

DAFTAR ISI

HALAMAN PENGESAHAN.....	i
PERNYATAAN.....	ii
HALAMAN MOTTO DAN PERSEMBAHAN.....	iii
PRAKATA.....	iv
DAFTAR ISI.....	vi
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xiii
INTISARI.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian.....	3
1.7 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA.....	7
BAB III LANDASAN TEORI.....	11
3.1 Video.....	11
3.2 Kriptografi.....	11
3.2.1 Algoritme Kriptografi	11
3.2.2 Kriptografi Kunci Simetri	13
3.2.3 Kriptografi Kunci Asimetri	14
3.3 Video Encryption Algorithm (VEA).....	15
3.4 Advanced Encryption Standard (AES)	17
3.4.1 Add Round Key	20
3.4.2 Susbtitute Bytes.....	20

3.4.3	Shift Rows	20
3.4.4	Mix Columns.....	21
3.4.5	Key Expansion	21
3.4.6	Inverse Shift Rows	22
3.4.7	Inverse Substitute Bytes	22
3.4.8	Inverse Mix Columns.....	23
3.5	Rivest Cipher 4(RC4).....	24
3.5.1	Key-scheduling algorithm (KSA)	25
3.5.2	Pseudo-random generation algorithm (PRGA).....	26
3.6	Analisis Statistik	26
3.6.1	Korelasi Koefisien.....	27
3.6.2	Analisis Histogram.....	27
3.6.3	Analisis Kualitas Enkripsi.....	28
BAB IV ANALISIS DAN PERANCANGAN		30
4.1	Analisis Sistem.....	30
4.1.1	Deskripsi Sistem	30
4.1.2	Deskripsi Data.....	30
4.2	Analisis Kebutuhan	30
4.2.1	Analisis Kebutuhan Fungsional	31
4.2.2	Analisis Kebutuhan Non Fungsional	31
4.3	Perancangan Sistem	32
4.3.1	Pengambilan Data	33
4.3.2	Pra Pemrosesan Data.....	33
4.3.3	Proses Pembuatan Kunci dengan PBKDF2	35
4.3.4	Proses Enkripsi VEA (<i>Video Encryption Algorithm</i>)	36
4.3.5	Proses Dekripsi VEA	38
4.3.6	Proses Enkripsi VEA Modifikasi AES	38
4.3.7	Proses Dekripsi VEA Modifikasi AES	38
4.3.8	Proses Enkripsi VEA Modifikasi RC4.....	39
4.3.9	Proses Dekripsi VEA Modifikasi RC4	40
4.4	Rancangan Pengujian	40

4.4.1	Rancangan Pengujian Histogram	40
4.4.2	Rancangan Pengujian Koefisien Korelasi	41
4.4.3	Rancangan Pengujian Kualitas Enkripsi	42
4.4.4	Rancangan Pengujian Waktu Komputasi Algoritme	42
4.4.5	Rancangan Pengujian Frame Rate	43
BAB V IMPLEMENTASI.....		44
5.1	Lingkungan Implementasi	44
5.1.1	Spesifikasi Perangkat Keras	44
5.1.2	Spesifikasi Perangkat lunak	44
5.2	Implementasi data	44
5.2.1	Implementasi Masukan Frame	45
5.3	Implementasi Pembuatan Kunci	45
5.3.1	Implementasi Pembuatan Kunci PBKDF2	46
5.3.2	Implementasi Kunci VEA	46
5.3.3	Implementasi Kunci VEA dengan AES	46
5.3.4	Implementasi Kunci VEA dengan RC4	47
5.4	Implementasi Pengambilan dan Penulisan Nilai RGB.....	47
5.5	Implementasi algoritme.....	48
5.5.1	Implementasi Enkripsi VEA Sederhana.....	48
5.5.2	Implementasi Dekripsi VEA Sederhana	48
5.5.3	Implementasi Enkripsi VEA Modifikasi AES	49
5.5.4	Implementasi Dekripsi VEA Modifikasi AES.....	50
5.5.5	Implementasi Enkripsi dan Dekripsi VEA Modifikasi RC4	51
5.6	Implementasi Pengujian	51
5.6.1	Implementasi Histogram	51
5.6.2	Implementasi Koefisien Korelasi	52
5.6.3	Implementasi Kualitas enkripsi.....	54
5.6.4	Implementasi Waktu Komputasi.....	55
5.6.5	Implementasi Analisis Frame Rate	56
BAB VI HASIL DAN PEMBAHASAN		57
6.1	Hasil Enkripsi dan Dekripsi	57

6.1.1	Hasil Enkripsi dan Dekripsi VEA sederhana	57
6.1.2	Hasil Enkripsi dan Dekripsi VEA Modifikasi AES	58
6.1.3	Hasil Enkripsi dan Dekripsi VEA Modifikasi RC4	59
6.2	Pengujian Hasil Pemrosesan	60
6.2.1	Pengujian Histogram	60
6.2.2	Pengujian Koefisien Korelasi	63
6.2.3	Pengujian Kualitas Enkripsi	64
6.2.4	Pengujian Waktu Komputasi	66
6.2.5	Pengujian Frame Rate	67
6.3	Hasil Komparasi	68
BAB VII KESIMPULAN		69
7.1	Kesimpulan	69
7.2	Saran	70
DAFTAR PUSTAKA		71
LAMPIRAN		73

