

**PENYEMBUNYIAN PESAN RAHASIA TERENKRIPSI
PADA BERKAS AUDIO MP3 MENGGUNAKAN
METODE *PARITY CODING***

SKRIPSI

Sebagai salah satu syarat untuk memperoleh
gelar Sarjana dalam bidang Komputer



Disusun Oleh :
RIZKY SETYO PAMBUDI
NIM. 0810963024

**PROGRAM STUDI INFORMATIKA / ILMU KOMPUTER
PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2013**

LEMBAR PERSETUJUAN

PENYEMBUNYIAN PESAN RAHASIA TERENKRIPSI PADA BERKAS AUDIO MP3 MENGGUNAKAN METODE *PARITY CODING*

SKRIPSI

Sebagai salah satu syarat untuk memperoleh
gelar Sarjana dalam bidang Komputer



Disusun Oleh :

RIZKY SETYO PAMBUDI

NIM. 0810963024

Telah diperiksa dan disetujui oleh :

Pembimbing I,

Pembimbing II,

Imam Cholissodin, S.Si., M.Kom.
NIK. 850719 16 1 1 0422

Edy Santoso, S.Si., M.Kom.
NIP. 19740414 200312 1 004

LEMBAR PENGESAHAN

**PENYEMBUNYIAN PESAN RAHASIA TERENKRIPSI PADA BERKAS
AUDIO MP3 MENGGUNAKAN METODE *PARITY CODING***

SKRIPSI

Sebagai salah satu syarat untuk memperoleh
gelar Sarjana dalam bidang Komputer

Disusun Oleh:

RIZKY SETYO PAMBUDI

NIM. 0810963024

Skripsi ini telah diuji dan dinyatakan lulus pada tanggal 19 Juli 2013

Penguji I

Penguji II

Suprpto, S.T., M.T.
NIP. 19710727 199603 1 001

Indriati, S.T., M.Kom.
NIK. 831013 06 1 2 0035

Penguji III

Novanto Yudistira, S.Kom., M.Sc.
NIK. 831110 16 1 1 0425

Mengetahui

Ketua Program Studi Teknik Informatika

Drs. Marji, M.T.
NIP. 19670801 199203 1 001

PERNYATAAN ORISINALITAS SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Rizky Setyo Pambudi

NIM : 0810963024

Program Studi : Informatika / Ilmu Komputer

Penulis skripsi berjudul : Penyembunyian Pesan Rahasia Terenkripsi Pada Berkas Audio MP3 Menggunakan Metode *Parity Coding*

Dengan ini menyatakan bahwa :

1. Isi dari Skripsi yang saya buat adalah benar-benar karya sendiri dan tidak menjiplak karya orang lain, selain nama-nama yang termaktub di isi dan tertulis di daftar pustaka dalam Skripsi ini.
2. Apabila dikemudian hari ternyata Skripsi yang saya tulis terbukti hasil jiplakan, maka saya akan bersedia menanggung segala resiko yang akan saya terima.

Demikian pernyataan ini dibuat dengan segala kesadaran.

Malang, Juli 2013

Rizky Setyo Pambudi

NIM. 0810963024

KATA PENGANTAR

Segala puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat serta hidayah-Nya, sehingga penyusun dapat menyelesaikan laporan skripsi dengan judul **“PENYEMBUNYIAN PESAN RAHASIA TERENKRIPSI PADA BERKAS AUDIO MP3 MENGGUNAKAN METODE *PARITY CODING*”** yang disusun guna memenuhi syarat menyelesaikan studi Ilmu Komputer Universitas Brawijaya dengan lancar.

Terselesaikannya laporan penelitian skripsi ini tentu tidak lepas dari bantuan beberapa pihak, oleh karena itu penyusun ingin menyampaikan ucapan terima kasih kepada :

