DAFTAR ISI

HALAMAN JUDUL i
HALAMAN PENGESAHAN PEMBIMBING ii
HALAMAN PENGESAHAN PENGUJI iii
SURAT KARYA ASLI TUGAS AKHIR iv
PERNYATAAN BEBAS PLAGIASI v
ABSTRAK vi
KATA PENGANTAR vii
DAFTAR ISI viii
DAFTAR TABEL x
DAFTAR GAMBAR xi
DAFTAR MODUL PROGRAM xii
BAB I PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 3
1.5 Manfaat Penelitian 3
1.6 Metodologi Penelitian dan Pengembangan Sistem 4
1.6.1 Metodologi Penelitian 4
1.6.2 Metode Pengembangan Sistem 4
1.7 Sistematika Penulisan 4
BAB II TINJAUAN LITERATUR 6
2.1 Citra Digital 6
2.1.1 Citra Warna 7
2.1.2 Format File Citra Digital 8
2.2 Steganografi 9
2.2.1 Uji Steganografi Kriteria *Fidelity* 9
2.2.2 Uji Steganografi Kriteria *Robustness* 10
2.3 Metode Redundant Pattern Encoding 10
2.4 Metode Advanced Encryption Standard (AES) 11
2.4.1 Transformasi *SubBytes()* 14
2.4.2 Transformasi *ShiftRows()* 15
2.4.3 Transformasi *MixColumns()* 16
2.4.4 Transformasi *AddRoundKey()* 17
2.5 Penelitian Sebelumnya 18
BAB III METODOLOGI PENELITIAN DAN PENGEMBANGAN SISTEM 22
3.1 Metodologi Penelitian 22
3.2 Metode Pengumpulan Data 22
3.3 Metode Pengembangan dan Perancangan Sistem 23
3.3.1 Analisis Kebutuhan Sistem 23

3.3.2 Pemodelan Rancangan Sistem / *Quick Design* 24
3.3.3 Perancangan Proses 25
3.3.4 Perancangan Antarmuka 28
3.4 Eksperimen dan Pengujian Metode 31
3.4.1 Metode Advanced Encryption Standard (AES) 31
3.4.2 Metode Redundant Pattern Encoding (RPE) 35
3.4.3 Perhitungan MSE dan PSNR 37
3.4.4 Perancangan Pengujian 38
BAB IV HASIL PENGUJIAN DAN PEMBAHASAN 40
4.1 Hasil Implementasi Penelitian 40
4.1.1 Halaman Enkripsi dan *Encode* 41
4.1.2 Halaman Dekripsi dan *Decode* 46
4.2 Pengujian dan Pembahasan Analisis *Robustness* dan *Fidelity* 48
4.2.1 Pengujian Robustness 49
4.2.2 Pengujian Fidelity 54
BAB V KESIMPULAN DAN SARAN 64
5.1 Kesimpulan 64
5.2 Saran 64
DAFTAR PUSTAKA 66

DAFTAR TABEL

Tabel 2. 1 Penetapan panjang kunci AES 12
Tabel 2. 2 Tabel *S-box* 14
Tabel 2. 3 Nilai *RC*[*j*] dalam heksadesimal 18
Tabel 2. 4 Penelitian Sebelumnya 18
Tabel 2. 5 Lanjutan Penelitian Sebelumnya 19
Tabel 2. 6 Lanjutan Penelitian Sebelumnya 20
Tabel 2. 7 Lanjutan Penelitian Sebelumnya 21
Tabel 3. 1 Konversi Nilai RGB menjadi Biner 36
Tabel 3. 2 Penyelesaian Penyisipan Pesan 37
Tabel 4. 1 Tabel Skenario Pengujian dengan *hidden text* berbeda 49
Tabel 4. 2 Pengujian *Robustness* dengan *plaintext* lebih 25 karakter 49
Tabel 4. 3 Lanjutan Pengujian *Robustness* dengan *plaintext* lebih 25 karakter 50
Tabel 4. 4 Pengujian *Robustness* dengan *plaintext* 20 hingga 25 karakter 50
Tabel 4. 5 Pengujian *Robustness* dengan *plaintext* 10 karakter 50
Tabel 4. 6 Pengujian *Robustness* pada seluruh *Stego Image* 51
Tabel 4. 7 Pengujian *Fidelity* pada *Stego Image* 54
Tabel 4. 8 Lanjutan Pengujian *Fidelity* pada *Stego Image* 55
Tabel 4. 9 Lanjutan Pengujian *Fidelity* pada *Stego Image* 56
Tabel 4. 10 Lanjutan Pengujian *Fidelity* pada *Stego Image* 57
Tabel 4. 11 Lanjutan Pengujian *Fidelity* pada *Stego Image* 58
Tabel 4. 12 Lanjutan Pengujian *Fidelity* pada *Stego Image* 59

