Penerapan Watermarking dalam proteksi media DVD

Fajar J. Ekaputra – 13503079

Program Studi Teknik Informatika,
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13079@students.if.itb.ac.id

Abstraksi

Proses merahasiakan pesan untuk menjaga kerahasiaan terbagi menjadi dua bagian besar, yaitu kriptografi dan steganografi. Steganografi sendiri dibagi menjadi dua bagian, yaitu steganografi dan watermarking, dimana perbedaannya terletak pada tujuan proses tersebut. Steganografi, seperti juga kriptografi bertujuan untuk melindungi pesan yang disamarkan agar tidak sampai diketahui keberadaannya dan keberadaan media penyamaran tidak berarti apa-apa, namun watermarking bertujuan sebaliknya, dimana keberadaan pesan tersembunyi tersebut ditujukan untuk melindungi media tempat dia disamarkan.

Sebagai salah satu media penyimpanan terpopuler saat ini, DVD menjadi target banyak pihak untuk penggandaan tanpa izin atau pembajakan. Telah banyak upaya yang dilakukan untuk mencegah hal ini terjadi. Salah satu cara yang banyak diaplikasikan adalah penggunaan watermark pada DVD untuk pengenalan apakah sebuah DVD merupakan hasil bajakan ataukah asli. Selain itu juga banyak berkembang standar-standar keamanan yang lain.

Makalah ini akan membahas tentang perkembangan standar keamanan media DVD terbaru yang menggunakan watermarking sebagai elemen utamanya., Berbagai macam standar keamanan yang sampai sekarang diterapkan, serta perbandingan kehandalan berbagai macam standar keamanan yang ada pada saat ini. Nantinya juga akan dibahas beberapa standar keamanan lain yang juga marak digunakan sebagai standar keamanan untuk DVD.

Kata Kunci : Watermarking, DVD, Proteksi

Bab I. Pendahuluan

Kriptografi (atau kriptologi; diterjemahkan dari bahasa Yunani *Kryptos* “tersembunyi”, dan *grafein* ”menulis”) adalah subject pembelajaran tentang perahasiaan pesan. Didalam masa modern, hal ini menjadi cabang dari teori informasi, sebagai studi matematis dari informasi, khususnya transmisi dari suatu tempat ketempat yang lain. Salah seorang kriptografer yang terkenal, Ron Rivest telah menemukan bahwa “Cryptography is about communication in presence of adversaries.”. Hal ini telah menjadi kontributor dasar dari beberapa bidang lain, diantaranya adalah keamanan informasi dan isu-isu terkait, otentifikasi, dan pengontrolan akses. Satu dari tujuan utama dari kriptografi adalah merahasiakan arti dari pesan, atau mungkin juga menghilangkan keberadaan pesan tersebut untuk orang-orang tertentu. Dalam masa sekarang ini, kriptografi juga berkontribusi didalam Computer Science. Kriptografi adalah menjadi sentral dalam perahasiaan pesan dalam komputer dan keamanan jaringan.

Kriptografi telah dikenal luas sebagai sebuah cara untuk merahasiakan pesan sejak berabad-abad lalu. Meski demikian, ternyata kriptografi bukanlah satu-satunya cara untuk melakukan hal tersebut. Steganografi atau ilmu menyembunyikan pesan didalam pesan lain adalah satu diantaranya.

Salah satu aplikasi unik steganografi dalam kehidupan sehari-hari adalah watermarking, dimana steganografi yang dilakukan justru untuk melindungi media penampung pesan tersebut. Watermarking dilakukan pertama kali di Itali, ketika pada akhir abad ke-13 pabrik kertas disana membuat kertas yang diberi watermark untuk digunakan oleh pelukis-pelukis besar sehingga karya mereka tidak dapat dipalsukan oleh orang lain.

Berabad-abad kemudian, Peran watermarking dalam kehidupan menjadi sangat penting. Maraknya penggunaan media digital sebagai media penyimpanan data memudahkan para pembajak hak cipta dalam melakukan tindakan pembajakan terhadap karya orang lain. Oleh karena itu, watermark kini banyak dikembangkan dalam mencegah hal tersebut.

