Studi Perbandingan Steganografi pada Audio, Video, dan Gambar

Gemita Ria The – NIM: 13507133
Program Studi Sistem dan Teknologi Informasi, Institut Teknologi Bandung
Jl. Ganeca 10, Bandung
E-mail: if17133@students.if.itb.ac.id

Abstrak

Makalah ini membahas studi mengenai perbandingan steganografi pada audio, video, dan gambar. Steganografi berhubungan dengan komunikasi dan merupakan metode yang digunakan untuk menyembunyikan pesan dengan menggunakan media digital berupa gambar, audio, maupun video. Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia di dalam *file* lain yang mengandung teks, gambar , bahkan audio tanpa menunjukkan ciri – ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari *file* semula.

Bagian awal makalah menjelaskan mengenai apa yang dimaksud dengan steganografi. Kemudian dilanjutkan dengan penjelasan bagaimana penerapan teknik steganografi tersebut pada *file* gambar, video, dan audio. Terdapat banyak metode yang dapat digunakan untuk menyembunyikan informasi di dalam media digital antara lain LSB, *injection*, *spread spectrum*, *echo hiding*, *low bit encoding*, dan sebagainya. Dua metode yang paling sering digunakan adalah LSB (*Least Significant Byte*) dan *Injection*. Bagian akhir dari makalah ini akan menganalisis perbandingan penerapan teknik – teknik steganografi pada media digital tersebut.

Kata kunci: steganografi, LSB, *Injection, spread spectrum, echo hiding, low bit encoding*

1. Pendahuluan

Komunikasi merupakan hal yang selalu dilakukan setiap saat. Seiring dengan berkembangnya teknologi dalam dunia telekomunikasi, semakin banyak pesan yang disampaikan dalam media digital. Steganografi merupakan salah satu metode yang dapat digunakan untuk menyembunyikan pesan dengan menggunakan media digital. Steganografi digital menggunakan media digital sebagai wadah penampung misalnya gambar, suara, teks, maupun video. Data rahasia yang disembunyikan juga dapat berupa gambar, suara, teks, maupun video.

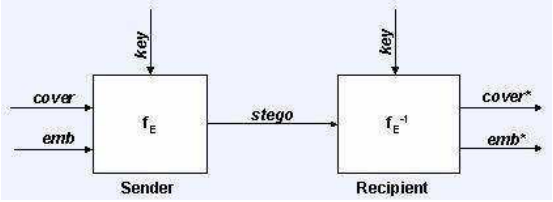
Teknik steganografi sendiri sudah dikenal sejak lama walaupun belum menggunakan media digital. Steganografi digunakan untuk menyembunyikan data di dalam data lain. Banyak metode yang dapat digunakan untuk menyembunyikan informasi di dalam gambar, audio, dan video di antaranya adalah metode LSB (*Least Significant Byte*), *Injection*, *masking* dan *filtering*, *transformation*, *low bit encoding*, dan metode – metode lainnya. Metode LSB dan *Injection* merupakan metode yang paling sering digunakan.

2. Steganografi

Steganografi berasal dari bahasa Yunani yaitu "*stego*" yang berarti tertutup dan "*graphia*" yang berarti menulis. Pengertian steganografi adalah ilmu dan seni dari menulis pesan rahasia di dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak disadari oleh indera manusia. Dengan menggunakan steganografi, sebuah pesan rahasia dapat disembunyikan di dalam sebuah informasi yang tidak mencurigakan dan mengirimkannya tanpa ada seorang pun yang mengetahui keberadaan pesan rahasia tersebut.

Format yang biasa digunakan sebagai media penyimpan pesan di antaranya:

- Format gambar: bitmap (bmp), gif, pcx, jpeg, dll
- Format audio: wav, voc, mp3, dll
- Format lain: teks file, html, pdf, dll



Gambar 1 Gambaran Umum Steganografi

2.1 Sejarah 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 SM. Histaeus mengirim pesan rahasia kepada anak lelakinya, Aristagoras, di Militus. Histaeus menulis pesan tersebut dengan menggunakan media kepala seorang budak. Histaeus mentato pesan rahasia tersebut pada kulit kepala budak tersebut setelah sebelumnya budak tersebut dibotaki. Ketika rambut

budak mulai tumbuh, Histaeus mengutus budak tersebut ke Militus untuk mengirimkan pesan rahasia yang terdapat di kepala budak tersebut ke anak lelakinya.

Selain metode tersebut, terdapat pula metode dengan menggunakan lilin. Pesan dituliskan dibawah kayu kemudian kayu tersebut dilapis dengan lilin.

Bangsa Romawi mengenal teknik steganografi lain yaitu dengan menggunakkan tinta yang tidak terlihat (*invisible ink*) untuk menuliskan pesan rahasia. Tinta tersebut dibuat dari campuran sari buah – buahan, susu, dan cuka. Untuk dapat membaca pesan yang ditulis dengan menggunakan tinta tidak terlihat tersebut, kertas berisi pesan rahasia tersebut harus dipanaskan dan pesan rahasia akan perlahan – lahan tampak jelas.

