KARYA ILMIAH

SISTEM KEAMANAN JARINGAN KOMPUTER

Penyembunyian (Steganografi) Pesan Menggunakan Image dan MP3

Oleh:

Meka Lestari 08053111053

Dosen Pembimbing: Deris Stiawan M.Kom

JURUSAN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2008

BAB. I PENDAHULUAN

a. Latar Belakang

Tidak semua informasi boleh diakses oleh setiap orang. Informasi merupakan sesuatu yang sangat berharga apabila informasi tersebut menyangkut tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Informasi yang terbatas pengaksesanya perlu dijaga keaslian, ketersediaan dan kerahasianya pada saat informasi tersebut akan dikirim kepihak yang berhak. Terdapat berbagai jenis teknik pengamanan informasi diantaranya dengan teknik "Steganografi".

Steganografi berasalah dari bahasa Yunani yaitu *steganos* yang artinya "*terselubung atau tersembunyi*" dan graphein yang artinya "menulis" sehingga steganografi artinya adalah "menulis (tulisan) terselubung". Teknik steganografi sudah dipakai lebih dari 2500 tahun. Steganografi adalah ilmu dan seni menyembunyikan (*embedded*) informasi dengan cara menyisipkan pesan di dalam pesan lain. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Disamping itu steganografi juga dapat digunakan untuk melakukan autentikasi terhadap suatu hasil karya sebagaimana pemanfaatan watermarking.

Steganografi terbagi menjadi beberapa zaman, yaitu ancient, renaissance, dan modern.

1. Ancient steganografi

   Ancient steganografi telah dikenal sejak zaman Herodotus (485-582 SM). Kemudian Pliny *the Elder* dengan *invisible ink* –nya.
2. Renaissance steganografi Renaissance

   steganografi dimulai sejak tahun 1518 oleh Johannes Trithemius yang menemukan cipher steganografi pada setiap huruf yang merepresentasikan sebuah kata. Tokoh lainnya yaitu Giovanni Battista Porta (1535-1615) yang menggunakan kulit telur sebagai *cover object* dan pesan yang ditulis dapat dibaca setelah kulit telur dilepaskan.
3. Modern steganografi Modern

   steganografi oleh Simmons pada tahun 1983 di USA.

Beberapa contoh penggunaan steganografi pada masa lampau yaitu :

- Pada tahun 480 sebelum masehi, seseorang berkebangsaan Yunani yaitu Demaratus mengirimkan pesan kepada polis Sparta yang berisi peringatan mengenai penyerangan Xerxes yang ditunda. Teknik yang digunakan adalah dengan menggunakan meja yang telah diukir kemudian diberi lapisan lilin untuk menutupi pesan tersebut, dengan begitu pesan dalam meja dapat disampaikan tanpa menimbulakn kecurigaan oleh para penjaga.
- Penggunaan tinta yang tidak terlihat pada pesan lainnya.

Untuk menyisipkan pesan yang akan dikirim digunakan beberapa tipe media. Tipe media ini nanti yang akan digunakan sebagai media pembawa pesan rahasia diantaranya file audio.

Berbeda dengan kriptografi, dimana karakter pesan diubah/diacak menjadi bentuk lain yang tidak bermakna, dalam steganografi pesannya itu sendiri tetap dipertahankan hanya dalam penyampaiannya dikaburkan/disembunyikan dengan berbagai cara. , maka dalam steganografi yang pertama kali harus dilakukan oleh seorang steganalis adalah menemukan stego objek terlebih dahulu, hal ini karena pesan yang dirahasiakan disembunyikan (tidak nampak) dalam medium lain (*cover*).

b. Tujuan Penelitian

Adapun tujuan memilih judul dan membuat karya ilmiah ini adalah untuk menambah pengetahuan tentang teknik yang digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak selain kriptografi.

c. Metode Penelitian

Metode yang digunakan dalam menyelesaikan karya ilmiah ini yaitu dengan cara observasi dari berbagai macam sumber misalnya dari buku-buku dan internet.

BAB. II LANDASAN TEORI

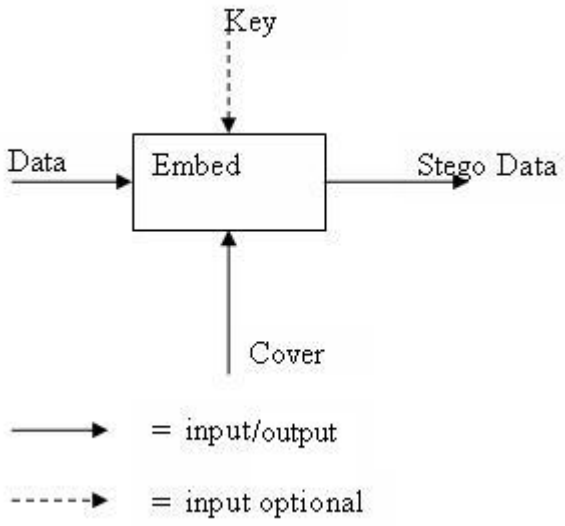
Ada berbagai macam media yang bisa digunakan untuk menyisipkan informasi atau pesan yang akan dikirim. Secara teori, semua file umum yang ada di dalam komputer dapat digunakan sebagai media, seperti file gambar berformat JPG, GIF, BMP, atau di dalam musik MP3, atau bahkan di dalam sebuah film dengan format WAV atau AVI.

Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganography yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas [Waheed, 2000].

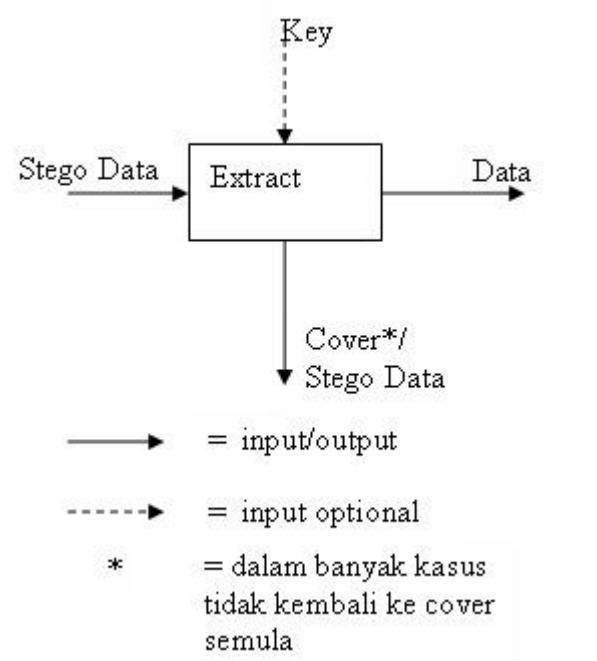
Teknik Steganografi ini telah banyak digunakan dalam strategi peperangan dan pengiriman sandi rahasia sejak jaman dahulu kala. Dalam perang Dunia II, teknik steganography umum digunakan oleh tentara Jerman dalam mengirimkan
pesan rahasia dari atau menuju Jerman [Simmons., 1983].

Sebagai fungsi yang umum, steganography digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi [Johnson, 2006].

Skema penyembunyian data dalam steganografi secara umum adalah sebagai berikut :



- Pada gambar di atas data atau informasi yang ingin disembunyikan disimpan dalam sebuah wadah (*cover*) melalui suatu algoritma steganografi tertentu (misalnya LSB). Untuk menambah tingkat keamanan data, dapat diberikan kunci, agar tidak semua orang mampu mengungkapkan data yang disimpan dalam berkas wadah (*cover*). Hasil akhir dari proses penyimpanan data ini adalah sebuah berkas stego (*stego data/stego file*).
- Sedangkan proses pengungkapan informasi dari berkas stego digambarkan pada gambar berikut :



Berkas stego diekstrak setelah memasukkan kunci yang dibutuhkan. Hasil ekstraksi ini adalah informasi atau data yang disimpan beserta berkas stego. Dalam kebanyakan teknik steganografi, ekstraksi pesan tidak akan mengembalikan berkas stego tepat sama dengan berkas wadah (*cover*) saat pesan disimpan, hal ini karena saat penyimpanan pesan tidak dilakukan pencatatan kondisi awal dari berkas wadah yang digunakan untuk menyimpan pesan. Dengan demikian jika diingikan penghilangan pesan dari berkas stego maka yang dapat dilakukan diantaranya adalah dengan melakukan pengubahan nilai pixel secara acak dari tempat pixel – pixel pesan disimpan dalam berkas.

BAB. III PEMBAHASAN

a. Steganalisis dan Stegosystem

Steganalisis dapat diartikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi. Stegosystem pada intinya berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu sistem steganografi. Terdapat dua jenis penyerang yaitu penyerangan pasif dimana penyerang hanya dapat memotong data dan penyerangan aktif dimana penyerang juga dapat memanipulasi data.

Steganografi tenyata digunakan juga untuk melakukan tindakan criminal. Diduga juga 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.

Ada beberapa istilah dalam steganografi yaitu :

- Carrier file : *file* yang berisi pesan rahasia
- Stego-medium : media yang digunakan untuk membawa pesan rahasia atau menyisipkan pesan rahasia tersebut.
- Redundant bits : sebagian informasi yang terdapat di dalam *file* yang jika dihilangkan tidak akan menimbulakn kerusakan yang signifikan (bagi indera manusia)
- Payload : informasi yang akan disembunyikan

Kata steganografi menjadi sering disebut di masyarakat bersama-sama dengan kata kriptografi setelah pemboman gedung WTC di AS, dimana para pejabat AS mengkalim bahwa para teroris menyembunyikan pesan-pesan kegiatan ternornya dalam berbagai gambar porno, file MP3 dan web site tertentu. Novel Da Vinci Code pun turut mempopulerkan steganografi dan kriptografi

b. Metode Steganografi Audio

Ada beberapa cara untuk mengaplikasikan steganografi pada file audio yaitu :

- Low Bit coding

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 disispkan relative besar, namun berdampak pada hasil audio yang berkualitas kurang dengan banyaknya noise.

