

**ANTARMUKA PENGIRIMAN PESAN RAHASIA  
PADA MEDIA GAMBAR DENGAN MENGGUNAKAN  
METODE *LEAST SIGNIFICANT BIT* (LSB)  
DALAM PERANGKAT BERBASIS ANDROID**



**SKRIPSI**

**Disusun Sebagai Salah Satu Syarat  
Untuk Memperoleh Gelar Sarjana Komputer  
Pada Jurusan Ilmu Komputer/Informatika**

**Disusun Oleh:  
GAGAT BANGUN KARYADI  
24010310120052**

**JURUSAN ILMU KOMPUTER/INFORMATIKA  
FAKULTAS SAINS DAN MATEMATIKA  
UNIVERSITAS DIPONEGORO**

**2014**

## **HALAMAN PERNYATAAN KEASLIAN SKRIPSI**

Dengan ini saya menyatakan bahwa dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan memperoleh gelar kesarjanaan di suatu Perguruan Tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah saya tulis atau terbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 29 Agustus 2014

Gagat Bangun Karyadi  
24010310120052

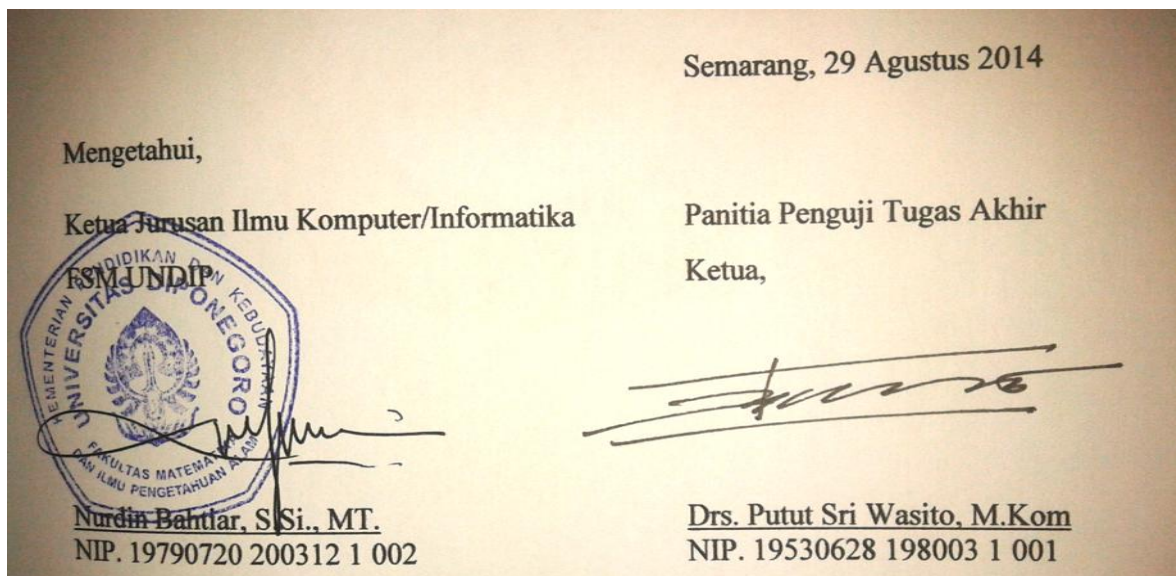
## HALAMAN PENGESAHAN

Judul : Antarmuka Pengiriman Pesan Rahasia Pada Gambar Dengan Menggunakan Metode *Least Significant Bit* (LSB) Dalam Perangkat Berbasis Android

Nama : Gagat Bangun Karyadi

NIM : 24010310120052

Telah diujikan pada sidang tugas akhir pada tanggal 22 Agustus 2014 dan dinyatakan lulus pada tanggal **28 Agustus 2014**.



