

SKRIPSI

**IMPLEMENTASI DAN ANALISIS STEGANOGRAFI
DENGAN METODE LSB, PIT, DAN MODIFIED PIT**



Gavrila Tiominar Sianturi

NPM: 2013730025

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2018**

UNDERGRADUATE THESIS

**IMPLEMENTATION AND ANALYSIS OF STEGANOGRAPHY
USING LSB, PIT, AND MODIFIED PIT METHOD**



Gavrila Tiominar Sianturi

NPM: 2013730025

**DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2018**

LEMBAR PENGESAHAN



**IMPLEMENTASI DAN ANALISIS STEGANOGRAFI DENGAN
METODE LSB, PIT, DAN MODIFIED PIT**

Gavrila Tiominar Sianturi

NPM: 2013730025

Bandung, 21 Mei 2018`

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Pascal Alfadian, M.Comp.

Anggota Tim Penguji

Husnul Hakim, M.T.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng



PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

IMPLEMENTASI DAN ANALISIS STEGANOGRAFI DENGAN METODE LSB, PIT, DAN MODIFIED PIT

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 21 Mei 2018



Gavrila Tiominar Sianturi
NPM: 2013730025

ABSTRAK

Steganografi merupakan salah satu teknik keamanan yang dapat digunakan untuk menjaga kerahasiaan informasi. Steganografi adalah ilmu untuk menyembunyikan pesan rahasia di dalam suatu media. Media tersebut dapat berupa gambar, audio, video, dan lain sebagainya. Media yang digunakan pada skripsi ini adalah gambar. Terdapat beberapa metode steganografi dengan menggunakan media gambar. Salah satunya adalah metode *Least Significant Bit*. Metode *Least Significant Bit* melakukan penyembunyian pesan rahasia dengan cara menyisipkan pesan rahasia tersebut pada bit terakhir pada setiap *channel* warna pada gambar. Metode ini dianggap memiliki pola penyisipan yang terlalu sederhana dan kurang aman untuk menjaga kerahasiaan informasi. Oleh karena itu, terdapat metode *Pixel Indicator Technique* yang merupakan pengembangan dari metode *Least Significant Bit*.

Pada skripsi ini akan dibangun perangkat lunak yang dapat mengimplementasikan steganografi dengan metode *Least Significant Bit*, metode *Pixel Indicator Technique*, dan modifikasi dari metode *Pixel Indicator Technique*. Pada perangkat lunak diimplementasikan modifikasi dari *Pixel Indicator Technique* dengan tujuan untuk melengkapi beberapa kelemahan yang terdapat pada metode *Pixel Indicator Technique*.

Berdasarkan hasil pengujian yang dilakukan, dapat disimpulkan bahwa perangkat lunak yang dibangun dapat mengimplementasikan steganografi dengan metode *Least Significant Bit*, metode *Pixel Indicator Technique*, dan modifikasi dari metode *Pixel Indicator Technique*.

Kata-kata kunci: Steganografi, *Least Significant Bit*, *Pixel Indicator Technique*, LSB, PIT, MPIT

ABSTRACT

Steganography is one of several techniques that can be used to protect the secrecy of information. Steganography is the science of hiding information by embedding data into media. Media that can be used to hide secret information are image, audio, video, etc. In this undergraduate thesis, the media that is used to hide secret information is image. There are several steganography methods that use image to hide secret information. Those type of steganography methods is called image steganography. Least Significant Bit is one of image steganography methods. In Least Significant Bit method, the least significant bit of every color channel in every pixel replace with a bit from secret information. This technique is too simple so the secret information that embedded in the image become unsecured. Therefore, Pixel Indicator Technique is created as the improvement of Least Significant Bit method.

In this undergraduate thesis, a software is developed to implement Least Significant Bit, Pixel Indicator Technique, and Modified Pixel Indicator Technique method. The purpose of implementing Modified Pixel Indicator Technique is to improve the original Pixel Indicator Technique.

Based on the test done, it can be concluded that the software can implement Least Significant Bit, Pixel Indicator Technique, and Modified Pixel Indicator Technique.

