Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

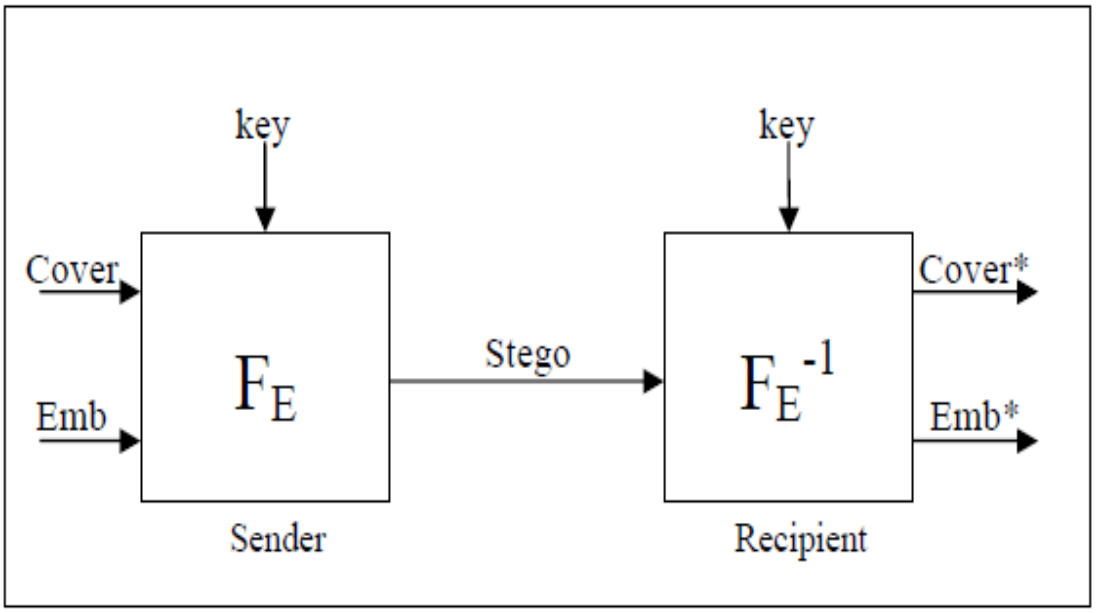
BAB II

LANDASAN TEORI

2.1. Steganografi

Steganografi berasal dari bahasa Yunani, *steganos* dan *graptos* yang memiliki arti tulisan yang disembunyikan (*covered writing*). Pada zaman Yunani dan Romawi dulu, cara melakukan teknik steganografi adalah pesan ditulis di kepala budak tunggu sampai tumbuh cukup rambut untuk menutupi pesan tersebut sebelum budak dikirim kepada orang yang dituju. Kemudian untuk melihat pesannya rambut budak akan dicukur kembali, sehingga pesan dapat terlihat. Steganografi dalam era modern ini berfungsi untuk menyembunyikan suatu pesan rahasia ke dalam media digital lain, sehingga orang lain tidak akan menyadari bahwa ada pesan tersembunyi di dalam media digital tersebut. Hanya orang yang dituju yang menyadari adanya pesan tersembunyi di dalam media digital tersebut. Steganografi berbeda dengan kriptografi, letak perbedaannya adalah hasil keluarannya. Hasil dari kriptografi biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan dan dapat dikembalikan ke bentuk semula. Sedangkan steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi di sini oleh indera manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya. Gambar 2.1 menunjukkan metode dasar bagaimana cara kerja steganografi (Bender, 1996).

Implementasi Metode ..., Muhammad Kresno Satryo Suryo Prakoso, FTI UMN, 2014



Gambar 2.1 Cara Kerja Steganografi

Keterangan:

FE = *Embedding* (Penggabungan berkas *cover* dengan berkas pesan)

FE^{-1} = *Extracting* (Pengambilan berkas pesan dari berkas *cover*)

Cover = Berkas data yang akan disisipkan informasi (*carrier*)

Key = Kunci yang digunakan

Emb = Pesan yang akan disisipkan

Stego = Berkas *cover* yang sudah berisi pesan

2.2. Kriteria dalam Steganografi

Dalam proses Steganografi terdapat beberapa kriteria yang harus dipenuhi, kriterianya adalah sebagai berikut (Munir R, 2006) :

A. **Impercepbility.** Keberadaan pesan tidak dapat dipersepsi oleh indra manusia, baik indra pendengaran maupun indra penglihatan.

