Data Hiding Through Media Audio

Sumi Khairani
Program Studi Teknik Informatika
Sekolah Tinggi Teknik Harapan
adek_sumi@yahoo.co.id

Abstract

Audio watermarking can use with various ways. Firstly, it have used for proving of ownership, production of information, copyright information in a form of a watermark, and it have routed directly in the recording. Specific owners have different insertion information. It can also be used for controlling access, watermark becomes a trigger to play music. Keeping track of unauthorized copies is a very important application. Personal information have inserted into the music. It used as numbers for customers to discover music.

Keywords: *Data Hiding, Audio watermarking , copyright*

1. PENDAHULUAN

Prinsip dasar *watermarking* bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan, atau data lain, pada materi multimedia tanpa mempengaruhi kualitasnya. Jadi pada citra (*image*) digital, mata kita tidak bisa membedakan apakah citra tersebut disisipi *watermarking* atau tidak. Demikian pula jika kita terapkan pada audio atau musik, telinga kita tidak bisa mendengar sisipan informasi tadi. Sehingga pada teknologi ini dikenal suatu persyaratan bahwa *watermarking* haruslah *imperceptible* atau tidak terdeteksi oleh indera penglihatan (*Human Visual System* / HVS) atau indera pendengaran (*Human Auditory System* / HAS). Sementara dokumen asli dan *watermarking* kita simpan dan rahasiakan, dokumen yang sudah disisipi *watermarking* bisa dipublikasikan. Teknologi *watermarking* merupakan suatu solusi didalam melindungi hak cipta kepemilikan terhadap data-data digital. Dengan perkembangan komputer digital dan perangkat-perangkat lainnya yang serba digital, telah membuat data digital banyak digunakan.

Ada beberapa faktor yang membuat data digital (seperti audio, citra, video, dan text) banyak digunakan, antara lain [1]:

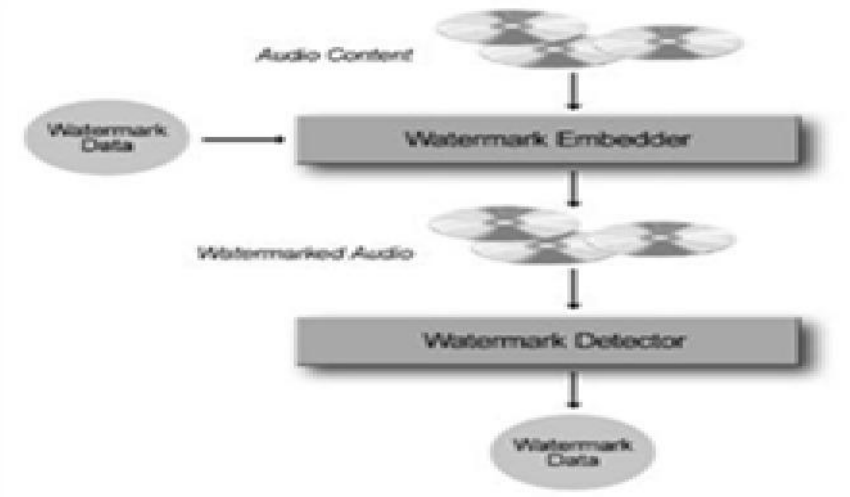
1. Mudah diduplikasi dan hasilnya sama dengan aslinya.
2. Murah untuk penduplikasian dan penyimpanan.
3. Mudah disimpan untuk kemudian diolah atau diproses lebih lanjut.
4. Mudah didistribusikan, baik dengan media disk maupun melalui jaringan seperti Internet.

Watermarking merupakan suatu bentuk aplikasi dari *Steganography* yang merupakan ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain. *Watermarking* ini agak berbeda dengan tanda air pada uang kertas. Tanda air pada uang kertas masih dapat dilihat oleh mata telanjang manusia (pada posisi kertas tertentu) tetapi *watermarking* pada media digital disini dimaksudkan agar tidak akan dirasakan kehadirannya oleh manusia tanpa alat bantu mesin pengolah digital seperti komputer dan sejenisnya.

Watermarking ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Dengan adanya kekurangan inilah, metoda *watermarking* ini dapat diterapkan pada berbagai media digital. Jadi *watermarking* merupakan suatu cara untuk penyembunyian atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran), dan mampu menghadapi proses-proses pengolahan sinyal digital sampai pada tahap tertentu.

