Aplikasi Steganografi dan Digital Watermark pada File Audio

Riffa Rufaida / 13507007[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*riffa.rufaida@gmail.com*

***Abstract*— Perkembangan teknologi membuat distribusi file audio digital tidak terkendali dan tidak mengindahkan adanya hak cipta dari pemiliki legalnya. Hal ini membuat label mengalami kerugian dan hak cipta dari pembuatnya dilanggar. Oleh karena itu, dibutuhkan mekanisme untuk membantu mengawasi perkembangan file audio digital resmi untuk membantu penyebaran file audio digital secara resmi dan legal. Salah satu cara yang dapat diterapkan adalah dengan menyisipkan digital watermark pada file audio yang merupakan aplikasi dari steganografi. Mekanisme ini dapat dimanfaatkan untuk menjaga jalur legal dari persebaran file audio resmi.**

***Index Terms* — audio watermark, aplikasi, DRM, copyright**

I. PENDAHULUAN

Musik merupakan bagian penting yang tidak bisa hilang kehidupan manusia. Secara umum music menjadi alat untuk menyalurkan ekspresi jiwa, baik bagi pembuatnya maupun penikmatnya. Musik sendiri telah menjadi bagian dari industry penting hiburan di dunia ini. Teknologi pula telah mempermudah distribusi music dari satu tempat ke tempat lain. Musik ini didistribusikan dengan format digital baik di dalam CD, DVD, maupun file digital pada *gadget*.

Distribusi ini menjadi tidak terkendali dengan adanya internet dan tidak mengindahkan adanya hak cipta yang terkandung di dalam music dengan format digital yang didistribusikan tersebut. Hak cipta merupakan hak eksklusif yang diberikan kepada pencipta dari suatu karya original, termasuk hak untuk mengopi, mendistribusi, maupun mengadaptasi karya tersebut. Seorang artis yang melepaskan album lagu melalui sebuah label, maka hak cipta untuk memperbanyak terdapat pada label tersebut. Di dalamnya telah ada perjanjian antara label dan artis untuk pengaturan pembagian keuntungan. Pada saat CD album dibeli oleh seseorang, orang tersebut tidak memiliki hak untuk memperbanyak dan menyebarkannya ke orang lain.

Keadaan saat ini di saat sebuah album atau single beredar, versi digital sudah dapat tersedia di internet untuk diunduh oleh khalayak ramai. Label mengalami kerugian karena penurunan penjualan CD resmi. Oleh karena itu, telah dilakukan upaya-upaya berupa perlindungan file audio digital pada CD yang diproduksi label untuk mencegah orang memperbanyak isi CD tersebut. Hal ini dikenal dengan DRM atau Digital Restriction Management. Hal ini mencegah sebuah file audio untuk dapat dikopi atau dijalankan di tempat lain selain menggunakan tempat/player yang ditentukan sehingga mencegah diperbanyaknya file audio digital. Meskipun saat ini label telah menghilangkan file audio dengan DRM, terdapat salah satu mekanisme yang menjadi bagian dari DRM, yaitu digital watermark pada file audio. Digital watermark dapat digunakan untuk tujuan berbeda yang termasuk di dalamnya, merekam pemiliki hak cipta, merekam distributor, merekam jalur distribusi, mengidentifikasi pembeli. Hal-hal ini dapat membantu menyediakan bukti legal dalam manajemen hak cipta atas file audio digital.

I.1 Steganografi

Steganografi merupakan ilmu dan seni menyembunyikan informasi dengan cara menyisipkan pesan rahasia di dalam pesan lain. Sedangkan steganografi digital merupakan steganografi pada data digital dengan menggunakan komputer digital.

