BAB I
PENDAHULUAN

1.1 Latar Belakang

Di seluruh dunia, internet sudah berkembang menjadi salah satu media komunikasi data yang sangat populer. Kemudahan dalam penggunaan dan fasilitas yang lengkap merupakan keunggulan yang dimiliki oleh internet dan bukan rahasia umum di kalangan masyarakat pengguna internet pada saat sekarang ini. Namun, seiring dengan berkembangnya media internet dan aplikasi yang menggunakan internet semakin bertambah pula kejahatan dalam sistem informasi. Dengan berbagai teknik pengambilan informasi secara ilegal yang berkembang, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Untuk itu, sejalan dengan berkembangnya media internet yang sangat cepat, harus juga diikuti dengan perkembangan pengamanan dalam sistem informasi yang berada dalam media internet tersebut.

Berbagai macam teknik yang digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak telah banyak dilakukan dalam upaya mengamankan suatu data penting dengan menggunakan sistem kriptografi yang melakukan enkripsi sebelum data penting tersebut ditransmisikan. Tindakan pengamanan menggunakan cara tersebut ternyata dianggap belum cukup dalam mengamankan suatu data karena adanya peningkatan kemampuan komputasi. Berbeda dengan teknik kriptografi, steganografi menyembunyikan pesan rahasia agar bagi orang awam tidak menyadari keberadaan dari pesan yang disembunyikan. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut. Caranya dengan menyembunyikan informasi rahasia di dalam suatu wadah penampung informasi dengan sedemikian rupa sehingga keberadaan informasi rahasia yang ditempelkan tidak terlihat. Wadah penampung informasi tersebut dapat berbentuk berbagai jenis *file* multimedia digital seperti teks, citra, audio, video. Dalam tugas akhir ini, peneliti membuat analisis dan merancang aplikasi steganografi dan merupakan solusi dari permasalahan tersebut. Dengan penggunaan teknik ini, data informasi dapat kita sembunyikan di dalam media digital yang kita punya.

1.2 Rumusan Masalah

Dari uraian latar belakang di atas, maka dapat dirumuskan masalah pada tugas akhir berikut:

1. Bagaimana metode LSB dapat digunakan sebagai salah satu metode steganografi dalam penyembunyian *file* ke dalam citra digital gambar GIF?
2. Bagaimana metode *Spread Spectrum* dapat digunakan sebagai salah satu metode steganografi dalam penyembunyian *file* ke dalam citra digital gambar GIF?
3. Bagaimana hasil pengecekan MSE dan PSNR terhadap hasil steganografi menggunakan metode LSB?
4. Bagaimana hasil pengecekan MSE dan PSNR terhadap hasil steganografi menggunakan metode *Spread Spectrum*?

1.3 Tujuan

Tujuan dari proposal tugas akhir ini adalah :

1. Mengetahui cara penggunaan metode LSB dalam steganografi pada citra digital GIF.
2. Mengetahui cara penggunaan metode *Spread Spectrum* dalam steganografi pada citra digital GIF.
3. Mengetahui hasil pengecekan MSE dan PSNR steganografi dengan metode LSB.
4. Mengetahui hasil pengecekan MSE dan PSNR steganografi dengan metode *Spread Spectrum*.

1.4 Batasan Masalah

Batasan masalah dari proposal tugas akhir ini adalah:

1. Format citra yang digunakan berupa citra digital GIF tidak bergerak. Karena citra GIF animasi menggunakan proses steganografi dengan menghitung gambar per frame dari GIF animasi yang mana sama seperti pada file video.
2. *File* yang disisipkan berupa *file* denga format ".txt"
3. Metode yang digunakan berupa metode LSB dan *Spread Spectrum.*
4. Pengujian yang dilakukan berupa hasil stego dan juga pengecekan MSE dan PSNR.

1.5 Metedologi Penelitian

Langkah yang ditempuh untuk menyelesaikan tugas akhir ini antara lain sebagai berikut.

1. Studi literatur dengan mengumpulkan, mencari, dan memahami baik jurnal, artikel, buku referensi, dan sumber lain yang berhubungan dengan masalah yang diangkat pada tugas akhir ini.
2. Merancang implementasi
3. Melakukan uji coba dengan beberapa parameter pengujian pada citra digital.
4. Menganalisa hasil uji coba dari segi ketahanan terhadap dearu atau gangguan.