- Phase coding

  Metode kedua yang digunakan ini 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.

- Spread Spectrum

  Metode yang ketiga adalah penyebaran spektrum. Dengan metode ini pesan dikodekan dan disebar ke setiap spectrum 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.

- Echo Hiding

  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 antara echo dan sinyal asli.

c. Steganografi dengan Media File Audio

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.

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:

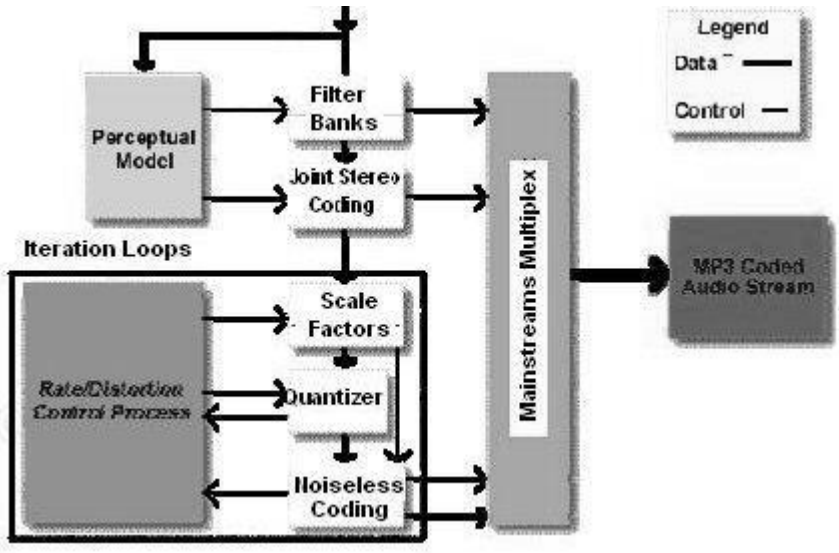
- Layer 1: paling baik pada 384 kbit/s
- Layer 2: paling baik pada 256...384 kbit/s, sangat baik pada 224...256 kbit/, baik pada 192...224 kbit/s
- Layer 3: paling baik pada 224...320 kbit/s, sangat baik pada 192...224 kbit/s, baik pada 128...192 kbit/s

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 pembahasan ini akan digunakan software MP3Stego untuk menyembunyaikan pesan kedalam file MP3. Program ini digunakan hanya untuk membuktikan bahwa steganografi dalam MP3 dapat dilakukan. 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.

Secara umum proses pengkodean dan kompresi MP3 terbagi menjadi dua siklus iterasi yaitu di dalam siklus iterasi berupa siklus untuk ratifikasi dan di luar siklus

iterasi untuk pengendalian distorsi dan *noise*. Berikut ini merupakan gambar bagan kompresi MP3 yaitu :



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.

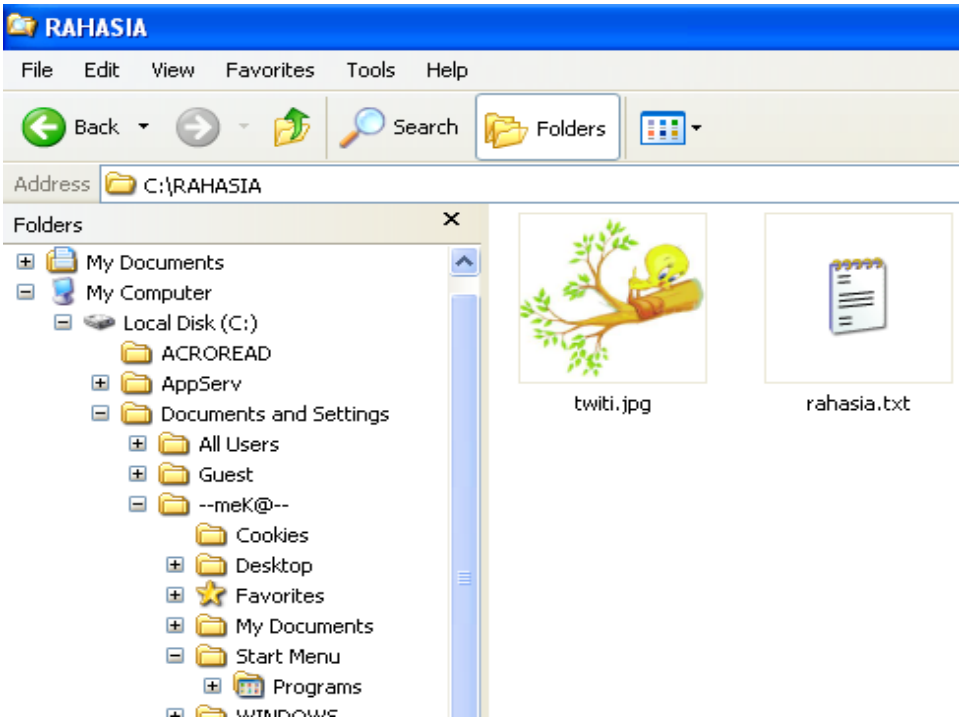
MP3Stego memiliki kelemahan karena software ini hanya merupakan program bebas yang belum disempurnakan. Salah satu kelemahanya yaitu MP3Stego tidak mampu menampung pesan yang memiliki ukuran yang besar karena besarnya ditentukan dari besar frame MP3 dimana setiap frame hanya dapat menampung 1 bit saja. Adapun spesifikasi file yang harus dipenuhi sebagai carrier file yaitu dalam format WAV, 44100Hz, 16 bit, PCM, dan mono. Jika tidak memenuhi spesifikasi tersebut proses penyisipan pesan akan gagal. Dan jika MP3 hasil kompresi tidak dalam bentuk mono maka akan menimbulkan kecurigaan.

