BAB II
TINJAUAN PUSTAKA

A. STEGANOGRAFI

1. Pengertian *Steganografi*

Steganografi adalah seni menyembunyikan pesan di dalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan di dalam media tersebut. Kata steganografi (*steganography*) berasal dari bahasa Yunani *steganos* yang artinya "tersembunyi/terselebung" dan *graphein* "menulis" sehingga kurang lebih artinya "menulis (tulisan) terselubung". Steganografi membutuhkan wadah penampung (*cover*) dan data yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks maupun video. Data yang disembunyikan juga dapat berupa citra, suara, teks, atau video (Sutoyo, et al. 2009). Steganografi merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain. Dengan demikian keberadaan informasi tersebut tidak diketahui oleh orang lain. Tujuan dari steganografi adalah menyembunyikan keberadaan pesan dan dapat dianggap sebagai pelengkap dari kriptografi yang bertujuan untuk menyembunyikan isi pesan. Berbeda dengan kriptografi, dalam steganografi pesan disembunyikan sedemikian rupa sehingga pihak lain tidak dapat mengetahui adanya pesan rahasia. Pesan rahasia tidak diubah menjadi karakter aneh seperti halnya kriptografi. Pesan tersebut hanya disembunyikan ke dalam suatu media berupa gambar, teks, musik, atau

media digital lainnya dan terlihat seperti pesan biasa. Pada masa kini, steganografi lebih banyak digunakan pada data digital dengan media teks, gambar, audio, dan video. Bisa dilihat dari Gambar 2 Ada dua buah proses dalam steganografi yakni proses penyisipan pesan dan proses ekstraksi pesan. Proses penyisipan pesan membutuhkan masukan media penyisipan, pesan yang akan disisipkan, dan kunci. Keluaran dari proses penyisipan ini adalah media yang telah berisi pesan. Proses ekstraksi pesan membutuhkan masukan media yang telah berisi pesan. Keluaran dari proses ekstraksi pesan adalah pesan yang telah disisipkan (Suryani & Martini 2008). Aplikasi ini sebelumnya pernah ada namun di buat dengan metode yang berbeda dengan aplikasi yang saya buat saat ini.

B. Citra RGB

1. Pengertian Citra RGB

Citra RGB disebut juga citra *truecolor*. Citra RGB merupakan jenis citra yang menyajikan warna dalam bentuk komponen R (merah), G (hijau), B (biru). Setiap komponen warna menggunakan delapan bit (nilainya bekisar antara 0 sampai 255). Dengan demikian, kemungkinan warna yang dapat disajikan mencapai 255 x 255 x 255 (Kadir, 2013). Tiap komponen juga memiliki intensitas kecerahan warna yang nantinya saat ketiga komponen digabungkan akan membentuk suatu kombinasi warna baru tergantung besarnya tingkat kecerahan warna yang disumbangkan tiap komponen. Tiap *layer* memiliki ukuran 8 bit sehingga setiap piksel membutuhkan 24 bit, berarti setiap warna mempunyai gradasi sebanyak

256 warna. Artinya tiap *layer* warna dapat menyumbang tingkat kecerahan warnanya dari rentang level 0 sampai level 255. Dimana 0 merepresentasikan warna hitam dan 255 merepresentasikan warna putih. (Wahana Komputer, 2013)

C. Keamanan Data

1. Pengertian keamanan data

Keamanan merupakan komponen yang vital dalam komunikasi data elektronis. Masih banyak orang yang tidak sadar bahwa dengan berkembangnya teknologi informasi maka berkembang pula kejahatan sistem informasi. Misalnya pencurian, pengerusakan atau penyalahgunaan data yang terkirim melalui jaringan komputer oleh pihak yang tidak bertanggung jawab. Ada beberapa teknik yang dapat digunakan untuk mengamankan pengiriman data-data elektronis. Antara lain *kriptografi* yaitu teknik untuk menyandikan sebuah data dengan kunci dan algoritma tertentu. Teknik lain untuk mengamankan data adalah dengan menyembunyikan/menyisipkan data tersebut pada suatu media tertentu yang disebut juga dengan teknik *Steganografi*, sehingga tidak terlihat oleh orang yang tidak berkepentingan.

D. Metode

1. Least significant bit (LSB)

Algoritma penyisipan LSB bekerja dengan cara mengganti bit terakhir dari masing - masing piksel dengan pesan yang akan disisipkan.

LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekuranganya adalah pesan/atau data yang akan disisipkan terbatas, sesuai dengan ukuran citra (Krisnawati, 2008). Sebagai contoh, urutan bit berikut ini menggambarkan 3 piksel pada *cover image* 24-bit.

piksel 1 = (00100111 11101001 11001000)

piksel 2 = (00100111 11001000 11101001)

piksel 3 = (11001000 00100111 11101001)

Pesan yang akan disisipkan adalah karakter "A", yang nilai biner-nya adalah **01000001**, maka akan dihasilkan *stego image* dengan urutan bit sebagai berikut:

piksel 1 = (0010011**0** 1110100**1** 1100100**0**)

piksel 2 = (0010011**0** 1100100**0** 1110100**0**)

piksel 3 = (1100100**0** 0010011**1** 11101001)

2. Vigenere Chiper

Vigenere Cipher atau biasa di sebut *vigenere* termasuk dalam *cipher* abjadmajemuk (*Polyalphabetic Substitution Cipher*) yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16 (tahun 1586, meskipun Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis dalam bukunya *La Cifra Del sig.* Giovan Batistan Belaso. *Vigenere Cipher* dipublikasikan pada tahun 1586, tetapi algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya *Cipher* tersebut kemudian dinamakan *Vigenere Cipher*. *Cipher* ini berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19. *Vigenere Cipher*

Digunakan oleh Tentara Konfiderasi pada perang Sipil America (*American Civil War*). Perang sipil terjadi setelah *Vigenere Cipher* berhasil dipecahkan.

Vigenere Cipher adalah algoritma menyandikan teks alfabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. Algoritma enkripsi jenis ini sangat dikenal karena mudah dipahami dan diimplementasikan.Teknik untuk menghasilkan *ciphertext* bisa dilakukan menggunakan substitusi angka maupun bujursangkar *vigènere*. Teknik susbtitusi *vigenere* dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka.

E. Pemodelan Sistem

1. Flowchart

Flowchart merupakan bagan yang memperlihatkan urutan dan hubungan antar proses beserta instrukturnya. Gambaran ini dinyatakan dengan symbol. Dengan demikian setiap simbol menggambarkan proses tertentu. Sedangkan hubungan antar proses digambarkan dengan garis penghubung.

Flowchart ini merupakan langkah awal pembuatan program. Dengan adanya flowchart urutan proses kegiatan menjadi lebih jelas. Jika ada penambahan proses maka dapat dilakukan lebih mudah. Setelah flowchart selesai disusun, selanjutnya pemrograman (programmer) menerjemahkan ke bentuk program dengan bahasa pemrograman.

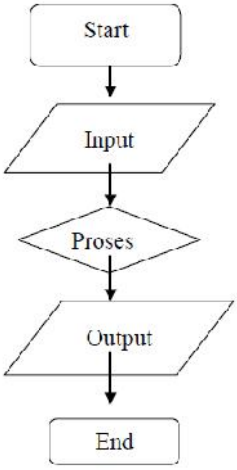
Terdapat 2 jenis flowchart yaitu sebagai berikut :

a) Sistem Flowchart

Sistem flowchart merupakan diagram alir yang menggabarkan suatu sistem peralatan computer yang digunakan dalam proses pengolahan data serta hubungan antar peralatan tersebut. Sistem flowchart tidak digunakan untuk menggambarkan urutan langkah untuk memecahkan masalah, tetapi hanya untuk menggambarkan prosedur dalam sistem yang dibentuk.

b) Flowchart Program

Merupakan bagan alur yang menggambarkan urutan logika dri suatu prosedur pemecahan masalah. Untuk menggambarkan flowchart program telah tersedia simbol-simbol standart. Berikut ini adalah gambar dari simbol-simbol standart yang digunakan pada flowchart program.



Gambar Konsep Flowchart

F. Penjelasan Sistem Steganografi

Penulis mengambil judul Penyembunyian Pesan pada *Image* berformat *JPEG* dengan metode *LSB* dan *Vigenere chiper*, karena Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimiliki oleh internet maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasi semakin berkembang pula kejahatan sistem informasi. Maka dari itu pemulis melakukan penelitian untuk membuat aplikasi pesan yang tidak di ketahui oleh pihak ketiga agar pesan tersebut sampai di tangan pihak kedua dengan aman.

Keunggulan aplikasi ini adalah pesan tidak dapat diketahui oleh orang lain. Dan pesan tersebut memiliki kode tersembunyi agar pihak ketiga tidak bisa membaca isi dari gambar yang sudah terenkripsi pesan ,dan kode tersebut tidak dapat dipecahkan, steganografi dan metode-metode tersebut digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.