Kriptografi dalam Proteksi *Digital Content*

Tresna Cahya Suciati[1], Steve Yulizar[2] dan Thesa Paska Utama [3]

Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if12005@students.if.itb.ac.id[1] , if12043@students.if.itb.ac.id[2],
if12071@students.if.itb.ac.id[3]

Abstrak

Seiring dengan semakin majunya teknologi digital, isu pembajakan media digital seperti halnya file musik, *video* atau *games* semakin mencuat. Pelanggaran berupa pengkopian atau penggunaan media digital tanpa memperhatikan hak cipta seringkali terjadi. Terdapat beberapa teknologi yang telah dikembangkan untuk melakukan proteksi terhadap digital content. Kriptografi pada umumnya digunakan sebagai salah satu bagian metode dalam teknik proteksi *digital content*.

Kata kunci: media digital¸ kriptografi, proteksi *digital content*

1 Pendahuluan

Teknologi *digital* telah membawa dampak besar bagi perkembangan industri *content*. Dalam satu sisi, penggunaan teknologi *digital* memungkinkan studio film untuk menciptakan film-film animasi, *games* dan *special effect* yang mampu meningkatkan kualitas film itu sendiri. Reproduksi media digital memungkinkan studio untuk mendistribusikan *content* dengan kualitas yang baik. Media *digital* berupa musik pun mempunyai keunggulan dalam kualitas suara bila dibandingkan dengan media musik dalam bentuk *tape*.

Selain itu penggunaan teknologi *digital* juga memberikan pilihan media komunikasi yang jauh lebih beragam, seperti CD, *minidisk*, *digital audio tape* (DAT), *pagers*, *mobile phones*, *answer-machines*, TV *digital*, *video digital*, radio *digital*, foto *digital*, internet, n*ewsgroups*, *database*, dan *e-mail*

Penggunaan teknologi *digital* juga telah memudahkan dan mempercepat distribusi media *digital*, misalnya dengan menyediakan situs untuk pembelian media *digital* melalui internet, sehingga distribusi musik, *game* atau *video* tidak lagi dibatasi oleh faktor perbedaan jarak dan waktu.

Namun disisi lain, penggunaan teknologi *digital* memungkinkan konsumen untuk membuat kopi dari media musik, *video*, dan *game* dan mendistribusikannya lagi ke pihak lain tanpa membayar. Hal ini dikarenakan, setelah media *digital* sampai ke tangan konsumen, pemakaian dari media *digital* tersebut tidak lagi dapat diawasi oleh produsen media *digital*.

Meskipun isu pembajakan media *digital* telah menjadi sebuah fenomena, namun ternyata masih sedikit penelitian yang dilakukan untuk mencari solusi teknis yang

mungkin diimplementasikan untuk mengatasi masalah tersebut[3].

2 Teknik Kriptografi yang Digunakan dalam Proteksi *Digital Content*

Proteksi d*igital content* bertujuan agar *content* tidak dapat digunakan oleh orang yang tidak berhak. Teknik kriptografi banyak digunakan sebagai salah satu metode dalam upaya proteksi *digital content*. Teknik kriptografi yang umum digunakan antara lain enkripsi, *digital watermarking*, dan *image scarring* (khusus untuk *content* berupa gambar)

2.1 Enkripsi

Enkripsi adalah proses menyandikan plainteks menjadi cipherteks. Sebelum didistribusikan atau dikirim, *content* terlebih dahulu disandikan sehingga kerahasiaannya terjamin.

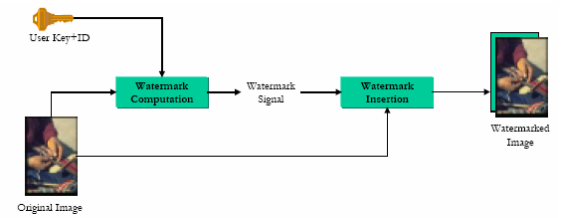
2.2 Digital Watermarking

Digital watermark adalah sinyal yang ditambahkan ke dalam data *digital* baik saat data diciptakan atau saat di*package* untuk distribusi dan dapat dideteksi kemudian untuk memeriksa keaslian dari data *digital*.

