

DAFTAR ISI

Halaman Judul	ii
Halaman Pengesahan	iii
Halaman Pernyataan	iv
Halaman Persembahan	v
PRAKATA	vi
DAFTAR ISTILAH	xxi
INTISARI	xxii
ABSTRACT	xxiv
I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	4
1.3 Tujuan Penelitian	4
1.4 Manfaat Penelitian	5
1.5 Batasan Masalah	5
1.6 Kontribusi Penelitian	6
II TINJAUAN PUSTAKA	8
2.1 Tinjauan Umum Metode Kompresi	8
2.2 Tinjauan Umum Metode Kriptografi	9
2.2.1 Model Keamanan Data Citra Menggunakan Metode Kriptografi Simetris	10
2.2.2 Model Keamanan Data Citra Menggunakan Metode Kriptografi Asimetris	13
2.3 Tinjauan Umum Penggabungan Metode Kompresi dan Kriptografi	15
2.3.1 Metode Kriptografi-Kompresi	15
2.3.2 Metode Kompresi-Kriptografi	16
2.3.3 Perbandingan Metode Penggabungan Kompresi dan Kriptografi	20
2.4 Tinjauan Umum Metode Penyisipan Pesan	23
III LANDASAN TEORI	25
3.1 Representasi Data Citra Digital	25
3.2 Metode Kompresi	27
3.2.1 Kompresi Citra Berbasis <i>Wavelet</i>	28
3.2.2 Kuantisasi	31
3.2.3 Koding	32
3.3 Metode Kriptografi	33
3.3.1 Metode Kriptografi Simetris	34
3.3.2 Metode Kriptografi Asimetris	38
3.3.3 Manajemen Kunci	40
3.4 Metode Penyisipan <i>End of File</i> (EoF)	43
3.5 Parameter Analisis Model	44
3.5.1 Uji Visual	44
3.5.2 Uji <i>Run Test</i>	44
3.5.3 Analisis Histogram	45

3.5.4	Analisis <i>Differential</i> (Sensitifitas Kunci)	45
3.5.5	Analisis Entropi	46
3.5.6	Analisis Korelasi	46
3.5.7	Kualitas Kompresi	47
3.5.8	Redudansi Data Citra	47
3.5.9	Analisis Kompleksitas Algoritme	48
IV	METODOLOGI PENELITIAN	50
4.1	Kerangka Penelitian	50
4.2	Model yang Dikembangkan	51
4.3	Data Penelitian	52
4.3.1	Data Citra untuk Menguji Kinerja Model Pembangkit Kunci Simetris	52
4.3.2	Data Citra untuk Menguji Parameter Nilai Kuantisasi dan Filter Wavelet yang Tepat untuk Model Kriptosistem yang Dikembangkan	54
4.3.3	Data Citra untuk Menguji Kinerja Model Kriptosistem yang Dikembangkan	55
4.4	Rancangan Pengujian Model	55
4.4.1	Rancangan Pengujian Kinerja Model Pembangkit Kunci Simetris	56
4.4.2	Rancangan Pengujian Kinerja Model Kriptosistem	57
4.4.3	Rancangan Pengujian Kompleksitas Algoritme Model Kriptosistem	59
4.4.4	Rancangan Pengujian Perbandingan Kinerja Keamanan Model Kriptosistem yang Dikembangkan dengan Penelitian Sebelumnya	59
V	MODEL PEMBANGKIT KUNCI SIMETRIS DAN KUNCI SESI	60
5.1	Model Pembangkit Kunci Simetris pada Citra <i>Grayscale</i>	61
5.1.1	Transformasi DWT 2D pada Citra <i>Grayscale</i>	61
5.1.2	Fungsi <i>Arnold Cat Map</i> (ACM) pada Citra <i>Grayscale</i>	63
5.1.3	Pembentukan Vektor a pada Citra <i>Grayscale</i>	65
5.1.4	Operasi <i>Cipher Block Chaining</i> (CBC)	66
5.2	Model Pembangkit Kunci Simetris pada Citra Warna	67
5.2.1	Transformasi Data Citra Warna	68
5.2.2	Transformasi DWT 2D pada Citra Warna	69
5.2.3	Fungsi <i>Arnold Cat Map</i> (ACM) pada Data Citra Warna	69
5.2.4	Pembentukan Vektor a	70
5.2.5	Operasi <i>Cipher Block Chaining</i> (CBC) pada Data Citra Warna	71
5.3	Algoritme Pembangkit Kunci Sesi	72
5.3.1	Algoritme Pembangkit Kunci Sesi KG_1	73
5.3.2	Algoritme Pembangkit Kunci Sesi KG_2	74
5.3.3	Algoritme Pembangkit Kunci Sesi KG_3	76
5.3.4	Algoritme Pembangkit Kunci Sesi KG_4	77
5.3.5	Algoritme Pembangkit Kunci Aliran	79