1. Bapak Imam Cholissodin, S.Si., M.Kom., selaku Dosen Pembimbing I yang telah bersedia memberikan bimbingan, arahan, motivasi, serta meluangkan waktunya sehingga proposal skripsi ini dapat terselesaikan.
2. Bapak Edy Santoso, S.Si., M.Kom., selaku Dosen Pembimbing II yang telah memberikan pengetahuan, bimbingan, dan nasihat untuk kesempurnaan penulisan proposal skripsi ini.
3. Drs. Mardji, M.T., selaku Ketua Prodi Teknik Informatika / Ilmu Komputer Universitas Brawijaya.
4. Moh. Fathoni dan Kasmi selaku orang tua penulis, serta keluarga yang selalu memberikan nasihat, semangat, dukungan, dan doa, serta motivasi sehingga penulis dapat menyelesaikan skripsi ini dengan baik.
5. Segenap Bapak dan Ibu dosen yang telah mendidik dan mengajarkan ilmunya kepada penulis selama menempuh pendidikan.
6. Staf administrasi Program Studi Ilmu Komputer, Program Teknologi Informasi dan Ilmu Komputer.
7. Dian Cahyono, Nur Hadi Sulaiman, Alfian Fardiansyah, dan Khoiron Nisaa yang telah memberikan bantuan dan arahan kepada penulis, serta mengajari penulis tentang hal-hal yang berkaitan dengan skripsi ini.
8. Muhammad Ishak Nurdiansyah, Heikal Mahendra Rukmana, Aditya Permana, Nita Adi Pangestuti, dan Resthy Kushardiana yang senantiasa

memberikan semangat dan motivasi kepada penulis, serta telah membagi segala keceriaan dan kebahagiaan selama penulis menyelesaikan skripsi ini.

9. Teman-teman Program Teknologi Informasi dan Ilmu Komputer angkatan 2008 yang selalu memberikan bantuan dan motivasinya demi kelancaran skripsi ini.
10. Semua pihak yang telah membantu terselesaikannya skripsi ini yang tidak dapat kami sebutkan satu per satu.

Semoga skripsi ini bermanfaat bagi pembaca sekalian, Akhirnya, penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan dan mengandung banyak kekurangan, sehingga dengan segala kerendahan hati penulis mengharapkan kritik dan saran membangun dari pembaca.

Malang, Juli 2013

Penulis



PENYEMBUNYIAN PESAN RAHASIA TERENKRIPSI PADA BERKAS AUDIO MP3 MENGGUNAKAN METODE *PARITY CODING*

ABSTRAK

Komunikasi telah menjadi bagian dari kehidupan manusia dan menjadi hal yang sangat penting seiring berkembangnya waktu. Dalam berkomunikasi, ada kalanya informasi yang dipertukarkan bersifat penting dan rahasia sehingga tidak boleh diketahui oleh pihak yang tidak berkepentingan. Teknik yang dapat digunakan untuk meningkatkan keamanan data adalah steganografi dan kriptografi.

Dalam penelitian pesan teks yang akan disembunyikan terlebih dahulu dienkripsi menggunakan algoritma kriptografi RSA untuk selanjutnya disembunyikan ke dalam berkas audio MP3 menggunakan metode *parity coding*. Selanjutnya akan dilakukan pengujian terhadap kualitas audio dengan menghitung nilai *Peak Signal to Noise Ratio* (PSNR) dan pengujian ketahanan steganografi terhadap manipulasi berupa penambahan derau *gaussian*.

Hasil pengujian terhadap kualitas audio MP3 yang telah disisipi pesan menunjukkan bahwa semakin besar ukuran pesan yang disisipkan, maka terjadi penurunan nilai PSNR, namun disisi lain semakin panjang ukuran kunci yang digunakan untuk enkripsi pesan, maka terjadi kenaikan nilai PSNR. Selain itu, semakin besar kapasitas audio MP3 sebagai media penampung, maka nilai PSNR-nya semakin tinggi. Sedangkan hasil pengujian ketahanan steganografi menunjukkan bahwa steganografi *parity coding* tidak memiliki ketahanan terhadap manipulasi berupa penambahan derau *gaussian*. Pesan yang disembunyikan pada berkas MP3 tidak dapat diungkapkan kembali ketika intensitas derau *gaussian* yang ditambahkan di atas 0.25 %.

Kata kunci : Steganografi *Parity Coding*, Kriptografi RSA, Audio MP3, *Peak Signal to Noise Ratio* (PSNR).

THE HIDING OF ENCRYPTED SECRET MESSAGE INTO MP3 AUDIO FILE USING PARITY CODING METHOD

ABSTRACT

Communication has been a part of human life and becomes very important over time. In communicating, sometimes, important and secret informations are exchanged that should not be known by unauthorized parties. Steganography and cryptography are technique that can be used to improve data security.

