MODEL PENGAMANAN DATA PADA FILE GAMBAR .BMP MENGGUNAKAN KOMBINASI METODE STEGANOGRAFI LSB DAN KRIPTOGRAFI AES 128

TESIS

Oleh:

DIKO MUHAMMAD ADAM

1411600297

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

JAKARTA
2016

MODEL PENGAMANAN DATA PADA FILE GAMBAR .BMP MENGGUNAKAN KOMBINASI METODE STEGANOGRAFI LSB DAN KRIPTOGRAFI AES 128

TESIS

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

Oleh:
DIKO MUHAMMAD ADAM
1411600297

PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2016

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa	:	Diko Muhammad Adam
Nomor Induk Mahasiswa	:	1411600297
Program Studi	:	Rekayasa Komputasi Terapan
Fakultas	:	Magister Komputer
Judul Tesis	:	MODEL PENGAMANAN DATA PADA FILE GAMBAR .BMP MENGGUNAKAN KOMBINASI METODE STEGANOGRAFI LSB DAN KRIPTOGRAFI AES 128

Jakarta, Februari 2016

Tim Penguji **Tanda Tangan**

Ketua,
Dr. Ir. Nazori AZ, M.T ..... 1.

Anggota,
Dr. M. Syafrullah, M. Kom, Msc. ..... 2.

Pembimbing Utama,
Prof. Dr. Moedjiono, Msc. .....

Ketua Program Studi,

.....

Dr. Ir. Nazori AZ, MT

PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertandatangan dibawah ini :

Nama : Diko Muhammad Adam.
NIM : 14116002 97
Program Studi : Rekayasa komputasi Terapan.
Fakultas : Magister komputer.

menyatakan bahwa TESIS yang berjudul:

Model Penyamaran Data pada file Gambar .BMP menggunakan kombinasi Metode Steganografi CSB dan Kriptografi AES 128.

1. merupakan hasil karya tulis ilmiah sendiri dan bkan 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 yang berlaku apabila dikemudian hari pernyataan ini tidak benar.

Jakarta, Februari 2016

METERAI TEMPEL 6000

(Diko Muhammad Adam)

ABSTRAK

Berbagai keunggulan yang dimiliki *internet* seperti, layananan tanpa terbatas waktu dan jarak atau biaya murah merupakan beberapa alasan pengguna memanfaatkannya. Bertumbuhnya pengguna, komunikasi masyarakat semakin sering dilakukan melalui *internet*. Dengan mengirim dan menerima pesan komunikasi melalui *internet* dilakukan, muncul kekhawatiran tentang keamanan dan kerahasian. Pertanyaan yang sering diutarakan seperti "Apakah pesan melalui *internet*, hanya pihak yang dituju mengetahuinya?". Beberapa metode dapat diterapkan untuk mengatasi kekhawatiran tersebut, pesan akan dimanipulasi sedemikian rupa, baik disembunyikan ataupun diacak. Penelitian ini bertujuan untuk membahas kombinasi metode tersebut. Hasil yang diharapkan yaitu, Steganografi (membuat *cover image*, langkah ini disebut proses *encoding*. Bertujuan untuk menyisipkan pesan "*plain text*" kedalam file gambar .bmp sebagai media penampung) dan Kriptografi (enkripsi menggunakan *key* enkripsi, kemudian data diacak menggunakan algoritma enkripsi. Dengan menerapkan metode ini, kemungkinan bagi pihak yang tidak diinginkan untuk dapat membaca data hampir tidak mungkin) yaitu, memberikan perlindungan yang lebih optimal dengan tujuan keamanan dan kerahasiaan pesan, saat pengiriman dilakukakan melalui jaringan.

Kata kunci : Steganografi LSB, Kriptografi AES, Keamanan pesan, Kerahasiaan pesan, metode kombinasi.

ABSTRACT

Various advantages of internet such as, low costs, no limit time service and distance, are some reasons why users use it. Growing users in community to communicate with each other via Internet also increased. By sending and receiving messages, this communications through the Internet are made. But then, there's concerns about security and confidentiality. Frequently asked questions such as " if you sent message through the Internet, wheter the only desired parties knows it?". Some methods can be applied to address such concerns, messages will be manipulated in such way, either hidden or scrambled. Research objectives is, discussing impact by combining such methods. Expected results, by combining methods of Steganography and Cryptography, is provides more optimal protection with objectives security and confidentiality of messages when delivered over network.