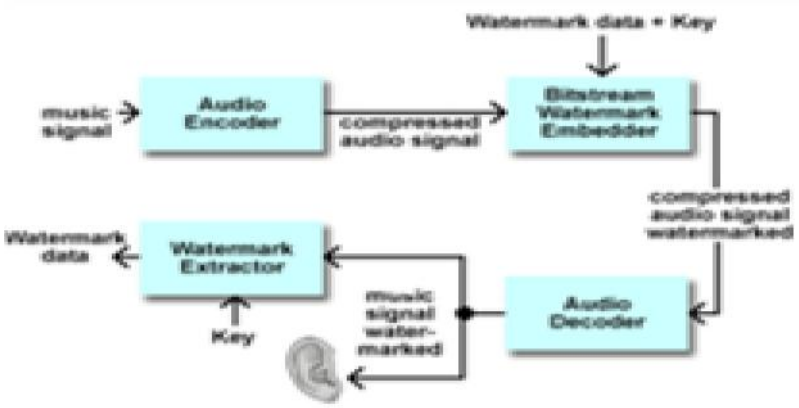
Sebenarnya, kata *watermark* berasal dari industri kertas. Suatu *watermark* adalah suatu desain timbul ke dalam secarik kertas selama produksi dan digunakan untuk identifikasi kertas dan pembuatan kertas. *Watermark* itu dapat dilihat ketika kertas diarahkan pada cahaya. Desain itu bisa beberapa pola atau gambaran-gambaran yang menandai adanya mutu merek dagang dari kertas. Lalu diperkenalkan kata *watermark* di dalam field digital. *Watermark* adalah suatu kode identifikasi yang membawa informasi tentang pemilik hak cipta, pencipta suatu pekerjaan dan konsumen-konsumen yang diberi hak juga.

Watemark adalah suatu tanda yang tidak kelihatan dan secara permanen menempel ke dalam data digital untuk perlindungan hak cipta dan sebagai tanda apabila data sudah dirusak. Dokumen elektronik yang diberi *watermark* dapat berupa gambar digital, audio atau bahkan video. Tetapi penulis hanya berkonsentrasi pada audio *watermark* berarti suatu *watermark* yang menempel dalam suatu arus audio untuk mengidentifikasi asal-muasalnya. Suatu sistem pendeteksi *watermark* pada file audio dapat dilihat pada gambar di bawah ini.



Gambar 1. Penyisipan *Watermark* Pada File Audio [5]

Penyisipan *watermark* pada file audio merupakan suatu cara untuk penyembunyian atau penanaman data/informasi tertentu kedalam suatu data digital tetapi tidak diketahui kehadirannya oleh indra penglihatan/indra pendengaran manusia dan mampu menghadapi proses pengolahan sinyal digital sampai pada tahap tertentu. Metode *watermarking* untuk audio ini menggunakan metode *Least Significant Bit* (LSB) yaitu metode yang mengubah nilai bit terakhir sehingga menghasilkan audio yang sangat mirip dengan aslinya. Penyisipan dilakukan dengan menggunakan suatu kunci pribadi untuk menyandi watermark digital kedalam audio, kemudian kunci publik digunakan untuk dekode watermark audio.



Gambar 2. *Bitstream P*emberian *Watermark* [5]

Di atas ini adalah gambar *watermark* audio ditempelkan ke dalam file termampatkan seperti MP3. Mekanisme itu disebut bitstream pemberian *watermark.* Caranya dengan menyisipkan file *watermark* kedalam file audio tanpa mengurangi mutu file audio dan mengubah kualitas dan kapasitasnya. Harus hampir tidak ada perbedaan antara audio yang diberi *watermark* dan yang tidak diberi *watermark.*

Beberapa persyaratan dasar yang harus dimiliki oleh suatu *watermark* audio yaitu [6]:

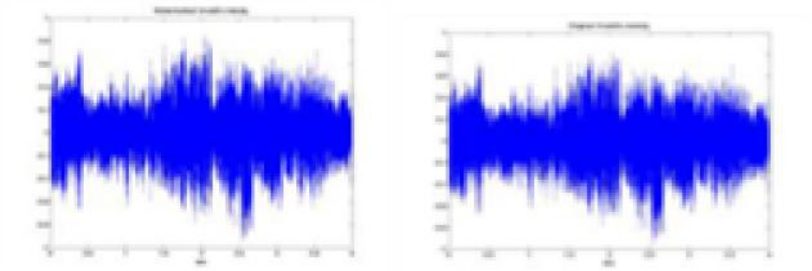
A. *Bersifat biaya komputasional rendah*
Biaya komputasional rendah berarti tidak memerlukan waktu bagi *watermark* untuk ditempelkan dan dideteksi. Ini merupakan suatu faktor yang penting di dalam sistim *watermark.*

B. *Tanpa Distorsi dari Sinyal Asli dan Perubahan Bentuk*
Watermark disisipkan di dalam file audio itu sama sekali tidak mengurangi mutu file audio dan mengubah bentuk. Jika suatu *watermark* ditempelkan dalam satu file MP3, pelanggan itu dapat juga memainkannya di beberapa player yang mendukung file MP3, mereka tidak perlu membeli player yang baru kembali.

