Forensic Watermarking dengan menggunakan *Digital Rights Management*

Alfiansyah Mahareksa
18217022
Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
18217022@std.stei.itb.ac.id

Abstraks--Penggunaan *digital watermarking* saat ini sangat diperlukan untuk melakukan proteksi maupun pencegahan agar tidak terjadi kebocoran dan distribusi ilegal pada data digital yang memiliki hak cipta maupun konten premium dari pemilih layanan terkait. Banyak *digital watermarking* yang dapat digunakan saat ini, contohnya yaitu *forensic watermarking* dan *digital rights management.* Kedua teknik tersebut saling melengkapi dan sangat baik digunakan dalam melakukan pencegahan kebocoran tersebut karena *digital rights management* digunakan untuk mencegah penggunaan konten yang tidak sah, dan *forensic watermarking* digunakan untuk melacak kebocoran dari konten ilegal. Salah satu platform yang skemanya menggunakan kedua teknik tersebut adalah Pallycon yang sudah terkenal di bidang *information security* sehingga tidak perlu diragukan kembali. Contoh penyedia layanan yang menggunakannya yaitu Netflix. Dapat kita lihat pula memang keamanan Netflix dapat dibilang sangat baik dan kebocoran yang muncul pun cukup minim.

Kata Kunci--*Watermarking, DRM, Illegal, Forensic Watermarking*

1. Pendahuluan

1.1. Latar Belakang

Seiring berkembangnya waktu, saat ini banyak produk seperti musik, gambar, video, dan lain sebagainya yang telah berubah ke dalam format digital. Oleh karena itu, sangat mudah sekali untuk mencari dan mendapatkan produk digital tersebut maupun *file-file* lainnya di media digital.

Secara umum produk - produk dengan format digital tersebut dapat dengan mudah diakses di internet dan diunduh (*download*) dengan gratis oleh penggunanya. Namun, tidak semua produk digital bersifat gratis, beberapa produk memiliki hak cipta dari pemiliknya ataupun konten yang bersifat *premium* sehingga untuk mendapatkannya diperlukan membeli produk tersebut baru dapat diunduh.

Namun, dengan berkembang pesatnya teknologi dan jaringan saat ini, sangat mudah dalam melakukan pengiriman dan pendistribusian data yang sudah tersebar di internet. Oleh sebab itu, semakin marak pembajakan digital yang terjadi saat ini karena pengambilan produk bajakan di internet bukanlah sesuatu yang sulit, Cooper dan Harrison (2015) menyimpulkan bahwa proses mengunduh produk bajakan di internet dapat dilakukan hanya kurang dari satu menit [1].

Untuk melakukan pencegahan terhadap pembajakan tersebut ditemukanlah sebuah teknik *digital watermarking* untuk melindungi pembajakan produk digital secara ilegal. *Watermarking* digunakan dengan menyisipkan informasi tentang kepemilikan, identitas, *copy control,* dan lain sebagainya untuk memastikan *file* tersebut tidak dibajak oleh pengguna yang tidak bertanggung jawab [2].

Beberapa cara untuk melakukan *digital watermarking* yaitu dengan *forensic watermarking* dan *digital rights Management*. *Forensic watermarking* digunakan untuk menyisipkan dan mengelola informasi yang penting dan rahasia seperti *copyright* pada data digital, juga digukanan untuk melacak kebocoran konten *illegal* tersebut. Sedangkan *digital rights Management* adalah suatu teknik yang digunakan untuk mencegah penggunaan konten yang *illegal* dengan cara mengatur apa saja yang boleh dan tidak boleh dilakukan terhadap *file digital*[3].

Dengan teknik tersebut akan memberikan kemungkinan untuk menurunkan jumlah pembajakan yang terjadi sehingga pengguna akan memilih untuk membeli konten tersebut daripada melakukan pembajakan.

1.2. Rumusan Masalah

Rumusan masalah yang diajukan pada makalah ini adalah sebagai berikut.

1. Apa itu *digital rights Management*?
2. Apa itu *forensic watermarking*?
3. Bagaimana penggunaan *forensic watermarking* dan *digital rights management* pada konten premium?

