STUDI STEGANOGRAFI DALAM FILE MP3

Simon Batara – NIM : 13503109

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13109@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang *steganografi* dalam file audio yang berekstensi *mp3*. Dalam perjalanan pembahasan makalah, dirunut suatu perkembangan teknologi dalam dunia telekomunikasi yaitu tentang penyembunyian informasi dalam proses komunikasi. Sejarah yang berjalan akhirnya memunculkan suatu teknik penyembunyian pesan yang disebut steganografi.

Perkembangan *steganografi* mulai merambah ke dunia dijital yang dalam makalah ini dikhususkan dalam file audio mp3. Teknik-teknik dalam melakukan pengembangan suatu proses steganografi dibahas secara singkat. Makalah juga mencoba menyajikan proses *steganografi* dalam perbandingan-perbandingan file audio dengan berdasarkan rumus-rumus yang ada pada literatur yang ada. Rumus-rumus tersebut berkisar antara *HVS, PSNR, Capacity*, dan alogritma lainnya.

Sebuah perangkat lunak bernama *MP3 Stego* digunakan untuk membantu proses observasi permasalahan dan menyelesaikan prose steganografi. *MP3 Stego* dicoba, diamati, dan dihipotesakan saran-saran pengembangan untuk kedepannya. Makalah juga mencoba untuk menilik sebagian kecil dari proses implementasi steganografi file *MP3* dari sudut pandang lainnya.

Setelah melihat lebih dalam tentang audio steganografi khususnya pada file audio *MP3* cukup berprospek dalam pengembangan selanjutnya. Baik dikaji dari faktor psikologis dan teknis, ternyata media *MP3* merupakan media yang sangat tepat untuk menjadi media penyembunyian pesan. Selain itu ternyata steganografi juga bisa digunakan dalam target yang lebih mendalam dan luas lagi antara lain sebagai saran kampanye, pemberitahuan, komunikasi organisasi, dan lain-lain.

Kata kunci : *MP3, Steganografi, HVS, PSNR, Capacity, MP3 Stego.*

Apa itu steganografi ?

Sekilas dari sejarah penyembunyian dan pengiriman pesan serta steganografi

Kata steganografi pada awalnya berasal dari kata steganos. Steganos sendiri sebenarnya merupakan kata dari bahasa Yunani. Kata steganos lebih lengkapnya : *steganos* memiliki arti penyamaran atau penyembunyian dan *graphein* atau *graptos* memiliki arti tulisan. Pengertian steganografi yang cukup sering digunakan dalam pembelajaran dengan metodologi sejarah adalah menulis tulisan yang tersembunyi atau terselubung" (Sellars, 1996).

Jadi secara harafiah dan dalam pengertian yang didewasakan steganografi dapat diartikan sebagai seni untuk menyamarkan atau menyembunyikan pesan rahasia tertulis ke dalam pesan lainnya dengan segala cara sehingga selain orang yang dituju, orang lain tidak akan tahu pesan rahasia apa yang sebenarnya ingin disampaikan.

Steganografi sudah diadakan sejak dulu untuk berbagai kebutuhan. Seperti yang kita ketahui, suatu barang teknologi atau produk teknologi akan lahir dari sebuah kebutuhan untuk mencapai suatu kondisi yang lebih baik lagi. Kebutuhan ini senantiasa berevolosi dan disempurnakan terus menerus. Dulunya orang hanya ingin menyembunyikan teks, yaitu dengan menyembunyikannya di kertas dan disimpan baik-baik dengan rahasia. Penyembunyian pesan ini kemudian menjadi berubah fungsi menjadi

pengiriman pesan rahasia. Hal ini terjadi karena adanya kebutuhan bahwa harus ada orang lain yang dapat menerima pesan rahasia ini dengan menjaga nilai-nilai yang ada seperti kerahasiaan pesan dan ketersampaian pesan dengan baik sehingga orang yang menerima pesan tersebut akan dapat mengerti arti pesan tersebut.

Hal pengiriman pesan ini tadinya hanya dilakukan menggunakan pengawal untuk melindungi pesan dan menjaga kerahasiaan. Semakin lama, seiring dengan berjalannya zaman dimana kekerasan tidak lagi dianggap rasional lagi. Hal ini menimbulkan kerahasiaan pesan tidak lagi dijaga dengan menggunakan kekerasan melainkan dengan metodologi-metodologi baru seperti enkripsi pada pesan. Proses penyamaran ini semakin lama semakin berkembang juga seiring dengan bertambahnya kebutuhan dan keinginan dengan kontinuitas yang tinggi.

Seluruh ulasan dan ringkasan diatas akhirnya mengarah pada suatu teknik steganografi.

Catatan pertama tentang steganografi ditulis oleh seorang sejarawan Yunani, Herodotus, yaitu ketika Histaeus seorang raja kejam Yunani dipenjarakan oleh Raja Darius di Susa pada abad 5 sebelum Masehi. Histaeus harus mengirim pesan rahasia kepada anak laki-lakinya, Aristagoras, di Militus. Histaeus menulis pesan dengan cara mentato pesan pada kulit kepala seorang budak dan ketika rambut budak itu mulai tumbuh, Histaeus mengutus budak itu ke Militus untuk mengirim pesan di kulit kepalanya tersebut kepada Aristagoras.

Cerita lain tentang steganografi datang juga dari sejarawan Yunani, Herodotus, yaitu dengan cara menulis pesan pada papan kayu yang ditutup dengan lilin. Demeratus, seorang Yunani yang akan mengabarkan berita kepada Sparta bahwa Xerxes bermaksud menyerbu Yunani. Agar tidak diketahui pihak Xerxes, Demaratus menulis pesan dengan cara mengisi tabung kayu dengan lilin dan menulis pesan dengan cara mengukirnya pada bagian bawah kayu, lalu papan kayu tersebut dimasukkan ke dalam tabung kayu, kemudian tabung kayu ditutup kembali dengan lilin.

Teknik steganografi yang lain adalah tinta yang tak terlihat. Teknik ini pertama digunakan pada zaman Romawi kuno yaitu dengan menggunakan air sari buah jeruk, urine atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas nyala lilin, tinta yang sebelumnya tidak terlihat, ketika terkena panas akan berangsur-angsur menjadi gelap, sehingga pesan dapat dibaca. Teknik ini pernah juga digunakan pada Perang Dunia II.

Steganografi, tepatnya dari 2500 tahun lalu sudah dipakai untuk berbagai kebutuhan seperti kepentingan politik, militer diplomatik, serta untuk kepentingan pribadi yaitu alat komunikasi pribadi. Beberapa penggunaan steganografi pada masa lampau bisa kita lihat dalam beberapa instans berikut ini :

- Pada perang dunia II, Jerman menggunakan *microdots* untuk berkomunikasi. Penggnaan teknik ini biasa digunakan pada *microfilm* chip yang harus diperbesar sekitar 200 kali. Dalam hal ini Jerman menggunakan steganografi untuk kebutuhan Perang sehingga pesan rahasia strategi atau apapun tidak bisa diketahui oleh pihak lawan. Teknologi yang digunakan dalam hal ini adalah teknologi baru yang pada saat itu belum bisa digunakan oleh pihak lawan.
- Pada perang dunia II, Amerika Serikat menggunakan suku Indian Navajo sebagai media untuk berkomunikasi. Dalam hal ini Amerika Serikat menggunakan steganografi untuk kebutuhan berperang. Amerika Serikat menggunakan teknologi kebudayaan sebagai suatu alat dalam steganografi. Teknologi kebudayaan yang dimiliki Amerika Serikat ini tidak diketahui atau dimiliki oleh pihak lawan.