Steganografi memiliki properti sebagai berikut :

1. *Embedded message*
   Pesan yang disembunyikan, dapat berupa teks, gambar, audio, video, dan lain-lain.
2. *Cover-object (Covertext)*
   Pesan yang digunakan untuk menyembunyikan *embedded message*, dapat berupa teks, gambar, audio, video, dan lain-lain.
3. *Stego-object (Stegotext)*
   Pesan yang telah berisi pesan *embedded message.*
4. *Stego-key*
   Kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari *stegotext.*

Kriteria dari steganografi yang baik adalah sebagai berikut :

1. *Imperceptible*
   Keberadaan pesan rahasia tidak dapat dipersepsi.
2. *Fidelity*

Mutu dari *cover-object* atau *covertext* tidak berubah terlalu jauh setelah disisipi *embedded message.*

3. *Recovery*
   Data yang disembunyikan harus dapat dikembalikan.

I.2 Digital Watermark

Dokumen digital memiliki karakter mudah didistribusikan, mudah diedit, serta tepat sama jika digandakan. Hal ini menyebabkan tidak ada perlindungan terhadap kepemilikan, hak cipta, maupun hak atas kekayaan intelektual. Salah satu solusi yang ada untuk perlindungan terhadap suatu karya digital merupakan aplikasi dari steganografi, yaitu berupa *digital watermark*.

Digital watermark merupakan penyisipan informasi (*watermark*) yang menyatakan kepemilikan data multimedia. Informasi yang disisipkan dapat menyatakan label kepemilikan dari suatu dokumen digital. Hal ini membuat setiap penggandaan dari dokumen digital atau data multimedia akan membawa informasi *watermark* di dalamnya. Informasi *watermark* ini tidak dapat dihapus atau dibuang karena telah disisipkan dan berada di dalam data digital maupun terintegrasi di dalam data digital.

Pada aplikasi di kehidupan nyata, digital watermark pada file audio akan memiliki beberapa macam pemanfaatan yang berbeda-beda, di antaranya adalah :

- perlindungan hak cipta,
- kopi control,
- merekam rantai distribusi,
- mengidentifikasi pembeli music.

DRM yang akan dibahas pada makalah ini berfokus kepada pemanfaatan steganografi dan audio *watermark* pada perlindungan hak cipta.

Proses yang terdapat *digital watermarking* terdiri atas proses ekstraksi dan deteksi. Proses ekstraksi berarti mengambil kembali (*recover/reveal*) bit informasi *watermark* dari data multimedia. Proses ini akan membutuhkan proses pembandingan dengan *watermark* asli untuk menentukan kecocokannya. Sedangkan proses deteksi akan menentukan apakah data multimedia yang dimaksud mengandung informasi *watermark* atau tidak.

Digital watermark pada penggunaannya memiliki perbedaan dengan steganografi, tetapi *digital watermark* ini merupakan pengaplikasian dari steganografi pada dokumen *digital.* Terdapat dua jenis dari *watermarking*, yaitu :

1. *Fragile watermarking*
   Watermarking ini memiliki tujuan untuk menjaga integritas atau orisinalitas dari sebuah data *digital*.
2. *Robust watermarking*
   Watermarking ini memiliki tujuan untuk menyisipkan label kepemilikan dari sebuah data *digital*.

I.3 DRM

DRM, *Digital Rights Management* atau *Digital Restrictions Management*, merupakan teknologi untuk mengontrol akses dan membatasi penggunaan dari sebuah data *digital.* Ide awalnya berupa perlindungan terhadap hasil karya manusia dalam bentuk digital melalui jalur legal. Perlindungan ini dibutuhkan karena persebaran media atau konten digital melalui computer mengalami peningkatan tajam dengan adanya internet dan tidak mengindahkan adanya hak cipta atas konten tersebut. DRM memungkinkan pihak-pihak yang memiliki hak legal atas suatu karya digital memperoleh apa yang menjadi haknya seiring berkembangnya penggunaan dan persebaran data digital yang dimilikinya. DRM merupakan suatu mekanisme yang berusaha membatasi dan melawan maraknya pembajakan saat internet berkembang.