Digital watermark dapat diklasifikasikan ke dalam jenis *visible*, dimana *watermark* dapat diamati oleh manusia, dan *invisible watermark* yang hanya dapat dideteksi dengan menggunakan algoritma deteksi. Idealnya, sebuah *content* yang telah ditambahkan *invisible mark* tidak dapat dibedakan dengan content tanpa *watermark.*

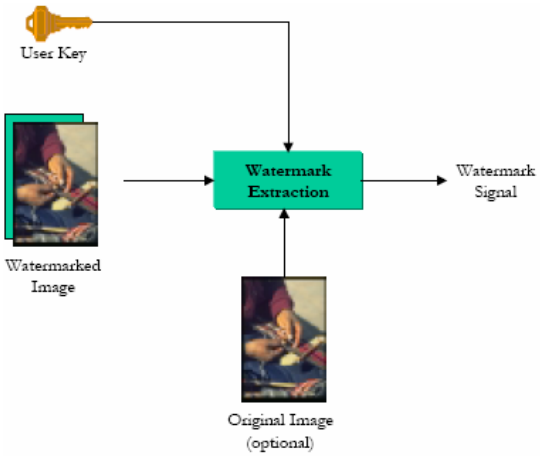
Watermark dapat juga diklasifikasikan ke dalam jenis *fragile* dan *robust*. *Fragile watermarks* akan menjadi *corrupted* jika salah satu bagian dari *content* yang diberi *watermark* berubah. Sedangkan *content* yang diberi *robust watermark* tahan terhadap perubahan-perubahan yang dilakukan terhadap *file* seperti *cropping*, *resizing*, dan sebagainya.

Untuk menambahkan *watermark* ke dalam sebuah *content* diperlukan sebuah ID dan kunci privat pengguna seperti diperlihatkan pada gambar berikut :

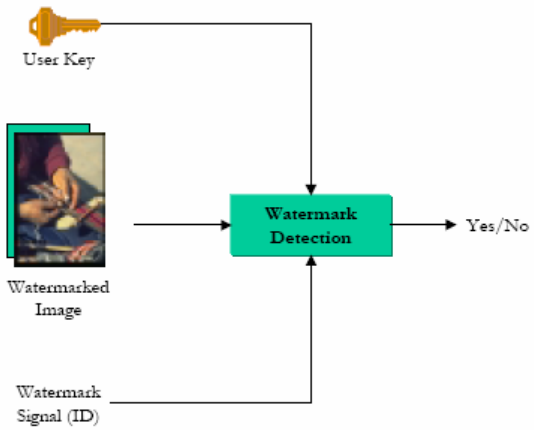


Gambar 1 Penambahan *Watermark*

Untuk ekstraksi *watermark* dari *content* diperlukan kunci, sedangkan untuk deteksi ada/tidaknya *watermark* diperlukan kunci dan ID yang telah dimasukkan saat proses penambahan *watermark.*



Gambar 2 Ekstraksi *Watermark*



Gambar 3 Deteksi *Watermark*

Untuk *content protection* digunakan *watermark visible* dan *robust*. Hal ini dimaksudkan agar *content* harus dapat diekstraksi terlebih dahulu sebelum dapat digunakan. Saat penambahan *watermark*, digunakan kunci privat dan ID tertentu yang unik. Agar *content* dapat digunakan, harus dilakukan ekstraksi yang memerlukan kunci yang sama. Oleh karena itu kunci harus didistribusikan melalui sarana komunikasi yang aman, sehingga hanya orang yang berhak yang dapat menggunakan *content* tersebut.