1.6 Sistematika Penulisan

Penulisan tugas akhir ini dibagi dalam beberapa bagian, diantaranya sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, perumusan masalah, tujuan, dan batasan masalah yang ada pada tugas akhir ini. Serta metodologi penilitian yang dilakukan dan sistematika penulisan Tugas Akhir.

BAB II DASAR TEORI

Bab ini berisi tentang beberapa teori yang didapatkan dari beberapa referensi baik buku jurnal maupun dari internet.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas tentang semua yang berhubungan dengan perancangan sistem dan analisis.

BAB IV PENGUJIAN

Bab ini membahas tentang skenario pengujian yang ada dalam aplikasi yang telah dibuat.

BAB V PENUTUP

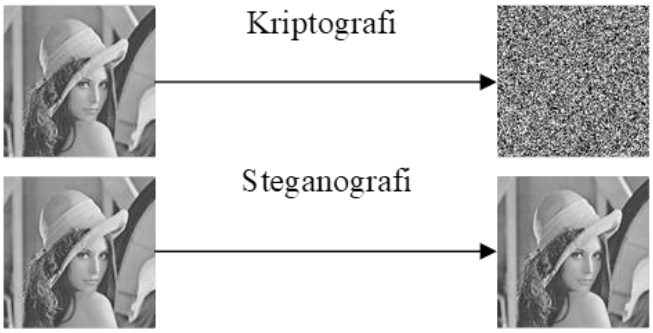
Bab ini berisi tentang kesimpulan, kritik dan saran dari hasil analisa dan pengujian yang diperoleh.

BAB II
DASAR TEORI

2.1. Steganografi

Steganografi berasal dari Bahasa Yunani, yaitu steganos yang artinya "tulisan tersembunyi (*covered writing*)" dan graphos yang berarti tulisan. Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui [2].

Steganografi membutuhkan dua properti yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode barang, atau pesan lain [2]. Steganografi berbeda dengan kriptografi, perbedaannya terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. Kriptografi melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya, sedangkan steganografi menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut, sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir sama [2]. Perbedaan kriptografi dan steganografi dapat diilustrasikan pada Gambar 2.1.



Gambar 2.1 Perbedaan Pesan yang Disembunyikan Sumber [2]

Tujuan steganografi adalah untuk menghindari kecurigaan sedangkan kriptografi menyembunyikan isi (content) pesan agar pesan tidak dapat dibaca.

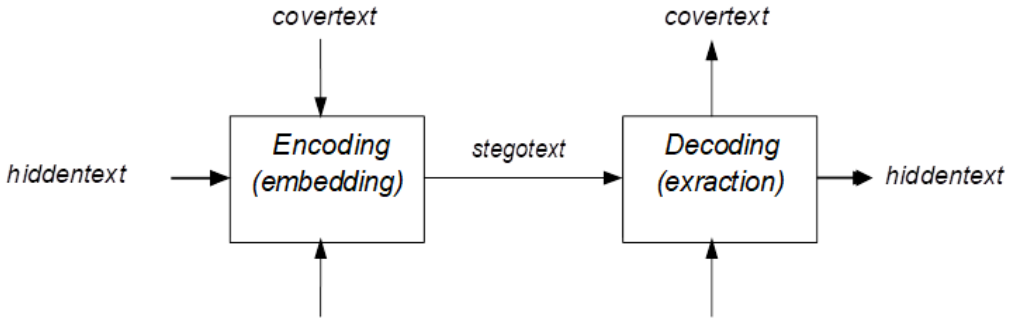
Steganografi memanfaatkan kelemahan indera manusia seperti indera pendengaran dan indera penglihatan. Dengan adanya kelemahan ini steganografi dapat diterapkan di berbagai media digital. Hasil keluaran *file* yang telah disisipi

pesan mempunyai persepsi bentuk yang sama dengan *file* aslinya. Penggunaan komputer diperlukan untuk mengetahui keberadaan pesan yang tersembunyi dalam *file* digital.

Terdapat beberapa istilah yang berkaitan dengan steganografi:

a. *Hiddentext* atau *embedded message*: pesan yang disembunyikan.
b. *Covertext* atau *cover-object*: pesan yang digunakan untuk menyembunyikan embedded message.
c. *Stegotext* atau *stego-object*: pesan yang sudah berisi *embedded message*.