DVD sebagai media yang populer sebagai media penyimpanan data digital tak luput dari masalah pembajakan tersebut. Oleh karena itu, para produsen keping DVD dan DVD player terus mencari sebuah standar yang dapat digunakan dalam produksi keping media DVD, sehingga pembajakan yang selama ini terjadi pada media tersebut dapat dihilangkan. Dalam pembuatan standar tersebut, Watermarking menjadi elemen penting, dimana walaupun banyak standar berbeda yang dikembangkan, cara yang digunakan sebagian besar menggunakan Watermarking sebagai elemen utama.

Sejarah proteksi DVD

DVD adalah sebuah 4,7 gigabyte media penyimpanan data, dan dapat menyimpan dua setengah jam video dengan format MPEG-2. Hollywood sebagai penghasil film terbesar di dunia mengharapkan bahwa DVD dapat menjadi bagian besar dari pasar home video dikarenakan kelebihanya dalam menghasilkan visual yang bersih dan berkualitas tinggi, seperti ketika CD meningkatkan penjualan musik pada tahun 1988 sampai dengan tahun 1995. Namun pengharapan tinggi tersebut juga diiringi kekhawatiran bahwa ada kemungkinan pembajakan merusak pasar DVD tersebut, karena sebelumnya juga MP3 dan internet menyebabkan kerugian besar dalam bisnis musik, dikarenakan pembajakan yang terjadi sangatlah besar dan merusak bisnis musik pada masa lampau.

Pada tahun 1996, Motion Picture Association of America (MPAA), Recording Industry Association of America (RIAA), dan Perusahaan-Perusahaan penghasil barang elektronik serta Perusahaan Teknologi Informasi bersatu membentuk DVD Copy Protection Technical Working Group (CPTWG) untuk memproteksi peluang bisnis baru pada media DVD untuk penggunaannya sebagai media Home-Video dari pembajakan.

Grup ini memulai tindakan proteksinya yang pertama dengan meluncurkan enkripsi yang diberi nama Content Scrambling System (CSS) pada tahun 1997. Namun, tidak ada satupun enkripsi yang dapat mencegah pengkopian illegal ini melalui output analog dari DVD player, atau menyetop sirkulasi kopian ilegal dari DVD dari orang ke orang yang lain. Sehingga, CSS tidak cukup untuk melakukan proteksi melawan Pembajakan.

Watermark sebagai Sarana Proteksi

Melalui penelitian secara spesifik, IBM's Tokyo Research Laboratory (TRL) pertama kali mengajukan teknologi watermark sebagai sarana untuk memproteksi DVD kepada CPTWG, dan membuktikan bahwa watermark mampu bertahan dari konversi digital-analog, juga menunjukkan bahwa teknologi yang digunakan oleh TRL ini mampu mendeteksi adanya watermark pada DVD yang terisi file berformat MPEG-2, juga pada file unformatted.

Hal ini memimpin perkembangan dari sebuah framework baru pada bagaimana pelaksanaan perekaman DVD dan alat untuk menjalankan DVD haruslah secara otomatis melakukan proteksi terhadap pemutaran DVD yang dikopi dengan tidak seharusnya, atau dengan kata lain melanggar Copy Control Information (CCI) yang terdeteksi pada isi Video tersebut. Framework ini juga termasuk didalamnya cara langsung dan agresif untuk mempromosikan proteksi pengkopian secara ilegal, namun tidak melakukan pelanggaran terhadap privasi dari pengguna legal, tidak seperti Watermark digital yang dikembangkan sebelumnya, dimana proses utamanya adalah melakukan monitoring dan tracking terhadap DVD, dimana diyakini melanggar privasi pengguna DVD tersebut.