DAFTAR GAMBAR

Gambar 2. 1 Sistem Koordinat yang dipergunakan untuk mewakili citra 6
Gambar 2. 2 Skema RGB dalam entuk kubus 7
Gambar 2. 3 Kubus warna dengan 24 bit 8
Gambar 2. 4 Steganografi dengan *watermark* yang meluas menjadi atribut dari gambar sampul dengan tanda air: "Invisible Man" © 1997, Neil F Johnson. 11
Gambar 2. 5 Diagram proses enkripsi 13
Gambar 2. 6 Ilustrasi array state 13
Gambar 2. 7 Ilustrasi urutan penyalinan *array state* 13
Gambar 2. 8 Proses Subtitusi 23 menjadi 26 15
Gambar 2. 9 Pergeseran secara *wrapping* 15
Gambar 2. 10 Contoh Transformasi *ShiftRows()* 15
Gambar 2. 11 Perkalian matriks state 16
Gambar 2. 12 Hasil *XOR* antara *state* dan *round key* 17
Gambar 3. 1 Alur Rancangan Penelitian 22
Gambar 3. 2 Metode *Prototyping (Pressman, 2010)* 23
Gambar 3. 3 Arsitektur perancangan aplikasi 24
Gambar 3. 4 Struktur Menu Aplikasi Utama 25
Gambar 3. 5 *Flowchart* Enkripsi dan *Embedding* 26
Gambar 3. 6 *Flowchart* Perhitungan MSE dan PSNR 27
Gambar 3. 7 *Flowchart* Proses Dekripsi dan *Decode* 28
Gambar 3. 8 *Wireframe* Tampilan Awal 29
Gambar 3. 9 *Wireframe* Tampilan Enkripsi dan *Encode* 29
Gambar 3. 10 *Wireframe* Tampilan Hasil Enkripsi dan *Encode* 30
Gambar 3. 11 *Wireframe* Tampilan Deskripsi 30
Gambar 3. 12 Citra Digital Lena 35
Gambar 4. 1 Halaman Utama pada Aplikasi 40
Gambar 4. 2 Halaman Enkripsi dengan *Input* Pesan dan Gambar 41
Gambar 4. 3 *Output* Hasil Penyisipan dan Enkripsi Pesan 42
Gambar 4. 4 Hasil *Plaintext* dari Proses *Decode Stego Image* 46
Gambar 4. 5 Citra *cover* yang digunakan (peppers.jpg, pinguin.png, baboon.bmp) 48
Gambar 4. 6 Pengujian *cropping* horizontal bawah 52
Gambar 4. 7 Pengujian *cropping* vertikal kanan 53
Gambar 4. 8 Grafik rata-rata presentase keberhasilan ekstraksi 53
Gambar 4. 9 Citra stego kode A terdapat *noise* yang ditunjuk panah merah 59
Gambar 4. 10 Citra stego kode B terdapat *noise* yang ditunjuk panah merah 60
Gambar 4. 11 Citra stego kode C terdapat *noise* yang ditunjuk panah merah 60
Gambar 4. 12 Perbandingan citra *cover* dan citra stego berformat .png 61
Gambar 4. 13 Perbandingan citra asli dan citra stego berformat .bmp 62
Gambar 4. 14 Grafik nilai PSNR seluruh citra stego yang diujikan 63

DAFTAR MODUL PROGRAM

Modul Program 4. 1 *Import Library*..... 41
Modul Program 4. 2 Proses *routing* menuju halaman utama 41
Modul Program 4. 3 *Routing* Tampilan Halaman *Encode* dan POST Data 43
Modul Program 4. 4 Modul Enkripsi Pesan dengan AES 43
Modul Program 4. 5 Modul Penyimpanan Citra dan Pemanggilan Fungsi *Encode*..... 44
Modul Program 4. 6 Fungsi *hidding data* 45
Modul Program 4. 7 Modul Program Perhitungan MSE dan PSNR..... 45
Modul Program 4. 8 *Routing* tampilan halaman dekripsi dan POST data 47
Modul Program 4. 9 Proses *decode* pesan dari gambar..... 47
Modul Program 4. 10 Proses dekripsi pesan 47