DRM secara konsep membatasi akses penggunaan dari sebuah konten digital dengan berbagai metode, yang biasanya berujung pada pemanfaatan suatu aplikasi ekslusif untuk sebuah konten digital tertentu. Contoh aplikasi dan metode yang digunakan di antaranya :

- Sebuah server e-book membatasi hak akses, hak kopi dan hak cetak berdasarkan hak cipta dari pemegang konten digital.
- Sebuah studio film menggunakan perangkat lunak pada DVD yang membatasi pengkopian sebanyak dua buah saja.
- Sebuah label music memroduksi CD yang mengandung bit informasi yang dapat menyulitkan perangkat lunak untuk mengkopi CD tersebut.

DRM menjadi sebuah topic hangat pada pertengahan tahun 2002. DRM pada akhirnya menjadi sebuah proteksi penuh akan sebuah konten digital, mulai dari distribusi hingga cara penggunaan dari user akan konten digital tersebut.

II. AUDIO WATERMARK

Algoritma pada audio *watermark* dikarakteristikan ke dalam lima properti penting. Properti tersebut adalah :

1. *Perceptual transparency*
2. *Watermark bit rate*
3. *Robustness*
4. *Blind/informed watermark detection*
5. *Security*

Keseluruhan algoritma yang berkembang dalam audio watermark memanfaatkan property perceptual dari sistem pendengaran manusia untuk memasukkan watermark. Menyisipkan informasi tambahan ke dalam

audio merupakan pekerjaan yang lebih tidak rumit dibandingkan *watermark* pada citra digital, karena sistem pendengaran manusia yang lebih unggul dari pada sistem penglihatan. Hal tersebut membuat jumlah data yang dapat disisipkan lebih sedikit jumlahnya daripada penyisipan pada citra digital. Di sisi lain, serangan pada algoritma *watermark* pada citra dan video tidak dapat digunakan pada audio *watermark.*

II.1 Properti pada Audio Watermark

Algoritma pada *watermark* dapat dikarakteristikan dengan beberapa property. Sebuah property akan memiliki derajat kepentingan yang relative, tergantung dengan aplikasi yang digunakan. Ini karena *watermark* pada konten audio akan berefek kepada aplikasi yang digunakan untuk menjalankan konten digital tersebut. Pada saat berkembangnya DRM pada file audio, banyak muncul CD dengan aplikasi *player* yang spesifik untuk memainkannya. Sebuah label tertentu yang mengaplikasikan mekanisme yang berbeda akan memiliki aplikasi pemutar yang berbeda. Aplikasi beserta mekanisme yang digunakan yang akan menentukan derajat kepentingan dari property-properti pada audio *watermark*. Properti tersebut adalah :

