

บทที่ 4

ผลการศึกษา



หลังจากที่ได้พัฒนาโปรแกรมจนสามารถนำมาใช้ในการนำเข้าข้อมูล และถอดกลับมาเป็นไฟล์ต้นฉบับได้แล้วนั้น ก็สามารถที่จะนำโปรแกรกดังกล่าว ไปใช้ทำการทดลองกับไฟล์ข้อมูลชนิดต่างๆ เพื่อเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัสต่อไป ซึ่งในบทนี้นำเสนอสองหัวข้อ ได้แก่ การออกแบบการทดลอง และเปรียบเทียบผลลัพธ์ตามกำหนดเกณฑ์

4.1 การออกแบบการทดลอง

ตามที่ได้มีการระบุไว้ตั้งแต่การออกแบบและพัฒนาโปรแกรมว่า โปรแกรมสามารถนำเข้าข้อมูลได้ทุกประเภท โดยมีข้อกำหนดคือต้องมีขนาดไม่เกิน 5 เมกกะไบต์ นั้น

หากเราจะนำมาทำการศึกษาเพื่อหาผลลัพธ์เพื่อวัดประสิทธิภาพ ก็ควรจะมีการกำหนดขอบเขตการทดลองเสียก่อน โดยการทดลองนี้จะทำเพื่อวัดค่าที่ได้จากการนำเข้าไฟล์ โดยใช้ไฟล์ที่มีประเภทแตกต่างกัน นำเข้ารหัสและบีบอัดด้วยอัลกอริทึมแต่ละแบบ และวัดค่าออกมาตามเกณฑ์ที่กำหนด จึงกำหนดขอบเขตการทดลอง ดังนี้

(1) ไฟล์นำเข้าข้อมูล

- แบ่งประเภทของข้อมูลที่จะนำเข้าเป็นสองประเภท ได้แก่
 - (ก) ไฟล์เอกสาร
 - (ข) ไฟล์ภาพ
- ทำการทดลองไฟล์ทั้งสองประเภทจำนวน 2 ครั้ง โดย
 - ครั้งที่ 1 ใช้ไฟล์ขนาด < 1 เมกกะไบต์
 - ครั้งที่ 2 ใช้ไฟล์ขนาด > 4 เมกกะไบต์ (แต่ไม่เกิน 5 เมกกะไบต์)

(2) อัลกอริทึมที่ใช้ในการบีบอัดและเข้ารหัสลับ จะจับคู่อัลกอริทึมที่ใช้ ดังนี้

- Huffman & DES
- Huffman & 3DES
- Huffman & AES
- Huffman & Blowfish
- Huffman & RC4

- Deflate & DES
- Deflate & 3DES
- Deflate & AES
- Deflate & Blowfish
- Deflate & RC4

(3) กำหนดเกณฑ์ (Criteria) ที่ใช้วัดประสิทธิภาพในด้านต่างๆ ได้แก่

- เวลาที่ใช้ในการดำเนินการ = Time (Millisecond)
- ขนาดของผลลัพธ์ = Size (bytes)
- อัตราส่วนในการบีบอัด = Compression Ratio (%)
- ประสิทธิภาพในการบีบอัด = Throughput (bytes/second)
- ประสิทธิภาพในด้านความปลอดภัย = Brute force time (years)

4.2. เปรียบเทียบผลลัพธ์ตามกำหนดเกณฑ์การทดลอง

- การทดลองครั้งที่ 1 ด้วยไฟล์ขนาด < 1 เมกกะไบต์

Original File: document1.doc

Original Size: 467,968 bytes

Process	Time (Millisecond)	Size (bytes)	Compression Ratio (%)	Throughput (bytes/second)	Brute force time (years)
Huffman & DES	1,009	122,784	73.76	342,105	1.15
Huffman & 3DES	6,410	122,784	73.76	53,851	6.90E+33
Huffman & AES	1,159	122,784	73.76	297,829	1.80E+60
Huffman & Blowfish	817	122,784	73.76	422,502	1.19E+118
Huffman & RC4	858	122,784	73.76	402,312	Infinity
Deflate & DES	778	122,760	73.77	443,712	1.25
Deflate & 3DES	6,297	122,760	73.77	54,821	6.24E+33
Deflate & AES	914	122,760	73.77	377,681	1.79E+60
Deflate & Blowfish	939	122,760	73.77	367,634	1.17E+118
Deflate & RC4	1,146	122,760	73.77	301,229	Infinity

