PENERAPAN *DIGITAL RIGHTS MANAGEMENT* DAN *WATERMARKING* PADA LAGU

Arya Tri Prabawa – NIM : 13506063

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16063@students.if.itb.ac.id

Abstrak

Berkembangnya teknologi di samping memberikan banyak kemudahan juga memunculkan tidak sedikit masalah. Salah satunya terjadi dalam industri musik. Industri musik yang menawarkan produk berupa Compact Disc (CD) yang berisi lagu-lagu para penyanyi dan musisi tidak lagi bisa tenang. Materi-materi ber-*copyright* itu kini dengan mudah dapat diperbanyak dan disebarluaskan. Dari media analog berupa CD tersebut, banyak orang dapat me-*rip*-nya menjadi file digital ke dalam komputer kemudian memperbanyaknya dan menyebarluaskan secara gratis melalui jaringan internet dengan kemudahan berbagai metode *file sharing* yang tersedia.

Industri musik pun terus mencoba berbagai cara untuk mengatasi masalah ini. Salah satu yang sempat digunakan oleh banyak label musik ternama adalah *Digital Rights Management* (DRM).

Tidak cukup bahwa sebuah file audio lagu sudah terenkripsi. File yang terenkripsi ini pada akhirnya tetap dapat diperbanyak dan disebarluaskan. Karena itu, DRM lebih menekankan pada mekanisme *copy control*. Tidak lama, muncullah berbagai tanggapan dari para konsumen yang mengeluhkan kinerja CD yang sudah dilengkapi dengan DRM, yaitu CD hanya bisa diputar pada pemutar tertentu dan banyak juga yang tidak bisa diputar di komputer. Dengan beragamnya keluhan, teknologi ini pun tidak lagi dipakai.

Industri musik pun mulai mengalihkan perhatiannya bukan pada *copy control* itu sendiri tetapi pada ketersediaan bukti-bukti yang kuat untuk mendukung pembuktian adanya penggandaan yang melanggar *copyright*. *Watermarking* pun dianggap dapat menjadi solusi yang tepat.

Watermarking adalah suatu mekanisme yang dapat menambahkan suatu informasi pada sebuah file lagu, misalnya, di mana informasi tersebut tidak merubah kualitas lagu dan tidak akan hilang ketika file lagu tersebut diperbanyak. Dengan demikian pada sebuah file hasil penggandaan dapat diperoleh informasi yang cukup mengenai file yang asli sehingga dapat menjadi bukti yang kuat menyangkut tindakan penggandaan yang ilegal.

Dalam makalah ini, penulis akan mencoba membandingkan penggunaan *Digital Rights Management* dengan *Watermarking* pada lagu. Pembahasan *Watermarking* akan menguraikan beberapa metode *Watermarking* yang ada. Pada akhirnya, penulis akan mencoba menganalisa jalannya penerapan *Digital Rights Management* dan *Watermarking* pada lagu.

***Kata kunci**: digital rights management*, *watermarking*, *audi*, *copyrights*.

1. Pendahuluan

Keresahan *publisher* lagu akan pembajakan dapat terlihat dari banyaknya usaha yang mereka lakukan untuk mengatasi tindak kejahatan yang satu ini. *Digital Rights Management* sempat marak dianggap sebagai solusi yang tepat di mana hak-hak penggunaan lagu yang telah dibeli dibatasi. Sayangnya, usaha ini justru menimbulkan banyak komplain dari pengguna karena dianggap menyulitkan dan memiliki banyak kekurangan.

Pihak produsen pun mulai beralih ke teknik *watermarking* yang memungkinkan pelacakan informasi yang menyangkut kepemilikan asli

lagu serta informasi lainnya yang diperlukan. Berikut adalah uraian mengenai kedua usaha melawan pembajakan tersebut.

2. *Digital Rights Management*

Digital Rights Management (DRM) adalah teknologi kontrol akses yang banyak digunakan oleh perusahaan-perusahaan pemegang hak cipta. Tidak hanya membatasi penggandaan media seperti *copy protection*, DRM memberikan kontrol kepada *publisher* untuk menentukan apa yang bisa dan tidak bisa dilakukan terhadap suatu media, seperti banyak penggunaan, jumlah penggandaan, atau peralatan apa saja yang mendukung penggunaannya.

