# Studi Mengenai Echo Hiding Steganografi

Dini Lestari Tresnani (13508096)
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*if18096@students.if.itb.ac.id*

***Abstrak*—Steganografi adalah seni atau ilmu untuk menyembunyikan pesan rahasia. Steganografi modern ini dapat diterapkan pada berbagai media digital, salah satunya pada media digital audio. Salah satu teknik untuk menyembunyikan pesan dalam media digital audio adalah Echo Hiding Steganografi.**

**Makalah ini berisi tentang studi khusus mengenai salah satu teknik steganografi pada file audio khususnya MP3 dan WAV dengan menggunakan teknik Echo Hiding Steganografi.**

***Kata Kunci*—steganografi, audio, echo hiding.**

## I. DASAR TEORI

### *A. Steganografi*

Steganografi adalah seni atau ilmu menyembunyikan pesan rahasia agar tidak diketahui oleh orang lain. Steganografi berasal dari bahasa Yunani yaitu *steganos* yang berarti "tersembunyi" atau "terselubung" dan *graphein* yang berarti "menulis".

Konsep steganografi adalah menyisipkan pesan rahasia di dalam suatu media tanpa memberikan perubahan yang signifikan pada media tersebut.

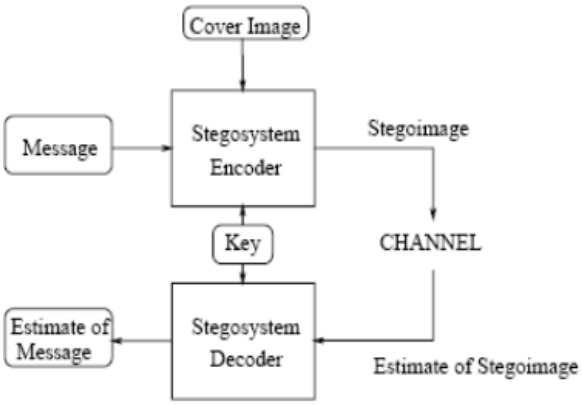
Sering kali orang salah mengartikan steganografi dengan kriptografi. Terdapat perbedaan mendasar di antara keduanya. Steganografi adalah seni atau ilmu menyembunyikan, sedangkan kriptografi hanya menyamarkan pesan.

Pada perkembangan modern, steganografi banyak menggunakan media digital sebagai tempat persembunyian dari pesan rahasia. Media digital yang umum dipakai untuk menyembunyikan pesan rahasia bisa berupa file apa saja (teks, gambar, suara, dll) selama file tersebut dapat diubah ke dalam bentuk bit-bit redundan yang dapat dimodifikasi. Sedangkan pesan yang dapat disembunyikan dengan menggunakan steganografi adalah hampir seluruh file digital.

Steganografi secara umum memiliki setidaknya tiga bagian:

a. *Hiddentext*: pesan yang disembunyikan.
b. *Covertext* atau *cover-object*: pesan atau objek yang digunakan untuk menyembunyikan pesan rahasia.
c. *Stegotext* atau *stego-object* : pesan atau objek yang sudah berisi pesan rahasia.

Gambaran yang terjadi dalam proses steganografi adalah seperti pada gambar di bawah ini:




**Gambar 1. Proses Steganografi**

Steganografi secara umum dapat dibagi menjadi 3 kelompok.

1. Steganografi pada file gambar
2. Steganografi pada file teks
3. Steganografi pada file suara

Teknik yang biasa dipakai pada steganografi adalah teknik LSB. Pada dasarnya teknik LSB adalah teknik dimana pesan rahasia akan dibuat menjadi bentuk bit-bit, kemudian setiap bit akan menggantikan bit paling kanan dari media penyisipan.

Salah satu media yang dapat digunakan untuk menyisipkan pesan rahasia adalah media digital suara. Pada makalah ini akan dibahas steganografi pada media digital suara khususnya MP3 dan WAV.

### *B. File Audio WAV*

WAV merupakan bentuk format file suara tanpa kompresi. Format ini menyimpan semua detil suara yang biasanya berupa dua kanal suara, 44100hz *sampling rate*, 16 bit setiap *sample*. Wav biasanya menyimpan format PCM yang juga merupakan format standar audio untuk CD. Tetapi audio CD tidak memakai format wav melainkan memakai red book audio format. Tetapi karena memakai format PCM maka data yang disimpan sama hanya berbeda pada headernya.