Dari catatan sejarah, pengalaman, dan contoh-contoh steganografi konvensional tersebut, dapat kita lihat dan sintesiskan bahwa semua teknik steganografi konvensional yang pernah dilakukan selalu berusaha merahasiakan komunikasi yang ingin dirahasiakan dengan cara menyembunyikan pesan, mengkamuflase ataupun menyamarkan pesan.

Jadi sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasian komunikasinya bukan pada datanya (Johnson, 1995).

Perkembangan teknologi yang semakin pesat terutama teknologi komputasi dan teknologi media yang semakin bervariasi dan semakin fleksibel untuk dimanipulasi, steganografi merambah juga ke media digital, walaupun steganografi dapat dikatakan mempunyai

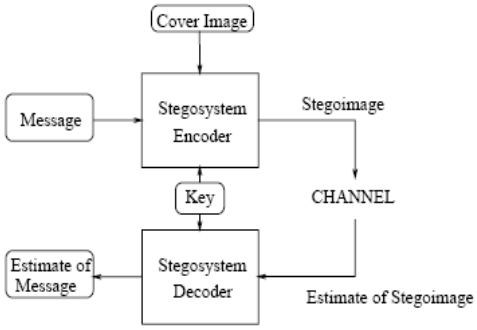
hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda.

Pengertian Steganografi

Setelah mengamati runtutan sejarah dan perkembangan pengertian serta penggunaan, maka dapat disimpulkan bahwa steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni menyembunyikan sesuatu informasi. Steganografi dapat dipandang atau dikelompokkan sebagai salah satu bagian atau cabang dari ilmu komunikasi. Kata steganografi berasal dari bahasa Yunani yang berarti "tulisan tersembunyi". Pada era informasi digital, steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak kelihatan atau dapat tersamarkan..

Secara teori, semua file umum yang ada di dalam komputer dapat digunakan sebagai media, seperti file gambar berformat JPG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI. Semua dapat dijadikan tempat bersembunyi, asalkan file tersebut memiliki bit-bit data redundan yang dapat dimodifikasi. Setelah dimodifikasi file media tersebut tidak akan banyak terganggu fungsinya dan kualitasnya tidak akan jauh berbeda dengan aslinya. Proses penyimpanan dengan memanfaatkan bit-bit ini sangatlah dikembangkan pada era ini karena lebih mudah dilakukan (teknologi komputasi yang semakin berkembang) dan lebih sulit dicurigai atau lebih baik dalam masalah keamananya (media dijital merupakan media yang sudah banyak diketahui orang dan memiliki kegunaan tersendiri sehingga orang akan memandangnya sebagai media yang memang untuk dipakai sesuai bentuknya).

Adapun proses yang biasa terjadi dalam proses steganografi sebagai berikut :



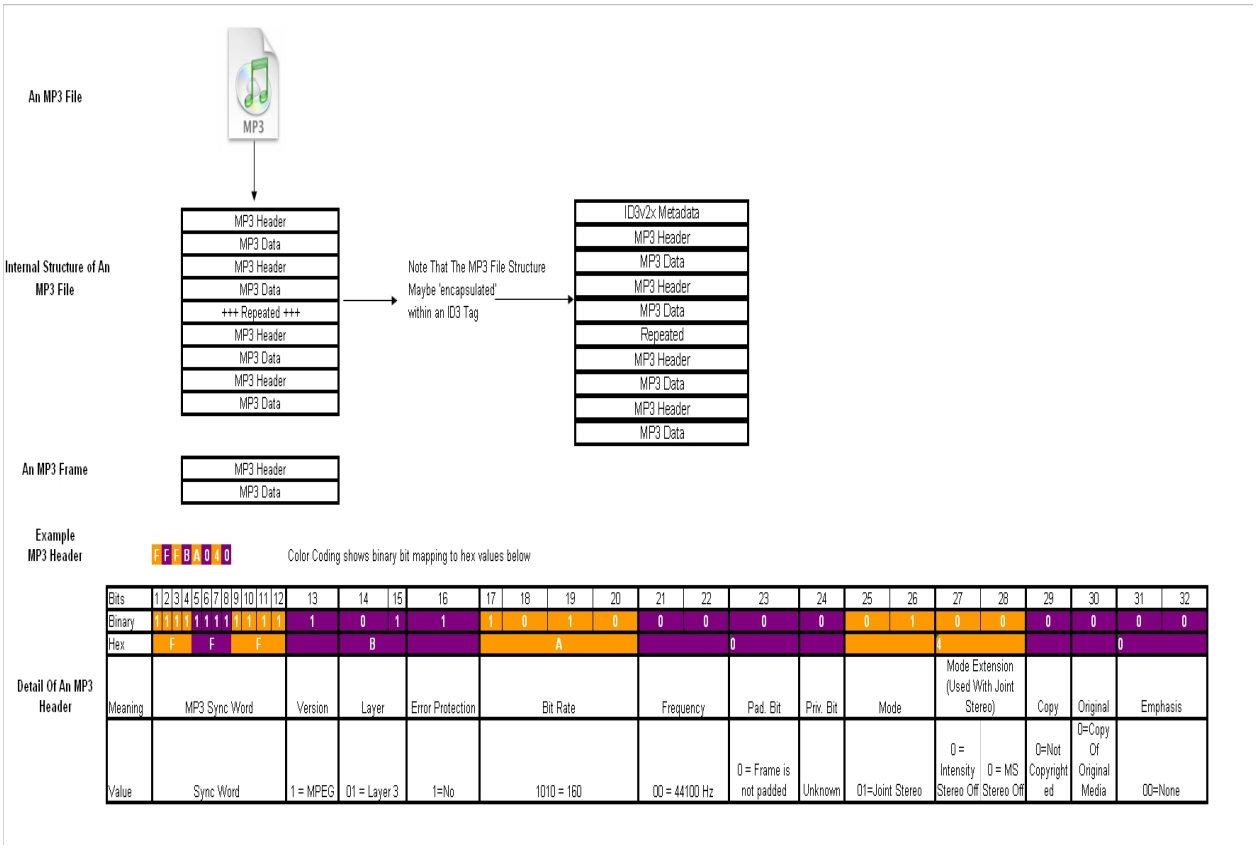
File MP3

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.

Sejarah mp3 dimulai dari tahun 1991 saat proposal dari Phillips (Belanda), CCET (Perancis), dan Institut für Rundfunktechnik (Jerman) memenankan proyek untuk DAB (Digital Audio Broadcast). Produk mereka Musicam (akan lebih dikenal dengan layer 2) tewrpilih 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.

