

**SKRIPSI**

**PERBANDINGAN KUALITAS GAMBAR PADA  
STEGANOGRAFI MENGGUNAKAN METODE LEAST  
SIGNIFICANT BIT DAN ALGORITMA TRIPLE A**



**Claudia Veronica Hanurawan**

**NPM: 2013730012**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS  
UNIVERSITAS KATOLIK PARAHYANGAN  
2019**

**UNDERGRADUATE THESIS**

**IMAGE QUALITY COMPARISON ON STEGANOGRAPHY  
USING LEAST SIGNIFICANT BIT METHOD AND TRIPLE A  
ALGORITHM**



**Claudia Veronica Hanurawan**

**NPM: 2013730012**

**DEPARTMENT OF INFORMATICS  
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES  
PARAHYANGAN CATHOLIC UNIVERSITY  
2019**

# LEMBAR PENGESAHAN

## PERBANDINGAN KUALITAS GAMBAR PADA STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DAN ALGORITMA TRIPLE A

Claudia Veronica Hanurawan

NPM: 2013730012

Bandung, 8 Januari 2019

Menyetujui,

Pembimbing

Mariskha Tri Adithia, P.D.Eng

Ketua Tim Penguji

Anggota Tim Penguji

Pascal Alfadian, M.Comp.

Natalia, M.Si.

Mengetahui,

Ketua Program Studi

Mariskha Tri Adithia, P.D.Eng

## **PERNYATAAN**

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

### **PERBANDINGAN KUALITAS GAMBAR PADA STEGANOGRAFI MENGUNAKAN METODE LEAST SIGNIFICANT BIT DAN ALGORITMA TRIPLE A**

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 8 Januari 2019

Meterai Rp. 6000
---------------------

Claudia Veronica Hanurawan  
NPM: 2013730012

## ABSTRAK

Informasi adalah hal yang sangat mudah menyebar khususnya pada era digital. Namun, ada informasi yang bersifat rahasia. Salah satu teknik keamanan yang dapat menjaga kerahasiaan sebuah informasi adalah steganografi. Steganografi adalah seni menyembunyikan informasi ke dalam sebuah media sehingga keberadaan dari suatu informasi tidak dapat diketahui. Media tersebut dapat berupa gambar, audio, video, dan lain-lain. Media yang digunakan pada skripsi ini adalah gambar. Terdapat beberapa metode dalam steganografi dengan menggunakan media gambar. Salah satu metode tersebut adalah *Least Significant Bit*. Penyembunyiannya dilakukan dengan cara menyisipkan pesan rahasia pada bit terakhir di setiap *channel* warna dari gambar. Metode ini dianggap sangat sederhana dan kurang aman sehingga dapat diserang dengan mudah. Oleh karena itu, terdapat metode lain yang merupakan pengembangan dari metode *Least Significant Bit* yaitu Algoritma Triple A.

Pada skripsi ini, dibangun sebuah perangkat lunak yang dapat mengimplementasikan steganografi dengan metode *Least Significant Bit* dan Algoritma Triple A. Berdasarkan hasil pengujian yang dilakukan, perangkat lunak yang dibangun dapat mengimplementasikan steganografi dengan metode *Least Significant Bit* dan Algoritma Triple A. Kualitas gambar yang dihasilkan juga berbeda, tergantung dari kapasitas setiap metode dan panjangnya pesan rahasia yang disisipkan.

**Kata-kata kunci:** Steganografi, *Least Significant Bit*, Algoritma Triple A, LSB

## **ABSTRACT**

Information is an easy thing to spread especially in this digital era. However, there is confidential information. Steganography is the art of hiding an information by embedding data into media. Many different digital file format can be used such as image, audio, video, and other digital files. Image is media that is used to hide secret message in this undergraduate thesis. There are several methods proposed for image based steganography. One of the those methods is called Least Significant Bit. In Least Significant Bit, the least significant bit for every channel of each pixel is replaced with a bit from the secret message. This method is the simplest one so that become unsecured. Therefore, Triple A Algorithm is created as the improvement of Least Significant Bit.

In this undergraduate thesis, a software is built to implement Least Significant Bit method and Triple A Algorithm method. For a conclusion based on some tests done, the software can implement Least Significant Bit and Triple A Algorithm method. Comparison of Image Quality produced is various, depends on the capacity of its method and the length of secret message that will be embedded.

