Implementasi Steganografi dalam Penyembunyian Pesan pada Citra Digital dengan Metode *Least Significant Bit*

Proposal

Disusun untuk melengkapi syarat-syarat

guna memeroleh gelar Sarjana Komputer

AMELIA APRILIANI

3145143626

PROGRAM STUDI ILMU KOMPUTER

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS NEGERI JAKARTA

2018

LEMBAR PENGESAHAN

Dengan ini saya mahasiswa Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Jakarta

Nama	: Amelia Apriliani
No. Registrasi	: 3145143626
Jurusan	: Ilmu Komputer
Judul	: Implementasi Steganografi dalam Penyembunyian Pesan pada Citra Digital dengan Metode *Least Significant Bit*.

Menyatakan bahwa proposal ini telah siap diajukan untuk seminar pra skripsi.

Menyetujui,

Dosen Pembimbing I	Dosen Pembimbing II
Drs. Mulyono, M.Kom.	**Ratna Widyati, S.Si, M.Kom.**
NIP. 119660517 199403 1 003	NIP. 19750925 200212 2 002

Mengetahui,

Ketua Program Studi Ilmu Komputer

Drs. Mulyono, M.Kom.

NIP. 119660517 199403 1 003

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

LATAR BELAKANG

1.1 Latar Belakang Masalah

Saat ini *internet* sudah berkembang menjadi salah satu media yang sangat populer di berbagai dunia [3]. Perkembangan *internet* memberikan pengaruh besar terhadap kemudahan dalam berkomunikasi dan menyampaikan informasi. Komunikasi merupakan salah satu hal yang penting bagi manusia. Manusia yang merupakan makhluk sosial cenderung melakukan komunikasi setiap hari, baik secara langsung maupun melalui media elektronik. Manusia melakukan komunikasi untuk bertukar informasi.

Kemudahan dalam berkomunikasi memberikan dampak positif dan negatif. Dampak positifnya yaitu cepatnya informasi dapat tersebar, baik antar daerah maupun antar negara. Dan dampak negatifnya adalah semakin berkembangnya kejahatan dalam penggunaan informasi. Dengan berbagai teknik, banyak orang yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu harus berkembang juga pengamanan sistem informasi.

Teknik pengamanan informasi yang ada saat ini seperti kriptografi dan steganografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan pesan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi telah ada dan digunakan sejak berabad-abad yang lalu dikenal dengan istilah kriptografi klasik, yang bekerja pada mode karakter alfabet [13].

Steganografi adalah seni dan sains komunikasi pesan yang tidak terlihat. Hal ini dilakukan dengan menyembunyikan informasi dalam informasi lain, misalnya menyembunyikan keberadaan informasi yang dikomunikasikan. Kata steganografi bera-

sal dari kata Yunani "stegos" yang berarti "cover" dan "grafia" yang berarti "menulis" yang mendefinisikannya sebagai "tulisan tertutup" [**?**].

Salah satu metode steganografi adalah *Least Significant Bit* (LSB). Algoritma LSB, menggantikan bit paling signifikan pada *file cover* sesuai dengan bit pesan. Teknik ini adalah teknik yang paling populer digunakan dalam steganografi untuk menyembunyikan pesan. Teknik ini biasanya efektif, karena substitusi LSB tidak menyebabkan degradasi kualitas yang signifikan [6].

Pengimplementasian metode Least Significant Bit pada steganografi sudah pernah dilakukan penelitian oleh Fahri Perdana Prasetyo dengan format file *.TIFF menggunakan bahasa pemrograman MATLAB [11]. Selain itu juga pernah dilakukan penelitian oleh Adiria dengan format file *.BMP menggunakan bahasa pemrograman Delphi [1]. Sedangkan yang akan penulis buat nantinya adalah dengan mengkombinasikan kedua penelitian tersebut.

Dengan penjabaran di atas, penulis mengkombinasikan jurnal-jurnal tersebut untuk melakukan penelitian tentang "**Implementasi Steganografi dalam Penyembunyian Pesan pada Citral Digital dengan Metode *Least Significant Bit***". Dengan adanya penelitian ini diharapkan dapat memberikan informasi mengenai steganografi.