1. *Perceptual transparency*
   Algoritma untuk audio *watermark* diharapkan berhasil memasukkan data tambahan tanpa memberi pengaruh pada kualitas sinyal audio yang dipersepsi oleh pendengarnya. Level kebenaran dari suatu algoritma *watermark* biasanya didefinisikan sebagai kesamaan persepsi yang didapatkan dari audio asli dan yang telah diberi *watermark.*
   Bagaimanapun, kualitas dari sebuah audio yang telah disisipkan *watermark* akan menurun, baik secara sengaja karena proses penyisispan maupun tidak disengaja pada saat proses pengiriman kepada penerima. Oleh karena itu, kesamaan persepsi yang dimaksud fokus kepada presentasi audio yang asli maupun yang telah memiliki *watermark* kepada *customer*.
2. *Watermark bit rate*
   Bit rate pada *watermark* yang akan di-*embedded* adalah angka bit yang di-*embedded* per unit waktu dan memiliki satuan bps (bit per second). Beberapa aplikasi audio *watermark,* misalkan yang mengontrol pengkopian audia, membutuhkan masukan yang berupa nomor serial ataupun ID, dengan bit rate maksimal sebesar 0.5 bps.
3. *Robustness*
   Pada sebuah algoritma, *robustness* didefinisikan sebagai kemampuan dari pendeteksi *watermark* untuk mengekstraksi *embedded watermark* setelah prosedur standar dalam pemrosesan sinyal dilakukan. Aplikasi biasanya membutuhkan *robustness* di saat adanya modifikasi dari pemrosesan sinyal, sehingga *watermark* dapat diekstraksi pada proses deteksi. Pada sisi lain, terdapat beberapa algoritma yang tidak menginginkan *robustness* dan algoritma tersebut dilabelkan sebagai algoritma *fragile audio watermarking.*
4. *Blind/informed watermark detection*
   Pada beberapa aplikasi, sebuah algoritma deteksi dapat menggunakan file audio asli untuk mengekstraksi *watermark* dari *watermark* audio sekuens. Ini berarti deteksi yang dilakukan merupakan *informed detection.* Hal ini akan meningkatkan kinerja dari detector, karena audio asli dapat dihilangkan dari kopi yang memiliki *watermark* dan menghasilkan sekuens *watermark* itu sendiri.
   Satu metode lain, yaitu *blind detection,* detector tidak memiliki akses terhadap file audio asli. Jumlah data yang dapat disisipkan menjadi menurun. Proses lengkap menyisipkan dan mengekstraksi *watermark* dapat dimodelkan sebagai jalur komunikasi di mana *watermark* menjadi menyimpang karena keberadaan inferensi dan efek dari jalur yang digunakan. Inferensi terjadi karena keberadaan audio asli, dan efek jalur yang digunakan berkoresponden dengan proses pemrosesan sinyal yang terjadi.
5. *Security*
   Algoritma *watermark* harus aman yaitu pihak yang tidak berkepentingan tidak bisa mendeteksi keberadaan dari *embedded* data, terlebih lagi menghilangkan *embedded* data tersebut. Keamanan dari sebuah proses *watermark* diinterpretasikan dengan definisi yang sama pada keamanan proses enkripsi dan tidak bisa terpecahkan kecuali oleh *user* yang memiliki akses ke kunci rahasia yang mengontrol penyisipan *watermark.*
   Pihak yang tidak berkepentingan tidak boleh memiliki akses dan kemampuan untuk mengekstraksi data meskipun memiliki pengetahuan tentang algoritma yang digunakan dan *watermark* pada audio. Kebutuhan keamanan ini berbeda pada setiap aplikasi dan pada beberapa kasus, data dienkripsi sebelum disisipkan ke file audio.
6. *Computational Complexity*
   Masalah prinsip dari sisi teknis pada audio *watermark* adalah kompleksitas komputasi pada algoritma penyisipan dan deteksi, beserta jumlah *embedders* dan detector pada sistem. Pada kasus perlindungan hak cipta, aplikasi tidak perlu

memperhitungkan waktu sebagai aspek yang penting pada saat implementasi. Selain itu, *embedders* dan detector dapat diimplementasikan dalam perangkat keras ataupun plug-in, akan memiliki perbedaan dalam kemampuan memroses pada perangkat yang berbeda.

III. APLIKASI AUDIO WATERMARK

III. 1 Ownership Protection

Aplikasi pada kategori ini akan memiliki *watermark* yang mengandung informasi pemilik ter-*embedded* pada sinyal audio. *Watermark* yang digunakan hanya akan diketahui oleh pemegang hak cipta konten audio yang bersangkutan, dan karakteristiknya harus aman dan *robust.* Hal ini untuk memungkinkan pemilik mampu menunjukkan eksistensi dari *watermark* jika ada keraguan akan kepemilikan. Deteksi *watermark* harus memiliki kemungkinan kesalahan yang sangat kecil. Pada sisi lain, aplikasi ini hanya membutuhkan kapasitas data *embedded* yang kecil karena jumlah bit yang disisipkan dan diekstraksi dengan ruang kecil untuk kesalahan tidak perlu berukuran besar.