1.3. Tujuan

Berdasarkan rumusan masalah sebelumnya, maka tujuan yang ingin dicapai adalah sebagai berikut.

1. Mengetahui *digital rights managements* beserta prosesnya
2. Mengetahui *forensic watermarking* beserta prosesnya
3. Mengetahui proses penggunaan *forensic watermarking* dan *digital rights management* pada konten premium

1.4. Metedologi

Pada makalah ini, penulis melakukan penelitian dengan menggunakan metode kajian pustaka dari berbagai jurnal dan artikel yang relevan. Makalah dibagi menjadi tiga bagian utama yaitu pendahuluan, pembahasan, dan penutup.

Tabel 1 Tabel Metodologi

No	Bagian	Deskripsi	Isi Bagian
1	Pendahuluan	Bagian pendahuluan berisi penjelasan mengenai penulisan beserta isi makalah	- Latar Belakang - Rumusan Masalah - Tujuan - Metodologi
2	Pembahasan	Bagian pembahasan merupakan inti makalah yang mengkaji dan membahas masalah yang ada pada rumusan masalah	- *Digital Rights Managements* - *Forensic Watermarking* - Penggunaan *forensic watermarking* dan *digital rights management* pada konten premium
3	Penutup	Bagian penutup menjelaskan penyelesaian dari masalah yang sudah dijabarkan sebelumnya	- Kesimpulan - Saran

2. Pembahasan

2.1. *Digital Rights Management*

Digital Right Management (DRM) adalah sebuah *tools* yang dapat digunakan untuk mengatur data digital dan memberikan keamanan/proteksi dari *user* yang tidak memiliki hak akses[4]. Teknologi DRM mengendalikan hak dalam melakukan penggunaan, modifikasi dan mendistribusikan data yang memiliki hak cipta atau bersifat premium. DRM dapat berasal dari banyak bentuk antara lain:

- Dokumen
- Gambar
- Musik
- Video
- dan lain sebagainya

Data digital yang premium tersebut berikutnya dapat diamankan oleh pemiliknya agar hanya orang - orang tertentu yang dapat mengaksesnya. Penerapan DRM sendiri memiliki banyak metode yang dapat digunakan, misalnya *vendor* - *vendor* besar seperti Netflix, Apple, Adobe, dan lain sebagainya pun mempunyai mekanisme DRM nya sendiri.

Sebagai contoh, Microsoft juga menggunakan DRM pada produknya yaitu Microsoft Office, Windows Media, dan Operating System Windows. Hal itu dilakukan agar tidak banyak pembajakan yang dilakukan kepada produk - produk milik Microsoft.

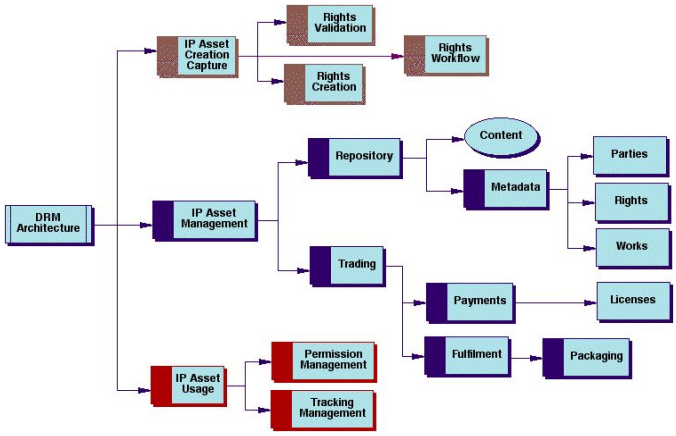
Keberadaan DRM bisa dibilang sangat penting bagi pemilik konten ataupun data digital yang bersifat premium. Singkatnya DRM dapat melakukan perlindungan terhadap suatu media dengan cara melakukan enkripsi data sehinga media tersebut tidak dapat diperbanyak maupun disebarluaskan dengan bebas.

