

DAFTAR ISI

HALAMAN PENGESAHAN.....	iii
PERNYATAAN.....	iv
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xii
INTISARI.....	xiii
ABSTRACT.....	xii
BAB I.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	5
1.6 Keaslian Penelitian.....	5
1.7 Metodologi Penelitian	5
1.8 Sistematika Penulisan.....	6
BAB II TINJAUAN PUSTAKA.....	8
BAB III LANDASAN TEORI.....	13
3.1 Kriptografi.....	13
3.1.1 Mekanisme Kriptografi	14
3.1.2 Enkripsi dengan <i>Data Encryption Standard</i> (DES).....	14
3.1.3 Pemrosesan Kunci.....	16
3.1.4 Permutasi Awal pada 64 bit data.....	19
3.1.5 Dekripsi algoritma <i>Data Encryption Standard</i> (DES).....	27
3.1.6 Algoritma <i>Triple DES</i>	29
3.2 Steganografi	31
3.2.1 Penyisipan pada steganografi.....	31
3.2.2 Ekstraksi pada steganografi	32
3.3 <i>Parity Coding</i>	33
3.4 Format wave.....	37
3.5 PSNR (<i>Peak Signal to Noise Ratio</i>)	38
BAB IV ANALISIS DAN RANCANGAN	39
4.1 Gambaran Umum Metode	39
4.2 Proses <i>padding</i> pada <i>plaintext</i>	41
4.3 Proses <i>padding</i> pada kunci	42
4.4 Enkripsi <i>Triple DES</i>	43
4.5 Dekripsi <i>Triple DES</i>	47
4.6 Penyisipan <i>ciphertext</i> dan kunci 3DES Pada <i>File Audio</i>	48
4.7 Ekstraksi Dari <i>File Audio</i>	50
4.7 RANCANGAN PENGUJIAN	52
BAB V IMPLEMENTASI.....	56
5.1 Implementasi Aplikasi.....	56
5.1.1 Implementasi proses enkripsi.....	56

5.1.2 Implementasi proses dekripsi.....	65
5.1.3. Implementasi proses Penyisipan	66
5.24 Implementasi proses Ekstraksi.....	71
5.25 Implementasi PSNR.....	73
BAB VI HASIL DAN PEMBAHASAN	74
6.1 Pengujian.....	74
6.1.2 Pengujian pada proses dekripsi.	75
6.1.3 Pengujian pada proses penyisipan.....	76
6.1.4 Pengujian pada proses ekstraksi <i>ciphertext</i> dan kunci 3DES.....	78
BAB VII PENUTUP.....	84
7.1 Kesimpulan	84
7.2 Saran	84
DAFTAR PUSTAKA	85

DAFTAR GAMBAR

Gambar 3.1 Konsep kerja enkripsi DES secara umum (Singh, 2013)	15
Gambar 3.2 Pemrosesan kunci (Narula, 2014)	19
Gambar 3.3. Skema umum enkripsi DES (Stalling, 2011)	23
Gambar 3.4 Satu putaran algoritma DES (Stalling, 2011)	25
Gambar 3.5 <i>Calculation of $f(R, K)$</i> (Narula, 2014)	26
Gambar 3.6. <i>Feistel Decryption 16 round</i> (Stalling, 2011)	28
Gambar 3.7 Proses enkripsi <i>Triple DES</i> menggunakan 3 DES (Singh, 2013)	30
Gambar 3.8 Gambar diagram untuk audio steganografi (Mahajan, 2014).	31
Gambar 3.9 Diagram penyisipan pada steganografi (Brute dkk, 2013)	32
Gambar 3.10 Diagram ekstraksi pada steganografi (Burate dkk, 2013)	32
Gambar 3.11 <i>Prosedure parity coding</i> (Brute dkk, 2013)	35
Gambar 3.12 format the canonical wave (Cheng, 2007)	37
Gambar 4. 1 Gambaran umum sistem	40
Gambar 4. 2 Proses Padding pada <i>plaintext</i>	41
Gambar 4. 3 Proses <i>Padding</i> pada kunci	42
Gambar 4. 4 Rancangan umum enkripsi algoritma DES	44
Gambar 4. 5 Skema satu putaran enkripsi DES	45
Gambar 4. 6 Skema Proses enkripsi 3DES	46
Gambar 4. 7 Skema proses dekripsi 3DES	47
Gambar 4. 8 Skema Proses Penyisipan <i>ciphertext</i>	48
Gambar 4. 9 Skema Proses Penyisipan kunci 3DES	49
Gambar 4. 10 Skema proses ekstraksi <i>ciphertext</i>	51
Gambar 4. 11 Skema proses ekstraksi kunci	52
Gambar 5. 1 Implementasi kode <i>padding</i> untuk <i>plaintext</i>	56
Gambar 5. 2 Implementasi kode padding untuk key 1	57
Gambar 5. 3 Implementasi kode untuk membagi <i>plaintext</i>	58
Gambar 5. 4 Implementasi kode konversi <i>plaintext</i> menjadi biner	58
Gambar 5. 5 Implementasi kode enkripsi 3DES	59
Gambar 5. 6 Prosedur CatatKunci(<i>Key</i>)	60
Gambar 5. 7 Prosedur TentukanCdanD()	60
Gambar 5. 8 Prosedur TentukanK()	61
Gambar 5. 9 Prosedur InitialPermutedPlaintext()	61
Gambar 5. 10 Prosedur <i>CreateL0R0</i> ()	61
Gambar 5. 11 Prosedur <i>ExpansiR</i> ()	62
Gambar 5. 12 Prosedur <i>XOR_ExpansiR_dan_K</i> ()	62
Gambar 5. 13 Prosedur Break XOR IntoB()	63
Gambar 5. 14 Prosedur <i>SubstitutionBox_dari_B</i> ()	63
Gambar 5. 15 Prosedur <i>PermutasiDariSubstitusi</i> ()	63
Gambar 5. 16 Prosedur <i>Create_LdanR</i> ()	64
Gambar 5. 17 <i>ReverseLR(R16L16)</i>	64
Gambar 5. 18 Prosedur <i>FinalPermutation</i> ()	64
Gambar 5. 19 Implementasi <i>code</i> proses <i>decrypt</i>	65
Gambar 5. 20 Implementasi kode pemilihan <i>file carrier</i>	67
Gambar 5. 21 Implementasi kode prosedur <i>IsiKarakterPure</i> ()	68