ตาราง 4.1 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ document1.doc

Original File: photo1.jpg

Original Size: 399,389 bytes

Process	Time (Millisecond)	Size (bytes)	Compression Ratio (%)	Throughput (bytes/second)	Brute force time (years)
Huffman & DES	1,783	584,032	- 46.23	- 103,557	1.27
Huffman & 3DES	28,240	584,032	- 46.23	- 6,538	5.97E+33
Huffman & AES	1,705	584,032	- 46.23	- 108,295	2.09E+60
Huffman & Blowfish	1,595	584,032	- 46.23	- 115,764	1.21E+118
Huffman & RC4	1,552	584,032	- 46.23	- 118,971	Infinity
Deflate & DES	1,963	584,016	- 46.23	- 94,053	1.21
Deflate & 3DES	28,072	584,016	- 46.23	- 6,577	5.59E+33
Deflate & AES	1,548	584,016	- 46.23	- 119,268	1.87E+60
Deflate & Blowfish	1,704	584,016	- 46.23	- 108,349	1.23E+118
Deflate & RC4	1,553	584,016	- 46.23	- 118,884	Infinity

ตาราง 4.2 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ photo1.jpg

จากผลการทดลองครั้งที่ 1 ด้วยไฟล์ขนาด < 1 เมกกะไบต์ ที่แสดงให้เห็นค่าที่วัดได้ตามเกณฑ์ต่างๆ ตามตาราง 4.1 และตาราง 4.2 จะเห็นได้ว่า การทดลองที่ใช้ไฟล์ document1.doc มีการตอบสนองต่ออัลกอริทึมที่ใช้ในการบีบอัดมากกว่าไฟล์ photo1.jpg ดังจะเห็นได้จากค่า size, compression ratio และ throughput ในด้านของไฟล์ document1.doc แสดงถึงค่าที่บ่งบอกได้ว่าถูกบีบอัดได้มากกว่า

ส่วนในด้านอื่นๆ ไฟล์ทั้งสองประเภทแสดงค่าออกมาเป็นไปในทิศทางเดียวกัน คือ ค่าที่ได้จะขึ้นอยู่กับอัลกอริทึมที่ใช้เป็นหลัก

- การทดลองครั้งที่ 2 ด้วยไฟล์ขนาด > 4 เมกกะไบต์ (แต่ไม่เกิน 5 เมกกะไบต์)

Original File: document2.doc

Original Size: 4,528,640 bytes

Process	Time (Millisecond)	Size (bytes)	Compression Ratio (%)	Throughput (bytes/second)	Brute force time (years)
Huffman & DES	7,112	2,908,968	35.77	227,738	1.41
Huffman & 3DES	142,475	2,908,968	35.77	11,368	6.68E+33
Huffman & AES	6,648	2,908,968	35.77	243,632	1.87E+60
Huffman & Blowfish	6,889	2,908,968	35.77	235,110	1.12E+118
Huffman & RC4	6,410	2,908,968	35.77	252,679	Infinity
Deflate & DES	6,975	2,908,944	35.77	232,214	1.09
Deflate & 3DES	141,303	2,908,944	35.77	11,463	6.15E+33
Deflate & AES	6,831	2,908,944	35.77	237,110	1.84E+60
Deflate & Blowfish	6,776	2,908,944	35.77	239,034	1.17E+118
Deflate & RC4	6,547	2,908,944	35.77	247,395	Infinity

ตาราง 4.3 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ document2.doc

Original File: photo2.jpg

Original Size: 4,747,270 bytes

Process	Time (Millisecond)	Size (bytes)	Compression Ratio (%)	Throughput (bytes/second)	Brute force time (years)
Huffman & DES	16,086	7,245,760	- 52.63	- 115,321	1.52
Huffman & 3DES	355,773	7,245,760	- 52.63	- 7,023	6.70E+33
Huffman & AES	15,708	7,245,760	- 52.63	- 159,058	2.01E+60
Huffman & Blowfish	15,758	7,245,760	- 52.63	- 158,554	1.04E+118
Huffman & RC4	15,652	7,245,760	- 52.63	- 159,628	Infinity
Deflate & DES	16,258	7,245,744	- 52.63	- 153,677	1.2
Deflate & 3DES	395,348	7,245,744	- 52.63	- 6,320	6.27E+33
Deflate & AES	15,758	7,245,744	- 52.63	- 158,553	1.97E+60
Deflate & Blowfish	15,948	7,245,744	- 52.63	- 156,664	1.27E+118
Deflate & RC4	15,906	7,245,744	- 52.63	- 157,077	Infinity

ตาราง 4.4 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ photo2.jpg

ผลการทดลองครั้งที่ 2 ด้วยไฟล์ขนาด > 4 เมกกะไบต์ (แต่ไม่เกิน 5 เมกกะไบต์) ให้ผลลัพธ์ที่เหมือนกันกับการทดลองครั้งที่ 1 คือประเภทไฟล์เอกสาร (document2.doc) ยังตอบสนองต่อการบีบอัดข้อมูลได้มากกว่าไฟล์รูปภาพ (photo2.jpg) แม้ว่าขนาดของไฟล์ต้นฉบับจะมากขึ้น แต่เมื่อมองในภาพรวมแล้วยังคงให้ผลลัพธ์ที่เหมือนกันกับการทดลองครั้งที่ 1