DRM merupakan sebuah perangkat lunak yang dimasukkan ke dalam CD atau dihubungkan dengan *file* musik sehingga dapat mengatur apa yang dapat kita lakukan. Ide sederhananya adalah kita mendapatkan sesuai dengan yang kita bayar. Misalnya, membeli sebuah CD memperbolehkan kita untuk mendengarkannya berulang kali, tetapi dengan perangkat lunak DRM terinstal, *record label* bisa mengatakan bahwa harga yang kita bayar tidak memperbolehkan kita untuk menggandakan CD tersebut dengan cara menghalangi lagu-lagu tersebut dari penggandaan. DRM-lah yang membuat lagu-lagu yang diunduh dari iTunes hanya bisa diputar di iPods (kecuali jika kita membeli vesi yang tanpa DRM) dan DRM pula yang menghalangi kita untu berbagi sebuah lagu lebih dari tiga kali pada *downloading services* berbayar.

Mulai tahun 2002, *major record label* mulai antusias menggunakan DRM. Awalnya, DRM hanya digunakan pada CD promo untuk mencegah penyebaran *unreleased tracks* di internet, tetapi tidak perlu waktu lama hingga akhirnya DRM dapat ditemukan pada hampir semua rilis komersial. Masalah mulai dirasakan pada tahun 2005 ketika diketahui bahwa Sony telah menyertakan DRM dalam produk-produk mereka tanpa memberikan himbauan kepada para pelanggannya. Padahal, keberadaan DRM memunculkan tidak sedikit masalah keamanan pada komputer. Hal ini berbuntut pada penarikan kembali jutaan produk dan beberapa tuntutan *class action*. Pada akhirnya, Sony setuju untuk menghentikan penggunaan DRM. Begitu pula *major record label* lainnya dengan EMI sebagai yang terakhir mengumumkan penghentian penggunaan DRM.

Tidak demikian dengan penggunaan DRM pada *file* musik digital. Kenyataannya, ada penjualan musik *online* yang menggunakan DRM dan ada yang tidak. *Downloads* iTunes menggunakan DRM, kecuali dengan penambahan 30 sen untuk memperoleh versi tanpa DRM. Situs lain, seperti eMusic tidak menggunakan DRM. *Record label* ingin menghilangkan sama sekali penggunaan DRM, tetapi itu berarti perselisihan dengan para penyedia musik *online.* Misalnya, Apples menyukai *file* musik yang hanya bisa diputar di iPod, untuk alasan yang sangat jelas.

Pada akhirnya, tidak dapat dihindari kenyataan bahwa *label* dan *provider* akan dipaksa untuk menghilangkan penggunaan DRM agar dapat tetap kompetitif. Dengan semakin banyaknya pemutar musik digital *portable* yang menantang iTunes, *label* dan *provider* akan dipaksa untuk menjual musik yang dapat diputar di berbagai pemutar ini. Satu-satunya cara adalah dengan menjual musik yang tanpa DRM.

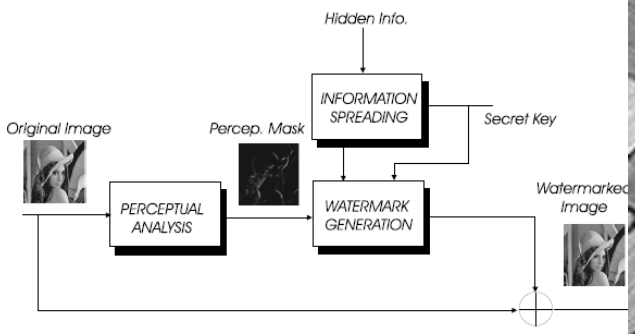
3. *Watermarking*

Digital watermark adalah sebuah informasi pembeda yang ditempelkan pada data dengan tujuan untuk melindungi data tersebut di mana akan sangat sulit untuk memisahkan atau menghilangkan informasi tersebut dari data yang bersangkutan. Karena *watermarking* dapat diterapkan pada berbagai tipe data, maka konstrainnya akan mengambil bentuk yang berbeda pula. Ada pula masalah lain, yaitu *robustness*. Yang harus diperhatikan adalah ketahanan terhadap manipulasi, tidak bisa dihilangkan secara statistik, serta harus tahan terhadap *watermarking* berulang.

