IMPLEMENTASI WATERMARKING CITRA SIDIK JARI PADA AUDIO DIGITAL DENGAN FORMAT WAVE (WAV) DENGAN METODE ECHO DATA HIDING

I Gusti Pratama Putra[1], Drs. I Wayan Santiyasa, M.Si[2], I Ketut Suhartana, S.Kom,.M.Kom[3]
Jurusan Ilmu Komputer FMIPA, Universitas Udayana
Kampus Bukit Jimbaran, Bali, 80361
Email: belog2007@gmail.com[1]

ABSTRAK

Seiring dengan semakin meluasnya jaringan multimedia, maka proses pengiriman dan pengaksesan dari media audio digital semakin mudah. Kemudahan distribusi media digital melalui Internet disisi lain dapat menimbulkan permasalahan ketika media tersebut tidak terlindungi hak cipta (*copyright*). *Watermarking* menjadi salah satu solusi untuk melindungi hak cipta dari audio digital. Objek pada penelitian ini adalah *File* audio digital *Waveform Audio Format* (WAV). Data yang disisipkan berupa data sidik jari. Data sidik jari digunakan karena sidik jari memiliki sifat unik dan berbeda untuk setiap orang. Metode *Echo Data Hiding* melakukan penyisipan data kedalam data suara digital dengan menambahkan *echo* pada sinyal suara. Data yang akan disembunyikan dalam bentuk *echo* dinyatakan dengan variasi dari tiga parameter, yaitu *initial amplitude, decay rate*, dan *offset (delay). Watermarking* pada *file audio* WAV dapat mengamankan hak cipta untuk audio digital dengan menyisipkan data citra sidik jari dan mengekstrak data citra sidik jari dalam *file audio* WAV menggunakan metode *Echo Data Hiding*.
Kata kunci: *Watermarking*, *Echo Data Hiding*, WAV

ABSTRACT

The wider the multimedia network, the easier the transmission and accessibility of the digital audio media will be. However, the easy distribution of the digital media through internet may lead to problems if the copyright of the media is not protected. One of the solutions to the protection of the copyright of the digital audio is watermarking. The object of the present study is the digital audio file and the waveform audio format (WAV). The data inserted were the data in the form of fingerprints. Fingerprints were used as the data they are unique. In addition, someone's finger print is different from another's. The Echo Data Hiding Method inserted the data into the digital sound data by adding echo to the sound signal. The data hidden in the form of echo were stated to be in three parameters; they are initial amplitude, decay rate, and offset (delay). The watermarking on the audio WAV file could protect the copyright of the digital audio by inserting the data in the form of fingerprints and extracting the image of the fingerprint in the file audio WAV using the Echo Data Hiding Method.
Keywords*: Watermarking, Echo Data Hiding,WAV*

I. PENDAHULUAN

1.1 Latar Belakang

Seiring dengan semakin meluasnya jaringan multimedia, maka proses pengiriman dan pengaksesan dari media audio digital semakin mudah. Kemudahan distribusi media digital melalui internet disisi lain dapat menimbulkan permasalahan ketika media tersebut tidak terlindungi hak cipta (*copyright*). Audio digital format WAV sering digunakan sebagai master record karena file audio digital dengan format WAV memiliki kualitas yang maksimal. Untuk itu, diperlukannya suatu sistem keamanan yang dapat mengamankan audio digital dari pihak-pihak yang tidak berkepentingan. Metode yang dikembangkan

untuk mengatasi masalah tersebut adalah *digital watermarking* dengan menggunakan metode *echo data hiding*. Data yang akan disisipkan yaitu sidik jari, karena sidik jari memiliki sifat unik dan berbeda untuk setiap orang. Pada penelitian ini, watermaking citra sidik jari pada audio digital format WAV dapat digunakan untuk mengamankan dan mengidentifikasi file audio digital.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka permasalahan yang akan diangkat dalam penelitian ini, bagaimana mengimplementasikan suatu aplikasi yang mampu melakukan *watermarking* terhadap suatu media WAV dengan menggunakan Metode *Echo Data Hiding* pada proses penyisipan dan proses ekstraksi.

