

DAFTAR ISI

| | |
|---|-------------|
| ABSTRAK | i |
| ABSTRACT | ii |
| KATA PENGANTAR..... | iii |
| DAFTAR ISI..... | v |
| DAFTAR TABEL | viii |
| DAFTAR GAMBAR..... | x |
| BAB I PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 3 |
| 1.3 Tujuan Penelitian..... | 3 |
| 1.4 Batasan Masalah..... | 3 |
| 1.5 Kerangka Pemikiran | 3 |
| 1.6 Metodologi Penelitian | 4 |
| 1.7 Sistematika Penulisan..... | 6 |
| BAB II KAJIAN LITERATUR | 7 |
| 2.1 Tinjauan Pustaka | 7 |
| 2.2 Landasan Teori | 12 |
| 2.2.1 Multimedia | 12 |
| 2.2.2 Kriptografi..... | 12 |
| 2.2.3 <i>Algoritma Advanced Encryption Standard</i> | 13 |
| 2.2.4 <i>Unified Modelling Language</i> | 18 |
| 2.2.5 Node JS | 20 |
| 2.2.6 Express JS | 20 |
| 2.2.7 Basis Data (<i>Database</i>)..... | 21 |

| | | |
|--|---|-----------|
| 2.2.8 | MySQL..... | 21 |
| 2.2.9 | Sequelize | 21 |
| 2.2.10 | <i>Watermarking</i> | 22 |
| BAB III METODOLOGI PENELITIAN | | 23 |
| 3.1 | Analisis Kebutuhan | 23 |
| 3.1.1 | Analisis Masalah | 23 |
| 3.1.2 | Analisis Sistem..... | 23 |
| 3.1.3 | Kebutuhan Fungsional | 23 |
| 3.1.4 | Kebutuhan Non Fungsional..... | 24 |
| 3.1.5 | Analisis Algoritma AES (<i>Advanced Encryption Standard</i>)..... | 24 |
| 3.1.6 | Simulasi Perhitungan Penyisipan <i>Watermarking</i> | 33 |
| 3.1.7 | Arsitektur Sistem..... | 35 |
| 3.2 | Perancangan Sistem..... | 36 |
| 3.2.1 | Use Case Diagram..... | 36 |
| 3.2.2 | <i>Sequence</i> Diagram..... | 44 |
| 3.2.3 | <i>Activity</i> Diagram..... | 51 |
| BAB IV HASIL DAN PEMBAHASAN | | 56 |
| 4.1 | Hasil..... | 56 |
| 4.1.1 | Implementasi Perangkat Keras (<i>Hardware</i>)..... | 56 |
| 4.1.2 | Implementasi Perangkat Lunak (<i>Software</i>)..... | 56 |
| 4.1.3 | Implementasi Basis Data..... | 56 |
| 4.1.4 | Implementasi Antarmuka | 58 |
| 4.1.5 | Implementasi Algoritma AES dan Teknik <i>Watermarking</i> | 63 |
| 4.2 | Pengujian | 74 |
| 4.2.1 | Rencana Pengujian | 74 |
| 4.2.2 | Hasil Pengujian | 76 |

| | | |
|---|---|-----------|
| 4.2.3 | Pengujian Aplikasi | 82 |
| 4.2.4 | Uji Keamanan Pada File Gambar dan Video | 84 |
| 4.3 | Pembahasan | 85 |
| 4.3.1 | Proses Enkripsi dan Penyisipan Pesan Pada File | 85 |
| 4.3.2 | Proses Dekripsi File | 85 |
| 4.3.3 | Proses Dekripsi Pesan (<i>Watermark</i>) Pada File..... | 85 |
| BAB V KESIMPULAN DAN SARAN | | 87 |
| 5.1 | Kesimpulan..... | 87 |
| 5.2 | Saran | 87 |
| DAFTAR PUSTAKA | | 89 |



