บทที่ 5
บทสรุปและข้อเสนอแนะ

ในบทนี้กล่าวถึงการสรุปผลการศึกษาที่ได้โดยการเปรียบเทียบประสิทธิภาพของการทำงานร่วมกันระหว่างการบีบอัดข้อมูลและการเข้ารหัสลับ เนื้อหาประกอบด้วยสรุปผลการศึกษา ปัญหาและข้อจำกัด และข้อเสนอแนะ

5.1. สรุปผลการศึกษา

จากการทดลองนำเข้าข้อมูลไฟล์ตามการทดลองที่กำหนดไว้ 4 รอบ โดยแบ่งประเภทของไฟล์ออกเป็น 2 แบบคือไฟล์เอกสาร และไฟล์รูปภาพ เมื่อทำการทดลองแล้วพบว่า มีความแตกต่างกันในด้านของการตอบสนองต่อการบีบอัดข้อมูล คือไฟล์เอกสารจะสามารถถูกบีบอัดได้มากกว่าไฟล์รูปภาพ โดยพิจารณาจากค่าขนาดหลังทำการบีบอัด ค่าอัตราส่วนในการบีบอัด และค่าประสิทธิภาพในการบีบอัด ที่เป็นไปในทิศทางเดียวกัน

เหตุที่เป็นเช่นนี้เนื่องจากว่า การบีบอัดข้อมูลเป็นเรื่องของการลดความซ้ำซ้อนของข้อมูล โดยปกติไฟล์ในระบบคอมพิวเตอร์จะมีความซ้ำซ้อนเกิดขึ้นได้เสมอ โดยไฟล์แต่ละชนิดก็จะมีอัตราความซ้ำซ้อนแตกต่างกันออกไป เช่น ไฟล์เอกสารจะเป็นไฟล์ที่มีความซ้ำซ้อนมาก เนื่องจากเวลาผู้ใช้งานพิมพ์ข้อความลงไป จะมีการพิมพ์คำที่ซ้ำกันเกิดขึ้นเสมอ เช่นในภาษาอังกฤษก็จะพบคำ the, a, is, am, are, I, you ได้บ่อย ทำให้เมื่อนำไฟล์ที่เป็นเอกสารไปผ่านขั้นตอนการบีบอัด จะทำให้ลดขนาดลงไปได้มาก ซึ่งต่างจากไฟล์ประเภทมัลติมีเดีย ซึ่งมีกระบวนการในการเก็บข้อมูลที่เฉพาะตัวแตกต่างกันออกไป และถึงแม้จะมีโอกาสในการเก็บข้อมูลที่ซ้ำซ้อนกันได้ แต่ก็น้อยกว่าไฟล์เอกสาร ทำให้เมื่อนำไฟล์มัลติมีเดียไปผ่านกระบวนการบีบอัดข้อมูล จะทำให้ไม่สามารถบีบอัดได้มากนัก ซึ่งบางครั้งอาจทำให้ไฟล์ประเภทนี้หลังจากถูกบีบอัดแล้วกลับมีขนาดที่เพิ่มขึ้นมากกว่าเดิม ก็เพราะว่าในการบีบอัดข้อมูล ก็จำเป็นที่จะต้องสร้าง header หรือข้อมูลอื่นๆ เพิ่มเข้าไปในไฟล์ด้วย

จากการทดลองกับไฟล์ตัวอย่างทั้ง 4 ไฟล์และนำค่าที่ได้มาจัดอันดับเพื่อให้น้ำหนักคะแนนตามเกณฑ์แต่ละด้านแล้ว สามารถสรุปคะแนนได้ตามตาราง ดังนี้

Process	Time	Size	Compression Ratio	Throughput	Brute Force Time
Huffman & DES	16	20	35	15	7
Huffman & 3DES	5	20	35	5	16
Huffman & AES	25	20	35	25	24
Huffman & Blowfish	29	20	35	29	29
Huffman & RC4	37	20	35	37	40
Deflate & DES	20	40	40	21	5
Deflate & 3DES	7	40	40	7	12
Deflate & AES	31	40	40	30	20
Deflate & Blowfish	24	40	40	24	31
Deflate & RC4	27	40	40	27	40