II. MATERI DAN METODE

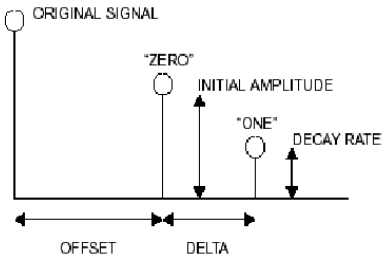
2.1 Watermarking

Watermarking adalah proses penambahan kode identifikasi secara permanen ke dalam data digital. Kode identifikasi tersebut dapat berupa teks, suara, gambar, atau video. *Watermarking* merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta atau watermark (Piarsa, 2010)

Digital watermarking adalah proses untuk menyisipkan data yang disebut dengan *watermark* ke dalam objek multimedia dengan sebuah cara sehingga *watermark* nantinya dapat dideteksi atau diekstraksi dengan tujuan penegasan kepemilkan (Terzija, 2006).

2.2. Echo Data Hiding

Metode *Data Echo Hiding* atau yang lebih sering disebut *Echo Hiding* melakukan penyisipan data kedalam data suara digital dengan menambahkan *echo* pada sinyal suara. (Bender, 1996)

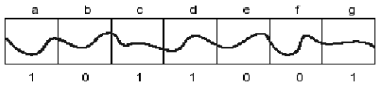


Gambar 2.1 Tiga Parameter dalam metode echo hiding (Bender, 1996)

Data yang akan disembunyikan dalam bentuk *echo* dinyatakan dengan variasi dari tiga parameter, yaitu *initial amplitude, decay rate*, dan *offset (delay)*. *Initial Amplitude* menyatakan amplitudo asal dari data suara tersebut, *decay rate* menyatakan besar *echo* yang akan diciptakan, dan *offset* menyatakan jarak antara sinyal suara dengan *echo* dalam bentuk fasa sudut dalam persamaan analog.

2.2.1. Penyisipan Watermarking

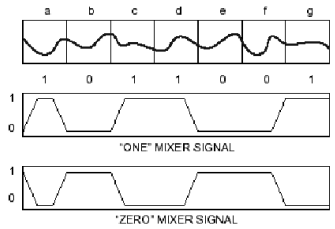
Pada peyisipan *watermark* yang terdiri lebih dari 1 bit, sinyal asli dapat dipecah menjadi beberapa bagian kecil. Setiap bagian dapat dilakukan penyisipan dengan bit yang diinginkan dengan menganggap bahwa bagian kecil tersebut sebagai sinyal yang independen. Setelah dilakukan proses *encoding echo* maka bagian bagian sinyal tersebut digabungkan kembali untuk menghasilkan sinyal awal.



Gambar 2.2 Sinyal awal dipecah menjadi beberapa bagian kecil (Bender, dkk, 1996)

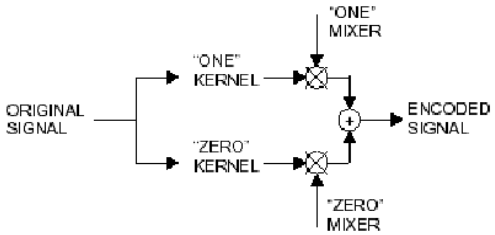
Sebagai contoh pada gambar 2.2 sinyal asli dibagi menjadi tujuh bagian yang diberi label a, b, c, d, e, f dan g. Pada bagian a, c, d, dan g akan disisipkan bit 1. Untuk itu akan digunakan kernel 1 sebagai fungsi sistem pada setiap bagian tersebut. Demikian sebaliknya bit 0 akan disisipkan pada bagian b, e, dan f maka akan digunakan kernel 0 sebagai fungsi sistem pada bagian tersebut. Untuk mencapai hasil yang tidak dapat didengar oleh pendengaran manusia, maka dapat dibuat sinyal *echo* 1 dengan melakukan pembuatan *echo* pada sinyal asli menggunakan kernel 1 dan membuat sinyal *echo* 0 dengan menggunakan kernel 0 sebagai fungsi sistem terhadap sinyal asli.

Untuk menggabungkan dua sinyal tersebut, maka dibuat dua sinyal *mixer*. Sinyal *mixer* terdiri dari nol dan satu tergantung dari bit yang ingin disembunyikan pada bagian dari sinyal asli.