Jerman mengembangkan sebuah teknik yang disebut dengan *microdot*. *Microdot* merupakan foto dengan ukuran kecil. *Microdot* dicetak pada sebuah surat atau pada amplop dan menjadi sangat kecil sehingga seringkali tidak disadari.

Selain itu, pemerintah Amerika Serikat mengatakan bahwa Osama bin Laden dan organisasi al-Qaeda menggunakan steganografi untuk mengirimkan pesan melalui *website*. Namun, belum ada bukti yang dapat membenarkan pernyataan tersebut.

Steganografi telah banyak digunakan untuk berbagai kepentingan seperti kepentingan politik, militer diplomatik, serta untuk kepentingan pribadi yaitu komunikasi pribadi. Semakin banyak motivasi untuk menggunakan steganografi sehingga teknik – teknik steganografi terus berkembang.

2.2 Perbedaan Steganografi dan Kriptografi

Steganografi dan kriptografi sangat erat kaitannya namun keduanya merupakan hal yang berbeda. Kriptografi mengacaukan pesan sehingga pesan tersebut tidak dapat dimengerti sedangkan steganografi menyembunyikan pesan sedemikian rupa sehingga tidak ada pihak yang mengetahui keberadaan pesan tersebut. Dalam beberapa situasi, mengirimkan sebuah pesan yang telah dienkripsi akan menimbulkan kecurigaan sedangkan sebuah pesan rahasia yang tidak tampak tentunya tidak akan dicurigai. Kedua teknik ini dapat digabungkan untuk menghasilkan perlindungan yang lebih baik terhadap sebuah pesan, yaitu ketika steganografi gagal dan pesan dapat terlihat, pesan tersebut masih tidak dapat diartikan karena telah dienkripsi menggunakan teknik – teknik kriptografi.

Namun, terdapat sebuah persamaan di antara kriptografi dan steganografi, yaitu kualitas kriptografi bergantung pada sebuah kunci, demikian pula dengan steganografi. Menemukan pesan rahasia baik yang disembunyikan melalui steganografi ataupun dienkripsi menggunakan kriptografi hanya mungkin terjadi jika mengetahui kunci yang tepat.

2.3 Kriteria Steganografi

Kriteria yang harus diperhatikan dalam melakukan penyembunyian data dengan menggunakan teknik steganografi adalah sebagai berikut:

- *Fidelity*, kualitas dari media penampung data tidak boleh jauh berubah dari kualitas aslinya.
- *Robustness*, data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan terhadap media penampung data.
- *Recovery*, data yang telah disembunyikan di dalam media penampung data tersebut harus dapat diambil kembali.

2.4 Istilah dalam Steganografi

- *Stego-medium*, media yang digunakan untuk membawa pesan rahasia
- *Redundant bits*, sebagian informasi yang terdapat di dalam *file* yang jika dihilangkan tak akan menimbulkan kerusakan yang signifikan
- *Payload*, informasi yang akan disembunyikan
- *Carrier file*, *file* yang berisi pesan rahasia tersebut
- *Steganalysis*, proses untuk mendeteksi keberadaan pesan rahasia dalam suatu *file*

2.5 Metode Steganografi

Terdapat banyak metode untuk menyembunyikan informasi di dalam *file* gambar, audio, dan video. Dua metode yang paling umum digunakan adalah LSB (*Least Significant Byte*) dan *Injection*.

2.5.1 Substitusi – Mengganti LSB

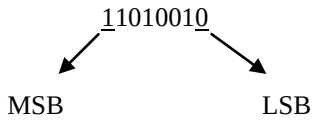
Ketika sebuah *file* dibuat, biasanya terdapat beberapa *byte* di dalam *file* yang tidak benar – benar dibutuhkan atau tidak penting. Area dari *byte* tersebut dapat diganti dengan informasi yang akan disembunyikan dan tidak akan merusak *file*. Hal ini memungkinkan seseorang untuk menyembunyikan informasi di dalam *file* dan yakin bahwa tidak ada seorang pun yang akan mengetahui perubahan di dalam *file*.

Metode LSB bekerja dengan baik pada *file* gambar yang memiliki resolusi tinggi dan memiliki warna yang beragam, dan pada *file* audio yang memiliki suara yang beragam dan memiliki bit *rate* yang tinggi. Metode LSB biasanya tidak mengubah ukuran *file*, namun hal ini juga tergantung pada

ukuran informasi yang akan disimpan ke dalam *file*.

Contoh penggunaan LSB:

Sebuah susunan bit pada sebuah *byte*:



MSB = *Most Significant Bit*
LSB = *Least Significant Bit*

Bit yang sesuai untuk ditukar adalah bit LSB karena perubahan pada daerah tersebut hanya akan menyebabkan nilai *byte* menjadi lebih tinggi 1 angka atau lebih rendah 1 angka dari nilai sebelumnya.

