Perpustakaan Universitas Budi Luhur

PROTOTIPE KEAMANAN PESAN RAHASIA DENGAN TEKNIK KRIPTOGRAFI DAN STEGANOGRAFI MENGGUNAKAN ALGORITMA LSB, RSA, CRT DAN HUFFMAN

TESIS

Oleh:

MOH. SOFJAN

1311600173

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015

Perpustakaan Universitas Budi Luhur

PROTOTIPE KEAMANAN PESAN RAHASIA DENGAN TEKNIK KRIPTOGRAFI DAN STEGANOGRAFI MENGGUNAKAN ALGORITMA LSB, RSA, CRT DAN HUFFMAN

TESIS

Diajukan untuk memenuhi salah satu persyaratan

Memperoleh gelar Magister Ilmu Komputer (MKOM)

Oleh:

MOH. SOFJAN

1311600173

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2015

Perpustakaan Universitas Budi Luhur

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

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini,

Nama Mahasiswa : MOH. SOFJAN
Nomor Induk Mahasiswa : 1311600173
Program Studi : MAGISTER ILMU KOMPUTER (MKOM)
Konsentrasi : REKAYASA KOMPUTASI TERAPAN

menyatakan bahwa TESIS yang berjudul :
PROTOTIPE KEAMANAN PESAN RAHASIA DENGAN TEKNIK KRIPTOGRAFI DAN STEGANOGRAFI MENGGUNAKAN ALGORITMA LSB, RSA, CRT DAN HUFFMAN.

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijinkan untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan apabila di kemudian pernyataan ini tidak benar.

Jakarta, Agustus 2015

METERAI TEMPEL 6000

(MOH. SOFJAN)

Perpustakaan Universitas Budi Luhur

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

LEMBAR PENGESAHAN

Nama Mahasiswa	: Moh. Sofjan
Nomor Induk Mahasiswa	: 1311600173
Konsentrasi	: Rekayasa Komputasi Terapan
Jenjang Studi	: Strata 2
Judul TESIS	: PROTOTIPE KEAMANAN PESAN RAHASIA DENGAN TEKNIK KRIPTOGRAFI DAN STEGANOGRAFI MENGGUNAKAN ALGORITMA LSB, RSA,CRT DAN HUFFMAN

Jakarta 31 Agustus 2015

Tim Penguji : Tanda tangan :

Penguji I (Ketua)
Prof. Dr. Moedjiono, M.Sc .....

Penguji II
Ir. Wendi Usino, MM.,M.Sc.,Ph.D .....

Pembimbing,
Dr., Ir. Nazori Az, M.T .....

Ketua Program Studi

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

Perpustakaan Universitas Budi Luhur

ABSTRAK

Kriptografi dan Steganografi merupakan metode pengiriman pesan secara rahasia. Pada kriptografi pesan yang dikirim tetap terlihat oleh pihak lain tapi dalam bentuk yang tersandi. Sementara pada steganografi pesan yang dikirim disembunyikan di balik media lain. Kombinasi keduanya akan memberikan tingkat keamanan pesan yang lebih tinggi. LSB merupakan salah satu metode steganografi yang cukup dikenal luas. Metode ini akan menggantikan bit-bit tertentu pada citra dengan pesan yang akan disembunyikan. Sementara RSA merupakan salah satu metode kriptografi bertipe tidak simetris yang banyak digunakan . Kriptografi tidak simetris adalah kriptografi yang terdiri atas kunci publik dan kunci *private*. Kunci publik akan disebar luaskan sementara kunci *private* hanya dimiliki oleh yang berhak. Sebuah pesan yang dienkripsi dengan kunci publik hanya dapat dibuka dengan kunci *private* yang berkaitan. Penelitian ini menggabungkan kriptografi RSA 1024 bit 8 faktor prima yang telah dimodifikasi dengan steganografi LSB. Pada proses enkripsi digunakan metode RSA yang digabungkan dengan metode *Huffman* untuk mengurangi jumlah bit yang akan disisipkan pada citra penampung. Sementara pada proses dekripsi digunakan metode *Huffman* yang dilanjutkan dengan modifikasi algoritma RSA dengan menggunakan *Chinese Remainder Theorem*, untuk mengurangi proses komputasi terhadap bilangan yang sangat besar. Hasil penelitian ini berupa citra gambar yang telah disisipi pesan rahasia yang terenkripsi , yang selanjutnya citra tersebut dibuka dengan menggunakan metode tersebut di atas. Pengujian dilakukan untuk membandingkan kecepatan dekripsi metode RSA standard an RSA CRT , tingkat keamanan pesan citra tersebut dan pengujian aplikasi.

Kata kunci: Citra, Kriptografi, Steganografi, RSA, LSB, CRT,*Huffman*.

Perpustakaan Universitas Budi Luhur

ABSTRACT

Cryptography and Steganography are methods os sending secret messages. In the cryptographic sent message is remain visible by others but in encrypted form. Meanwhile in steganography sent messages is hidden behind other media. Both combination would provide higher level security.LSB is one of the steganographic methods which quite well known. This method will replace certain bits of the image with the messages that will be hidden. While RSA is asymmetric cryptography method that is widely used. Asymmetric Cryptography is the cryptography which consist of public key and private key. The public key will be disseminated while the private key is only held by eligible. A message encrypted with the public key can only be opened with the associated private key .This research combines a 1024-bit 8 prime factors RSA Cryptography that have been modified with LSB Steganography. At the encryption process, we use RSA method that combining with the Huffman method to reduce the number of bits that will be inserted into cover image. Meanwhile in the decryption process, we use modified RSA algorithm using Chinese Remainder Theorem to reduce the computation process time to the very large number.Results of this research is an image that have been inserted an encrypted secret message, and then this stego image is opened by using the method above. The test will be conducted to compare decryption speed of standard RSA and RSA CRT, stego image security level and application testing.