MP3 adalah pengembangan dari teknologi sebelumya sehingga dengan ukuran yang lebih kecil dapat menghasilkan kualitas yang setara dengan kualitas CD. Spesifikasi dari layer-layer sebagai berikut:

- Layer 1: paling baik pada 384 kbit/s
- Layer 2: paling baik pada 256...384 kbit/s, sangat baik pada 224...256 kbit/, baik pada 192...224 kbit/s
- Layer 3: paling baik pada 224...320 kbit/s, sangat baik pada 192...224 kbit/s, baik pada 128...192 kbit/s



Kompresi pada MP3

Kompresi yang dilakukan oleh mp3 seperti yang telah disebutkan diatas, tidak mempertahankan bentuk asli dari sinyal input. Melainkan yang dilakukan adalah menghilangkan suara-suara yang keberadaannya kurang/tidak signifikan bagi sistem pendengaran manusia. Proses yang dilakukan adalah :

Tahap 1
menggunakan model dari sistem pendengaran manusia dan menentukan bagian yang terdengar bagi sistem pendengaran manusia.
Tahap 2.
Setelah itu sinyal input yang memiliki domain waktu dibagi menjadi blok-blok dan ditransformasi menjadi domain frekuensi.
Tahap 3.
Kemudian model dari sistem pendengaran manusia dibandingkan dengan sinyal input dan dilakukan proses pemfilteran yang menghasilkan sinyal dengan range frekuensi yang signifikan bagi sistem pendengaran manusia.

Proses diatas adalah proses pengirisan dua sinyal yaitu sinyal input dan sinyal model sistem pendengaran manusia.

Tahap 4.
Langkah terakhir adalah kuantisasi data, dimana data yang terkumpul setelah pemfilteran akan dikumpulkan menjadi satu keluaran dan dilakukan pengkodean dengan hasil akhir *file* dengan format mp3.

Proses pengkompresian mp3 dapat menghasilkan keluaran yang hampir setara dengan aslinya disebabkan oleh kelemahan dari sistem pendengaran manusia yang dapat dieksploitasi. Berikut adalah beberapa kelemahan dari sistem pendengaran manusia yang digunakan dalam pemodelan:

- Terdapat beberapa suara yang tidak dapat didengar oleh manusia (diluar jangkauan frekuensi 30-30.000 Hz).
- Terdapat beberapa suara yang dapat terdengar lebih baik bagi pendengaran manusia dibandingkan suara lainnya.
- Bila terdapat dua suara yang dikeluarkan secara simultan, maka pendengaran manusia akan mendengar

yang lebih keras sedangkan yang lebih pelan akan tidak terdengar.

File Gambar

Pada komputer, suatu gambar adalah suatu array dari bilangan yang merepresentasikan intensitas terang pada point yang bervariasi (pixel). Pixel ini menghasilkan *raster data* gambar. Suatu ukuran gambar yang umum adalah 640 x 480 pixel dan 256 warna (atau 8 bit per pixel). Suatu gambar akan berisi kira-kira 300 kilobit data.

Gambar digital disimpan juga secara khusus di dalam file 24-bit atau 8-bit. Gambar 24-bit menyediakan lebih banyak ruang untuk menyembunyikan informasi; bagaimanapun, itu dapat sungguh besar (dengan perkecualian gambar JPEG). Semua variasi warna untuk pixel yang diperoleh dari tiga warna dasar: merah, hijau dan biru. Setiap warna dasar direpresentasikan dengan 1 byte; gambar 24-bit menggunakan 3 byte per pixel untuk merepresentasikan suatu nilai warna. 3 byte ini dapat direpresentasikan sebagai nilai hexadecimal, decimal, dan biner. Dalam banyak halaman Web, warna latar belakang direpresentasikan dengan bilangan 6 digit hexadecimal, yang aktualnya tiga ikatan merepresentasikan merah, hijau dan biru. Latar belakang putih akan mempunyai nilai FFFFFF: 100% merah (FF), 100% hijau (FF) dan 100% biru (FF). Nilai decimal-nya 255,255,255 dan nilai biner-nya adalah 11111111, 11111111, 11111111, yang adalah tiga byte yang menghasilkan putih.

Definisi latar belakang putih adalah analog dengan definisi warna dari pixel tunggal dalam suatu gambar. Pixel merepresentasikan kontribusi pada ukuran file. Untuk contoh, andaikan kita mempunyai gambar 24-bit luasnya 1,024 pixel dengan ketinggian 768 pixel, yang merupakan resolusi umum untuk grafik beresolusi tinggi. Suatu gambar mempunyai lebih dari dua juta pixel, masing-masing mempunyai definisi yang akan menghasilkan suatu kelebihan file 2 Mbyte. Karena gambar 24-bit masih relative tidak umum pada internet, ukuran seperti ini akan menarik perhatian selama transmisi. Kompresi file akan menguntungkan, jika tidak perlu transmisi file seperti itu.

Kompresi pada File Gambar

Dua kandungan dari kompresi adalah *lossless* dan *lossy*. Kedua metoda ini menghemat ruang penyimpanan tetapi mempunyai hasil yang berbeda, yang bertentangan dengan penyembunyian informasi. Kompresi *lossless* membiarkan kita merekonstruksi pesan asli yang sama; oleh karena itu, lebih disukai ketika informasi asli harus tetap utuh (seperti dengan gambar steganography). Kompresi *lossless* khusus untuk gambar yang tersimpan sebagai GIF (*Graphic Interchange Format*) dan BMP 8-bit (file bitmap Microsoft Windows dan OS/2).

Kompresi *lossy*, pada penanganan lainnya, menghemat ruangan tetapi tidak menjaga integritas gambar aslinya. Metoda ini secara khusus untuk gambar yang tersimpan sebagai JPEG (*Joint Photographic Experts Group*).

Kenapa harus MP3 ?

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. Walaupun begitu, pemilik hak paten dari mp3 telah memberikan pernyataan bahwa penggunaan mp3 untuk keperluan perorangan tidak dikenai biaya. Keuntungan lainnya adalah kemudahaan akses mp3, dimana banyak sofware yang dapat menghasilkan file mp3 dari CD dan keberadaan *file* mp3 yang bersifat *ubiquitos* (kosmopolit).

Pada perbandingan kualitas suara antara beberapa format kompresi audio hasil yang dihasilkan bervariasi pada bitrate yang berbeda, perbandingan berdasarkan codec 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 mp3pro menjadi yang teratas diantara codec lainnya. Dan untuk diatas 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.

Penggunaan MP3 sekarang menjadi sangat tinggi karena pada dasarnya seorang manusia akan lebih suka melakukan hal yang bisa menghibur lebih dibandingkan hal yagn statik dan tidak menghibur. Perbedaan ini membuat MP3 lebih dipilih untuk digunakan dibandingkan menggunakan file gambar. Dalam melakukan

penyembunyian pesan, akan lebih dipilih format yang lebih lumrah digunakan sehingga tidak menimbulkan kecurigaan yang terlalu berlebih.

Maka dari itu penggunaan mp3 sebagai salah satu media steganografi merupakan langkah yang baik. Lalu lintas pertukaran mp3 di internet merupakan hal biasa sehingga steganografi menggunakan mp3 adalah teknik yang baik untuk mengamankan pesan rahasia melalui media internet. Selain itu jika kita tidak bicara dalam konteks internet, steganografi juga menjadi media yang paling digemari karena paling sering digunakan sebagai sarana hiburan. Semakin sering file itu atau semakin terlihat file itu maka akan semakin kecil kecurigaan bahwa terdapat pesan tersembunyi dalam file tersebut. Ada pepatah yang mengatakan :
"Tempat yang paling aman adalah di kandang musuh"

Steganalysis dan Penggunaan Steganografi

Steganalysis merupakan suatu teknik atau yang digunakan untuk mengungkapkan keberadaan pesan tersembunyi atau tersamar dari steganografi. Steganalysis menjadi suatu misteri tersendiri untuk dapat diketahui bagaimana teknik untuk melakukan proses dekripsi atau pemecahan atau penemuan pesan tersebut. Terdapat beberapa *software* yang dapat melakukan analisa adanya penggunaan teknik steganografi. Dalam praktiknya cara pemecahan teknik apa yang digunakan dalam steganalysis sendiri secara empirik berkisar diantara :

- Menganalisa dari perubahan yang dilakukan terhadap meta data *file* tersebut.
- Menganalisa dari ciri-ciri *file* telah menggunakan *software* tertentu untuk steganografi.
- Membandingkan *file* asli, lalu dicari perbedaannya dan pola yang digunakan sehingga dengan cara ini bukan saja dapat diketahui *file* telah mengalami psoses steganografi dapat pula diketahui pesan yang disembunyikan.