In this thesis, text message will be encrypted using RSA cryptography algorithm and then embedded into MP3 audio file using parity coding steganography. Furthermore, the test will be carried out on audio quality by calculating the value of Peak Signal to Noise Ratio (PSNR). The other test will be carried out on steganography's robustness by add gaussian noise on the audio MP3 that text message has been embedded on it.

The audio quality test result shows that the larger size of the text message that is embedded, the lower value of PSNR gained, in other side, the longer the encryption key, the higher value of PSNR gained. Moreover, the larger size of MP3 audio file, the higher value of PSNR gained. Meanwhile, steganography's robustness test shows that parity coding steganography has no robustness to the gaussian noise addition. The hidden message in MP3 audio can not retrieved when the intensity of noise is added up to 0.25 %.

Keyword : Parity Coding Steganography, RSA Cryptography, MP3 Audio, Peak Signal to Noise Ratio (PSNR).

DAFTAR ISI

LEMBAR PERSETUJUAN	i
LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS SKRIPSI.....	iii
KATA PENGANTAR.....	iv
ABSTRAK	vi
ABSTRACT	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xiv
DAFTAR SOURCE CODE	xv
DAFTAR LAMPIRAN	xvi
 BAB I	
PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	4
 BAB II	
TINJAUAN PUSTAKA	6
2.1 Steganografi	6
2.1.1 Pengertian Steganografi.....	6
2.1.2 Kriteria Steganografi.....	7
2.1.3 Audio Steganografi	8
2.2 Metode <i>Parity Coding</i>	9
2.2.1 <i>Parity Bit</i>	9

2.2.2	<i>Parity Coding</i>	10
2.2.3	<i>LSB (Least Significant Bit)</i>	13
2.3	Kriptografi	13
2.3.1	Pengertian Kriptografi	13
2.3.2	Komponen Kriptografi	14
2.3.3	Kriptografi Asimetris	15
2.4	Metode Kriptografi RSA	16
2.4.1	Pengertian RSA	16
2.4.2	Konsep Matematis Pada RSA	17
2.4.3	Enkripsi dan Dekripsi Pada RSA	21
2.5	<i>Sieve of Eratosthenes</i>	22
2.6	Audio MP3	24
2.6.1	Pengertian Audio	24
2.6.2	Format Berkas Audio	25
2.6.3	MPEG Audio Layer 3 (MP3)	25
2.6.4	Struktur Berkas MP3	27
2.7	PSNR (Peak Signal to Noise Ratio)	33
2.7.1	MSE (Mean Square Error)	34
2.8	Bit Error Rate	34
2.9	Penambahan Derau	35
 BAB III		
METODOLOGI DAN PERANCANGAN		36
3.1	Deskripsi Umum Sistem	37
3.2	Perancangan Sistem	37
3.2.1	Pembangkitan Bilangan Prima	42
3.2.2	Enkripsi	44
3.2.3	Penyisipan Informasi Jumlah Region	46
3.2.4	Embedding	48
3.2.5	Parity Bit	51
3.2.6	Pengambilan Informasi Jumlah Region	52
3.2.7	Retrieving	55

3.2.8	Dekripsi.....	58
3.3	Perhitungan Manual	59
3.3.1	Pembentukan Kunci	59
3.3.2	Penyembunyian Pesan	61
3.3.2.1	Enkripsi	61
3.3.2.2	<i>Embedding</i>	64
3.3.3	Pengungkapan Pesan	66
3.3.3.1	<i>Retrieving</i>	66
3.3.3.2	Dekripsi	69
3.3.4	PSNR (<i>Peak Signal to Noise Ratio</i>)	72
3.4	Perancangan Uji Coba dan Analisis	75
3.5	Perancangan Antarmuka.....	77
 BAB IV		
IMPLEMENTASI		82
4.1	Lingkungan Implementasi.....	82
4.1.1	Lingkungan Perangkat Keras.....	82
4.1.2	Lingkungan Perangkat Lunak	82
4.2	Implementasi Program	82
4.2.1	Proses Penyembunyian Pesan.....	83
4.2.1.1	Implementasi Pembacaan Pesan	83
4.2.1.2	Implementasi Pembangkitan Kunci	84
4.2.1.3	Implementasi Enkripsi.....	86
4.2.1.4	Implementasi Pembacaan Berkas Audio	88
4.2.1.5	Implementasi Penyisipan Informasi Jumlah Region	89
4.2.1.6	Implementasi <i>Embedding</i>	91
4.2.2	Proses Pengungkapan Pesan.....	94
4.2.2.1	Implementasi Pengambilan Informasi Jumlah Region	95
4.2.2.2	Implementasi <i>Retrieving</i>	97
4.2.2.3	Implementasi Dekripsi	99
4.2.3	Proses Pengujian	101