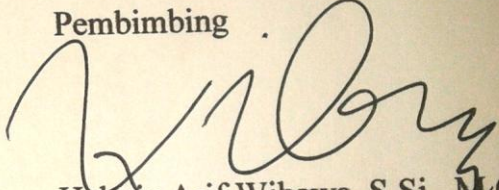
## HALAMAN PENGESAHAN

Judul : Antarmuka Pengiriman Pesan Rahasia Pada Gambar Dengan Menggunakan Metode *Least Significant Bit* (LSB) Dalam Perangkat Berbasis Android

Nama : Gagat Bangun Karyadi

NIM : 24010310120052

Telah diujikan pada sidang tugas akhir pada tanggal 22 Agustus 2014.

Semarang, 29 Agustus 2014  
Pembimbing .  
  
Helmie Arif Wibawa, S.Si, M.Cs  
NIP. 19780516 200312 1 001

## ABSTRAK

*Instant messenger* merupakan salah satu aplikasi dalam perangkat android yang dapat digunakan untuk melakukan pertukaran data. *Instant Messenger* menggunakan jaringan internet untuk melakukan proses pertukaran data. Hal tersebut membuat *instant messenger* rentan akan penyadapan. Dibutuhkan suatu metode penyelesaian untuk masalah tersebut. Pada Tugas Akhir ini dibahas tentang pembuatan antarmuka yang dapat melakukan penyembunyian pesan pada media gambar dan menghubungkannya ke *instant messenger* untuk dikirim pada penerima. Metode yang digunakan *Least Significant Bit* (LSB) yaitu metode steganografi dengan cara menyisipkan pesan dengan merubah *bit* terakhir dari gambar. Metode ini digunakan karena tidak membutuhkan perhitungan dan komputasi yang besar untuk melakukan proses penyisipan sehingga cocok untuk digunakan pada *smartphone* berbasis Android yang memiliki memori dan prosesor yang rendah. Hasil dari proses penyisipan menunjukkan nilai *Peak Signal to Noise Ratio* (PSNR) berkisar antara 43dB sampai dengan 48db yang berarti gambar hasil penyisipan tidak jauh berbeda dengan gambar asli sebelum mengalami proses penyisipan.

Kata Kunci : *Instant Messenger*, Android, Steganografi, *Least Significant Bit* (LSB), *Peak Signal to Noise Ratio* (PSNR).

## ABSTRACT

Instant messenger is an application which allows android devices to exchange data. Instant messenger uses internet to exchange the data. This makes the data exchange through the devices prone to illegal tapping activity. A method is needed to solve the problem. This final project is about the development of an application interface which allows the user to conceal a message from an image and send it to the recipient through the instant messenger. LSB is the proposed method of steganography which interject the message by changing the last bit of the image. This method doesn't require much calculation and computation on the interjection process that makes it perfect for an android-based smartphone which has low memory capacity and processing power. The results from the PSNR are ranged between 43dB to 48dB which means that the image has not much difference from the image before the interjection process.

Keyword : *Instant Messenger, Android, Steganografi, Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR).*

## KATA PENGANTAR

Segala puji syukur bagi Allah SWT atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan laporan Tugas Akhir ini.

Laporan Tugas Akhir yang berjudul “**Antarmuka Pengiriman Pesan Rahasia Pada Media Gambar Dengan Menggunakan Metode *Least Significant Bit (Lsb)* Dalam perangkat Berbasis Android**” disusun sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada Jurusan Ilmu Komputer/Informatika Universitas Diponegoro. Penelitian Tugas Akhir ini mahasiswa dituntut untuk mengimplementasikan ilmu yang didapat di bangku perkuliahan untuk menyelesaikan suatu permasalahan yang ada dengan menggunakan teknik penelitian ilmiah.

Penyusunan laporan ini tentulah Penulis banyak mendapat bimbingan dan bantuan dari berbagai pihak. Kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada :

1. Dr. Muhammad Nur, DEA, selaku Dekan Fakultas Sains dan Matematika (FSM) Universitas Diponegoro.
2. Nurdin Bahtiar, S.Si, M.T, selaku Ketua Jurusan Ilmu Komputer/Informatika FSM UNDIP.
3. Indra Waspada, S.T, M.T, selaku Dosen Koordinator Tugas Akhir Jurusan Ilmu Komputer/Informatika FSM UNDIP.
4. Helmie Arif Wibawa, S.Si, M.Cs selaku Dosen Pembimbing yang telah membantu dalam proses bimbingan hingga terselesaikannya laporan Tugas Akhir ini.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan Penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan.

Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya

Semarang, 29 Agustus 2014

Penulis,

## DAFTAR ISI

	Hal
HALAMAN PERNYATAAN KEASLIAN SKRIPSI .....	ii
HALAMAN PENGESAHAN .....	iii
ABSTRAK .....	v
ABSTRACT .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI .....	viii
DAFTAR GAMBAR .....	x
DAFTAR TABEL .....	xii
BAB I PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	3
1.3. Tujuan dan Manfaat .....	3
1.4. Ruang Lingkup .....	3
1.5. Sistematika Penulisan .....	4
BAB II LANDASAN TEORI .....	5
2.1. Android .....	5
2.2. <i>Instant Messenger (IM)</i> .....	9
2.3. Steganografi .....	11
2.4. Metode <i>Least Significant Bit (LSB)</i> .....	12
2.5. <i>Peak Signal to Noise Ratio (PSNR)</i> .....	14
2.6. Konsep Berorientasi Objek .....	14
2.7. <i>Unified Process</i> .....	16
2.8. <i>Unified Modelling Language</i> .....	21
BAB III DEFINISI KEBUTUHAN, ANALISIS DAN PERANCANGAN .....	28
3.1. Definisi Kebutuhan .....	28
3.1.1. Gambaran Umum .....	28
3.1.2. Model <i>Use Case</i> .....	31



3.1.3. Kebutuhan Non-fungsional Perangkat Lunak.....	40
3.2. Analisis.....	40
3.3. Perancangan.....	43
3.3.1. <i>Use Case Realization</i> Tahap Perancangan .....	43
3.3.2. <i>Class</i> Perancangan .....	48
BAB IV IMPLEMENTASI DAN PENGUJIAN .....	49
4.1. Implementasi .....	49
4.1.1. Spesifikasi Perangkat .....	49
4.3.2. Implementasi <i>Class</i> .....	49
4.2. Analisa Perhitungan .....	56
4.2.1. Proses <i>Embedding</i> .....	56
4.2.2. Proses Ekstraksi .....	59
4.3. Pengujian.....	61
4.3.1. Lingkungan Pengujian.....	61
4.3.2. Rencana Pengujian .....	62
BAB V PENUTUP .....	66
5.1. Kesimpulan.....	66
5.2. Saran .....	66
DAFTAR PUSTAKA .....	68
LAMPIRAN 1 .....	69

## DAFTAR GAMBAR

	Hal
Gambar 2.1 Arsitektur Android .....	6
Gambar 2.2. Siklus <i>Activity</i> Android .....	8
Gambar 2.3 <i>Instant messenger</i> dengan Arsitektur <i>Client-Server</i> .....	10
Gambar 2.4 Ilustrasi kriptografi dan steganografi pada citra .....	11
Gambar 2.5 Proses penyisipan dan ekstraksi pada steganografi .....	12
Gambar 2.6 Susunan <i>bit</i> pada sebuah <i>byte</i> .....	13
Gambar 2.7. Contoh Kelas <i>Student</i> .....	15
Gambar 2.8. Hubungan Fase dengan <i>Workflow</i> dalam <i>Unified Process</i> .....	18
Gambar 2.9. Contoh <i>Dependency</i> .....	22
Gambar 2.10. Contoh <i>Association</i> .....	22
Gambar 2.11. Contoh <i>Generalization</i> .....	23
Gambar 3.1. Deskripsi umum antarmuka pengiriman pesan rahasia pada gambar dengan menggunakan Metode LSB dalam perangkat berbasis Android .....	29
Gambar 3.2. Alur proses antarmuka pengiriman pesan rahasia pada gambar dengan menggunakan Metode LSB dalam perangkat berbasis Android .....	29
Gambar 3.3. Alur proses <i>Embedding</i> antarmuka pengiriman pesan rahasia pada gambar dengan menggunakan Metode LSB dalam perangkat berbasis android .....	30
Gambar 3.4. Alur proses Ekstraksi antarmuka pengiriman pesan rahasia pada gambar dengan menggunakan Metode LSB dalam perangkat berbasis android .....	31
Gambar 3.5. <i>Use case Diagram</i> .....	33
Gambar 3.6. <i>Activity Diagram</i> Mengirim Pesan .....	33
Gambar 3.7. <i>Activity Diagram</i> Menyisipkan Pesan.....	34
Gambar 3.8. <i>Activity Diagram</i> Mengambil Pesan .....	34
Gambar 3.9 Sketsa Tampilan Awal Antarmuka Pengiriman .....	36
Gambar 3.10 Sketsa Tampilan Mengirim Pesan .....	36
Gambar 3.11 Sketsa Tampilan menyisipkan pesan .....	38
Gambar 3.12 Sketsa Tampilan Ambil Pesan .....	39
Gambar 3.13 <i>Analysis Class Use Case</i> Kirim Pesan .....	41
Gambar 3.14 <i>Analysis Class Use Case</i> Menyisipkan Pesan .....	41