Tetapi teknik steganalysis tidak dapat digunakan untuk mengetahui pesan yang disembunyikan bila ternyata pesan tersebut mengalami kriptografi atau pengkodean pesan lagi. Jadi cara yang baik untuk melakukan steganografi adalah dengan melakukan asumsi bahwa orang akan tahu bahwa ada pesan yang disembunyikan sehingga dilakukan pengamanan lagi dengan kriptografi. Pemilihan kriptografi juga jangan dilakukan dengan sembarangan dan gunakan yang sudah terbukti keampuhannya seperti 3DES dan SHA-1.

Penggunaan steganografi khususnya *digital watermarking* biasanya digunakan untuk menyimpan informasi yang rahasia. Karena ukuran pesan yang dapat disimpan menggunakan *digital watermarking* relatif kecil, maka informasi yang disimpan juga sesuatu yang rahasia namun dalam ukuran kecil. Contoh penggunaannya adalah untuk nomor PIN, nomor rekening, nomor kunci public, dan sebagainya. Selain itu penggunaan steganografi juga dapat digunakan untuk untuk memberikan tanda *copyright* terhadap *file* gambar, audio (seperti mp3), dan video.

Dalam sudut pandang yang lebih negatif lagi kita bisa memandang steganografi sebagai teknologi yang berdampak buruk bagi kehidupan masyarakat. Steganografi tenyata digunakan juga untuk melakukan tindakan kriminal. Terdapat dugaan juga bahwa steganografi digunakan oleh para teroris untuk menjalankan aksinya. Dengan steganografi, peta, sasaran , dan rencana tindakan teroris disamarkan dalam situs-situs *mailing list* olahraga dan pada situs-situs porno. Maka dari itu kelebihan dari steganografi sangat disayangkan bila dipakai untuk tujuan kejahatan. Tindakan kejahatan lainnya yang mungkin difasilitasi oleh steganografi yaitu untuk perjudian, penipuan, virus, dan lain-lain.

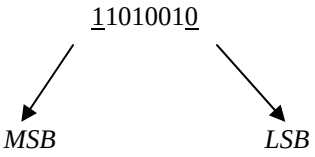
Dalam sudut pandang lain, teknologi steganografi ini bisa dijadikan senjata yang ampuh dalam permainan politik ataupun kebijakan yang diambil satu organisasi. Dengan menggunakan steganografi, seorang calon presiden atau calon ketua bisa melakukan pengiriman pesan pada kader-kadernya di daerah tanpa diketahui oleh orang lain ataupun panitia pemilihan sehingga strategi atau kebijakan yang diambil tidak bisa dibaca oleh pihak lawan padahal dia bisa menyebarkannya dengan cara yang terbuka dan *fair*. Hal ini merupakan keuntungan bagi yang memang menggunakan steganografi sebagai alat teknologi untuk targetan yang lebih jauh lagi. Hal ini juga jauh lebih mudah untuk diimplementasikan ketimbang mendistribusikan pesan rahasia yang nantinya akan dicurigai serta menimbulkan biaya besar dalam pendistribusiannya yang dilakukan secara rahasia.

Audio Steganografi pada MP3

Pada pembahasan ini akan dibahas teknik steganografi dalam MP3 secara umum dan secara khusus mengacu pada *software* MP3Stego. MP3Stego adalah *software* yang dapat digunakan untuk meyembunyikan pesan dalam MP3. Produk ini dapat digunakan secara bebas, namun terdapat beberapa kelemahan dari produk ini karena hanya merupakan program bebas yang belum disempurnakan. Keberadaan program ini ditujukan oleh pembuat hanya untuk membuktikan bahwa steganografi dalam MP3 dapat dilakukan.

Cara untuk mengaplikasikan steganografi pada *file* audio terdiri dari beberapa cara yang lazim digunakan, antara lain dengan cara mengganti atau menambahkan bit. Berikut adalah beberapa teknik yang digunakan:

- Penggantian LSB
  Metode pertama adalah dengan penggantian LSB. Cara ini biasa digunakan dalam teknik digital steganografi yaitu mengganti LSB input setiap samplingnya dengan data yang dikodekan. Dengan metode ini keuntungan yang didapatkan adalah ukuran pesan yang disispkan relative besar, namun berdampak pada hasil audio yang berkualitas kurang dengan banyaknya *noise*.

  LSB = Least Significant Bit
  MSB = Most Siginificant Bit

  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

- Rekayasa sinyal masukan
  Metode kedua yang digunakan adalah merekayasa fasa dari sinyal masukan. Teori yang digunakan adalah dengan mensubstitusi awal fasa dari tiap awal segment dengan fasa yang telah dibuat sedemikian rupa dan merepresentasikan pesan yang disembunyikan. Fasa dari tiap awal segment ini dibuat sedemikian rupa sehingga setiap segmen masih memiliki hubungan yang berujung pada kualitas suara yang tetap terjaga. Teknik ini menghasilkan keluaran yang jauh lebih baik daripada metode pertama namun harus dibayar mahal dengan kerumitan dalam realisasi dan implementasinya..

- Penyebaran Spektrum
  Metode yang ketiga adalah penyebaran spektrum. Dengan metode ini pesan dikodekan dan disebar ke setiap spektrum frekuensi yang memungkinkan. Maka dari itu akan sangat sulit bagi yang akan mencoba memecahkannya kecuali ia memiliki akses terhadap data tersebut atau dapat merekonstruksi sinyal random yang digunakan untuk menyebarkan pesan pada range frekuensi.

- Teknik *Echo*
  Metode terakhir yang sering digunakan adalah menyembunyikan pesan melalui teknik *echo*. Teknik menyamarkan pesan ke dalam sinyal yang membentuk *echo*. Kemudian pesan disembunyikan dengan menvariasikan tiga parameter dalam *echo* yaitu besar amplitudo awal, tingkat penurunan atenuasi, dan offset. Dengan adanya offset dari *echo* dan sinyal asli maka *echo* akan tercampur dengan sinyal aslinya, karena sistem pendengaran manusia yang tidak

memisahkan antaha *echo* dan sinyal asli.

Keempat metode di atas memiliki kesamaan yaitu menggunakan kelemahan dari sistem pendengaran manusia. Maka dari itu teknik steganografi dalam MP3 juga akan menggunakan kelemahan ini untuk menyembunyikan pesan.

Ada sebuah teknik lagi yang memanfaatkan *metrics* pada file. Teknik ini dikenal dengan teknik *Existing Metrics*. Sebagai lanjutan, teknik ini akan dibahas dalam bagian tersendiri setelah ini.