1.2 Batasan Masalah

Batasan masalah dalam tugas akhir ini mencakup:

- *Software* yang digunakan adalah Matlab R2013b.
- Format *file* citra *digital* yang dapat digunakan untuk menyimpan pesan adalah berformat *.bmp.
- Format *file* citra *digital* yang dihasilkan dari program steganografi ini adalah berformat *.bmp.

- Pesan yang dapat disimpan hanya berformat *.txt.
- Metode yang digunakan adalah *Least Signifiant Bit*.

1.3 Rumusan Masalah

Rumusan masalah berdasarkan latar belakang di atas adalah:

1. Bagaimana cara menyembunyikan pesan teks ke dalam citra pada steganografi dengan menggunakan metode *Least Significant Bit*?
2. Bagaimana cara mendapatkan pesan teks dari dalam citra pada proses steganografi dengan menggunakan metode *Least Significant Bit*?
3. Bagaimana perubahan dalam *file* citra hasil keluaran sebelum dan sesudah disisipkan pesan teks?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Memberikan informasi bagaimana teknik steganografi dapat diterapkan untuk menyembunyikan pesan teks dalam *file* citra *digital* dengan menggunakan metode *Least Significant Bit*.
2. Memberikan informasi bagaimana teknik steganografi dapat diterapkan untuk mendapatkan pesan teks dalam *file* citra *digital* dengan menggunakan metode *Least Significant Bit*.
3. Mengetahui perubahan yang terjadi dari hasil keluaran *file* citra *digital*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Bagi Penulis, diharapkan dapat menambah pengetahuan dan pemahaman tentang steganografi.

2. Bagi Program Studi Ilmu Komputer, Penulisan penelitian ini memberikan gambaran bagi seluruh mahasiswa khususnya bagi mahasiswa program studi Ilmu Komputer Universitas Negeri Jakarta tentang bagaimana teknik stegaografi dapat menyembunyikan pesan dalam *file* citra *digital*.

3. Bagi Masyarakat, diharapkan dapat menjadi salah satu solusi dalam mengamankan *file* mereka dari orang-orang yang tidak mempunyai hak untuk melihatnya.

1.6 Jenis Penelitian

Jenis Penelitian yang dijalani oleh Peneliti berjenis Kajian Teori. Jenis penelitian ini mengarahkan penulis kepada penulis kepada penerapan metode *Least Significant Bit* dalam pengembangan steganografi dalam penyembunyian pesan.

BAB II

KAJIAN TEORI

2.1 Steganografi

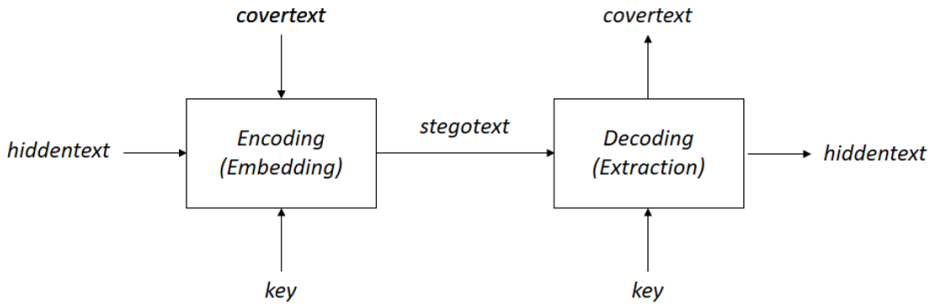
2.1.1 Pengertian Steganografi

Menurut **Ir. Rinaldi Munir, M.T.** dalam Diktat Kuliah Kriptografi dengan judul Steganografi dan *Watermaking*:

"Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia." [10]

Menurut **Gary C. Kessler** dalam jurnalnya *Steganography Hiding Data Within Data*:

"Steganografi adalah ilmu menyembunyikan informasi. Tujuan steganografi adalah untuk menyembunyikan data dari pihak ketiga." [7]



Gambar 2.1: Diagram penyisipan dan ekstraksi pada pesan

Istilah di dalam steganografi:

1. *Covertext* merupakan media atau tempat pesan yang digunakan untuk menyembunyikan *hiddentext*. *Covertext* bisa berupa teks, gambar, audio, video, dll.
2. *Hiddentext* atau biasa disebut *embedded message* merupakan pesan atau informasi yang ingin disembunyikan. Contohnya bisa berupa teks, gambar, audio, video, dll.
3. *Stegotext* merupakan pesan yang sudah berisi *embedded message*.
4. *Encoding* yaitu penyisipan pesan ke dalam media *covertext*.
5. *Decoding* yaitu ekstraksi pesan dari *stegotext*.

