

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

TESIS



Oleh:

DIKO MUHAMMAD ADAM

1411600297

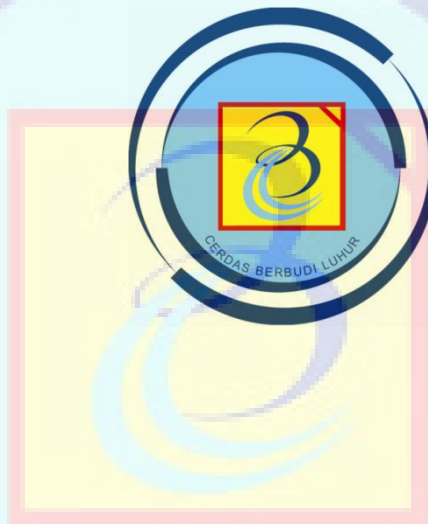
**PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2016**

**MODEL PENGAMANAN DATA PADA FILE GAMBAR .BMP
MENGUNAKAN 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

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

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 : 1411600297
Program Studi : Rekayasa Komputasi Temporal.
Fakultas : Magister Komputer.

menyatakan bahwa TESIS yang berjudul:

Model Pengamanan Data pada File Gambar .BMP
menggunakan kombinasi Metode Geometriografi CSB
dan Kriptografi AES 128.

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin 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



(Diko Muhammad Adam)

ABSTRAK

Berbagai keunggulan yang dimiliki *internet* seperti, layanan 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 kerahasiaan. 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 dilakukan 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, whether 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
ABSTRAK	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	iv
DAFTAR GAMBAR	vi
DAFTAR TABEL.....	vii
DAFTAR LAMPIRAN.....	viii
BAB I : PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Masalah Penelitian	3
1.2.1. Identifikasi Masalah.....	3
1.2.2. Batasan Masalah.	3
1.2.3. Rumusan Masalah	3
1.3. Tujuan dan Manfaat Penelitian	4
1.3.1. Tujuan Penelitian	4
1.3.2. Manfaat Penelitian	4
1.4. Daftar Istilah	4
BAB II : LANDASAN TEORI DAN KERANGKA KONSEP PENELITIAN.....	5
2.1. Tinjauan Pustaka	5
2.1.1. Steganografi.	5
2.1.1.1. Pengertian Steganografi.....	5
2.1.1.2. Proses Steganografi.....	5
2.1.1.3. Metode LSB(<i>Least Significant Bit</i>).....	6
2.1.2. Kriptografi.....	7
2.1.2.1. Pengertian Kriptografi.	7
2.1.2.2. Algoritma Kriptografi	8
2.1.2.3. Algoritma AES(<i>Advanced Encryption Standard</i>).....	11
2.1.2.4. Enkripsi AES	13
2.1.2.5. Dekripsi AES	19
2.1.3. ISO 9126	21
2.1.4. Pengujian <i>Black Box</i>	23
2.2. Tinjauan Studi	25
2.3. Tinjauan Objek Penelitian.....	29
2.4. Pola Pikir Pemecahan Masalah.....	29
2.5. Hipotesis	31
BAB III : METODOLOGI PENELITIAN	32
3.1. Metode Penelitian	32
3.2. Metode Pengumpulan Data.....	33
3.2.1. Metode Observasi	33
3.2.2. Metode Studi Pustaka	33
3.3. Instrumentasi.....	33
3.3.1. Perangkat Keras	33
3.3.2. Perangkat Lunak	34
3.4. Teknik Analisis	34
3.5. Langkah-langka Penelitian.....	35
3.5.1. Pemilihan Obyek.....	35
3.5.2. Perumusan Masalah	35
3.5.3. Studi Pustaka.....	35
3.5.4. Formulasi Hipotesis	36

3.5.5. Desain Pengembangan Sistem	36
3.5.5.1. Desain Sistem Steganografi	36
3.5.5.2. Desain Sistem Kriptografi	36
3.5.5.3. Desain Sistem Kombinasi	37
3.5.6. Pengujian dan Analisis	38
3.5.7. Penarikan Kesimpulan	38
3.5.8. Jadwal Penelitian	38
BAB IV : PEMBAHASAN HASIL PENELITIAN	39
4.1. Gambaran Umum Sistem	39
4.2. Alur Proses Sistem	40
4.2.1. Alur Proses <i>Encode</i> Steganografi	40
4.2.2. Alur Proses <i>Decode</i> Steganografi	40
4.2.3. Alur Proses <i>Encode</i> Kriptografi	41
4.2.4. Alur Proses <i>Decode</i> Kriptografi	41
4.3. Implementasi Sistem	42
4.3.1. Menu Utama	42
4.3.1.1. Menu Steganografi	43
4.3.1.2. Menu Kirim Pesan Kriptografi	43
4.3.1.3. Menu MD5Hash	44
4.3.2. Tampilan Layar Sisipkan Pesan	44
4.3.3. Tampilan Layar Ekstraksi Pesan	46
4.3.4. Tampilan Layar Kirim Pesan Kriptografi	48
4.3.4.1. Tampilan Layar Login Kirim Pesan Kriptografi	48
4.3.4.2. Tampilan Layar Enkripsi File	49
4.3.4.3. Tampilan Layar Dekripsi File	51
4.3.5. Tampilan Layar MD5Hash	52
4.4. Pengujian	54
4.4.1. Pengujian Black Box	54
4.4.1.1. Data yang digunakan untuk pengujian	54
4.4.1.2. Hasil pengujian	55
4.4.2. Pengujian ISO 9126	57
4.4.2.1. <i>Functionality</i>	58
4.4.2.2. <i>Reliability</i>	59
4.4.2.3. <i>Usability</i>	59
4.4.2.4. <i>Efficiency</i>	60
4.4.2.5. Rekapitulasi Aspek-Aspek Penilaian ISO 9216	60
4.5. Implikasi Penelitian	61
4.6. Rencana Implementasi	61
BAB IV : PENUTUP	63
5.1. Kesimpulan	63
5.2. Saran	64
DAFTAR PUSTAKA	65
LAMPIRAN	66
RIWAYAT HIDUP SINGKAT	82