B. **Fidelity.** Mutu media pembawa tidak berubah banyak akibat proses penyisipan.

C. **Recovery.** Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai kebutuhan.

2.3. Istilah-Istilah dalam Steganografi

Ada beberapa istilah umum di dalam steganografi sebagai berikut:

A. Embedding Data

Data *embedded* yang tersembunyi dalam suatu media audio digital membutuhkan dua *file*. Pertama adalah media audio digital asli yang belum dimodifikasi yang akan menangani informasi tersembunyi, yang disebut *cover* audio. *File* kedua adalah informasi pesan yang disembunyikan. Suatu pesan dapat berupa teks, baik itu *plainteks, cipherteks*, gambar, atau apapun yang dapat ditempelkan ke dalam *bit-stream*. Ketika dikombinasikan, *cover* audio dan pesan yang ditempelkan membuat *stego-audio*. Suatu *stego-key* (suatu *password* khusus) juga dapat digunakan secara tersembunyi, pada saat *decode* selanjutnya dari pesan.

B. Covertext

Disebut juga *cover-object*. Pesan yang digunakan untuk menyembunyikan *embedded message*.

C. Stegotext

Disebut juga *stego-object*. Pesan yang sudah berisi *embedded message.*

D. Encoding

Data *encoding* adalah proses menempatkan urutan karakter tertentu (huruf, angka, tanda baca, dan simbol tertentu) ke dalam format khusus untuk transmisi yang efisien atau penyimpanan. Sebuah *encoder* mengambil data yang masuk bersamaan dengan beberapa *metadata* (seperti *signal* yang mengindikasikan apakah data mewakili data yang sesungguhnya atau *control character*) dan menghasilkan sebuah nilai yang sudah ter-*encode*.

E. Decoding

Data *decoding* adalah proses yang berlawanan, konversi dari format yang disandikan kembali ke urutan asli dari karakter. *Encoding* dan *decoding* digunakan dalam komunikasi data, jaringan dan penyimpanan. Istilah *encoding* dan *decoding* sering digunakan dalam referensi untuk proses analog ke digital konversi dan digital ke analog konversi. Dalam pengertian ini dapat diterapkan pada segala bentuk data, termasuk teks, gambar, audio, video, multimedia, dan lain- lain (Munir R. 2006).

2.4. Least Significant Bit

Metode steganografi yang paling umum pada format audio adalah *Least Significant Bit*. LSB ini banyak digunakan karena komputasinya tidak terlalu kompleks dan pesan yang disembunyikan tidak terlalu memberikan dampak kepada *file carrier*. Cara kerja metode ini ialah dengan cara memodifikasi nilai yang paling kurang signifikan dari jumlah bit dalam satu *byte* di *file carrier.* Nilai bit yang

terendah adalah 2^0. Kebalikan dari metode *Least Significant Bit* (LSB) adalah *Mass Significant Bit* (MSB). Metode ini jarang dipakai karena MSB mengubah nilai yang paling *significant* dari jumlah bit dalam satu *byte*. Hal ini dapat mengakibatkan *file carrier* mengalami dampak yang besar, bahkan dapat merusak *file carrier* itu sendiri. Sebagai contoh 10010001 nilai satu yang digaris bawah di contoh *byte* ini memiliki pengaruh yang besar jika diubah, artinya bila terjadi perubahan pada bit tersebut akan menghasilkan perubahan yang sangat signifikan. Sedangkan bit yang digaris bawah di contoh berikut 10010001 memiliki nilai terendah, sehingga bila terjadi perubahan pada bit ini akan menghasilkan perubahan yang tidak terlalu signifikan. Berikut contoh, dari proses penyembunyian karakter 'K' (ASCII 75) pada *file carrier* yang berukuran delapan *byte*.

Karakter 'K' dalam biner dengan ukuran 1 *byte* :

'01001011'

Kedelapan bit ini nantinya akan dimasukkan ke dalam *Least Significant Bit* dari tiap-tiap *byte* pada *file carrier* seperti berikut ini:

File carrier dalam biner dengan ukuran delapan *byte*:

'11010100 - 11101101 - 10001001 - 10110110 - 11001111 - 11101011 – 10111111 - 00011100'

Karakter 'K' dalam biner dengan ukuran 1 *byte*:

' 01001011 '

Proses *Least Significant Bit Modification*:

‘11010100 - 11101101 - 10001000 - 10110110 - 11001111 - 11101010 – 10111111 - 00011101’