Untuk memperkuat teknik penyembunyian data, bit – bit data rahasia tidak digunakan mengganti *byte* yang berurutan namun dipilih susunan *byte* yang acak. Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan 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 merupakan algoritma kriptografi yang digunakan untuk enkripsi dan dibangun dengan menggunakan algoritma DES (*Data Encryption Standard*), algoritma *hash* MD5, dan mode kriptografi CFB (*Chipher-Feedback Mode*).

Misalkan segmen dari data sebelum ditukar adalah:

00110011 10100010 11100010 01101111

Setelah data ‘0110’ disembunyikan, segmen menjadi:

00110010 10100011 11100011 01101110

2.5.2 *Injection*

Injection merupakan sebuah metode yang cukup mudah yaitu dengan langsung menyisipkan informasi rahasia ke dalam *file*. Namun, permasalahan dari metode ini adalah metode ini dapat meningkatkan ukuran *file*.

3. Implementasi Steganografi

Informasi rahasia dapat disembunyikan pada berbagai media termasuk media digital. Jaman sekarang ini, kebanyakan teknik steganografi digunakan untuk menyembunyikan pesan di dalam gambar karena merupakan hal yang paling mudah untuk diimplementasikan. Hal yang paling penting dari pemilihan media penyimpanan informasi adalah penyesuaian ukurannya dengan jumlah data yang akan disimpan di dalamnya agar ketika dilakukan steganografi, ukuran media penyimpanan tersebut tidak berubah jauh. Ketika sebuah gambar tampak rusak atau sebuah lagu terdengar aneh dari aslinya, maka media tersebut akan dengan mudah dicurigai.

3.1 Steganografi pada Gambar

Menyembunyikan pesan di dalam gambar merupakan teknik yang paling sering digunakan sekarang ini. Sebuah gambar dengan sebuah pesan rahasia di dalamnya dapat dengan mudah disebarluaskan melalui web atau forum. Penggunaan steganografi di dalam forum telah diriset oleh Niels Provos, ahli steganografi Jerman.

Metode yang biasa digunakan untuk menyembunyikan informasi di dalam gambar adalah LSB, *masking*, *filtering* dan *transformation on the cover image*. Teknik – teknik tersebut dapat digunakan dengan berbagai tingkat kesuksesan pada berbagai tipe file gambar.

3.1.1 Modifikasi LSB

Teknik yang paling sering digunakan untuk menyembunyikan data adalah menggunakan LSB. Meskipun terdapat beberapa kekurangan dari teknik ini, namun teknik ini mudah untuk diimplementasikan sehingga membuatnya menjadi teknik yang paling terkenal. Karena metode ini menggunakan bit – bit dari setiap *pixel* yang ada di dalam gambar, penting untuk menggunakan *file* gambar yang tidak menggunakan algoritma kompresi sebagai media penyimpanan informasi.

Ketika menggunakan gambar 24 bit, setiap bit dari komponen merah, hijau, dan biru dapat digunakan, sehingga total dari ketiga bit tersebut dapat disimpan di setiap *pixel* gambar. Sebuah gambar dengan ukuran 800 x 600 *pixel* dapat menyimpan pesan rahasia kira – kira sebesar 1440000 bit (180000 *byte*).

Contoh berikut adalah 3 *pixel* dari gambar 24 bit menggunakan memori 9 *byte*:

(00100111	11101001	11001000)
(00100111	11001000	11101001)
(11001000	00100111	11101001)

Ketika karakter A yang memiliki nilai *binary* 10000001 dimasukkan, maka hasilnya akan menjadi:

(00100111	11101000	11001000)
(00100110	11001000	11101000)
(11001000	00100111	11101001)

Pada kasus ini, hanya tiga bit yang perlu diganti untuk memasukkan karakter tersebut dengan sukses. Biasanya, hanya setengah dari jumlah bit dalam gambar yang perlu dimodifikasi untuk menyembunyikan pesan menggunakan ukuran maksimal dari gambar. Hasil modifikasi yang dibuat pada bit LSB sangat kecil untuk disadari oleh mata manusia, sehingga pesan tersebut akan tetap tersembunyi.

Walaupun gambar 24 bit merupakan tipe yang paling bagus untuk menyembunyikan informasi, beberapa orang lebih memilih menggunakan gambar 8 bit BMP ataupun format gambar lain seperti GIF karena ukurannya tidak terlalu besar jika dibandingkan dengan ukuran gambar 24 bit.

Jika menggunakan gambar 8 bit, maka perlu digunakan pendekatan yang berbeda. Ketika gambar 24 bit menggunakan tiga *byte* untuk merepresentasikan sebuah *pixel*, 8 bit hanya menggunakan satu *byte*. Perubahan LSB pada *byte* tersebut akan menyebabkan perubahan warna yang jelas terlihat, karena itu gambar yang dipilih harus lebih hati – hati dan lebih baik jika warnanya *grayscale* sehingga mata manusia tidak akan mudah melihat perbedaan warna yang terjadi dibandingkan dengan perbedaan warna pada warna lain.