DAFTAR GAMBAR

Gambar	Halaman
II.1 : Alur Proses Steganografi.....	6
II.2 : Proses enkripsi dan dekripsi.....	10
II.3 : Algoritma simetri	10
II.4 : Algoritma asimetri	11
II.5 : Proses Input Bytes, State Array, dan Output Bytes pada AES	13
II.6 : Ilustrasi Proses Enkripsi	14
II.7 : Transformasi <i>SubByte</i> pada S-Box.....	16
II.8 : Proses <i>SubByte</i>	16
II.9 : Transformasi <i>ShiftRows</i>	17
II.10 : Perkalian Matriks <i>Mixcolumns</i>	17
II.11 : Contoh Operasi Transformasi <i>Mixcolumns</i>	18
II.12 : Contoh Proses <i>AddRoundkey</i>	19
II.13 : Proses Dekripsi algoritma AES	19
II.14 : Transformasi <i>InvShiftRows</i>	20
II.15 : Proses <i>Inverse MixColumns</i>	21
II.16 : Tahapan proses pengujian <i>Black Box</i>	24
II.17 : Pola Pikir Pemecahan Masalah	30
III.1 : Tahapan Penelitian.....	35
III.2 : Alur proses kombinasi <i>encode</i>	37
III.3 : Alur proses kombinasi <i>decode</i>	38
IV.1 : Arsitektur sistem aplikasi	39
IV.2 : <i>Flowchart</i> alur proses <i>encode</i> steganografi	40
IV.3 : <i>Flowchart</i> alur proses <i>decode</i> steganografi	40
IV.4 : <i>Flowchart</i> alur proses <i>encode</i> kriptografi.....	41
IV.5 : <i>Flowchart</i> alur proses <i>decode</i> kriptografi.....	41
IV.6 : Menu utama	42
IV.7 : Menu Steganografi	43
IV.8 : Menu Kirim Pesan Kriptografi	43
IV.9 : Menu MD5Hash	44
IV.10 : Tampilan Layar Sisipkan Pesan	44
IV.11 : Tampilan Layar Sisipkan Pesan setelah proses	46
IV.12 : Tampilan Layar tombol Lihat Gambar	46
IV.13 : Tampilan Ekstraksi Pesan.....	47
IV.14 : Tampilan Layar Ekstraksi Pesan setelah proses	48
IV.15 : Tampilan Layar Login Kirim Pesan Kriptografi	49
IV.16 : Tampilan Layar Menu Enkripsi File	49
IV.17 : Tampilan Layar Enkripsi File.....	50
IV.18 : Proses Enkripsi selesai.....	51
IV.19 : Perbandingan file gambar yang sudah dienkripsi	51
IV.20 : Tampilan Layar Dekripsi File.....	52
IV.21 : Tampilan Layar Menu MD5Hash.....	53
IV.22 : Tampilan Layar Menu MD5Hash setelah proses	54
IV.23 : Data set <i>cover image</i>	54
IV.24 : Hasil pengecekan data pertama dengan metode checksum MD5Hash	56
IV.25 : Hasil pengecekan data kedua dengan metode checksum MD5Hash.....	56

DAFTAR TABEL

Tabel	Halaman
II.1 : Versi-versi AES	12
II.2 : Tabel <i>Plaintext</i> ke kunci.....	14
II.3 : Tabel Konversi Biner ke Heksadesimal	14
II.4 : Tabel <i>S-Box</i> Algoritma AES	15
II.5 : <i>Inverse S-Box</i> Algoritma AES	20
II.6 : Karakteristik Kualitas Software Sesuai ISO 9126	22
IV.1 : Hasil pengujian ukuran file setelah proses Steganografi.....	56
IV.2 : Hasil pengujian enkripsi file gambar stego	56
IV.3 : Hasil pengujian dekripsi file gambar stego	57
IV.4 : <i>Range</i> Kriteria Penilaian ISO 9216	59
IV.5 : Skor aspek <i>Functionality</i>	59
IV.6 : Skor aspek <i>Reliability</i>	60
IV.7 : Skor aspek <i>Usability</i>	60
IV.8 : Skor aspek <i>Efficiency</i>	61
IV.9 : Rekapitulasi Aspek-Aspek Penilaian ISO 9126	61
IV.10 : Kegiatan Implementasi Penelitian	62

DAFTAR LAMPIRAN

Lampiran	Halaman
1 Petunjuk Pengisian Kuesioner	67
2 Kuesioner Data Koresponden	68
3 Kuesioner Pengujian Dan Evaluasi Hasil Sistem Aplikasi	69
4 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi	70
5 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi	71
6 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi	72
7 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi	73
8 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi	74
9 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi	75
10 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi.....	76
11 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi.....	77
12 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi.....	78
13 Hasil Kuesioner Validasi Solusi Komponen Model Aplikasi.....	79
14 Source Code	80

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.



- [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