Terkadang, bagi pihak - pihak yang terkena imbasnya mengartikan DRM sebagai *Digital Restriction Management* karena mendapat pengalaman yang tidak mengenakkan karenanya. Mereka berpendapat DRM sebagai sebuah sistem yang melarang untuk melakukan hal-hal yang seharusnya adalah hak mereka.

DRM sendiri sebaiknya dapat mencapai tujuan - tujuan tertentu agar penggunanya setuju dan yakin dalam penggunaan DRM pada kontennya. Beberapa tujuan yang sebaiknya dicapai oleh DRM adalah sebagai berikut.

1. DRM dapat memberikan dan memastikan keabsahan dari suatu media digital
2. DRM dapat memberikan perlindungan terhadap media digital
3. DRM dapat memberikan jaminan penyebaran media digital yang aman dari transaksi yang legal

Selanjutnya, dalam melakukan implementasi DRM tidak ada arsitektur pasti yang digunakan, karena DRM memiliki banyak kemungkinan metode yang dapat digunakan. Namun, secara umum arsitektur DRM adalah sebagai berikut



Gambar 1 Arsitektur DRM

(Sumber: https://www.researchgate.net/profile/Renato_Iannella/publication/33391833/figure/fig1/AS:505306523410432@1497485871602/DRM-Functional-Architecture.png)

Dari gambar tersebut dapat dilihat bahwa arsitektur DRM dapat dibagi menjadi 3 bagian sebagai berikut.

1. *Intellectual Property (IP) Asset Creation and Capture*

   Sebuah proses untuk melakukan pengelolaan dan pembuatan konten, konten tersebut juga akan diberikan lisensi saat dibuat sehingga mempermudah dalam proses distribusinya.

2. *IP Asset Management*

   Sebuah proses untuk melakukan pengelolaan pertukaran konten dan juga melakukan penerimaan suatu konten dari pemilik ke dalam suatu manajemen aset yang sudah disediakan.

3. *IP Asset Usage*

   Sebuah proses untuk melakukan pengelolaan terhadap konten yang sudah sampai di tangan pengguna, yaitu memberikan batasan - batasan dari penggunaan konten tersebut maupun kendala - kendala yang memungkinkan terjadi.

2.2. *Forensic Watermarking*

Forensic Watermarking adalah sal satu bidang teknologi dalam penerapan *Digital Watermarking*. Dimana yang dimaksud dari *digital watermarking* adalah teknk yang digunakan untuk menyisipkan dan mengelola informasi yang rahasia dan pentinf seperti hak cipta dalam berbagai data digital seperti foto, musik, video, dan lain sebagainya[5].

Namun, *digital watermarking* yang konvensional hanya digunakan untuk melakukan klaim hak cipta dengan cara menyisipkan informasi pemilik hak cipta pada konten tersebut. Sedangkan *forensic watermarking* bekerja jauh lebih dari itu, yaitu

melakukan penyisippan informasi pengguna juga pada konten sehingga dapat dilakukan pelacakan jika terjadi distribusi ilegal dari pengguna yang bersangkutan.

Jadi, saat pemilik hak cipta dari konten atau penyedia layanan konten premium tersebut menemukan adanya indikasi distribusi ilegal dari suatu pengguna, mereka dapat mengeceknya dari "*watermark"* yang sudah disisipkan. Lalu pemilik dapat melacak pengguna tersebut dan dapat menghentikan pengguna dari penggunaan layanan, ataupun dapat digunakan untuk melaporkan sebagai tindakan hukum untuk mencegah kemungkinan distribusi ilegal yang akan datang kedepannya[3].

Ada beberapa dasar - dasar dalam penggunaan *forensic watermarking.* Namun, setidaknya ada dua persyaratan yang sangat penting jika akan melakukan *forensic watermarking* yaitu sebagai berikut.

- *Imperceptibility*

  Harus memastikan bahwa perbedaan antara gambar yang asli dan gambar yang sudah diberi *watermark* tidak dapat dikenali secara visual

- *Robustness*

  Harus memastikan bahwa informasi dari *watermark* yang sudah disisipkan harus tahan dari berbagai serangan yang terjadi seperti *re-encoding, cropping,* dan *filtering.*

Mengapa 2 hal tersebut penting dikarenakan *watermarking* yang "terlihat" sangat tidak cocok dengan *forensic watermarking* karena akan menurunkan kualitas dari konten yang aslinya dan dapat dengan mudah dihapus dengan pengeditan sederhana. Oleh karena itu, untuk memenuhi syarat *watermark* yang "tidak terlihat". Biasanya *forensic watermarking* akan menyisipkan

informasi *watermark* ke dalam area gambar suatu frame yang tidak terlihat.