c. Percobaan

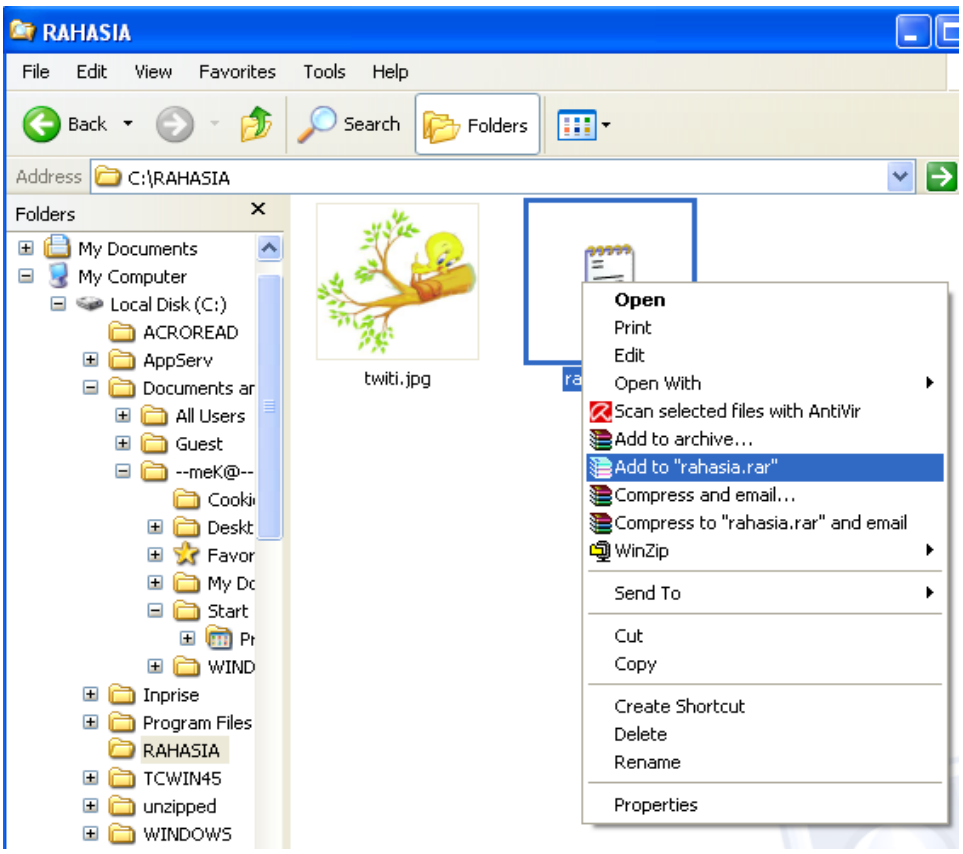
- Menyisipkan File Pribadi Pada File Gambar

  Langkah-langkahnya yaitu :