Di dalam steganografi digital, baik *hiddentext* maupun *covertext* dapat berupa teks, citra, audio, maupun video. Jadi, kita dapat menyembunyikan pesan berupa kode program di dalam sebuah citra, atau video, dan kita juga dapat menyembunyikan gambar rahasia di dalam citra lain atau di dalam sebuah berkas musik mp3. Penyisipan pesan ke dalam media *covertext* dinamakan encoding, sedangkan ekstraksi pesan dari stegotext dinamakan decoding. Kedua proses ini mungkin memerlukan kunci rahasia (yang dinamakan stegokey) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan pesan dan ekstraksi pesan [2].



Gambar 2.2 Diagram Penyisipan dan Ekstraksi Pesan [2]

Penyembunyian pesan rahasia ke dalam media penampung pasti mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian pesan adalah:

a. *Imperceptibility* : Keberadaan pesan rahasia tidak dapat dipersepsikan oleh indrawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya.
b. *Fidelity* : Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsi oleh indrawi. Misalnya, jika *covertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan

oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio (misalnya berkas mp3, wav, midi, dan sebagainya), maka audio *stegotext* tidak rusak dan indra telinga tidak dapat mendeteksi perubahan tersebut.

c. *Recovery* : Pesan yang disembunyikan harus dapat rekonstruksi kembali (reveal). Karena tujuan stganografi adalah data hiding, maka sewaktu-waktu pesan rahasia di dalam steganotext harus dapat diambil kembali untuk digunakan lebih lanjut [6].

2.2. GIF

Graphics Interchange Format (GIF) adalah sebuah format berkas citra yang diperkenalkan pada tahun 1987 oleh *CompuServe* untuk menggantikan format RLE yang hanya mampu menampilkan gambar dengan warna hitam dan putih saja [4].

GIF adalah salah satu format berkas citra yang paling sering ditemui di dunia digital. Hal ini terjadi karena format ini berukuran relatif kecil. Sebagai contoh untuk citra yang sama, berkas dengan format GIF dapat berukuran lebih kecil jika dibandingkan dengan format JPG [8].

Hal ini disebabkan karena *file* GIF hanya menggunakan 256 palet warna. Sehingga tentunya ukuran *file* akan lebih kecil. Namun 256 palet warna tersebut tidak mutlak hanya 256 warna tertentu. Namun warna tersebut dapat dipilih dari 24-bit palet warna RGB. Sehingga dengan singkat kata dapat disimpulkan bahwa berkas dengan format GIF akan membuang palet warna yang tidak diperlukan dan mengambil hanya 256 palet warna yang diperlukan [4],[10].

Ukuran palet sebesar 256 warna adalah standar GIF'89 dan 87. Beberapa versi dari gif sekarang telah dapat menampilkan warna dengan lebih dari 256 warna. GIF dengan format GIF'89 dan GIF'87 dapat dibedakan melalui header *file* [10].

2.3. Metode *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 3bit 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* 8bit *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 masingmasing 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 dikompres dengan format *lossy compression* [7],[2].

2.4. Metode *Spread Spectrum*

Dalam metode *spread spectrum*, penyisipan pesan atau informasi terdapat kunci atau key yang digunakan untuk mengenkripsi pesan. Key tersebut kita dapatkan melalui pembangkit bilangan semu acak dengan algoritma LCG. Sebelum pesan disisipkan kedalam *cover image*, maka terlebih dahulu menentukan wilayah penyisipannya. Setelah menentukan wilayah penyisipan, selanjutnya adalah proses spreading. Spreading dilakukan sesuai dengan bilangan pengali skalar yang ditentukan. Pada proses ini citra rahasia diambil nilai intensitas perpixel nya, lalu diubah kedalam bilangan biner. Kemudian bilangan biner tersebut disebar sesuai bilangan pengali skalar yang telah ditentukan, maka hasil keluaran dari proses spreading ini adalah deret bilangan biner yang telah tersebar dengan panjang setiap deretnya sebesar 32 bit.