**Keywords:** Steganography, Least Significant Bit, Triple A Algorithm, LSB

*Dipersembahkan kepada Tuhan Yang Maha Esa dan orang-orang  
yang selalu ada di hati penulis*

## KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa karena atas berkat dan rahmatNya penulis berhasil menyelesaikan penyusunan skripsi yang berjudul "Perbandingan Kualitas Gambar Pada Steganografi Menggunakan Metode Least Significant Bit dan Algoritma Triple A". 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 sebagai dosen pembimbing atas motivasi dan bimbingannya sehingga mampu menyelesaikan penyusunan skripsi.
- Keluarga yang selalu memberikan dukungan dan semangat untuk menyelesaikan penyusunan skripsi.
- Pak Pascal dan Ibu Natalia sebagai dosen penguji atas saran yang diberikan untuk perbaikan penyusunan skripsi.
- Kevin Sipit sebagai pahlawan tanpa tanda jasa yang sangat membantu dalam penyusunan skripsi.
- Fadel atas kehadiran dan ketersediaan untuk menemani saat pengerjaan skripsi.
- Ilham dan Bima atas kontrakan BJ 7B dan Raben I 9B yang sudah menyediakan tempat untuk penulis mengerjakan skripsi ini.
- Glorya dan Caca atas dukungan dan dorongan untuk makan pada dini hari sehingga penulis menambah berat badannya sebanyak 7 kg dan mencapai puncak berat badan penulis semasa hidup.
- Glorya, Renal, Jessica, Nancy, Rachael, dan Wesley yang selalu membantu melatih keteguhan hati penulis untuk tidak bermain.
- Mondy, Kiwil, dan Ethman yang selalu mengajak penulis untuk bernyanyi dalam *band* sehingga penulis dapat menambah pundi-pundi uang jajan.
- Semua pihak yang tidak dapat disebutkan satu-persatu atas dukungan dan bantuan dalam pengerjaan skripsi.

Semoga dukungan dan bantuan dari semua pihak mendapat berkah dari Tuhan Yang Maha Esa. Akhir kata, penulis memohon maaf jika terdapat kekurangan pada penulisan skripsi ini. Semoga skripsi ini dapat berguna bagi pihak yang membutuhkan.

Bandung, Januari 2019

Penulis



## DAFTAR ISI

<b>KATA PENGANTAR</b>	<b>xv</b>
<b>DAFTAR ISI</b>	<b>xvii</b>
<b>DAFTAR GAMBAR</b>	<b>xix</b>
<b>DAFTAR TABEL</b>	<b>xxi</b>
<b>1 PENDAHULUAN</b>	<b>1</b>
1.1 Latar Belakang . . . . .	1
1.2 Rumusan Masalah . . . . .	2
1.3 Tujuan . . . . .	2
1.4 Batasan Masalah . . . . .	2
1.5 Metodologi . . . . .	2
1.6 Sistematika Pembahasan . . . . .	3
<b>2 LANDASAN TEORI</b>	<b>5</b>
2.1 Steganografi . . . . .	5
2.2 Steganografi dengan Metode <i>Least Significant Bit</i> . . . . .	6
2.3 Steganografi dengan Metode Algoritma Triple A . . . . .	8
2.4 Perhitungan Kualitas Gambar . . . . .	10
2.4.1 <i>Peak Signal-to-Noise Ratio</i> [PSNR] . . . . .	10
2.4.2 <i>Mean-Squared Error</i> (MSE) . . . . .	11
<b>3 ANALISIS</b>	<b>13</b>
3.1 Analisis masalah . . . . .	13
3.2 Analisis Metode Steganografi . . . . .	14
3.2.1 Analisis Metode Steganografi <i>Least Significant Bit</i> . . . . .	15
3.2.2 Analisis Metode Steganografi Algoritma Triple A . . . . .	16
3.3 Perhitungan Kualitas Gambar . . . . .	17
3.4 Analisis Perangkat Lunak . . . . .	18
3.4.1 Diagram Aktivitas . . . . .	18
3.4.2 Diagram Kelas Awal . . . . .	21
<b>4 PERANCANGAN</b>	<b>23</b>
4.1 Kebutuhan Masukan dan Keluaran . . . . .	23
4.2 Rancangan Antarmuka . . . . .	24
4.3 Diagram Kelas Rinci . . . . .	26
4.4 Rincian Metode . . . . .	27
4.4.1 Kelas GUIMainMenu . . . . .	28
4.4.2 Kelas GUIHide . . . . .	28
4.4.3 Kelas GUIExtract . . . . .	28
4.4.4 Kelas CoverMedia . . . . .	29