Keywords: Steganography, Least Significant Bit Method, Pixel Indicator Technique, LSB, PIT, MPIT

«Dipersembahkan kepada Tuhan Yang Maha Esa, keluarga, Ibu Mariskha, dan setiap orang yang membantu proses pengerjaan skripsi ini»

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmat-Nya penulis berhasil menyelesaikan penyusunan skripsi yang berjudul "Implementasi dan Analisis Steganografi dengan Metode LSB, PIT, dan Modified PIT". Penulis menyadari bahwa penyusunan skripsi ini tidak akan selesai tanpa bantuan dan dukungan berbagai pihak. Oleh karena itu, penulis ingin mengucapkan terimakasih kepada:

- Ibu Mariskha atas motivasi dan bimbingan yang membantu meningkatkan semangat belajar penulis sehingga dapat menyelesaikan penyusunan skripsi.
- Kedua orang tua dan adik penulis atas kesabaran dan dukungannya.
- Pak Pascal dan Pak Husnul atas masukan dan saran yang telah diberikan sebagai dosen penguji.
- Abraham atas kesabarannya mengajari penulis serta ketekunannya dalam belajar sehingga penulis merasa tidak mau kalah dan semakin terpacu untuk menyelesaikan penulisan skripsi.
- Pincanny, Raymond, Senna, Jill atas kesabarannya tidak mengajak penulis untuk main sehingga penulis dapat menyelesaikan penulisan skripsi.
- Glorya, Vica, Caca, Rachael, dan Nancy yang seringkali saling menjatuhkan sehingga membuat penulis tahan banting menghadapi perkuliahan.
- Teman-teman IT 2013 yang menemani dan menghibur penulis sepanjang masa perkuliahan.
- Semua pihak yang tidak mungkin disebutkan satu-persatu yang sudah memberikan bantuan dan dukungan sepanjang masa perkuliahan dan pengerjaan skripsi ini.

Semoga segala bantuan dan dukungan dari semua pihak tersebut mendapat berkah dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf apabila terdapat kekurangan dalam penyusunan skripsi ini. Semoga skripsi ini berguna bagi semua pihak yang memerlukan.

Bandung, Mei 2018

Penulis

DAFTAR ISI

| | |
|-------------------------------------------------------------------------------|-------------|
| KATA PENGANTAR | xv |
| DAFTAR ISI | xvii |
| DAFTAR GAMBAR | xix |
| DAFTAR TABEL | xxi |
| 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Tujuan | 2 |
| 1.4 Batasan Masalah | 2 |
| 1.5 Metodologi | 3 |
| 1.6 Sistematika Pembahasan | 3 |
| 2 LANDASAN TEORI | 5 |
| 2.1 Steganografi | 5 |
| 2.2 Steganografi dengan Metode <i>Least Significant Bit</i> | 6 |
| 2.3 Steganografi dengan Metode <i>Pixel Indicator Technique</i> | 7 |
| 2.4 Perhitungan Kualitas Gambar | 8 |
| 2.4.1 <i>Mean-Squared Error</i> | 8 |
| 2.4.2 <i>Peak Signal to Noise Ratio</i> | 9 |
| 2.5 Steganalisis <i>Chi-Squared</i> | 9 |
| 3 ANALISIS | 11 |
| 3.1 Analisis Masalah | 11 |
| 3.2 Analisis Metode Steganografi | 12 |
| 3.2.1 Analisis Metode Steganografi <i>Least Significant Bit</i> | 13 |
| 3.2.2 Analisis Metode Steganografi <i>Pixel Indicator Technique</i> | 14 |
| 3.3 Modifikasi Metode Steganografi <i>Pixel Indicator Technique</i> | 16 |
| 3.4 Perhitungan Kualitas Gambar | 18 |
| 3.5 Analisis Steganalisis <i>Chi-squared</i> | 19 |
| 3.6 Analisis Perangkat Lunak | 20 |
| 3.6.1 Diagram Aktivitas | 20 |
| 3.6.2 Diagram Kelas Awal | 23 |
| 4 PERANCANGAN | 25 |
| 4.1 Kebutuhan Masukan dan Keluaran | 25 |
| 4.2 Rancangan Antarmuka | 26 |
| 4.3 Diagram Kelas Rinci | 28 |
| 4.4 Rincian Metode | 29 |
| 4.4.1 Kelas ImageProcessor | 29 |