4.2.3.1	Implemetasi PSNR	102
4.2.3.2	Implementasi <i>Bit Error Rate</i>	104

BAB V

PEMBAHASAN	105
------------------	-----

5.1	Implementasi Uji Coba	105
-----	-----------------------------	-----

5.1.1	Implementasi Pengujian Kualitas Berkas MP3	106
-------	--	-----

5.1.2	Implementasi Pengujian Ketahanan Steganografi <i>Parity Coding</i>	107
-------	---	-----

5.2	Hasil Pengujian dan Pembahasan.....	107
-----	-------------------------------------	-----

5.2.1	Hasil dan Pembahasan Pengujian Kualitas Berkas MP3	108
-------	--	-----

5.2.2	Hasil dan Pembahasan Pengujian Ketahanan Steganografi <i>Parity Coding</i>	121
-------	---	-----

BAB VI

PENUTUP.....	126
--------------	-----

6.1	Kesimpulan	126
-----	------------------	-----

6.2	Saran.....	126
-----	------------	-----

DAFTAR PUSTAKA	128
----------------------	-----

DAFTAR GAMBAR

Gambar 2.1 Proses Steganografi	7
Gambar 2.2 Pembagian Region Pada Pesan 24 bit.....	11
Gambar 2.3 Gambaran Umum Proses Kriptografi	14
Gambar 2.4 Skema Kriptografi Asimetris.....	16
Gambar 2.5 Struktur Berkas MP3	27
Gambar 2.6 Struktur <i>Frame</i> MP3.....	27
Gambar 2.7 Struktur <i>Header</i> MP3	28
Gambar 3.1 Alur Penelitian.....	36
Gambar 3.2 Diagram Alir Proses Pembentukan Kunci.....	38
Gambar 3.3 Diagram Alir Proses Penyembunyian.....	40
Gambar 3.4 Diagram Alir Proses Pengungkapan.....	42
Gambar 3.5 Diagram Alir Proses Pembangkitan Bilangan Prima.....	44
Gambar 3.6 Diagram Alir Proses Enkripsi.....	46
Gambar 3.7 Diagram Alir Proses Penyisipan Informasi Jumlah Region	48
Gambar 3.8 Diagram Alir Proses <i>Embedding</i>	51
Gambar 3.9 Diagram Alir Proses <i>Parity Bit</i>	52
Gambar 3.10 Diagram Alir Proses Pengambilan Informasi Jumlah Region.....	54
Gambar 3.11 Diagram Alir Proses <i>Retrieving</i>	57
Gambar 3.12 Diagram Alir Proses Dekripsi.....	59
Gambar 3.13 Rancangan antarmuka Penyembunyian Pesan.....	78
Gambar 3.14 Rancangan Antarmuka Pengungkapan Pesan.....	79
Gambar 3.15 Rancangan Antarmuka Pengujian.....	80
Gambar 4.1 Antarmuka Penyembunyian Pesan	83
Gambar 4.2 Antarmuka Pengungkapan Pesan	95
Gambar 4.3 Antarmuka Pengujian	102
Gambar 5.1 Grafik Nilai PSNR Skenario Pengujian 1.....	109
Gambar 5.2 Grafik Nilai PSNR Skenario Pengujian 2.....	111
Gambar 5.3 Grafik Nilai PSNR Skenario Pengujian 3.....	113
Gambar 5.4 Grafik Nilai PSNR Skenario Pengujian 4.....	115
Gambar 5.5 Grafik Nilai PSNR Skenario Pengujian 5.....	117

