Penyembunyian Informasi (steganography) Gambar Menggunakan Metode LSB (*Least Significant Bit*)

Irfan[1)]
[1)] Program Studi Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Prof. Dr. HAMKA, Jakarta.
Jalan Limau II, Kebayoran Baru, Jakarta 12130. Indonesia.
Telp: +62-21-7256659, Fax: +62-21-7256659, Mobile: +622194469819
Email : irfan03092008@gmail.com

Abstrak

Dengan semakin populernya media digital, perhatian pada tingkat keamanan akan menjadi semakin penting. Salah satu isu penting adalah tingkat keamanan pengiriman informasi. Hal ini dapat dilakukan dengan menggunakan enkripsi atau steganografi. Steganografi merupakan suatu metode untuk menyisipkan potongan sebuah informasi rahasia dalam suatu objek media lain. Dalam steganografi dikenal data hiding atau data embedding yaitu penyembunyian data yang nampak sangat familiar dengan enkripsi. Namun, data hiding dalam steganografi dan enkripsi sangat berbeda, dimana enkripsi melakukan data hiding dengan mengubah susunan karakter dalam suatu media yang sama. Sedangkan dalam steganografi, data hiding dilakukan dengan cara mengubah atau menukar beberapa informasi yang tidak terlihat penting dalam media host pembawa pesan. Dalam jurnal ini, judul yang diajukan adalah penggunaan media gambar sebagai data masukan media pembawa pesan rahasia berupa gambar dengan format BMP, metode yang digunakan adalah LSB (least significant bit).

Kata kunci: *steganografi, BMP, LSB*

Abstract

With the growing popularity of digital media, attention to the level of security will become increasingly important. One important issue is the security level of information delivery. This can be done using encryption or steganography. Steganography is a method to insert a piece of confidential information in an object other media. In steganography, the hiding of data or data known embedding the hiding of data that look very familiar with encryption. But data hiding in steganography and encryption are very different, where the encryption to the data hiding by changing the arrangement of characters in the same medium. While in steganography, data hiding is done by changing or exchange some important information that is not visible in the host media messengers. In this paper, the title proposed is the use of media images as input data carrier with a secret message is an image format of BMP, the method used is the LSB (least significant bit).

Key words: *steganography, BMP, LSB*

1 PENDAHULUAN

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "*steganografi*" berasal dari bahasa Yunani ***steganos***, yang artinya "tersembunyi atau terselubung", dan ***graphein***, "menulis".

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang

benar ke dalam algoritma yang digunakan.

Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.

1.1 Rumusan masalah

Dalam pelaksanaan tugas penelitian ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut :

1. Bagaimana menyisipkan suatu pesan rahasia berupa gambar ke dalam sebuah file gambar agar tidak mudah diketahui oleh yang tidak berhak, tapi mudah di buka oleh yang berhak?
2. Apakah terjadi perubahan dalam file gambar hasil keluaran baik itu kualitas file maupun besar data file dan seberapa besar perubahan itu terjadi dalam penyisipan pesan rahasia tersebut?

1.2 Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, maka penulis memberikan batasan-batasan masalah sebagai berikut:

1. Informasi yang disembunyikan adalah berupa file gambar yang memiliki format BMP.
2. Metode yang penulis ambil adalah LSB (*least significant bit*)
3. Objek penelitian difokuskan pada kualitas file dan besar file keluaran.

2 LANDASAN TEORI

2.1 Pengertian Steganografi

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas [Waheed, 2000].

Steganografi biasanya sering disalah-kaprahkan dengan kriptografi karenanya keduanya sama-sama bertujuan untuk melindungi informasi yang berharga. Perbedaan yang mendasar antara keduanya yaitu steganografi berhubungan dengan informasi tersembunyi sehingga tampak seperti tidak ada informasi tersembunyi sama sekali. Jika seseorang mengamati objek yang menyimpan informasi tersembunyi tersebut, ia tidak akan menyangka bahwa terdapat pesan rahasia dalam objek tersebut, dan karenanya ia tidak akan berusaha memecahkan informasi (dekripsi) dari objek tersebut.