Gambar 3.15 <i>Analysis Class Use Case</i> Mengambil Pesan.....	42
Gambar 3.16 Realisasi <i>Use Case</i> Mengirim Pesan.....	44
Gambar 3.17 <i>Sequence Diagram</i> Mengirim Pesan.....	44
Gambar 3.18 Realisasi <i>Use Case</i> Menyisipkan Pesan.....	45
Gambar 3.19 <i>Sequence Diagram</i> Menyisipkan Pesan.....	46
Gambar 3.20 Realisasi <i>Use Case</i> Mengambil Pesan .....	47
Gambar 3.21 <i>Sequence Diagram</i> Mengambil Pesan .....	47
Gambar 4.1 Menu Utama .....	50
Gambar 4.2 Tampilan <i>Form</i> Mengirim Pesan.....	51
Gambar 4.3 Tampilan Proses Menyisipkan Pesan .....	52
Gambar 4.4 Tampilan Proses Memilih <i>Messenger</i> .....	52
Gambar 4.5 Tampilan <i>Form</i> Menyisipkan Pesan .....	53
Gambar 4.6 <i>Tampilan</i> Proses Menyisipkan Pesan .....	53
Gambar 4.7 Tampilan <i>Dialog Box</i> Saat Gambar Tersimpan.....	54
Gambar 4.8 Tampilan Proses Memilih Gambar .....	55
Gambar 4.9 Tampilan Proses Menampilkan Pesan .....	55

## DAFTAR TABEL

	Hal
Tabel 2.1. Nilai PSNR.....	14
Tabel 2.2. Notasi <i>Use Case Diagram</i> .....	24
Tabel 2.3. Simbol <i>Activity Diagram</i> .....	25
Tabel 2.4 Simbol <i>Class Diagram</i> .....	25
Tabel 2.5 Simbol <i>Streotype</i> .....	26
Tabel 2.6 Simbol <i>Sequence Diagram</i> .....	26
Tabel 3.1. Daftar Aktor .....	32
Tabel 3.2. Daftar <i>Use Case</i> .....	32
Tabel 3.3. Detail <i>Use Case</i> Mengirim Pesan.....	35
Tabel 3.4. Detail <i>Use Case</i> Menyisipkan Pesan .....	37
Tabel 3.5. Detail <i>Use Case</i> Mengambil Pesan .....	38
Tabel 3.6. Hasil Identifikasi <i>Analysis Class</i> .....	42
Tabel 3.7. Daftar Tanggung Jawab dan <i>Attribut Analysis Class</i> .....	42
Tabel 3.8. Identifikasi <i>Class</i> perancangan <i>Use Case</i> Mengirim Pesan.....	43
Tabel 3.9. Identifikasi <i>Class</i> Perancangan <i>Use Case</i> Menyisipkan Pesan.....	45
Tabel 3.10. Identifikasi <i>Class</i> Perancangan <i>Use Case</i> Mengambil Pesan .....	46
Tabel 3.11. Hasil Identifikasi <i>Class</i> Perancangan .....	48
Tabel 4.1. Implementasi <i>Class</i> .....	50
Tabel 4.2. Tabel Rencana Pengujian Berdasarkan <i>Use Case</i> .....	62
Tabel 4.3. Tabel Gambar Uji.....	63
Tabel 4.4. Tabel Macam-macam <i>Instant Messenger</i> .....	64
Tabel 4.5. Tabel Hasil Pengujian Kualitas Gamar .....	64
Tabel 4.6. Tabel Hasil Pengujian <i>Instant Messenger</i> .....	65