2.3 *Image scarring*

Image scarring adalah sebuah teknik yang mirip dengan *visible watermarking*. Sebagian kecil area dari content berupa *image* diacak sedemikian rupa sehingga *content* tersebut tidak dapat digunakan dengan baik pada resolusi maksimal. Dengan demikian *content* dapat didistribusikan dengan bebas sebagai versi *demo*.

Jika *content* akan digunakan dalam resolusi maksimal, maka diperlukan sebuah kunci yang hanya dimiliki oleh pembeli yang berhak. Kunci ini digunakan untuk mengembalikan area yang diacak ke dalam bentuk aslinya dengan menggunakan program *free "enabler"*.

3 Kriptografi dalam Teknologi Proteksi *Digital Content*

Terdapat beberapa teknologi yang telah dikembangkan untuk melakukan proteksi terhadap *digital content*. Beberapa diantaranya menggunakan teknik kriptografi sebagai salah satu bagian metodenya. Berikut ini adalah beberapa teknologi proteksi *digital content* yang menggunakan teknik kriptografi

3.1 *Content Scramble System*

Content Scramble System (CSS) merupakan teknologi proteksi *content video* yang didistribusikan pada DVD. CSS telah diimplementasikan pada hampir semua *video* DVD yang dirilis oleh studio Hollywood, sehingga menjadi teknologi proteksi *content* untuk media yang paling banyak digunakan. *Content* dikompresi, kemudian dienkripsi dengan algoritma kriptografi tertentu (seperti AES), dan didistribusikan pada *read-only media*.

Agar *video* dapat dimainkan, tiap *player* memiliki semua kunci yang diperlukan untuk mendekripsi semua media. Skema keamanan didefinisikan di *player* dan sangatlah sederhana, dimana semua *device* dengan kunci yang *valid* dapat mendekripsi semua media yang *valid* pada wilayahnya. Skema tersebut sangatlah lemah karena kunci yang digunakan semua sama dan tidak dapat membangkitkan *individual decoder*. Kelemahan CSS lainnya berupa ketidakmampuan CSS untuk mengubah kebijakan keamanan ketika beradaptasi dengan ancaman keamanan baru, karena mengubah skema keamanan CSS berarti mengubah skema *player*.

Enkripsi CSS merupakan sebuah sistem enkripsi yang digunakan pada DVD. Enkripsi ini memungkinkan *file* untuk dikopi dari DVD, tetapi menghasilkan *file* yang mengandung data yang tidak dapat dibaca dan tidak dapat dimainkan. Tidak semua *file* pada DVD dienkripsi dan *file* yang berbeda mungkin menggunakan kunci dekripsi yang berbeda. CSS menggunakan algoritma enkripsi 40-bit yang lemah. Himpunan kunci CSS dilisensikan pada perusahaan yang produknya berhubungan dengan CSS seperti DVD *drives*, DVD *players*, dan DVD *movie*. Pada umumnya DVD *player* dilengkapi dengan modul dekripsi CSS. Kunci CSS merupakan sebuah term kolektif untuk *authentication key*, *disc key*, *player key*, *title key*, *second disk key set*, dan *encrypted key*.

Pada bulan Oktober 1999, algoritma ini di-*reverse-engineer* oleh Jon Johansen dan menghasilkan DeCSS. Algoritma CSS kemudian diketahui mudah untuk diserang dengan serangan *brute-force*. Kelemahan dari proteksi ini terletak pada sharing skema enkripsi pada beberapa user (misalnya pada manufakturer DVD) yang mana membagi pengetahuan rahasia mengenai cara membangkitkan kunci dekripsi.