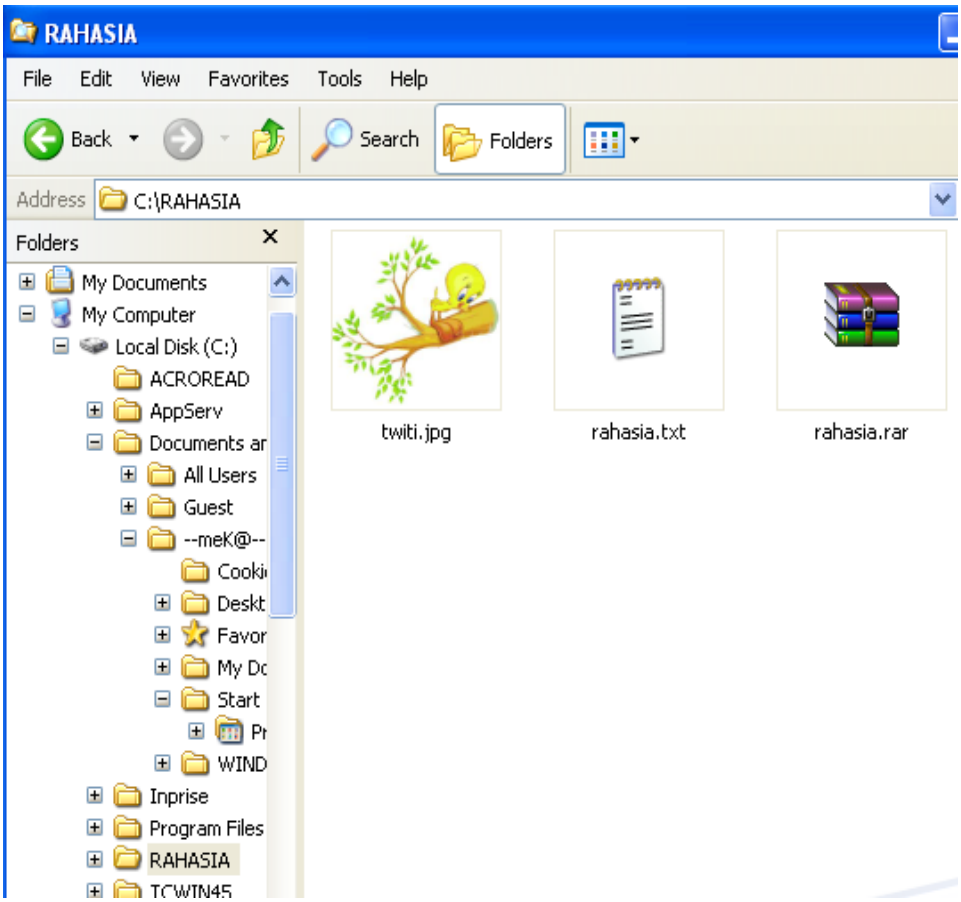
  1) Siapkan file yang akan disisipkan dan file gambar sebagai media untuk menyisipkan file pribadi. Simpan dalam satu folder. File pribadi disimpan dalam format .txt dan file gambar dalam format .jpg.



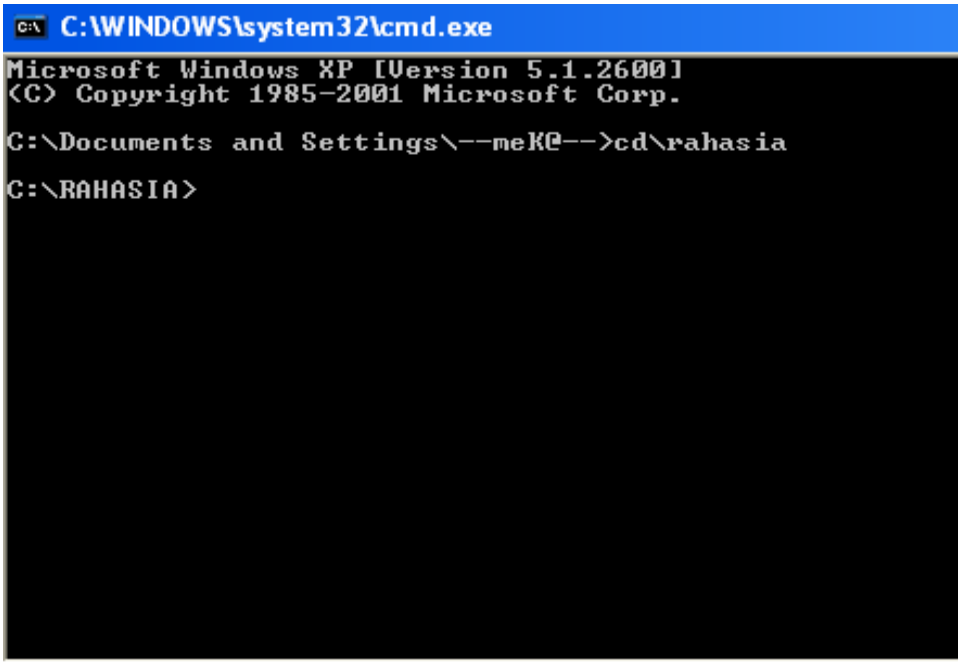
2) Kemudian add file pribadi tersebut pada “new RAR archieve” (pesan.rar).