Mekanisme ini termasuk mudah untuk diaplikasikan karena hanya membutuhkan penyisipan data yang tidak terlalu besar pada file audio. Informasi pemilik akan disisipkan dan tersembunyi pada file audio tanpa memberikan banyak perubahan pada file audio. *Watermark* yang disisipkan pada file audio hanya diketahui oleh pemilik hak cipta dan dapat mendukung pembuktian kepemilikan dari sebuah file audio dan dengan ini memenuhi tujuan perlindungan hak cipta.

III. 2 Proof of Ownership

Watermark dibutuhkan tidak hanya untuk identifikasi dari pemilik dari hak cipta, tetapi sebagai bukti nyata kepemilikan. Masalah terjadi jika terdapat pihak yang mengedit *watermark* dan meletakkan ulang *watermark* serta mengklaim konten tersebut sebagai pemiliknya.

Pihak yang dapat mendeteksi *watermark* dapat menghilangkannya juga, dan detector *watermark* dapat dengan mudah didapatkan oleh pihak yang tidak berkepentingan.

Untuk mencegah pihak yang tidak memiliki hak ini serta meningkatkan keamanan untuk pembuktian kepemilikan, dilakukan pembatasan keberadaan detector *watermark*. Di saat pihak tersebut tidak memiliki detector, proses penghilangan *watermark* akan menjadi sangat sulit. Tetapi, hal lain juga dapat terjadi yaitu berupa pihak ketiga menggunakan sistem *watermark*-nya sendiri menambahkan *watermark* dan membuat seolah-olah *watermark* berada pada file asli.

Solusi untuk hal ini yaitu dengan melakukan pembuktian melalui algoritma. Algoritma dapat membuktikan *watermark* oleh pihak ketiga disisipkan ke dalam konten yang telah memiliki *watermark*. Algoritma tersebut akan menyediakan bukti tidak langsung karena adanya konten dengan *watermark* sebelumnya.

Mekanisme aplikasi ini berfokus pada penyisipan *watermark*, tetapi berbeda dengan aplikasi perlindungan kepemilikan dimana hanya pemilik hak cipta yang mengetahui *watermark*. Pada mekanisme ini, detector yang diperoleh oleh pihak lain dapat mendeteksi dan menghilangkan *watermark*. Tetapi pembatasan detector dan penggunaan algoritma dapat membantu pembuktian kepemilikan dan melindungi hak cipta pada file audio.

III.3 Authentication and Tampering Detection

Pada aplikasi autentikasi, sebuah kumpulan kedua dari data disisipkan ke dalam sinyal audio dan digunakan untuk menentukan apakah sinyal tersebut telah dirusak atau tidak. Pada aplikasi ini *robustness* tidak dibutuhkan karena motivasi penyerang tidak terkait dengan penghilangan *watermark*.

Kapasitas penyisipan *watermark* harus besar mengingat kebutuhan akan data tambahan. Deteksi dilakukan tanpa adanya sinyal asli karena keasliannya yang dipertanyakan.

Mekanisme aplikasi ini berkembang lebih jauh dengan menambahkan kumpulan data yang akan mengidentifikasi perusakan yang dilakukan pada file audio. Dengan hal ini integritas dari file asli dapat dijaga. Meskipun begitu, mekanisme ini membutuhkan kapasitas penyisipan data yang besar karena adanya data untuk mendeteksi perusakan. Pada perlindungan hak cipta terhadap file audio, aplikasi ini hanya akan memberikan informasi mengenai perubahan yang dilakukan pada file, sedangkan informasi yang dibutuhkan tetap tersimpan pada data yang disisipkan pada kumpulan pertama. Jika dikhawatirkan terjadi penyerangan pada file audio maka aplikasi seperti ini dapat diterapkan tetapi bukan merupakan fokus pada perlindungan hak cipta.

