Steganografi File Audio Mp3 menggunakan Mp3Stego

Herny Februariyanti dan Setyawan Wibisono
Program Studi Teknik Informatika
Fakultas Teknologi Informasi, Universitas Stikubank
email : herny@unisbank.ac.id, sonny_setya@yahoo.com

Abstrak

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi sangat kontras dengan kriptografi. Jika kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, maka steganografi menutupi keberadaan pesan. Pesan rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti aslinya. 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 program atau pesan lain.

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.

Kompresi yang biasa dilakukan oleh mp3, tidak mempertahankan bentuk asli dari sinyal input. Melainkan yang dilakukan adalah menghilangkan suara-suara yang keberadaannya kurang/tidak signifikan bagi sistem pendengaran manusia.

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.

Kata kunci : Steganografi, MPEG, audio, MP3Stego

PENDAHULUAN

Teknik menjaga kerahasiaan pesan tidak hanya dengan menggunakan kriptografi. Ada teknik lain yang sudah digunakan sejak berabad – abad lalu, yaitu steganografi (steganography). Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi berasal dari Bahasa Yunani, yaitu "steganos" yang artinya tulisan tersembunyi (*covered writing*). Steganografi sangat kontras dengan kriptografi. Jika kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, maka steganografi menutupi keberadaan pesan.

Steganografi dapat dipandang sebagai kelanjutan kriptografi dan dalam prakteknya pesan rahasia dienkripsi terlebih dahulu, kemudian cipherteks disembunyikan di dalam media lain, sehingga pihak ketiga tidak menyadari keberadaannya. Pesan rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti aslinya. Steganografi membutuhkan dua properti yaitu media penampung dan pesan rahasia. Meda penampung yang umum digunakan adalah gambar, suara, video atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode program atau pesan lain.

Keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media

penampung yaitu membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Ini berbeda dengan kriptografi di mana cipherteks menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia.

Satu hal esensial yang menjadi kelebihan steganografi adalah kemampuannya untuk menipu persepsi manusia, manusia tidak memiliki insting untuk mencurigai adanya arsip-arsip yang memiliki informasi yang tersembunyi didalamnya, terutama bila arsip tersebut tampak seperti arsip normal lainnya. Namun begitu terbentuk pula suatu teknik yang dikenal dengan steganalysis, yaitu suatu teknik yang digunakan untuk mendeteksi penggunaan steganografi pada suatu arsip.

Seorang steganalyst tidak berusaha untuk melakukan dekripsi terhadap informasi yang tersembunyi dalam suatu arsip, yang dilakukan adalah berusaha untuk menemukannya. Terdapat beberapa cara yang dapat digunakan untuk mendeteksi steganografi seperti melakukan pengamatan terhadap suatu arsip dan membandingkannya dengan salinan arsip yang dianggap belum direkayasa, atau berusaha mendengarkan dan membandingkan perbedaannya dengan arsip lain bila arsip tersebut adalah dalam bentuk audio.

SEJARAH STEGANOGRAFI

Pengamanan dengan menggunakan steganografi membuat seolah-oleh pesan rahasia tidak ada atau tidak nampak. Padahal pesan tersebut ada. Hanya saja tidak disadari bahwa ada pesan tersebut di sana. Contoh steganografi antara lain:

a. Di jaman perang antara Yunani dan Persia, pesan rahasia disembunyikan dengan cara menuliskannya di meja (mebel) yang kemudian dilapisi dengan lilin (*wax*). Ketika diperiksa, pesan tidak nampak. Akan tetapi sesampainya di tujuan pesan tersebut dapat diperoleh kembali dengan mengupas (kerok) lilin yang melapisinya.

b. Pesan rahasia dapat juga dikirimkan dengan mengirim surat pembaca ke sebuah surat kabar. Huruf awal setiap kalimat (atau bisa juga setiap kata) membentuk pesan yang ingin diberikan. Cara lain adalah dengan membuat puisi dimana huruf awal dari setiap baris membentuk kata-kata pesan sesungguhnya.