Pembentukan Data Hiding Sub-Group (DHSG)

Framework baru tersebut yang meliputi recording dan pemutaran kembali dengan tetap memiliki watermark didalamnya, membutuhkan standardisasi dari watermarking untuk menjadikannya lebih efektif untuk mengimplementasikannya dalam bisnis DVD. Dalam bulan mei 1997, Data Hiding Sub-Group (DHSG) dibentuk dibawah CPTWG, dan mengeluarkan Call for Proposal (CFP). Didalam CFP tersebut terdapat persyaratan yang harus dipenuhi, dan diranking apakah hal tersebut merupakan hal yang essensial atau hanyalah menjadi nilai lebih saja. Persyaratan yang essensial untuk mengirim proposal tersebut ada sebagai berikut *) :

- Transparency
- Low-cost digital detection
- Digital detection domain: The digital detection can be done in the source data (uncompressed digital video), MPEG-2 compressed elementary data, a

multiplexed stream (program/transport), and/or logical sector data.
- Generational copy control for one copy
- Low false positive detection rate: no error lasting 10 seconds in 400 hours of operation.
  (Consumer electronics manufacturers now claim no error in "316,890 years" instead of no error in "400 hours.")
- Reliable detection
- Ability of watermark to survive normal video processing in consumer use.
- Licensable under reasonable terms
- No restrictions on export/import
- Technical maturity
- Data payload; three states (Never copy, No More Copying, and Copy Once) and an additional 2 bits for APS at a minimum.
  (the DVD CPTWG agrees to 8 bits of data payload)
- Minimum impact on content preparation
- Data Rate: at least 11.08 Mb/s

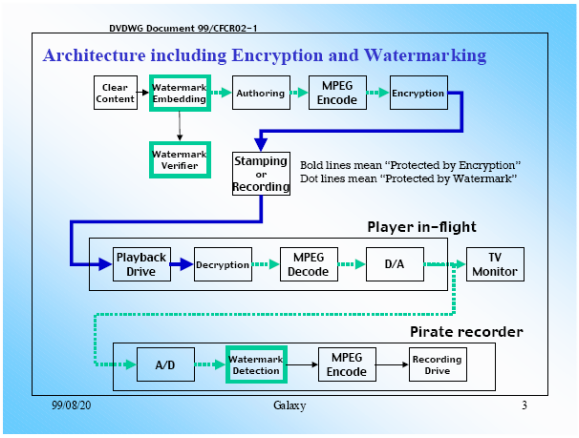
*) Dikutip dari http://www.trl.ibm.com/projects/RightsManagement/datahiding/dhvgx_e.htm

Proposal Hasil Seleksi

Secara keseluruhan, ada sebelas proposal yang datang kepada CFP. Yang selanjutnya dites menggunakan klip video sample pada rentang waktu Oktober 1997 sampai Februari 1998. Pada bulan mei 1998, DHSG mengeluarkan laporan sementara berjudul “Result of Phases I and II” dan proposal dari IBM adalah yang terbaik dalam data survive. Laporan ini menyebabkan adanya merger dari sebelas proposal tersebut menjadi tiga proposal pada bulan Juli 1998, yaitu : proposal IBM-NEC, proposal Pioneer-Hitachi-Sony, dan proposal Macrovision-Digimarc-Philips. Dimulai dari akhir 1998, Grup IBM-NEC dan grup Pioneer-Hitachi-Sony bertemu dan melakukan evaluasi terhadap proposal mereka secara teknikal. Sebagai hasilnya, grup Pioneer-Hitachi-Sony mengakui bahwa watermark milik IBM-NEC lebih baik dalam transparansi. Sehingga, pada Februari 1999, IBM, NEC, Pioneer, Hitachi, dan Sony mengumumkan bahwa mereka bergabung menjadi tim Galaxy untuk melakukan standardisasi watermark untuk DVD.