Karena tidak di kompresi maka absennya suara tidak menjadikan ukuran file berubah tidak seperti format *lossy*. Tetapi wav masih sering digunakan sebagai *master record* karena kualitasnya yang maksimal.

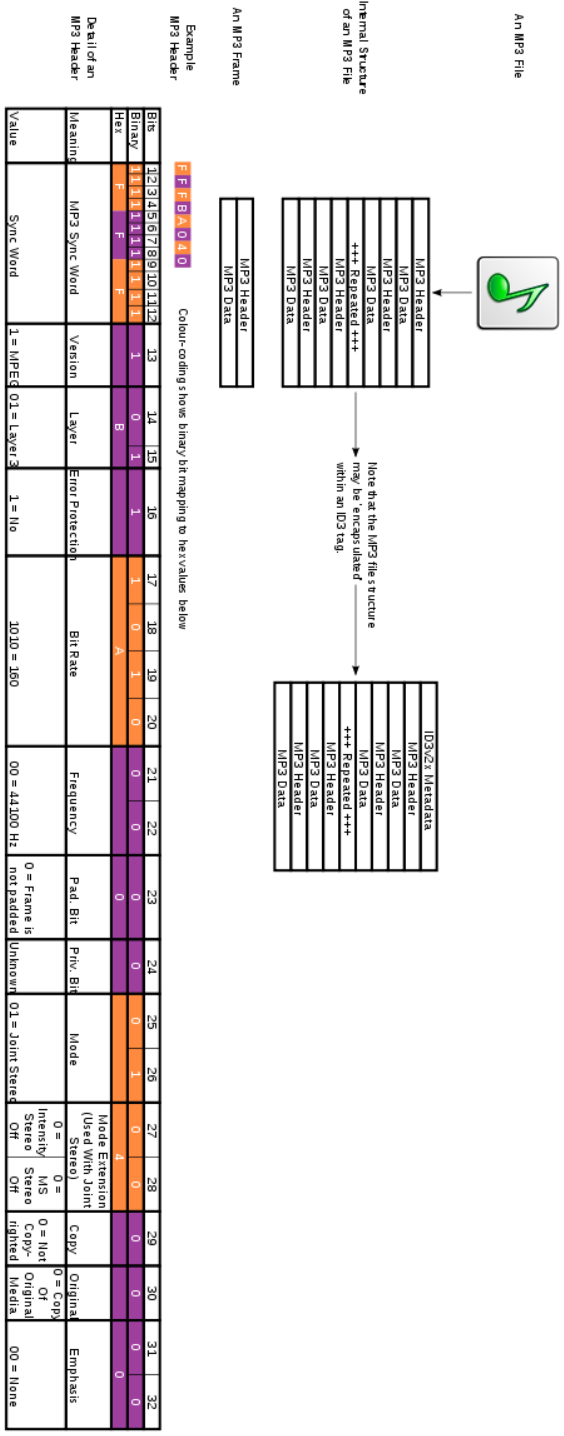
Permasalahan pada format ini adalah besarnya ukuran file yang mencapai 10 MB untuk setiap menit suara yang disimpan. Oleh karena itu dicarilah metode kompresi yang dapat secara signifikan mengurangi ukuran dari format ini serta mempertahankan kualitasnya. Terdapat berbagai macam format kompresi suara saat ini, dapat berupa *lossless* maupun *lossy*. *Lossless* berarti dapat dikembalikan dengan sempurna kepada bentuk aslinya, sedangkan *lossy* tidak karena bentuk lossy menghilangkan detil-detil yang kurang signifikan dalam suara tersebut. [3]

## *C. File Audio MP3*

MPEG (*Moving Picture Expert Group)*-1 audio layer III atau yang lebih dikenal sebagai MP3 adalah salah satu tipe file suara yang dapat digunakan pada steganografi. MP3 dapat memiliki hingga 6 kanal suara untuk membuat suara terdengar lebih hidup. Tipe file ini sangat terkenal pada saat ini karena ukuran file MP3 biasanya jauh lebih kecil dari file suara berformat WAV karena pada file MP3, aspek-aspek yang tidak signifikan pada pendengaran manusia dihilangkan agar besarnya file audio dapat diperkecil. Sebagian besar orang menyebut file audio MP3 adalah file audio hasil kompresi dari file audio WAV.