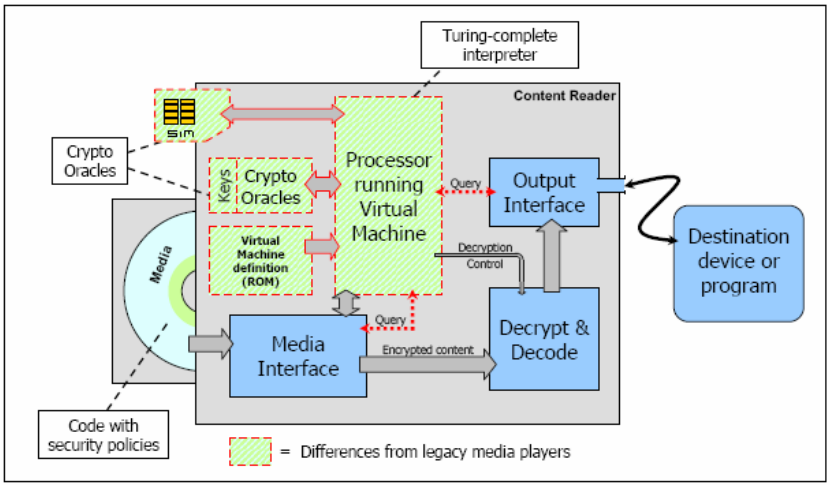
3.2 Conditional Access (CA)

Conditional access merupakan teknologi untuk proteksi *content* yang didistribusikan melalui kabel dan satelit. *Content* terlebih dahulu dienkripsi sebelum dikirimkan ke tujuan. Meskipun transmisi *content* ke tujuan (rumah pengguna) melalui infrastruktur transmisi yang tidak aman, *content* tetap terproteksi dikarenakan telah dienkripsi sebelumnya. *Device* seperti *set-top box* harus memiliki lisensi terlebih dahulu untuk memiliki kunci yang diperlukan untuk dekripsi *content*.

3.3 Self-Protecting Digital Content

Self-Protecting Digital Content (SPDC) merupakan teknologi yang dikembangkan untuk memperbaiki kelemahan-kelemahan yang terdapat pada teknologi CSS. Kode keamanan (*security code*) didistribusikan pada content dan player memiliki lingkungan eksekusi (*execution environment*) untuk kode keamanan tersebut. *Player* juga akan menyediakan kode *content* dengan akses ke primitif-primitif kriptografi dan detil data mengenai lingkungan *playback* seperti informasi *player* (model, faktor bentuk, status revisi, *serial number*, dll.), informasi media (format, kapasitas, *serial number*, dll.), informasi *output* (tipe, perusahaan pembuat, dll.), informasi *user* (nama, alamat *email*, nomor telepon, dll.), dan berbagai informasi lainnya. Informasi mentah yang digunakan player akan dikontrol penggunaannya oleh kode content. Misalnya ketika *user* membuat sebuah *copy* dari *content*, *content* dapat memutuskan untuk membuat *copy* dengan kualitas yang lebih jelek.

Perbedaan mendasar SPDC dengan CSS adalah pemisahan desain *player* dengan kode keamanan (*security code*). Dengan pemisahan ini, maka perubahan skema keamanan tidak membutuhkan perubahan skema *player*. Selain itu dapat meningkatkan keamanan karena kode keamanan yang berada pada *content* dapat dikostumisasi seaman mungkin dan berbeda-beda pada tiap *content*. Keuntungan lainnya adalah teknologi ini dapat meningkatkan kemampuan *user* untuk mengatur skema proteksi *digital content*, sebagai contoh user dapat mengurangi kualitas *playback*, menambahkan langkah verifikasi *user*, menampilkan *warning message* yang dikostumisasi, dll.



