Studi Perbandingan Metode-metode Digital Watermarking pada File Audio dan Pendeteksiannya

Steven Andrew / 13509061
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
andy165@students.itb.ac.id

***Abstract*—Digital watermarking dapat membantu author untuk menentukan apakah salinan hasil karya lagunya asli atau tidak (bajakan). Terdapat berbagai metode Digital watermarking pada file audio (lagu), yaitu modifikasi LSB, *spread-spectrum*, dan *echo data hiding*. Ketiga metode tersebut memiliki keunggulan dan kelemahan sendiri, terutama dari segi pengaruh kualitas audio dan *robustness* ("ketahanbantingan" watermark terhadap berbagai modifikasi audio). Dari hasil percobaan pada aplikasi yang dibuat, ditunjukkan bahwa watermark yang disisipkan dengan metode *spread-spectrum* paling *robust*.**

***Indeks Istilan*—LSB, *spread-spectrum*, steganografi, watermark.**

I. PENDAHULUAN

Seperti yang telah kita ketahui bahwa Indonesia termasuk negara dengan kasus pembajakan terbesar, terutama pembajakan lagu. Banyak kalangan muda yang ingin menikmati dan mendapatkan lagu-lagu. Sekarang ini, banyak di antara mereka yang ingin mendapatkannya dengan cara yang lebih mudah tanpa harus membayar lebih. Tidak seperti dahulu di mana mereka mendapatkannya dengan membeli kaset.

Namun sekarang kaset sudah mulai ditinggalkan dan beralih ke CD. Tetapi untuk kalangan ekonomi menengah ke bawah, harga penjualan CD cukup mahal, sehingga pembajakan CD lagu mulai merebak dan banyak yang membeli CD bajakan tersebut. Apalagi dengan pengaruh banyaknya penggunaan internet, banyak juga yang ingin mengunduh lagu gratis dari internet.

Dengan maraknya pembajakan lagu, banyak author lagu yang mengalami kerugian karena hasil karyanya dibajak. Apalagi mungkin ada seseorang atau pembajak yang mengambil hak ciptanya (mengklaim sebagai karya sendiri). Oleh karena itu, diperlukan perlindungan hak ciptanya, salah satunya yang dibahas di sini yaitu dengan *digital watermarking*.

Tidak seperti pada *image watermarking*, watermark yang disisipkan pada file audio adalah yang tidak dapat dipersepsi, yang dapat dipersepsi jarang digunakan. Secara lazim, penyisipan watermark yang tidak dapat dipersepsi dilakukan dengan teknik steganografi.

II. STEGANOGRAFI

Kerap kali kita ingin merahasiakan pesan yang dikirim tanpa diketahui orang (perantara). Hal ini dapat dilakukan dengan mengenkripsikan pesan. Namun ini dapat menimbulkan kecurigaan perantara. Maka ada cara lain, yaitu menyembunyikan pesan rahasia dalam pesan inang yang dikirim (berupa artikel, gambar, audio, dan video). Cara tersebut dinamakan steganografi. Steganografi terdiri dari dua proses, yaitu penyisipan (*embedding* atau *encoding*) dan ekstraksi (*decoding*).

Proses penyisipan dilakukan dengan menyembunyikan pesan rahasia (*embedded message*) ke dalam pesan inang (*cover-object*). Proses ini dapat menggunakan kunci (*stego-key*) dalam proses berupa penyisipan elemen-elemen pesan rahasia dalam urutan yang ditentukan dengan pembangkit bilangan acak semu, atau dalam bentuk lainnya. Pesan hasil penyisipan (*stego-object*) akan terlihat sama secara perseptual dengan pesan inang yang belum disisipkan.

Untuk mendapatkan kembali pesan rahasia dari *stego-object*, dilakukan ekstraksi dengan *stego-key* yang sama.

Steganografi yang baik memiliki kriteria sebagai berikut.

