

**PENGAMANAN PESAN RAHASIA BERBASIS *MOBILE*
MENGUNAKAN *STEGANOGRAFI LSB, RSA-OAEP, AES-
GCM*, DAN AUTENTIKASI BIOMETRIK SIDIK JARI**

TUGAS AKHIR



Muhammad Noval

2201020014

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2025/2026**

**PENGAMANAN PESAN RAHASIA BERBASIS *MOBILE*
MENGUNAKAN *STEGANOGRAFI LSB, RSA-OAEP, AES-
GCM*, DAN AUTENTIKASI BIOMETRIK SIDIK JARI**

Tugas Akhir

Skema Skripsi

Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana

Teknik pada Program Studi Teknik Informatika



Muhammad Noval

2201020014

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2025/2026**

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “PENGAMANAN PESAN RAHASIA BERBASIS *MOBILE* MENGGUNAKAN *STEGANOGRAFI LSB, RSA-OAEP, AES-GCM*, DAN AUTENTIKASI BIOMETRIK SIDIK JARI” adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, Januari 2026



Muhammad Noval
NIM 2201020014

© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

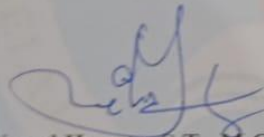
Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.



HALAMAN PERSETUJUAN

Judul : Pengamanan pesan rahasia berbasis *mobile*
menggunakan *Steganografi LSB, RSA-OAEP, AES-GCM* dan Autentikasi Biometrik Sidik Jari
Nama : Muhammad Noval
NIM : 2201020014
Program Studi : Teknik Informatika
Tanggal Persetujuan :

Disetujui oleh,
Komisi Pembimbing


Nurul Hayatv, S.T., M.Cs
(Ketua)


Rifaldi Herikson M.Kom
(Anggota)

HALAMAN PENGESAHAN

Judul : Pengamanan pesan rahasia berbasis mobile
menggunakan *Steganografi LSB, RSA-OAEP,*
AES-GCM dan Autentikasi Biometrik Sidik Jari

Nama : Muhammad Noval

NIM : 2201020014

Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	: Nurfalinda, S.T., M.Cs	(.....)
Anggota I	: Feri Irawan, S.Kom., M.Kom	(.....)
Anggota II	: Muhamad Fadli, M.Kom	(.....)
Anggota III	: Nurul Hayaty, S.T., M.Cs	(.....)
Anggota IV	: Rifaldi Herikson M.Kom	(.....)

Mengetahui,

Ketua Jurusan Teknik Elektro dan Informatika


Hollanda Arief Kusuma, S.IK., M.Si
NIP. 198904012019031016

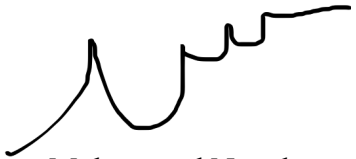
Tanggal Ujian: 14 Januari 2026 Tanggal Lulus:

PRAKATA

Puji dan syukur penulis panjatkan ke hadirat Allah subhanahu wa ta'ala atas rahmat dan karunia-Nya, sehingga Tugas Akhir ini dapat diselesaikan. Tugas Akhir ini disusun sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji. Adapun judul Tugas Akhir ini adalah “Pengamanan Pesan Rahasia Berbasis *Mobile* Menggunakan *Steganografi LSB, RSA-OAEP, AES-GCM*, dan Autentikasi Biometrik Sidik Jari”.

Pada kesempatan ini, penulis menyampaikan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan bantuan, bimbingan, dan dukungan selama proses penyusunan Tugas Akhir ini, khususnya kepada: Ibu Nurul Hayaty, S.T., M.Cs selaku dosen pembimbing yang telah memberikan arahan, masukan, serta motivasi selama penyusunan Tugas Akhir. Bapak Rifaldi Herikson, M.Kom selaku dosen pembimbing yang telah membimbing dan membantu penulis dalam penyempurnaan penelitian dan penulisan laporan. Teman-teman seperjuangan dan semua pihak yang tidak dapat disebutkan satu per satu, yang telah membantu melalui diskusi, kritik, dan semangat selama pengerjaan. Penulis menyadari bahwa Tugas Akhir ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk penyempurnaan di masa mendatang. Semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca dan menjadi kontribusi bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi. Semoga laporan tugas akhir ini bermanfaat.