Pada MP3 encoder akan mengambil sebanyak 576 sample untuk tiap frame dan channel untuk signal dengan banyak detil dan 192 sample untuk sinyal yang memiliki sedikit detil. Kemudian dari sampel ini dihilangkan bagian yang kurang Signifkan pada manusia, bagian yang dihilangkan inilah yang menyebabkan MP3 termasuk kompresi *lossy*. Setelah itu dilakukan kompresi *lossless* untuk menghilangkan bagian yang masih ada redundansi.

Adapun struktur file MP3 dapat dilihat pada gambar di bawah ini:




**Gambar 2. Struktur File MP3**

Steganografi dalam file audio MP3 dapat dilakukan dengan beberapa teknik. Teknik steganografi dalam file MP3 adalah:

- Penyebaran Spektrum
  Dengan metode ini pesan dikodekan dan disebar ke tiap spectrum frekuensi yg memungkinkan. Maka dari itu akan sangat sulit bagi yg akan mencoba memecahkan kecuali ia memiliki akses terhadap data tersebut atau dapat merekonstruksi sinyal random yg digunakan utk menyebarkan pesan pada

range frekuensi.

- Teknik Echo Hiding
  Teknik menyamarkan pesan ke dalam sinyal yg membentuk *echo*. Kemudian pesan disembunyikan dgn menvariasikan tiga parameter dalam *echo* yaitu besar amplitude awal tingkat penurunan atenuasi dan offset. Dengan ada offset dari *echo* dan sinyal asli maka *echo* akan tercampur dgn sinyal asli krn sistem pendengaran manusia yg tak memisahkan antaha *echo* dan sinyal asli. Pada makalah ini, teknik ini lah yang akan dipelajari dan diujicobakan.
- Penggantian LSB
  Cara ini lazim digunakan dalam teknik digital steganografi yaitu mengganti LSB input tiap sampling dgn data yg dikodekan. Dengan metode ini keuntungan yg didapatkan adl ukuran pesan yg disisipkan relative besar namun berdampak pada hasil audio yg berkualitas kurang dgn banyak *noise*.
- Merekayasa Fasa Sistem Masukan
  Teori yg digunakan adl dgn mensubstitusi awal fasa dari tiap awal segment dgn fasa yg telah dibuat sedemikian rupa dan merepresentasikan pesan yg disembunyikan. Fasa dari tiap awal segment ini dibuat sedemikian rupa sehingga tiap segmen masih memiliki hubungan yg berujung pada kualitas suara yg tetap terjaga. Teknik ini menghasilkan keluaran yg baik namun sangat rumit.

Seluruh teknik steganografi dalam file audio MP3 memiliki kesamaan yaitu sama-sama memanfaatkan kelemahan indera pendengaran manusia.

## II. Echo Hiding Steganografi

Echo Hiding Steganografi adalah salah satu teknik steganografi pada file audio. Echo hiding steganografi menyembunyikan data yang hendak disisipkan menjadi sinyal host dengan cara membuat echo. Echo secara harfiah dapat diterjemahkan sebagai gema.

Data yang hendak disembunyikan menggunakan variasi dari tiga parameter berikut: *initial amplitude*, *decay rate*, dan *offset* atau *delay*. Seiring dengan berkurangnya offset antara sinyal orisinil dengan echo-nya, kedua sinyal tersebut menyatu. Pada titik tertentu, pendengaran manusia tidak dapat membedakan antara kedua sinyal tersebut, dan kemudian hanya terdengar sebagai resonansi tambahan. Hal ini tergantung pada faktor-faktor seperti kualitas rekaman asli, jenis suara, dan pendengar.

Dengan menggunakan dua waktu delay yang berbeda, keduanya dibawah tingkat persepsi pendengaran manusia, kita dapat meng-encode biner satu ataupun nol. Decay rate dan initial amplitude juga dapat disesuaikan di bawah kemampuan pendengaran manusia, untuk memastikan bahwa data yang disembunyikan tidak diketahui keberadaannya. Untuk meng-encode lebih dari satu bit, sinyal orisinalnya dibagi-bagi menjadi bagian-bagian yang lebih kecil, yang setiap bagiannya dapat di-echo-kan untuk dikodekan pada bit yang diinginkan. Sinyal akhir yang dihasilkan ini adalah rekombinasi dari seluruh port sinyal yang dikodekan secara independen.