Keywords : Image, Cryptography, Steganography, RSA, LSB, Huffman.

Perpustakaan Universitas Budi Luhur

KATA PENGANTAR

Assalamu'alaikum Warohmatullohi Wabarokatuh.

Segala puji dan syukur senantiasa terpanjatkan ke hadirat Allah SWT yang telah memberikan taufiq dan hidayah-Nya sehingga penulis dapat menyelesaikan proposal tesis yang berjudul "**Prototipe keamanan pesan rahasia dengan teknik kriptografi dan steganografi menggunakan algoritma LSB, RSA, CRT dan Huffman**". Shalawat serta salam senantiasa tercurah pada Rasulullah Muhammad SAW beserta keluarga shahabat dan umatnya yang setia hingga akhir zaman.

Dalam kesempatan ini penulis ingin menyampaikan rasa terima kasih kepada semua pihak yang telah yang telah memberikan bantuan atas penyelesaian penulisan proposal tesis ini, dengan segala ketulusan hati penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Orang tua serta keluargaku yang tercinta yang senantiasa memberikan kasih sayang, nasihat, dorongan serta doa yang tak pernah berhenti mengalir.
2. Bapak Prof. Dr. Moedjiono, M.Sc. sebagai Direktur Program Pascasarjana Universitas Budi Luhur.
3. Bapak Dr., Ir. Nazori AZ, M.T. sebagai Ketua Program Studi Magister Komputer Universitas Budi Luhur sekaligus sebagai pembimbing yang telah banyak memberikan saran dan masukan penyusunan proposal tesis ini. Terima kasih juga kepada beliau yang mengajarkan ilmu steganografi dan kriptografi kepada penulis selama perkuliahan Komputasi Terapan.
4. Bapak Prof. Dr. Moedjiono, M.Sc sebagai dosen penguji
5. Bapak Ir. Wendi Usino, MM., M.Sc., Ph.D sebagai dosen penguji
6. Bapak Mardi Hardjianto M.Kom yang mengajarkan metode *Huffman* kepada penulis selama perkuliahan Keamanan Sistem dan Jaringan Komputer.

Perpustakaan Universitas Budi Luhur

7. Bapak Ir. Teddy Mantoro M.sc.,Ph.D yang mengajarkan metode RSA dan pemrograman Android kepada penulis selama perkuliahan *Mobile Computing*.
8. Seluruh dosen, staff karyawan dan karyawati Universitas Budi Luhur yang telah memberikan bantuannya.
9. Seluruh rekan-rekan kuliah MKOM Universitas Budi Luhur.

Penulis menyadari penulisan tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun demi tercapainya penulisan yang lebih baik. Saran dan kritik dapat dikirimkan ke alamat e-mail msofjan70@gmail.com

Wassalamu'alaikum Warohmatullohi Wabarokatuh.

Jakarta, Agustus 2015

Moh. Sofjan

Perpustakaan Universitas Budi Luhur

DAFTAR ISI

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

DAFTAR GAMBAR

Perpustakaan Universitas Budi Luhur

DAFTAR TABEL

Perpustakaan Universitas Budi Luhur

Perpustakaan Universitas Budi Luhur

DAFTAR LAMPIRAN

Perpustakaan Universitas Budi Luhur

DAFTAR PUSTAKA

[Bateman 2008] Bateman, Philip, *Image Steganography and Steganalysis*, University of Surrey Guildford, United Kongdom, 2008.

[Hardjianto 2014] Hardjianto,Mardi, *Keamanan Sistem dan Jaringan Komputer*, Universitas Budi Luhur, Jakarta, 2014.

[Lee 2014] Lee,Holden, Oleg Muskarov, Teo Andrica, *Number Theory*, http://web.mit.edu/holden1, 2014.

[Mantoro 2014] Mantoro,Teddy, *Mobile Computing*, Universitas Budi Luhur, Jakarta, 2014.

[Marques 2011] Marques, Oge, *Practical Image and Video Processing Using Matlab*, John Wiley & Sons, Inc, New Jersey, 2011

[Maurya 2011] Maurya, Shweta, Vishal Shrwastava, *An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace*, IOSR Journal of Computer Engineering, India, 2014

[Nazori 2014] Nazori AZ, *Komputasi Terapan Lanjutan*, Universitas Budi Luhur, Jakarta, 2014.

[Rosen 1986] Rosen, Kenneth H, *Elementary Number Theory and Its Applications*, Addison-Wesley Publishing Company,Massachusetts, 1986.

[Sommerville 2003] Sommerville, Ian, *Software Engineering*, Erlangga , 2003.

[Stinson 2006] Stinson, Douglas R, *Cryptography – Theory and Practice*, Chapman & Hall/CRC, 3rd Edition, Ontario, 2006.

[Sugiyono 2007] Sugiyono, *Metode Penelitian Administrasi*, Bandung 2007.

[Wikipedia 2015] , *http://en.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search*, 2015.