KOMPARASI KRIPTOGRAFI AES DAN RC4 PADA METODE LEAST SIGNIFICANT BIT (LSB) PADA CITRA DIGITAL DENGAN FORMAT BITMAP

TESIS

Oleh:

Rahmat Sulaiman

1511601740

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2017

KOMPARASI KRIPTOGRAFI AES DAN RC4 PADA METODE LEAST SIGNIFICANT BIT (LSB) PADA CITRA DIGITAL DENGAN FORMAT BITMAP

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)

Oleh:

Rahmat Sulaiman

1511601740

PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2017

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Nama Mahasiswa : RAHMAT SULAIMAN
Nomor Induk Mahasiswa : 15116017140
Konsentrasi : Rekayasa Komputasi Terapan
Fakultas / Program : Magister Ilmu Komputer
Jenjang Studi : Strata 2

Mennyatakan bahwa TESIS yang berjudul :

KOMPARASI KRIPTOGRAFI AES DAN RC4 PADA METODE LEAST SIGNIFICANT BIT (LSB) PADA CITRA DIGITAL DENGAN FORMAT BITMAP

1. Merupakan hasil karya tulis ilmiah sendiri bukan merupakan kaya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain.
2. Saya izinka untuk dikeola oleh Universitas Budi Luhur sesuai dengan nnorma hukum da etika yang berlaku,

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yag berlaku apabila dikemudian hari penyataan ini tidak benar.

Jakarta, 8 Agustus 2017

(Rahmat Sulaiman)

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa	: Rahmat Sulaiman
Nomor Induk Mahasiswa	: 1511601740
Konsentrasi	: Rekayasa Komputasi Terapan
Jenjang Studi	: Strata 2
Judul Tesis	: KOMPARASI KRIPTOGRAFI AES DAN RC4 PADA METODE LEAST SIGNIFICANT BIT (LSB) PADA CITRA DIGITAL DENGAN FORMAT BITMAP

Jakarta, 4 Agustus 2017

Tim Penguji — Tanda Tangan

Ketua,

(Prof. Dr. Moedjiono, M.Sc) .....

Anggota,

(Deni Mahdiana, M.M, M.Kom) .....
Pembimbing Utama

(Dr. Ir. Nazori AZ, M.T) .....

Ketua Program Studi
Magister Ilmu Komputrer

(Dr. M. Syafrullah, M.Kom, M.Sc)

ABSTRAK

Keamanan pesan merupakan suatu hal yang harus dijaga kerahasiaannya. Namun, untuk menjaga keamanan dan kerahasiaan suatu pesan dibutuhkan dua buah metode yang berbeda. Untuk menjaga keamanan pesan, ilmu yang telah banyak digunakan adalah dengan menggunakan kriptografi. Sedangkan untuk menjaga kerahasiaan pesan, ilmu yang digunakan adalah steganografi. Untuk itu dibutuhkannya suatu pengamanan pesan yang dapat menjaga keamanan dan kerahasiaan pesan secara bersamaan. Berbagai algoritma telah banyak diterapkan dalam pengamanan data, namun tidak diketahui algoritma mana yang memiliki kecepatan yang lebih unggul jika diterapkan dalam LSB. Pengujian dilakukan dengan menghitung lama proses waktu enkripsi dan dekripsi dari masing-masing algoritma dengan jumlah pesan dan panjang kunci yang sama. Pengukuran waktu dilakukan sebanyak 10 kali, kemudian diambil nilai rata-ratanya untuk mendapatkan waktu yang konsisten karna ketidakstabilan sistem. Oleh karena itu, akan dilakukan perbandingan kecepatan proses enkripsi dan dekripsi dengan menerapkan algoritma AES dan RC4 pada LSB menggunakan Microsoft Visual Studio 2008. Hasil penelitian proses enkripsi dan dekripsi yang dilakukan, algoritma AES lebih unggul dalam hal kecepatan dibandingkan dengan algoritma RC4. Nilai MSE dan PSNR yang dihasilkan dari gambar yang sudah dienkripsi berdasarkan algoritma AES dan RC4 tidak mengalami perbedaan nilai yang signifikan. Pada penelitian ini secara keseluruhan membuktikan bahwa algotima AES lebih baik dalam hal kecepatan jika diterapkan pada LSB dibandingkan dengan algoritma RC4.

Kata Kunci: Kriptografi, Steganografi, LSB, AES, RC4

ABSTRACT

Message security is something that must be kept secretly. However, to maintain the security and the secret of a message it takes two different methods. To maintain the security of messages, the science that has been widely used is to use cryptography. As for maintaining the secret of the message, the science used is steganography. For that we need a security message that can maintain the security and the secret of the message simultaneously. Various algorithms have been widely applied in data security, but it is unknown which algorithm has a superior speed when applied in the LSB. The test is done by calculating the length of the encryption time process and the decryption time process of each algorithm with the same number of messages and key lengths. Measurement time is done as much as 10 times, then taken average value to get consistent time because system instability. Therefore, we will compare the speed of encryption and decryption process by applying AES and RC4 algorithm to LSB in Visual Studio 2008. In the process of encryption and decryption, the AES algorithm is superior in terms of speed compared to RC4 algorithm. The MSE and PSNR values generated from the encrypted images based on the AES and RC4 algorithm doesn't show significant value. Overall the AES algorithm is better than RC4 algorithm when applied in LSB.