4.3. สรุปผลลัพธ์ตามกำหนดเกณฑ์

หลังจากที่ได้ทำการทดลองกับไฟล์ตัวอย่างครบทั้ง 4 ไฟล์แล้ว สามารถนำข้อมูลสถิติที่ได้มาสรุปเป็นผลลัพธ์ด้วยการให้น้ำหนักคะแนนตามกำหนดเกณฑ์แต่ละด้าน ดังนี้

4.3.1 ด้านเวลาในการดำเนินการ

ให้น้ำหนักคะแนนของอัลกอริทึมที่ใช้เวลาน้อยที่สุด 10 คะแนน และให้คะแนนลดลงไปในแต่ละอันดับจนถึงอันดับที่ใช้เวลามากที่สุดให้ 1 คะแนน ดังนั้นจากผลการทดลองจึงสามารถให้คะแนนในแต่ละอัลกอริทึมได้ดังนี้

Process	Criteria: Time				Sum
	document1.doc	photo1.jpg	document2.doc	photo2.jpg	
Huffman & DES	5	4	3	4	16
Huffman & 3DES	1	1	1	2	5
Huffman & AES	3	5	8	9	25
Huffman & Blowfish	9	7	5	8	29
Huffman & RC4	8	9	10	10	37
Deflate & DES	10	3	4	3	20
Deflate & 3DES	2	2	2	1	7
Deflate & AES	7	10	6	8	31
Deflate & Blowfish	6	6	7	5	24
Deflate & RC4	4	8	9	6	27

ตาราง 4.5 สรุปคะแนนตามเกณฑ์ด้านเวลาในการดำเนินการ

จากตาราง 4.5 จะเห็นได้ว่า Huffman & RC4 ทำคะแนนด้านเวลาในการดำเนินการได้เป็นอันดับที่ 1 โดยมีอัลกอริทึม Deflate & AES ได้อันดับรองลงมา และอัลกอริทึมที่ได้คะแนนน้อยที่สุดคือ Huffman & 3DES

4.3.2 ด้านขนาดของผลลัพธ์

ให้นำหนักคะแนนของอัลกอริทึมที่มีขนาดของไฟล์เล็กที่สุด 10 คะแนน และให้คะแนนลดลงไปในแต่ละอันดับจนถึงอันดับที่มีขนาดไฟล์ใหญ่ที่สุดให้ 1 คะแนน ดังนั้นจากผลการทดลองจึงสามารถให้คะแนนในแต่ละอัลกอริทึมได้ดังนี้

Process	Criteria: Size				Sum
	document1.doc	photo1.jpg	document2.doc	photo2.jpg	
Huffman & DES	5	5	5	5	20
Huffman & 3DES	5	5	5	5	20
Huffman & AES	5	5	5	5	20
Huffman & Blowfish	5	5	5	5	20
Huffman & RC4	5	5	5	5	20
Deflate & DES	10	10	10	10	40
Deflate & 3DES	10	10	10	10	40
Deflate & AES	10	10	10	10	40
Deflate & Blowfish	10	10	10	10	40
Deflate & RC4	10	10	10	10	40

ตาราง 4.6 สรุปคะแนนตามเกณฑ์ด้านขนาดของผลลัพธ์

จากผลคะแนนตามตาราง 4.6 พบว่า ขนาดของผลลัพธ์นั้นขึ้นอยู่กับอัลกอริทึมในการบีบอัดเป็นหลัก ดังนั้นอัลกอริทึมที่ใช้หลักการบีบอัดแบบเดียวกัน ก็จะได้คะแนนที่เท่ากันไม่ว่าจะจับคู่กับอัลกอริทึมเข้ารหัสลับแบบใดก็ตาม โดยคะแนนสรุปที่ได้ออกมาก็คือ อัลกอริทึมที่บีบอัดข้อมูลได้ดีกว่าคือ Deflate

4.3.3 ด้านอัตราส่วนในการบีบอัด

ให้นำหนักคะแนนของอัลกอริทึมที่มีเปอร์เซ็นต์การบีบอัดได้มากที่สุด 10 คะแนน และให้คะแนนลดลงไปในแต่ละอันดับจนถึงอันดับที่มีเปอร์เซ็นต์การบีบอัดได้น้อยที่สุดให้ 1 คะแนน ดังนั้นจากผลการทดลองจึงสามารถให้คะแนนในแต่ละอัลกอริทึมได้ดังนี้