III. 4 Fingerprinting

Data tambahan yang disisipkan *watermark* pada aplikasi *fingerprinting* digunakan untuk melacak pemula atau penerima dari sebuah kopi spesifik file multimedia. Aplikasi ini pada audio *watermark* dilakukan dengan memberikan *watermark* dengan nomor ID yang berbeda pada kopi CD yang berbeda sebelum didistribusikan ke penerimanya.

Algoritma yang diimplementasikan pada aplikasi ini harus memiliki *robustness* tinggi untuk melawan serangan dan modifikasi dari pemrosesan sinyal. Aplikasi ini juga harus memiliki property *anticollusion*,

yang berarti bahwa tidak mungkin menyisipkan lebih dari satu nomor ID pada sebuah file multimedia. Jika terdapat lebih dari satu nomor ID, detector tidak akan mampu membedakan kopi dari file tersebut.

Kapasitas yang dibutuhkan oleh aplikasi ini berada di dalam jangkauan kapasitas yang dibutuhkan pada aplikasi perlindungan hak cipta, dalam beberapa bps.

Aplikasi fingerprinting ini sempat digunakan dalam mekanisme DRM pada persebaran CD. Setiap kopi CD akan memiliki nomor serial atau ID yang merepresentasikan sebuah kopi dari file audio. Mekanisme ini membuat dibutuhkannya perangkat lunak berupa pemutar-ulang khusus yang harus terdapat pada computer konsumen. Terdapat aplikasi berbeda untuk membaca produk dari perusaahaan berbeda dengan mekanisme ini.

Mekanisme ini tentu menjaga dan melindungi hak cipta dari file audio digital karena hanya konsumen yang membeli CD saja yang mampu memutar file audio tersebut. Tetapi terdapat ketidaknyamanan yang membatasi gerak konsumen. Di sisi lain, muncul pertanyaan-pertanyaan berupa batasan akses seperti apa yang dapat dimiliki oleh seorang konsumen yang membeli konten audio tersebut. Apakah akses tersebut hanya untuk computer pribadi, dan apa yang harus dilakukan jika konsumen tersebut ingin memutar CD di luar computer, misalkan di mobil.

Munculnya masalah social seperti ini membatasi gerak mekanisme DRM, selain itu selalu ada pihak ketiga yang berusaha membuat perangkat lunak untuk melumpuhkan mekanisme ini sehingga aka nada suatu titik dimana mekanisme ini tidak berjalan secara efektif dan memiliki pengaruh banyak terhadap perlindungan hak cipta.

III. 5 Broadcast Monitoring

Aplikasi pada audio *watermark* terdapat dalam *field* broadcasting. *Watermark* pada *broadcasting* menyediakan metode untuk mengidentifikasi informasi dari sebuah tayangan aktif. Peralatan siaran, digital maupun analog, biasanya telah mengimplementasikan proses penyisipan *watermark* ini. Dukungan peralatan dasar untuk siaran ini membantu dalam melakukan perlindungan hak cipta akan bahan siaran yang dimiliki oleh suatu stasiun tertentu.

III. 6 Copy Control dan Access Control

Pada aplikasi kopi control, *watermark* merepresentasikan sebuah kebijakan terkait kopi control atau akses control. Detektor dari *watermark* biasanya terintegrasi di dalam sistem perekam atau pemutar-ulang. Setelah *watermark* terdeteksi dan di dekripsi, peraturan kopi control maupun akses control diterapkan dengan mengarahkan perangkat keras atau perangkat lunak tertentu untuk menghentikan ataupun menjalankan modul perekam maupun pemutar-ulang tersebut.

Aplikasi ini membutuhkan algoritma *watermark* untuk melawan serangan dan modifikasi pemrosesan sinyal, mampu melakukan *blind detection,* dan mampu menyisipkan bit dengan jumlah yang tidak sedikit pada sinyal.

Selain *fingerprinting*, aplikasi ini merupakan mekanisme yang banyak digunakan pada saat perkembangan DRM. Mekanisme ini membuat adanya perlindungan penuh terhadap karya cipta yang dimiliki sebagai produk dari suatu perusahaan.