Sebagai sebuah biner, satu direpresentasikan oleh suatu delay, dan biner nol direpresentasikan oleh suatu delay lainnya, deteksi dari sinyal yang sudah diembed hanya tinggal mendeteksi perbedaan dari echo-echo.

Echo hiding steganografi ditemukan berjalan sangat lancar pada file-file suara yang tidak memiliki degradasi tambahan, seperti dari baris noise atau lossy encoding, dan saat file tersebut tidak memiliki bagian yang tidak bersuara (silent).

## III. Uji Coba Aplikasi

### *A. MP3Stego*

Uji coba echo hiding steganografi akan dilakukan pada aplikasi freeware bernama MP3Stego. Aplikasi ini ditemukan dan dikembangkan oleh Fabien Petitcolas. Aplikasi ini dapat diunduh di http://www.petitcolas.net/fabien/steganography/mp3stego/index.html.

Aplikasi ini dibuat dikarenakan Fabien Petitcolas, sang pembuat merasa aplikasi echo hiding steganografi yang beredar di internet tidak dapat menggunakan file audio MP3. Padahal pada era modern ini, hampir sebagian besar file audio merupakan MP3 atau WMA. Sangat jarang ada yang menggunakan WAV. Pembuat aplikasi mengakui format audio WMA memang memiliki kualitas suara yang lebih baik dari MP3, namun karena format WMA tipenya secure (tidak dapat dilihat kodenya) dipilihlah MP3.

MP3Stego akan menyembunyikan data pada saat proses kompresi berlangsung. Pertama-tama data dikompresi, dienkripsi, dan baru kemudian disembunyikan di dalam file suara (MP3 ataupun WAV).

Cara penggunaan aplikasi ini adalah dengan menjalankan program dan memasukkan syntax berikut:

```
encode -E file.txt -P kunci input.wav output.mp3
```

Di atas adalah contoh syntax untuk melakukan enkripsi dengan file audio input.wav sebagai media penyembunyian, file.txt sebagai file yang hendak disembunyikan, kunci sebagai string kunci, dan output.mp3 adalah output yang diharapkan telah di steganografi-kan oleh MP3Stego.

```
decode -X -P kunci output.mp3
```

Di atas adalah contoh syntax untuk melakukan *decode* dengan file yang sudah di-*encode* sebelumnya dengan menggunakan aplikasi MP3Stego. File yang sudah di-*encode* sebelumnya dan hendak diekstrak adalah output.mp3, sedangkan kunci adalah kunci yang digunakan saat mengenkripsi file yang disembunyikan.

Hasil dekripsi output.mp3 adalah file yang dienkripsi sebelumnya dan output.mp3.pcm. File output.mp3.pcm adalah file mp3, dapat dimainkan kembali dengan menggunakan mp3player dengan cara menghapus ekstensi *.pcm dari nama file. File output berupa file *.pcm sebagai penanda saja bahwa file mp3 tersebut pernah menyembunyikan file.

Keterbatasan program adalah hanya dapat menyembunyikan file teks *.txt. Dan keterbatasan program yang lain adalah hanya dapat menerima masukan WAV baru kemudian oleh program akan dikonversi ke dalam bentuk MP3, dan hanya bisa memberikan keluaran dalam bentuk MP3. Selain itu, file yang terkait (file aplikasi, file teks yang hendak disembunyikan, file suara untuk menyembunyikan file teks) harus disimpan pada folder yang sama. Hasil keluaran dari MP3Stego juga akan disimpan pada folder yang sama.

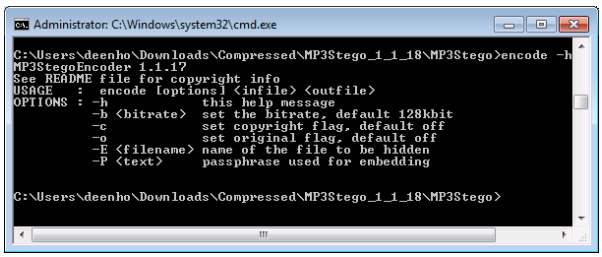
Sedangkan aplikasi sendiri berbentuk console, walaupun sudah ada yang mencoba membuat MP3Steno GUI sebagai bentuk GUI dari aplikasi MP3Stego. MP3Steno dibuat oleh Frans Vyncke berdasarkan aplikasi MP3Stego yang dibuat oleh Fabien Petitcolas.