Jadi terdapat 3 file dalam folde C:\rahasia

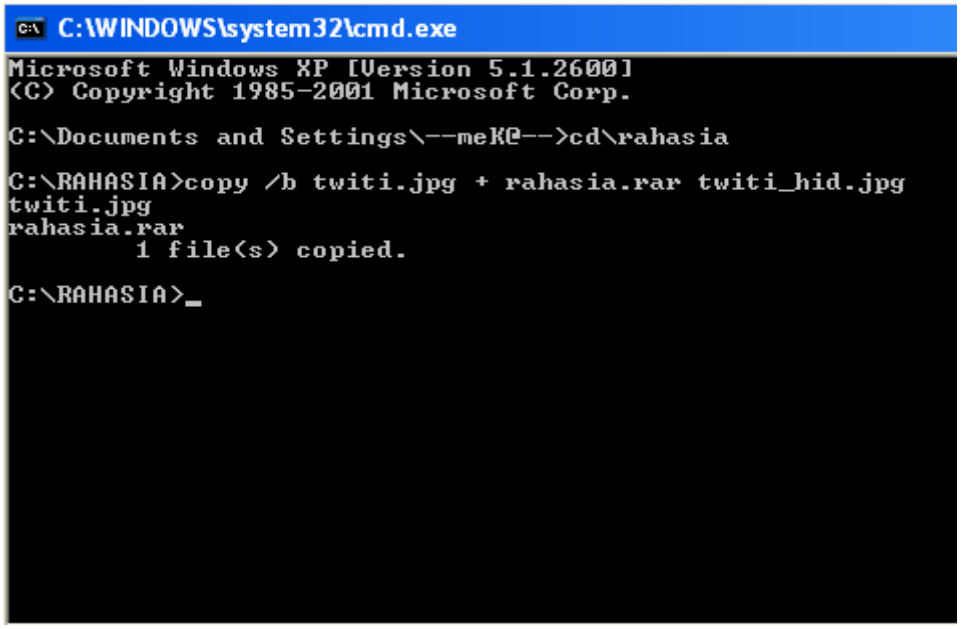


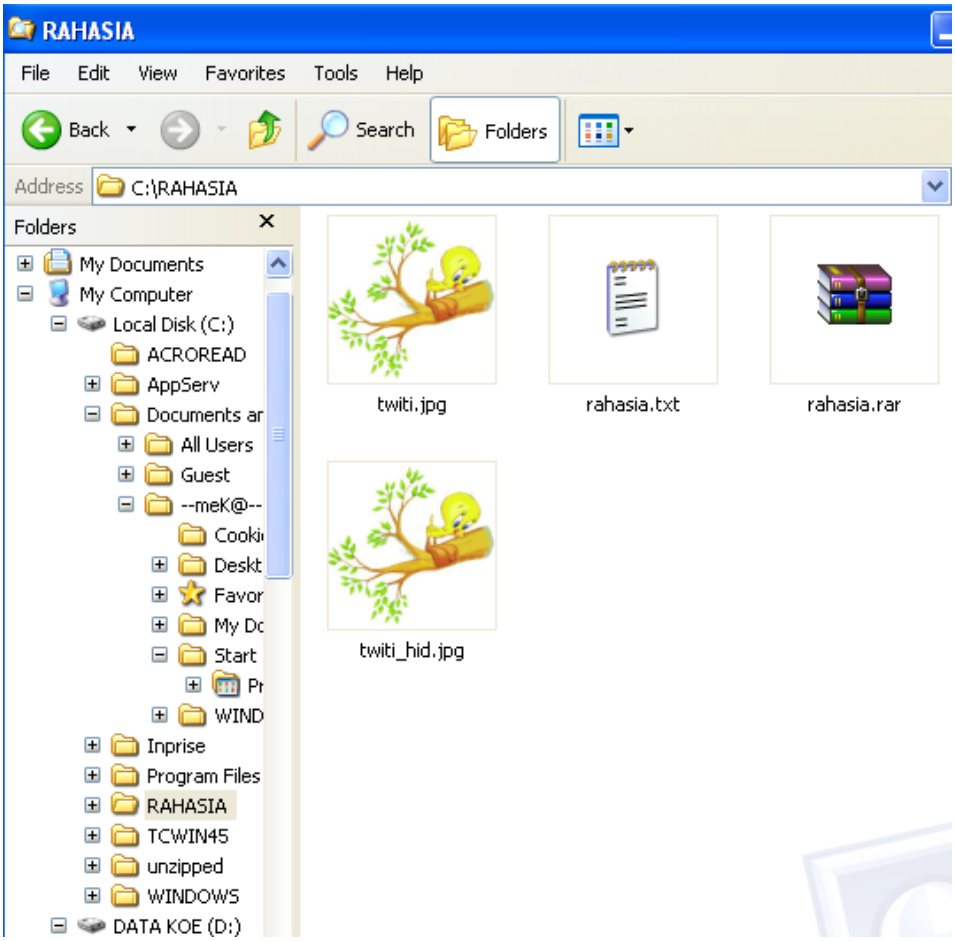
3) Buka “command prompt atau cmd”.
4) Arahkan ke folder C:\rahasia



5) Ketik copy /b twiti.jpg + rahasia.rar twiti_hid.jpg

twiti.jpg adalah file gambar asal, rahasia.rar adalah file yang akan disisipkan sedangkan twiti_hid.jpg adalah file yang mengandung kedua file tersebut.





Maka sekarang file rahasia.rar (file rahasia.txt yang di”rar”kan) telah berhasil di sisipkan pada file twiti_hid.jpg. Saat file twiti_hid.jpg dibuka tidak akan timbul kecurigaan. Seperti gambar di bawah ini :

Jika ingin mendapatkan file rahasia.txt kembali dari gambar di atas maka kita harus melakukan perintah seperti dibawah ini :

```
C:\RAHASIA>copy /b twiti.jpg + rahasia.rar twiti_hid.rar
twiti.jpg
rahasia.rar
        1 file(s) copied.

C:\RAHASIA>
```

Setelah itu akan muncul file twiti_hid.rar. Extract file tersebut kemudian akan muncul file rahasia.txt

- Menyisipkan File Pribadi Pada File MP3

  Langkah-langkahnya yaitu :

  1). Siapkan file pribadi yang akan disisipkan dan file .wav dengan spesifikasi format WAV, 44100Hz, 16 bit, PCM, dan mono jika tidak maka proses penyisipan akan gagal. Disini saya menggunakan file LoopyMusic.wav dan file pribadi secret.txt. Simpan kedua file ke dalam folder yang sama dengan

software MP3Stego (dalam sat direktori). Proses ini akan dilakukan di command promt.