| | | |
|----------|--------------------------------------------------------------------------------------------|-----------|
| 4.4.2 | Kelas Steganography | 32 |
| 4.4.3 | Kelas LSBSteganography | 33 |
| 4.4.4 | Kelas PITSteganography | 34 |
| 4.4.5 | Kelas MPITSteganography | 38 |
| 4.4.6 | Kelas HideGUI | 41 |
| 4.4.7 | Kelas ExtractGUI | 41 |
| 5 | IMPLEMENTASI DAN PENGUJIAN | 43 |
| 5.1 | Implementasi Antarmuka | 43 |
| 5.2 | Pengujian Fungsional | 43 |
| 5.2.1 | Pengujian Fungsional Metode <i>Least Significant Bit</i> | 45 |
| 5.2.2 | Pengujian Fungsional Metode <i>Pixel Indicator Technique</i> | 46 |
| 5.2.3 | Pengujian Fungsional Metode <i>Modified Pixel Indicator Technique</i> | 47 |
| 5.2.4 | Kesimpulan Pengujian Fungsional | 48 |
| 5.3 | Pengujian Eksperimental | 48 |
| 5.3.1 | Pengujian Panjang Karakter <i>Secret Data</i> | 49 |
| 5.3.2 | Pengujian Kualitas Gambar | 51 |
| 5.3.3 | Pengujian Ketahanan Metode Steganografi terhadap Steganalisis <i>Chi-squared</i> | 52 |
| 5.3.4 | Kesimpulan Pengujian Eksperimental | 54 |
| 6 | KESIMPULAN DAN SARAN | 55 |
| 6.1 | Kesimpulan | 55 |
| 6.2 | Saran | 56 |
| | DAFTAR REFERENSI | 57 |
| | A KODE PROGRAM | 59 |
| | B KODE PROGRAM IRVAN FEBRIANTO HALIM (2012730061) | 85 |

DAFTAR GAMBAR

| | | |
|------|-----------------------------------------------------------------------------------------------------------------------|----|
| 1.1 | Steganografi dengan media gambar | 1 |
| 2.1 | Tampilan antarmuka perangkat lunak <i>Chi-squared</i> yang dibangun oleh Irvan Febrianto Halim (2012730061) | 10 |
| 3.1 | Contoh keluaran perangkat lunak <i>Chi-squared</i> yang dimodifikasi | 20 |
| 3.2 | <i>Stego image</i> yang digunakan untuk implementasi <i>Chi-squared</i> | 20 |
| 3.3 | Diagram aktivitas proses implementasi penyisipan pesan ke dalam gambar pada perangkat lunak | 21 |
| 3.4 | Diagram aktivitas proses ekstraksi pesan dari dalam gambar pada perangkat lunak | 22 |
| 3.5 | Diagram kelas awal | 23 |
| 4.1 | Rancangan antarmuka proses penyisipan <i>secret data</i> | 26 |
| 4.2 | Rancangan antarmuka proses ekstraksi <i>secret data</i> | 28 |
| 4.3 | Diagram Kelas Rinci | 29 |
| 4.4 | Kelas ImageProcessor | 31 |
| 4.5 | Kelas Steganography | 32 |
| 4.6 | Kelas LSBSteganography | 34 |
| 4.7 | Kelas PITSteganography | 37 |
| 4.8 | Kelas MPITSteganography | 38 |
| 4.9 | Kelas HideGUI | 41 |
| 4.10 | Kelas ExtractGUI | 41 |
| 5.1 | Tampilan antarmuka penyisipan pesan rahasia | 44 |
| 5.2 | Tampilan jendela <i>pop up</i> apabila proses berhasil | 44 |
| 5.3 | Tampilan antarmuka ekstraksi pesan rahasia | 44 |
| 5.4 | Pengujian fungsional implementasi penyisipan <i>secret data</i> dengan metode LSB | 45 |
| 5.5 | Pengujian fungsional implementasi ekstraksi <i>secret data</i> dengan metode LSB | 45 |
| 5.6 | Jendela <i>pop up</i> yang tampil apabila penyisipan berhasil dilakukan | 46 |
| 5.7 | Pengujian fungsional implementasi penyisipan <i>secret data</i> dengan metode PIT | 46 |
| 5.8 | Jendela <i>pop up</i> yang tampil apabila penyisipan berhasil dilakukan | 46 |
| 5.9 | Pengujian fungsional implementasi ekstraksi <i>secret data</i> dengan metode PIT | 47 |
| 5.10 | Pengujian fungsional implementasi penyisipan <i>secret data</i> dengan metode <i>Modified</i> PIT | 47 |
| 5.11 | Pengujian fungsional implementasi ekstraksi <i>secret data</i> dengan metode <i>Modified</i> PIT | 48 |
| 5.12 | Jendela <i>pop up</i> yang tampil apabila penyisipan berhasil dilakukan | 48 |
| 5.13 | <i>Cover image</i> pertama untuk pengujian panjang <i>secret data</i> | 49 |
| 5.14 | <i>Cover image</i> kedua untuk pengujian panjang <i>secret data</i> | 49 |
| 5.15 | <i>Cover image</i> untuk pengujian kualitas gambar | 51 |
| 5.16 | <i>Cover image</i> pertama untuk pengujian ketahanan metode steganografi | 52 |
| 5.17 | <i>Cover image</i> kedua untuk pengujian ketahanan metode steganografi | 52 |

