

ห้องสมุดงานวิจัย สำนักงานคณะกรรมการวิจัยแห่งชาติ



250633

การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัด
และการเข้ารหัส

ภูเบศร์ แบนขุนทด

วิทยาศาสตร์มหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์

บัณฑิตวิทยาลัย
มหาวิทยาลัยเชียงใหม่
พฤษภาคม 2555



การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัด
และการเข้ารหัส



ภูเบศร์ แบนขุนทด

การค้นคว้าแบบอิสระนี้เสนอต่อบัณฑิตวิทยาลัยเพื่อเป็นส่วนหนึ่ง
ของการศึกษาตามหลักสูตรปริญญา
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์

บัณฑิตวิทยาลัย
มหาวิทยาลัยเชียงใหม่
พฤษภาคม 2555

การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัด และการเข้ารหัส

ภูเบศร์ แบนขุนทด

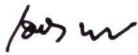
การค้นคว้าแบบอิสระนี้ได้รับการพิจารณาอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์

คณะกรรมการสอบการค้นคว้าแบบอิสระ

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ


.....ประธานกรรมการ

รองศาสตราจารย์ ดร.สุรนนท์ น้อยมณี


.....

รองศาสตราจารย์ ดร.เอกรัง บุญเชียง


.....กรรมการ

รองศาสตราจารย์จักรภพ วงศ์ละคร


.....กรรมการ

รองศาสตราจารย์ ดร.เอกรัง บุญเชียง

23 พฤษภาคม 2555

© ลิขสิทธิ์ของมหาวิทยาลัยเชียงใหม่

กิตติกรรมประกาศ

การค้นคว้าแบบอิสระเรื่องการเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส ได้สำเร็จลุล่วงเป็นอย่างดีด้วยความกรุณาจาก รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง ที่ได้อนุเคราะห์ให้คำแนะนำ ให้คำปรึกษา และตรวจสอบข้อบกพร่องต่าง ๆ ตลอดจนการค้นคว้าแบบอิสระนี้สำเร็จสมบูรณ์และขอขอบพระคุณ รองศาสตราจารย์ ดร. จิรยุทธ ไชยจารุวนิช ผู้ช่วยศาสตราจารย์ ดร.วัชร จ่าปามูล ผู้ช่วยศาสตราจารย์ ดร.เสมอแซ สมหอม ผู้ช่วยศาสตราจารย์ ดร.รัฐสิทธิ์ สุขะหุด ดร.วิจักขณ์ ศรีสังจะเลิสวาจา และคณาจารย์ในภาควิชาวิทยาการคอมพิวเตอร์ทุกท่านเป็นอย่างสูง ที่ประสิทธิประสาทวิชา ความรู้ให้คำแนะนำเป็นอย่างดีตลอดมา

ขอขอบพระคุณ รองศาสตราจารย์ ดร.สุรนนท์ น้อยมณี ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ที่ได้ให้เกียรติเป็นประธานกรรมการ และ รองศาสตราจารย์จักรภพ วงศ์ละคร สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยแม่โจ้ ที่ได้ให้เกียรติเป็นกรรมการผู้ทรงคุณวุฒิ ในการสอบการค้นคว้าแบบอิสระนี้ ซึ่งอาจารย์ทั้งสองท่านได้ให้คำแนะนำที่เป็นประโยชน์ ชี้ให้เห็นถึงข้อบกพร่อง ข้อควรปรับปรุง และแนะนำแนวทางในการนำไปใช้ต่อในอนาคต

ท้ายที่สุด ผู้จัดทำหวังว่าการค้นคว้าแบบอิสระนี้คงเป็นประโยชน์บ้างไม่มากนักน้อยสำหรับผู้ที่สนใจที่จะศึกษาต่อไป