Kata *steganografi* berasal dari bahasa Yunani, yaitu dari kata *Steganï£¡* (tersembunyi) dan Graptos (tulisan). Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio, atau video. Teknik *Steganografi* ini telah banyak digunakan dalam stratgei peperangan dan pengiriman sandi rahasia sejak jaman dahulu kala. Dalam perang Dunia II, teknik steganografi umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman [Simmons., 1983]. Semakin pentingnya nilai dari sebuah informasi, maka semakin berkembang pula metode-metode yang dapat digunakan untuk melakukan penyisipan informasi yang didukung pula dengan semakin berkembangnya media elektronik. Berbagai macam media elektronik kini telah dapat digunakan untuk melakukan berbagai fungsi steganografi dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. Sebagai fungsi yang umum, steganografi digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi [Johnson, 2006].

Satu hal esensial yang menjadi kelebihan steganografi adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi di dalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya. Namun begitu terbentuk pula suatu teknik yang dikenal dengan *steganalysis*, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan steganografi pada suatu arsip. Seorang *steganalyst* tidak berusaha untuk melakukan dekripsi terhadap

informasi yang tersembunyi dalam suatu arsip, yang dilakukan adalah berusaha untuk menemukannya. Terdapat beberapa cara yang dapat digunakan untuk mendeteksi steganografi seperti melakukan pengamatan terhadap suatu arsip dan membandingkannya dengan salinan arsip yang dianggap belum direkayasa, atau berusaha mendengarkan dan membandingkan perbedaannya dengan arsip lain bila arsip tersebut adalah dalam bentuk audio.

2.2 Sejarah Steganografi

Seperti kriptografi, penggunaan *steganografi* sebetulnya telah digunakan berabad-abad yang lalu bahkan sebelum istilah steganografi itu sendiri muncul. Berikut adalah contoh penggunaan *steganografi* di masa lalu:

- 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.
- Pada sejarah Yunani kuno, masyarakatnya biasa menggunakan seorang pembawa pesan sebagai perantara pengiriman pesan. Pengirim pesan tersebut akan dicukur rambutnya, untuk kemudian dituliskan suatu pesan pada kepalanya yang sudah botak. Setelah pesan dituliskan, pembawa pesan harus menunggu hingga rambutnya tumbuh kembali sebelum dapat mengirimkan pesan kepada pihak penerima. Pihak penerima kemudian akan mencukur rambut pembawa pesan tersebut untuk melihat pesan yang tersembunyi.
- Metode lain yang digunakan oleh masyarakat Yunani kuno adalah dengan menggunakan lilin sebagai media penyembunyi pesan mereka. Pesan dituliskan pada suatu lembaran, dan lembaran tersebut akan ditutup dengan lilin untuk menyembunyikan pesan yang telah tertulis. Pihak penerima kemudian akan menghilangkan lilin dari lembaran tersebut untuk melihat pesan yang disampaikan oleh pihak pengirim.

2.3 Metode Steganografi pada Gambar menggunakan *Least significant bit*

Sudah banyak metode yang digunakan untuk menyembunyikan pesan di dalam sebuah *image* tanpa mengubah tampilan *image*, sehingga pesan yang disembunyikan tidak akan terlihat. Berikut akan dibahas beberapa metode umum yang digunakan pada *image* steganografi. Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan Least-Significant Bit (LSB). Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang. Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada stego, harus digunakan format *lossless compression*, karena metode ini menggunakan bit-bit pada setiap piksel pada *image*. Jika digunakan format *lossy compression*, pesan rahasia yang disembunyikan dapat hilang. Jika digunakan *image* 24 *bit color* sebagai *cover*, sebuah bit dari masing-masing komponen Red, Green, dan Blue, dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah *image* 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia. Misalnya, di bawah ini terdapat 3 piksel dari *image* 24 *bit color* :

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

jika diinginkan untuk menyembunyikan karakter A (10000001b) dihasilkan :