Watermarking, seperti kriptografi, juga menggunakan kunci rahasia untuk memetakan informasi kepada pemilik, walaupun caranya berbeda karena pada *watermarking* objeknya harus tetap dapat berfungsi dengan baik. Informasi yang ditambahkan lewat *watermarking* biasanya berupa identitas pemilik, penerima, dan distributor ataupun tanggal transaksi.

4. Struktur Sistem *Watermarking*

Setiap sistem *watermarking* terdiri dari setidaknya dua bagian berbeda: *watermark embedding unit* dan *watermark detection and extraction unit*. Gambar 1 memperlihatkan contoh *embedding unit* untuk *still images*.

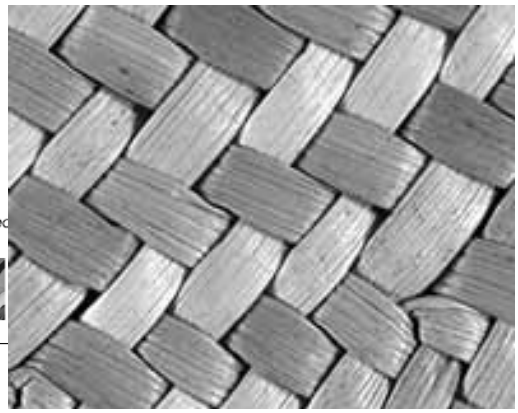


Gambar 1 Watermark Insertion Unit

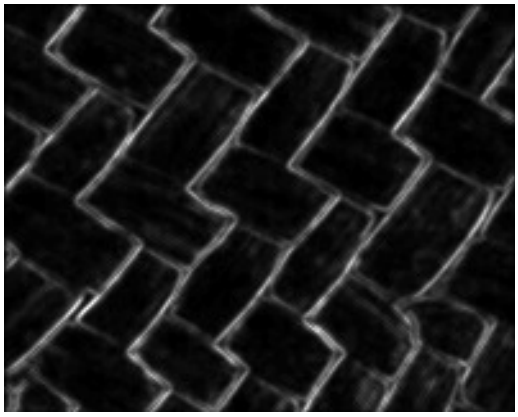
Image yang tidak ditandai dilewatkan pada blok analisis yang menentukan seberapa banyak sebuah pixel tertentu dapat diubah sehingga *image* yang telah ditandai tidak dapat dibedakan dari yang aslinya. Diperhatikan pula sensitivitas mata manusia pada perubahan di area-area datar dan toleransi yang cukup besar terhadap perubahan pada bagian-bagian ujung.

Setelah melalui proses ini dan dihasilkan *perceptual mask*, informasi yang akan disembunyikan dibentuk dan disebarkan ke seluruh bagian *image* yang asli. Teknik penyebarannya mirip dengan *interleaving* yang digunakan pada aplikasi lain yang melibatkan pengodean, seperti *compact disc storage*, untuk mencegah kerusakan informasi yang disebabkan oleh goresan dan debu. Penyebaran ini dimaksudkan agar informasi yang tersembunyi itu tidak hilang ketika *image* di-*crop*. Lebih jauh lagi, proses penyebaran dilakukan sesuai kunci rahasi sehingga sulit untuk memperoleh informasi yang disembunyikan tanpa memiliki kunci rahasia tersebut.

Teknik serupa juga digunakan pada *spread spectrum systems* (lebih tepatnya pada *Code-Division Multiple Access*) untuk memisahkan informasi yang diinginkan dari gangguan yang ada atau dari pengguna lainnya. Ketidakjelasan yang meilbatkan kunci juga dapat diperkenalkan pada pembesaran pixel. Terakhir, *watermark* ditambahkan pada *image* yang asli.