DAFTAR TABEL

| | | |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 2.1 | Tabel contoh nilai piksel awal untuk steganografi dengan metode LSB | 6 |
| 2.2 | Tabel contoh nilai piksel <i>stego image</i> untuk steganografi dengan metode LSB . . . | 6 |
| 2.3 | Tabel kriteria pemilihan indikator <i>channel</i> warna | 7 |
| 2.4 | Tabel kriteria pemilihan indikator <i>channel</i> warna | 8 |
| 3.1 | Tabel nilai piksel pada <i>cover media</i> | 13 |
| 3.2 | Tabel perbandingan nilai piksel awal dan nilai piksel setelah disisipkan bit <i>secret data</i> dengan metode LSB | 14 |
| 3.3 | Tabel perbandingan nilai piksel awal dan nilai piksel setelah disisipkan panjang <i>secret data</i> | 14 |
| 3.4 | Tabel perbandingan nilai piksel awal dan nilai piksel setelah disisipkan bit <i>secret data</i> dengan teknik indikasi piksel | 16 |
| 3.5 | Tabel perbandingan nilai piksel awal dan nilai piksel setelah disisipkan bit <i>secret data</i> dengan teknik indikasi piksel yang dimodifikasi | 17 |
| 3.6 | Tabel perbandingan nilai piksel <i>cover image</i> dan nilai piksel <i>stego image</i> | 18 |
| 5.1 | Tabel pengujian eksperimental dengan <i>secret data</i> "IT" dengan panjang karakter sama dengan 2 | 49 |
| 5.2 | Tabel pengujian eksperimental dengan masukan <i>secret data</i> "IT123" dengan panjang karakter sama dengan 5 | 50 |
| 5.3 | Tabel pengujian eksperimental dengan <i>secret data</i> "informatik" dengan panjang karakter sama dengan 10 | 50 |
| 5.4 | Tabel pengujian eksperimental dengan <i>secret data</i> "Informatika2013" dengan panjang karakter sama dengan 15 | 50 |
| 5.5 | Tabel pengujian eksperimental dengan <i>secret data</i> "Informatika Unpar 2013!!!" dengan panjang karakter sama dengan 25 | 51 |
| 5.6 | Tabel pengujian eksperimental dengan <i>secret data</i> "Teknik Informatika UnikaParahyangan" dengan panjang karakter sama dengan 35 | 51 |
| 5.7 | Tabel pengujian eksperimental dengan <i>secret data</i> "Teknik Informatika Universitas Parahyangan!!!" dengan panjang karakter sama dengan 45 | 51 |
| 5.8 | Tabel pengujian eksperimental kualitas gambar | 52 |
| 5.9 | Tabel pengujian eksperimental <i>Chi-squared</i> dengan panjang <i>secret data</i> 50 | 53 |
| 5.10 | Tabel pengujian eksperimental <i>Chi-squared</i> dengan panjang <i>secret data</i> 100 | 53 |
| 5.11 | Tabel pengujian eksperimental <i>Chi-squared</i> dengan panjang <i>secret data</i> 100 | 53 |
| 5.12 | Tabel pengujian eksperimental <i>Chi-squared</i> dengan panjang <i>secret data</i> 255 | 54 |

BAB 1

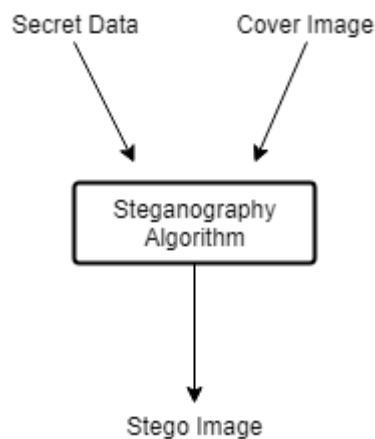
PENDAHULUAN

1.1 Latar Belakang

Informasi pada saat ini menjadi kebutuhan pokok bagi manusia. Teknologi yang digunakan untuk menyebarkan informasi pun selalu dikembangkan sehingga setiap orang bisa mendapatkan informasi dengan mudah. Namun, tidak semua informasi bersifat umum. Beberapa informasi bersifat rahasia dan hanya boleh diketahui oleh satu atau sekelompok orang tertentu. Penyebaran informasi yang bersifat rahasia harus dilakukan dengan hati-hati supaya informasi rahasia tersebut tidak diterima oleh pihak-pihak yang salah. Oleh karena itu, dibutuhkan teknik-teknik keamanan yang dapat menjaga kerahasiaan informasi dalam penyebarannya.