Keywords: Cryptography, Steganography, LSB, AES, RC4

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Allah SWT, Tuhan Yang Maha Esa, karena berkat nikmat dan rahmat-Nya penulis bisa menyelesaikan laporan penelitian tesis ini. Tujuan dari penulisan laporan penelitian tesis ini adalah sebagai salah satu syarat untuk menyusun tesis pada Program Studi Magister Ilmu Komputer, Universitas Budi Luhur Jakarta.

Rasa dan ucapan serta ungkapan terima kasih penulis persembahkan kepada semua pihak yang telah membantu penulis dalam menyusun laporan penelitian tesis ini baik secara materiil dan moril:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Ibu saya yang tercinta, yang tidak pernah berhenti memberikan dukungan kepada penulis, baik dalam bentuk moril, materiil, do'a serta kasih sayang yang luar biasa.
3. Kakak-kakak saya yang tercinta yang selalu mendukung dan memberikan semangat yang tiada henti-hentinya kepada penulis.
4. Bapak Drs. Djaetun HS yang telah mendirikan Universitas Budi Luhur.
5. Bapak Drs. Harry Sudjikianto, MM, MBA selaku ketua pengurus harian yayasan Atma Luhur yang telah memberikan Beasiswa kepada penulis.
6. Bapak Dr. Ir. Nazori AZ, M.T, selaku dosen pembimbing tesis yang telah membimbing dan memotivasi penulis dalam mengerjakan penelitian tesis ini.
7. Bpak Dr. Suhartono, M.A, MBA selaku Direktur Program Pasca Sarjana dan Bapak Dr. M. Syafrullah, M.Kom., M.Sc selaku Kaprodi MKom beserta Bapak dan Ibu Dosen pengampu mata kuliah di Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang telah dengan sabar dan tulus memberikan ilmu pengetahuan, pencerahan, dan bimbingan dalam belajar.
8. Rekan-rekan mahasiswa MKOM Universitas Budi Luhur, terima kasih atas kebersamaan, kerja keras dan dukungan semangatnya.
9. Thanks to my best roomate, Tri Sugihartono.

Penulis menyadari masih banyak kekurangan dari laporan penelitian tesis ini, oleh karena itu penulis mengharapkan kritik dan saran yang bersifat membangun demi kesempurnaan penelitian tesis ini. Semoga penelitian tesis ini masih dapat memberikan manfaat dari keterbatasannya. *Amin*.

Jakarta, Agustus 2017

Rahmat Sulaiman

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar Halaman

DAFTAR TABEL

Tabel Halaman

DAFTAR PUSTAKA,

Bruice, S. 2007, *Applied Cryptography, Cryptography Protocols, Algorithm and Source Code in C,* Second edition. Wiley India edition

Katzenbeisser, FAP. 2000, *Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House*, Norwood.

Simmons, G.J. 2000, *The prisoners' problem and the subliminal channel in Proc. Advances in Cryptology*

Cheddad, A., Joan, C., Curran, K. & Paul, M.K. 2010, *Digital image steganography: Survey and analysis of current methods Signal Processing 90*

Rian, A. & Lucky, T.O. 2013, *Artikel Implementasi Kriptografi dan Steganografi MenggunakanAlgoritma RSA dan Metode LSB*

N.P, Indah, F.A. & Awang, H.K. 2015, *Jurnal Implementasi Kriptografi Pengamanan Data Pada File Teks, Isi File Dokumen dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard.* Jurnal Informatika Mulawarman Vol. 10 No.1

Putri, A. 2009, *Artikel Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital,* Mahasiswa Jurusan Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi ,Universitas Gunadarma

Adetya, K.P. *Pengamanan Data Dengan Metode Advanced Cryption Standard dan Metode Least Significant Bit,* Mahasiswa Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang.

Gede, W.B, & Made, I.W.2015, *Implementasi Algoritma Kriptografi AES 256 dan Metode Steganografi LSB pada Gambar Bitmap,* Jurnal Ilmiah Ilmu Komputer, Universitas Udayana, Vol. 8, No. 2, September

Handa, G., *Penggunaan Metode Steganografi dan Kriptografi Dengan Algoritma RC4 Stream Cipher Dalam Pengaanan Citra Digital Perusahaan,* Mahasiswa Pasca Sarjanan, Universitas Budi Luhur

Hartono, B. 2004, *Ruang Lingkup Kriptografi Untuk Mengamankan Data,* Jurnal Dinamika Informatika, Vol.9, No.2 1-8

Dony, A. 2005, *Computer Security*, Yogyakarta, Penerbit Andi Yogyakarta, 2005

Nurhayati & Syukuri, S.H. 2014,*Steganography for Inserting Message on Digital Image Using Least Significant Bit and AES Cryptographic Algorithm*, Informatics Engineering Department, Science and Technology Faculty Syarif Hidayatullah State Islamic University (UIN) Jakarta,.