DAFTAR TABEL

| | |
|---|----|
| Tabel 2. 1 <i>State of the Art</i> | 7 |
| Tabel 2. 2 Jumlah Putaran Algoritma AES | 14 |
| Tabel 2. 3 Bilangan Polinomial untuk <i>Mix Column</i> | 16 |
| Tabel 2. 4 Bilangan Polinomial Proses Dekripsi | 18 |
| Tabel 3. 1 <i>Plaintext</i> dan <i>Key</i> pada matriks 4×4 | 25 |
| Tabel 3. 2 Konversi <i>Plaintext</i> dan <i>Key</i> ke heksadesimal | 25 |
| Tabel 3. 3 <i>Add Round Key</i> | 26 |
| Tabel 3. 4 Hasil substitusi <i>key</i> dengan tabel S-Box | 26 |
| Tabel 3. 5 Perhitungan Rot Word dan Sub-Byet kolom terakhir <i>Key State 0</i> | 26 |
| Tabel 3. 6 Hasil Pencarian <i>key Expansion</i> kedua..... | 27 |
| Tabel 3. 7 Hasil Pencarian <i>key Expansion</i> ketiga | 27 |
| Tabel 3. 8 Hasil Pencarian <i>Key Expansion</i> keempat..... | 27 |
| Tabel 3. 9 Hasil Pencarian <i>Key Expansion</i> kelima | 28 |
| Tabel 3. 10 Hasil pencarian <i>Key Expansion</i> keenam atau <i>key state 1</i> | 28 |
| Tabel 3. 11 Proses <i>sub bytes</i> | 28 |
| Tabel 3. 12 Pergeseran baris pertama pada <i>shift rows</i> | 29 |
| Tabel 3. 13 Pergeseran baris kedua pada <i>shift rows</i> | 29 |
| Tabel 3. 14 Pergeseran baris ketiga pada <i>shift rows</i> | 29 |
| Tabel 3. 15 Pergeseran baris keempat pada <i>shift rows</i> | 30 |
| Tabel 3. 16 Hasil <i>shift rows</i> | 30 |
| Tabel 3. 17 Proses <i>Mix column</i> | 31 |
| Tabel 3. 18 Hasil <i>Mix Column</i> | 32 |
| Tabel 3. 19 <i>Add Round Key</i> | 33 |
| Tabel 3. 20 Definisi Aktor | 37 |
| Tabel 3. 21 <i>Use Case</i> | 37 |
| Tabel 3. 22 Skenario <i>Use case</i> Daftar | 38 |
| Tabel 3. 23 Skenario <i>Use Case</i> Login..... | 38 |
| Tabel 3. 24 Skenario <i>Use Case</i> Dashboard..... | 39 |
| Tabel 3. 25 Skenario <i>Use Case</i> Enkripsi File | 40 |
| Tabel 3. 26 Skenario <i>Use Case</i> Dekripsi File | 41 |
| Tabel 3. 27 Skenario <i>Use Case</i> <i>History</i> File..... | 43 |

| | |
|--|----|
| Tabel 4. 1 Rencana Pengujian..... | 75 |
| Tabel 4. 2 Hasil Pengujian Halaman Daftar..... | 76 |
| Tabel 4. 3 Hasil Pengujian Halaman Login | 77 |
| Tabel 4. 4 Hasil Pengujian Halaman Enkripsi | 77 |
| Tabel 4. 5 Hasil Pengujian Halaman Dekripsi..... | 78 |
| Tabel 4. 6 Hasil Pengujian Halaman Dekripsi <i>Watermark</i> | 80 |
| Tabel 4. 7 Hasil Pengujian Halaman <i>History</i> File | 81 |
| Tabel 4. 8 History File Dekripsi..... | 81 |
| Tabel 4. 9 Pengujian Enkripsi dan Dekripsi File | 82 |



DAFTAR GAMBAR

| | |
|---|----|
| Gambar 1. 1 Kerangka Pemikiran | 4 |
| Gambar 1. 2 Metode Pengembangan | 5 |
| Gambar 2. 1 Proses Enkripsi | 15 |
| Gambar 2. 2 Rijndael S-Box | 16 |
| Gambar 2. 3 Proses Dekripsi | 17 |
| Gambar 2. 4 Inverse S-Box | 18 |
| Gambar 3. 1 Arsitektur Sistem | 35 |
| Gambar 3. 2 <i>Use Case</i> Diagram | 36 |
| Gambar 3. 3 <i>Sequence</i> Diagram Daftar | 45 |
| Gambar 3. 4 <i>Sequence</i> Diagram Login | 46 |
| Gambar 3. 5 <i>Sequence</i> Diagram Enkripsi File | 47 |
| Gambar 3. 6 <i>Sequence</i> Diagram Dekripsi File | 48 |
| Gambar 3. 7 <i>Sequence</i> Diagram Dekripsi <i>watermark</i> | 49 |
| Gambar 3. 8 <i>Sequence</i> Diagram <i>History</i> File Enkripsi | 50 |
| Gambar 3. 9 <i>Sequence</i> Diagram <i>History</i> File Dekripsi | 50 |
| Gambar 3. 10 <i>Activity</i> Diagram Proses Daftar | 51 |
| Gambar 3. 11 <i>Activity</i> Diagram Proses Login | 52 |
| Gambar 3. 12 <i>Activity</i> Diagram Proses Enkripsi | 53 |
| Gambar 3. 13 <i>Activity</i> Diagram Proses Dekripsi | 54 |
| Gambar 3. 14 <i>Activity</i> Diagram <i>History</i> File Enkripsi | 55 |
| Gambar 3. 15 <i>Activity</i> Diagram <i>History</i> File Dekripsi | 55 |
| Gambar 4. 1 Struktur <i>Database</i> | 57 |
| Gambar 4. 2 Struktur Tabel files | 57 |
| Gambar 4. 3 Struktur Tabel users | 57 |
| Gambar 4. 4 Struktur Tabel sequelizemeta | 58 |
| Gambar 4. 5 Halaman Awal | 58 |
| Gambar 4. 6 Halaman Daftar | 59 |
| Gambar 4. 7 Halaman Login | 59 |
| Gambar 4. 8 Halaman Dashboard | 60 |
| Gambar 4. 9 Halaman Enkripsi File | 61 |
| Gambar 4. 10 Halaman Dekripsi (Daftar File Hasil Enkripsi) | 61 |

| | |
|---|----|
| Gambar 4. 11 Form Dekripsi | 62 |
| Gambar 4. 12 Halaman Dekripsi <i>Watermark</i> | 62 |
| Gambar 4. 13 Halaman <i>History File</i> | 63 |
| Gambar 4. 14 Halaman <i>History File</i> Dekripsi | 63 |