(00100111 11101000 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

Dapat dilihat bahwa hanya 3 bit saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif. Jika digunakan *image* 8 *bit color* sebagai *cover*, hanya 1 bit saja dari setiap piksel warna yang dapat dimodifikasi sehingga pemilihan *image* harus dilakukan dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada citra. Akan lebih baik jika *image* berupa *image grayscale* karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia. Proses

ekstraksi pesan dapat dengan mudah dilakukan dengan mengekstrak LSB dari masing-masing piksel pada stego secara berurutan dan menuliskan nya ke *output* file yang akan berisi pesan tersebut. Kekurangan dari metode modifikasi LSB ini adalah bahwa metode ini membutuhkan ”tempat penyimpanan” yang relatif besar. Kekurangan lain adalah bahwa stego yang dihasilkan tidak dapat dikompress dengan format *lossy compression.*

2.4 Sejarah Matlab

MATLAB adalah sebuah program untuk menganalisis dan mengkomputasi numerik dan merupakan suatu bahasa pemrograman matematika lanjutan yang dibentuk dengan dasar pemikiran menggunakan sifat dan bentuk matriks. Awalnya, program ini merupakan *interface* untuk koleksi rutin-rutin numerik dari proyek LINPACK dan EISPACK dikembangkan menggunakan bahasa FORTRAN namun sekarang merupakan produk komersial dari perusahaan Mathworks, Inc. yang dalam perkembangan selanjutnya dikembangkan menggunakan bahasa C++ dan assembler (utamanya untuk fungsi-fungsi dasar MATLAB).

MATLAB telah berkembang menjadi sebuah *environment* pemrograman yang canggih yang berisi fungsi-fungsi *built-in* untuk melakukan tugas pengolahan sinyal, aljabar linier, dan kalkulasi matematis lainnya. MATLAB juga berisi *toolbox* yang berisi fungsi- fungsi tambahan untuk aplikasi khusus. MATLAB bersifat *extensible*, dalam arti bahwa seorang pengguna dapat menulis fungsi baru untuk ditambahkan pada *library* ketika fungsi-fungsi *built-in* yang tersedia tidak dapat melakukan tugas tertentu. Kemampuan pemrograman yang dibutuhkan tidak terlalu sulit bila Anda telah memiliki pengalaman dalam pemrograman bahasa lain seperti C, PASCAL, atau FORTRAN. MATLAB merupakan *merk software* yang dikembangkan oleh Mathworks.Inc. merupakan *software* yang paling efisien untuk perhitungan *numeric* berbasis matriks. Dengan demikian jika di dalam perhitungan kita dapat menformulasikan masalah ke dalam format matriks maka MATLAB merupakan *software* terbaik untuk penyelesaian *numeric*-nya. MATLAB (MATrix LABoratory) yang merupakan bahasa pemrograman tingkat tinggi berbasis pada matriks sering digunakan untuk teknik komputasi numerik,yang digunakan untuk menyelesaikan masalah-masalah yang melibatkan operasi matematika elemen, matrik, optimasi, aproksimasi dan lain-lain. Sehingga Matlab banyak digunakan pada:

- Matematika dan Komputansi
- Pengembangan dan Algoritma
- Pemrograman modeling, simulasi, dan pembuatan prototipe
- Analisis Data, eksplorasi dan visualisasi
- Analisis numerik dan statistik
- Pengembangan aplikasi teknik

3 PEMBAHASAN

3.1 Metode Perancangan

Pada bab ini dibahas tentang metode perancangan secara lengkap dengan prinsip kerjanya dan *flowchart* aplikasi **Prinsip Kerja (Algoritma) LSB.** Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen suatu data dengan bit-bit data rahasia. Salah satu metode penyembunyian data yang sederhana adalah LSB. Perhatikan contoh sebuah susunan bit pada sebuah byte:

11010010

MSB LSB

LSB = *Least significant bit*

MSB = Most Siginificant Bit

Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna keabuan tertentu, maka perubahan satu bit LSB tidak mengubah warna keabuan tersebut secara berarti. Lagipula, mata manusia tidak dapat membedakan perubahan yang kecil.