4.4.5	Kelas Steganography . . . . .	30
4.4.6	Kelas LSB . . . . .	31
4.4.7	Kelas TripleAAlgorithm . . . . .	33
<b>5</b>	<b>IMPLEMENTASI DAN PENGUJIAN</b>	<b>37</b>
5.1	Implementasi Antarmuka . . . . .	37
5.2	Pengujian Fungsional . . . . .	39
5.2.1	Pengujian Fungsional Metode <i>Least Significant Bit</i> . . . . .	39
5.2.2	Pengujian Fungsional Metode Algoritma Triple A . . . . .	41
5.3	Pengujian Eksperimental . . . . .	43
5.3.1	Pengujian Eksperimental Menggunakan Gambar Berwarna . . . . .	43
5.3.2	Pengujian Eksperimental Menggunakan Gambar Hitam Putih . . . . .	44
5.3.3	Pengujian Eksperimental Menggunakan Gambar Polos Berwarna . . . . .	45
5.3.4	Pengujian Eksperimental dengan Memaksimalkan Kapasitas metode LSB . . . . .	45
5.3.5	Kesimpulan Pengujian Fungsional dan Eksperimental . . . . .	46
<b>6</b>	<b>KESIMPULAN DAN SARAN</b>	<b>49</b>
6.1	Kesimpulan . . . . .	49
6.2	Saran . . . . .	50
	<b>DAFTAR REFERENSI</b>	<b>51</b>
	<b>A KODE PROGRAM</b>	<b>53</b>

## DAFTAR GAMBAR

2.1	Contoh <i>cover media</i> untuk steganografi dengan metode LSB. . . . .	7
2.2	Contoh hasil <i>stego image</i> setelah dilakukan penyisipan dengan metode LSB. . . . .	8
2.3	Contoh <i>cover media</i> untuk steganografi dengan metode Algoritma Triple A. . . . .	9
3.1	Contoh <i>Cover media</i> untuk analisis metode steganografi . . . . .	14
3.2	Hasil perhitungan <i>MSE</i> dan <i>PSNR</i> . . . . .	17
3.3	Diagram aktivitas proses penyisipan . . . . .	19
3.4	Diagram aktivitas proses ekstraksi <i>secret message</i> . . . . .	20
3.5	Diagram kelas awal . . . . .	21
4.1	Rancangan antarmuka menu awal . . . . .	24
4.2	Rancangan antarmuka proses penyisipan . . . . .	25
4.3	Rancangan antarmuka proses ekstraksi <i>secret message</i> . . . . .	26
4.4	Diagram Kelas Rinci . . . . .	27
4.5	Diagram Kelas GUIMainMenu . . . . .	28
4.6	Diagram Kelas GUIHide . . . . .	28
4.7	Diagram Kelas GUIExtract . . . . .	29
4.8	Diagram Kelas CoverMedia . . . . .	29
4.9	Diagram Kelas Steganography . . . . .	30
4.10	Diagram kelas LSB . . . . .	31
4.11	Diagram kelas TripleAAlgorithm . . . . .	33
5.1	Tampilan antarmuka menu awal . . . . .	37
5.2	Tampilan antarmuka proses penyisipan . . . . .	38
5.3	Tampilan antarmuka proses ekstraksi . . . . .	39
5.4	Tampilan antarmuka jendela <i>pop up</i> apabila masukan salah . . . . .	39
5.5	Pengujian fungsional hasil implementasi penyisipan <i>secret message</i> dengan metode LSB . . . . .	40
5.6	Hasil <i>stego image</i> dari penyisipan . . . . .	40
5.7	Pengujian fungsional hasil implementasi ekstraksi <i>secret message</i> dengan metode LSB . . . . .	41
5.8	Pengujian fungsional hasil implementasi antarmuka jika masukkan salah . . . . .	41
5.9	Pengujian fungsional hasil implementasi penyisipan <i>secret message</i> dengan metode Algoritma Triple A . . . . .	42
5.10	Pengujian fungsional hasil implementasi ekstraksi <i>secret message</i> dengan metode Algoritma Triple A . . . . .	42
5.11	Pengujian fungsional hasil implementasi antarmuka jika masukkan salah . . . . .	43
5.12	Gambar berwarna . . . . .	44
5.13	Gambar hitam putih . . . . .	44
5.14	Gambar polos berwarna . . . . .	45
5.15	Gambar 4x4 piksel . . . . .	45