Tanjungpinang, 8 Januari 2026

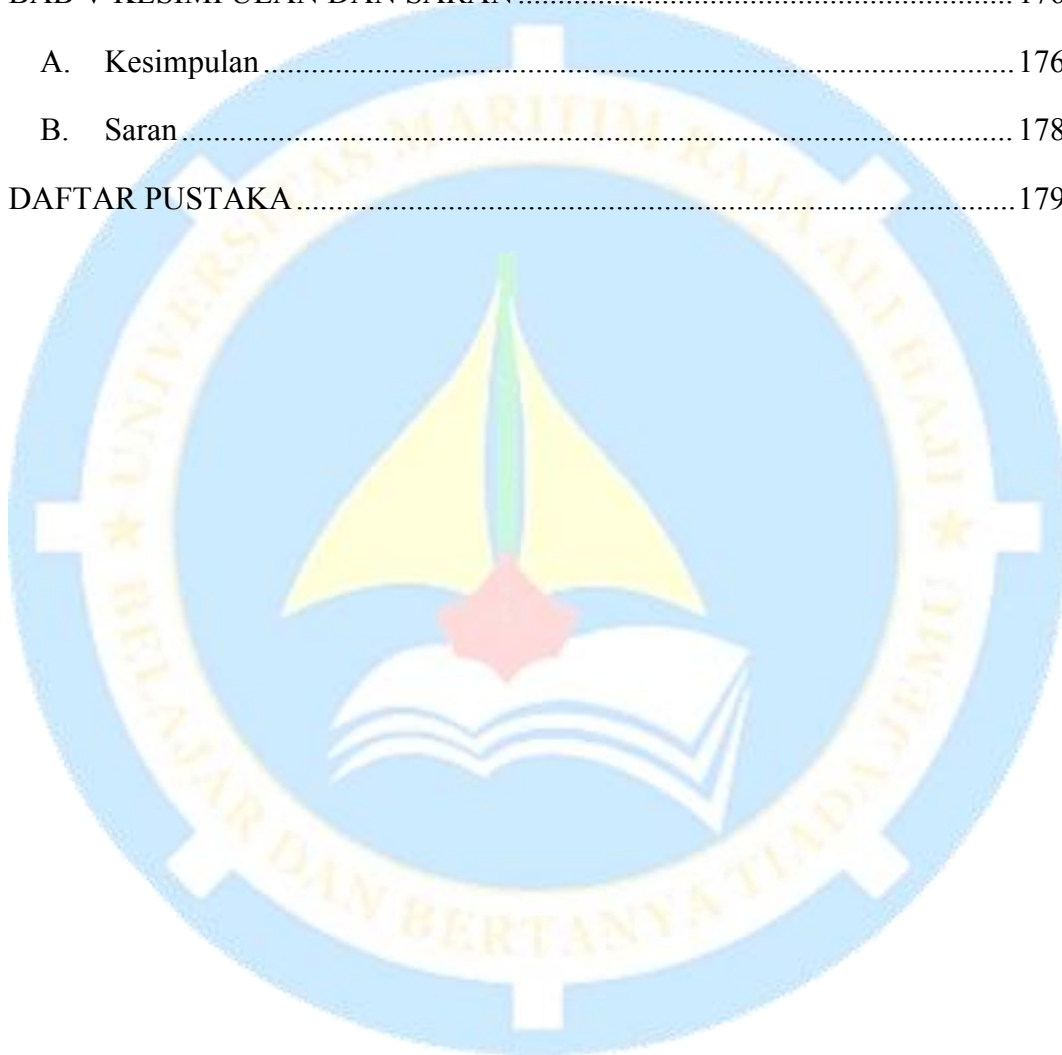


Muhammad Noval

DAFTAR ISI

HALAMAN PERSETUJUAN	iv
HALAMAN PENGESAHAN	v
PRAKATA	vi
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Rumusan Masalah	3
C. Batasan Penelitian	3
D. Tujuan Penelitian	4
E. Manfaat Penelitian	4
BAB II KAJIAN LITERATUR	6
A. Tinjauan Pustaka	6
B. Landasan Teori	11
BAB III METODE PENELITIAN	39
A. Waktu dan Tempat Penelitian	39
B. Bahan dan Alat	40
C. Prosedur Pelaksanaan Penelitian	42
D. Gambaran Umum Sistem	47
E. Alur kerja Sistem	63
F. Pengujian	72
G. Perhitungan Manual	81
H. Pengujian Keseluruhan sistem	106

