Watermarking Audio File dengan Teknik Echo Data Hiding dan Perbandingannya dengan Metode LSB dan Phase Coding

Roy Indra Haryanto - 13508026
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
royindra@students.itb.ac.id

Pada makalah ini akan dibahas mengenai watermarking audio file dengan teknik echo data hiding dan bagaimana perbandingannya dengan metode lainnya seperti metode LSB (Least Significant Bit) dan Phase Coding yang merupakan metode yang cukup umum dipakai padawatermarking audio file. Bagian awal makalah akan dijelaskan mengenai apa itu watermarking dengan teknik Echo Data Hiding, LSB dan Phase Coding, lalu akan dijelaskan juga bagaimana melakukan watermarking dengan teknik Phase Coding serta bagaimana analisis perbandingan hasil dari watermarking dengan ketiga metode tersebut, apa kelebihan dan kekurangannya masing – masing.

Kata Kunci : Echo Data Hiding, LSB, Phase Coding, Watermarking Audio File

I. PENDAHULUAN

Pada masa sekarang ini, dimana melakukan penggandaan terhadap audio file adalah seperti semudah membalikkan telapak tangan, adalah hal yang seperti bumerang bagi industri produksi musik dan multimedia. Di satu sisi, hal tersebut sangat memudahkan user untuk memainkan dan menyimpan lagu yang sudah dibeli, tetapi di sisi lain juga akan sangat menghambat perkembangan dari industri musik karena penggandaan dan manipulasi secara sempurna dan tanpa batas pada end user juga sangat mudah dilakukan.

Digital watermarking adalah sebuah teknologi yang digunakan untuk mengatur penggandaan, mengidentifikasi media, pelacakan dan proteksi isi dari hak pemilik. Proteksi terhadap isi file audio dapat dilakukan dengan beberapa metode watermarking yaitu seperti Echo Data, LSB ataupun Phase Coding.

Pada suatu format digital, isi dinyatakan sebagai rangkaian dari angka 0 dan 1. Isi dapat dengan mudah digandakan secara sempurna dalam waktu yang tidak terbatas. Seorang user dapat melakukan manipulasi pada file – file ini dengan sangat mudah. Untuk mendukung keamanan dan mencegah penggandaan dan manipulasi isi, maka seharusnya disediakan mekanisme proteksi terhadap isi dari file audio tersebut. Proses mekanisme proteksi terhadap isi berarti mengusahakan untuk melindungi hak – hak dari pembuat isi, distributor dan user. Pemilik dari isi menempatkan sebuah deskripsi yang unik dari file asli pada sebuah registration authority. Mekanisme yang unik ini mungkin menggunakan suatu nilai atau deskripsi berupa teks. Identifikasi yang unik ini adalah sesuatu yang berhubungan dengan data pemilik dari isi file tersebut.

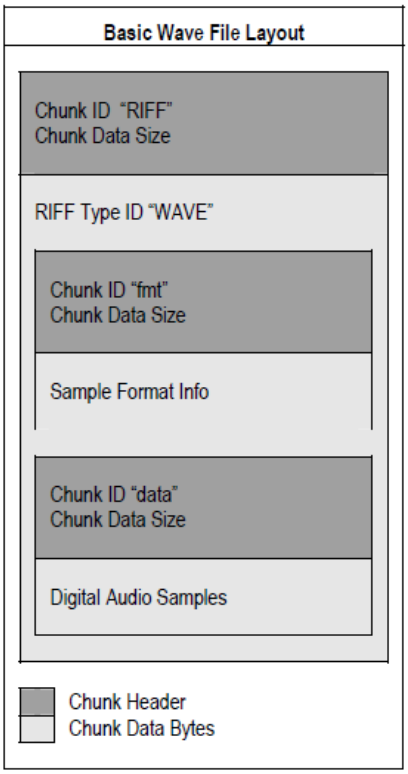
Digital watermark ini secara aman dan rahasia menggabungkan angka identifikasi yang unik dengan isi yang asli. Kualitas dari isi yang merupakan hasil penggabungan dalam file audio pasti mengalami penurunan walaupun hanya sedikit. Dengan menggunakan metode echo data hiding, apabila dibutuhkan pembuktian tentang pemilik dari isi tersebut maka angka identifikasi yang unik tadi dapat diekstrak langsung dari isi yang telah di-watermark. Sebagai tambahan untuk menyisipkan sebuah watermark dalam isi secara rahasia, seorang pemilik dari isi dapat menambahkan sebuah ‘label’ yang berhubungan dengan angka identifikasi yang unik. Label ini merupakan pemberitahuan secara umum yang menginformasikan kepada user tentang hak kekayaan intelektual dari isi tersebut.