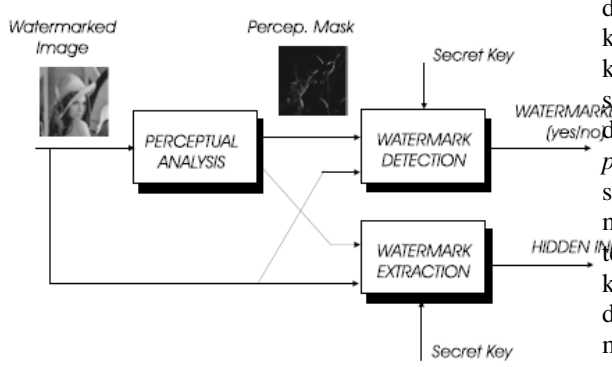


Gambar 2 *Image* asli



Gambar 3 *Perceptual Mask*

Gambar 3 memperlihatkan hasil analisis *image* yang digambarkan dalam Gambar 2. Intensitas yang lebih tinggi (terlihat lebih putih) menunjukkan semakin dapat dilakukan perubahan tanpa menghasilkan distorsi pada bagian tersebut. Terlihat bahwa hal ini berhubungan dengan bagian-bagian ujung pada gambar. *Mask* ini dikomputasi dengan menggunakan hasil-hasil penelitian ada mengenai cara kerja mata manusia pada domain-domain ruang. Hasil yang berbeda diperoleh ketika bekerja pada domain lain, seperti DCT (*Discrete Cosine Transform*) atau *Wavelet transform*. Ketika bekerja pada domain koefisien DCT dapat diperoleh keuntungan dari ketidakbergantungan antara perubahan yang mungkin dilakukan pada setiap koefisien. Hal ini menjadi berguna ketika berurusan dengan *mask* untuk keperluan *watermarking*.



Gambar 4 Watermark Detection and Extraction Unit

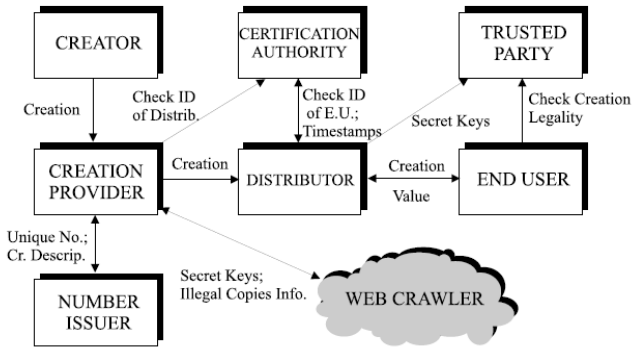
Gambar 4 memperlihatkan konfigurasi tipikal dari *watermark detection and extraction unit*. *Watermark detection* memutuskan apakah sebuah *image* tertentu telah diberi *watermark* dengan kunci yang diberikan. Perlu dicatat bahwa sebuah *watermark detector* menghasilkan keluaran biner. Yang perlu diperhatikan di sini adalah kemungkinan deteksi yang benar PD (bahwa memang ada *watermark*) dan kemungkinan deteksi yang salah PF. Kedua aspek penilaian ini memungkinkan kita untuk membandingkan skema-skema *watermarking*: satu metode adalah lebih baik jika menghasilkan PD yang lebih tinggi untuk nilai PF tertentu. Sebuah algoritma *watermarking* akan bermanfaat jika memiliki kemungkinan deteksi salah yang kecil.

Watermark detection biasanya dilakukan dengan menghubungkan *image* yang telah diberi *watermark* dengan *watermark* yang dibentuk dalam lokal penerima. Korelasinya menjadi tinggi ketika *watermark* diperoleh dengan kunci yang tepat. Performansi detektor dapat ditingkatkan dengan mengeliminasi *noise* yang dihasilkan dengan *signal processing*. Patut dicatat bahwa beberapa orang memilih menggunakan *image* yang asli pada proses deteksi. Walaupun menyederhanakan perlakuan lebih lanjut dari *watermark* pada sisi penerima, hal ini tidak realistis diterapkan pada kebanyakan aplikasi, terutama yang berhubungan dengan *E-commerce*. Sekali keberadaan *watermark* telah terdeteksi dengan benar, informasi yang disembunyikan dapat dipisahkan.

Prosedur ini juga umumnya dilakukan dengan menggunakan sebuah *cross-corelation* tetapi dalam hal ini sebuah keputusan yang independen harus dapat diambil dari setiap informasi yang diperoleh. Ketika statistikanya tersedia, struktur korelasi masih dapat diperbaiki. Misalnya, koefisien DCT yang banyak digunakan pada standar JPEG dan MPEG-2 dapat dihitung dengan baik oleh *generalized gaussian probability density functions* yang menghasilkan skema ekstraksi yang berbeda. Tentunya, ketika memisahkan informasi, parameter yang paling tepat untuk perbandingan adalah kemungkinan kesalahan bit Pb, mirip dengan yang digunakan dalam komunikasi digital. Hal ini tidak mengejutkan karena *watermarking* menciptakan sebuah jalur tersembunyi (kadang disebut steganografik) tempat informasi dibawa.