2). Kemudian kita memulai untuk mengencode file LoopyMusic.wav menjadi LoopyMusic.mp3. Ketikan encode -E pesan.txt rx.wav rx.mp3. Kemudian akan muncul pernyataan meminta sebuah kata rahasia yang akan digunakan dalam proses enskripsi dan penyebaran pesan dan juga meminta confirm/mengetik ulang kata rahasia tersebut. Berikut ini merupakan gambar dari proses encodingnya, kata rahasia yang digunakan adalah "meka" :

```
C:\MP3Stego>encode -E secret.txt LoopyMusic.wav LoopyMusic.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length:  0: 0:10
MPEG-I layer III, mono  Psychoacoustic Model: AT&T
Bitrate=128 kbps  De-emphasis: none  CRC: off
Encoding "LoopyMusic.wav" to "LoopyMusic.mp3"
Hiding "secret.txt"
Enter a passphrase:
Confirm your passphrase:
Enter a passphrase:
Confirm your passphrase:
[Frame    408 of    408] (100.00%) Finished in  0: 0:29
```

Terdapat beberapa pilihan dalam proses encoding yaitu :

```
C:\MP3Stego>encode -h secret.txt LoopyMusic.wav LoopyMusic.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
USAGE   :  encode [options] <infile> <outfile>
OPTIONS : -h            this help message
          -b <bitrate>  set the bitrate, default 128kbit
          -c            set copyright flag, default off
          -o            set original flag, default off
          -E <filename> name of the file to be hidden
          -P <text>     passphrase used for embedding
```

3). Kemudian dari file LoopyMusic.mp3 kita akan mencoba mengambil pesan yang disembunyikan sebelumnya. Ketikan decode -X rx.mp3. Lalu program akan menanyakan kata rahasia yang digunakan pada saat proses kompresi sebelumnya. Sama seperti tadi program akan meminta mengetik/confirm kata rahasia tersebut. Kemudian akan dihasilkan file dalam format PCM dan LoopyMusic.mp3.txt. Berikut merupakan gambar proses decoding yaitu :

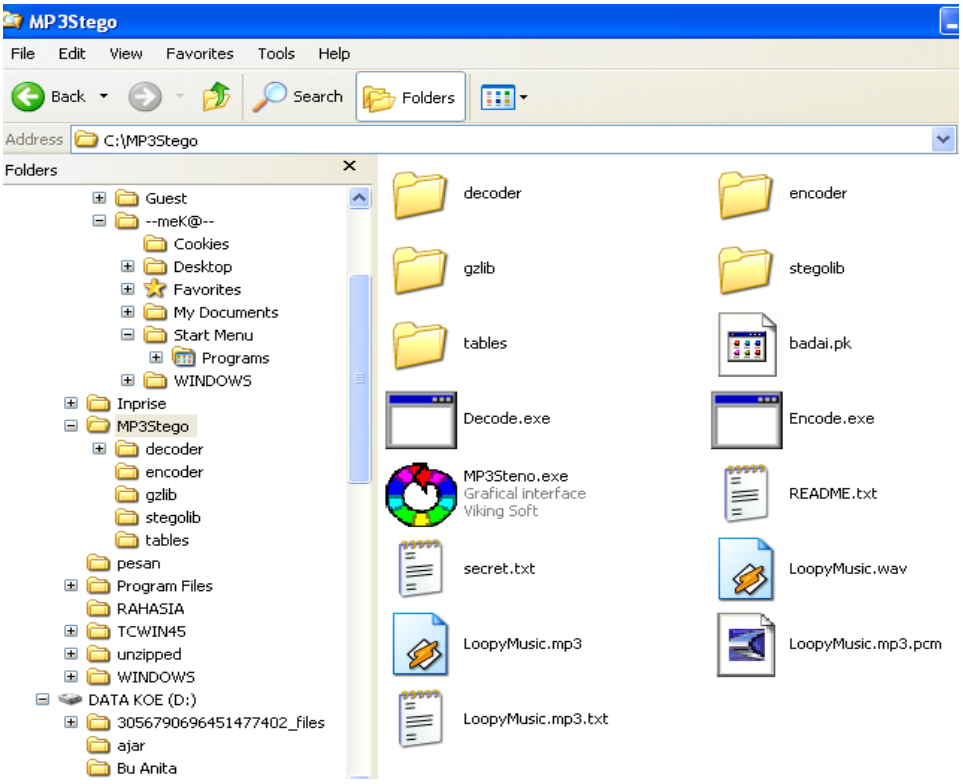
```
C:\MP3Stego>decode -X LoopyMusic.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'LoopyMusic.mp3'  output file = 'LoopyMusic.mp3.pcm'
Will attempt to extract hidden information. Output: LoopyMusic.mp3.txt
Enter a passphrase:
Confirm your passphrase:
the bit stream file LoopyMusic.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame  408]Avg slots/frame = 416.943; b/smp = 2.90; br = 127.689 kbps
Decoding of "LoopyMusic.mp3" is finished
The decoded PCM output file name is "LoopyMusic.mp3.pcm"
```