II. LANDASAN TEORI

A. File Audio WAVE

Format file wave merupakan salah satu format yang digunakan untuk menyimpan suara pada rentang frekuensi 20 Hz sampai 20 kHz. Gelombang suara mempunyai data yang kontinyu sehingga gelombang tersebut bila digambarkan akan berupa kurva yang tidak putus-putus, akan tetapi komputer hanya dapat menyimpan data dalam bentuk digital. File dengan format wave menggunakan metode pulse code modulation (PCM) untuk menyimpan suara yang bersifat analog menjadi data digital pada komputer. PCM adalah salah satu cara merepresentasikan data analog dalam bentuk digital dimana data sinyal analog tersebut diambil sampelnya pada setiap selang periode tertentu kemudian dijadikan nilai pada sistem digital. Selang waktu yang digunakan untuk mengambil sampel pada sinyal analog tersebut menentukan kualitas suara yang dihasilkan. Semakin banyak sampel sinyal analog yang diambil

dalam selang waktu tertentu maka semakin baik pula kualitas suara yang dihasilkan (hasil suara akan mendekati dengan suara aslinya). Data mentah hasil PCM ini kemudian disimpan dalam format file .WAV.



Gambar 1 – Struktur File Audio WAVE

B. Watermarking

Pada dasarnya, teknik *watermark* adalah proses penambahan kode identifikasi secara permanent kedalam data digital. Kode identifikasi tersebut dapat berupa teks, suara, gambar, atau video. Selain tidak merusak data digital yang dilindungi, kode identifikasi seharusnya memiliki ketahanan (*robustness*) terhadap bebagai pemrosesan lanjutan seperti pengubahan, kompresi, enkripsi, dan lain sebagainya. Penyisipan *watermark* pada dokumen memiliki berbagai macam tujuan. Untuk aplikasi perlindungan hak cipta, tanda yang disisipkan pada dokumen (gambar, teks, atau audio) digunakan sebagai identifier yang menunjukkan hak kepemilikan atau hak penggunaan dokumen. Jenis tanda air mempengaruhi keefektifan tanda air itu sendiri dalam setiap aplikasinya. Baik tanda air *perceptible* maupun *imperceptible*, keduanya dapat mencegah terjadinya penyalahgunaan, namun dengan cara yang berbeda. Tanda air digital digunakan untuk memberikan identifikasi sebuah dokumen atas informasi sumber daya, penulis, kreator, pemilik, distributor, dan konsumer yang berhak atas dokumen tersebut.

Ada beberapa karakteristik yang diinginkan dari penggunaan *watermark* pada suatu dokumen, diantaranya tidak dapat terdeteksi (*imperceptible*), *robustness*, *security*, *fragility*, dan *tamper resistance*.