Kekurangan dari menggunakan metode LSB ini adalah dibutuhkan sebuah media penyimpanan yang sangat besar untuk menyediakan tempat yang besar pula untuk pesan yang akan disimpan. Kekurangan lainnya adalah ketika melakukan kompresi pada gambar yang telah dimasukkan pesan rahasia dengan menggunakan *lossy compression algorithm*, pesan rahasia tersebut akan hilang setelah kompresi selesai dilakukan.

3.1.2 *Masking* dan *Filtering*

Teknik *masking* dan *filtering* biasanya terbatas pada gambar 24 bit atau gambar *grayscale*. Metode ini mirip dengan *watermarking* pada kertas yang akan memberikan tanda pada gambar. Hal ini diperoleh dengan memodifikasi bagian cahaya gambar.

Informasi tidak disimpan pada "*noise*" *level* tetapi disimpan di bagian gambar yang terlihat jelas, sehingga lebih cocok digunakan dalam kasus *lossy compression algorithm* seperti pada gambar JPEG.

3.1.3 *Transformations*

Sebuah teknik yang lebih kompleks untuk menyembunyikan pesan di dalam gambar dilakukan dengan menggunakan *discrete cosines transformations* (DCT). DCT digunakan oleh algoritma kompresi JPEG untuk mengubah 8 x 8 blok *pixel* dari gambar menjadi 64 koefisien DCT. Setiap koefisien DCT *F(u,v)* dari 8 x 8 blok *pixel f(x,y)* ditentukan dari:

$$F(u,v) = \frac{1}{4} C(u)\ C(v)\ \left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * cos\frac{(2x+1)u\pi}{16}\ cos\frac{(2y+1)v\pi}{16}\right]$$

dimana C(x) = $1/\sqrt{2}$ ketika x = 0 dan C(x)=1. Operasi kuantisasi menjadi:

$$F^{Q}(u,v) = \left[\frac{F(u,v)}{Q(u,v)}\right]$$

dimana Q(u,v) adalah table kuantisasi 64 elemen. Sebuah algoritma *pseudo-code* sederhana untuk menyimpan pesan di dalam gambar JPEG akan tampak seperti berikut ini:

```
Input: message, cover image
Output: steganographic image containing message
while data left to embed do
        get next DCT coefficient from left image
        if DCT ≠ 0 and DCT ≠ 1 then
                get next LSB from message
                replace DCT LSB with message bit
        end if
        insert DCT into steganographic image
end while
```

Untuk menyembunyikan data dilakukan menggunakan DCT atau *wavelet transform* dari *cover image* dan menemukan koefisien tertentu. Bit tersebut kemudian diganti dengan bit yang akan disembunyikan (misalnya menggunakan LSB) kemudian mengambil *inverse transform* dan menyimpannya sebagai gambar biasa.

Untuk mengambil kembali data yang telah disimpan dapat dilakukan dengan cara menggunakan *transform* dari gambar yang telah dimodifikasi dan menemukan koefisiennya. Kemudian ekstraksi masing – masing bit data dari setiap koefisien dan kombinasikan menjadi pesan semula.

3.1.4 *Redundant Pattern Encoding*

Redundant pattern encoding adalah menggambar pesan kecil pada kebanyakan gambar.

3.1.5 *Spread Spectrum*

Pada metode *spread spectrum*, steganografi terpencar – pencar sebagai pesan yang diacak (enkripsi) melalui gambar (tidak seperti dalam LSB). Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*.

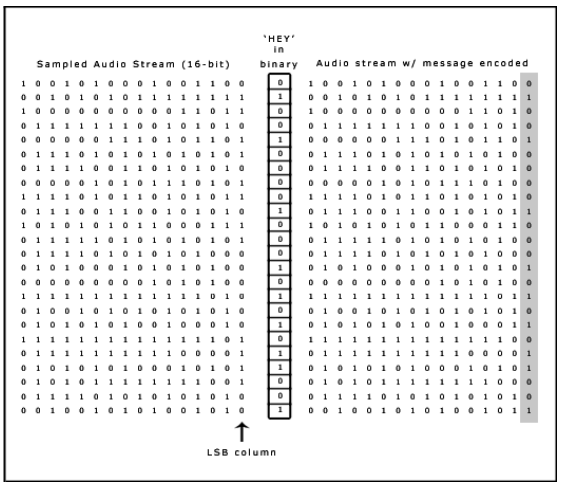
3.2 Steganografi pada Audio

Cara untuk mengimplementasikan steganografi pada *file* audio terdiri dari beberapa cara, yaitu sebagai berikut:

3.2.1 *Low Bit Encoding / Least Significant Bit*

Teknik yang biasa digunakan untuk menyembunyikan informasi di dalam file audio ialah *low bit encoding* yang mirip dengan teknik LSB yang biasa digunakan di gambar yaitu dengan menyisipkan bit – bit dari pesan yang akan disembunyikan ke dalam bit media penampung pesan tersebut.