# BAB I

## PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat serta ruang lingkup penelitian tugas akhir mengenai antarmuka pengiriman pesan rahasia pada gambar dengan menggunakan Metode *Least Significant Bit* (LSB) dalam perangkat berbasis Android.

### 1.1. Latar Belakang

Perkembangan teknologi dari tahun ke tahun semakin berkembang, termasuk perkembangan teknologi di bidang telekomunikasi. Salah satu contohnya adalah semakin banyaknya pengguna ponsel pintar (*smartphone*) sebagai salah satu alat telekomunikasi. Android merupakan salah satu sistem operasi yang paling banyak digunakan dalam *smartphone*.

Salah satu aplikasi yang sering digunakan pada *smartphone* adalah *instant messenger* yang mana dapat digunakan untuk melakukan pertukaran informasi seperti file, gambar maupun video. Beberapa contoh *instant messenger* yang bisa dijalankan pada *smartphone* adalah WhatsApp, LINE, BlackBerry Messenger (BBM), Wechat. Keamanan dan kerahasiaan informasi yang dikirim melalui beberapa *instant messenger* tersebut belum terjamin sepenuhnya sehingga rawan terhadap penyadapan data (Suryawan et al., 2013).

Berdasarkan masalah yang ada dibutuhkan suatu antarmuka penghubung ke *instant messenger* tersebut yang dapat membantu untuk menyembunyikan informasi atau pesan agar orang yang tidak memiliki wewenang tidak dapat melihat informasi atau pesan yang dikirim.

Pengamanan informasi atau pesan yang biasa dipakai adalah kriptografi. Kriptografi merupakan salah satu cara pengamanan pesan yang dilakukan dengan cara menyandikan pesan rahasia tersebut ke dalam bentuk yang tidak dapat dimengerti lagi maknanya atau biasa disebut chiperteks. Seiring dengan kemajuan teknologi, kriptanalis atau orang yang bertugas memecahkan chiperteks mulai bisa memecahkannya. Hal tersebut disebabkan pesan yang disandikan atau dienkrpsi

menghasilkan chiperteks yang terlihat dan kriptanalis menggunakan chiperteks tersebut untuk mendapatkan informasi yang ada dengan mencoba memecahkannya dengan metode dekripsi yang ada. Sehingga dibutuhkan metode pengamanan informasi yang tidak dapat diketahui orang lain selain pengirim dan penerima. Salah satu metode penyembunyian pesan tersebut adalah steganografi.

Steganografi merupakan salah satu metode penyembunyian pesan dengan cara menyisipkan pesan pada media penampung sehingga keberadaannya tidak diketahui. Steganografi memanfaatkan keterbatasan indra manusia sehingga pesan yang disisipkan tidak dapat terdeteksi. Salah satu metode steganografi yang digunakan untuk menyisipkan informasi adalah *Least Significant Bit (LSB)*.

Metode LSB adalah metode steganografi yang menyisipkan pesan rahasia dengan cara mengubah *bit* paling kanan dari media penyimpanan pesan dengan *bit* pesan rahasia tersebut. Sehingga perbedaan antara media penyimpanan yang sudah disisipkan pesan dan yang belum tersisipkan tidak terlalu terlihat atau kasat mata.