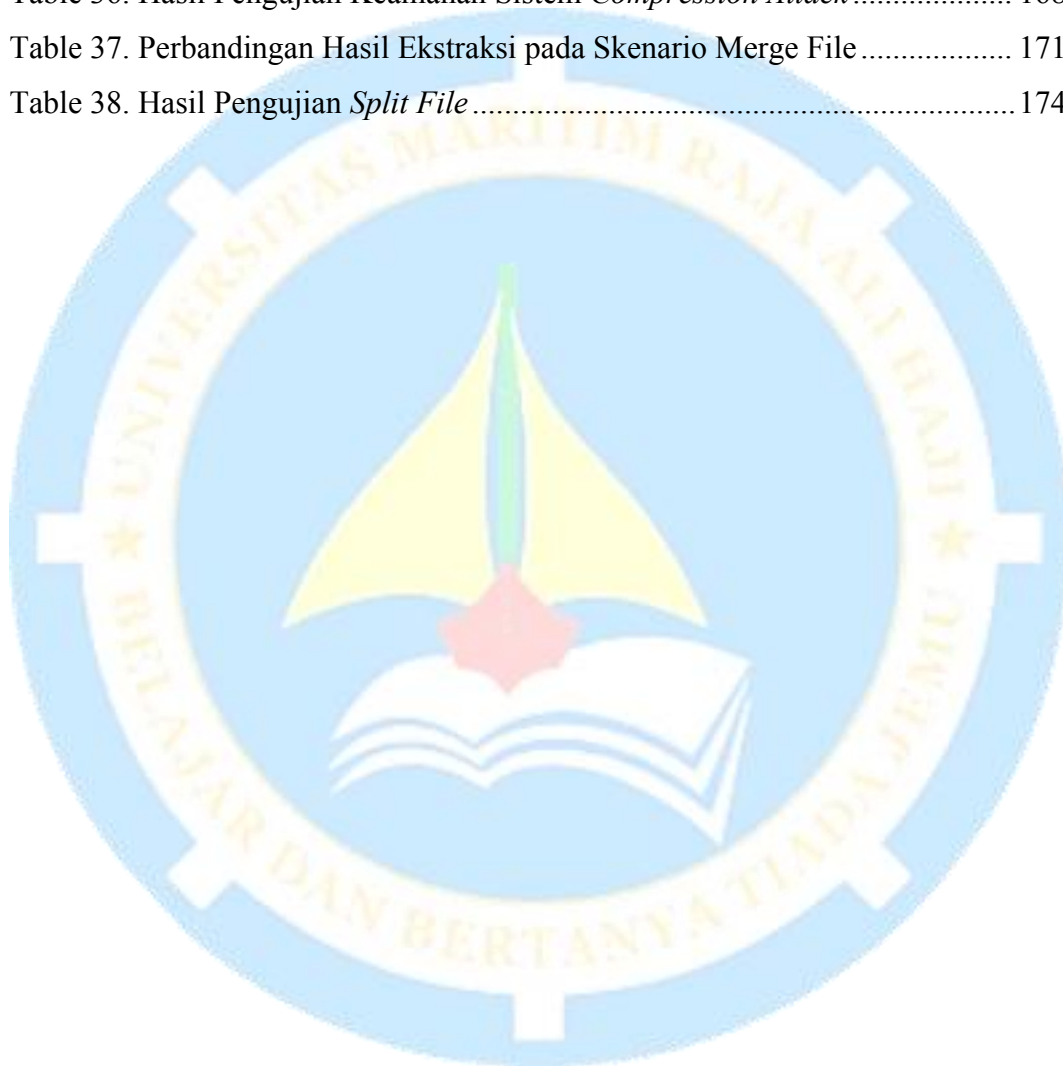
I. Pengujian Ketahanan Sistem Terhadap Serangan	107
J. Jadwal Penelitian	134
BAB IV HASIL DAN PEMBAHASAN	135
A. Hasil Implementasi Sistem	135
B. Analisis Data	138
BAB V KESIMPULAN DAN SARAN	176
A. Kesimpulan	176
B. Saran	178
DAFTAR PUSTAKA	179