Menurut **Munir**, ada kriteria yang harus diperhatikan dalam penyembunyian pesan, yaitu meliputi *Imperceptible*, *Fidelity*, *Recovery* dan *Capacity*.

1. *Imperceptible*

   Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audio. Jika *covertext* berupa *file* citra, maka *stegotext* yang dihasilkan harus sukar dibedakan oleh kasat mata dengan *covertext*-nya. Dan jika *covertext* berupa *file* audio, maka telinga tidak dapat mendeteksi perubahan yang ada pada audio *stegotext*-nya.

2. *Fidelity*

   Kualitas *file* citra penampung tidak jauh berubah. Setelah penambahan pesan rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat pesan rahasia.

3. *Recovery*

   Pesan yang disembunyikan harus dapat diekstrak kembali. Karena tujuan steganografi adalah menyembunyikan pesan atau informasi, maka jika informasi itu dibutuhkan harus dapat diambil kembali untuk dapat digunakan.

4. *Capacity*

   Ukuran pesan yang akan disembunyikan sedapat mungkin besar. Agar dapat memaksimalkan manfaat dari steganografi itu sendiri. [10]

2.1.2 Sejarah Steganografi

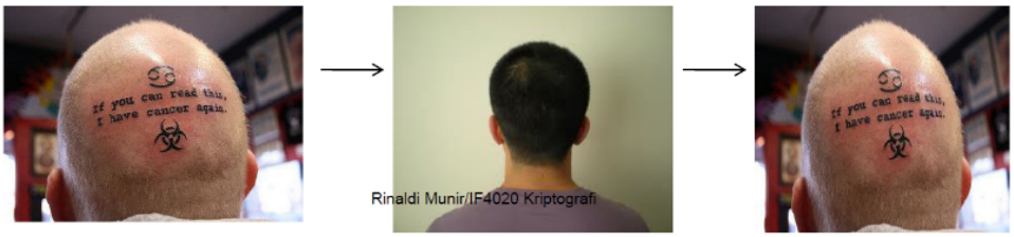
Seperti kriptografi, penggunaan steganografi sebetulnya telah digunakan berabad-abad yang lalu bahkan sebelum istilah steganografi itu sendiri muncul. Periode sejarah steganografi dapat dibagi menjadi:

1. Steganografi Kuno (*Ancient Steganography*)

   (a) Steganografi dengan media kepala budak

   Ditulis oleh **Herodatus** (485âĂŞ525 BC), sejarawan Yunani pada tahun 440 BC di dalam buku: *Histories of Herodatus*). Kisah perang antara kerajaan Persia dan rakyat Yunani. **Herodatus** menceritakan cara **Histaiaeus** mengirim pesan kepada **Aristagoras of Miletus** untuk melawan Persia.

   Caranya adalah dengan dipilih beberapa budak. Kemudian kepala budak tersebut digunduli dan ditulis pesan dengan cara ditato. Setelah pesan dituliskan, budak harus menunggu hingga rambutnya tumbuh kembali. Setelah rambut pada kepala budak tersebut tumbuh, budak dikirim ke tempat penerima. Di sana kepala budak digunduli agar pesan dapat dibaca.



Gambar 2.2: Steganografi dengan media kepala budak

(b) Penggunaan tablet *wax*

Orang-orang Yunani kuno menulis pesan rahasia di atas kayu yang kemudian ditutup dengan lilin (*wax*). Di dalam bukunya, **Heradatus** menceritakan **Demaratus** mengirim peringatan tentang serangan yang akan datang ke Yunani dengan menulis langsung pada tablet kayu yang kemudian dilapisi lilin dari lebah.