ภูเบศร์ แบนขุนทด

ชื่อเรื่องการค้นคว้าแบบอิสระ

การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส

ผู้เขียน

นายภูเบศวร์ แบนขุนทด

ปริญญา

วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ

รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง

บทคัดย่อ

250633

การค้นคว้าแบบอิสระการเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส มีวัตถุประสงค์เพื่อศึกษาเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส และเพื่อพัฒนาโปรแกรมเข้ารหัสและการบีบอัดเพื่อใช้งานส่วนบุคคล

การศึกษาค้นคว้าครั้งนี้ได้ทำการแบ่งขอบเขตในการศึกษาออกเป็นด้านต่างๆ คือ ขอบเขตด้านอัลกอริทึมที่ใช้ในการเข้ารหัสลับ ได้เลือกใช้อัลกอริทึมแบบสมมาตร ได้แก่ DES, 3DES, AES, Blowfish และ RC4 ด้านอัลกอริทึมที่ใช้ในการบีบอัดข้อมูล ได้เลือกใช้อัลกอริทึมเพื่อการบีบอัดข้อมูลแบบไม่สูญเสีย ซึ่งเหมาะกับการใช้งานทั่วไป ได้แก่ Huffman Coding และ Deflate ด้านข้อมูลนำเข้าและผลลัพธ์ที่ได้จากโปรแกรม ได้กำหนดให้ข้อมูลนำเข้าสามารถใช้ไฟล์ประเภทใดก็ได้ที่มีขนาดไม่เกิน 5 เมกกะไบต์ และให้แสดงผลลัพธ์ในรูปแบบของตัวอักษร ในด้านกำหนดเกณฑ์ที่ใช้วัดประสิทธิภาพด้านต่างๆ ประกอบด้วยเวลาในการดำเนินการ ขนาดของผลลัพธ์ อัตราส่วนในการบีบอัด ประสิทธิภาพในการบีบอัดต่อหน่วยเวลา และระยะเวลาในการเจาะรหัสข้อมูลแบบ Brute force ซึ่งหลังจากได้ดำเนินการพัฒนาโปรแกรมเป็นที่เรียบร้อยแล้ว ได้ทำการออกแบบการทดลองโดยแบ่งประเภทของไฟล์นำเข้าเป็นสองประเภทคือ ไฟล์เอกสาร และไฟล์รูปภาพ ซึ่งได้ทำการทดลองไฟล์แต่ละประเภท 2 ครั้ง คือครั้งแรกใช้ไฟล์ที่มีขนาดเล็กกว่า 1 เมกกะไบต์ และครั้งที่สองใช้ไฟล์ที่มีขนาดมากกว่า 4 เมกกะไบต์ (แต่ไม่เกิน 5 เมกกะไบต์)

ผลสรุปจากการทดลองแสดงให้เห็นว่าไฟล์เอกสาร และไฟล์รูปภาพ มีความแตกต่างกันในด้านการตอบสนองต่อการบีบอัดข้อมูล คือไฟล์เอกสารจะสามารถถูกบีบอัดได้มากกว่าไฟล์รูปภาพ โดยพิจารณาจากค่าขนาดหลังทำการบีบอัด ค่าอัตราส่วนในการบีบอัด และค่าประสิทธิภาพในการบีบอัด ที่เป็นไปในทิศทางเดียวกัน ส่วนในด้านของเวลาในการดำเนินการตัวแปรขึ้นอยู่กับ