1. *Imperceptible*: memberikan karakteristik *watermark* agar sebisa mungkin harus tidak dapat terlihat atau berbeda dengan dokumen aslinya. Hal ini dimaksudkan untuk tidak merubah status dokumen yang bernilai tinggi secara hukum maupun komersial.
2. *Robustness*: Karakteristik ini tergantung aplikasi dari *watermark* itu sendiri. Apabila digunakan sebagai identifikasi kepemilikan/*copyright*, *watermark* harus memiliki ketahanan terhadap berbagai macam modifikasi yang mungkin bisa dilakukan untuk merubah/menghilangkan *copyright*. Jika digunakan untuk otentikasi *content*, *watermark* sebisa mungkin bersifat *fragile*, sehingga apabila isinya telah mengalami perubahan, maka *watermark* akan mengalami perubahan/rusak, sehingga dapat terdeteksi adanya usaha modifikasi terhadap isi.
3. *Security*: Teknik *watermark* harus dapat mencegah usaha-usaha untuk mendeteksi dan memodifikasi informasi watermark yang disisipkan ke dalam dokumen. Kunci *watermark* menjamin hanya orang yang berhak saja yang dapat melakukan hal tersebut. Namun aspek ini tidak dapat mencegah siapapun untuk membaca dokumen yang bersangkutan.
4. *Fraggility*: berlawanan dengan *robust*, konsep ini menghendaki *watermarking* bersifat rapuh. Tentu saja hal ini dilakukan dalam beberapa aplikasi tertentu. Sebagai contoh adalah *watermarking* fisik yang diberikan pada surat-surat yang berharga yang dibuat sehingga *watermarking* tersebut tidak akan tahan terhadap proses pengkopian. Tujuannya tentu saja untuk menjaga keotentikannya. Kelihatannya pembuatan *watermarking* itu sengaja didesain rapuh terhadap beberapa modifikasi, namun juga tahan terhadap modifikasi tertentu. Jenis *watermarking* ini biasanya tidak diimplementasikan dalam bentuk digital.
5. *Tamper Resistance*: konsep ini menghendaki *watermarking* tahan terhadap segala modifikasi yang dilakukan terhadap sinyal media yang memang dilakukan dengan tujuan untuk menghilangkan *watermarking*, dibandingkan dengan konsep *robust* yang menghendaki ketahanan terhadap sinya media. Modifikasi dengan tujuan semacam ini dinilai berhasil jika mampu merusak *watermarking* tanpa menurunkan kualitas sinyal media secara drastis. Penurunan kualitas ini tentunya dinilai secara *perceptual* bersifat signifikan sehingga

jika *watermarking* rusak, maka sinyal media akan mengalami penurunan kualitas secara pendengaran.

C. Echo Data Hiding

Metode *Echo data hiding* dilakukan dengan menambahkan data pada sinyal suara penampung dengan memunculkan *echo*. Data yang akan disembunyikan dalam bentuk *echo* dinyatakan dengan variasi dari tiga parameter, yaitu amplitudo awal, *decay rate*, dan *offset (delay)*. Amplitudo awal menyatakan amplitudo asal dari data suara tersebut, *decay rate* menyatakan seberapa besar *echo* yang akan diciptakan, dan *offset* menyatakan jarak antara sinyal suara dengan *echo* dalam bentuk fasa sudut dalam persamaan analog. Jika *offset* dari sinyal asal dan *echo* berkurang, maka kedua sinyal akan bercampur. *Echo* ini akan terdengar sebagai resonansi.

Selanjutnya, untuk proses pengkodean, sinyal suara asal dipecah menjadi beberapa bagian. Pada setiap bagian, *echo* dimunculkan dengan menggunakan waktu tunda sesuai bit data yang akan disembunyikan. Waktu tunda tersebut dinyatakan dalam parameter *offset*, serta besarnya *echo* yang akan disisipkan dinyatakan dengan *decay rate*. Setelah selesai, semua pecahan sinyal digabungkan kembali sehingga menjadi sinyal yang utuh.

D. Least Significant Bit (LSB)

Metode *Least Significant Bit* adalah cara yang paling sederhana untuk menyimpan data kedalam data yang lain. Dengan mengganti bit yang paling tidak penting atau *least significant bit (LSB)* pada setiap titik *sampling* dengan string berkode biner (*coded binary string*), kita dapat mengenkode sejumlah besar data ke dalam suara digital. Secara teori, kapasitas saluran adalah 1 kb per detik (1 kbps) per 1 kHz.

E. Phase Coding

Cara kerja metode ini adalah dengan mengganti fase bagian awal sinyal suara dengan fase yang berhubungan yang mewakili data. Fase bagian lain yang mengikuti diatur untuk melindungi fase relatif antar bagian.