Setelah proses spreading yang selanjutnya adalah proses modulasi pesan. Proses ini merupakan proses pengacakan pesan yang telah disebar dengan bilangan pseudonoise yang telah dibangkitkan menggunakan algoritma LCG. Panjang dari bilangan pseudonoise ini disesuaikan dengan panjang dari pesan. Jika panjang pesan lebih kecil dari panjang bilangan pseudonoise, bilangan pseudonoise tersebut akan dipotong sesuai dengan ukuran pesan. Sebaliknya, jika panjang pesan lebih besar dari panjang bilangan pseudonoise, maka bilangan tersebut akan diulang sampai panjangnya sama dengan panjang pesan. Proses modulasi tersebut dilakukan dengan menggunakan fungsi XOR (Exclusive OR). Nilai yang dihasilkan dari proses modulasi inilah yang kemudian akan disisipkan ke dalam berkas *cover image*. Setelah pesan disisipkan maka *output* nya merupakan *stego object* yang sudah tersisipi sebuah pesan.

Proses yang berikutnya di dalam metode *spread spectrum* setelah dilakukan penyisipan pesan adalah proses ekstraksi. Di dalam proses ekstraksi terlebih dahulu dilakukan pembacaan data yang disisipkan di dalam *stego object* dalam hal ini adalah *image*. Pembacaan data yang dilakukan berdasarkan informasi wilayah penyisipan pesan. Pembacaan akan dilakukan secara berselang-seling pada matriks frekuensi yang terdapat pada citra dan berlangsung sampai data yang dibaca besarnya sama dengan informasi ukuran berkas yang disisipkan.

Setelah data tersembunyi berhasil dikumpulkan, dilakukan proses demodulasi terhadap data tersebut. Proses demodulasi ini melibatkan bilangan acak yang dibangkitkan dari kunci masukan menggunakan algoritma LCG. Adapun proses pembangkitan bilangan acak yang dilakukan pada tahap ekstraksi pesan sama seperti proses pembangkitan bilangan acak pada tahap penyisipan pesan. Hasil dari proses demodulasi tersebut akan mengalami proses de-spreading. Proses *de-spreading* ini bekerja menggunakan faktor besaran pengali yang dimasukkan oleh pengguna pada proses penyisipan pesan. Proses *de-spreading* ini adalah proses yang dilakukan untuk mendapatkan *bit-bit* dari pesan tersembunyi, maka hasil keluaran dari proses *de-spreading* ini adalah deret bilangan biner yang telah disusutkan dengan panjang setiap deretnya sebesar 8 bit Lalu *bit-bit* tersebut dikonversi kedalam bilangan desimal, yang selanjutnya akan disusun sebagai nilai intensitas tiap piksel pada citra rahasia.

2.5. MSE dan PSNR

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan *decibel* (db). PSNR digunakan untuk mengetahui perbandingan kualitas citra *cover* sebelum dan sesudah disisipkan pesan. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE (*Mean Square Error*). MSE adalah nilai *error* kuadrat rata-rata antara antara citra asli (*cover-image*) dengan citra hasil penyisipan (*stego-image*) [9],[11].

Dalam suatu pengembangan dan pelaksanaan rekonstruksi gambar diperlukan perbandingan antara gambar hasil rekonstruksi dengan gambar asli. Ukuran umum yang digunakan untuk tujuan ini adalah PSNR. Nilai PSNR yang lebih tinggi menyiratkan kemiripan yang tinggi antara hasil rekonstruksi dan gambar asli. PSNR didefinisikan sebagai :

$$PSNR = 10.log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (1)$$

Dimana,

PSNR : *Peak Signal to Noise Ratio*

MSE : *Mean Square Error*

MAX : nilai piksel terbesar pada keseluruhan citra.

Dimana MSE didefinisikan sebagai :

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\|I(i,j) - K(i,j)\|^2 \quad (2)$$

Dimana,

m : jumlah baris dari citra

n : jumlah kolom dari citra

I (i,j) : nilai piksel dari *cover image*

K (i,j) : nilai piksel pada *stego image*

i : menyatakan baris ke-i

j : menyatakan kolom ke-j

Pada tahap pengujian MSE harus menghasilkan nilai MSE yang mendekati nol, karena nilai MSE akan sangat berpengaruh terhadap nilai PSNR dimana nilai MSE dan PSNR mempunyai hubungan berbanding terbalik antara satu dengan yang lainnya. Semakin kecil nilai MSE maka akan semakin besar nilai PSNR, sebaliknya semakin besar nilai MSE maka akan semakin kecil nilai PSNR nya. Maka diharapkan hasil dari nilai MSE itu sekecil mungkin agar didapatkan nilai PSNR diatas 30 dB yang mana menjadi nilai standar minimum dari nilai PSNR itu sendiri [9],[11].