Process	Criteria: Compression Ratio				Sum
	document1.doc	photo1.jpg	document2.doc	photo2.jpg	
Huffman & DES	5	10	10	10	35
Huffman & 3DES	5	10	10	10	35
Huffman & AES	5	10	10	10	35
Huffman & Blowfish	5	10	10	10	35
Huffman & RC4	5	10	10	10	35
Deflate & DES	10	10	10	10	40
Deflate & 3DES	10	10	10	10	40
Deflate & AES	10	10	10	10	40
Deflate & Blowfish	10	10	10	10	40
Deflate & RC4	10	10	10	10	40

ตาราง 4.7 สรุปคะแนนตามเกณฑ์ด้านอัตราส่วนในการบีบอัด

จากคะแนนสรุปตามตาราง 4.7 แสดงให้เห็นว่าอัตราส่วนในการบีบอัดก็ยังคงเป็นผลลัพธ์ที่ขึ้นอยู่กับอัลกอริทึมในการบีบอัดเป็นหลักเช่นเดียวกันกับขนาดของผลลัพธ์ โดยอัลกอริทึมที่ทำคะแนนในด้านของอัตราส่วนในการบีบอัดดีก็คือ Deflate

4.3.4 ด้านประสิทธิภาพในการบีบอัด

ให้นำน้ำหนักคะแนนของอัลกอริทึมที่มี throughput มากที่สุด 10 คะแนน และให้คะแนนลดลงไปในแต่ละอันดับจนถึงอันดับที่มี throughput น้อยที่สุดให้ 1 คะแนน ดังนั้นจากผลการทดลองจึงสามารถให้คะแนนในแต่ละอัลกอริทึมได้ดังนี้

Process	Criteria: Throughput				Sum
	document1.doc	photo1.jpg	document2.doc	photo2.jpg	
Huffman & DES	5	4	3	3	15
Huffman & 3DES	1	1	1	2	5
Huffman & AES	3	5	8	9	25
Huffman & Blowfish	9	7	5	8	29
Huffman & RC4	8	9	10	10	37
Deflate & DES	10	3	4	4	21
Deflate & 3DES	2	2	2	1	7
Deflate & AES	7	10	6	7	30
Deflate & Blowfish	6	6	7	5	24
Deflate & RC4	4	8	9	6	27

ตาราง 4.8 สรุปคะแนนตามเกณฑ์ด้านประสิทธิภาพในการบีบอัด

ประสิทธิภาพในการบีบอัด เป็นอีกหนึ่งเกณฑ์ที่อิงค่าตามเวลาในการดำเนินการ ดังนั้นผลลัพธ์ที่ได้จึงสอดคล้องกับผลลัพธ์ที่ได้ในส่วนของเวลา คือ Huffman & RC4 มีประสิทธิภาพในการบีบอัดเป็นอันดับ 1 โดยมี Deflate & AES ได้อันดับรองลงมา และอัลกอริทึมที่ได้อันดับสุดท้ายคือ Huffman & 3DES

4.3.5 ด้านความปลอดภัย

ให้นำนักคะแนนของอัลกอริทึมที่ใช้เวลาในการเจาะรหัสด้วยวิธี Brute force มากที่สุด 10 คะแนน และให้คะแนนลดลงไปในแต่ละอันดับจนถึงอันดับที่มีเวลาในการเจาะรหัสด้วยวิธี Brute force น้อยที่สุดให้ 1 คะแนน ดังนั้นจากผลการทดลองจึงสามารถให้คะแนนในแต่ละอัลกอริทึมได้ดังนี้

Process	Criteria: Brute Force Time				Sum
	document1.doc	photo1.jpg	document2.doc	photo2.jpg	
Huffman & DES	1	2	2	2	7
Huffman & 3DES	4	4	4	4	16
Huffman & AES	6	6	6	6	24
Huffman & Blowfish	8	7	7	7	29
Huffman & RC4	10	10	10	10	40
Deflate & DES	2	1	1	1	5
Deflate & 3DES	3	3	3	3	12
Deflate & AES	5	5	5	5	20
Deflate & Blowfish	7	8	8	8	31
Deflate & RC4	10	10	10	10	40

ตาราง 4.9 สรุปคะแนนตามเกณฑ์ด้านความปลอดภัย

ประสิทธิภาพในด้านความปลอดภัย เป็นเกณฑ์ที่ผลลัพธ์ขึ้นอยู่กับอัลกอริทึมในการเข้ารหัสลับเป็นหลัก ซึ่งจากผลลัพธ์แสดงให้เห็นว่า ระยะเวลาในการเจาะรหัสด้วยวิธี brute force attack กับอัลกอริทึม DES จะใช้เวลาเร็วที่สุด และจะใช้ระยะเวลานานที่สุดเมื่อนำไปใช้กับอัลกอริทึม RC4