Gambar 5. 22 Implementasi kode prosedur IsiDataPure().....	68
Gambar 5. 23 Implementasi kode prosedur IsiAmpPure()	69
Gambar 5. 24 Implementasi kode prosedur IsiAmpBinPure().....	69
Gambar 5. 25 Implementasi kode proses penyisipan.....	70
Gambar 5. 26 Implementasi kode proses penyimpanan.....	71
Gambar 5. 27 Implementasi kode ambil <i>file audio</i> untuk ekstraksi.....	72
Gambar 5. 28 Implementasi code ekstraksi pesan	72
Gambar 5. 29 Kode program untuk pengujian menggunakan PSNR	73
Gambar 6. 1 Cuplikan <i>plaintext</i>	74
Gambar 6. 2 Cuplikan <i>ciphertext</i>	75
Gambar 6. 3 <i>Plaintext</i> hasil dekripsi	75
Gambar 6. 4 Proses penyisipan <i>ciphertext</i>	76
Gambar 6. 5 Proses penyimpanan pesan ke <i>audio carrier</i>	77
Gambar 6. 6 Proses penyisipan kunci	77
Gambar 6. 7 Proses penyimpanan kunci ke <i>audio carrier</i>	78
Gambar 6. 8 Ekstraksi <i>ciphertext</i> dan kunci 3DES.....	79
Gambar 6. 9 Grafik penyisipan teks 128 bit pada audio 25456 bit.....	79
Gambar 6. 10 Grafik penyisipan teks 128 bit pada audio 730108 bit.....	80
Gambar 6. 11 Grafik penyisipan teks 25408 bit pada audio 25456 bit.....	81
Gambar 6. 12 Tampilan jika pesan melebihi kapasitas audio.....	83

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka	11
Tabel 3 1 <i>Permuted Choice</i> (PC-1) (Stalling, 2011)	17
Tabel 3 2 <i>Schedule of left shifts</i> (Stalling, 2011)	17
Tabel 3 3 <i>Permuted Choice Two</i> (PC-2) (Stalling, 2011)	18
Tabel 3 4 <i>Initial Permutation</i> (IP) (Stalling 2011)	20
Tabel 3 5 <i>Expansion E</i> (Stalling, 2011)	20
Tabel 3 6 S-Box 1 (Stalling, 2011)	21
Tabel 3 7 <i>Permutation Function</i> (P) (Stalling, 2011)	22
Tabel 3 8 <i>Inverse Intial Permutation</i> (IP-1) (Stalling, 2011)	22
Tabel 3 9 Tabel ASCII	36
Tabel 4. 1 Data pengujian teks 10752 bit pada beberapa audio	53
Tabel 4. 2 Data pengujian teks pada audio 267198 bit	53
Tabel 4. 3 Data pengujian teks pada audio 25456 bit	54
Tabel 4. 4 Data pengujian teks pada audio 589828 bit	54
Tabel 4. 5 Data pengujian teks pada audio 624524 bit	54
Tabel 4. 6 Data pengujian teks pada audio 572900 bit	55
Tabel 6. 1 Data pengujian teks 10752 bit pada beberapa audio	81
Tabel 6. 2 Hasil PSNR untuk pengujian pada audio 267198 bit	82
Tabel 6. 3 Hasil PSNR untuk pengujian pada audio 925456 bit	82
Tabel 6. 4 Hasil PSNR untuk pengujian pada audio 589828 bit	82
Tabel 6. 5 Hasil PSNR untuk pengujian pada audio 624524 bit	83
Tabel 6. 6 Hasil PSNR untuk pengujian pada audio 572900 bit	83