หมายเหตุ: เกณฑ์แต่ละด้านมีคะแนนเต็ม 40 คะแนน

ตาราง 5.1 สรุปคะแนนตามตามเกณฑ์แต่ละด้าน

จากการสรุปผลลัพธ์ตามกำหนดเกณฑ์ของอัลกอริทึมในแต่ละแบบพบว่า ในด้านของเวลาในการดำเนินการ (Time) และด้านประสิทธิภาพในการบีบอัด (Throughput) นั้น Huffman & RC4 ทำเวลาเป็นอันดับ 1 และอันดับสุดท้ายคือ Huffman & 3DES ตัวแปรสำคัญมาจากอัลกอริทึมที่ใช้ในการเข้ารหัสลับ โดย RC4 เป็นอัลกอริทึมแบบ stream cipher ซึ่งมีความเร็วสูง และคีย์ที่ใช้มีจำนวนมากทำให้เกิดความยืดหยุ่น ส่วนอัลกอริทึม 3DES เป็นอัลกอริทึมที่มีเวลาดำเนินการช้าเนื่องจากต้องทำงานตามกระบวนการแบบเดียวกันกับ DES ถึง 3 รอบ แต่แม้ว่าความเร็วในการเข้ารหัสจะช้ากว่า DES 3 เท่า แต่ก็ได้มาซึ่งความปลอดภัยที่เพิ่มขึ้นเป็นพันล้านเท่า

ในด้านของขนาดผลลัพธ์ (Size) และอัตราส่วนในการบีบอัด (Compression Ratio) ขึ้นอยู่กับอัลกอริทึมที่ใช้ในการบีบอัดเป็นหลัก ซึ่งจากผลที่ได้แสดงให้เห็นว่า Deflate สามารถบีบอัดข้อมูลได้ดีกว่า Huffman เนื่องมาจากว่า Deflate เป็นอัลกอริทึมที่พัฒนามาจากหลักการของ Huffman coding คือใช้หลักการแทนค่าสัญลักษณ์ตัวอักษรแบบโครงสร้างต้นไม้แล้วทำการสร้างตารางระยะทาง (distance code) เพื่อเก็บระยะทางที่จะเข้าไปแทนที่สัญลักษณ์ที่ระบุไว้ในข้อมูล จึงทำให้เข้าถึงข้อมูลได้ดีกว่า Huffman coding ที่ใช้การเก็บค่าสัญลักษณ์แทนตัวอักษรแบบคงที่ (static)

ผลสรุปในด้านของความปลอดภัย (Brute Force Time) นั้น ขึ้นอยู่กับอัลกอริทึมที่ใช้ในการเข้ารหัสลับเป็นหลัก โดยอัลกอริทึมที่ใช้ระยะเวลาในการถอดรหัสด้วยวิธี brute force attack ได้เร็วที่สุดคือ DES และจะใช้ระยะเวลานานที่สุดเมื่อนำไปใช้กับอัลกอริทึม RC4 เนื่องจากว่า การคำนวณเวลาในการถอดรหัสแบบ brute force attack ขึ้นอยู่กับตัวแปรสองตัวเป็นหลัก คือ ขนาดของ key ที่ใช้ในการเข้ารหัส และความสามารถในการประมวลผลของ CPU

ในการศึกษาครั้งนี้ได้ใช้อัลกอริทึมที่มีการเข้ารหัสลับแบบกุญแจสมมาตร ซึ่ง DES เป็นอัลกอริทึมที่มีการใช้ขนาดกุญแจน้อยที่สุดคือ 56 bits และ RC4 เป็นอัลกอริทึมที่ใช้ขนาดของกุญแจในการเข้ารหัสมากที่สุดคือ 2048 bits ดังนั้นค่าผลลัพธ์ที่ได้จึงทำให้ RC4 เป็นอัลกอริทึมที่ใช้เวลาในการถอดรหัสแบบ brute force นานที่สุดนั่นเอง

5.2. ปัญหาและข้อจำกัด

จากการพัฒนาโปรแกรมในการศึกษาครั้งนี้ ผู้ศึกษาได้พบปัญหาและข้อจำกัดที่เกิดขึ้น คือ

(1) การหาค่า MIPS ที่ใช้เป็นตัววัดประสิทธิภาพการทำงานของ CPU นั้น เป็นค่าที่ไม่เสถียร เนื่องจากค่า MIPS นั้นขึ้นอยู่กับสภาวะแวดล้อมการทำงานของคอมพิวเตอร์ในหลายๆ ส่วน หากในขณะที่ทำการทดลอง หรือขณะที่กำลังทำการหาค่า MIPS นั้น ผู้ใช้งานได้เปิดโปรแกรมใช้งานประเภทอื่นๆ ควบคู่ไปด้วยหลายอย่าง จะทำให้ค่า MIPS ที่ได้ลดลง นั่นก็คือค่าที่ได้ไม่สามารถบอกได้แน่นอนว่าเป็นประสิทธิภาพของเครื่องสูงสุดหรือไม่ ซึ่งจะส่งผลต่อการคำนวณหา brute force time ด้วยเช่นกัน ดังนั้น หากจะเข้าสู่กระบวนการทดลองเพื่อวัดประสิทธิภาพการทำงาน ก็ควรจะมีข้อกำหนดสภาวะแวดล้อมของระบบให้เหมาะสมด้วย เช่น ปิดโปรแกรมอื่นๆ นอกเหนือจากโปรแกรมคำนวณให้หมดเป็นต้น