Misalkan segmen data sebelum perubahan:

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 0 1 1 0 1 1 1 1

Segmen data setelah ’0 1 1 1 ’ disembunyikan:

0 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 1 1 0 0 0 1 1 0 1 1 0 1 1 1 1

Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti byte-byte yang berurutan, namun dipilih susunan byte secara acak. Misalnya jika terdapat 50 byte dan 6 bit data yang akan disembunyikan, maka maka byte yang diganti bit LSB-nya dipilih secara acak, misalkan byte nomor 36, 5, 21, 10, 18, 49.

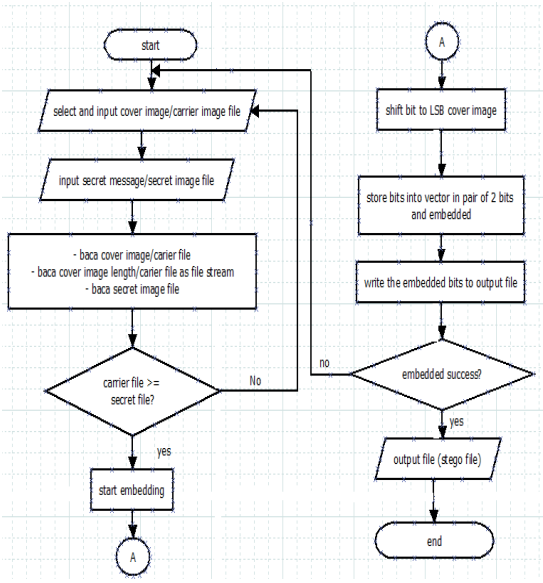
Bilangan acak dibangkitkan dengan *pseudo-random-number-generator* (PRNG) kriptografi. PRNG kriptografi sebenarnya adalah algoritma kriptografi yang digunakan untuk enkripsi. PRNG dibangun dengan algoritma DES (Data Encryption Standard), algoritma hash MD5, dan mode kriptografi CFB (Chiper-Feedback Mode). Tujuan dari enkripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi.

Pengkode LSB watermark biasanya memilih sebuah subset dari seluruh host suara yang mungkin dengan menggunakan sebuah kunci rahasia. Operasi substitusi pada LSB dilakukan di subset tersebut.

Proses ekstraksi dilakukan dengan membaca bit-bit yang diterima dari aliran bit suara yang diterima. Alat penerjemah memerlukan semua bagian dari data suara yang digunakan selama proses penempelan pesan rahasia. Metode pengkodean LSB standar dengan mudah mengganti bit pada suara asli pada lapisan ke-i dengan bit dari aliran bit data rahasia. Algoritma LSB yang digunakan harus melakukan penempelan bit yang menimbulkan distorsi yang minimal pada suara yang ditempeli.