Gambar 2 Hasil penyisipan dari *forensic watermarking*

(Sumber: https://www.researchgate.net/figure/Original-image-Lenna-left-the-watermarked-copy-with-parameters_fig1_3720351)

Sesudah menyisipkan *watermark* ke dalam area frame yang tidak terlihat, pastikan juga hasil dari gambar yang sudah diberi *watermark* terlihat sama seperti gambar aslinya, seperti gambar diatas dimana gambar yang kiri adalah hasil dari gambar asli disebelah kanan yang sudah disisipkan *watermark*.

Watermark yang memiliki *robustness* terlalu tinggi juga tidak baik karena akan membuat *watermark* yang sudah disisipkan mudah terlihat. Sehingga kuncinya yaitu diperlukan tingkatan yang sesuai dan tepat untuk memenuhi kedua syarat dari *forensic watermarking* tersebut.

Pada saat ini teknologi dari *forensic watermarking* terus dikembangkan dan mulai banyak digunakan di berbagai bidang untuk melacak kebocoran ilegal misalnya pada konten video seperti berikut ini.

- *Screener (Pre-release)*

  Biasanya ada konten film yang didistribusikan terlebih dulu dalam bentuk *file* ataupun kaset yang ditujukan kepada *stakeholders* terkait untuk dicek sebelum perilisan film yang sesungguhnya. Oleh karenanya, jika ada kebocoran ilegal dari situ akan menyebabkan kerusakan yang sangat besar untuk pemilik hak ciptanya sehingga dibutuhkan *forensic watermarking* untuk mengetahui jika ada distribusi ilegal dan mencegah kebocoran yang mungkin terjadi kedepannya.

- *Digital Cinema*

  Forensic Watermarking juga dapat disisipkan pada konten film yang ditampilkan pada teater dalam bentuk film digital. Hal yang penting dilakukan yatu memasukkan informasi seperti teater apa dan waktu pemutaran film tersebut pada *watermark* lalu dihubungkan dengan sistem dari *digital cinema* yang berkaitan.

- *OTT VOD Service*

  Forensic Watermarking dapat pula diterapkan pada konten premium seperti layanan film online misalnya Netflix. Dengan begitu dapat disisipkan *watermark* untuk informasi dari pengguna secara *real time* sehingga dapat memudahkan melacak kebocoran ilegal saat itu juga

- *Live Stream Service*

  Kemudian, untuk *streaming* secara langsung seperti piala dunia, *forensic watermarking* juga dapat digunakan untuk mendeteksi jika ada kegiatan ilegal dari pengguna dan dapat langsung memblokir pengguna tersebut dari *streaming* ilegal yang dibuatnya.