Gambar 2.3: Tablet *wax*

(c) Penggunaan tinta tak-tampak (*invisible ink*)

Pliny the Elder menjelaskan penggunaan tinta dari getah tanaman *thithymallus*. Jika dituliskan pada kertas maka tulisan dengan tinta terse-

but tidak kelihatan, tetapi bila kertas dipanaskan berubah menjadi gelap/coklat.

(d) Penggunaan kain sutra dan lilin

Orang Cina kuno menulis catatan pada potongan-potongan kecil sutra yang kemudian digumpalkan menjadi bola kecil dan dilapisi lilin. Selanjutnya bola kecil tersebut ditelan oleh si pembawa pesan. Pesan dibaca setelah bola kecil dikeluarkan dari perut si pembawa pesan.

2. Steganografi Zaman Renaisans (*Renaissance Steganography*)

Tahun 1499, **Johannes Trithemius** menulis buku *Steganographia*, yang menceritakan tentang metode steganografi berbasis karakter. Selanjutnya tahun 1518 dia menulis buku tentang steganografi dan kriptografi berjudul *Polygraphiae*.

Giovanni Battista Porta menggambarkan cara menyembunyikan pesan di dalam telur rebus. Caranya, pesan ditulis pada kulit telur yang dibuat dari tinta khusus yang dibuat dengan satu ons tawas dan setengah liter cuka. Prinsipnya penyembunyiannya adalah tinta tersebut akan menembus kulit telur yang berpori, tanpa meninggalkan jejak yang terlihat. Tulisan dari tinta akan membekas pada permukaan isi telur yang telah mengeras (karena sudah direbus sebelumnya). Pesan dibaca dengan membuang kulit telur.

3. Steganografi Zaman Perang Dunia (*World War Steganography*)

Gambar 2.4: Steganografi zaman perang dunia

Selama terjadinya Perang Dunia ke-2, tinta yang tidak tampak (*invisible ink*) telah digunakan untuk menulis informasi pada lembaran kertas sehingga saat kertas tersebut jatuh di tangan pihak lain hanya akan tampak seperti lembaran kertas kosong biasa. Cairan seperti air kencing (*urine*), susu, vinegar, dan jus buah digunakan sebagai media penulisan sebab bila salah satu elemen tersebut dipanaskan, tulisan akan menggelap dan tampak melalui mata manusia. [10]

4. Steganografi *Digital*

   Sejalan dengan perkembangan maka konsep awal steganografi diimplementasikan pula dalam dunia komputer, yang kemudian dikenal dengan istilah steganografi *digital*. Dalam hal ini, steganografi *digital* memiliki dua properti dasar yaitu media penampung (*cover data* atau *data carrier*) dan data *digital*

yang akan disisipkan (*secret data*), dimana media penampung dan data *digital* yang akan disisipkan dapat berupa *file* multimedia (teks/dokumen, citra, audio maupun video). Terdapat dua tahapan umum dalam steganografi *digital*, yaitu proses *embedding* atau *encoding* (penyisipan) dan proses *extracting* atau *decoding* (pemekaran atau pengungkapan kembali (*reveal*)). Hasil yang didapat setelah proses *embedding* atau *encoding* disebut *stego object* (apabila media penampung hanya berupa data citra maka disebut *stego image*). [12]

2.1.3 Metode Steganografi

Berdasarkan ranah operasinya, metode-metode steganografi dapat dibagi menjadi dua kelompok:

1. *Spatial (time) domain methods*

   Memodifikasi langsung nilai byte dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna *pixel* atau amplitudo). Contoh: Metode modifikasi LSB

2. *Tranform domain methods*

   Memodifikasi hasil transformasi sinyal dalam ranah transform (hasil trnasformasi dari ranah spasial ke ranah lain (misalnya ranah frekuensi). Contoh: Metode *Spread Spectrum* [10]

Ada empat jenis metode steganografi:

1. *Least Significant Bit Insertion* (LSB)

   Metode yang digunakan untuk menyembunyikan pesan pada media *digital* tersebut berbeda-beda. Contohnya, pada berkas *image* pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data *pixel* yang menyusun *file* tersebut. Pada berkas

bitmap 24 bit, setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna *Red*, *Green* dan *Blue* (RGB) yang masing-masing disusun oleh bilangan 8 bit (*byte*) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap *pixel* berkas *bitmap* 24 bit kita dapat menyisipkan 3 bit data.