250633

อัลกอริทึมที่ใช้ในการเข้ารหัสลับ โดย RC4 เป็นอัลกอริทึมแบบ stream cipher ซึ่งมีความเร็วสูง และคีย์ที่ใช้มีจำนวนมากทำให้เกิดความยืดหยุ่น จึงสามารถทำเวลาได้ดีที่สุด และในด้านของความปลอดภัยนั้น ขึ้นอยู่กับอัลกอริทึมที่ใช้ในการเข้ารหัสลับเป็นหลัก โดยอัลกอริทึมที่ใช้ระยะเวลาในการเจาะรหัสด้วยวิธี brute force attack ซึ่งการคำนวณเวลาในการถอดรหัส ขึ้นอยู่กับตัวแปรสองตัวเป็นหลัก คือ ขนาดของ key ที่ใช้ในการเข้ารหัส และความสามารถในการประมวลผลของ CPU โดย DES เป็นอัลกอริทึมที่มีการใช้ขนาดกุญแจน้อยที่สุดคือ 56 bits และ RC4 เป็นอัลกอริทึมที่ใช้ขนาดของกุญแจในการเข้ารหัสมากที่สุดคือ 2048 bit ดังนั้นค่าผลลัพธ์ที่ได้จึงทำให้ RC4 เป็นอัลกอริทึมที่ใช้เวลาในการเจาะรหัสแบบ brute force นานที่สุด และ DES จึงเป็นอัลกอริทึมที่ใช้เวลาในการเจาะรหัสได้เร็วที่สุดนั่นเอง

Independent Study Title	Performance Comparison of Integration Between Compression and Encryption
Author	Mr. Phubate Bankhuntot
Degree	Master of Science (Computer Science)
Independent Study Advisor	Assoc. Prof. Dr.Ekkarat Boonchieng

ABSTRACT

250633

The objective of this independent study entitled “Performance Comparison of Integration between Compression and Encryption” was to compare performances of integration between Compression and Encryption. Another objective was to develop the compression and encryption program for personal uses.

The area of this independent study about encryption algorithms were DES, 3DES, AES, Blowfish and RC4. Compression algorithms were Huffman coding and Deflate algorithm. Input file was limited at 5 Mb. for any type and output shown in text format. Criteria for the experiments were Time, Size, Compression ratio, Throughput and Brute force time. The design of sample test was take file input in two type, document and picture, was test 2 times that the first used file less than 1 Mb. and the second used file more than 4 Mb. (but less than 5 Mb.)

Conclusion of the result table shown that document file reacted by compression more than picture file type. RC4 was the fastest encryption algorithm because RC4 was a stream cipher that makes the process smooth and the large key size makes its flexible. The security test was use brute force attack method to calculated time for decryption that ups to key of encryption algorithm and CPU clock speed. DES is the least key size by 56 bits and RC4 is the biggest key size by 2048 bits. The result shown RC4 was the strongest algorithm that took the longest time to attack by brute force method.

สารบัญ

	หน้า
กิตติกรรมประกาศ	ก
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	ฉ
สารบัญตาราง	ฉ
สารบัญภาพ	ญ
บทที่ 1 บทนำ	
1.1 ที่มาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการศึกษา	2
1.3 ประโยชน์ที่จะได้รับจากการศึกษา	2
1.4 ขอบเขตและวิธีการศึกษา	2
1.5 สถานที่ที่ใช้ในการดำเนินการศึกษาและรวบรวมข้อมูล	5
บทที่ 2 แนวคิดและทฤษฎีที่เกี่ยวข้อง	
2.1 การบีบอัดข้อมูล	6
2.2 การเข้ารหัสลับ	10
2.3 การเข้ารหัสแบบ Base64	15
2.4 Million Instructions per Second (MIPS)	16
2.5 Brute Force Attack	16
2.6 เอกสารงานวิจัยที่เกี่ยวข้อง	18
บทที่ 3 ขั้นตอนการออกแบบและพัฒนาโปรแกรม	
3.1 กระบวนการทำงานของโปรแกรม	20
3.2 การออกแบบหน้าจอส่วนติดต่อผู้ใช้	21
3.3 การเขียนโปรแกรม	24
3.3.1 การบีบอัดข้อมูล	24
3.3.2 การเข้ารหัสข้อมูล	26
3.3.3 การเข้ารหัสด้วย Base64	29

สารบัญ (ต่อ)