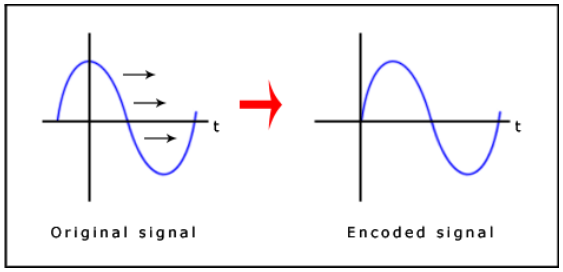
Masalah penggunaan teknik *low bit encoding* ialah biasanya terdengar oleh telinga manusia sehingga teknik tersebut merupakan teknik yang cukup beresiko untuk digunakan jika ingin menutupi sebuah informasi di dalam *file* audio.



Gambar 2 contoh penyimpanan pesan 'HEY' ke dalam 16-bit audio

3.2.2 *Phase Coding*

Phase Coding merupakan metode yang merekayasa fasa dari sinyal masukan. Teori yang digunakan ialah dengan mensubstitusi awal fasa dari setiap awal segmen dengan fasa yang telah dibuat sedemikian rupa dan merepresentasikan pesan yang disembunyikan. Fasa dari setiap awal segmen dibuat sedemikian rupa sehingga setiap segmen masih memiliki hubungan dan dapat menjaga kualitas suara. Teknik ini menghasilkan keluaran yang jauh lebih baik dari metode pertama namun realisasinya sangatlah rumit.



Gambar 3 Proses Phase Coding

Langkah – langkah *phase coding*:

- Suara asli dibagi ke dalam segmen – segmen yang lebih kecil yang panjangnya sama dengan pesan yang akan disembunyikan
- DFT (*Discrete Fourier Transform*) diaplikasikan ke setiap segmen untuk membuat matriks dari fase dan besaran *Fourier transform*
- Fase yang berbeda di antara setiap segmen dihitung
- Pesan hanya dapat disembunyikan pada fase vektor yang segmen sinyal pertamanya sebagai berikut:

$$phase\_new = \begin{cases} \pi/2 & if \ \ message \ \ bit = 0 \\ -\pi/2 & if \ \ message \ \ bit = 1 \end{cases}$$

- Sebuah fase matriks dibuat dengan menggunakan fase baru dari segmen pertama dan perbedaan dengan fase asli
- Dengan menggunakan matriks fase baru dan matriks besaran asli, sinyal suara direkonstruksi dengan mengaplikasikan *inverse* DFT kemudian menggabungkan segmen suara tersebut.

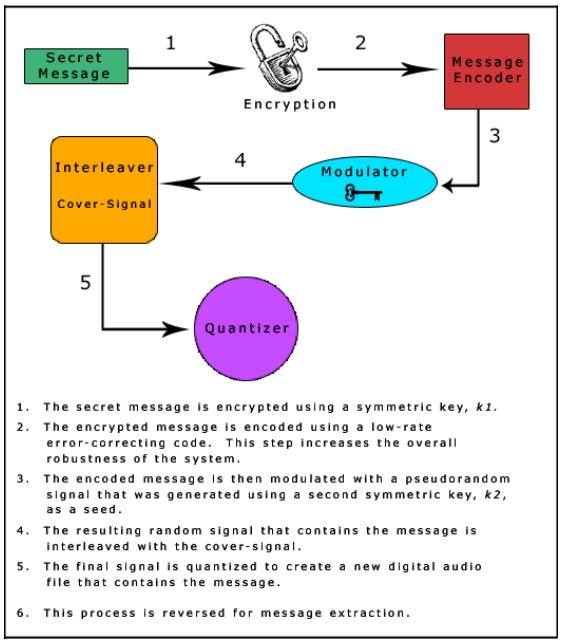
Agar dapat mengekstraksi pesan tersembunyi dari *file* audio, penerima harus mengetahui panjang segmen. Penerima kemudian dapat menggunakan DFT untuk mendapatkan fasenya dan mengekstraksi pesan.

3.2.3 *Spread Spectrum*

Spread Spectrum merupakan metode lain yang digunakan untuk menyimpan informasi di dalam *file* audio. Metode ini bekerja dengan cara pesan dikodekan dan disebarkan ke setiap spektrum frekuensi yang memungkinkan. Metode ini sulit untuk dipecahkan kecuali memiliki akses terhadap data yang disimpan atau dapat merekonstruksi sinyal random yang digunakan untuk menyebarkan pesan.

Ada dua versi dari *Spread Spectrum* yang dapat digunakan di dalam steganografi audio yaitu *direct-sequence* dan *frequency-hopping schemes*. Pada *direct-sequence spread spectrum*, pesan rahasia

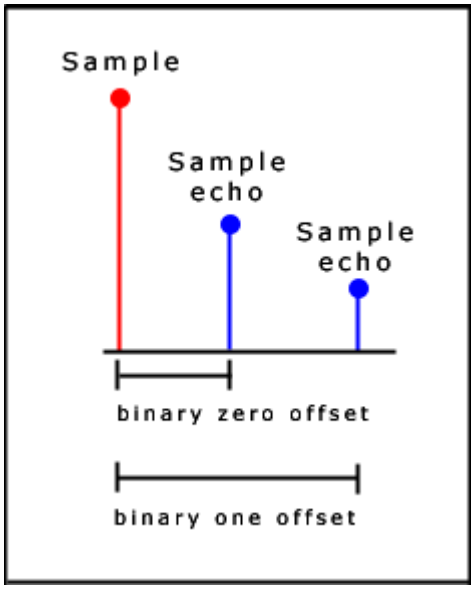
disebar dengan konstanta yang disebut *chip rate* dan kemudian dimodulasikan dengan sinyal *pseudorandom*. Kemudian digabungkan dengan *cover-signal*. Pada *frequency-hopping spread spectrum*, spektrum frekuensi *file* audio digantikan sehingga akan menyebar secara acak dalam frekuensi.