Pengujian akan dilakukan pada aplikasi MP3Stego versi 1.1.18 for Windows. Pengujian dilakukan pada laptop penulis serta dilakukan oleh penulis sendiri. Adapun spesifikasi umum laptop penulis adalah Processor Intel U7300 1.3GHz, RAM 2GB, dan Sistem Operasi Windows 7 Professional.

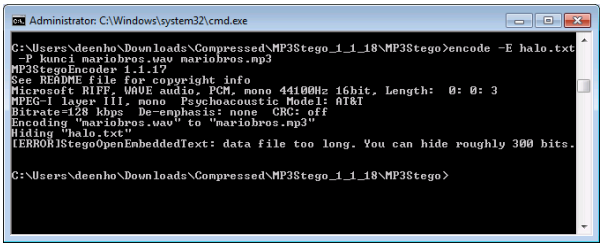
File yang akan coba disembunyikan adalah file halo.txt yang berisi:

```
halo nama saya dini
```

File ini akan coba disembunyikan pada file suara mariobros.wav yang merupakan file suara dari sebuah game bernama Mario Bross.

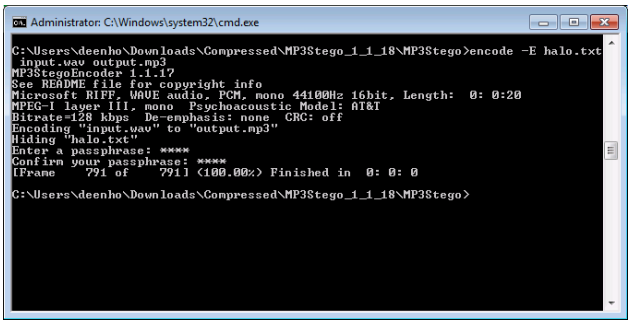



**Gambar 3. Berbagai Menu Pilihan Pada Encode**



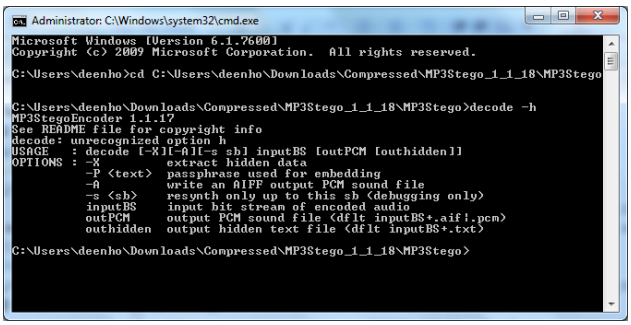

**Gambar 4. Encode Gagal**

Dapat dilihat bahwa hasilnya *encode* gagal. Hal ini dikarenakan file audio WAV yang dijadikan tempat bersembunyi lebih kecil dibandingkan file yang hendak disembunyikan. Pada gambar 4 dapat dilihat bahwa file maksimum yang dapat disembunyikan adalah 300 bits. Jumlah ini didapatkan dari jumlah frame dikalikan dengan 2. 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. Karena itu akan diujikan file audio lain yang lebih besar seperti konversi WAV dari file audio lagu Train – Soul Sister.mp3.

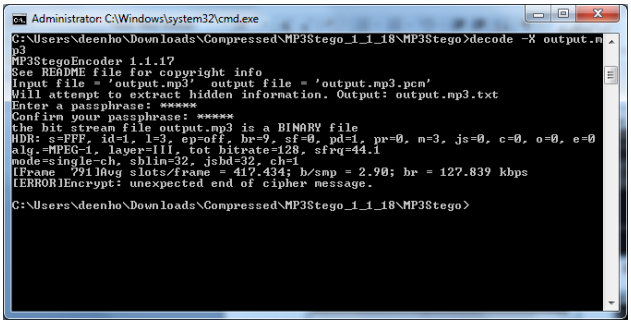



**Gambar 5. Proses Encode Berhasil**

Dapat dilihat di atas bahwa file halo.txt hendak disembunyikan ke dalam file audio input.wav. Kemudian file tersebut di-*encode* menjadi output.mp3. Adapun permintaan "Enter a passphrase" adalah permintaan memasukkan kunci untuk mengenkripsi file teks yang hendak disisipkan. Pada percobaan ini, kunci yang digunakan adalah 'dini'.