Sama seperti proses encoding, pada proses decoding terdapat berbagai macam pilihan yaitu :

```
C:\MP3Stego>decode -h
MP3StegoEncoder 1.1.15
See README file for copyright info
decode: unrecognized option h
USAGE   : decode [-X][-A][-s sb] inputBS [outPCM [outhidden]]
OPTIONS : -X          extract hidden data
          -P <text>   passphrase used for embedding
          -A          write an AIFF output PCM sound file
          -s <sb>     resynth only up to this sb (debugging only)
          inputBS     input bit stream of encoded audio
          outPCM      output PCM sound file (dflt inputBS+.aif!.pcm)
          outhidden   output hidden text file (dflt inputBS+.txt)

C:\MP3Stego>=
```

File-file yang ada dalam MP3Stego yaitu :



Kemudia pada file LoopyMusic.mp3.txt memiliki isi sebagai berikut :

Menggunakan MP3. Tampak jelas bahwa file yang dihasilkan sama dengan

file yang disispkan tadi.

Apabila pada proses decoding kita memasukan kata rahasia yang salah maka proses eksekusi tetap dilakukan tetapi pada akhirnya akan muncul pesan error oleh program tersebut, seperti gambar dibawah ini :

```
C:\MP3Stego>decode -X LoopyMusic.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Input file = 'LoopyMusic.mp3'  output file = 'LoopyMusic.mp3.pcm'
Will attempt to extract hidden information. Output: LoopyMusic.mp3.txt
Enter a passphrase:
Confirm your passphrase:
the bit stream file LoopyMusic.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=3, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=single-ch, sblim=32, jsbd=32, ch=1
[Frame  408]Avg slots/frame = 416.943; b/smp = 2.90; br = 127.689 kbps
[ERROR]Encrypt: unexpected end of cipher message.

C:\MP3Stego>_
```

Kemudia saya akan mencoba menyisipkan file yang lebih besar yaitu file readme.txt yang terdapat pada program itu. Maka hasil yang didapatkan sabagai berikut :

```
C:\MP3Stego>encode -E README.txt LoopyMusic.wav LoopyMusic.mp3
MP3StegoEncoder 1.1.15
See README file for copyright info
Microsoft RIFF, WAVE audio, PCM, mono 44100Hz 16bit, Length:  0: 0:10
MPEG-I layer III, mono  Psychoacoustic Model: AT&T
Bitrate=128 kbps  De-emphasis: none  CRC: off
Encoding "LoopyMusic.wav" to "LoopyMusic.mp3"
Hiding "README.txt"
Enter a passphrase:
Confirm your passphrase:
[ERROR]StegoOpenEmbeddedText: data file too long. You can hide roughly 816 bits.

C:\MP3Stego>_
```

BAB. IV KESIMPULAN

Dari uraian di atas dapat ditarik berberapa kesimpulan yaitu :

1. Steganografi merupakan metode untuk menyembunyikan pesan di dalam sebuah pesan baik yang berupa image, suara, dan file-file yang mengandung teks tanpa menunjukan cirri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula sehingga orang lain tidak menyadari bahwa ada sesuatu didalam pesan tersebut.
2. Keunggulan teknik steganografi dibandingkan dengan teknik kriptografi yaitu dengan steganografi keberadaan pesan yang disembunyikan tidak dapat dideteksi dengan mudah karena pesan disembunyikan sedemikian rupa sehingga tidak akan menimbulkan kecurigaan. Sedangkan untuk kriptografi keberadaan dari informasi yang disembunyikan dengan jelas diketahui.
3. File yang telah mengalami kompresi dengan dengan disisipi pesan menggunakan MP3Stegos tidak dapat diberlakukan layaknya seperti file MP3. Jika file tersebut dipotong maka akan menghasilkan suara yang jelek.
4. Jika proses enkripsi menggunakan kata rahasia yang palsu akam menghasilkan pesan error dari program. Jadi tanpa kata rahasia pesan tetap aman tidak dapat diakses oleh pihak lain.
5. File yang akan disisipkan tidak boleh terlalu panjang, maksimum data 14964 bits. Jika melebihi batas maksimum maka proses encoding akan error.
6. 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.

Karena masih terbatasnya kemampuan yang dimiliki oleh penyusun sehingga masih terdapat banyak kekurangan pada karya ilmiah ini maka saya mengaharapkan saran dan

kritik bagi para pembaca. Karya imiah ini dapat dikembangkan lagi karena masih ada beberapa hal yang masih bisa diperdalam bagi yang ingin mengembangkanya.

DAFTAR PUSTAKA

www.informatika.org

www.ilmukomputer.com

www.indoskripsi.com