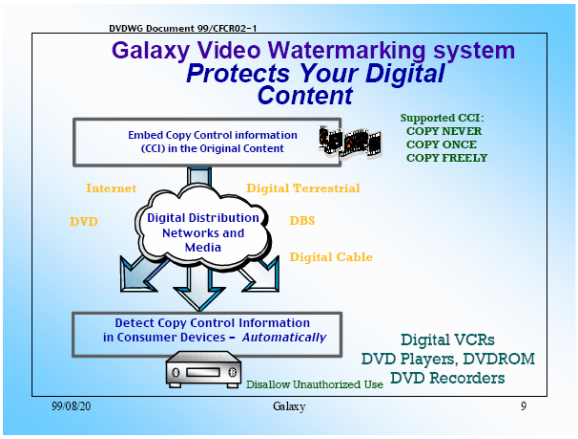
Bab II. Galaxy Watermark Proposal

Grup Galaxy membuat proposal mengenai watermark dengan mengkompromikan sebuah Primary Mark dan sebuah Copy Mark, untuk mencegah pembajakan DVD dan pemutaran hasil bajakan tersebut pada perangkat keras DVD dan juga PC. Ketika focus dari proposal system yang diajukan adalah DVD, ternyata hal ini juga dapat diaplikasikan kedalam banyak hal, diantaranya dalah satelit, kabel, dan segala macam distribusi dari video. Sistem ini menawarkan control pemutaran kembali, perekaman, dan kontrol untuk perbanyakan DVD melalui empat status jenis proteksi terhadap pengopian content, yaitu : “Copy Freely”, “Copy Once”, “No More Copying” dan “Never Copy” yang mana status tersebut akan dispesifikasikan dengan Primary Mark dan Copy Mark didalam isi Video.



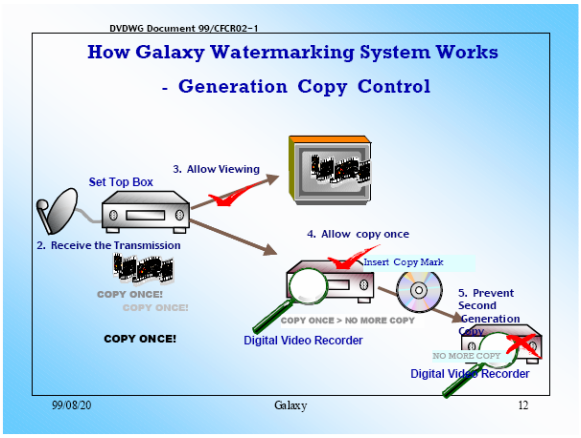
Primary Mark

Sebuah primary mark adalah 8-bit watermark digital transparan yang dimasukkan kedalam data video digital. Teknologi dari galaxy ini memungkinkan device yang menerima DVD mendeteksi adanya primary mark didalam baseband (data yang tidak terkompresi), juga didalam domain kompresi MPEG-2. Dua bit pertama dari primary mark adalah Copy Control Information (CCI) dan merepresentasikan “Copy Freely”, “Copy Once” dan “Never Copy” pada kasus dimana pada DVD tersebut tidak terdapat Copy Mark. Dua bit selanjutnya adalah APS Trigger bits. Sisa empat bit lainnya adalah cadangan untuk digunakan oleh sang pemilik dari isi DVD tersebut.



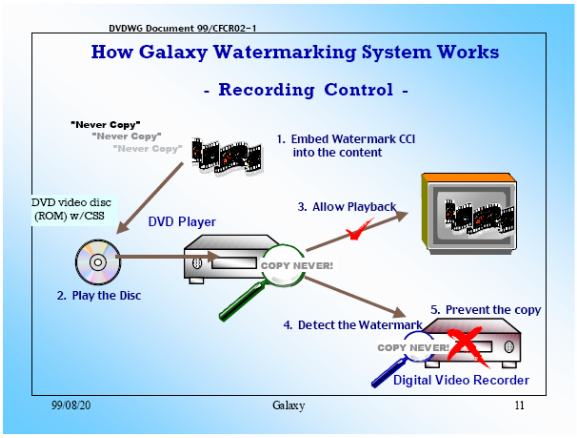
Copy Mark

Sebuah Copy Mark adalah digital watermark transparan lainnya, dimana tidak terkait dengan primary mark. Sama seperti primary mark, copy mark juga dapat dideteksi pada base band dan juga MPEG-2 Domain. Sebuah DVD recorder, jika dimasukkan kedalamnya sebuah DVD dengan status “Copy Once”, status didalam DVD tersebut akan berubah menjadi “No More Copying” untuk kegunaan kontrol dari pengopian DVD tersebut.



