



SISTEM PENGKODEAN FILE DENGAN STEGANOGRAFI LSB

SKRIPSI

oleh

Ferry Refiandhi
NIM 071810101072

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2014



SISTEM PENGKODEAN FILE DENGAN STEGANOGRAFI LSB

SKRIPSI

Diajukan guna melengkapi dan memenuhi salah satu syarat
Untuk menyelesaikan Program Studi Matematika (S1)
Dan mencapai gelar Sarjana Sains

oleh

Ferry Refiandhi
NIM 071810101072

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER
2014

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

1. Ayahanda Safari dan Dasuki Suryanto, Ibunda Nafisah dan Sujiati yang tercinta, atas dorongan semangat, doa dan kasih sayangnya yang telah mengiringi selama menuntut ilmu;
2. adik-adikku Fahrur Rozi dan Fahrizal Rifqi yang tersayang;
3. istri tercinta Eva Noviana yang selalu menyemangatiku;
4. guru-guru sejak dari taman kanak-kanak sampai perguruan tinggi;
5. Almamater Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember; SMA Negeri 1 Ambulu; SMP Negeri 1 Ambulu; SDN Ambulu 03.

MOTTO

“Demi masa. Sungguh, manusia berada dalam kerugian, kecuali orang-orang yang beriman dan mengerjakan kebajikan serta saling menasihati untuk kebenaran dan saling menasihati untuk kesabaran.”
(Terjemahan Surat Al ‘Asr) *)

*) Bayan Qur’an. 2009. Al Qur’an Bayan. Depok: C.V. Bayan Quran

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

nama : Ferry Refiandhi

NIM : 071810101072

menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul “Sistem Pengkodean *File* Menggunakan RC4 dan MD4 pada Steganografi LSB” adalah benar-benar hasil karya sendiri, kecuali kutipan yang sudah saya sebutkan sumbernya, belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak mana pun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, Juni 2014

Yang menyatakan,

Ferry Refiandhi

NIM 071810101072

SKRIPSI

**SISTEM PENGKODEAN FILE MENGGUNAKAN RC4 DAN MD5
PADA STEGANOGRAFI LSB**

Oleh

Ferry Refiandhi
NIM 071810101072

Pembimbing

Dosen Pembimbing Utama : Kusbudiono S.Si., M.Si.

Dosen Pembimbing Anggota : Kiswara Agung Santoso, S.Si, M.Kom.

PENGESAHAN

Skripsi yang berjudul “Sistem Pengkodean *File* Menggunakan RC4 dan MD5 pada Steganografi LSB” telah diuji dan disahkan pada:

hari, tanggal :

tempat : Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas
Jember

Tim Penguji:

Ketua,

Sekretaris,

Kusbudiono, S.Si., M.Si.
NIP 19770430 2005 01 1 001

Kiswara Agung Santoso, S.Si., M.Kom.
NIP 19720907 1998 03 1 003

Penguji I,

Penguji II,

Drs. Rusli Hidayat, M.Sc.
NIP 196610121993031001

Kosala Dwidja Purnomo, S.Si. M.Si.
NIP 196908281998021001

Mengesahkan

Dekan,

Prof. Drs. Kusno, DEA, Ph.D.

RINGKASAN

Sistem Pengkodean *File* Menggunakan RC4 dan MD5 pada Steganografi LSB. Ferry Refiandhi, 071810101072; 2014: 131 halaman; Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Steganografi adalah pilihan yang baik untuk mengatasi kelemahan dari kriptografi. Teknik steganografi menggunakan dua media yang berbeda secara bersamaan yaitu *cover media* sebagai tempat untuk menyembunyikan sesuatu yang dirahasiakan dan *embeded media* sebagai data atau sesuatu yang disembunyikan. Hasil dari proses penyisipan ini adalah *stegomedia*. Pada skripsi ini, implementasi menggunakan algoritma RC4 (*Rivest Cipher 4*) dan MD5 (*Message Digest 5*) sebagai proses enkripsi dan dekripsi *file* dan sandi sebelum disisipkan dengan metode steganografi LSB (*Least Significant Bit*). Dengan menggabungkan teknik steganografi dan kriptografi ini diharapkan membantu upaya dalam peningkatan pengamanan terhadap penyimpanan dan pengiriman suatu *file*.

Pada analisis sistem pengkodean *file* dengan steganografi LSB ini digunakan citra pembawa dengan format citra bitmap 24 bit dengan berbagai ukuran. Pengujian dilakukan dengan menyisipkan beberapa tipe *file* dengan berbagai *format* ke dalam citra pembawa, menyisipkan satu *file* ke dalam beberapa citra pembawa, menyisipkan beberapa *file* sekaligus ke dalam citra pembawa dan pengujian dengan menggunakan sandi yang sama dan berbeda. Kemudian dari hasil pengujian tersebut, dilakukan perbandingan besar *file* antara *file* sebelum dan sesudah proses steganografi. Beberapa pengujian yang telah dilakukan analisa ukuran citra pembawa dan citra steganografi terjadi perubahan besar citra masing-masing sebesar 2 *byte*. Perubahan ini tidak terlalu besar, hal ini

dikarenakan pada proses penyisipan dengan metode LSB hanya pada bit terakhir yang digunakan, bit ini hanya bernilai 1 dan 0. Hal ini juga mempengaruhi nilai masing-masing piksel yang sedikit merubah kualitas citra pembawa sehingga *file* yang disembunyikan ke dalam citra pembawa tidak dapat dipersepsi oleh indrawi manusia. Pada pengujian dengan menggunakan sandi yang sama, *file* dapat didekripsi dengan baik, sedangkan pengujian dengan menggunakan sandi yang berbeda, *file* dapat didekripsi tetapi *file* tidak bisa dibaca komputer.