Existing Metrics

Dalam menyembunyikan data, kita memiliki dua tujuan utama yaitu data harus sulit diketahui oleh pihak luar dan harus bisa dibuka dengan baik oleh si penerima pesan atau yang membutuhkan data rahasia tersebut. Sangat sulit untuk mengkuantifikasi seberapa sulit data itu disembunyikan.

Dalam kasus steganografi pada file gambar, banyak pemecah kode mendeteksi resource yang ada termasuk HVS khusunya analis komputer. Dari sekian banyak metode yang ada, penyembunyian data terindikasi dari mengilustrasikan gambar asli dan bagian-bagiannya dengan data yang tergabung di dalamnya, sehingga perbedaan visualnya bisa terlihat kemudian. Sebagai tambahan *mean-squared-error (MSE)* atau *peak-signal-to-noise-ratio (PSNR)* antara file asli dan file yang sudah tersteganografi bisa diketahui atau bisa terlihat. Pixel dari gambar asli sebagai xi dan pixel dari gambar yang sudah tersteganografi didefinisikan sebagai x^ i. Variabel L mendefinisikan *peak signal level* (L=255 untuk *grayscale image*).

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2.$$

$$PSNR = 10\log_{10}\frac{L^2}{MSE}.$$

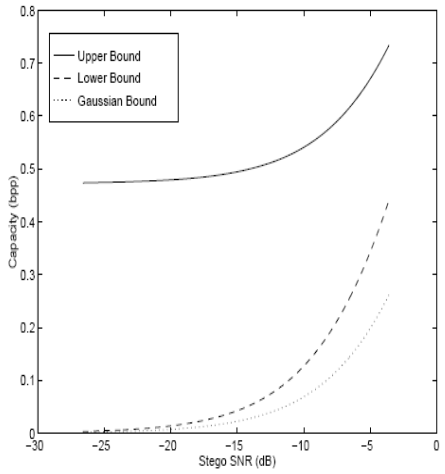
Dalam audio steganografi, pemecah kode menggunakan sistem pendengaran manusia sama baiknya dengan menggunakan analisis komputer dalam mendeteksi *device*. Sebagai perbandingan pendekatan, spektogram dari sinyal asli dan yang sudah terubah biasanya diberikan atau dihadirkan dalam bentuk data. Spektogram adalah plot sederhana yang berisi frekuensi dari konten sinyal audio sebagai fungsi waktu. Dalam beberapa kasus tertentu, kualitas dari file audio yang berisi data tersembunyi bisa diperkirakan menggunakan *perceptual audio measure, noise-to-mask ratio*, atau SNR.

$$SNR = \frac{\sigma^2_{signal}}{\sigma^2_{noise}}.$$

Dua variabel yang hadi r diatas dan dibawah merepresentasikan varians contoh dari sinyal perspektif. Dalam persamaan di atas, data tersembunyi dimodelkan sebagai sinyal dan data penyembunyi sebagai *noise*. SNR, yang juga bisa digunakan dalam file gambar, menyediakan estimasi kasar dari ketersembunyian pesan dengan banyak hal yang dibandingkan dan dipertimbangkan. Semakin tinggi SNR, maka semakin jelas juga ketersembunyian pesan yang ada.

Sebagai perkiraan yang jauh dari efisiensi atau kapasitas yang bisa digunakan dalam *Gaussian channel*. Kekuatan sinyal dari file tersembunyi direpresentasikan dalam variabel S dan kekuatan dari data penyembunyi direpresentasikan dalam variabel N. Formulasi mengasumsikan bahwa statistik dari data penyembunyi ternyata mematuhi atau mengikuti distribusi *Gaussian.* Banyak juga pemikiran yang setuju bahwa semakin baik model dari *channel noise* maka semakin baik pula estimasi dari kapasitas.

$$C = \frac{1}{2}\log\left(1 + \frac{S}{N}\right).$$



Gambar diatas adalah gambar tentang perbandingan kapasitas dalam file yang ada dimodelkan dalam sebuah grafik kapasitas berbanding dengan SNR atau lebih dikenal dengan *Generic Steganographic Channel Capcity*

Sebuah Pendekatan lain tentang MP3 Steganografi File System

Pendekatan ini dirancang bukan oleh penulis. Penulis hanya mencari referensi untuk semakin menjelaskan proses stegaografi dalam praktik yang lebih dekat lagi. mplementasi yang diinginkan adalah implementasi yang implementasi yang bisa bebas atau tidak tergantung pada sistem operasi atau teknologi lain. Karena itu file sistem diimplementasikan diatas file biasa.

File sistem steganografi ini harus fleksibel dan mudah untuk diimplementasikan dalam berbagai bahasa atau siste operasi manapun. Media penyimpanan juga diperhatikan ketika pengguna juga bisa menggunakan media penyimpanan lokal atau *removable USB key*. Ini bisa membebaskan pengguna dari isu pada level yang lebih rendah.

File yang paling sulit untuk dicurigai adalah media hiburan yang sering digunakan oleh orang banyak. Maka dari itu MP3 merupakan jenis file yang cocok untuk diimplementasikan. Dan medianya bisa menggunakan iPod ataupun MP3 player.

Persyaratan dari file sistem yang ada juga tidak terlalu lebar. Hal ini memberika pengguna kemampuan untuk menyimpan berbagai macam file di dalam direktori-direktori yang berbeda, jika memang memungkikan.

Operasi yang didukung atau dilayani oleh file sistem adalah :

- Memperluas
  Melakukan looping terus melalui list dari file mp3 dan mempersiapkan mereka untuk data ke depannya.

- Memformat
  Menghapus seluruh file yang tersedia dalam dile sistem

- Menambah
  Mengkopi sebuah file ke dalam file sistem ataupun dari file sistem

- Membuang
  Menghapus file yang ada dari file sistem

- Mengganti nama
  Mengganti nama dari file yang ada

- Mengekstrak
  Mengkopi file dari file sistem ke tempat lain

Implementasi sederhana

Setiap file MP3 yang dimiliki mempunyai tempat kosong bagi data untuk disimpan, jadi besar space penyimpanan file sistem adalah jumlah seluruh tempat penyimpanan yang kosong dari setiap file MP3. Setia file MP3 akan diperlakukan sebagai stream, karena itu tempat penyimpanan yang kosong akan diisi dengan potongan dari file asli yang ingin disimpan. Setiap potongan file akan berisikan header sederhana yang menjelaskan potongan itu. Hal itu bisa diimplementasikan mengikuti struktur berikut ini :

```
typedef struct _ORIGFILE_CHUNK {
   /* crc32 of the current chunk */
   UINT32 chunk_crc32;
   UINT32 origfile_crc32;

   struct orig_filename {
      UINT8 filename_size;
      CHAR filename[];
   };
```

```
   struct orig_data {
      /* the offset from the original file */
      UINT32 offset;
      UINT32 chunk_size;
      BYTE chunk_data[];
   };
} ORIGFILE_CHUNK, *PORIGFILE_CHUNK;
```

File asli akan disimpan dalam potongan. Dengan asumsi sebesar-bearnya sesuai dengan yang file butuhkan. Proses pengembalian akan dilakukan dengan cara-cara sebagai berikut :

- Baca semua potongan ke dalam memory
- Cek atau validasi keutuhan dari seluruh potongan yang tersimpan
- Rancang dan bangun sebuah kamus dengan nama file yang asli sebagai kunci
- Kembalikan atau bangunlah file asli dari potongan-potongan tersebut

Setelah langkah-langkah diatas telah selesai dilakukanm kita harus mengecek ulang keutuhan dari setiap file yang ada. Kita akan melakukan itu dengan menggunakan *origfile_crc32* dari setiap potongan. Kemudia kita bandingkan mereka dengan crc32 yang sudah terkalkulasi dari seluruh file data yang asli dari potongan-potongan yang bisa bereaksi atau berfungsi.