	หน้า
3.3.4 เวลาที่ใช้ในการดำเนินการ	30
3.3.5 ขนาดของผลลัพธ์	30
3.3.6 อัตราส่วนในการบีบอัด	31
3.3.7 ประสิทธิภาพในการบีบอัด	31
3.3.8 MIPS	31
3.3.9 Brute force time	32
บทที่ 4 ผลการศึกษา	
4.1 การออกแบบการทดลอง	33
4.2 เปรียบเทียบผลลัพธ์ตามกำหนดเกณฑ์การทดลอง	34
4.3 สรุปผลลัพธ์ตามกำหนดเกณฑ์	37
บทที่ 5 บทสรุปและข้อเสนอแนะ	
5.1 สรุปผลการศึกษา	42
5.2 ปัญหาและข้อจำกัด	44
5.3 ข้อเสนอแนะ	45
บรรณานุกรม	46
ภาคผนวก	
ภาคผนวก ก การติดตั้งโปรแกรมและการถอดถอนการติดตั้งโปรแกรม	48
ภาคผนวก ข คู่มือการใช้โปรแกรม	51
ประวัติผู้เขียน	57

สารบัญตาราง

ตาราง	หน้า
2.1 ตารางแสดงสัญลักษณ์ที่ใช้ในอัลกอริทึม Deflate	9
2.2 ตารางแสดงตัวอย่างการเข้ารหัสแบบ Base 64	15
4.1 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ document1.doc	34
4.2 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ photo1.jpg	35
4.3 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ document2.doc	36
4.4 ตารางเปรียบเทียบค่าตามเกณฑ์ต่างๆ ของไฟล์ photo2.jpg	36
4.5 สรุปคะแนนตามเกณฑ์ด้านเวลาในการดำเนินการ	37
4.6 สรุปคะแนนตามเกณฑ์ด้านขนาดของผลลัพธ์	38
4.7 สรุปคะแนนตามเกณฑ์ด้านอัตราส่วนในการบีบอัด	39
4.8 สรุปคะแนนตามเกณฑ์ด้านประสิทธิภาพในการบีบอัด	40
4.9 สรุปคะแนนตามเกณฑ์ด้านความปลอดภัย	41
5.1 สรุปคะแนนตามตามเกณฑ์แต่ละด้าน	43

สารบัญภาพ

ภาพ	หน้า
2.1 โครงสร้างการทำงานของ DES	12
2.2 โครงสร้างการทำงานของ Triple DES	13
2.3 ตัวอย่างการถอดรหัสด้วยวิธี Brute Force Attack	17
3.1 Block Diagram แสดงกระบวนการทำงานของโปรแกรม	20
3.2 หน้าจอหลักของโปรแกรม	22
3.3 หน้าจอในส่วนของการนำเข้าข้อมูล	22
3.4 หน้าจอในส่วนของระบบนำกลับคืนมาเป็นไฟล์ต้นฉบับ	23
ก.1 ไฟล์ติดตั้ง โปรแกรม	47
ก.2 เริ่มกระบวนการติดตั้งโปรแกรม	47
ก.3 โปรแกรม CryptoN!ce ติดตั้งเสร็จสมบูรณ์	48
ก.4 การถอดถอนโปรแกรม CryptoN!ce	48
ก.5 หน้าต่างการถอดถอน โปรแกรม CryptoN!ce	49
ข.1 การใช้งานนำเข้าข้อมูล	50
ข.2 หน้าต่างโปรแกรมส่วนของการนำเข้าข้อมูล	51
ข.3 หน้าต่างแสดงผลการทำงานเมื่อเสร็จสิ้นกระบวนการนำเข้าข้อมูล	52
ข.4 การใช้งานถอดรหัสข้อมูลกลับมาเป็นไฟล์ต้นฉบับ	53
ข.5 ข้อมูลตัวอักษรที่จะนำมาแปลงกลับไปเป็นไฟล์ต้นฉบับ	53
ข.6 หน้าต่างโปรแกรมส่วนของการแปลงกลับไปเป็นไฟล์ต้นฉบับ	54
ข.7 หน้าต่างแสดงผลการทำงานเมื่อเสร็จสิ้นกระบวนการแปลงกลับไปเป็นไฟล์ต้นฉบับ	55