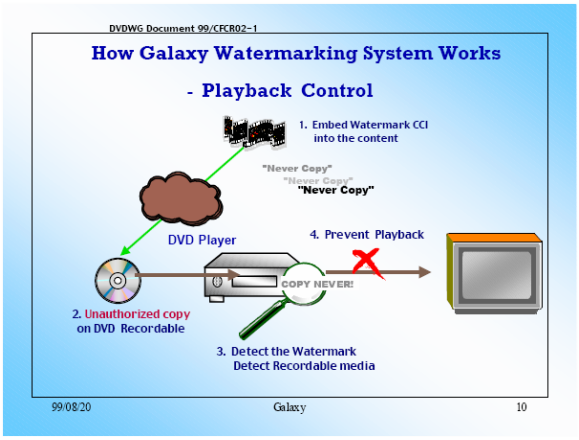
Record Copy dan Generational Copy Control

Sebuah detector mengirimkan signal kepada controller recording untuk berhenti atau memasukkan suara ketika detektor menemukan “Never Copy” atau “Copy Once” dengan sebuah Copy Mark



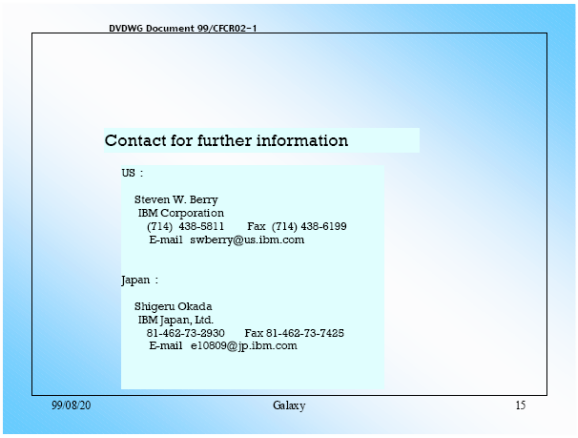
Playback Control

Sebuah detector juga mengirimkan sinyal kepada controller pemutaran DVD agar berhenti atau memasukkan noise ketika detector menemukan "Never Copy" atau "Copy Once" dengan sebuah Copy Mark didalam media recordable / rewriteable.



Galaxy Technology

Teknologi dari Galaxy menyediakan tingkat ketransparanan yang tinggi, juga primary dan Copy mark yang aman. DVD hasil proses proteksi dari galaxy mampu bertahan dari konversi digital-analog, MPEG-2 coding/encoding, dan berbagai macam proses signal. Detector dari galaxy menggunakan algoritma deteksi periode adaptif untuk mendeteksi primary mark dengan nilai rasio error yang sudah ditetapkan sebelumnya. Bahkan ketika isi dari DVD terdegradasi hebat, deteksi yang reliable dapat dicapai tanpa melewati error rasio yang sudah ditentukan sebelumnya., yang diset agar kurang dari 10-12 setiap sepuluh detik, melalui trade off yang melibatkan waktu pendeteksian window yang lebih lama. Primary mark mampu bertahan dari proses yang suksesif dari proses video studio, MPEG-2 compression, perekaman VHS, dan MPEG-2 recompression. Proses video studio yang diaplikasikan termasuk didalamnya filter brick wall, aperture enhancement, pengurangan bunyi yang menggangu, pengurangan kecepatan sampai dengan 98%, pencampuran watermark sampai 50%, konversi letterbox, konversi letterbox offset, spatial shifting secara acak, dan shifting hue.