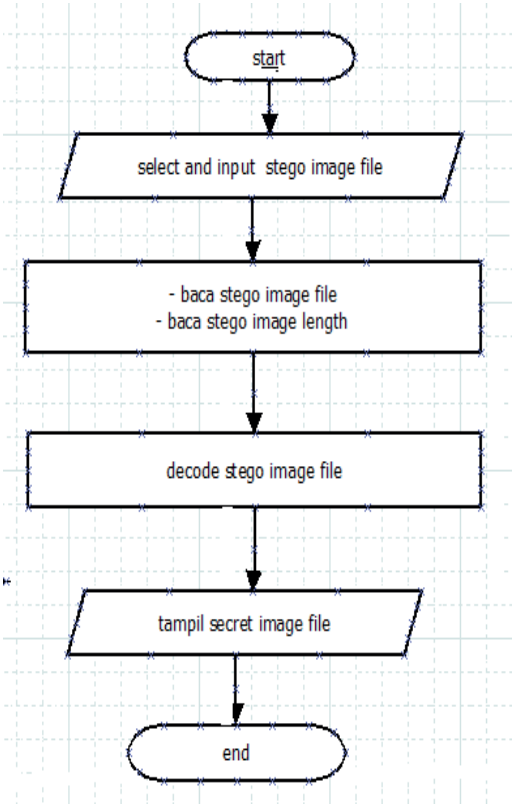
3.2 Flowchart aplikasi

A. Menyembunyikan informasi gambar berupa bitmap



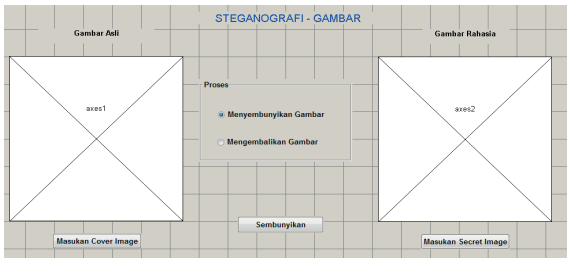
Gambar 1 *Flowchart menyembunyikan citra*

B. Me-*recover* (mengembalikan) gambar yang tersembunyi



Gambar 2 *Flowchart merecover citra*

3.3 Desain Aplikasi



Gambar 2 *Desain aplikasi steganografi gambar*

3.4 Pengujian

Pada fase pengujian ini terdapat 2 menu yaitu, menyembunyikan gambar dan mengembalikan gambar, untuk menyembunyikan gambar, maka langkahnya adalah sebagai berikut:

a. Memasukan *Cover image*

Untuk memasukan *Cover image*, diklik buton "masukan *Cover image*" seperti gambar dibawah ini.

Gambar 4 *Memasukan cover image*

b. Memasukan *Secret image*

Setelah dimasukan *Cover image*, maka masukan gambar yang akan disembunyikan dengan mengklik *button* "masukan *Secret image*" seperti gambar berikut:

Gambar 5 *Memasukan secret image*

Setelah itu klik buton "sembunyikan" maka sistem akan meminta agar menyimpan file hasil stego nya.

c. Mengembalikan gambar

Untuk mengemballikan gambar, maka kita pilih menu radio buton "mengembalikan gambar", selanjutnya kita masukan *Cover image* nya dari hasil gambar stegonya, lalu kita pilih recover, maka sistem akan menampilkan gambar yang disembunyikan tadi. Dapat dilihat seperti gambar berikut.

Gambar 6 *Merecover gambar*

4 SIMPULAN DAN SARAN

4.1 Simpulan

Dari hasil pengujian sistem yang dilakukan pada bab sebelumnya, maka dapat disimpulkan beberapa hal antara lain:

1. Metode LSB adalah metode yang baik untuk menyembunyikan informasi berupa file gambar yang berekstensi bitmap, karena antara gambar *Cover image* sebelum dan sesudah di lakukan proses steganografi tidak terlihat perubahan yang terjadi secara kasat mata.
2. Hasil dari *Cover image* file akan menjadi lebih besar setelah dilakukan proses steganografi menggunakan metode LSB
3. Gambar yang akan disembunyikan harus lebih kecil dari *Cover image* nya.

4.2 Saran

1. Diharapkan dapat mengembangkan berbagai jenis file yang tidak hanya bitmap tapi juga berbagai jenis format file gambar lain seperti jpg, png, tiff, dan lain-lain.
2. Diharapkan dapat mengembangkan pula pada berbagai jenis file lain seperti text dan video

DAFTAR KEPUSTAKAAN

[1] [Bender, 1998] Bender,W. Gruhl, D. M. N. L. (August 1998). *A.: Techniques for Data Hiding*. PhD thesis.

[2] [Bender, 1996] Bender, D. Gruhl, N. A. L. (Februari 1996). Techniques for data hiding. IBM System, 35(3-4).

[3] [Johnson, 2006] Johnson, N. F. (2006). http://www.jjtc.com/ihws98/jjgmu.html.

[4] [Simmons., 1983] Simmons., G. (1983). The prisoner's problem and the subliminal channel. In Crypto'83:halaman 51–67.

[5] [Waheed, 2000] Waheed, Q. (2000). *Steganografi and Steganalysis*. PhD thesis.

[6] [Westfeld, 1999] Westfeld, A. (1999). The steganographicalgorithmf5.http://wwwrn.inf.tudresden.de/Ÿwestfeld/f5.html.