Keywords : Steganography LSB, AES cryptography, security messages, message confidentiality, combination methods.

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah SWT atas segala berkah, hikmah, hidayah dan karunia-Nya sehingga penulisan tesis dengan judul "MODEL PENGAMANAN DATA PADA FILE GAMBAR .BMP MENGGUNAKAN KOMBINASI METODE STEGANOGRAFI LSB DAN KRIPTOGRAFI AES 128" dapat diselesaikan.

Pada kesempatan ini, tidak lupa penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu, baik secara langsung ataupun tidak langsung dalam pembuatan tugas akhir ini hingga dapat diselesaikan. Dengan kerendahan hati, penulis juga ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah SWT. yang telah memberikan rahmat dan hidayah-Nya dalam menyelesaikan tugas akhir ini.
2. Orang tua Ibu Asdiwati, S.Sos. dan Bapak Alm. Asil, S.E., kakak Dika Rahmakartika Sari, S.Si, Apt., dan kakak Ivan Syahrizal, S.Kom. yang telah memberi doa, semangat dan kasih sayang tak terhingga.
3. Bapak Prof. Dr. Ir. Suryo Hapsoro Tri Utomo, Phd. selaku Rektor Universitas Budi Luhur.
4. Bapak Prof. Dr. Moedjiono, Msc. selaku Direktur Program Pascasarjana Universitas Budi Luhur sekaligus pembimbing penulisan tesis ini, terima kasih banyak bimbingan yang telah diberikan.
5. Bapak Dr. Ir. Nazori AZ, M.T selaku ketua program studi M.Kom Universitas Budi Luhur yang telah banyak memberikan ilmu yang bermanfaat.
6. Bapak Dr. M. Syafrullah, M. Kom, Msc. yang banyak membantu penulisan tesis ini.
7. Dwi Nurmayunita, S.E. yang tersayang dan tercinta selamanya, untuk selalu setia dan sabar melewati berbagai cerita hidup bersama.
8. Tidak lupa keluarga besar Kampleng bin Sirin dan keluarga besar H, Surdada, S.Pd yang terhormat ditempat, terima kasih doa dan semangatnya.
9. Dosen-dosen M.Kom, Sekretariat M.Kom dan Direktorat Universitas Budi Luhur.
10. Teman-teman seperjuangan selama menempuh program Pascasarjana di Universitas Budi Luhur Program Studi M.Kom angkatan 2014 kelas XK, Nico, Arief Maulana Sugiantoro, Ajar Rohamanu, Andi Jumardi dan teman-teman yang belum disebutkan.

Akhir kata dengan segala kerendahan hati penulis mohon maaf sebesar-besarnya atas segala kekurangan dalam penulisan tesis. Segala saran dan kritik yang bersifat membangun, sangat penulis harapkan untuk perbaikan di masa mendatang, besar harapan penulis agar tugas akhir ini dapat bermanfaat bagi seluruh pihak yang membutuhkan.

Jakarta, Februari 2016

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR TABEL

Tabel **Halaman**

DAFTAR LAMPIRAN

2. Menggunakan teknik-teknik lain kriptografi, steganografi, kompresi dan checksum dengan tujuan mencari teknik yang lebih baik.
3. Untuk mengimplementasikan aplikasi ini, perlu dilakukan pengadaan *hardware* dan *software* yang menunjang kinerja aplikasi,
4. Evaluasi sistem yang telah diuji harus dilakukan kemudian, bertujuan untuk menentukan apakah aplikasi dapat digunakan seperti seharusnya.

DAFTAR PUSTAKA

[Abdul 2011] Adnan Abdul-Aziz, Gutub,2010, "Pixel Indicator Technique for RGB Image Steganography", Journal Of Emerging Technologies In Web Intelligence, Vol.2, No.1, February 2010.

[Arjana 2012] Putu H. Arjana[1], Tri Puji Rahayu[2], Yakub Hariyanto[3], "Implementasi Enkripsi Data dengan Algoritma Vigenere Cipher", Yogyakarta: 2012.

[Aryasanti 2014] Agnes Aryasanti[1], Mardi Hardjianto[2], "Model Pengamanan Berkas Bank Soal dengan Metode Steganografi LSB Dan Kompresi", Jurnal TICOM Vol.2 No.2, 2014