Bab III. Millenium Proposal

Dengan maraknya video recerode dan disc burner yang menggunakan DVD untuk kebutuhan komputer personal yang kini muncul di pasar, sebuah koalisi industri video telah mengumumkan sebuah teknologi watermarking yang komprehensif untuk digital video yang diharapkan mampu untuk mencegah ketakutan akan terjadinya pembajakan seperti yang sekarang menghantui bisnis musik. Grup millennium, yang terdiri atas Philips Electronics, Macrovision, dan Digimarc, mengklaim bahwa system ini akan mencegah penggandaan DVD tanpa izin dan mencegah DVD bajakan dari kemungkinan dapat dimainkan pada player DVD>

Sistem ini akan diaplikasikan kedalam semua perangkat yang berbasiskan DVD, termasuk didalamnya Video recorder rumahan dan pembakar DVD untuk komputer personal, seperti yang dijanjikan oleh juru bicara grup Millenium ini pada tanggal 13 juli 2000. Kontrol penggandaan untuk video digital telah disiapkan untuk dibuat dan sebelumnya telah diimplementasikan dalam berbagai macam form, namun grup Millenium melangkah didepan dengan mengusulkan teknik yang disebut wobbletrack, dimana teknik ini akan memberitahukan DVD player ketika mereka diisi dengan Disk yang terdaftar.

Teknik anti pembajakan dari system ini juga tersedia untuk operasi copy-once, jika pemilik data mengingikan hal tersebut. Ketika copy-once diperbolehkan, hasil penggandaan akan dikodekan dalam cara tertentu sehingga hasil penggandaan tersebut tidak dapat lagi digandakan lagi, dalam sebuah teknik yang disebut watermark re-marking.

Generasi selanjutnya dari recording video digital akan datang dengan system ini terdapat didalamnya. Tidak akan ada degradasi yang terlihat maupun yang tidak terlihat terjadi akibat dari watermark ini, dan system ini disebut cukup kuat untuk menghilangkan ketakutan terbesar dari industri. “Kami yakin bahwa proposal baru Millenium ini akan memenuhi kebutuhan setiap orang, baik komunitas hardware, juga komunitas pemilik data ”, sebut wakil presiden Philips, Gerry Wirtz. “Kami menawarkan watermark yang kuat dan aman yang akan mencakup video format dari yang standar sampai dengan high-definition TV.. juga kompatibel dengan media fisik, seperti DVD dan kaset video dan metoda transmisi seperti terrestrial dan broadcast satellite, kabel, dan internet. Sebagai tambahan, Millenium proposal menyediakan sebuah fitur play-control yang kuat berbasiskan teknologi buatan kami, Wobbletrack”.

Digimarc CEO Bruce Davis mengatakan bahwa Millenium grup telah mendapatkan lima hak paten dalam waktu enam bulan terakhir. Sistem ini diharapkan menjadi sebuah kunci perpindahan system proteksi copyright untuk seluruh industri entertainment. “Kami telah memutuskan untuk menawarkan Millenium solution ini kepada industri dengan jaminan identifikasi patent yang kami percaya akan diterima oleh semua pengguna” sebut pemilik Macrovision John Ryan. “Grup Millenium menawarkan sebuah solusi komplit kepada semua jenis gambar bergerak, dan industri komputer personal akan memberikan pengguna dan industri keuntungan dari kemajuan termuktahir didalam video digital”.