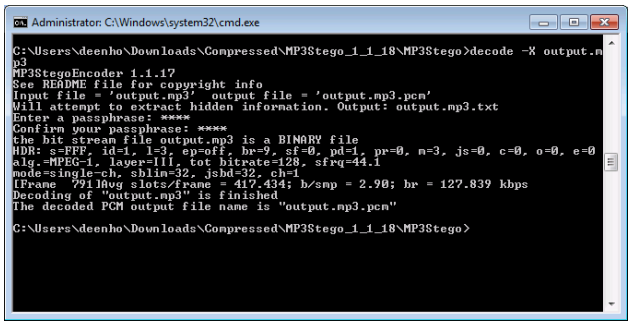



**Gambar 6. Berbagai Menu Pilihan Pada Decode**



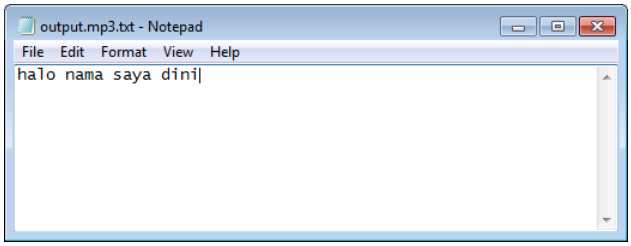

Gambar 7. Tampilan Jika Decode Gagal

Pada gambar 7 terlihat bahwa proses *decode* gagal. Hal ini disebabkan oleh masukan kunci oleh pengguna tidak sesuai dengan kunci saat file di-*encode*.




**Gambar 8. Proses Decode Berhasil**

Dapat dilihat pada gambar di atas bahwa proses decode berhasil. Sehingga dihasilkan output.mp3.pcm yang merupakan hasil ekstraksi dari file mp3 (ekstensi *.pcm hanya sebagai penanda bahwa file tersebut merupakan file audio yang pernah disteganografikan). Sedangkan hasil ekstraksi file tersembunyinya adalah output.mp3.txt. Berikut disertakan gambar hasil teks dari ekstraksi.




**Gambar 9. Isi File Teks Hasil Enkripsi**

Dapat dilihat pada gambar 7 bahwa file teks hasil ekstraksi output.mp3 sama dengan file halo.txt yang sebelumnya merupakan file yang disisipkan pada file audio. Hal ini membuktikan bahwa steganografi dengan menggunakan file audio sebagai media penyembunyi dapat dilakukan.

Walaupun jika didengarkan, file audio yang belum disisipkan pesan dan file audio yang telah disisipkan pesan sedikit terdengar berbeda. Namun perbedaan ini dirasa karena perbedaan kualitas file audio.

### *B. StegDroid Alpha*

Aplikasi ini adalah aplikasi steganografi lain yang memanfaatkan file audio sebagai media persembunyian file. Aplikasi ini merupakan aplikasi untuk Android yang tersedia secara gratis pada Android Market.

Aplikasi ini dikembangkan oleh Tom Medley sebagai salah satu bagian dari Proyek II saat beliau berkuliah di Universitas Cambridge jurusan *Computer Science*.

Aplikasi ini akan merekam audio, lalu menjadikannya satu dengan pesan teks rahasia ke dalam file audio yang baru direkam tersebut. Pesan rahasia dapat di enkripsi dengan sebuah kunci rahasia sebagai tambahan keamanan.

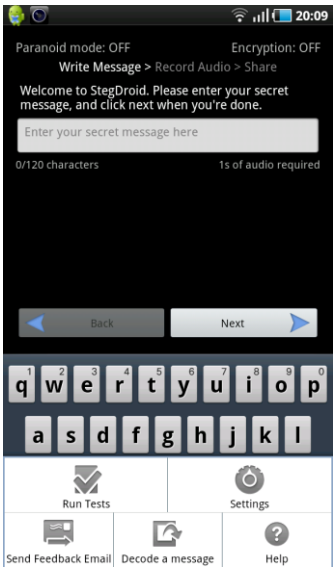
Aplikasi ini menggunakan Echo Hiding Steganografi sebagai teknik untuk menyembunyikan pesan. Perbedaan antara file suara yang sudah diencode dengan yang belum diencode tidak dapat didengar oleh telinga manusia. Hanya dengan menggunakan steganalisis yang komplek maka akan terlihat perbedaannya.

Percobaan aplikasi ini akan dilakukan sendiri oleh penulis dengan menggunakan Samsung Galaxy Tab yang memiliki system operasi Android Froyo (2.2) sebagai media untuk melakukan percobaan.