Steganografi merupakan salah satu teknik yang digunakan untuk menjaga keamanan suatu informasi dengan cara menyembunyikannya dalam suatu media [1]. Salah satu bentuk dari informasi rahasia adalah teks berupa String. Informasi rahasia disebut dengan istilah *secret data*. Penyembunyian *secret data* dapat dilakukan dengan menggunakan berbagai bentuk media, antara lain teks, audio, gambar, video, dan lain sebagainya. Media yang digunakan untuk menyembunyikan *secret data* disebut *cover media*.

Salah satu media yang dapat digunakan untuk menyembunyikan *secret data* adalah gambar. Jenis gambar yang dapat digunakan untuk menyisipkan *secret data* dapat bermacam-macam seperti gambar hitam putih dan *grayscale*, serta gambar berwarna seperti gambar RGB dan CMYK. Selain itu, format gambar yang dapat digunakan untuk penyembunyian *secret data* juga bermacam-macam. Salah satu format gambar yang direkomendasikan untuk digunakan dalam implementasi steganografi adalah BMP. Gambar BMP memiliki kelebihan yaitu *lossless compression* [2] sehingga gambar yang sudah diubah dapat direkonstruksi kembali. Apabila media yang digunakan untuk implementasi steganografi adalah gambar, maka *cover media* dapat disebut juga dengan *cover image*. Gambar hasil implementasi steganografi disebut dengan *stego image*. Ilustrasi steganografi dengan media gambar dapat dilihat pada Gambar 1.1.



Gambar 1.1: Steganografi dengan media gambar

Banyak metode steganografi dapat digunakan untuk menyembunyikan informasi dalam gambar. Salah satu metode steganografi yang sudah banyak digunakan adalah *Least Significant Bit (LSB)*. Teknik ini memanfaatkan nilai-nilai *channel* warna pada piksel-piksel *cover media*. *Secret data* akan disisipkan pada bit terakhir setiap *channel* warna dalam setiap piksel secara berurutan. Bit yang digunakan dalam penyisipan adalah bit-bit terakhir supaya nilai-nilai setiap *channel* warna tidak mengalami perubahan besar sehingga tidak menimbulkan perbedaan besar antara *cover media* dengan *stego image*. Penyisipan bit-bit *secret data* dengan teknik LSB tergolong sangat sederhana dan mudah diimplementasikan. Selain itu, karena pola penyisipan *secret data* mudah ditebak, pihak yang tidak berkepentingan dapat dengan mudah mendapatkan *secret data* yang terdapat pada gambar. Oleh karena itu, dibangunlah pengembangan dari metode LSB, yaitu *Pixel Indicator Technique (PIT)*. Sama seperti LSB, metode PIT memanfaatkan nilai-nilai *channel* warna pada piksel-piksel *cover media* dan menggunakan bit-bit terakhir untuk penyisipan *secret data*. Bedanya, metode PIT tidak menyembunyikan *secret data* di setiap *channel* warna pada setiap piksel. Letak penyisipan *secret data* bergantung pada panjang *secret data* itu sendiri. Dari panjang *secret data* tersebut kemudian akan ditentukan *channel* warna yang akan menjadi indikator penyisipan *secret data* pada setiap piksel. Meskipun terlihat lebih aman daripada LSB, metode PIT masih memiliki kelemahan karena panjang *secret data*, yang menjadi penentu pola penyisipan, ikut disisipkan ke dalam *cover image*. Oleh karena itu, dibangunlah metode *Modified PIT* yang merupakan modifikasi dari metode PIT untuk mengatasi kelemahan metode PIT tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah pada skripsi ini adalah sebagai berikut.

1. Bagaimana cara melakukan modifikasi terhadap metode *Pixel Indicator Technique* supaya dapat mengatasi kelemahan metode tersebut?
2. Bagaimana cara mengimplementasikan steganografi dengan metode *Least Significant Bit*, *Pixel Indicator Technique*, dan *Modified Pixel Indicator Technique*?
3. Bagaimana perbandingan steganografi dengan metode *Least Significant Bit*, *Pixel Indicator Technique*, dan *Modified Pixel Indicator Technique*?