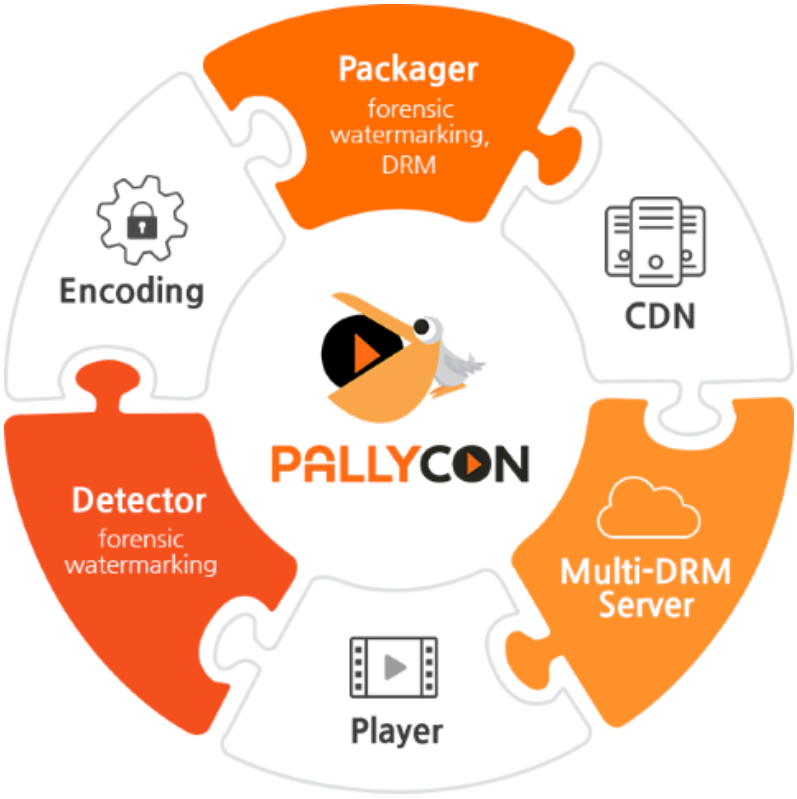
2.3. Penggunaan *Forensic Watermarking* dan *DRM* pada Konten Premium

Setelah kita memahami apa itu *digital rights management* dan *forensic watermarking*, kedua teknik tersebut dapat digunakan bersama untuk melindungi konten premium sebaik mungkin. Salah satu DRM yang digunakan yaitu Multi-DRM, Multi-DRM dapat mendukung *browser* tanpa menggunakan *plug-ins* juga mendukung berbagai macam *mobile* dan OTT. Multi-DRM sangat berguna dibandingkan dengan DRM biasa yang digunakan.

Namun, untuk penyedia layanan untuk konten premium yang ingin menerapkan Multi-DRM akan sedikit kesulitan dalam implementasinya karena menggunakan teknik yang kompleks dan sulit untuk mengintegrasikan DRM pada layanan yang disediakan.

Sehingga jika ingin menerapkan teknologi Multi-DRM yang kompleks ini dengan mudah dan cepat, sebaiknya menggunakan Multi-DRM yang mengintegrasikan beberapa teknologi DRM dan menyediakan API yang sesuai dan diintegrasikan dengan media terkait seperti *encoder* dan *player*nya.

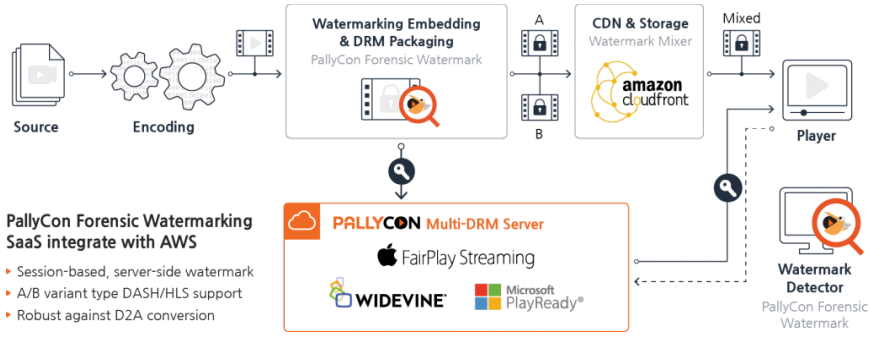
Untuk itu, ada plaform yang bernama PallyCon Multi DRM. Yaitu sebuah *one-stop multi-DRM cloud service* yang disediakan oleh INKA Entworks, salah satu spesialis dalam teknologi keamanan konten dan aplikasi. PallyCon menyediakan layanan yang stabil untuk berskala besar dan berjangka panjang sehinga dapat membantu penggunaan Multi-DRM dengan *forensic watermarking*[6].