VI	MODEL PENGAMANAN DATA CITRA DAN PENDISTRIBUSIAN KUNCI SIMETRIS	81
6.1	Model Kompresi-Kriptografi pada Citra <i>Grayscale</i>	83
6.1.1	Metode Kompresi pada Citra <i>Grayscale</i>	83
6.1.2	Metode kriptografi pada Citra <i>Grayscale</i>	88
6.2	Model Pendistribusian Kunci Simetris pada Citra <i>Grayscale</i>	99
6.2.1	Metode Pengamanan Kunci Simetris pada Citra <i>Grayscale</i>	100
6.2.2	Metode Penyisipan Kunci Simetris pada citra <i>Grayscale</i>	104
6.3	Model Kompresi-Kriptografi pada Data Citra Warna	107
6.3.1	Metode Kompresi pada Citra Warna	108
6.3.2	Metode Kriptografi pada Citra Warna	112
6.4	Model Pendistribusian Kunci Simetris pada Citra Warna	118
6.4.1	Metode Pengamanan Kunci Simetris	119
6.4.2	Metode Penyisipan Kunci Simetris pada Citra Warna	121
VII	MODEL REKONSTRUKSI <i>CIPHER IMAGE</i>	124
7.1	Model Rekonstruksi <i>Cipher Image Grayscale</i>	124
7.1.1	Proses Pemisahan <i>Cipher Image</i> dengan <i>Cipher Key</i>	124
7.1.2	Model Dekripsi-Verifikasi Kunci Simetris pada Citra <i>Grayscale</i>	126
7.1.3	Proses Pemisahan <i>Plain Key</i> pada Citra <i>Grayscale</i>	129
7.1.4	Proses Pembangkit Kunci Sesi pada Citra <i>Grayscale</i>	129
7.1.5	Metode Dekripsi pada Citra <i>Grayscale</i>	130
7.1.6	Metode Rekonstruksi pada Citra <i>Grayscale</i>	139
7.2	Model Rekonstruksi <i>Cipher Image</i> Warna	144
7.2.1	Transformasi Ruang Warna	144
7.2.2	Proses Pemisahan <i>Cipher Image</i> dengan <i>Cipher Key</i> dan <i>Padding</i>	146
7.2.3	Model Dekripsi-Verifikasi Kunci Simetris pada Citra Warna	148
7.2.4	Proses Pemisahan <i>Plain Key</i> pada Citra Warna	149
7.2.5	Proses Pembangkit Kunci Sesi pada Citra Warna	149
7.2.6	Metode Dekripsi pada Citra Warna	150
7.2.7	Metode Rekonstruksi pada Citra Warna	155
VIII	ANALISIS DAN PEMBAHASAN	160
8.1	Analisis Kinerja Model Pembangkit Kunci Simetris	160
8.1.1	Hasil Pengujian Pengaruh Kualitas Data Citra Terhadap Kunci Simetris yang Terbentuk	160
8.1.2	Hasil Pengujian Secara Visual Keacakan Kunci Simetris yang Terbentuk	165
8.1.3	Hasil Pengujian Keacakan Kunci Simetris yang Terbentuk Menggunakan Uji <i>Run-Test</i>	167
8.2	Analisis Kinerja Model Kriptosistem	169
8.2.1	Hasil Pengujian Parameter Nilai Kuantisasi dan Jenis Filter Wavelet yang tepat	169
8.2.2	Hasil Pengujian Kinerja Keamanan dari Model Kriptosistem	172
8.2.3	Hasil Pengujian Kinerja Model Dekripsi-Rekonstruksi	182

8.3	Analisis Kompleksitas Algoritme Model Kriptosistem	183
8.3.1	Analisis Ruang Kunci	183
8.3.2	Analisis Kompleksitas Waktu	184
8.4	Perbandingan Kinerja Keamanan Model Kriptosistem yang Dikem- bangkan dengan Penelitian Sebelumnya	191
8.4.1	Hasil Perbandingan Model Kriptosistem Berbasis <i>Chaos</i> de- ngan Menggunakan Penggabungan Model Kompresi dengan Tanpa Kompresi	191
8.4.2	Hasil Perbandingan Model Kompresi-Kriptografi Selektif yang Diimplementasikan pada Citra Grayscale	194
8.4.3	Hasil Perbandingan Model Kompresi-Kriptografi Selektif yang Diimplementasikan pada Citra Warna	197
IX	PENUTUP	199
9.1	Kesimpulan	199
9.2	Saran	200
	LAMPIRAN	208
A	Pengujian Parameter Nilai Kuantisasi dan Filter Wavelet	209
B	Hasil Pengukuran Secara Statistik pada Citra Uji	214
B.1	Hasil Pengukuran pada Citra <i>Grayscale</i>	214
B.2	Hasil Pengukuran pada Citra Warna	216
C	Hasil Pengukuran Efektifitas Metode End of File (EoF)	220
D	Kompleksitas Waktu	224
D.1	Kompleksitas Waktu Algoritme Pembangkit Kunci Simetris	224
D.2	Kompleksitas Waktu Model Kompresi-Kriptografi	229
D.3	Kompleksitas Waktu Model Pendistribusian Kunci Simetris	236
D.4	Model Dekripsi Cipher Image	238
D.5	Model Rekonstruksi Cipher Image	241