Landasan Teori

1. Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain pengirim dan penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Berbeda dengan kriptografi yang menyamarkan arti pesan ke bentuk yang tidak ada maknanya. Kata steganografi berasal dari Bahasa Yunani, *steganos*, yang artinya ‘tersembunyi atau terselubung’ dan *graphein*, menulis.

Sekarang, istilah steganografi juga digunakan untuk menyebutkan penyembunyian pesan melalui media digital. Contohnya pada berkas citra, setiap bit terakhir setiap *pixel* diubah menjadi bit-bit pesan.

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan. Dalam praktiknya, kebanyakan pesan disembunyikan pada media yang membuat perubahan tipis dan tidak akan menarik perhatian.

Pada steganografi digital atau modern ini, banyak berkas-berkas digital yang dapat dijadikan sebagai media untuk menyembunyikan pesan. Format yang biasa digunakan antara lain:

* 1. Citra: bitmap (bmp), png, gif, jpeg, dll.
  2. Audio: wav, mp3, dll.
  3. Format lain seperti berkas teks, html, pdf, dll.

Kelabihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesan tidak menimbulkan kecurigaan. Tetapi steganografi tidak menyediakan keamanan total, sehingga biasanya metode ini digabung dengan kriptografi.

Banyak metode steganografi yang telah dikembangkan mulai dari menyisipkan bit-bit pesan kedalam *pixel* citra. Metode ini paling popular karena mudah untuk diimplementasikan, tetapi kapasitas yang dapat ditampung kecil. Ada beberapa kategori agar suatu teknik steganografi, yaitu:

1. Tidak menimbulkan kecurigaan.
2. Memiliki kapasitas penyimpanan pesan yang besar.
3. Kualitas ­*cover-object* tidak jauh berubah akibat penyisipan pesan rahasia.
4. Pesan yang disembunyikan harus dapat diekstrasi kembali.
5. Metode Modifikasi LSB
6. Metode BPCS
7. Citra Bitmap
8. Berkas Suara