5. Sebuah Model Referensi untuk *Copyright Management*

Pada seksi ini, akan dedeskripsikan secara singkat sebuah subset dari *Common Reference Set*, yang dikembangkan dalam proyek IMPRIMATUR dari Eropa yang mendefinisikan sebuah *framework* konseptual untuk pengembangan *electronic copyright management systems*. Kegunaan model ini terletak pada kemampuannya untuk memetakan tugas dan agen berbeda yang terlibat dalam *copyright management* ke dalam entitas-entitas yang didefinisikan secara jelas. Hal ini penting mengingat aplikasi utama dari *watermarking* berhubungan dengan *e-commerce* dengan data multimedia, terutama di Internet.



Gambar 5 Model Referensi untuk *Copyright Management*

Model yang telah disederhanakan ini digambarkan dalam Gambar 5. Istilah *creator* melibatkan setiap konten yang memulai rantai nilai, termasuk pencipta lagu, fotografer, pembuat video, dan sebagainya. *Creator provider* membuat konten tersedia untuk publik

dalam bentuk yang selanjutnya dapat didistribusikan, misalnya, melalui server WWW oleh *distributors*. *Creator provider* di sini termasuk *publishers*, *multimedia company*, *agencies*, dan lain sebagainya. *Rights holder* mengatur *entitlements* dan *responsibilities* dari *creator* dan memfasilitasi pembuatan lisensi dan pemungutan royalti. Setiap kreasi diidentifikasi dengan sebuah *creation identification number* yang memungkinkan *rights holder* untuk menjual lisensi eksploitasinya. Contohnya adalah ISBN yang mengidentifikasi buku. Nomor ini menjadi bagian dari informasi yang disembunyikan seperti dideskripsikan, dan diberikan oleh organisasi yang ditunjuk oleh komunitas *creator providers*. *Purchaser* mewakili pengguna, baik individual maupun organisasi. Pada level inilah biaya teknologi *copyrights management* kritis, yang berarti bahwa perangkat keras tertentu (bahkan mengkin juga perangkat lunak) harus dihindari. Pada sisi ini, pengguna harusnya dapat mengecek apakah sebuah objek telah diperoleh secara legal, dengan cara melakukan tugas deteksi dan ekstraksi. Sayangnya, karena belum ada *watermarking* kunci public yang dikembangkan, tidak mungkin melakukan tugas tersebut tanpa perangkat lunak *tamperproof* yang menggunakan kunci rahasia. Cara lain adalah dengan menggunakan pihak ketiga yang dipercaya yang akan mengecek validitas *watermark* dan mengirim informasi yang tersembunyi dalam bentuk terenkripsi ke *end user* (bisa dengan protokol kunci publik). Untuk melakukan semua ini diperlukan sebuah *certification authority* untuk memverifikasi identitas dari berbagai agen yang terlibat dalam proses dan untuk memberikan *timestamp*.

Terakhir, jika *rights* akan dibeli, harus ada pertukaran informasi antara *end user* dan *rights holder*. Ada juga bagian penting yang tidak secara eksplisit termasuk ke dalam model IMPRIMATUR, yaitu agen yang mencari *copy-copy* ilegal di dalam jaringan. Terlalu naif untuk beranggapan bahwa semua *end user* akan mengecek *rights* dari objek. Hal ini terjadi dalam Internet dengan *file* musik MP3 yang diunduh oleh banyak pengguna tanpa memperhatika pelanggaran *copyrights*. Karena itu, *creation provider* harus bisa menemukan situs-situs ilegal yang ada.

6. Serangan

Berikut ini adalah beberapa serangan yang terjadi pada penggunaan teknik *watermarking*.

Filtering. *Low-pass filtering* tidak menciptakan degradasi tetapi dapat mempengaruhi performansi *watermark* dengan frekuensi tinggi.

Cropping. Penyerang bisa saja hanya tertarik dengan sebagian kecil dari *image* atau *audio* yang diberi *watermark*. Oleh karena itu, *watermark* harus tersebar sehingga tidak hilang.

Compression. *Watermark* tidak boleh hilang ketika media yang diberi *watermark* dikompresi.