Gambar 5.6 Grafik Nilai Rata-rata PSNR Skenario Pengujian..... 120



DAFTAR TABEL

Tabel 2.1 Ilustrasi <i>parity coding</i>	12
Tabel 2.2 Klasifikasi audio berdasarkan frekuensi.....	24
Tabel 2.3 Fungsi dan kebutuhan bit <i>header</i>	29
Tabel 2.4 Bit <i>id</i> 2 bit.....	30
Tabel 2.5 Bit <i>layer</i>	30
Tabel 2.6 <i>Bitrate</i>	30
Tabel 2.7 Bit frekuensi	31
Tabel 2.8 Bit <i>mode</i>	32
Tabel 3.1 Representasi biner dari <i>ciphertext</i>	64
Tabel 3.2 Perhitungan <i>parity</i> bit pada region ke-1 dan ke-2	65
Tabel 3.3 Penyisipan bit pesan ke MP3 <i>carrier</i>	65
Tabel 3.4 Pengungkapan bit pesan dari <i>stego</i> MP3.....	67
Tabel 3.5 Pengubahan pesan ke bentuk karakter.....	68
Tabel 3.6 Tabel perhitungan MSE.....	72
Tabel 3.7 Tabel contoh pengujian nilai PSNR	76
Tabel 3.8 Tabel contoh pengujian ketahanan steganografi <i>parity coding</i>	77
Tabel 5.1 Daftar berkas MP3	105
Tabel 5.2 Daftar berkas teks.....	105
Tabel 5.3 Daftar kunci.....	106
Tabel 5.4 Hasil pengujian nilai PSNR pada skenario pengujian 1.....	108
Tabel 5.5 Hasil pengujian nilai PSNR pada skenario pengujian 2.....	110
Tabel 5.6 Hasil pengujian nilai PSNR pada skenario pengujian 3.....	112
Tabel 5.7 Hasil pengujian nilai PSNR pada skenario pengujian 4.....	114
Tabel 5.8 Hasil pengujian nilai PSNR pada skenario pengujian 5.....	116
Tabel 5.9 Nilai terbesar rasio ukuran pesan terhadap ukuran berkas MP3 pada seluruh skenario pengujian	118
Tabel 5.10 Hasil pengujian 1 ketahanan steganografi <i>parity coding</i>	121
Tabel 5.11 Hasil pengujian 2 ketahanan steganografi <i>parity coding</i>	122
Tabel 5.12 Hasil pengujian 3 ketahanan steganografi <i>parity coding</i>	123
Tabel 5.13 Hasil pengujian 4 ketahanan steganografi <i>parity coding</i>	123

DAFTAR SOURCE CODE

Source code 4.1 Implementasi pembacaan berkas bertipe teks (.txt)	84
Source code 4.2 Implementasi pembangkitan dua buah bilangan prima.....	85
Source code 4.3 Implementasi pembentukan kunci	86
Source code 4.4 Implementasi enkripsi	88
Source code 4.5 Implementasi pembacaan berkas audio.....	89
Source code 4.6 Pengubahan pesan ke dalam bentuk biner	90
Source code 4.7 Pengubahan informasi panjang ke dalam bentuk biner	90
Source code 4.8 Implementasi penyisipan informasi jumlah region	91
Source code 4.9 Implementasi <i>embedding</i>	93
Source code 4.10 Implementasi penghitungan <i>parity</i> bit	93
Source code 4.11 Implementasi pembentukan berkas audio MP3	94
Source code 4.12 Implementasi penyisipan informasi jumlah region	97
Source code 4.13 Implementasi <i>retrieving</i>	98
Source code 4.14 Pengubahan bit pesan ke pesan	99
Source code 4.15 Implementasi dekripsi	100
Source code 4.16 Implementasi pembentukan berkas bertipe teks (.txt)	101
Source code 4.17 Implementasi pengujian PSNR	104
Source code 4.18 Implementasi pengujian <i>bit error rate</i>	104

DAFTAR LAMPIRAN

Lampiran 1 <i>Ciphertext</i> hasil enkripsi	131
Lampiran 2 Pengujian ketahanan steganografi <i>parity coding</i>	132
Lampiran 3 Berkas teks asli dan hasil pengungkapan pada pengujian ketahanan steganografi <i>parity coding</i>	137

