

DAFTAR ISI

PRAKATA.....	v
INTISARI.....	xii
ABSTRACT	xiii
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 Metode Penelitian	4
1.7 Sistematika Penelitian	5
BAB II TINJAUAN PUSTAKA.....	7
BAB III LANDASAN TEORI	10
3.1 Kriptografi	10
3.2 Enkripsi.....	11
3.3 AES	12
3.4 RSA	18
3.5 Chaos	20
3.6 Analisis Statistik	31
BAB IV ANALISIS DAN PERANCANGAN SISTEM	34
4.1 Deskripsi Umum Sistem.....	34
4.2 Analisis Data.....	35
4.3 Rancangan Program	35
4.4 Rancangan Algoritma	38
4.5 Rancangan Pengujian	51
BAB V IMPLEMENTASI	56
5.1 Spesifikasi Sistem	56
5.2 Implementasi Data Citra.....	56
5.3 Implementasi Pembuatan Kunci	57
5.4 Implementasi Algoritma	59
5.5 Implementasi Pengujian	65
BAB VI HASIL PENELITIAN DAN PEMBAHASAN	70
6.1 Hasil Enkripsi dan Dekripsi.....	70
6.2 Enkripsi dan Dekripsi AES.....	70
6.3 Enkripsi dan Dekripsi RSA	72
6.4 Enkripsi dan Dekripsi Chaos	73
6.5 Evaluasi Data Citra	74
6.6 Pengujian Waktu Komputasi	79

BAB VII KESIMPULAN DAN SARAN	82
7.1 Kesimpulan	82
7.2 Saran	82

DAFTAR TABEL

Tabel 2.1 Perbandingan penelitian terdahulu dengan penulis	8
Tabel 4.1 Contoh hasil urutan chaotic.....	47
Tabel 4.2 Contoh hasil pengurutan chaotic.	47
Tabel 4.3 Contoh hasil pembuatan urutan difusi.	48
Tabel 4.4 Contoh hasil cipher tahap pertama.	48
Tabel 4.5 Hasil enkripsi tahap kedua.	49
Tabel 4.6 Pembuatan kunci untuk dekripsi	49
Tabel 4.7 Contoh proses dekripsi tahap pertama.....	50
Tabel 4.8 Hasil nilai pixel dan hasil pengurutan chaotic.	50
Tabel 4.9 Contoh hasil final proses dekripsi.	51
Tabel 4.10 Hasil pemasangan pixel secara horizontal	53
Tabel 4.11 Hasil pemasangan pixel secara vertikal	54
Tabel 4.12 Hasil pemasangan pixel secara diagonal.....	54
Tabel 6.1 Hasil nilai simpang baku citra hasil enkripsi	76
Tabel 6.2 Hasil korelasi koefisien citra.....	76
Tabel 6.3 Hasil MSE dan PSNR AES dan Chaos.....	77
Tabel 6.4 Hasil MSE dan PSNR RSA	78
Tabel 6.13 Hasil waktu komputasi AES, RSA, dan Chaos	79

DAFTAR GAMBAR

Gambar 3.1 Proses enkripsi menggunakan algoritma AES	13
Gambar 3.2 Tabel S-Box (Paar & Pelzl, 2010)	14
Gambar 3.3 Ilustrasi Shift Rows	15
Gambar 3.4 Formula Perkalian Mix Columns	15
Gambar 3.5 Proses dekripsi menggunakan algoritma AES	16
Gambar 3.6 Formula Perkalian Mix Columns	17
Gambar 3.7 Ilustrasi Inverse Shift Rows	17
Gambar 3.8 Tabel Inverse S-Box (Paar & Pelzl, 2010).....	18
Gambar 3.9 Contoh macam representasi bentuk chaotic maps.....	22
Gambar 3.10 Diagram Bifurikasi Logistic Map.....	25
Gambar 3.11 Bifurikasi Sine Map.....	26
Gambar 3.12 Bifurikasi Chebyshev Map.....	27
Gambar 3.13 Bifurifikasi Logistic Logistic Map	28
Gambar 3.14 Diagram Bifurikasi SSM dan CCM.....	29
Gambar 3.15 Proses Enkripsi Menggunakan Chaotic Map	30
Gambar 4.1 Ilustrasi perubahan bentuk citra	36
Pseudocode 4.1 Proses perubahan bentuk citra.....	37
Pseudocode 4.2 Proses hasil proses enkripsi ke bentuk citra	38
Gambar 4.2 Contoh kunci dalam bentuk 128-bit	39
Gambar 4.3 Contoh proses RotWord dan Substitusi Byte.....	39
Gambar 4.4 Contoh proses xor dengan rcon	40
Gambar 4.5 Contoh proses penentuan W4.....	40
Gambar 4.6 Contoh penentuan W-n	41
Gambar 4.7 Contoh proses pembentukan W8-W11	42
Gambar 4.8 Contoh proses AddRoundKey	43
Gambar 4.9 Contoh proses SubstitutionBytes	43
Gambar 4.10 Contoh proses ShiftRows.....	43
Gambar 4.11 Contoh proses MixColumn	43