Gambar 2.4 Sinyal Mixer (Bender, dkk, 1996)

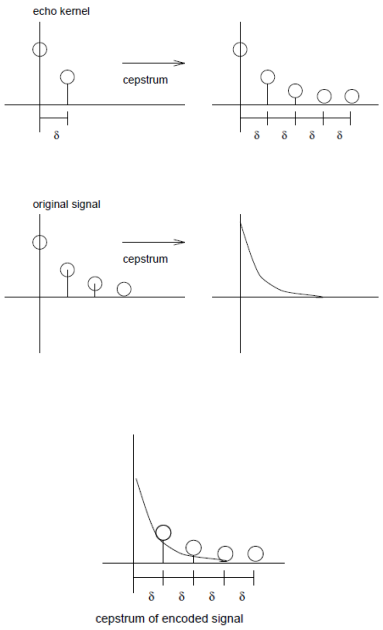
Sinyal *mixer* 0 kemudian dikalikan dengan sinyal *echo* 0 sedangkan sinyal *mixer* 1 dikalikan dengan sinyal *echo* 1, kemudian kedua hasil tersebut dijumlahkan. Sebagai catatan bahwa sinyal *mixer* 0 merupakan komplemen dari sinyal *mixer* 1 dan transisi antara masing masing sinyal adalah bertahap atau melandai.



Gambar 2.5 Proses encoding echo (Bender, dkk, 1996)

2.2.2 Ekstraksi Watermarking

Proses ekstraksi *watermark*, informasi yang disisipkan ke sinyal dengan menggemakan sinyal asli menggunakan salah satu dari dua kernel penundaan. biner satu diwakili oleh kernel gema dengan delay (δ1) detik. Biner nol diwakili oleh delay (δ0) detik. Ekstraksi informasi yang tertanam melibatkan pendeteksian jarak antara gema. Untuk memeriksa jarak antara gema dilakukan dengan memeriksa besarnya dari autokorelasi (di dua lokasi) dari cepstrum sinyal yang dikodekan.

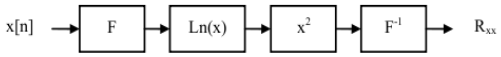


Gambar 2.6. Cepstrum Dari Sinyal Echo-Encoded (Bender, dkk, 1996)

Untuk menemukan cepstrum. Hasil mengambil cepstrum membuat jarak antara echo dan sinyal asli sedikit lebih jelas. Hasil dari cepstrum juga merupakan duplikat *echo* setiap (δ) detik (Bender, 1996). Pada Gambar 2.6, hal ini digambarkan oleh kereta impuls pada output. Selanjutnya, besarnya impuls mewakili *echo* adalah relatif kecil dibandingkan dengan sinyal asli. Dengan demikian, mereka sulit untuk dideteksi. Solusi untuk masalah ini adalah dengan mengambil autokorelasi dari cepstrum.

2.2.2.1 Autokorelasi Pada Cepstrum

Dengan menggunakan cepstrum, fungsi autokorelasi pada dirinya sendiri dari sinyal input dapat ditemukan dengan menghitung nilai cepstrum dan mengkuadratkan hasilnya. Langkah-langkah dari proses ini digambarkan pada Gambar 2.7. Sebelum mengkuadratkan hasil cepstrum, maka hasil cepstrum tersebut harus diubah terlebih dahulu dengan transformasi fourier. Lalu sebuah sistem linier x2 dilakukan pada nilai yang telah berubah ke area frekuensi tersebut. Akhirnya, fungsi invers fourier digunakan untuk mengembalikan nilai tersebut ke area waktu. (Prajetno, 2008)



Gambar 2.7 Representasi Cepstral Autokorelasi (Prajetno, 2008)

III. HASIL DAN PEMBAHASAN

3.1. PENGUJIAN

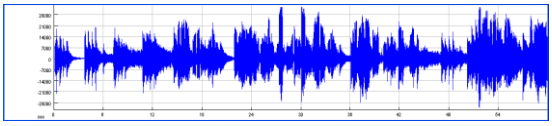
Tahap pengujian merupakan tahap untuk memastikan apakah sistem yang akan dibuat telah sesuai dengan tujuannya. Apabila sistem telah diuji dan sesuai dengan tujuan maka akan dilanjutkan pada tahap berikutnya yaitu tahap instalasi dan implementasi sistem. Pengujian sistem watermaking akan menggunakan metode SNR (*Signal to Noise Ratio)*. Selanjutnya dilakukan uji ketahanan dengan memberikan serangan pada *watermarked audio*. Dengan memberikan serangan, bertujuan untuk mengetahui *data* sidik jari yang tersisipi pada *watermarked audio* tersebut apakah mengalami gangguan atau tetap seperti awal sebelum dikenakan serangan.

