DAFTAR ISI

ABSTRAK ..... **i**

ABSTRACT ..... **ii**

KATA PENGANTAR ..... **iii**

DAFTAR ISI ..... **v**

DAFTAR GAMBAR ..... **xi**

DAFTAR TABEL ..... **xv**

DAFTAR SIMBOL ..... **xx**

DAFTAR LAMPIRAN ..... **xxiii**

BAB I PENDAHULUAN **1**

1. 1. Latar Belakang Masalah 1

1. 2. Perumusan Masalah 3

1. 3. Maksud dan Tujuan 3

1. 4. Batasan Masalah 4

1. 5. Metodologi Penelitian 5

1. 6. Sistematika Penulisan 7

BAB II LANDASAN TEORI **9**

2. 1. Komunikasi Data 9

2. 2. Keamanan Informasi 10

2. 3. Pengantar Multimedia 11

2. 3. 1. Definisi Multimedia 11

2. 3. 2. Fungsi Multimedia 12

2. 4. File Multimedia 13

2. 4. 1. File Teks 14

2. 4. 2. File Gambar 16

2. 4. 3. File Suara 19

2. 4. 4. File Video 26

2. 5. Pengenalan Kriptografi 28

2. 5. 1. Definisi dan Sejarah 28

2. 5. 2. Aplikasi Kriptografi 31

2. 5. 2. 1. *Confidentality* dan *Privacy* 31

2. 5. 2. 2. Otentikasi (*Authentication*) 33

2. 5. 2. 3. Integritas (*Integrity*) 34

2. 5. 2. 4. *Nonrepudation* 34

2. 5. 3. Jenis-jenis Kriptografi 35

2. 5. 3. 1. Kunci Simetris 35

2. 5. 3. 2. Kunci Asimetris 36

2. 6. Pengenalan Steganografi 38

2. 6. 1. Kriteria Steganografi 41

2. 6. 2. *Media Cover* 41

2. 6. 3. *Least Significant Bit* (LSB) 43

2. 6. 4. *Dynamic Cell Spreading* (DCS) 44

2. 7. *Digital Signature* 45

2. 7. 1. Manajemen Kunci 48

2. 7. 2. *Digital Signature Algorithm* (DSA) 48

2. 8. Fungsi HASH 51

2. 9. Pemodelan Sistem 53

2. 9. 1. UML (Unified Modelling Language) 53

2. 9. 2. *Use case* 54

2. 9. 3. *Class Diagram* 55

2. 9. 4. *Sequence Diagram* 56

2. 9. 5. *Activity Diagram* 57

2. 9. 6. *Collaboration Diagram* 58

2. 9. 7. *State Diagram* 58

2. 10. Sistem Operasi Java 59

2. 10. 1. Java2 60

2. 11. Pengujian Perangkat Lunak 60

2. 11. 1. *White Box Testing* 61

2. 11. 2. *Black Box Testing* 67

BAB III ANALISIS DAN PERANCANGAN SISTEM 71

3. 1. Analisis Sistem 71
3. 1. 1. Analisis Masalah 71
3. 1. 2. Analisis Algoritma 72
3. 1. 2. 1. Analisis Algoritma SHA-1 74
3. 1. 2. 2. Analisis *Digital Signature Algorithm* (DSA) 78
3. 1. 2. 3. Analisis Teknik *Dynamic Cell Spreading* (DCS) 89
3. 1. 3. Spesifikasi Kebutuhan Perangkat Lunak 93
3. 1. 4. Analisis Kebutuhan Non Fungsional 95
3. 1. 4. 1. Analisis Kebutuhan Perangkat Keras 96
3. 1. 4. 2. Analisis Kebutuhan Perangkat Lunak 96
3. 1. 4. 3. Analisis Pemakai 97
3. 1. 5. Analisis Kebutuhan Fungsional 97
3. 1. 5. 1. *Use Case Diagram* 98
3. 1. 5. 2. Skenario *Use Case* 98
3. 1. 5. 3. *Activity Diagram* 106
3. 1. 5. 4. *Sequence Diagram* 111
3. 1. 5. 5. *Class Diagram* 116
3. 2. Perancangan Sistem 116
3. 2. 1. Perancangan Struktur File 117
3. 2. 2. Perancangan Struktur Menu 118

3. 2. 3. Perancangan Antarmuka Perangkat Lunak 118

3. 2. 3. 1. Perancangan Antarmuka *Home* 119

3. 2. 3. 2. Perancangan Antarmuka *Embed File* 120

3. 2. 3. 3. Perancangan Antarmuka *Extract File* 121

3. 2. 4. Perancangan Pesan 121

3. 2. 5. Jaringan Semantik 126

3. 2. 6. Perancangan *Method* 126

3. 2. 6. 1 *Method Embed File* 127

3. 2. 6. 2 *Method Extract File* 129

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM 131

4. 1. Implementasi Sistem 131

4. 1. 1. Implementasi Antarmuka 132

4. 2. Pengujian Sistem 137

4. 2. 1. Rencana Pengujian 137

4. 2. 2. Pengujian *White Box* 137

4. 2. 2. 1. Pengujian *Generate Key Pair* 138

4. 2. 2. 2. Pengujian *Create Digital Signature* 140

4. 2. 2. 3. Pengujian *Verify Digital Signature* 142

4. 2. 3. Pengujian *Black Box* 144

4. 2. 3. 1. Pengujian Kecepatan Membuat Signature 144

4. 2. 3. 2. Pengujian Penyisipan Terhadap File Gambar 146

4. 2. 3. 3. Pengujian Penyisipan Terhadap File Suara 154

4. 2. 3. 4. Pengujian Penyisipan Terhadap File Video..... 160

4. 2. 3. 5. Pengujian Ekstraksi Terhadap File Citra 175

4. 2. 3. 6. Pengujian Ekstraksi Terhadap File Audio 178

4. 2. 3. 7. Pengujian Ekstraksi Terhadap File Video 181

4. 2. 3. 8. Pengujian Kecepatan Verifikasi Signature 186

4. 2. 3. 9. Hasil Pengujian Penyisipan Dan Ekstraksi..... 188

4. 2. 3. 10. Pengujian *Robustness* Pada File Citra 189

4. 2. 3. 11. Pengujian *Robustness* Pada File Audio 189

4. 2. 3. 12. Pengujian *Robustness* Pada File Video 190

4. 2. 3. 13. Pengujian Penyebaran File Stego Melalui Internet 190

4. 2. 3. 14. Pengujian Deteksi Menggunakan *Steganalisys* 191

4. 2. 3. 15. Perbandingan File Berdasarkan Histogram 191

4. 2. 3. 16. Hasil Pengujian Berdasarkan Kriteria Steganografi 214

4. 2. 4. Kesimpulan Hasil Pengujian 217

BAB V KESIMPULAN DAN SARAN 219

5. 1. Kesimpulan 219

5. 2. Saran 220

DAFTAR PUSTAKA 221