การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส

ภูเบศวร์ แบนขุนทด

วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์

บัณฑิตวิทยาลัย
มหาวิทยาลัยเชียงใหม่
พฤษภาคม 2555

การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส

ภูเบศวร์ แบนขุนทด

การค้นคว้าแบบอิสระนี้เสนอต่อบัณฑิตวิทยาลัยเพื่อเป็นส่วนหนึ่ง
ของการศึกษาตามหลักสูตรปริญญา
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์

บัณฑิตวิทยาลัย
มหาวิทยาลัยเชียงใหม่
พฤษภาคม 2555

การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส

ภูเบศวร์ แบนขุนทด

การค้นคว้าแบบอิสระนี้ได้รับการพิจารณาอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษา
ตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์

คณะกรรมการสอบการค้นคว้าแบบอิสระ

.....ประธานกรรมการ
รองศาสตราจารย์ ดร.สุรนันท์ น้อยมณี

.....กรรมการ
รองศาสตราจารย์จักรภพ วงศ์ละคร

.....กรรมการ
รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ

.....
รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง

23 พฤษภาคม 2555

กิตติกรรมประกาศ

การค้นคว้าแบบอิสระเรื่องการเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส ได้สำเร็จลุล่วงเป็นอย่างดีด้วยความกรุณาจาก รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง ที่ได้อนุเคราะห์ให้คำแนะนำ ให้คำปรึกษา และตรวจสอบข้อบกพร่องต่าง ๆ ตลอดจนการค้นคว้าแบบอิสระนี้สำเร็จสมบูรณ์และขอขอบพระคุณ รองศาสตราจารย์ ดร. จีรยุทธ ไชยจารุวณิช ผู้ช่วยศาสตราจารย์ ดร.วัชรี จำปามูล ผู้ช่วยศาสตราจารย์ ดร.เสมอแข สมหอม ผู้ช่วยศาสตราจารย์ ดร.รัฐสิทธิ์ สุขะหุต ดร.วิจักษณ์ ศรีสัจจะเลิสวาจา และคณาจารย์ในภาควิชาวิทยาการคอมพิวเตอร์ทุกท่านเป็นอย่างสูง ที่ประสิทธิประสาทวิชา ความรู้ให้คำแนะนำเป็นอย่างดีตลอดมา

ขอขอบพระคุณ รองศาสตราจารย์ ดร.สุรนันท์ น้อยมณี ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ที่ได้ให้เกียรติเป็นประธานกรรมการ และรองศาสตราจารย์จักรภพ วงศ์ละคร สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยแม่โจ้ ที่ได้ให้เกียรติเป็นกรรมการผู้ทรงคุณวุฒิ ในการสอบการค้นคว้าแบบอิสระนี้ ซึ่งอาจารย์ทั้งสองท่านได้ให้คำแนะนำที่เป็นประโยชน์ ชี้ให้เห็นถึงข้อบกพร่อง ข้อควรปรับปรุง และแนะนำแนวทางในการนำเอาไปใช้ต่อยอดในอนาคต

ท้ายที่สุด ผู้จัดทำหวังว่าการค้นคว้าแบบอิสระนี้คงเป็นประโยชน์บ้างไม่มากก็น้อยสำหรับผู้ที่สนใจที่จะศึกษาต่อไป

ภูเบศวร์ แบนขุนทด

ชื่อเรื่องการค้นคว้าแบบอิสระ การเปรียบเทียบประสิทธิภาพการทำงานร่วมกันระหว่างการบีบอัดและการเข้ารหัส

ผู้เขียน นายภูเบศวร์ แบนขุนทด

ปริญญา วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

อาจารย์ที่ปรึกษาการค้นคว้าแบบอิสระ รองศาสตราจารย์ ดร.เอกรัฐ บุญเชียง

บทคัดย่อ

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 คือครั้งแรกใช้ไฟล์ที่มีขนาดน้อยกว่า 1 เมกกะไบต์ และครั้งที่สองใช้ไฟล์ที่มีขนาดมากกว่า 4 เมกกะไบต์ (แต่ไม่เกิน 5 เมกกะไบต์)

ผลสรุปจากการทดลองแสดงให้เห็นว่าไฟล์เอกสาร และไฟล์รูปภาพ มีความแตกต่างกันในด้านของการตอบสนองต่อการบีบอัดข้อมูล คือไฟล์เอกสารจะสามารถถูกบีบอัดได้มากกว่าไฟล์รูปภาพ โดยพิจารณาจากค่าขนาดหลังทำการบีบอัด ค่าอัตราส่วนในการบีบอัด และค่าประสิทธิภาพในการบีบอัด ที่เป็นไปในทิศทางเดียวกัน ส่วนในด้านของเวลาในการดำเนินการตัวแปรขึ้นอยู่กับ

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

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

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