3.1. Uji Coba Kualitas *Audio*

Uji coba ini dilakukan untuk mengetahui kualitas suara dari *File* WAV setelah dilakukan

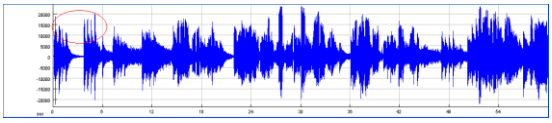
proses penyisipan data sidik jari. Uji coba kualitas ini dilakukan dengan file audio wav berukuran 5,292,044 bytes dengan durasi 60 detik. Data yang disisipkan berupa data citra sidik jari berukuran 2,382 bytes.

1. Uji coba kualitas suara menggunakan *File* yang berukuran 5,292,044 bytes dengan data yang disipkan berukuran 2,382 bytes.
   a. Uji coba dengan menggunakan *Waveform* (dB)
      - *File* audio WAV sebelum proses penyisipan



Gambar 3.1 Grafik Sinyal Suara Asli Menggunakan *Waveform* Untuk *File* 5,292,044 bytes

- File audio WAV hasil dari proses penyisipan.



Gambar 3.2 Grafik Sinyal Suara hasil Menggunakan *Waveform* Untuk *File* 5,292,044 byte

Pada gambar grafik 3.1 dan grafik 3.2. Terlihat terjadi perbedaan pada bagian awal grafik sinyal sebelum dan sesudah data sidik jari disisipkan pada file audio WAV.

3.2. Uji Coba SNR

Pengujian SNR dilakukan pada *file* audio WAV dengan durasi 60 detik. Data yang disisipkan berupa data citra sidik jari berukuran 2,382 bytes.

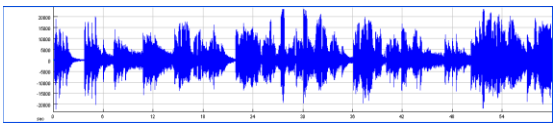
Tabel 3.1 Tabel Uji SNR dengan sample rate berbeda

Nama file audio	Sample Rate	Ukuran Sinyal audio	Ukuran data sidik jari	s (n) (db)	ŝ (n) (db)	SNR (db)
Lagu.wav	8000 Hz	5,292,044 bytes	2,382 bytes	77.03	74.26	28.88
Lagu.wav	11025 Hz	5,292,044 bytes	2,382 bytes	77.04	74.27	28.88
Lagu.wav	22050 Hz	5,292,044 bytes	2,382 bytes	77.05	74.28	28.89
Lagu.wav	44000 Hz	5,292,044 bytes	2,382 bytes	77.07	74.31	28.92

3.3. Pengujian terhadap ketahanan audio watermaked

Pengujian ketahanan *watermarked audio* dilakukan dengan cara membandingkan *watermark* asal dan *watermark* hasil ekstraksi dengan meberikan serangan pada audio yang telah diwatermark. Berikut adalah serangan-serangan yang akan digunakan untuk menguji *watermarked audio*:

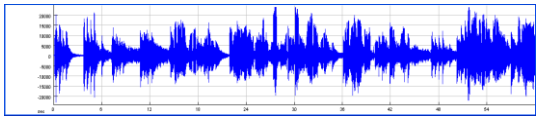
1. Pada serangan *resampling*, perubahan frekuensi *sampling* yang digunakan adalah 22050 Hz sedangkan frekuensi *sampling* berkas audio asal adalah 44100 Hz.



Gambar 3.3. Grafik Sinyal *Watermarked Audio* frekuensi 44100 Hz

Gambar. 3.4 Data Citra Sidik Jari Hasil Ekstraksi *Watermarked Audio* Frekuensi 44100 Hz

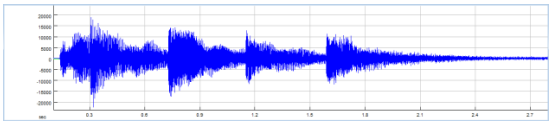
Pada serangan *resampling*, sampling frekuensi *watermarked audio* diubah menjadi 22050 Hz. Resample dilakukan dengan menggunakan bantuan Aplikasi Audacity. Berikut adalah gambar sinyal *audio watermark* yang telah diresample menjadi 22050 Hz:



Gambar 3.5 *Watermarked Audio* dengan *Resample* 22050Hz

Watermarked audio dengan sampling frekuensi 22050 Hz kemudian diekstraksi dengan menggunakan metode yang sama. Pada saat proses ekstraksi, data citra sidik jari tidak dapat diekstraksi karena adanya perubahan data pada *watermarked audio.*

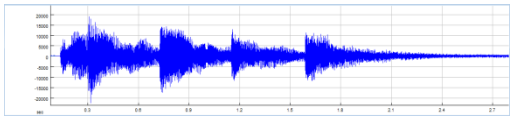
2. Pada serangan penambahan *noise*, sinyal *watermarked audio* pada domain waktu akan ditambahkan *noise* dengan amplitudo yang kecil di sepanjang audio.