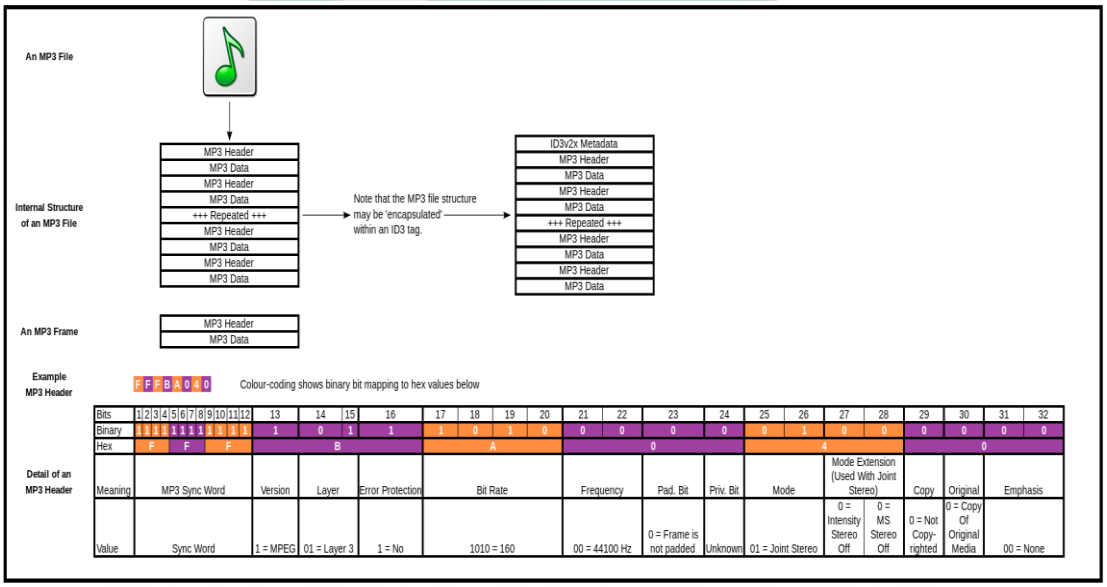
Pada contoh di atas, hanya sebagian dari *Least Significant Bit file carrier* yang berubah (ditunjukkan dengan karakter yang digaris bawah). Berdasarkan teori yang didapat adalah bahwa kemungkinan terjadinya perubahan bit adalah sekitar 50 %, karena peluangnya perubahannya adalah antara 0 atau 1, dan dengan mengubah *Least Significant Bit* maka ukuran dari *file* pembawa tidak akan berubah sehingga akan sulit untuk terdeteksi (Bender, 1996)

2.5. *File* Audio Mp3

MPEG (*Moving Picture Expert Group)* - 1 *audio layer* III atau yang lebih dikenal dengan mp3, adalah salah satu dari pengkodean dalam digital audio dan juga merupakan format kompresi audio yang memiliki sifat “menghilangkan”. Istilah menghilangkan yang dimaksud adalah kompresi audio ke dalam format mp3 menghilangkan aspek-aspek yang tidak signifikan pada pendengaran manusia untuk mengurangi besarnya *file* audio (Aminah Rizky Lubis, 2012).

Sejarah mp3 dimulai dari tahun 1991 saat proposal dari Phillips (Belanda), CCET (Perancis), dan Institut für Rundfunktechnik (Jerman) memenangkan proyek untuk DAB (Digital Audio Broadcast). Produk mereka seperti *Musicam* (akan lebih dikenal dengan *layer* 2) terpilih karena kesederhanaan, ketahanan terhadap kesalahan, dan perhitungan komputasi yang sederhana untuk melakukan pengkodean yang menghasilkan keluaran yang memiliki kualitas tinggi. Pada akhirnya ide dan

teknologi yang digunakan dikembangkan menjadi MPEG-1 *audio layer* 3. Kepopuleran dari mp3 yang sampai saat ini belum tersaingi disebabkan oleh beberapa hal. Pertama mp3 dapat didistribusikan dengan mudah dan hampir tanpa biaya, walaupun sebenarnya hak paten dari mp3 telah dimiliki dan penyebaran mp3 seharusnya dikenai biaya. Pada perbandingan kualitas suara antara beberapa format kompresi audio yang dihasilkan bervariasi pada *bit rate* yang berbeda, perbandingan berdasarkan *codec* (hasil pengkodean) yang digunakan. Pada 128 kbit/s, LAME mp3 unggul sedikit dibandingkan dengan Ogg Vorbis, AAC, MPC and WMA Pro. Kemudian pada 64 kbit/s, AAC-HE dan mp3 pro menjadi yang teratas di antara *codec* lainnya. Dan untuk di atas 128 kbit/s tidak terdengar perbedaan yang signifikan. Pada umumnya format mp3 sekarang menggunakan 128 kbit/s dan 192 kbit/s sehingga hasil yang dihasilkan cukup baik (Binanto I, 2010).



Gambar 2.2 Mp3 Header.

Sumber (Tech-Analyser, 2014)

2.6. Penarikan Sampel Sederhana

Penentuan besar sampel berkaitan dengan seberapa jauh pengujian menginginkan ketelitian dari suatu sampel. Dan dalam menentukan besar sampel ada tiga hal yang perlu diperhatikan, yaitu keragaman (variasi) dari populasi, batas kesalahan sampel yang dikehendaki (*sampling error*), dan interval kepercayaan (*confidence interval*). Penentuan sampel berdasarkan keragaman populasi berdasarkan keseragaman anggotanya. Bila keseragaman anggota dari sampel bersifat (homogen) tidak diperlukan jumlah sampel yang besar. Bahkan pengujian dapat dilakukan cukup dengan mengambil satu sampel saja. (Eriyanto, 2007).