C. *Serta Ketahanan dari Hal yang Tak Dapat Diketahui*
Ketahanan mengacu pada kemampuan untuk mendeteksi *watermark* setelah operasi pengolahan sinyal yang umum dan serangan-serangan lainnya yang mungkin bisa terjadi. Contoh dari operasi yang umum di file audio yakni memasukkan didalamnya suara gaduh (*noise*), pengurangan (*kompressi*), penyesuaian volume atau normalisasi, konversi digital ke analog dan sebagainya.

Sejauh ini terjadi penyerangan yang berbeda pada *watermark* audio. Serangan yang terjadi adalah penyerangan gabungan, penyerangan sinyal dan penyerangan yang tidak terdeteksi. Suatu serangan gabungan mempunyai salinan dari file audio dengan *watermark* yang sama, penyerang merata-ratakan nilai *watermark* dari sinyal audio. Sebagai suatu nilai perhitungan pada jenis serangan, dan menjadi lebih baik untuk menyisipkan *watermark* lebih dari satu kali dalam satu file audio atau menyisipkan *watermark* yang berbeda untuk file-file yang berbeda. Sinyal penghancur penyerang mengacu pada operasi sinyal yang berbeda seperti lossy kompressi, modulasi, konversi, dll. Sekarang dimungkinkan untuk menyisipkan *watermark* lebih dari satu pada suatu file audio.
Jika seseorang mencuri file yang diberi *watermark* dan file *watermark* tersebut telah diberi kunci pribadi. Bisa dipastikan bahwa file yang dicuri tersebut dapat ditemukan pemiliknya karena telah diberikan *watermark.* Bagaimanapun, satu serangan pada file akan memeriksa prosedur penciptaan. Dengan demikian sulit untuk memutuskan siapa sebagai pemilik riil dari file audio. Properti yang lain dari audio *watermark* adalah hal tak dapat diketahui (*imperceptibility*). Harus hampir tidak ada perbedaan antara yang diberi *watermark* dan yang tidak diberi *watermark.* Pada gambar ada suatu grafik gelombang suara dari musik yang sama dengan *watermark* dan yang tidak diberi *watermark.*

Seperti yang terlihat, hanya ada sedikit perbedaan yang tidak diperhatikan karena hanya terjadi di sepintas lalu dan dapat juga diabaikan.

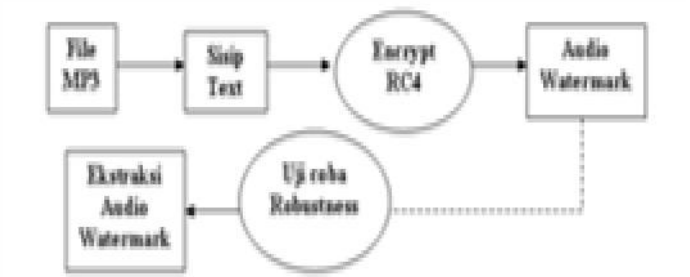


Gambar 3. Gelombang Suara Dari File Audio Yang Sama

Audio *Watermarking* dapat digunakan dengan banyak cara. Pertama dapat digunakan untuk pembuktikan dari kepemilikan, informasi selama produksi, informasi hak cipta dalam suatu bentuk *watermark*, dapat diarahkan secara langsung di dalam perekaman. Kepemilikan spesifik mempunyai informasi penyisipan yang berbeda. Dapat juga digunakan untuk kendali akses, *watermark* menjadi suatu pemicu untuk untuk memainkan musik. Melacak salinan tidak sah adalah suatu aplikasi yang sangat penting. Informasi pribadi disisipkan ke dalam musik. Informasi pribadi bisa dijadikan nomor bagi pelanggan untuk menelusuri musik. Jika musik seperti itu ditemukan di dalam internet, maka *watermark* akan dikacaukan dan nomor pelanggan bisa dikenal untuk tindakan-tindakan hukum selanjutnya.

2. METODOLOGI

Penelitian dan pengujian yang dilakukan pada sebuah file MP3 adalah untuk mempraktekkan hasil dari analisa yang bertujuan untuk menguji keberhasilan dari metode penyisipan file *watermarking* yang telah dipilih, penganalisaan di lakukan dengan cara membandingkan teori dan praktek sehingga diperoleh gambaran yang jelas tentang persamaan dan perbedaan diantara keduanya.