c. Hal yang sama dapat dilakukan dengan membuat urutan gambar buah dimana pesan tersebut merupakan gabungan dari huruf awal dari nama buah tersebut.

d. Pengarang Dan Brown dalam buku novelnya yang berjudul "The Da Vinci Code" memberikan pesan di sampul bukunya dengan membuat beberapa huruf dalam cetakan tebal (***bold***). Jika disatukan, huruf-huruf yang ditulis dalam cetakan tebal tersebut membuat berita yang dimaksud.

e. Di dunia digital, steganografi muncul dalam bentuk *digital watermark*, yaitu tanda digital yang disisipkan dalam gambar (*digital image*) atau suara. Hak cipta (*copyright*) dari gambar dapat disisipkan dengan menggunakan high-bit dari pixel yang membentuk gambar tersebut. Gambar terlihat tidak berbeda - karena kemampuan (atau lebih tepatnya ketidakmampuan) mata manusia yang tidak dapat membedakan satu bit saja - akan tetapi sebenarnya mengandung pesan-pesan tertentu.

f. Steganografi juga muncul dalam aplikasi digital audio, seperti misalnya untuk melindungi lagu dari pembajakan. Contoh lain adalah menyisipkan informasi sudah berapa kali lagu tersebut didengarkan. Setelah sekian kali didengarkan, maka pengguna harus membayar sewa lagu. (Meskipun pendekatan ini masih bermasalah.)

g. Selama Perang Dunia II, agen – agen spionase juga menggunakan steganografi untuk mengirim pesan. Caranya dengan menggunakan titk – titik yang sangat kecil, sehingga keberadaannya tidak dapat dibedakan pada tulisan biasa yang diketik.

Saat ini steganografi sudah banyak diimplementasikan pada media digital. Steganografi digital menggunakan media digital sebagai penampung, seperti citra digital, video digital, atau audio. Informasi yang disembunyikan juga berbentuk digital seperti teks, citra, data audio, atau data video. Steganografi digital dapat dipakai di negara – negara yang menerapkan sensor ketat terhadap

informasi atau di negera di mana enkripsi pesan terlarang. Pada negara – negera seperti itu informasi rahasia dapat disembunyikan dengan menggunakan steganografi.

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.

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 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.

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:

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

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 menggunakan model dari sistem pendengaran manusia dan menentukan bagian yang terdengar bagi sistem pendengaran manusia. Setelah itu sinyal input yang memiliki domain waktu dibagi menjadi blok-blok dan ditransformasi menjadi domain frekuensi. 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 konvolusi dua sinyal yaitu sinyal input dan sinyal model sistem pendengaran manusia. 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:

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

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.

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 atau tidak signifikan bagi sistem pendengaran manusia. Proses yang dilakukan adalah :

1. Tahap 1: menggunakan model dari sistem pendengaran manusia dan menentukan bagian yang terdengar bagi sistem pendengaran manusia.
2. Tahap 2 : Setelah itu sinyal input yang memiliki domain waktu dibagi menjadi blok-blok dan ditransformasi menjadi domain frekuensi.
3. Tahap 3 : Kemudian model dari sistem pendengaran manusia d ibandingkan 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.
4. 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.