Dasar dari pendekatan steganografi bisa berasal dari apapun yang dipikirkan atau sesuatu yang ingin dijadikan ide.. Sebuah proyek yang baik diambil sebagai contoh adalah MP3 Stego. MP3 Stego bisa digunakan untuk mengimplementasikan bagian-bagian dari proses steganografi. Datanya sendiri dilindungi lebih lanjut dengan menggunakan proses enkripsi.

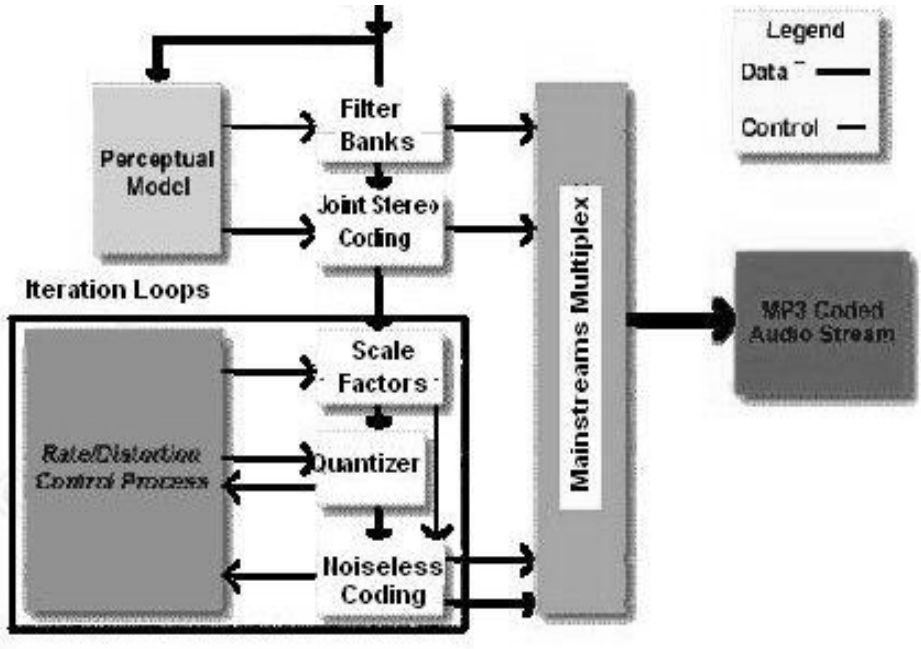
MP3 Stego

Seperti yang disebutkan diatas, MP3Stego dapat digunakan untuk steganografi. Cara kerja dari program ini berdasarkan dari teknik kompresi audio dari WAV ke MP3. Seperti yang sudah diketahui, MP3 adalah kompresi yang bersifat “menghilangkan” data-data yang tidak signifikan bagi pendengaran manusia, maka dari itu program ini menggunakan keuntungan itu dengan tidak menghilangkan seluruh data yang *redundant*, melainkan digantikan dengan pesan yang akan dimasukan.

Proses pengkodean dan kompresi MP3 secara umum terbagi menjadi dua siklus iterasi, yaitu :

- Di dalam siklus iterasi berupa siklus untuk ratifikasi
- Di luar siklus iterasi untuk pengendalian distorsi dan *noise*.

Sebelumnya kita sudah membahas tentang tahapan pengkompresian file MP3. Proses pengkompresian dapat dilihat lebih jelas dengan diagram ini :



MP3 Stego memasukan data pada saat proses kompresi pada proses di dalam siklus iterasi.

Proses penyembunyian pesan secara garis besar adalah pesan dikompresi lalu dienkripsi dan terakhir disembuyikan pada rangkaian bit MP3. Setelah mengalami kompresi, lalu pesan tersebut dienkripsi untuk menjami keamananya. Seperti yang telah dibahas diatas, pesan steganografi dianggap dapat diketahui keberadaannya maka untuk keamanan pesan tersebut harus dilakukan tindakan pengamanan, antara lain enkripsi. Enkripsi yang digunakan adalah 3DES yang sudah teruji keandalannya, sehingga walaupun keberadaannya diketahui isi pesan akan tetap aman.

Kemudian dilanjutkan dengan proses penyebaran pesan terenkripsi pada rangkaian bit MP3. Proses ini merupkan proses yang terumit dalam keseluruhan proses. Ada beberapa tahapan proses dalam melakukan penyebaran pesan yang sudah terenkripsi tersebut dalam rangkaian proses yang ada.

- Kuantitasi data dalam siklus iterasi
  Pertama-tama proses ini terjadi pada di dalam siklus iterasi, di dalam siklus iterasi ini terjadi kuantisasi data dari sinyal input yang sesuai dengan model sistem pendengaran manusia.
- Pengumpulan data
  Mengumpulkan data-data tersebut hingga mencapai ukuran yang tepat sehingga dapat dikodekan.
- Spesifikasi model
  Sedangkan siklus lainnya memastikan data memenuhi spesifikasi model sistem pendengaran manusia.
- Pengubahan pesan
  Kemudian untuk menyisipkan pesan, pesan dijadikan *parity bit* untuk *Huffman code* dan *scale factor*.
- Penyesuaian
  Tentu saja dengan penggantian parity ini harus ada yang disesuaikan, yaitu tahap akhir dari dalam siklus iterasi.
- Penyebaran data dilakukan secara acak yang didasarkan atas SHA-1.

Melihat proses yang begitu mengutamakan keamanan maka penyimpanan pesan menggunakan MP3Stego merupakan pilihan yang tepat. Satu-satunya kemungkinan isi pesan dapat terungkap bila kata rahasia yang digunakan untuk enkripsi dan penyebaran data diketahui.

Sayangnya MP3Stego tidak dapat menampung pesan yang memiliki ukuran besar, karena besarnya ditentukan dari besar *frame* MP3 dimana setiap *frame* hanya dapat menampung 1 bit saja. Selain itu *file* audio yang digunakan sebagai *carrier file* harus memiliki spesifikasi format WAV, 44100Hz, 16 bit, PCM, dan mono.

Diluar spesifikasi tersebut proses penyisipan pesan tidak dapat dilakukan, MP3 hasil kompresi juga mono dimana *file* MP3 tidak wajar dengan format mono yang akan menimbulkan kecurigaan. Tetapi sekali lagi program ini ditujukan unuk menunjukan bahwa steganografi menggunakan MP3 dapat dilakukan.

Penggunaan MP3 Stego

Pengujian ini dilakukan oleh Stefanus Soehono. Proses pengambilan gambar dan pengetesan juga dilakukan oleh Stefanus Soehono. Penulis hanya kembali menjelaskan tentang proses pengujian yang terjadi.