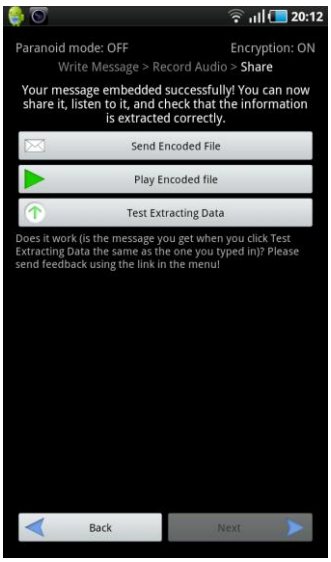
Tulisan yang hendak disisipkan pada kali ini sama dengan percobaan sebelumnya.

```
halo nama saya dini
```

File audio yang akan dijadikan sebagai media penyisipan akan direkam dengan menggunakan aplikasi yang sama.



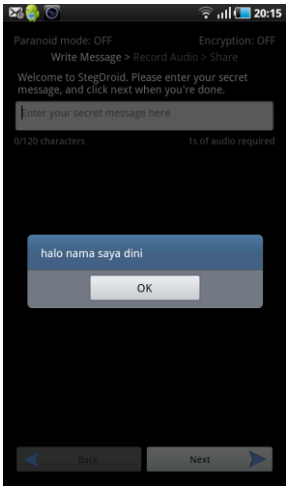

**Gambar 10. Tampilan Utama StegDroid**




**Gambar 11. Proses Steganografi Berhasil**

Dapat dilihat pada gambar 11 bahwa pesan rahasia berhasil disembunyikan pada file audio yang baru saja direkam. File audio yang berisi pesan rahasia lalu disimpan di dalam folder StegDroid yang terdapat pada

root directory. File audio hasil encode tersebut lalu akan di ektraksi untuk melihat hasil pesan rahasianya. Hasil dari ekstraksi file tersebut adalah seperti pada gambar 12.




**Gambar 12. Hasil Decode File Audio**

Terlihat di atas bahwa file audio berhasil di ekstraksi menjadi pesan rahasia yang sesuai dengan pesan rahasia yang diketikkan pada saat melakukan proses *encode*.

Keterbatasan aplikasi ini adalah pesan rahasia yang hendak disisipkan bukan merupakan file, melainkan hanya string biasa yang diinputkan saat hendak melakukan *encode*. Selain itu file audio yang digunakan untuk menyembunyikan pesan rahasia tidak dapat menggunakan file audio yang sudah ada melainkan harus membuat rekaman suaranya terlebih dahulu.

Jika didengarkan, suara yang telah disisipkan pesan rahasia dengan suara yang belum disisipkan pesan rahasia tidak memiliki perbedaan ataupun suara-suara tambahan yang menandakan file suara tersebut telah dimodifikasi.

Hal ini membuktikan bahwa steganografi dengan menggunakan file audio dapat dilakukan.

## IV. KESIMPULAN

Steganografi adalah teknik menyembunyikan pesan pada suatu benda. Di zaman modern ini, steganografi telah berkembang dan dapat disembunyikan dalam berbagai media digital. Salah satu media digital yang dapat digunakan untuk menyembunyikan pesan rahasia adalah file audio.

Steganografi berbeda dengan kriptografi, steganografi adalah menyembunyikan pesan, sedangkan kriptografi adalah menyamarkan pesan.

Teknik steganografi pada file audio ada berbagai macam teknik. Salah satunya adalah teknik Echo Hiding Steganografi, dimana itu adalah steganografi pada file audio dengan cara menyembunyikan pesan pada echo yang tidak terdengar oleh telinga manusia.

## REFERENSI


[1] Meliza T.M Silalahi, *Eksplorasi Steganografi: Kakas dan Metode*.
[2] http://id.wikipedia.org/wiki/Steganografi
[3] http://blog.ub.ac.id/teguh0610630106/2010/04/06/format-file-audio-wav/
[4] http://blog.re.or.id/teknik-teknik-steganografi-dalam-file-audio-mp3.htm
[5] http://www.scribd.com/doc/36573284/Steganography-the-Art-of-Hiding-Information
[6] http://www.petitcolas.net/fabien/steganography/mp3stego/
[7] Android Market


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 18 Maret 2011

Dini Lestari Tresnani
13508096