Gambar 4 Proses *Spread Spectrum*

3.2.4 *Echo Hiding*

Echo data hiding juga merupakan metode untuk menyembunyikan informasi di dalam *file* audio. Metode ini menggunakan *echo* yang ada di dalam *file* audio untuk mencoba menyembunyikan informasi. Pesan akan disembunyikan dengan memvariasikan tiga parameter dalam *echo* yaitu besar amplitudo awal, tingkat penurunan atenuasi, dan *offset*. Ketiga parameter tersebut diatur sedemikian rupa di bawah pendengaran manusia sehingga tidak mudah untuk dideteksi. Sebagai tambahan, *offset* divariasikan untuk merepresentasikan *binary* pesan yang disembunyikan. Nilai *offset* pertama merepresentasikan nilai *binary* 1 dan nilai *offset* kedua merepresentasikan *binary* 0.

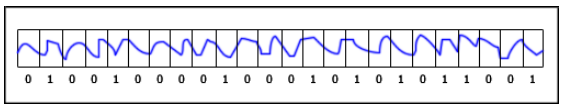


Gambar 5 Contoh *echo*

Jika hanya 1 *echo* yang dihasilkan dari sinyal asli, hanya 1 bit informasi yang dapat di *encoding*. Karena itu, sinyal awal dibagi – bagi ke dalam beberapa blok sebelum proses *encoding* dimulai. Ketika proses *encoding* telah selesai, blok – blok tersebut digabungkan kembali membentuk sinyal baru.

Berikut ini contoh penerapan *echo hiding*:

Awalnya, sinyal dibagi ke dalam blok – blok dan setiap blok diisi dengan 1 atau 0 berdasarkan pesan yang disimpan. Dalam kasus ini, pesan yang akan disimpan ialah ‘HEY’.

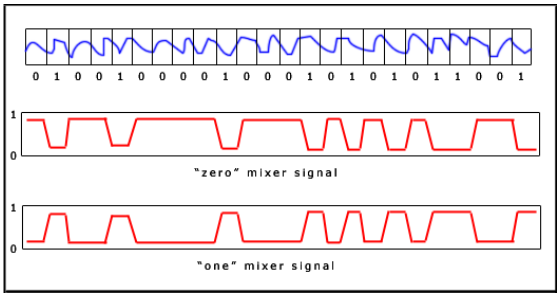


Gambar 6 contoh blok sinyal

Kemudian algoritma yang digunakan untuk mengenkripsi setiap blok ialah sebagai berikut:

```
init(Block blocks[]) {
   for (int i=0;i<blocks.length;i++) {
      if (blocks[i].echoValue() == 0)
         blocks[i]=offset0(blocks[i]);
      else
         blocks[i]=offset1(blocks[i]);
   }
}
Block offset0(Block block) {
   return (block+(block - OFFSET_0));
}
Block offset1(Block block) {
   return(block+(block- OFFSET_1));
}
```

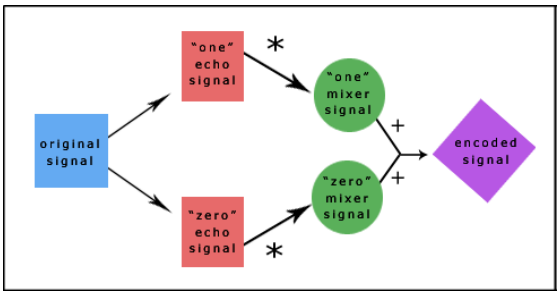
Blok – blok tersebut dikombinasikan untuk menghasilkan sinyal baru.



Gambar 7 dua buah sinyal gabungan

Sinyal *echo* "1" kemudian dikali dengan sinyal *mixer* "1" dan sinyal *echo* "0" dikali dengan sinyal *mixer* "0". Kemudian kedua hasil tersebut dijumlahkan untuk mendapatkan sinyal akhir.

Dengan adanya *offset* dari *echo* dan sinyal asli maka *echo* akan tercampur dengan sinyal aslinya. Kelebihan dari metode ini dibandingkan dengan metode lain ialah sistem pendengaran manusia tidak dapat memisahkan antara *echo* dan sinyal asli.