Hal baru yang Ditawarkan Millenium

- Secondary mark instead of tickets for copy once
- Improved security
    - No “Copy Free” watermark state
    - Improved frame-adaptive embedding
- Additional Features
    - Postmarking to allow players with enhanced image processing (e.g. extensions to existing zoom features)
    - Easy transition to High Definition Video
    - Compatible with CSS and CPRM play & record control
- New Digimarc audio/video watermarking patent
- Deployment Schedule
    - WARP Tested Detector
    - Scale resistant detectors & secondary mark embedder – December 2000
    - Professional Embedders - December 2000
    - HD video compatible detectors– 2nd quarter 2001
- Licensing agreements available September 30

Licence Agreement Millenium
Signing allows licensee to obtain:

Modules
- C- Reference Code
- VHDL code

Compliance rules
- Courses to accelerate the design process
- "Designing the Watermark Detector into your IC"
- "Designing the Secondary Watermark Embedder into your IC"
- "Designing the WobbleTrackTM Detector into your IC"
- "Design of Millennium Compliant Products"

Semiconductor & Hardware Licencees

Self-Test
- Modules are provided with test vectors
- For players, disc based watermarked content
- For recorders, analog video input with watermarks

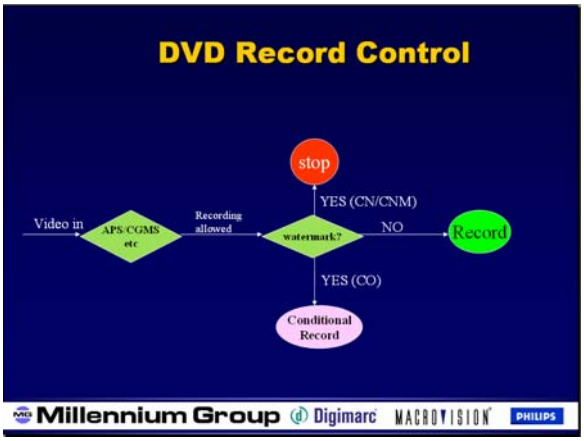
Certification
- Millennium compliance certification will occur in parallel with Macrovision APS certification

Millennium Technical Update

Copy Never - represented by primary watermark
Copy Once - represented by primary watermark
Copy No More - only by secondary watermark
Copy Free - by the absence of a watermark

Primary Watermarks – Usage
- The "copy never" (CN) watermark is to be used for pre-recorded video, and for e.g. PPV content.
  - CN watermarked video content on a DVD-ROM disc will be CSS-encrypted.
- The "copy once" (CO) watermark can be used for broadcasts or any form of digital transmission.
  - The exact role of the CO state still needs to be discussed by the industries.

Record Control Rules
- Record control rule: Millennium-compliant recorders (DVD, D-VHS, …) shall check unencrypted video content on their inputs for the presence of primary and secondary watermarks.
- Any content containing a CN or a CNM watermark shall not be recorded.
- Any content containing a CO watermark shall only be recorded using an approved CO protection scheme. For DVD recordables, this includes encryption (e.g. CPRM) and Millennium secondary mark embedding.

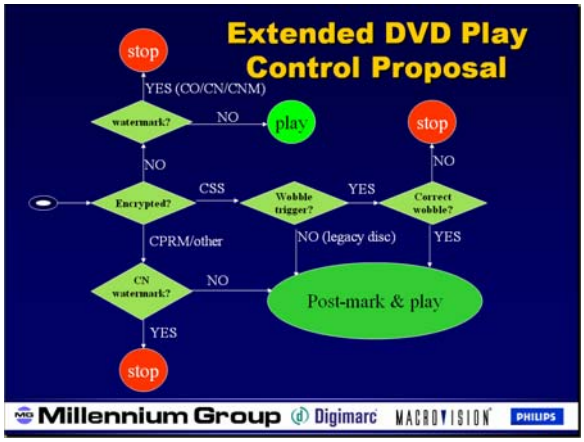


Secondary Mark Embedding

The secondary (CNM) watermark will be embedded by means of:
1. Pre-marking:
CNM mark is embedded *before* CPRM encryption
in CPRM-enabled *recorders*
2. Post-marking:
CNM mark is embedded *after* CPRM decryption
in CPRM-enabled *players*

Post Marking extension Proposal

Always post-mark CSS /CPRM encrypted video content where (Macrovision) APS is activated.
Advantages:
1. Fancy video processing features in players that happen to remove watermarks are no longer a security threat.
2. Watermark protection for existing discs having no primary watermark yet.