1.3 Tujuan

Berdasarkan rumusan masalah, maka tujuan dari skripsi ini adalah sebagai berikut.

1. Mempelajari cara melakukan modifikasi terhadap metode *Pixel Indicator Technique* supaya dapat mengatasi kelemahan metode tersebut.
2. Mengimplementasikan steganografi dengan metode *Least Significant Bit*, *Pixel Indicator Technique*, dan *Modified Pixel Indicator Technique*.
3. Membandingkan steganografi dengan metode *Least Significant Bit*, *Pixel Indicator Technique*, dan *Modified Pixel Indicator Technique* berdasarkan kapasitas penyisipan *secret data*, perhitungan kualitas gambar, uji Steganalisis *Chi-squared*.

1.4 Batasan Masalah

Batasan-batasan masalah dalam skripsi ini adalah sebagai berikut.

1. *Cover image* merupakan gambar bertipe RGB.

2. *Secret data* merupakan karakter yang terdapat pada Tabel ASCII.
3. *Stego image* merupakan gambar dengan format BMP.

1.5 Metodologi

Metodologi yang digunakan dalam penyusunan skripsi ini adalah sebagai berikut.

1. Melakukan studi literatur mengenai steganografi dengan metode *Least Significant Bit*.
2. Melakukan studi literatur mengenai steganografi dengan metode *Pixel Indicator Technique*.
3. Mengimplementasikan steganografi dengan metode *Least Significant Bit* dan *Pixel Indicator Technique* secara manual.
4. Melakukan perancangan kelas yang akan digunakan untuk mengimplementasikan metode *Least Significant Bit*, *Pixel Indicator Technique*, dan *Pixel Indicator Technique* yang dimodifikasi.
5. Mengimplementasikan hasil perancangan kelas ke dalam bahasa pemrograman *Java*.
6. Melakukan pengujian fungsional dan pengujian eksperimental terhadap perangkat lunak yang mengimplementasikan *Least Significant Bit*, *Pixel Indicator Technique*, dan *Pixel Indicator Technique* yang dimodifikasi.
7. Menarik kesimpulan berdasarkan hasil pengujian.

1.6 Sistematika Pembahasan

Skripsi ini akan tersusun dalam enam bab secara sistematis. Enam bab tersebut terdiri dari pendahuluan, dasar teori, analisis, perancangan, implementasi dan pengujian, dan kesimpulan. Berikut merupakan sistematika pembahasan dalam skripsi ini.

1. Bab 1 Pendahuluan

Bab ini berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, dan sistematika pembahasan.

2. Bab 2 Dasar Teori

Bab 2 berisi dasar teori mengenai steganografi dengan metode *Least Significant Bit*, steganografi dengan metode *Pixel Indicator Technique*, *Mean-Squared Error (MSE)* dan *Peak Signal to Noise Ratio (PSNR)* untuk menghitung kualitas gambar, serta steganalisis *Chi-squared* untuk menguji ketahanan metode steganografi.

3. Bab 3 Analisis

Bab 3 berisi analisis masalah, analisis metode steganografi *Least Significant Bit*, *Pixel Indicator Technique* dan *Pixel Indicator Technique* yang dimodifikasi, analisis perhitungan kualitas gambar, analisis steganalisis *Chi-squared*, diagram aktivitas, dan diagram kelas awal.

4. Bab 4 Perancangan

Bab 4 berisi perancangan perangkat lunak yang akan dibangun, meliputi kebutuhan masukan dan keluaran, rancangan antarmuka, diagram kelas rinci, dan rincian metode yang digunakan pada perangkat lunak.

5. Bab 5 Implementasi dan Pengujian

Bab 5 berisi implementasi antarmuka perangkat lunak, pengujian fungsional terhadap perangkat lunak yang mengimplementasikan *Least Significant Bit*, *Pixel Indicator Technique* dan *Pixel Indicator Technique* yang dimodifikasi, serta pengujian eksperimental terhadap perangkat lunak yang mengimplementasikan *Least Significant Bit*, *Pixel Indicator Technique* dan *Pixel Indicator Technique* yang dimodifikasi.

6. Bab 6 Kesimpulan dan Saran

Bab 6 berisi kesimpulan dari awal hingga akhir skripsi beserta saran untuk pengembangan selanjutnya.