## DAFTAR TABEL

2.1	Tabel contoh nilai piksel awal untuk steganografi dengan metode LSB . . . . .	7
2.2	Tabel contoh nilai piksel awal bernilai biner untuk steganografi dengan metode LSB	7
2.3	Tabel contoh nilai piksel setelah disisipkan <i>secret message</i> . . . . .	7
2.4	Tabel <i>seed</i> 1 . . . . .	8
2.5	Tabel <i>seed</i> 2 . . . . .	8
2.6	Tabel contoh nilai piksel awal untuk steganografi dengan metode Algoritma Triple A	9
2.7	Tabel contoh nilai bilangan biner piksel awal untuk steganografi dengan metode Algoritma Triple A . . . . .	9
2.8	Tabel contoh nilai bilangan biner hasil iterasi pertama metode Algoritma Triple A	9
2.9	Tabel contoh nilai bilangan biner hasil iterasi kedua metode Algoritma Triple A . .	10
2.10	Tabel contoh nilai bilangan biner hasil iterasi ketiga metode Algoritma Triple A . .	10
3.1	Tabel nilai piksel bernilai desimal <i>cover media</i> untuk analisis metode steganografi .	14
3.2	Tabel nilai piksel bilangan biner <i>cover media</i> untuk analisis metode steganografi .	15
3.3	Tabel nilai piksel bilangan biner <i>stego image</i> setelah disisipkan <i>secret message</i> dengan metode LSB . . . . .	15
3.4	(b) Tabel nilai piksel bilangan biner <i>stego image</i> setelah disisipkan <i>secret message</i> menggunakan Algoritma Triple A . . . . .	16
3.5	Tabel nilai piksel <i>cover media</i> sebelum dilakukan penyisipan . . . . .	17
3.6	Tabel <i>stego image</i> hasil penyisipan menggunakan metode LSB . . . . .	17
5.1	Tabel hasil pengujian eksperimental dengan gambar berwarna . . . . .	43
5.2	Tabel hasil pengujian eksperimental dengan gambar hitam putih . . . . .	44
5.3	Tabel hasil pengujian eksperimental dengan gambar hitam putih . . . . .	45
5.4	Tabel nilai piksel bernilai desimal <i>stego image</i> setelah disisipkan <i>secret message</i> menggunakan Algoritma Triple A . . . . .	46

# BAB 1

## PENDAHULUAN

### 1.1 Latar Belakang

Informasi adalah hal yang sangat mudah menyebar. Seiring berkembangnya teknologi yang ada saat ini, informasi dapat dengan mudah diakses di belahan dunia manapun. Namun, informasi tidak semuanya bersifat umum. Ada informasi yang bersifat rahasia atau hanya boleh diketahui oleh orang-orang yang memiliki wewenang untuk mengaksesnya. Oleh karena itu, dibutuhkan teknik keamanan untuk menjaga agar hanya orang-orang yang berwenang yang dapat mengetahui informasi tersebut.

Salah satu teknik keamanan yang dapat digunakan adalah steganografi. Kata steganografi berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein* yang artinya menulis [1]. Pada zaman Yunani kuno, orang menulis pesan rahasia di sebuah papan kayu kemudian menutupinya dengan lilin atau dengan cara mencukur kepala seseorang, merajahnya, dan menunggu sampai rambutnya kembali tumbuh kemudian dikirimkan kepada penerima pesan.

Steganografi merupakan suatu seni untuk menyembunyikan informasi dengan cara menyisipkannya ke dalam sebuah media [2]. Informasi yang disembunyikan disebut *secret message*, sedangkan media yang dipakai untuk menyembunyikan *secret message* adalah *cover media*. *Secret message* yang digunakan berupa teks sehingga akan bertipe data String. *Cover Media* yang digunakan dapat berupa gambar, audio, video, dan lain-lain. Pada skripsi ini, *cover media* yang akan digunakan berupa gambar.

Gambar memiliki 2 jenis yaitu gambar tidak berwarna (hitam putih dan grayscale) dan gambar berwarna (RGB dan CMYK). Bentuk format gambar juga bermacam-macam seperti JPEG, BMP, PNG, GIF, dan lain sebagainya. Format yang direkomendasikan untuk digunakan untuk teknik steganografi salah satunya adalah PNG. Gambar PNG dipilih karena PNG merupakan salah satu format gambar dengan tingkat kompresi yang rendah (*lossless compression*) sehingga kualitas gambar tidak akan berubah.