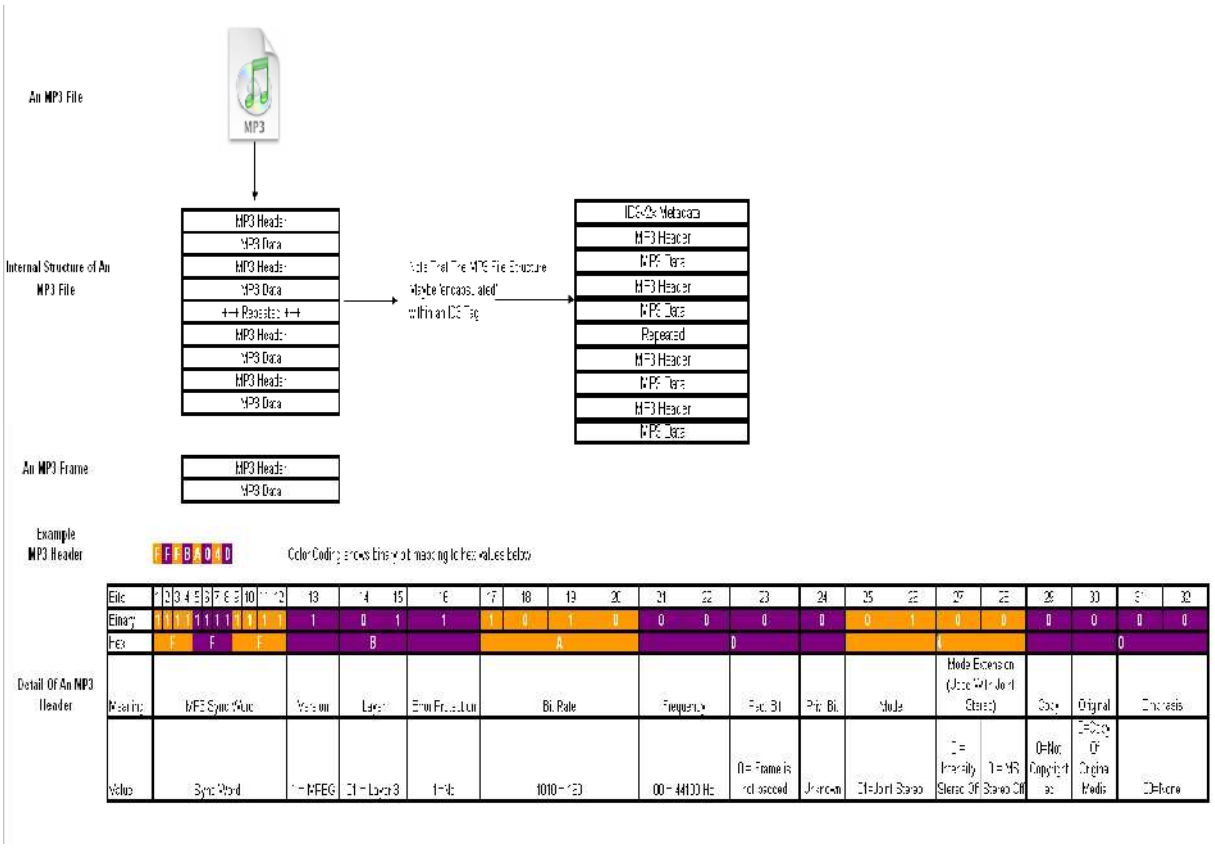
Proses pengkompresian mp3 dapat menghasilkan keluaran yang hampir setara dengan aslinya disebabkan oleh kelemahan dari sistem pendengaran manusia yang dapat dieksploitasi. Berikut adalah beberapa kelemahan dari sistem pendengaran manusia yang digunakan dalam pemodelan:

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

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 dan 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.



Gambar 1. Format File MP3

Penggunaan MP3 sekarang menjadi sangat tinggi karena pada dasarnya seorang manusia akan lebih suka melakukan hal yang bisa lebih menghibur dibandingkan hal yang 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 tidak membicarakan 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"

AUDIO STEGANOGRAFI MENGGUNAKAN FILE AUDIO 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:

1. Penggantian LSB. Cara ini lazim 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 disisipkan relatif besar, namun berdampak pada hasil audio yang berkualitas kurang dengan banyaknya *noise*.
2. 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 dikompensasikan dengan kerumitan dalam realisasinya.
3. 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 memiliki akses terhadap data tersebut atau dapat merekonstruksi sinyal random yang digunakan untuk menyebarkan pesan pada range frekuensi.
4. 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 amplitude 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.