Gambar 8 Proses *Echo Hiding*

3.3 Steganografi pada Video

Teknik yang biasa digunakan untuk menyimpan informasi di dalam video adalah DCT (*Discrete Cosine Transform*). DCT merupakan representasi dari banyak *data point* yang merupakan penjumlahan dari fungsi kosinus yang berosilasi pada frekuensi yang berbeda-beda. DCT bekerja dengan mengubah sedikit gambar dari beberapa *frame* dalam video sehingga perubahan yang terjadi tidak dirasakan. DCT sebenarnya menimpa nilai dari beberapa bagian dari gambar di video. Selebihnya teknik penyusupan pesan memiliki cara yang sama dengan penggunaan steganografi pada gambar (seperti penggantian LSB).

Steganografi di video sangat mirip dengan steganografi di gambar, kecuali informasi disimpan pada setiap *frame* video. Ketika informasi yang disimpan hanya sedikit, maka perubahan pada video tidak akan tampak, namun jika informasi yang disimpan banyak, perubahan pada video akan semakin jelas terlibat.

4. Perbandingan Steganografi pada Audio, Video, dan Gambar

4.1 Steganografi Gambar

4.1.1 Modifikasi LSB

- Kelebihan:
  - Kelebihan terbesar dari algoritma LSB ini adalah cepat dan mudah
  - Algoritma ini juga memiliki *software* steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi gambar
- Kekurangan:
  - Jika menggunakan contoh 8 bit *pixel*, LSB dapat secara drastis mengubah unsur pokok warna dari *pixel*. Hal ini dapat menunjukkan perbedaan yang nyata dari *cover image* menjadi *stego image*, sehingga tanda tersebut menunjukkan keadaan dari steganografi.
  - Antara 8 bit dan 24 bit *image* mudah diserang dalam pemrosesan gambar, seperti *cropping* dan *compression*.

4.1.2 *Masking* dan *Filtering*

- Kelebihan:
  - Cocok digunakan dalam kasus *lossy compression algorithm* seperti pada gambar JPEG.
- Kekurangan:
  - Hanya mungkin digunakan pada gambar – gambar 24 bit dan *grayscale*.

4.1.3 *Transformations*

- Kelebihan:
  - Kualitas gambar asli hampir tidak terpengaruh
- Kekurangan:
  - Membutuhkan perhitungan matematis yang rumit

4.1.4 *Redundant Pattern Encoding*

- Kelebihan:
  - Dapat bertahan dari *cropping*
- Kekurangan:
  - Tidak dapat menggambar pesan yang lebih besar.

4.1.5 *Spread Spectrum*

- Kelebihan:
  - Kecil kemungkinan untuk terdeteksi
- Kekurangan:

- Masih mudah diserang melalui penghancuran atau merusak kompresi dan proses gambar
- Peningkatan kompleksitas dalam proses perhitungan

4.2 Steganografi Audio

4.2.1 *Low Bit Encoding* / LSB

- Kelebihan:
  - Mudah diimplementasikan dan proses *encoding* yang cepat
- Kekurangan:
  - Biasanya terdengar oleh telinga manusia sehingga teknik tersebut merupakan teknik yang cukup beresiko untuk digunakan jika ingin menutupi sebuah informasi di dalam *file* audio

4.2.2 *Phase Coding*

- Kelebihan:
  - Merupakan teknik yang cukup robust dalam penyisipan watermark ke dalam suatu bekas MP3 karena teknik ini tahan terhadap proses pencuplikan ulang, pemotongan berkas MP3 (selain bagian awal berkas), pemberian derau (selain bagian awal berkas), dan kompresi (pengubahan format berkas)
  - Kualitas suara yang dihasilkan oleh berkas MP3 yang telah disisipi watermark dengan teknik ini cukup baik (hampir tidak terdeteksi adanya derau)
- Kekurangan:
  - Jika dilakukan pemotongan atau pemberian derau pada bagian awal berkas MP3 yang disisipi *watermark*, maka *watermark* dapat hilang atau tidak dapat diekstraksi dengan baik
  - Hanya dapat digunakan ketika ingin menyembunyikan data yang ukurannya kecil

4.2.3 *Spread Spectrum*

- Kelebihan:
  - Penyembunyian sinyal (kepadatan energi yang rendah, mirip derau)
  - Komunikasi yang aman
  - Penolakan *multi path*, hanya menerima *direct path*
  - Proteksi terhadap inferensi yang tidak disengaja (*narrowband*)
  - Kecil kemungkinan untuk terdeteksi
  - Adanya ketersediaan *license-free* ISM (*Industrial, Scientific, and Medical*) *frequency-bands*
- Kekurangan:
  - Tidak adanya perbaikan performansi melalui penggunaan derau Gaussian
  - Peningkatan bandwith (penggunaan frekuensi, *wideband receiver*)
  - Peningkatan kompleksitas dalam proses perhitungan
  - Dapat menimbulkan derau

4.2.4 *Echo Hiding*

- Kelebihan:
  - Sistem pendengaran manusia tidak dapat memisahkan antara *echo* dan sinyal asli
- Kekurangan:
  - Kurang bagus digunakan pada *file* audio yang memiliki *silence gap* yang cukup besar karena *echo* akan terdengar jelas

4.3 Steganografi Video

Untuk kelebihan dan kekurangan pada steganografi video mirip dengan steganografi pada gambar karena teknik yang digunakan pada steganografi video tidak jauh berbeda dengan steganografi pada gambar.