PRAKATA

Puji syukur kami yang sebesar-besarnya atas kehadiran Allah SWT yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan skripsi yang berjudul “Sistem Pengkodean *File* Menggunakan RC4 dan MD5 pada Steganografi LSB”. Skripsi ini disusun untuk memenuhi salah satu syarat untuk menyelesaikan pendidikan strata satu (S1) pada Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Penulis juga banyak mendapatkan bantuan dari berbagai pihak baik dalam penyelesaian skripsi ini. Oleh karena itu pada kesempatan ini, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. H. Abdul Khaliq Fadjuani, S.H. sebagai Guru pembimbing hidup;
2. Ayahanda Safari dan Dasuki Suryanto, Ibunda Nafisah dan Sujiati, Adik Fahrur Rozi, Adik Fahrizal Rifqi dan istri tercinta Eva Noviana, serta saudara-saudaraku yang telah memberikan bantuan doa dan semangatnya demi terselesaikannya skripsi ini;
3. Kusbudiono S.Si., M.Si. dan Kiswara Agung Santoso, S.Si, M.Kom., selaku dosen pembimbing yang telah membimbing selama penulisan skripsi ini;
4. Drs. Rusli Hidayat, M.Sc. dan Kosala Dwija Purnomo, S.Si., M.Si. selaku dosen penguji yang telah memberikan masukan dalam skripsi ini;
5. teman-teman “Akatsuki 07” khususnya Fitroh, Titi, Marihot, Silvi, Prastowo, Hasyim dan teman-teman yang lain;
6. serta seluruh pihak yang turut membantu kelancaran penyelesaian skripsi ini yang tidak dapat disebutkan satu-persatu.

Penulis menerima kritik dan saran dari semua pihak demi kesempurnaan skripsi ini. Akhirnya penulis berharap semoga skripsi ini dapat bermanfaat.

Jember, 24 September 2014

Penulis

DAFTAR ISI

	Halaman
HALAMAN SAMPUL	i
HALAMAN JUDUL	ii
HALAMAN PERSEMBAHAN	iii
HALAMAN MOTTO	iv
HALAMAN PERNYATAAN	v
HALAMAN PEMBIMBING	vi
HALAMAN PENGESAHAN	vii
RINGKASAN	viii
PRAKATA	x
DAFTAR ISI	xi
DAFTAR TABEL	xiv
DAFTAR GAMBAR	xv
DAFTAR LAMPIRAN	xvi
BAB 1. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan	4
1.5 Manfaat	4
BAB 2. TINJAUAN PUSTAKA	5
2.1 Dasar Komputer	5
2.1.1 Data	5
2.1.2 Bytes	5
2.1.3 Program Code dan Files	6
2.1.4 Ekstensi Files	7
2.2 Sistem Bilangan	8
2.2.1 Sistem Bilangan Heksadesimal di Komputer.....	10
2.2.2 Representasi File dengan Heksadesimal.....	11
2.3 Piksel	13

2.4 Citra Digital	14
2.4.1 Format Citra Digital	14
2.4.2 Format File Bitmap	14
2.5 Teori Bilangan	15
2.5.1 Bilangan Bulat	15
2.5.2 Aritmetika Modulo	16
2.6 Kriptografi	16
2.6.1 Definisi Kriptografi	16
2.6.2 Tujuan Kriptografi	17
2.6.3 Teknik Kriptografi	18
2.6.4 RC4 (<i>Rivest Cipher 4</i>)	19
2.7 Fungsi Hash	21
2.7.1 Definisi Fungsi <i>Hash</i>	21
2.7.2 MD5 (<i>Message Digest Algorithm 5</i>)	22
2.8 Steganografi	25
2.8.1 Definisi Steganografi	25
2.8.2 Kriteria Penyembunyian Data	25
2.8.3 Teknik Steganografi	26
2.8.4 LSB (<i>Least Significant Bit</i>)	27
BAB 3. METODE PENELITIAN	31
BAB 4. HASIL DAN PEMBAHASAN	34
4.1 Enkripsi	34
4.1.1 <i>File</i> Citra Pembawa dan <i>File</i> yang akan dikodekan	33
4.1.2 Enkripsi Sandi dengan Menggunakan Algoritma MD5	35
4.1.3 Enkripsi <i>File</i> dengan Menggunakan Algoritma RC4	41
4.1.4 Penyisipan dengan Metode Steganografi LSB	45
4.2 Dekripsi	47
4.2.1 Pengambilan Bit Terakhir Nilai Pixel	47
4.2.2 Dekripsi dengan Menggunakan RC4 dan MD5	48