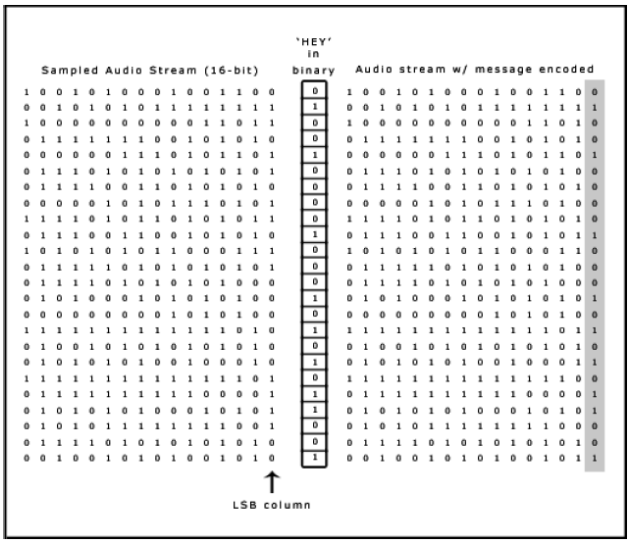
Phase coding merupakan metode yang paling efektif dari segi perbandingan noise *signal-to-perceived.* Jika hubungan fase antar antar setiap komponen frekuensi diubah secara dramatis, akan terjadi dispersi fase yang tampak dengan jelas. Akan tetapi, selama modifikasi fase cukup kecil (tergantung pada pengamat), *coding* yang tidak mungkin terdengar dapat dilakukan.

III. IMPLEMENTASI

A. Least Significant Bit (LSB)

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.

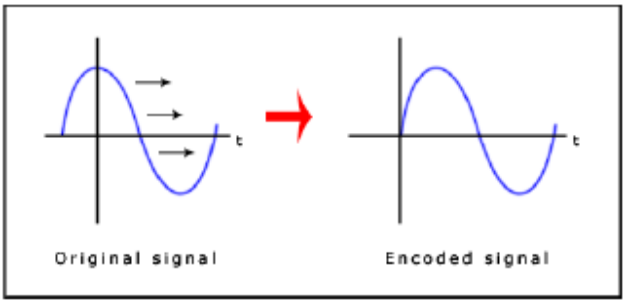
Masalah penggunaan teknik *low bit encoding* ialah biasanya terdengar oleh telinga manusia sehingga teknik tersebut merupakan teknik yang cukup beresiko untuk digunakan jika ingin menutupi sebuah informasi di dalam *file* audio.