Proses penyisipan pesan pada beberapa metode steganografi membutuhkan proses perhitungan yang rumit dan komputasi yang cukup besar. Berbeda dengan *Personal Computer (PC)* yang memiliki kemampuan prosesor maupun memori yang bisa melakukan komputasi yang berat dan rumit, banyak *smartphone* tidak memiliki kemampuan untuk melakukan komputasi yang besar sehingga pada implementasi steganografi pada media gambar berbasis Android ini digunakan metode LSB, metode yang sebenarnya paling dasar dalam teknik steganografi namun dalam metode ini tidak memerlukan proses perhitungan dan komputasi yang kompleks seperti metode steganografi yang lainnya sehingga metode ini dapat mempercepat proses penyisipan pesan dan tepat diterapkan pada perangkat berbasis android yang memiliki spesifikasi prosesor yang terbatas.

Pengembangan aplikasi steganografi dengan metode LSB berbasis J2ME yang dapat mengirimkan pesan rahasia melalui MMS pernah dilakukan oleh Azizi. Aplikasi tersebut memiliki keterbatasan yaitu tidak dapat mengirimkan gambar berukuran lebih dari 30 KB, sehingga diperlukan aplikasi atau antarmuka yang dapat mengirimkan pesan yang berukuran lebih besar dari 30 KB (Azizi, 2012).

Dalam tugas akhir ini dibangun sebuah aplikasi antarmuka pengiriman pesan rahasia pada media gambar dengan metode *Least Significant Bit* (LSB) pada perangkat berbasis Android yang dapat menyisipkan pesan pada media gambar sebelum dikirim melalui *instant messenger* agar pesan yang dikirim tidak dapat terdeteksi oleh orang yang tidak mempunyai hak atas pesan tersebut.

## 1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi yaitu bagaimana membuat suatu antarmuka pengiriman pesan rahasia berukuran sampai dengan 500 *Kilo Bytes* pada media gambar dengan Metode *Least Significant Bit* (LSB) dalam perangkat berbasis Android untuk menyembunyikan pesan yang dikirim agar tidak terdeteksi oleh pihak yang tidak memiliki hak atas pesan tersebut.

## 1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan suatu antarmuka pengiriman pesan rahasia pada media gambar dengan Metode *Least Significant Bit* (LSB) dalam perangkat berbasis Android.

Manfaat dari penelitian tugas akhir ini adalah dapat membantu pengirim dalam menyembunyikan pesan rahasia yang dikirim melalui *instant messenger* agar tidak terdeteksi oleh pihak yang tidak memiliki hak atas pesan tersebut.

## 1.4. Ruang Lingkup

Ruang lingkup pada antarmuka pengiriman pesan rahasia pada media gambar dengan Metode *Least Significant Bit* (LSB) dalam perangkat berbasis Android adalah sebagai berikut:

1. *Input* berupa gambar atau citra diam.
2. *Input* berupa citra berformat *.Jpeg* dan *.png*.
3. Bahasa pemrograman yang digunakan adalah *java*.
4. Menggunakan *Android Develompent Tools* dalam pembangunan antarmuka ini.
5. Tidak membahas mengenai persebaran kunci.

## 1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

### BAB I PENDAHULUAN

Merupakan pendahuluan yang berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan.

### BAB II DASAR TEORI

Berisi kumpulan studi pustaka yang berhubungan dengan topik tugas akhir. Dasar teori ini meliputi pengertian sistem operasi android, *instant messenger*, steganografi, metode *least significant bit* (LSB), *peak signal to noise ratio* (PSNR), konsep berorientasi objek, metode pengembangan perangkat lunak *unified process*, *unified modelling language*.

### BAB III DEFINISI KEBUTUHAN, ANALISIS, DAN PERANCANGAN

Membahas tahap definisi kebutuhan, analisis, dan tahap perancangan, serta hasil yang didapat pada ketiga tahap tersebut.

### BAB IV IMPLEMENTASI DAN PENGUJIAN

Membahas tahap implementasi dan rincian pengujian sistem yang dibangun dengan metode *black box*.

### BAB V PENUTUP

Berisi kesimpulan yang diambil berkaitan dengan sistem yang dikembangkan dan saran-saran untuk pengembangan sistem lebih lanjut.