Gambar 3.6 Grafik Sinyal *Watermarked Audio* Sebelum Ditambahkan *Noise*

Gambar. 3.7 Data Citra Sidik Jari Hasil Ekstraksi *Watermarked Audio* Sebelum Ditambahkan *Noise*

Pada serangan penambahan *noise*, sinyal *watermarked audio* pada domain waktu akan ditambahkan *white noise* dengan amplitudo 0,1 berdurasi 0,01 detik.



Gambar 3.8 Grafik Sinyal *Watermarked Audio* Sesudah Ditambahkan *Noise*

Watermarked audio dengan ditambahkan *white noise* dengan amplitudo 0,1 berdurasi 0,01 detik, kemudian diekstraksi dengan menggunakan metode yang sama. Pada saat proses ekstraksi, data citra sidik jari tidak dapat diekstraksi karena adanya perubahan data pada *watermarked audio.*

IV. KESIMPULAN

4.1. Kesimpulan

Kesimpulan yang dapat diambil dari penelitian yang telah dilakukan adalah sebagai berikut:

1. *Watermarking* pada *file audio* WAV dapat mengamankan hak cipta untuk

audio digital dengan menyisipkan data citra sidik jari dan mengekstrak data citra sidik jari dalam *file audio* WAV menggunakan metode *Echo Data Hiding*, sehingga dapat mengamankan audio digital dari pihak-pihak yang tidak berkepentingan.

2. Berdasarkan pengujian terhadap kualitas *audio watermark*, nilai SNR berpengaruh terhadap sampling frekuensi. Pada table 4.3 terlihat, perubahan sampling frekuensi pada *audio watermark* dapat merubah nilai SNR pada audio *watermark.*
3. Berdasarkan hasil pengujian ketahanan *audio watermark*, pada aplikasi pengamanan *file audio* yang dibangun menggunakan metode *echo data hiding*, serangan perubahan *resample* dan penambahan *noise* pada *watermarked audio* dapat mempengaruhi data sidik jari yang disisipkan pada *file audio watermark.*

DAFTAR PUSTAKA

[1] Bahri, K. S. Sjachriyanto, W. 2008. *Teknik Pemrograman Delphi*. Bandung : Informatika bandung.

[2] Bender, Walter, Daniel Gruhl, & N. Morimoto. 1996. *Techniques for data hiding.* Ibm Systems Journal, Vol 35, Nos 3&4, 1996

[3] Hadi, Ronal. 2010. *"Studi dan Evaluasi Watermarking Audio Digital Dengan Metode Removal DC".* 17 Jurnal Informatika, Volume 5 Nomor 2, November 2009

[4] Kendall, Kenneth E dan Julie E. Kendall. 2006. "*Analisis dan Perancangan Sistem*". Edisi Kelima. Indeks. Jakarta.

[5] Piarsa, Nyoman dan Dharmadi, Ady . 2010. "*Implementasi Watermarking Pada Suara Digital Dengan Metode Echo Hiding".* Jurnal Vol. 9 No.2 Juli - Desember 2010.

[6] Putra, Darma. 2010. Pengolahan Citra Digital. Yogyakarta: CV Andi Offset.

[7] Setiawan, Budi, Soegijoko, Soegijardjo, Sugihartono dan Tjondronegoro, Suhartono. 2006. "*Model Sinusoida Secara Segmental Untuk Pengkodean Sinyal Suara".* Makara, Teknologi, Vol. 10, No. 2, November 2006: 61-66.

[8] Sugiono, Prajetno dan Setiawan, Yuantoro. 2008. "*Watermarking Pada File Audio PCM Wave Dengan metode Echo Data Hiding".* Konferensi Nasional Sistem dan Informatika 2008; Bali, November 15, 2008 KNS&I08-019

[9] Terzija, Natasa. 2006. *Robust Digital Image Watermarking Algorithms for Copyright Protection*. Universität Duisburg-Essen.

[10] Tresnani, Lestari. 2010. *"Studi Mengenai Echo Hiding Steganografi".* http://www.informatika.org (diakses 15 november 2011)