DAFTAR GAMBAR

Gambar 3.1 Ilustrasi dari proses kriptografi sederhana (Septia,2012).....	12
Gambar 3.2 Proses Enkripsi/Dekripsi Algoritme Simetris (Septia,2012).....	14
Gambar 3.3 Proses Enkripsi/Dekripsi Algoritme Asimetris (Septia,2012)	14
Gambar 3.4 Diagram Aliran VEA untuk frame video (Septia,2012)	16
Gambar 3.5 Flowchart Enkripsi dari algoritme AES-128 (Zarkari, 2013)	18
Gambar 3.6 Flowchart Dekripsi dari algoritme AES-128 (Zarkari, 2013).....	19
Gambar 3.7 Tabel S-Box (Paar & pelzl, 2010).....	20
Gambar 3.8 Ilustrasi Shift Rows (Zarkari, 2013).....	21
Gambar 3.9 Formula Perkalian Mix Columns (Zarkari, 2013).....	21
Gambar 3.10 Ilustrasi Inverse Shift Rows (Zarkari, 2013).....	22
Gambar 3.11 Tabel Inverse S-Box(Paar & Pelzl, 2010).....	23
Gambar 3.12 Formula Perkalian Mix Columns (Zarkari, 2013).....	23
Gambar 3.13 Proses Enkripsi Algoritme RC4 (Sumartono, 2016).....	25
Gambar 4.1 Skema perancangan system.....	32
Gambar 4.2 Alur pra pemrosesan	34
Gambar 4.3 Proses PDKDF2	35
Gambar 4.4 Format Enkripsi Pada Parameter 2.....	36
Gambar 4.5 Contoh Proses Enkripsi VEA.....	37
Gambar 4.6 Proses Inisiasi S-Box dan Kunci Awal Algoritme RC4.....	39
Gambar 4.7 Proses Pengacakan S-Box Algoritme RC4	39
Gambar 4.8 Proses Pseudo Random Algoritme RC4.....	39
Gambar 4.9 Contoh Sampel Data Untuk Histogram.....	40
Gambar 4.10 Hasil histogram gambar 4.9	40
Gambar 4.11 Ilustrasi nilai frame pada suatu posisi	41
Gambar 4.12 Contoh frame asli dan hasil enkripsi dalam nilai histogram	42
Gambar 5.1 Implementasi Masukan Frame	45
Gambar 5.2 Implementasi Frame ke Picture Box	45
Gambar 5.3 Implementasi Pembuatan Kunci PBKDF2.....	46

Gambar 5.4 Implementasi Kunci VEA	46
Gambar 5.5 Implementasi Kunci VEA dengan AES	46
Gambar 5.6 Implementasi Kunci VEA dengan RC4	47
Gambar 5.7 Implementasi Pengambilan Nilai RGB	47
Gambar 5.8 Implementasi Penulisan Nilai RGB	47
Gambar 5.9 Implementasi Enkripsi VEA Sederhana.....	48
Gambar 5.10 Implementasi Dekripsi VEA Sederhana	48
Gambar 5.11 Pra Proses Enkripsi VEA Modifikasi AES	49
Gambar 5.12 Implementasi Algoritme Enkripsi AES.....	49
Gambar 5.13 Pra Proses Dekripsi VEA Modifikasi AES	50
Gambar 5.14 Implementasi Algoritme Dekripsi AES	50
Gambar 5.15 Implementasi Algoritme Enkripsi dan Dekripsi RC4	51
Gambar 5.16 Implementasi mengambil nilai histogram	51
Gambar 5.17 Implementasi histogram membuat chart	52
Gambar 5.18 Implementasi pemasangan frame secara horizontal.....	52
Gambar 5.19 Implementasi pemasangan frame secara vertical	53
Gambar 5.20 Implementasi pemasangan frame secara diagonal	53
Gambar 5.21 Implementasi perhitungan korelasi	54
Gambar 5.22 Implementasi perhitungan maximum deviation.....	54
Gambar 5.23 Implementasi perhitungan irregular deviation	55
Gambar 5.24 Implementasi perhitungan waktu komputasi.....	55
Gambar 5.25 Implementasi perhitungan frame rate.....	56
Gambar 6.1 Frame ke 2 640x480 (a) asli, (b) enkripsi, dan (c) dekripsi	57
Gambar 6.2 Frame ke 2 1280x720 (a) asli, (b) enkripsi, dan (c) dekripsi	58
Gambar 6.3 Frame ke 2 640x480 (a) asli, (b) enkripsi, dan (c) dekripsi AES.....	58
Gambar 6.4 Frame ke 2 1280x720 (a) asli, (b) enkripsi, dan (c) dekripsi AES....	59
Gambar 6.5 Frame ke 2 640x480 (a) asli, (b) enkripsi, dan (c) dekripsi RC4.....	59
Gambar 6.6 Frame ke 2 1280x720 (a) asli, (b) enkripsi, dan (c) dekripsi RC4....	60
Gambar 6.7 Contoh Frame asli (a) 640x480, dan (b) 1280x720	60
Gambar 6.8 Histogram frame asal (a) 640x480, dan (b) 1280x720.....	61
Gambar 6.9 Histogram enkripsi (a) 640x480, dan (b) 1280x720 VEA.....	61

Gambar 6.10 Histogram enkripsi (a) 640x480, dan (b) 1280x720 VEA & AES . 61

Gambar 6.11 Histogram enkripsi (a) 640x480, dan (b) 1280x720 VEA & RC4.. 61

Gambar 6.12 Grafik waktu enkripsi resolusi 640x480 66

Gambar 6.13 Grafik waktu enkripsi resolusi 1280x720 67

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka	9
Tabel 4.1 Hasil pemasangan pixel secara horizontal	41
Tabel 6.1 Hasil rata-rata perbedaan histogram	62
Tabel 6.2 Hasil persentase nilai histogram terhadap nilai threshold.....	62
Tabel 6.3 Hasil koefisien korelasi	63
Tabel 6.4 Hasil kualitas enkripsi	65
Tabel 6.5 Hasil Waktu Komputasi	66
Tabel 6.6 Hasil framerate limit	67
Tabel 6.7 Hasil komparasi	68