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

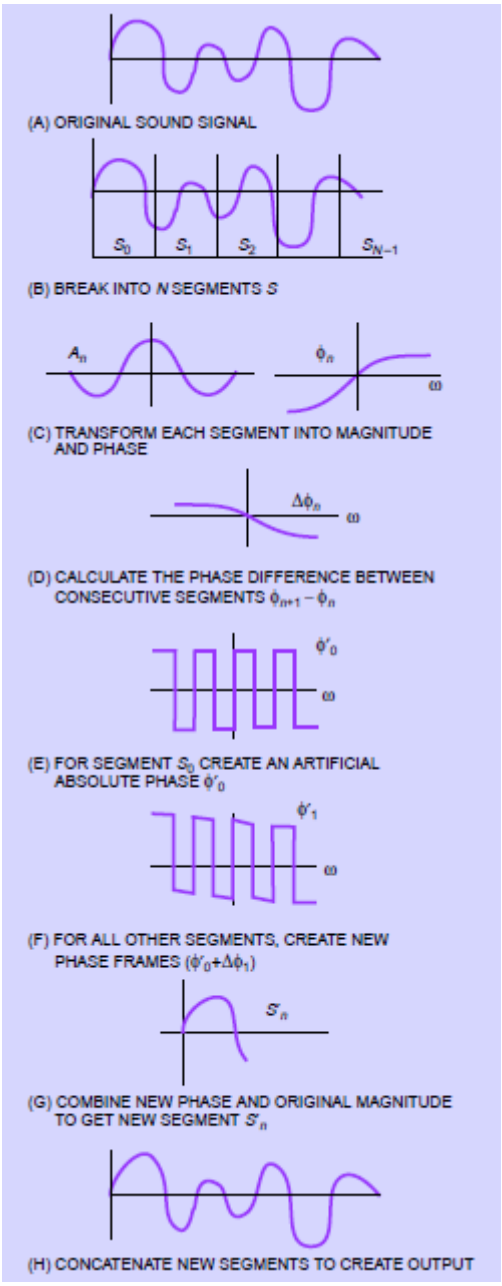
B. Phase Coding

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

Secara garis besar, skema phase coding ditunjukkan pada gambar dibawah ini :



Gambar 4 – Skema *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:

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

- 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.

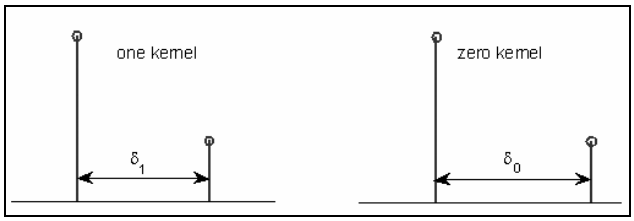
Agar dapat mengekstraksi pesan tersembunyi dari *file* audio, penerima harus mengetahui panjang segmen. Penerima kemudian dapat menggunakan DFT untuk mendapatkan fasenya dan mengekstraksi pesan.

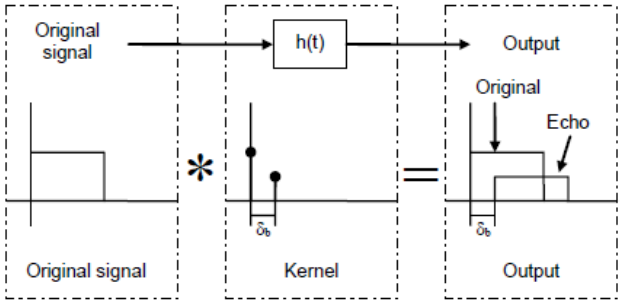
C. Echo Data Hiding

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.

Echo Data Hiding menempatkan informasi sisipan pada sinyal asli (yang selanjutnya disebut cover audio) dengan menggunakan sebuah “echo.” Pada hal tertentu telinga manusia tidak dapat mendengar sinyal asli dan echo secara bersamaan, melainkan hanya berupa sinyal distorsi tunggal. Hal ini sulit ditentukan secara tepat, ini tergantung pada kualitas rekaman sinyal asli, tipe suara yang di-echo dan pendengar. Fungsi sistem yang digunakan pada domain waktu adalah discrete time exponential yang cara membedakannya hanya pada delay antar impuls. Untuk membentuk echo hanya menggunakan dua buah impuls yang disebut kernel.

Kernel “satu” dibuat dengan delay δ1 detik sedangkan kernel “nol” dibuat dengan delay δ0 detik.



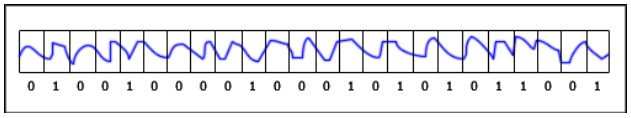


Gambar 5 – Kernel dan Proses Pembentukan Echo

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’.