DAFTAR TABEL

Table 1. Tinjauan Pustaka	8
Table 2. hasil performa terbaik pada <i>FVC-onGoing</i> [26]	14
Table 3. Bahan yang Digunakan	40
Table 4. Alat yang Digunakan	41
Table 5. <i>The execution times of the proposed model and each of RSA and AES algorithms separately on the transmitter's side for various file sizes.</i>	80
Table 6. <i>The execution times of the proposed model and each of RSA and AES algorithms separately on the receiver's side for various file sizes.</i>	80
Table 7. <i>ASCII</i> Table	81
Table 8. Hasil konversi <i>Plaintext</i> ke <i>ASCII</i> dan <i>heksadesimal</i>	83
Table 9. Hasil Konversi Kunci <i>AES</i>	84
Table 10. Konversi kunci <i>AES-256</i> (<i>K_AES256</i>) ke <i>ASCII</i> dan <i>heksadesimal</i>	85
Table 11. Contoh <i>AES S-Box</i> Sederhana	87
Table 12. Perhitungan <i>XOR per-byte</i> ($P1 \text{ XOR } S1 = C1$)	89
Table 13. Parameter contoh perhitungan <i>AES-256-GCM</i>	93
Table 14. Parameter contoh perhitungan <i>RSA</i> (sederhana)	95
Table 15. Nilai RGB Cover-Image	99
Table 16. perubahan nilai kanal	99
Table 17. Nilai RGB Stego-Image	101
Table 18. Proses Ekstraksi <i>LSB</i> per Kanal	101
Table 19. Hasil Akhir Dekripsi <i>LSB</i>	102
Table 20. Parameter <i>RSA</i>	103
Table 21. Hasil <i>P1</i>	106
Table 22. Komponen dan nilai <i>payload</i>	110
Table 23. Jadwal Rencana Pelaksanaan Penelitian	134
Table 24. Analisis Perbandingan Kualitas Citra	139
Table 25. Analisis Kualitas Ekstraksi Pesan	141
Table 26. Analisis autentikasi biometrik	143
Table 27. <i>Key space hybrid encryption</i>	146
Table 28 analisis entropi sisi pengirim	147
Table 29. Analisis <i>entropy</i> sisi penerima	148

Table 30. <i>Correlation Analysis</i>	150
Table 31. Perbandingan Performa Sisi Pengirim	151
Table 32. Tabel performa sistem sisi penerima	152
Table 33. Hasil Pengujian <i>Payload Modification Attack</i>	158
Table 34. Pengujian Keamanan Sistem <i>Unauthorized Access Attempt</i>	161
Table 35. Hasil Pengujian Keamanan Sistem <i>Cropping Attack</i>	164
Table 36. Hasil Pengujian Keamanan Sistem <i>Compression Attack</i>	168
Table 37. Perbandingan Hasil Ekstraksi pada Skenario Merge File	171
Table 38. Hasil Pengujian <i>Split File</i>	174



DAFTAR GAMBAR

Gambar 1. <i>CIA Triad</i> Keamanan Informasi Data	12
Gambar 2. Alur Proses Enkripsi AES	20
Gambar 3. Alur Proses Enkripsi AES	21
Gambar 4. Peta lokasi penelitian	39
Gambar 5. <i>Flowchart</i> Pelaksanaan Penelitian	42
Gambar 6. Registrasi Gagal	47
Gambar 7. Registrasi Berhasil	48
Gambar 8. <i>Login</i> gagal	49
Gambar 9. <i>Login</i> berhasil	50
Gambar 10. <i>Dashboard</i>	50
Gambar 11. Kirim Pesan – Gagal Verifikasi Penerima	51
Gambar 12. Kirim Pesan – Penerima Terverifikasi	52
Gambar 13. Halaman Ekstrak Pesan	53
Gambar 14. Ekstrak Pesan Berhasil – Pesan Rahasia Ditampilkan	54
Gambar 15. Ekstrak Pesan Gagal – Hanya Gambar Ditampilkan	54
Gambar 16. proses enkripsi pengirim	55
Gambar 17. Proses dekripsi penerima	59
Gambar 18. <i>Use Case Diagram</i> Aplikasi <i>GoSnap</i>	63
Gambar 19. <i>Sequences Diagram</i> Registrasi	66
Gambar 20. <i>Sequences Diagram</i> Login	67
Gambar 21. <i>Sequences Diagram</i> Pengiriman Pesan	69
Gambar 22. <i>Sequence Diagram</i> Penerimaan dan Pembacaan Pesan	70
Gambar 23. Contoh Cover Image	96
Gambar 24. <i>Sketsa area piksel yang dipilih untuk contoh perhitungan manual</i>	97
Gambar 25. Hasil Stego-Image	100
Gambar 26. Flowchart Pengujian Pra-Implementasi <i>Payload Modification Attack</i>	109
Gambar 27. Flowchart Pengujian pasca Implementasi <i>Payload Modification Attack</i>	113
Gambar 28. Flowchart Pengujian Pra-Implementasi <i>Unauthorized access attempt</i> (Upaya Akses Tidak Sah)	115
Gambar 29. Flowchart Pengujian Pasca Implementasi <i>Unauthorized access attempt</i> (Upaya Akses Tidak Sah)	117