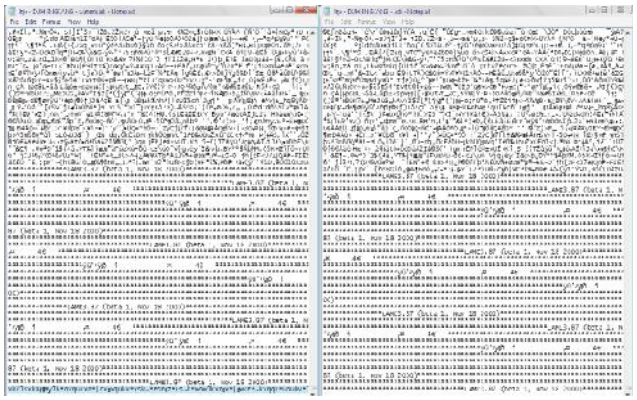
Gambar 4. Konsep Dasar Aplikasi Penyisipan Text pada File MP3 [4]

Gambar di atas memperlihatkan prosedur awal dari file MP3 yang akan disisipkan dokumen text yang dijadikan file *watermarking*. Caranya text yang disisipkan pada file MP3 seolah berantakan, jika ada seseorang yang tidak memiliki wewenang mengakses file MP3 dan coba menghapusnya. Namun bila terjadi hal demikian maka file MP3 itu akan mengalami kerusakan dan tidak dapat dimainkan lagi dengan bantuan *audio player* apapun. Teknik enkripsi ini juga digunakan agar kapasitas file tidak mengalami perubahan yang signifikan jika disisipi text dan tentu saja agar keberadaan text yang menyisip pada file MP3 tersebut tidak diketahui oleh panca indra manusia (*robustness*). Sebelumnya dibuatkan password agar akses text yang dimasukkan hanya diketahui oleh pemegang hak cipta. Selanjutnya merupakan konsep dasar penyisipan teks yang di *encrypt* dengan RC4 lalu menjadi file yang ter*watermark* yang diuji coba untuk mengetahui *robustness* pada file MP3 dengan berbagai *noise/distorsi* yang dilakukan penulis.

3. UJI COBA

Secara logika, jika text yang dijadikan file *watermark* berukuran 1000 bit maka, kapasitas file juga akan mengalami perubahan ukuran, tetapi dengan dilakukan enkripsi pada text, maka ukuran file hanya mengalami perubahan yang tidak berarti, bahkan tidak mempengaruhi kualitas suara sedikitpun. Berikut ini ini merupakan isi dari file MP3 yang digunakan pada uji coba ini. Pada file MP3 yang terwatermark terlihat pada bit terakhir ada penyisipan text dan terlihat acak, hal ini terjadi karena enkripsi pada text.

File MP3 yang disebelah kiri merupakan file MP3 yang diberi watermark, sedangkan file MP3 yang disebelah kanan merupakan file MP3 yang asli. File MP3 ini dibuka dengan notepad yang dapat melihat text yang terlihat acak pada file MP3 yang diuji coba oleh penulis.



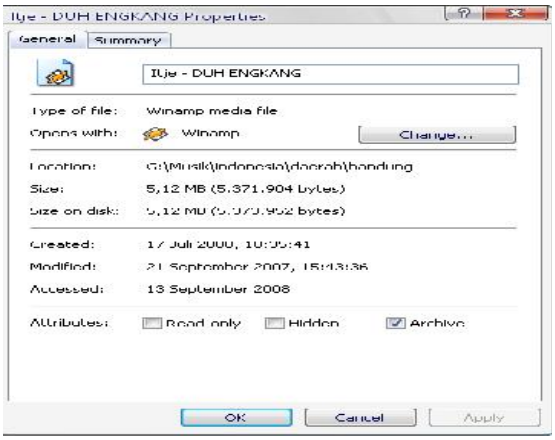
Gambar 5 Penyisipan Text Pada Bit Terakhir (kiri)

Pengujian tingkat keberhasilan dengan analisis *robustness* akan terlihat pada pengujian ini. File MP3 akan dikompressi dengan tool kompressi yang penulis anggap cocok dengan penelitian yang dilakukan. Awal mula program dijalankan terlihat tampilan sebagai berikut:

Gambar 6. Tampilan Awal Aplikasi MP3 *watermark*

Masuk ke proses selanjutnya adalah membuka file audio dan memasukkan *password*, ,kemudian melakukan pengetikan pesan secara manual tanpa batasan pada *interface* yang telah dibangun terakhir melakukan penyimpanan file mp3.