Gambar 4.12 Contoh proses InverseShiftRows	44
Gambar 4.13 Contoh proses InverseMixColumns	45
Gambar 4.14 Contoh sampel data untuk histogram	52
Gambar 4.15 Hasil histogram pada gambar 4.4	52
Gambar 4.16 Ilustrasi nilai citra pada channel biru.....	53
Gambar 4.17 Contoh citra asli dan dekripsi dalam bentuk nilai pixel.....	55
Gambar 5.1 Cuplikan implementasi masukan citra	57
Gambar 5.2 Implementasi perubahan bentuk citra	57
Gambar 5.3 Implementasi pembuatan kunci AES	58
Gambar 5.4 Implementasi pembuatan kunci RSA	58
Gambar 5.5 Implementasi pembuatan kunci Chaos LLM	59
Gambar 5.6 Implementasi membagi data berdasarkan limit.....	59
Gambar 5.7 Implementasi enkripsi AES	60
Gambar 5.8 Implementasi dekripsi AES	60
Gambar 5.9 Implementasi pengambilan kunci privat RSA	61
Gambar 5.10 Implementasi pengambilan kunci publik RSA.....	61
Gambar 5.11 Implementasi enkripsi RSA	62
Gambar 5.12 Implementasi dekripsi RSA	62
Gambar 5.13 Implementasi penggabungan nilai pixel	63
Gambar 5.14 Implementasi pengurutan nilai chaotic	63
Gambar 5.15 Implementasi confusion dan pergeseran nilai	64
Gambar 5.16 Implementasi dekripsi Chaos	64
Gambar 5.17 Implementasi pembalikan nilai difusi.....	64
Gambar 5.18 Implementasi pembalikan nilai confusion	65
Gambar 5.19 Implementasi pembalikan nilai urutan chaos	65
Gambar 5.20 Implementasi histogram.....	66
Gambar 5.21 Implementasi perhitungan waktu komputasi.....	66
Gambar 5.22 Implementasi pemasangan citra secara horizontal	66
Gambar 5.23 Implementasi pemasangan citra secara vertikal	67
Gambar 5.24 Implementasi pemasangan citra secara diagonal.....	67
Gambar 5.25 Implementasi perhitungan korelasi.....	68

Gambar 5.26 Implementasi perhitungan PSNR	68
Gambar 6.1 Data citra 256x256 (a) asli, (b) hasil enkripsi, dan (c) dekripsi	70
Gambar 6.2 Data citra berukuran 2048x2048 (a) asli, (b) hasil enkripsi, dan (c) hasil dekripsi.....	71
Gambar 6.3 Data citra berukuran 1024x1024 (a) asli, (b) hasil enkripsi, dan (c) hasil dekripsi.....	71
Gambar 6.4 Data citra berukuran 512x512 (a) asli, (b) hasil enkripsi, dan (c) dekripsi.....	71
Gambar 6.5 Citra asli (a, d, g, j), hasil enkripsi (b, e, h, k) dan dekripsi (c, f, i, l) menggunakan RSA	72
Gambar 6.6 Citra asli (a, d, g, j), hasil enkripsi (b, e, h, k) dan dekripsi (c, f, i, l) menggunakan Chaos	73
Gambar 6.7 Data citra asli dan histogram.....	74
Gambar 6.8 Histogram data citra hasil enkripsi AES	74
Gambar 6.9 Histogram data citra hasil enkripsi RSA.....	75
Gambar 6.10 Histogram data citra hasil enkripsi Chaos.....	75
Gambar 6.11 Perubahan data hasil dekripsi RSA.....	79
Gambar 6.12 Grafik waktu enkripsi AES, RSA, dan Chaos	80
Gambar 6.13 Grafik waktu dekripsi AES, RSA, dan Chaos	80
Gambar 6.14 Grafik waktu dekripsi AES dan Chaos	81