1. *Imperceptible*: Pesan rahasia tidak dapat diketahui secara perseptual.
2. *Fidelity*: Kualitas pesan inang tidak berubah signifikan akibat penyisipan.
3. *Recovery*: Pesan yang disembunyikan harus dapat diungkapkan kembali.
4. *Robustness* (opsional): Pesan tersembunyi masih dapat diekstraksi meskipun pesan inang telah diberi gangguan (berupa *noise*, modifikasi seperti pemotongan, pengubahan ukuran, dll).

Dari segi domain pemrosesan pesan, teknik-teknik steganografi dibedakan atas dua jenis sebagai berikut.

1. Domain spasial: Pemrosesan (modifikasi)

langsung dilakukan pada tiap-tiap sinyal (elemen pesan inang). Contoh: metode modifikasi LSB

2. Domain transform: Sinyal ditransformasikan terlebih dahulu dalam bentuk tertentu sebelum diproses. Contoh: metode *spread spectrum*

Dari kedua jenis tersebut, steganografi pada domain transform cenderung lebih *robust* terhadap gangguan.

Manfaat steganografi. Karena komunikasi pesan dengan kriptografi dapat dicurigai, para teroris dan pelaku kriminal sering melakukannya dengan steganografi untuk memberi instruksi-instruksi, dll secara rahasia.

Steganografi dan digital watermarking. Penyisipan watermark untuk yang tidak dapat dipersepsi jelaslah dilakukan dengan teknik steganografi. Namun dalam *watermarking*, kriteria *robustness* merupakan hal yang penting untuk mengatasi usaha-usaha untuk menghilangkannya.

III. METODE-METODE AUDIO WATERMARKING

Terdapat beberapa metode *watermarking* untuk file audio (atau metode steganografi audio). Masing-masing memiliki kelebihan dan kekurangannya sendiri, terutama dalam segi pengaruh kualitas audio, *robustness*, dan kapasitas *payload* dalam penyisipan.

A. Metode Modifikasi LSB

Algoritma *watermarking* ini menyisipkan watermark dalam data *sample* audio dengan cara mengganti nilai bit terakhirnya (*least significant bits*, LSB). Algoritma ini bekerja dalam domain spasial (atau waktu dalam audio). Algoritma ini memiliki tiga parameter, yaitu:

1. Kunci rahasia *k*, sebagai umpan untuk pembangkit bilangan acak semu (PRNG) dalam urutan pemilihan *sample*.
2. Kode koreksi galat (ECC) *c*, jika digunakan panjang pesan yang disisipkan dilipatgandakan dan galat selama pemrosesan dapat dideteksi dan dikoreksi pada ambang tertentu.
3. Parameter *m* untuk menentukan pesan rahasia dan menyisipkannya dalam sinyal audio.

B. Metode Spread Spectrum

Algoritma *watermarking* ini mentransformasikan sinyal audio terlebih dahulu ke dalam domain frekuensi menggunakan transformasi Fourier. Watermark disisipkan ke dalam koefisien-koefisien frekuensi. Algoritma ini memiliki tiga parameter, yaitu:

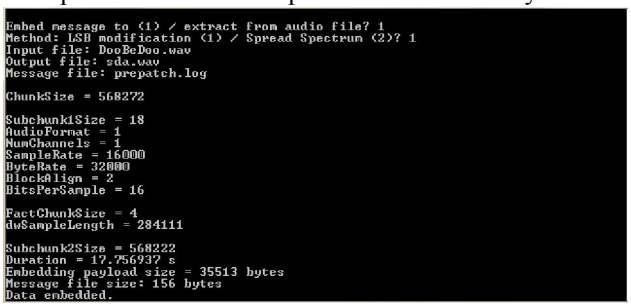
1. Parameter *m* untuk menyisipkan pesan rahasia dalam sinyal audio.
2. Kunci rahasia *k*, sebagai umpan untuk pembangkit bilangan acak semu (PRNG) dalam urutan pemilihan *sample*.
3. Parameter *l* dan *h* menentukan *bandwidth* dengan memilih batas frekuensi bawah (*l*) dan atas (*h*) untuk penyisipan. Kedua parameter tersebut menunjukkan rentang frekuensi.