Gambar 3 *PallyCon Multi DRM and Forensic Watermarking*

(Sumber: https://miro.medium.com/max/960/1*BLmiXzXiY01M0FWIKTB-Vg.png)

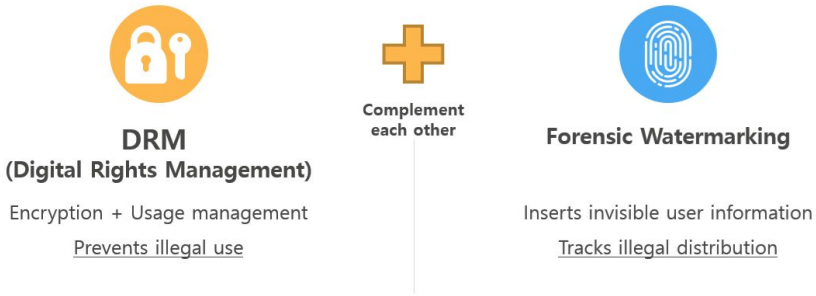
PallyCon dapat menjamin *robustness* untuk menahan berbagai serangan yang mungkin terjadi seperti *re-encoding, cropping, filterin,* dan *camcording.* Contoh dari layanan yang menggunakan cara ini yaitu Netflix juga sudah mulai diterapkan pada film *hollywood* terbaru saat ini. Skema dari cara kerjanya adalah sebagai berikut.



Gambar 4 *PallyCon Forensic Watermarking and Multi-DRM workflow*

(Sumber:https://miro.medium.com/max/1400/1*_XcsisKUAg5ZEYJ_sodYGQ.png)

Oleh karena itu, penggunaan DRM dan *Forensic Watermarking* sangat penting untuk melakukan pencegahan tindakan ilegal karena keduanya saling melengkapi yaitu DRM digunakan untuk mencegah penggunaan konten yang tidak sah, dan *forensic watermarking* digunakan untuk melacak kebocoran dari konten ilegal.



Gambar 5 *DRM and Forensic Watermarking*

(Sumber:https://miro.medium.com/max/1400/1*KDQTHf8tbFmRlqimcpoVqg.png)

3. Penutup

3.1. Kesimpulan

Berdasarkan hasil pemaparan dan analisis diatas, maka dapat didapat kesimpulan sebagai berikut.

1. DRM adalah salah satu teknik untuk mencegah kebocoran data digital yang dapat digunakan dengan cara melakukan mencegah penggunaan konten yang tidak sah.
2. *Forensic Watermarking* juga termasuk teknik untuk mencegah kebocoran data digital yang dapat digunakan dengan cara melacak kebocoran dari konten ilegal yang disebarluaskan.
3. Untuk melakukan pencegahan pada konten premium dapat menggunakan *Forensic Watermarking* dan Multi-DRM dengan menggunakan platform Pallycon yang memang sudah banyak digunakan oleh penyedia layanan seperti Netflix.

3.2. Saran

Dari pemaparan dan kesimpulan tersebut, dapat disarankan jika ingin melindungi konten premium sebaiknya menggunakan *Forensic Watermarking* dan Multi-DRM dikarenakan keamanan yang sangat baik dan dapat mencegah adanya kebocoran maupun distribusi ilegal.

REFERENSI

[1] Cooper, Jan., dan Daniel Harrison. 2015. "The Social Organization of Audio Piracy on the Internet."Media, Culture & Society 23: 71–89.

[2] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques applications and attacks," *International Journal of Engineering and Innovative Technology*, vol. 2, no. 9, pp. 165–175, 2013.

[3] Kim, Daniel, "How Netflix protects its content — Part 2," [Online]. Available https://medium.com/pallycon/how-netflix-protects-contents-part-2-33c1b60002a3 [Diakses 27 April 2020]

[4] INDICARE, "Consumer's guide to Digital Rights Management", INDICARE Project, April 2006.

[5] "Digital Watermarking," [Online]. Available: https://en.wikipedia.org/wiki/Digital_watermarking [Diakses 27 April 2020]

[6] Kim, Daniel, "How Netflix protects its content — Part 1," [Online]. Available https://medium.com/pallycon/how-netflix-protects-contents-part-1-a40508ed0001 [Diakses 27 April 2020]

[7] D. Das, "Automated Security Testing Framework for Validating Content Rights On Video Streaming Devices," TENCON 2019 -2019 IEEE Region 10 Conference (TENCON), Kochi, India, 2019, pp. 516-521.