Pertama-tama akan dicoba untuk menyembunyikan pesan singkat yang memiliki nama pesan.txt, yang berisi:

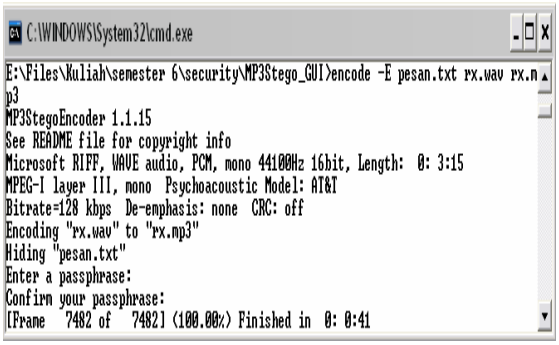
hello world, what's up!
This is testing using mp3stego.=>

Kemudian *file* WAV yang akan digunakan memiliki nama rx.wav yang sesuai dengan spesifikasi di atas.

Lalu dengan dua *file* sudah cukup untuk memulai proses. Jalannya proses ini dilakukan dalam lingkungan command di WindowXP, kedua *file* harus berada dalam direktori yang sama dengan program. Selanjutnya sesuai dengan manual, akan dnjalankan proses dengan hasil rx.mp3, dengan perintah seperti berikut:

encode -E pesan.txt rx.wav rx.mp3

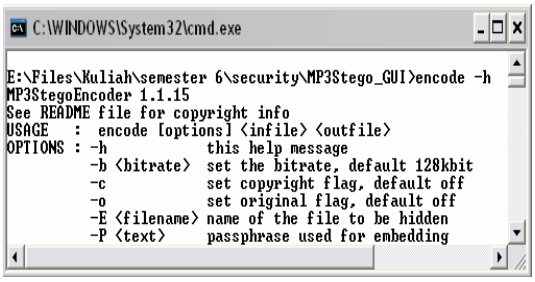
Setelah itu akan diminta sebuah kata rahasia yang akan digunakan dalam proses enkripsi dan penyebaran pesan, dan juga diminta untuk mengulangi mengetik kata tersebut lagi. Terakhir proses kompresi dan penyisipan dilakukan. Berikut adalah ilustrasinya:



Gambar 1. proses encoding

Kata rahasia yang digunakan adalah: stefanus.

Untuk proses encoding terdapat beberapa pilihan yang dapat digunakan sebagai berikut:

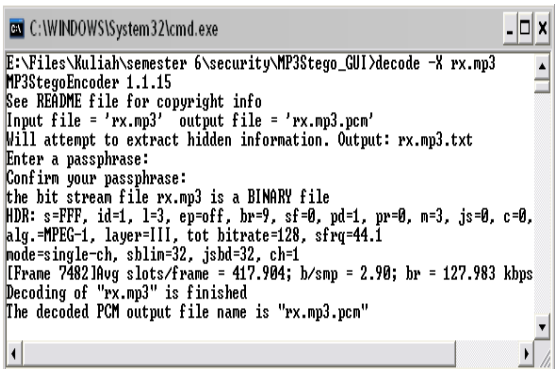


Gambar 2. pilihan dalam encoding

Selanjutnya dari *file* rx.mp3 akan dicoba untuk mengambil pesan yang telah disembunyikan sebelumnya. Perintah yang digunakan adalah:

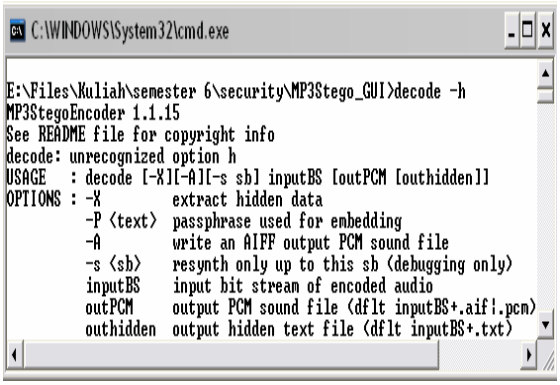
decode -X rx.mp3

Kemudian akan ditanyakan kata rahasia yang digunakan pada saat kompresi dahulu, dan akan diminta untuk konfirmasi lagi. Setelah itu pesan akan ditampilkan dalam *file* rx.mp3.txt sebelumnya akan dihasilkan *file* dalam format PCM terlebih dahulu.



Gambar 3. proses decoding

Sama seperti proses encoding, pada proses decoding ini juga disediakan beberapa pilihan, sebagai berikut:



Gambar 4. pilihan dalam decoding

Kemudian pada *file* rx.mp3 memiliki isi sebagai berikut:

hello world, what's up!
This is testing using mp3stego.=>

Hasil dari *file* ini sama dengan pesan yang disisipkan tadi. Sehingga secara keseluruhan program dapat berjalan dengan baik dan proses berjalan dengan baik

Pengujian Ketahanan

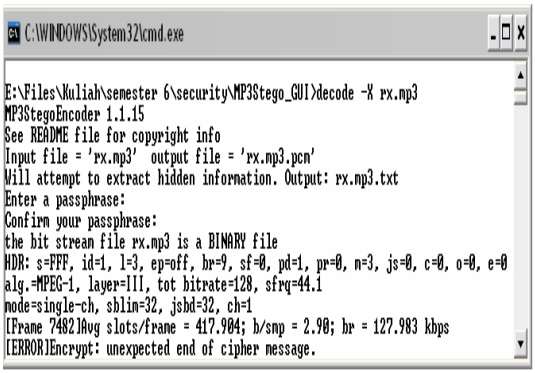
Proses uji file hasil :
Sekarang untuk menguji ketahanannya, saya mencoba untuk memotong *file* MP3 hasil kompresi selama 20 detik. Kemudian saya mencoba untuk mendengarkan *file* yang sudah dipotong tersebut dengan menggunakan Winamp.

Hasil pengujian :
Ternyata hasil keluaran suara sangat jelek, dan waktu yang seharusnya 20 detik berkurang menjadi 5 detik.

Hipotesa :
Tampaknya *file* yang telah mengalami kompresi dengan disisipi pesan menggunakan MP3Stego tidak dapat diperlakukan seperti *file* MP3 biasanya.

Pengujian lanjutan :

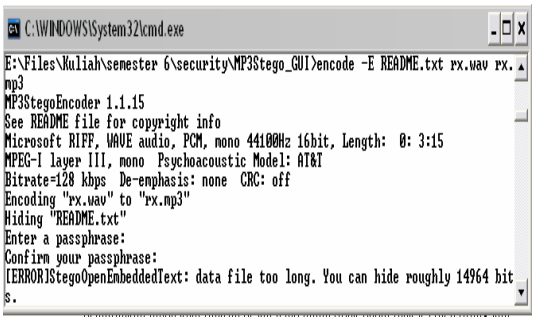
- Melakukan proses decoding lanjutan dari file hasil tadi dan hasilnya adalah pesan *error* dari program tersebut.
- Mencoba untuk menggunakan kata rahasia yang salah. Ternyata proses ekstraksi data tetap dilakukan, namun pada akhirnya muncul pesan *error* oleh program tersebut.



Gambar 5. pesan *error* dari program

Jadi proses enkripsi dilakukan dengan menggunakan kata rahasia palsu tersebut, namun hasil yang dihasilkan salah sehingga muncul pesan *error* dari program. Dapat disimpulkan tanpa kata rahasia pesan tetap aman tidak dapat diakses oleh orang lain.

Setelah itu untuk mengetahui seberapa besar dari kapasitas pesan yang dapat disisipkan, percobaan juga dilakukan untuk menggunakan *file* dengan ukuran 4 kbytes yaitu *file* readme.txt dari program. Saya menggunakan cara yang sama seperti sebelumnya untuk encoding dan hasilnya seperti ilustrasi di bawah ini:



Gambar 6. tampilan bila ukuran pesan terlalu besar

Pada tampilan dapat dilihat ukuran maksimum data 14964 bits, angka ini didapatkan dari jumlah frame (7482 frame) yang dikalikan dengan dua. *File* input WAV memiliki format 16 bit setiap sample sama dengan 2 byte untuk setiap sample. Dengan ini satu frame mampu menampung 2 bit data pesan.