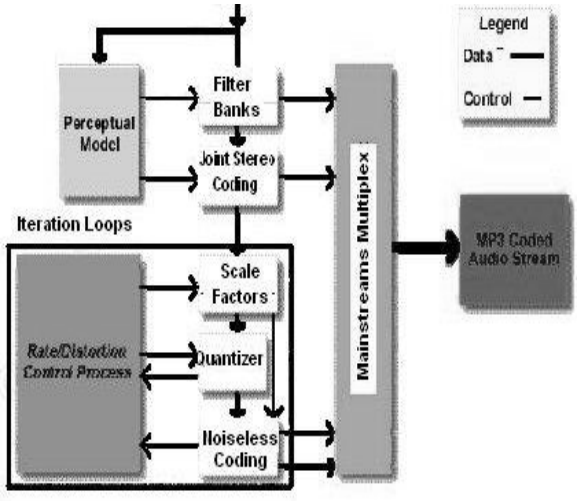
Keempat metode di atas memiliki kesamaan yaitu menggunakan kelemahan dari sistem pendengaran manusia. Maka dari itu teknik steganografi dalam MP3 juga akan menggunakan kelemahan ini untuk menyembunyikan pesan.

MP3Stego dapat digunakan untuk steganografi audio. Program ini dibuat oleh Fabien Petitcolas dengan bahasa C. Program dapat didownload di internet dengan alamat http://www.petitcolas.net/fabien/steganography/mp3stego/.

Cara kerja dari program ini berdasarkan dari teknik kompresi audio dari WAV ke MP3. 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.

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.

Proses pengkodean dan kompresi MP3 secara umum terbagi menjadi dua siklus iterasi, yaitu di dalam siklus iterasi berupa siklus untuk ratifikasi dan di luar siklus iterasi untuk pengendalian distorsi dan *noise*. Gambar bagan kompresi MP3 seperti di gambar 2:



Gambar 2. Diagram Proses Kompresi MP3

MP3Stego memasukan data pada saat proses kompresi pada proses di dalam siklus

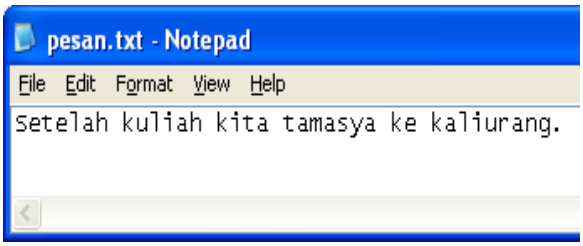
iterasi. Proses penyembunyian pesan secara garis besar adalah pesan dikompresi lalu dienkripsi dan terakhir disembuyikan pada rangkaian bit MP3. Setelah mengalami kompresi, lalu pesan tersebut dienkripsi untuk menjami keamananya. Seperti yang telah dibahas diatas, pesan steganografi dianggap dapat diketahui 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. 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, dan mengumpulkan data-data tersebut hingga mencapai ukuran yang tepat sehingga dapat dikodekan. Sedangkan siklus lainnya memastikan data memenuhi spesifikasi model sistem pendengaran manusia. Kemudian untuk menyisipkan pesan, pesan dijadikan *parity bit* untuk *Huffman code* dan *scale factor*. 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.

Percobaan dilakukan dengan menyisipkan pesan yang ditulis pada file teks "pesan.txt" seperti pada gambar 3. Sedangkan file pembawanya adalah file "svega.wav".



Gambar 3. File pesan

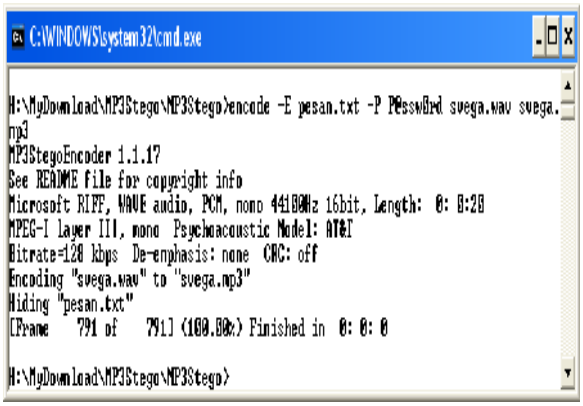
Encode

Untuk menyembunyikan pesan ke dalam file audio dapat dilakukan dengan menuliskan perintah sebagai berikut:

Encode –E pesan.txt –P P@ssw0rd svega.wav svega.mp3

Keterangan:

Kompress pesan.txt dan svega.wav menjadi svega.mp3. Untuk mengenkripsi pesan.txt digunakan password "P@ssw0rd". Proses encode akan tampak seperti pada gambar 4.