Gambar 4 Arsitektur SPDC

Gambar 4 menggambarkan implementasi Self Protecting Digital Content. Player ROM mengandung kode keamanan yang akan dieksekusi interpreter. Sebagai mana telah dijelaskan sebelumnya, interpreter juga mengandung kode *content* dengan informasi mengenai lingkungan *playback* dan juga mendukung kriptografi. Jika perlu, beberapa kunci dapat ditempatkan pada sebuah modul kemanan yang *removable*, seperti sebuah *smart card*

3.4 Digital Rights Management

Dalam dunia IT terutama bidang *multimedia* dan *entertainment*, terdapat suatu kebutuhan akan adanya kontrol terhadap penggunaan objek media hasil *download*. Objek tersebut misalnya *ringtone* ataupun mp3 dan gambar pada *handphone*. *Content provider* tentunya ingin agar hanya yang diberi hak sajalah yang dapat menggunakan objek media tersebut, misalnya mendengarkan mp3 tersebut maupun menggunakan gambar tersebut sebagai *background*. *Digital Rights Management* (DRM) ditujukan agar terdapat pengontrolan terhadap penggunaan objek media hasil *download*.

Dengan DRM, *content provider* dapat menentukan aturan-aturan mengenai bagaimana objek media hasil *download* seharusnya digunakan. Objek media yang berbeda dapat pula dikenakan hak yang berbeda, dan hak yang berbeda dapat memiliki harga yang berbeda pula. *Content provider* dapat memberi hak kepada pengguna untuk dapat melihat *preview* dari objek media secara gratis dan mengenakan biaya hanya untuk hak penuh penggunaan. Dengan DRM, hak untuk menggunakan objek media lah dijual dan bukan objek media itu sendiri. Hal ini memungkinkan karena nilai daripada *content* tersebut bukan terdapat pada objek medianya melainkan pada hak untuk menggunakannya.

Salah satu metode DRM adalah *separate delivery*. Dalam metode ini, *content provider* mengubah bentuk objek media asli ke dalam bentuk DRM *content format* (DCF). Dalam konversi ini, terdapat pula penggunaan algoritma enkripsi simetris untuk mengamankan *content*. Hal ini membuat objek *content* yang dilindungi oleh DRM menjadi tidak berguna bagi pihak-pihak yang tidak memiliki *Content Encription Key* (CEK). Oleh karena itu, *content* dalam format DRM dapat didistribusikan melalui jalur pengiriman yang biasa digunakan (tidak aman), akan tetapi untuk pengiriman hak dari objek yaitu CEK menggunakan jalur pengiriman yang lebih aman.

4 Kesimpulan

Teknik kriptografi bermanfaat dalam teknik proteksi *digital content*. Namun, teknik kriptografi saja tidaklah cukup untuk melakukan proteksi *digital content*. Teknik kriptografi tersebut perlu digabungkan dengan teknik-teknik proteksi lainnya agar dapat benar-benar memadai dalam mengurangi pembajakan *digital content*.

Teknik-teknik proteksi yang dibahas untuk sementara dapat mengatasi pembajakan *digital content*. Namun, pembajakan *digital content* bukanlah sebuah masalah yang dapat dipecahkan secara keseluruhan. Teknologi proteksi *digital content* yang ada saat ini tetap memiliki banyak kekurangan dan perlu untuk dikembangkan lebih lanjut.

[1] *Digital and Non-Digital - A Binary Opposition*, http://www.tasc.ac.uk/depart/media/staff/ls/Modules/MED1140/adv.html diakses tanggal 3 Januari 2006.
[2] *Forum Digital Digest*. http://forum.digital-digest.com/showthread.php?t=57044 diakses tanggal 5 Januari 2006
[3] Intel Corporation, *Protecting Content in the Digital Age : Balancing CreativeUse with Creator Right*, http://www.intel.com/standards/case/case_dtcp.htm, diakses tanggal 26 Desember 2005
[4] Open Mobile Allience, *Digital Rights management*, 2004
[5] P. Kocher et al., *Self-Protecting Digital Content : A Technical Report from the CRI Content Security Research Initiative*, http://www.cryptography.com/technology/spdc, diakses tanggal 26 Desember 2005
[6] P. Missier, *Technology for the copyright protection of digital images*, Bell Communication Research