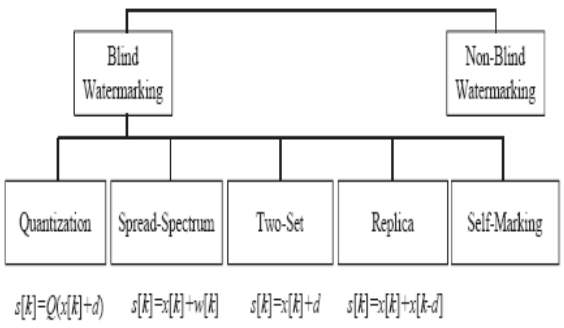
Multiple Watermarking. Penyerang bisa saja menambahkan *watermark* pada objek yang telah memiliki *watermark* lalu mengklaim kepemilikan terhadap objek tersebut. Cara mengatasinya yang paling mudah adalah dengan memberikan *timestamp* pada informasi yang disembunyikan oleh sebuah *certification authority*.

7. *Audio Watermarking*

Audio watermarks adalah sinyal khusus yang ditambahkan pada audio digital. Sinyal ini dipisahkan oleh mekanisme deteksi lalu didekodekan. Skema *audio watermarking* mengandalkan ketidaksempurnaan dari sistem pendengaran manusia. Walaupun demikian, telinga manusia jauh lebih sensistif ketimbang sensor lainnya. Karena itu, skema *audio watermarking* yang baik sulit untuk dirancang.

Walaupun teknik yang ada sekarang masih jauh dari sempurna, dalam dekade terakhir ini skema *audio watermarking* telah digunakan secara luas.

Skema *audio watermarking* yang ada saat ini dapat digambarkan sebagai berikut:



Gambar 6 Skema *Audio Watermarking*

Skema *watermarking non-blind* secara teoritis menarik, tetapi tidak praktis karena memerlukan kapasitas penyimpanan dan *bandwidth* komunikasi yang berlipat ganda untuk deteksi. Tentunya, skema *non-blind* bisa jadi berguna sebagai mekanisme verifikasi *copyright* dalam sebuah perdebatan *copyright*.

Sedangkan, skema *watermarking blind* dapat mendeteksi dan mengekstraksi *watermarks* tanpa menggunakan audio aslinya. Karena itu, skema ini hanya memerlukan setengah dari kapasitas dan *bandwidth* yang diperlukan oleh skema *non-blind*.

Seperti terlihat pada Gambar 6, terdapat lima skema *blind watermarking* dan secara singkat dapat dijelaskan sebagai berikut:

Quantization. Skema ini memperhitungkan kuantitas nilai sampel untuk membuat nilai sampel yang valid dan yang tidak valid.

Spread-Spectrum. Skema ini mendasarkan pada kesamaan antara audio yang telah diberi *watermark* dengan sekuens yang *pseudo-random*.

Two-Set. Skema ini mendasarkan pada perbedaan antara dua atau lebih set, yang termasuk skema *patchwork*.

Replica. Skema ini menggunakan *close copy* dari audio aslinya, yang termasuk skema modulasi replika.

Yang terakhir adalah ***Self-Marking***.

8. Kesimpulan

Perkembangan teknologi telah memberikan kemudahan bagi penggandaan dan penyebaran media yang mengandung *copyright*, termasuk lagu, secara ilegal. Salah satu solusi yang sempat digandrungi oleh *major record label* untuk memberikan proteksi terhadap lagu yang mereka jual adalah dengan menerapkan *Digital Rights Management*. Kesulitan yang dialami pengguna akibat penerapan metode ini mendorong produsen musik untuk mulai mengembangkan penerapan teknik *audio watermarking*. Dengan penerapan teknik ini, produsen dapat menambahkan informasi tambahan pada lagu, seperti kepemilikan asli lagu, yang sulit untuk dipisahkan ataupun dihilangkan. Teknik ini diharapkan dapat membantu menyelesaikan masalah perdebatan *copyroghts* yang mungkin terjadi.

DAFTAR PUSTAKA

[1] Kim, Hyoung Joong. *Audio Watermarking Techniques*. Kangwon National University.

[2] Perez-Gonzales, Fernando. *A Tutorial On Digital Watermarking*. Vigo University.

[3] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[4] ICT Results (2008, December 10). *Robust Watermarking Offers Hope Against Digital Piracy.* ScienceDaily. Retrieved March 13, 2009, from http://www.sciencedaily.com-/releases/2008/12/081208092114.htm

[5] Cvejic, Nedeljko. *Algorithms for Audio Watermarking and Steganography.* 2004. University of Oulu.