Secondary Mark Embedding

- First generation operates in baseband
- Small hardware cost (< 3 Kgates, 3 KBytes)
- Detectable by primary mark detector
  - So no additional gate count for detectors
- Invisible & robust
  - Little difference with primary mark embedding

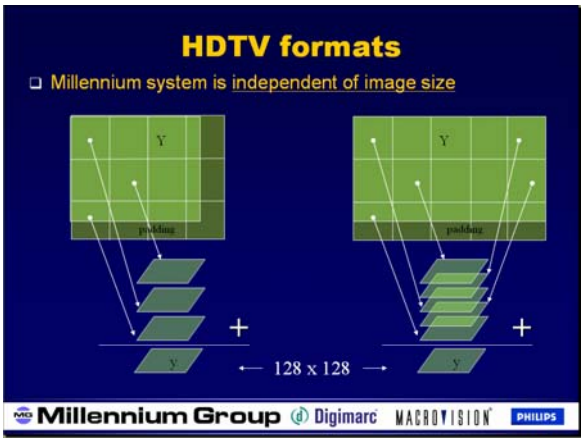
Summary of Features

As verified in the WARP testing:

- Invisible
- Payload: 8 bits
- Detection time: 1 to 10 seconds
- False positive probability: < 10-12
- Robustness (MPEG, noise, filtering, etc.)
  - WARP testing survived of 5 DA/AD conversions
- Low cost implementation (memory sharing)

Security Features

- Millennium offers a secure, future-proof method for recordable media type recognition: ROM-wobble.
- No "Copy Free" state: so the CF watermark cannot be misused to overrule e.g. a CN watermark.
- Separate software keys, with renewability options, will be used if software implementations are required. A compromise of "SW keys" would then not affect "HW keys".
- Even in the event keys would leak, they are hardly useful to hackers, because the embedding process has numerous "random" elements in the frame-adaptive embedding.
- Proposed "post-marking" scenario deals with all future fancy image processing features in players.



HDTV and Other Formats

- 1920 x 1080, 1280 x 720, 704 x 480, 640 x 480 … (progressive/interlaced)

Embedding remains the same
Detection remains the same

- Format conversions such as

1280 x 720 704 x 480

can be handled as a scaling/zooming/re-sampling problem

Millennium scale resistance

August 1999 CPTWG demonstration:

- Watermark resistance against arbitrary scalings ranging from 60% to 140%, approximately
- Independent horizontal and vertical scale
- Using an upgrade of the WARP-tested Millennium technology, so no new embedding!
- No consequence for false positives, visibility, etc.
- Implementation impact:
  - Longer detection times (30 seconds, but only for scaled video);
  - Required memory size (36 Kbytes -> 72 Kbytes, no issue when integrated in e.g. MPEG encoder/decoder)
  - Additional gate count of 2K gates

Millennium products

- Detectors and secondary mark embedders
- For both baseband and MPEG domain
- C-reference code and VHDL code
- Preferably integrated in existing IC's for
  - Cost-effectiveness
  - Security

IV. Kesimpulan

Kedua proposal yang diajukan pada dasarnya sudah memenuhi sebagian keinginan dari masyarakat industri, terutama industri musik dan perfilman, juga industri perangkat keras. Namun alangkah baiknya jika suatu saat nanti, kedua standar yang ada pada saat ini tersebut dapat disatukan menjadi sebuah standar baku yang mampu untuk mengatasi keseluruhan permasalahan yang ada pada pembajakan ini.

Penulis berharap, nantinya hak cipta akan menjadi suatu hal yang sangat penting, sehingga hak cipta intelegensia dapat dilindungi demi kebaikan seluruh umat manusia.

V. Daftar Pustaka

[1]http://www.trl.ibm.com/projects/RightsManagement/datahiding/dhvg2_e.htm
[2]http://ultimateavmag.com/news/
[3]http://wikipedia.org/en/
[4]http://www.cmpnetasia.com/
[5]Buku Kriptografi IF5054