Gambar 4. Proses Encode

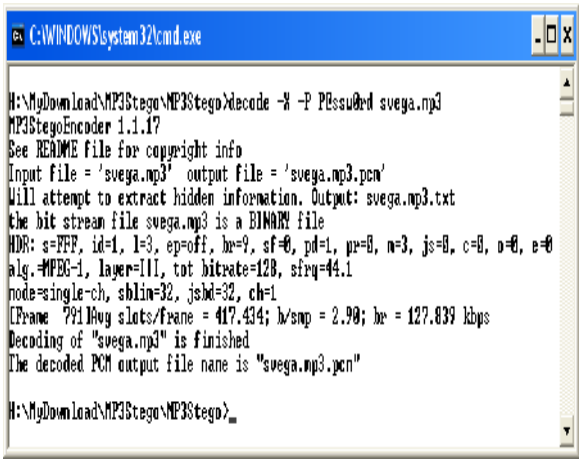
Decode

Untuk membuka pesan dari file audio dapat dilakukan dengan menuliskan perintah sebagai berikut:

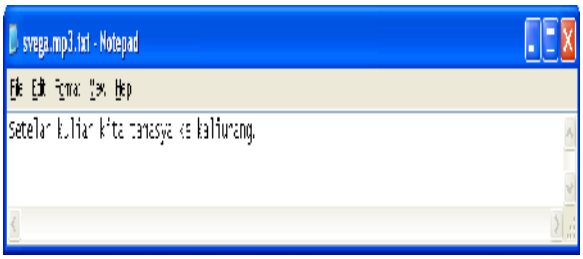
Decode –X –P P@ssw0rd svega.mp3

Keterangan:

Decode file svega.mp3 dengan password "P@ssw0rd". Hasil decode adalah file teks dengan nama svega.mp3.txt. Proses Decode akan tampak seperti pada gambar 5. Sedangkan hasilnya akan tampak seperti gambar 6.



Gambar 5. Proses Decode



Gambar 6. Hasil Decode

KESIMPULAN & SARAN

Teknik steganografi dibandingkan dengan kriptografi memiliki keunggulan yaitu dengan steganografi keberadaan dari informasi yang disembunyikan tidak dapat dideteksi dengan mudah, dengan steganografi informasi disembunyikan sedemikian rupa sehingga menghilangkan kecurigaan. Sedangkan untuk kriptografi keberadaan dari informasi yang disembunyikan dengan jelas diketahui.

Dengan meluasnya teknologi digital, 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*.

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. 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. 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, sehingga dengan asumsi tersebut kerahasiaan dari imformasi 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.

Pengguanaan steganografi pada MP3 dapat dijadikan alternatif media menyampaikan pesan rahasia. Pertama karena sifat dari steganografi yang sulit dideteksi keberadaannya. Lalu 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.

DAFTAR PUSTAKA

Petitcolas, F., 2008, *mp3stego*, http://www.cl.cam.ac.uk/~fapp2/steganography/mp3stego, 24 Maret 2009.

Rahardjo, B., 2005, *Keamanan Sistem Informasi Berbasis Internet Versi 5.4*, PT Insan Infonesia, Bandung dan PT INDOCISC, Jakarta.

Batara, S., 2007, *Studi Steganografi dalam File MP3*, http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Makalah1/Makalah1-054.pdf, 21 Maret 2009.

Arubusman, YR., 2007, *Audio Steganografi*, http://iwayan.info/FileMahasiswa/SkirpsiYus_AudioSteganografi_2007.pdf, 21 Maret 2009.

Soehono, S., 2006, *Audio Steganografi Menggunakan mp3*, http://budi.insan.co.id/courses/security/2006/StefanusSoehono_report.doc, 24 Maret 2009.