(2) การใช้งานบางฟังก์ชั่นของ Microsoft Visual Basic 2008 ไม่รองรับระบบปฏิบัติการ Windows ในเวอร์ชั่นที่ต่ำกว่า Vista ได้ ซึ่งอาจจะทำให้โปรแกรมทำงานได้ไม่สมบูรณ์ โดยผู้ใช้ที่จำเป็นต้องใช้งานโปรแกรมบนระบบปฏิบัติการอื่น อาจจะต้องทำการติดตั้งโปรแกรมส่วนเพิ่มเติมเช่น .NET Framework 3.5 เป็นต้น

(3) ในการศึกษาครั้งนี้ ได้ใช้การทดลองกับไฟล์ตัวอย่างเพียงสองประเภทเท่านั้น ถึงแม้ว่าโปรแกรมจะสามารถทำงานร่วมกับไฟล์ทุกประเภทได้ แต่ยังไม่สามารถสรุปได้ว่าไฟล์ประเภทอื่นจะมีผลเหมือนหรือแตกต่างจากไฟล์ตัวอย่างที่ใช้

ทดลองอย่างไร ซึ่งในการศึกษาครั้งต่อไป ควรใช้ไฟล์ตัวอย่างในการทดลองที่หลากหลายเพิ่มขึ้น

5.3. ข้อเสนอแนะ

การค้นคว้าอิสระในครั้งนี้ ผู้ศึกษาได้มีข้อเสนอแนะเพื่อเป็นแนวทางให้ผู้ที่สนใจศึกษาหรือต้องการนำไปพัฒนาต่อ ดังนี้

(1) เครื่องคอมพิวเตอร์ที่ใช้พัฒนาโปรแกรม หากต้องการทำงานด้วยฟังก์ชั่นที่ครบถ้วน ควรติดตั้งระบบปฏิบัติการ Windows 7 และใช้ควบคู่กับ .NET Framework 4.0 จึงจะทำให้มีฟังก์ชั่นที่สามารถใช้ได้เป็นปัจจุบันที่สุด

(2) ในการวัดประสิทธิภาพทางด้านความปลอดภัย หากจะใช้ค่า MIPS ควรเลือกใช้ค่าที่มาจากฐานข้อมูลที่ได้จากโรงงานผลิต เพราะนั่นเป็นค่าที่ตายตัว ไม่ขึ้นอยู่กับปัจจัยแวดล้อมอื่นๆ หรือเลือกใช้ค่าที่ไม่มีการแกว่งตัวตามสภาวะแวดล้อมการทำงานภายในระบบ

(3) หากต้องการนำไปพัฒนาต่อยอดความรู้ ในการเลือกอัลกอริทึมมาประกอบการใช้งาน ผู้พัฒนาโปรแกรมสามารถที่จะเลือกใช้อัลกอริทึมที่มีการเข้ารหัสด้วยกุญแจแบบอสมมาตรเข้ามาด้วยเพื่อให้รูปแบบการทำงานที่หลากหลายมากขึ้น โดยอาจจะแบ่งส่วนให้ผู้ใช้สามารถเลือกได้ว่า สะดวกในการเข้ารหัสแบบใด เพราะในบางโอกาสที่ผู้ใช้อาจจะไม่สะดวกในการเข้ารหัสแบบกุญแจเดี่ยว (Secret Key) โปรแกรมก็ยังมีช่องทางให้ผู้ใช้ได้เลือกเข้ารหัสแบบกุญแจสาธารณะ (Public Key) ตามหลักของการเข้ารหัสด้วยกุญแจแบบอสมมาตรได้

(4) จากผลการวิจัยพบว่า ในการบีบอัดข้อมูลและการเข้ารหัสลับเมื่อนำมาใช้งานร่วมกันแล้ว สามารถทำงานร่วมกันได้เป็นอย่างดี โดยโปรแกรมนี้เหมาะที่จะนำไปใช้งานกับไฟล์ประเภทเอกสาร เนื่องจากค่าคะแนนที่แสดงผลออกมาสามารถทำได้ดีกว่าไฟล์ประเภทรูปภาพ และเป็นโปรแกรมที่เหมาะกับลักษณะงานที่ต้องการส่งข้อมูลที่เป็นความลับผ่านไปทางช่องทางสาธารณะต่างๆ เช่น webboard, blog หรือแม้กระทั่ง e-mail เพราะสามารถส่งเป็นข้อความโพสลงในกระทู้หรือเขียนเป็นจดหมายส่งให้ผู้รับได้โดยไม่ต้องแนบไฟล์ใดๆ ไปด้วยเลย