IV. PERCOBAAN DAN HASILNYA

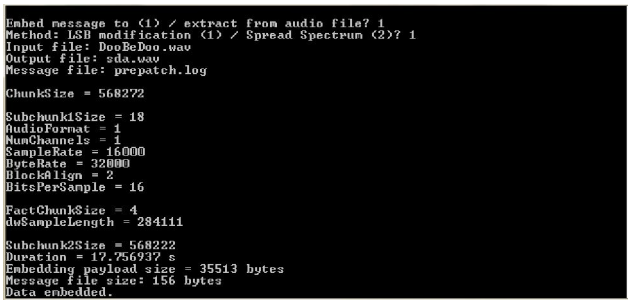
Pada percobaan ini digunakan sebuah file audio dengan ukuran 568272 bytes dan sebuah pesan watermark dengan ukuran 156 bytes yang disisipkan.

A. Metode Modifikasi LSB

Pada file audio tersebut, ukuran tiap sample adalah 4 bytes sehingga ukuran maksimum watermark yang dapat disisipkan untuk domain spasial adalah 35513 bytes.



Gambar 1. Penyisipan pesan dengan modifikasi LSB



Gambar 2. Ekstraksi pesan dengan modifikasi LSB

```
Blizzard PrePatch v2.70 compiled on
Jul  7 2003
This program patches Warcraft 3

Log created at  6:32 pm on 12/13/2008

RESULT: Prepatch successful
```

Gambar 3. Pesan watermark yang disisipkan

```
Blizzard PrePatch v2.70 compiled on
Jul  7 2003
This program patches Warcraft 3

Log created at  6:32 pm on 12/13/2008

RESULT: Prepatch successful
```

Gambar 4. Pesan watermark yang diekstraksi dari file audio yang tidak dimodifikasi

```
>æYšrÌ •üÓU½ÐG¿úŧe[÷ÿÿ1ÿÿoÿÿÿÿie ÿÿÿJ
ÿÿ 7
27ÿÿÿŠThiÿ¿ðro ÿñm?ÿÿÿëoÿÿ ÿÿÿc ÷ft  3-
ÿÿëLog                          creaõçä!ÿþ
ïÿÿó3þpmæooÿÿò/13/>00>?û
SES ÿÿú Pre át÷ûósuccusswÿý
```

```
/
```

Gambar 5. Pesan watermark yang diekstraksi dari file audio yang telah dimodifikasi dengan amplify 200% dan 50% berturut-turut.

Terlihat bahwa dengan modifikasi sedikit apapun, hasil ekstraksi akan menjadi rusak total, dengan kata lain watermark sudah tidak dapat dideteksi lagi.

Mengenai kualitas suara, mungkin terdapat sedikit noise.

V. KESIMPULAN

Penyisipan watermark dengan modifikasi LSB sangat rapuh (*fragile*) terhadap modifikasi sedikit apapun, sedangkan metode *spread spectrum* lebih "tahan banting" (*robust*) terhadap berbagai bentuk modifikasi.

DAFTAR PUSTAKA

[1] ECRYPT report: Audio Benchmarking Tools and Steganalysis

[2] Stefan Katzenbeisser, Fabien A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking*. Artech House Books, Sebastopol: O'Reilly, 1999, ch. 2,4,5.

[3] *http://en.wikipedia.org/wiki/Digital_watermarking*, diakses pada 28/2/2012.

[4] *http://en.wikipedia.org/wiki/Watermark_detection*, diakses pada 28/2/2012.

[5] *http://www.slidefinder.net/a/audio_steganography_echo_data_hiding/jeff_england_audio_steganography/24367218*, diakses pada 28/2/2012.

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, 17 Desember 2010

Steven Andrew / 13509061