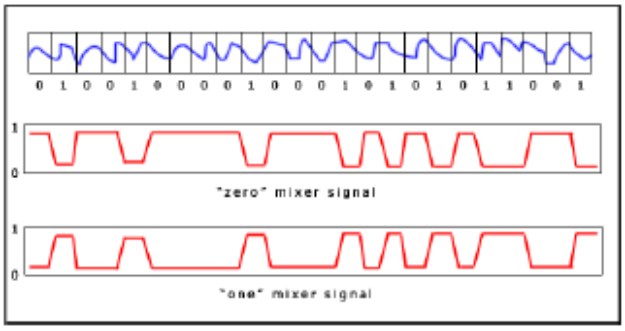


Gambar 6 - Contoh Blok Sinyal

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)); }
```

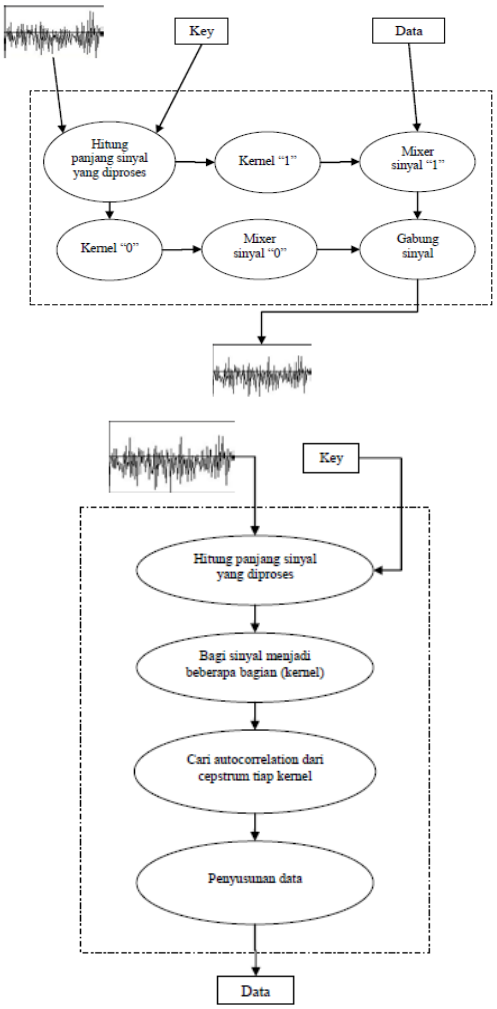
Blok – blok tersebut dikombinasikan untuk menghasilkan sinyal baru.



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 – Penyisipan dan Ekstraksi pada Echo Data Hiding

IV. Analisis Perbandingan

A. Least Significant Bit (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
- Lemahnya kekebalan terhadap manipulasi. Pada prakteknya, metode ini hanya berguna pada lingkungan digital-to-digital yang tertutup.

B. 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.

C. Echo Data 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

V. Kesimpulan dan Saran

Proteksi pada audio file dan identifikasi pemilik dari audio file tersebut merupakan hal yang cukup penting untuk masa sekarang ini, dimana penggandaan dan pembajakan file audio adalah hal yang sedang marak – maraknya terutama di Indonesia.

Untuk mengatasi hal tersebut maka dapat digunakan watermarking pada audio file. Digital watermark ini secara aman dan rahasia menggabungkan angka identifikasi yang unik dengan isi yang asli.

Pada masalah ini diperlukan teknik watermarking yang mengalami penurunan kualitas yang paling sedikit dan tidak dapat dibedakan dengan file aslinya. Teknik yang paling bagus digunakan adalah teknik *echo hiding* karena menghasilkan *file* yang tidak dapat dibedakan dengan *file* aslinya. Sehingga dengan menggunakan teknik echo data hiding ini, user yang menggunakan file audio tersebut tidak terganggu dengan efek dari watermarking tersebut.

Dengan mengetahui teknik – teknik yang dapat digunakan pada watermarking di file audio dan mengetahui kekurangan dan kelebihan masing – masing teknik, maka masyarakat atau produsen musik 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. Penjelasan di atas hanya membantu memudahkan dan memberikan penjelasan mengenai implementasi watermarking pada audio file.

References

[1] W. Bender, D. Gruhl, N. Morimoto. IBM Systems Journal. 1996. Vol 35, No 3&4.

[2] "Digital Watermarking" : http://blog.re.or.id/digital-watermarking.htm Diakses pada : 2 Maret 2011.

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

[4] http://www.snotmonkey.com/work/school/405/methods.html Diakses pada : 2 Maret 2011

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, 23 Maret 2011

ttd

Roy Indra Haryanto
13508026