Berikut ini merupakan ukuran file yang ada sebelum terjadinya penyisipan program *watermark* berupa dokumen text.

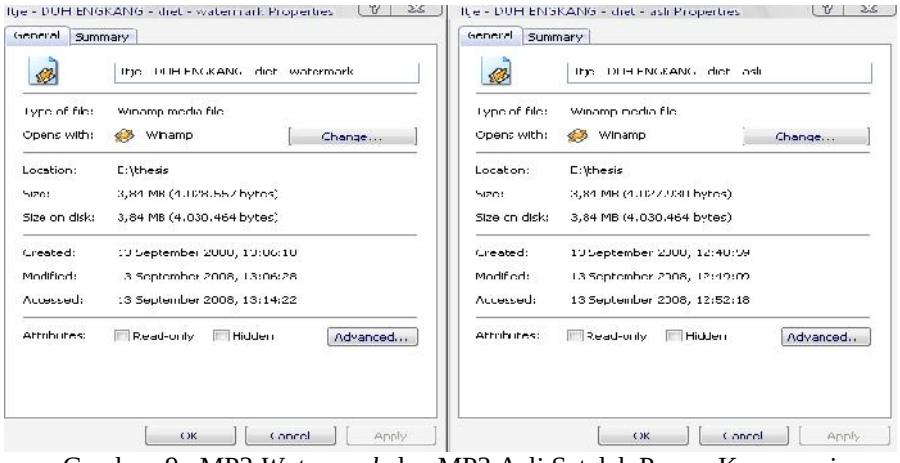


Gambar 7. Ukuran File MP3 Sebelum Penyisipan

Selanjutnya merupakan tampilan file ketika sudah terjadinya penyisipan.

Gambar 8. Ukuran File MP3 Setelah Penyisipan

Kalau diperhatikan secara sekilas tidak terlihat adanya perubahan pada kapasitas file, tetapi jika dilihat lebih teliti maka akan tampak perubahan yang tidak terlalu mencolok pada file MP3 itu. Proses berikutnya adalah melakukan kompressi pada file MP3 yang telah disisipkan label *watermark* yang ukuran awalnya 5.12 MB menjadi 3.84 MB. Hasil tersebut dapat terlihat pada gambar di bawah.



Gambar 9. MP3 *Watermark* dan MP3 Asli Setelah Proses Kompressi

4. KESIMPULAN

Audio watermarking dapat digunakan untuk pembuktian dari kepemilikan informasi selama produksi perekaman data digital juga sebagai kendali akses untuk melacak salinan yang tidak sah dengan menyisipkan informasi pribadi yang digunakan untuk menelusuri musik yang original (*copyright-labeling*) sebagai bukti otentik kepemilikan hak cipta kekayaan intelektual. Metode *Least Significant Bit* (LSB) yang dipilih merupakan yang paling sederhana dan yang paling tidak tahan terhadap berbagai serangan walaupun dilakukan sekecil mungkin seperti kompressi yang dilakukan pada penelitian ini..

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Ketua Jurusan Sistem Informasi FST Universitas Islam Negeri Sumatera Utara Bapak M. Irwan Padli Nasution dan Ibu Dharmawati, S. Pd, M. Hum yang telah memberikan banyak dukungan, saran dan kritik terhadap penelitian ini. Semoga allah SWT melimpahi kebaikan dan keberkahan kepada keduanya karena selalu memberikan motivasi dan semangat bagi saya untuk selalu melakukan Tridharma.

BAHAN REFERENSI

[1] Munir, Rinaldi. 2004. *Pengolahan Citra Digital*. Informatika, Bandung.
[2] Munir, Rinaldi. 2004. *Kriptografi*. Informatika. Bandung.
[3] Angel, Edward, Interactive. 2005. *Computer Graphics - A Top Down Approach Using Open GL*, Pearson, Addison Wesley.
[4] I. Wiseto P. Agung, Digital Watermarking . *Teknologi Pelindung HAKI Multimedia Elektro Indonesia*, Nomor 35, Tahun VI, Februari 2001.
[5] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett. 2004. *Steganography And Digital Watermarking*, School of Computer Science, The University of Birmingham.
[6] Suhono H. Supangkat, Kuspriyanto, Juanda. 2007. *Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital*. Departemen Teknik Elektro, Institut Teknologi Bandung
[7] Nasution, Muhammad Irwan Padli, 2008, Urgensi Keamanan Pada Sistem Informasi, *Jurnal Iqra' Volume 02 Nomor 02*, https://www.researchgate.net/publication/305726044_URGENSI_KEAMANAN_PADA_SISTEM_INFORMASI