4.3 Programasi	48
4.3.1 Tampilan Menu Utama	48
4.3.2 Tampilan Menu Enkripsi	49
4.3.3 Tampilan Menu Dekripsi	53
4.4 Analisa Hasil	55
4.4.1 Format Citra Pembawa dan <i>File</i> yang dikodekan	55
4.4.2 Analisa Besar Citra Pembawa dan Citra Steganografi	56
4.4.3 Analisa Gambar Citra Pembawa dan Citra Steganografi	63
4.4.3 Analisa Proses Enkripsi dan Dekripsi dengan Sandi	64
BAB 5. PENUTUP	71
5.1 Kesimpulan	71
5.2 Saran	71
DAFTAR PUSTAKA	73
LAMPIRAN	75

DAFTAR TABEL

	Halaman
Tabel 2.1 Tipe-tipe Dari <i>File</i> Komputer	8
Tabel 2.2 Hubungan Antara 1 Digit Heksadesimal Dengan 4 Digit Binari...	11
Tabel 2.3 Struktur File <i>Bitmap</i>	15
Tabel 2.4 Tabel nilai t_i	24
Tabel 4.1 Tabel kunci setelah diurutkan (heksadesimal).....	36
Tabel 4.2 Tabel nilai register penyangga	36
Tabel 4.3 Nilai register putaran pertama dengan fungsi FF.....	38
Tabel 4.4 Nilai register putaran pertama dengan fungsi GG	39
Tabel 4.5 Nilai register putaran pertama dengan fungsi HH	39
Tabel 4.6 Nilai register putaran pertama dengan fungsi II.....	40
Tabel 4.7 Konversi plainteks dari heksadesimal ke binari.....	44
Tabel 4.8 Proses XOR plainteks dan kunci.....	44
Tabel 4.9 Representasi warna citra pembawa dalam desimal.....	45
Tabel 4.10 Representasi warna citra pembawa dalam biner	45
Tabel 4.11 Representasi biner citra steganografi	46
Tabel 4.12 Representasi warna citra steganografi dalam desimal	46
Tabel 4.13 Proses XOR bit LSB citra steganografi dan kunci.....	48
Tabel 4.13 Besar <i>file</i> citra pembawa	55
Tabel 4.14 Tipe-tipe dari <i>file</i> yang akan dienkripsi	56
Tabel 4.15 Besar citra pembawa, <i>file</i> dan citra steganografi	57
Tabel 4.16 Presentase perubahan besar <i>file</i>	58
Tabel 4.17 Besar <i>file</i> , citra pembawa dan citra steganografi	59
Tabel 4.18 Presentase perubahan besar <i>file</i>	60
Tabel 4.19 Besar citra pembawa, <i>file</i> dan citra steganografi	61
Tabel 4.20 Presentase perubahan besar <i>file</i> dengan beberap <i>file</i> disisipkan ..	62

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Diagram Proses Enkripsi dan Deskripsi.....	17
Gambar 2.2 Fungsi <i>Hash</i>	22
Gambar 2.3 Satu Operasi MD5	22
Gambar 2.4 Representasi Biner.....	28
Gambar 4.1 <i>File</i> citra pembawa	34
Gambar 4.2 Representasi citra pembawa 3×4 piksel	35
Gambar 4.3 Representasi citra steganografi 3×4 piksel.....	47
Gambar 4.4 Tampilan menu utama	49
Gambar 4.5 Tampilan menu program enkripsi	50
Gambar 4.6 Tampilan setelah “Buka Citra Penampung”	51
Gambar 4.7 Tampilan setelah “Tambah <i>File</i> Rahasia”	52
Gambar 4.8 Tampilan setelah proses enkripsi selesai.....	53
Gambar 4.9 Tampilan menu program dekripsi	53
Gambar 4.10 Tampilan setelah “Buka <i>StegoImage</i> ”	54
Gambar 4.11 Tampilan setelah “Ekstrak <i>File</i> Rahasia”	55
Gambar 4.12 Citra pembawa dan citra steganografi dengan 5 <i>file</i> rahasia	63
Gambar 4.13 Citra pembawa dan citra steganografi dengan 9 <i>file</i> rahasia	63
Gambar 4.14 Citra pembawa dan citra steganografi dengan 13 <i>file</i> rahasia ..	64
Gambar 4.15 Gambar ketika sandi dimasukkan	65
Gambar 4.16 Tampilan setelah proses enkripsi selesai.....	66
Gambar 4.17 Tampilan setelah proses dekripsi selesai.....	67
Gambar 4.18 Perbandingan <i>file</i> citra dengan sandi yang sama.....	67
Gambar 4.19 Perbandingan <i>file</i> dokumen dengan sandi yang sama	68
Gambar 4.20 Perbandingan <i>file</i> citra dengan sandi yang berbeda	69
Gambar 4.21 Perbandingan <i>file</i> dokumen dengan sandi yang berbeda	69

DAFTAR LAMPIRAN

	Halaman
A. Kode Program Forms	75
B. Kode Program Class Module	83
C. Kode Program Module	127