Kemudian dicoba untuk mengetahui besarnya *file* mp3 dengan data yang disisipkan berbeda ukuran. Ternyata pada hasil akhirnya besar dari *file* mp3 tetap sama, walaupun ukuran pesan

yang disisipkan memiliki selisih yang cukup besar. Dengan ini berarti dalam proses kompresi memang disediakan tempat sebanyak dua kali jumlah frame untuk alokasi pesan rahasia. Maka dari itu dengan ukuran pesan yang berbeda dapat menghasilkan ukuran *file* mp3 yang sama.

Prospek Pengembangan MP3 Stego

Ada banyak hal yang sebenarnya masih bisa dikembangkan dalam MP3 stego. Hal ini sangat terbukti dan bisa terlihat dari proses pengujian yang dilakukan sebelumnya.

Dari segi tampilan, MP3stego masih membutuhkan banyak sekali pengembangan. Hal ini bisa terlihat dari aplikasi MP3 stego yang harus dilakukan dengan fasilitas command propmpt ataupun console di UNIX. Sebenarnya proses pengembangan tampilan sangat mempengaruhi kemapanan dari suatu perangkat lunak.

Dari segi sistem teknik steganografi yang dilakukan, ternyata masih banyak kebolongan yang sangat nyata dan tidak bisa ditutupi. Hal ini bisa terlihat dari pengujian ketahanan. Seharusnya file mp3 yang telah berhasil diproses dapat tetap memiliki fungsi layaknya file mp3 yang lainnya. Hal ini menjadi sangat penting karena bisa memicu kecurigaan pada satu file MP3 hasil enkripsi yang tidak bisa didengarkan dan diberikan pada orang yang dituju.

Ternyata pada proses pengkompresian pun, MP3 stego masih memiliki banyak celah karena adanya kesamaan besar data dari dua buah file yang disispkan pesan yang berbeda. Seharusnya file yang dihasilkan berbeda-beda. Hal seperti jugabisa menimbulkan kecurigaan yang mendalam, karena jarang sekali ada file MP3 yang memiliki besar yang sama. Dengan kebolongan ini bisa dibilang proses psikologis yang membuat steganografi pada MP3 dianggap baik belum bisa ditunjukkan secara nyata.

Kesimpulan

Teknik steganografi jika dibandingkan dengan kriptografi memiliki beberapa keunggulan yaitu dengan steganografi keberadaan dari informasi yang ingin disembunyikan tidak dapat dideteksi dengan mudah, dengan menggunakan teknik steganografi, informasi rahasia disembunyikan sedemikian rupa sehingga menghilangkan kecurigaan. Sedangkan untuk kriptografi keberadaan dari informasi yang disembunyikan dengan jelas diketahui dan kita hanya diberi keleluasaan untuk mengkodekan fakta yang ada menjadi fakta lain.

Seiring dengan berkembangnya teknologi, maka semakin meluas juga teknologi digital. Karena teknologi dijital yang merambah e semua hal maka steganografi pun mulai diterapkan pada *file-file* digital yang dikenal dengan sebutan *digital watermarking*. Penerapannya pada *file-file* gambar, audio, dan juga video. Biasanya *digital watermarking* mengeksploitasi kelemahan indera manusia baik pendengaran maupun penglihatan. Teknik yang paling awam digunakan adalah penggantian LSB (Least significant bit) dari suatu rangkaian data dengan informasi yang hendak disisipkan. Namun ukuran informasi yang dapat disisipkan tergantung dari besar *carrier file*.

Dalam praktiknya, teknik steganografi dalam *file* multimedia dapat juga diterapkan dalam proses kompresi data. Dengan menggunakan format kompresi yang bersifat *loosy* (menghilangkan), data-data *redundant* yang seharusnya dihilangkan beberapa dapat diganti dengan informasi yang ingin disisipkan atau fakta yang ingin disembunyikan. Biasanya dalam proses kuantisasi data proses penyisispan informasi tersebut terjadi.

Penggunaan MP3Stego sebagai alat steganografi ternyata memiliki hasil yang cukup baik. Hal ini membuktikan bahwa audio steganografi dapat dilakukan Dengan adanya pengamanan enkripsi data menggunakan 3DES dan juga penyebaran data yang dilakukan secara acak mnggunakan prinsip SHA-1 yang mana keduanya telah diuji ketangguhannya. Pesan yang disimpan akan aman tidak dapat diakses oleh orang yang tidak memiliki kata rahasia yang dipakai. *File* mp3 dari hasil kompresi tidak dapat diperlakukan sama seperti *file* mp3 biasanya, seperti dipotong (Ini adalah kekurangan yang cukup berdampak). Selain itu *error handling* dari program ini memadai sehingga program ini dapat digunakan dengan keamanan yang terjamin.

Teknik steganografi yang baik memiliki prinsip bahwa informasi tersebut dapat diakses oleh orang lain (seperti tidak terjadi apa-apa pada file tersebut), sehingga dengan asumsi tersebut kerahasiaan dari informasi tersebut akan dijaga contohnya menggunakan enkripsi. Teknik steganalysis hanya dapat mengetahui keberadaan

steganografi saja dan belum dapat mengetahui isi dari informasi yang dirahasiakan bila digunakan enkripsi data.

Penerapan steganografi menggunakan media MP3 dapat dijadikan alternatif media menyampaikan pesan rahasia.

- Pertama karena sifat dari steganografi yang sulit dideteksi keberadaannya.
- Kedua karena sifat dari MP3 yang *ubiquitos* sehingga memungkinkan proses transfer tidak menimbulkan kecurigaan.

Dengan kedua kelebihan tersebut maka steganografi MP3 merupakan alat yang baik untuk menyembunyikan pesan dan masih sangat terbuka lebar jalan untuk mengembangkan teknik-teknik atau algoritma steganografi yang harusnya bisa semakin baik lagi, baik jika ditinjau dari sisi efisiensi dan keamanan, serta psikologis kecurigaan.

DAFTAR PUSTAKA

Petitcolas, Fabien A. P. “mp3stego” URL: http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego

Noto, Mark. “MP3Stego : Hiding text in MP3 Files” URL: http://www.securitydocs.com/library/2159

James C. Judge. ”Steganography : Past, Present, Future” URL: http://www.securitydocs.com/library/2157

Mangarae, Aelphaeis. “Steganography FAQ” URL: http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangrae.pdf

Wikipedia.”MP3” URL: http://en.wikipedia.org/wiki/Mp3

Wikipedia.”Steganography” URL: http://en.wikipedia.org/wiki/Steganography

Westphal, Khristy.”Steganography Revealed” URL: http://www.securityfocus.com/infocus/1684.htm

Marvel, Lisa M. “Image Steganography For Hidden Communication” URL : http://www.eecis.udel.edu/~marvel/marvel_th.ps

Andino. “Pengantar Steganografi” URL : http://www.ilmukomputer.com

Sellars, Duncan, An Introduction to Steganography, URL : http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html

Sukmawan, Budi, Steganografi, URL : http://students.ukdw.ac.id/~22033120/steganografi.html