C. Key Space Analysis

ตารางที่ ก-55 ตารางแสดงขนาดของกุญแจของวิธีการที่นำเสนอกับ DES Standard (ภาพ Zelda)

	DES standard	Our proposed method
Key space	128 บิต	704 บิต

D. Diffusion Analysis

ตารางที่ ก-56 ตารางแสดงค่า NPCR และค่า UACI ของภาพที่ถูกเข้ารหัส (ภาพ Zelda)

NPCR	99.63%
UACI	33.42%

ประวัติผู้เขียนวิทยานิพนธ์

วิภาวดี อวยพร เกิดวันที่ 15 กรกฎาคม พ.ศ. 2531 มีภูมิลำเนาอยู่ที่จังหวัดนครปฐม เป็นบุตรสาวของนาวาอากาศตรีสุพจน์ อวยพร และนางวิจิตรา อวยพร สำเร็จการศึกษาระดับมัธยมศึกษาตอนปลายที่โรงเรียนมหิดลวิทยานุสรณ์ จ.นครปฐม จากนั้นได้รับทุนรัฐบาลไปศึกษาต่อ ณ ประเทศสหรัฐอเมริกา และได้สำเร็จการศึกษาระดับปริญญาบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ จาก Brown University ประเทศสหรัฐอเมริกา ในปี พ.ศ. 2554 และในภาคปลายปีการศึกษา 2555 ได้เข้าศึกษาในระดับปริญญามหาบัณฑิตที่จุฬาลงกรณ์มหาวิทยาลัย คณะวิศวกรรมศาสตร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ สาขาวิศวกรรมคอมพิวเตอร์ มีความสนใจทางด้านการประมวลผลภาพ วิทยาการเข้ารหัสลับ และความมั่นคงของข้อมูล