4.4 Perbandingan antara Steganografi Audio, Video, dan Gambar

Sebenarnya di antara steganografi audio, video, dan gambar tidak dapat ditentukan manakah implementasi steganografi yang bagus. Masing – masing implementasi memiliki kelebihan dan kekurangan masing – masing.

Untuk memilih implementasi steganografi pada media digital mana yang paling bagus digunakan untuk menyembunyikan sebuah data itu tergantung pada ukuran data dan tingkat keamanan yang diinginkan untuk menyembunyikan data tersebut.

Jika pesan yang disembunyikan kecil dan tidak membutuhkan keamanan yang sangat tinggi, maka yang paling bagus adalah menggunakan steganografi pada gambar karena gambar hanya dapat menampung pesan yang ukurannya kecil dan masih rentan untuk dapat ditemukan perbedaannya dengan gambar asli.

Jika pesan yang disembunyikan cukup besar dan membutuhkan tingkat keamanan yang relatif tinggi, maka pergunakanlah steganografi pada audio karena *file* audio yang dihasilkan dari steganografi tersebut sulit untuk dapat dibedakan dengan *file* aslinya sedangkan jika ukuran pesan besar, maka gunakanlah steganografi pada video karena ukuran video yang besar dan terdiri dari banyak *frame* menyebabkan mampu menampung pesan yang berukuran besar pula.

5. Kesimpulan

Steganografi adalah ilmu dan seni dari menulis pesan rahasia di dalam sebuah media sedemikian rupa sehingga tidak disadari oleh indera manusia. Terdapat banyak teknik yang dapat digunakan untuk menerapkan steganografi pada media digital. Masing – masing teknik tersebut memiliki kelebihan dan kekurangannya masing – masing dan masing – masing teknik cocok ditetapkan pada media digital tertentu.

Untuk media gambar, teknik yang cukup bagus digunakan adalah *transformations* dan *spread spectrum* karena teknik tersebut walaupun cukup rumit untuk diimplementasikan namun hasilnya cukup bagus dan tidak akan dapat disadari langsung.

Untuk media audio, teknik yang paling bagus digunakan adalah teknik *echo hiding* karena menghasilkan *file* yang tidak dapat dibedakan dengan *file* aslinya sedangkan untuk *file* video karena teknik yang digunakan mirip dengan gambar, maka dapat menggunakan teknik yang sama dengan steganografi gambar.

Untuk dapat menentukan manakah steganografi yang paling bagus di antara steganografi pada gambar, audio, atau video itu tergantung pada kebutuhannya yaitu tergantung pada ukuran data yang akan disembunyikan dan tingkat keamanan yang diinginkan pada data tersebut.

Dengan mengetahui teknik – teknik yang dapat digunakan pada steganografi di media digital dan mengetahui kekurangan dan kelebihan masing – masing teknik, maka masyarakat dapat memilih teknik yang paling sesuai dengan kebutuhan mereka. Perbandingan mengenai implementasi yang paling sesuai untuk pesan yang ingin disembunyikan seperti yang telah diuraikan pada beberapa paragraf sebelumnya itu tidaklah mutlak harus dilakukan. Semuanya kembali kepada masyarakat yang akan menggunakan teknik steganografi ini. Namun, penjelasan di atas membantu memudahkan dan memberikan penjelasan mengenai implementasi steganografi pada audio, video, dan gambar.

6. Referensi

[1] “Steganography and Steganalysis”. J.R.Krenn. January 2004.
URL: http://www.krenn.nl/univ/cry/steg/article.pdf

[2] “Mirage – A Steganographic Data Security Algorithm with Reduced Steganalysis Threat”. Mohammad Fahmi Birzeit University, Birzeit – Palestine
URL:http://www.scribd.com/doc/3367439/Steganography

[3] “Steganography FAQ”. Aelphaeis Mangarae [Zone-H.Org]. March 18th 2006.
URL:http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf

[4] “Digital Watermarking”
URL:http://blog.re.or.id/digital-watermarking.htm

[5] Munir, Rinaldi. Steganografi.2006. Departemen Teknik Informatika, Institut Teknologi Bandung.

[6] Dewi, Risa Astari. “Penerapan Audio Steganografi dalam Infrasonics”. 2009. Departemen Teknik Informatika. Institut Teknologi Bandung.

[7] Vembrina, Yus Gias. “Spread Spectrum Steganography”. 2006. Departemen Teknik Informatika. Institut Teknologi Bandung.

[8] Rumondang, Martharany. “Perlindungan Hak Cipta pada Data Audio Menggunakan Teknik Watermarking Phase Coding”. 2006. Departemen Teknik Informatika. Institut Teknologi Bandung.

[9]http://www.snotmonkey.com/work/school/405/methods.html. Tanggal akses: 23 Maret 2010 pukul 17.00 WIB