2. *Algorithms and Transformation*

   Algoritma compression adalah metode steganografi dengan menyembunyikan data dalam fungsi matematika. Dua fungsi tersebut adalah *Discrete Cosine Transformation* (DCT) dan *Wavelet Transformation*. Fungsi DCT dan *Wavelet* yaitu mentransformasi data dari satu tempat (*domain*) ke tempat (*domain*) yang lain. Fungsi DCT yaitu mentransformasi data dari tempat *spatial* (*spatial domain*) ke tempat frekuensi (*frequency domain*).

3. *Redundant Pattern Encoding Redundant Pattern Encoding* adalah menggambar pesan kecil pada kebanyakan gambar. Keuntungan dari metode ini adalah dapat bertahan dari *cropping* (kegagalan). Kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar.

4. *Spread Spectrum Method Spread Spectrum* steganografi terpencar-pencar sebagai pesan yang diacak (*encrypted*) melalui gambar (tidak seperti dalam LSB). Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image* (gambar)

2.2 Perbedaan Steganografi dan Kriptografi

2.3 LSB (*Least Significant Bit*)

2.4 ASCII

2.5 *Citra Digital*

2.5.1 Pengertian Citra *Digital*

2.5.2 Pengolahan Citra *Image Processing*

2.5.3 Perbandingan *File* Gambar BMP (*Bitmap*) dengan JPG, GIF, atau PNG

2.6 MATLAB

DAFTAR PUSTAKA

[1] Adiria. (2010). "ANALISIS DAN PERANCANGAN APLIKASI STEGANOGRAFI PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT)". Skripsi Sarjana pada Universitas Islam Negeri Jakarta

[2] Arymurthy, A. M., dan Setiawan, S. (1992). "Pengantar Pengolahan Citra. Jakarta: PT Elex Media Komputindo".

[3] Bunyamin, H., dan Adrian. (2009). "Aplikasi Steganography pada File dengan Menggunakan Teknik Low Bit Encoding dan Least Significant Bit". Jurnal Informatika UKM, Vol. 5, No. 2, pp. 107âĂŞ117.

[4] Hermawati, F. A. (2013). "Pengolahan Citra Digital". Yogyakarta: ANDI.

[5] Irfan. (2013). "Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB (Least Significant Bit)". Rekayasa Teknologi Vol. 5, No. 1.

[6] Joshi, K., dan Yadav, R. (2015). "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication". Third International Conference on Image Infomation Processing.

[7] Kessler, G. C. (2001). "Steganography Hiding Data Within Data".

[8] M. K., Kadam, K., Koshti, A., dan Dunghav, P. (2012). "Steganography Using Least Signicant Bit Algorithm". International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp. 338-341.

[9] Munir, R. (2004). "Pengolahan Citra Digital". Bandung: Informatika.

[10] Munir, R. (2006). "Kriptografi". Bandung: Informatika.

[11] Prasetyo, F. P. (2010). "STEGANOGRAFI MENGGUNAKAN METODE LSB DENGAN SOFTWARE MATLAB". Skripsi Sarjana pada Universitas Islam Negeri Jakarta

[12] Prayudi, Y., dan Kuncoro, P. S. (2005). "IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN TEKNIK ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT (AMELSBR)". Seminar Nasional Aplikasi Teknologi Informasi.

[13] Rakhmat, B., dan Fairuzabadi, M. (2010). "STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN KOMBINASI ALGORITMA KRIPTOGRAFI VIGENÃĹRE DAN RC4". Jurnal Dinamika Informatika, Volume 5, Nomor 2.

[14] Setiana, dan Mahmudy, W. F. (2006). "Steganografi Pada File Citra Bitmap 24 Bit Untuk Pengamanan Data Menggunakan Metode Least Significant Bit (LSB) Insertion". Kursor, vol. 2, no. 2, pp. 38-44.

[15] Wikipedia. (n.d.). Retrieved from https://id.wikipedia.org/wiki/Steganografi