Ada beberapa metode yang digunakan untuk menerapkan teknik steganografi, yaitu, *Least Significant Bit (LSB)*, *Pixel Indicator*, *Stego Color Cycle*, dan Algoritma Triple A. 2 metode yang akan dibahas pada skripsi ini adalah metode LSB dan Algoritma Triple A. LSB adalah metode paling sederhana dan mudah untuk diimplementasikan. Pertama-tama, piksel pada *cover media* dan *secret message* yang bertipe desimal diubah menjadi biner. Kemudian setiap bit pada *secret message* disisipkan ke bit terakhir pada setiap piksel *cover media* sehingga terbentuklah *stego image*. Untuk mendapatkan kembali *secret message*, dibutuhkan panjang dari *secret message* kemudian mengambil bit paling terakhir dari setiap *channel* sebanyak panjang dari *secret message* dan disusun menjadi *secret message*. Algoritma Triple A merupakan pengembangan dari metode LSB. Pemilihan jumlah bit dan channel dilakukan secara acak. Pengacakan jumlah bit dan channel dihasilkan dari *Pseudo Random Number Generator (PRNG)*. PRNG akan menghasilkan 2 buah bilangan yang disebut *seed 1* dan *seed 2*. *Seed 1* menunjukkan channel yang akan dipakai, *seed 2* menunjukkan jumlah bit yang dipakai. Bilangan-bilangan yang dibangkitkan dari PRNG dijadikan *stego key* dan dipakai untuk mendapatkan kembali *secret message*.

## 1.2 Rumusan Masalah

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

1. Bagaimana cara mengimplementasikan steganografi dengan metode *Least Significant Bit* dan Algoritma Triple A?
2. Bagaimana perbandingan kualitas gambar steganografi antara metode *Least Significant Bit* dan Algoritma Triple A?

## 1.3 Tujuan

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

1. Mengimplementasikan steganografi dengan metode *Least Significant Bit* dan Algoritma Triple A.
2. Membandingkan kualitas gambar steganografi antara metode *Least Significant Bit* dan Algoritma Triple A.

## 1.4 Batasan Masalah

Batasan-batasan masalah dalam skripsi ini adalah sebagai berikut.

1. *Cover media* yang dipakai dan *stego image* yang dihasilkan merupakan gambar bertipe PNG dengan model warna bertipe RGB.
2. *Secret message* yang dipakai merupakan karakter yang terdapat pada Tabel Unicode 0-7F.

## 1.5 Metodologi

Metodologi yang digunakan dalam penyusunan skripsi ini adalah sebagai berikut.

1. Melakukan studi literatur mengenai steganografi, metode *Least Significant Bit*, dan Algoritma Triple A.
2. Mengimplementasikan steganografi dengan metode *Least Significant Bit* dan Algoritma Triple A secara manual.
3. Melakukan perancangan diagram kelas dan diagram aktivitas yang akan digunakan untuk mengimplementasikan metode *Least Significant Bit* dan Algoritma Triple A.
4. Mengimplementasikan hasil perancangan ke dalam bahasa pemrograman *Java*.
5. Melakukan pengujian fungsional dan eksperimental terhadap perangkat lunak yang mengimplementasikan *Least Significant Bit* dan Algoritma Triple A.
6. 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, steganografi dengan metode *Least Significant Bit* dan Algoritma Triple A, *Mean-Squared Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR) untuk menghitung kualitas gambar.
3. Bab 3 Analisis Bab 3 berisi analisis masalah, analisis metode steganografi *Least Significant Bit* dan Algoritma Triple A, analisis perhitungan kualitas gambar, diagram kelas awal, dan diagram aktivitas.
4. Bab 4 Perancangan Bab 4 berisi perancangan perangkat lunak yang akan dibangun, termasuk kebutuhan masukan dan keluaran, rancangan antarmuka, diagram kelas rinci, dan rincian metode yang akan digunakan pada perangkat lunak.
5. Bab 5 Implementasi dan Pengujian Bab 5 berisi implementasi antarmuka perangkat lunak, implementasi metode *Least Significant Bit* dan Algoritma Triple A pada perangkat lunak, pengujian fungsional terhadap perangkat lunak yang mengimplementasikan metode *Least Significant Bit* dan Algoritma Triple A, serta pengujian eksperimental terhadap perangkat lunak yang mengimplementasikan metode *Least Significant Bit* dan Algoritma Triple A.
6. Bab 6 Kesimpulan dan Saran Bab 6 berisi kesimpulan dari awal hingga akhir skripsi beserta saran untuk pengembangan selanjutnya.