Gambar 30. Flowchart Pengujian Pra-Implementasi <i>Cropping Attack</i>	119
Gambar 31. Flowchart Pengujian Pra-Implementasi <i>Compression Attack</i>	120
Gambar 32. Flowchart Pengujian Pasca Implementasi <i>Cropping Attack</i>	122
Gambar 33. Flowchart Pengujian Pasca Implementasi <i>Compression Attack</i>	123
Gambar 34. Flowchart Pengujian Pra Implementasi <i>Merge file</i>	126
Gambar 35. Flowchart Pengujian Pasca Implementasi <i>Merge file</i>	129
Gambar 36. Flowchart Pengujian Pra Implementasi <i>Split file</i>	131
Gambar 37. Flowchart Pengujian Pasca Implementasi <i>Split file</i>	133
Gambar 38. Halaman Login	135
Gambar 39. Halaman Registrasi	136
Gambar 40. Halaman Menu Utama	136
Gambar 41. Halaman Penyisipan Pesan	137
Gambar 42. Halaman Ekstrak Pesan	138
Gambar 43. <i>Log Output Terminal Payload Modification Attack – ct_rate_0.001</i> (<i>Ciphertext bit-flip rate 0.001</i>)	156
Gambar 44. <i>Log Output Terminal Payload Modification Attack – ct_rate_0.005</i> (<i>Ciphertext bit-flip rate 0.005</i>)	156
Gambar 45. <i>Log Output Terminal Payload Modification Attack – tag_flip_1bit</i> (<i>Tag AES-GCM 1 bit</i>)	157
Gambar 46. <i>Log Output Terminal Payload Modification Attack – tag_flip_8bit</i> (<i>Tag AES-GCM 8 bit</i>)	157
Gambar 47. <i>Log Output Terminal Payload Modification Attack – ct_tag_flip_2bits_each</i> (<i>Ciphertext + Tag</i>)	158
Gambar 48. <i>Log Output Terminal Payload Modification Attack – rsa_key_flip_1bit</i> (<i>RSA-OAEP encrypted session key 1 bit</i>)	158
Gambar 49. <i>Log Output Terminal Unauthorized Access Attempt - SUCCESS</i> (sidik jari valid)	162
Gambar 50. <i>Log Output Terminal Unauthorized Access Attempt - LOCKED_OUT</i> (<i>Reject=5; lockout 30 detik</i>)	162
Gambar 51. <i>Log Output Terminal Unauthorized Access Attempt - LOCKED_OUT</i> (<i>Reject=10</i>)	162

Gambar 52. <i>Log Output Terminal Unauthorized Access Attempt - LOCKED_OUT (Reject=15)</i>	163
Gambar 53. <i>Log Output Terminal Unauthorized Access Attempt - PERM_LOCKED_OUT (Reject=16)</i>	163
Gambar 54. <i>Log Output Terminal Cropping Attack - Crop 0% (tanpa cropping)</i>	165
Gambar 55. <i>Log Output Terminal Cropping Attack - Crop 10%</i>	165
Gambar 56. <i>Log Output Terminal Cropping Attack - Crop 20%</i>	166
Gambar 57. <i>Log Output Terminal Cropping Attack - Crop 30%</i>	166
Gambar 58. <i>Log Output Terminal Compression Attack - JPEG Quality 50% (Q50)</i>	169
Gambar 59. <i>Log Output Terminal Compression Attack - JPEG Quality 60% (Q60)</i>	170
Gambar 60. <i>Log Output Terminal Compression Attack - JPEG Quality 70% (Q70)</i>	170
Gambar 61. <i>Log Output Terminal Merge File</i>	172
Gambar 62. <i>Log sistem pengujian Split file – rejoin salah</i>	174
Gambar 63. <i>Log sistem pengujian Split file – rejoin salah</i>	175