Perlindungan penuh ini dimulai sejak awal proses distribusi hingga cara penggunaan konten digital oleh consumen.

Informasi jalur distribusi dapat disisipkan pada file audio. Selain itu, control akses dan control kopi dikendalikan penuh dengan penggunaan perangkat lunak dan perangkat keras khusus yang dibuat secara spesifik untuk produk file audio tertentu.

Terkadang teknologi DRM yang mengaplikasikan mekanisme ini melanggar privasi ataupun hak konsumen dengan meminta identitas dan hak untuk memiliki akses terhadap file konsumen. Perlindungan dengan control yang terlalu ketat ini menyulitkan pihak konsumen karena terganggu hak dan privasinya, serta merugikan bagi artis ataupun pencipta karena membuat ruang lingkup pasar menjadi sempit. Pasar menjadi sempit karena banyak konsumen yang tidak menyukai invasi terhadap privasi dan menghindari pembelian file audio dengan DRM.

III. 7 Information Carrier

Aplikasi ini menyisipkan *watermark* yang memiliki kapasitas besar dan dideteksi serta didekrispi menggunakan algortima *blind detection.* Level tertentu dari *robustness* dibutuhkan untuk menghadapi pemrosesan standar seperti kompresi MPEG. Sebuah *watermark* public yang disisipkan ke konten multimedia mungkin digunakan sebagai penghubung ke basis data eksternal yang mengandung informasi tambahan mengenai file multimedia itu sendiri, seperti informasi hak cipta dan kondisi lisensi.

Mekanisme ini fokus kepada penyisipan informasi yang dibawa oleh file audio dengan *watermark* berupa jalur hubungan ke basis data. Terkait pemanfaatan untuk perlindungan hak cipta, aplikasi ini dapat dimanfaatkan untuk menyimpan jalur terhadap informasi pemegang hak cipta dan dimanfaatkan sebagai manajemen hak cipta.

V. KESIMPULAN

Konsep perlindungan hak cipta yang dibawa oleh DRM dapat dipenuhi dengan steganografi yang berupa

pengaplikasian digital *watermark* pada file audio. Tetapi bagaimanapun, mekanisme DRM yang berusaha membatasi persebaran file audio secara ketat berujung kepada adanya aplikasi spesifik untuk penggunaan mekanisme tertentu pada *watermarking* file multimedia. Hal ini terdapat pada aplikasi kopi control serta akses control.

Hal ini tidak secara efektif menghentikan penyebaran file audio di internet. Di sisi lain, pihak-pihak yang membuat serangan untuk melumpuhkan mekanisme DRM dari perusaahaan pun terus terjadi.

Bagi konsumen, aplikasi ini membuat konsumen menjadi terkungkung dan konsumen harus memiliki aplikasi ataupun perangkat keras tertentu untuk dapat memutar produk suatu perusahaan tertentu. Hal ini menyulitkan konsumen dan membuat DRM mulai ditinggalkan oleh perusahaan-perusaahaan besar dan kembali memproduksi file audio tanpa mekanisme DRM.

Berdasarkan daftar aplikasi yang dapat digunakan audio *watermark*, saat ini beberapa aplikasi dari audio *watermark* tetap dapat dimanfaatkan. Diantaranya untuk merekam beragam informasi, dari pemiliki, distributor, rantai distributor, beserta pembeli. Informasi ini di kemudian hari saat dibutuhkan dapat dimanfaatkan untuk menyediakan keterangan terkait manajemen hak cipta.

REFERENCES

[1] Nedeljko Cvejic, Tapio Seppanen, "Digital Audio Watermarking Techniques and Technologies". New York : Hersey. 2008.

[2] Chenyu, W., Jie, Z., Zhao, B., & Gang, R. (2003). Robust crease detection in fngerprint images. In Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition (pp. 505-510). Madison, Wisconsin.

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

Riffa Rufaida / 13507007