PENGAMANAN KONTEN MULTIMEDIA

Rizkial Achmad

Jurusan Sistem Informasi
Fakultas Ilmu Komputer dan Manajemen Informatika
Universitas Sains dan Teknologi Jayapura

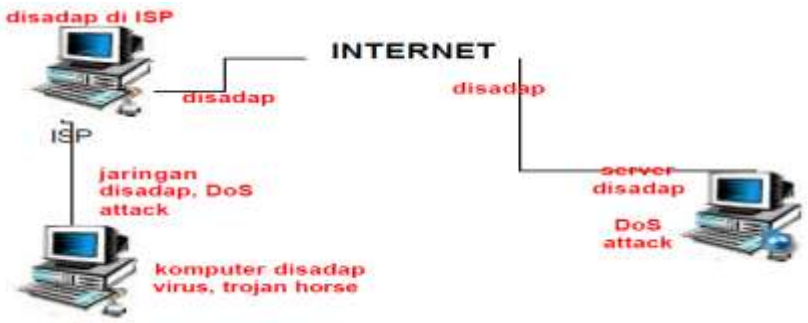
Abstraksi - *Dewasa ini, manusia dalam kehidupan sehari-harinya dimudahkan dengan adanya kemajuan teknologi, terutama kemudahan di bidang informasi dan komunikasi yang sangat dibantu oleh teknologi informasi dan komunikasi yang ada. Namun, seiring dengan berkembangnya TIK yang dapat membantu manusia dalam berkomunikasi, maka berkembang pula media dan konten yang dapat kita kirim dan kita terima dalam proses komunikasi tersebut. Secara umum, konten informasi atau yang sering kita sebut sebagai data yang dikirimkan melalui media TIK antara lain dokumen, foto atau gambar, musik dan bahkan audio visual seperti video. Untuk mengamankan konten multimedia tersebut agar dapat didownload oleh orang–orang yang telah diberi otorisasi, maka dapat digunakan beberapa teknik pengaman agar file multimedia hanya dapat didownload oleh orang yang diberi otoriasasi. Teknik yang dapat diterapkan adalah Steganography, Teknik Watermarking, Digital Rights Management (DRM**).**

Key Word :Konten, Steganography, Teknik Watermarking, Digital Rights Management (DRM)

1. PENDAHULUAN

Akses internet Dewasa ini sangat mudah didapatkan, manusia dalam kehidupan sehari-harinya dimudahkan adanya kemajuan teknologi internet, terutama kemudahan di bidang informasi dan komunikasi yang sangat dibantu oleh teknologi informasi dan komunikasi yang ada. Namun, seiring dengan berkembangnya TIK yang dapat membantu manusia dalam berkomunikasi, maka berkembang pula media dan konten yang dapat kita kirim dan kita terima dalam prses komunikasi tersebut.

Secara umum, konten informasi atau yang sering kita sebut sebagai data yang dikirimkan melalui media TIK antara lain dokumen, foto atau gambar, musik dan bahkan audio visual seperti video.Untuk mengamankan konten multimedia tersebut agar hanya dapat didownload oleh orang-orang yang telah diberi otorisasi, maka dapat digunakan beberapa teknik pengamanan. Secara umum hubungan antara pengguna Internet sebuah website (Web Server) dapat dilihat pada gambar di bawah ini :



Gambar 1. Alur Hubungan antara pengguna internet sebuah website

Pengguna terhubung ke Internet melalui layanan Internet Service Provider (ISP), baik dengan menggunakan modem, DSL, cable modem, wireless, maupun dengan menggunakan leased line. ISP ini kemudian terhubung ke Internet melalui network provider (atau upstream). Di sisi Web Server, terjadi hal yang serupa. Server Internet terhubung ke Internet melalui ISP atau network provider lainnya. Gambar tersebut juga menunjukkan beberapa potensi lubang keamanan (security hole).

Di sisi pengguna, komputer milik pengguna dapat disusupi virus dan trojan horse sehingga data-data yang berada di komputer pengguna (seperti nomor PIN, nomor kartu kredit, dan kunci rahasia lainnya) dapat disadap, diubah, dihapus, dan dipalsukan. Jalur antara pengguna dan ISP dapat juga di sadap. Sebagai contoh, seorang pengguna yang menggunakan komputer di lingkungan umum (public facilities) seperti di Warung Internet (warnet) dapat disadap informasinya oleh sesamepengguna warnet tersebut (atau pemilik warnet yang tidak bertanggung jawab) ketika dia mengetikkan data-data rahasia melalui web.

2. TINJAUAN PUSTAKA

A. Steganography

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik *steganography* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas

Steganography juga berbeda dengan *cryptography* yaitu terletak pada hasil keluarannya. Hasil dari *cryptography* biasanya berupa data yang berbeda dari bentuk aslinya dan biasanyadatanya seolah-olah berantakan namun dapat dikembalikan ke data semula. Sedangkan hasil dari keluaran steganography memiliki bentuk yang sama dengan data aslinya, tentu saja persepsi ini oleh indra manusia, tetapi tidak oleh komputer atau pengolah data digital lainnya. Selain itu, pada *steganography* keberadaan informasi yang disembunyikan tidak terlihat/diketahui dan terjadi penyampulan tulisan *(covered writing*), sedangkan pada *cryptography* informasi dikodekan dengan enkripsi atau teknik pengkodean dan informasi diketahui keberadaanya tetapi tidak dimengerti maksudnya.

Namun secara umum *steganography* dan *cryptography* mempunyai tujuan yang sama yakni mengamankan data, bagaimana supaya data tidak dapat dibaca, dimengerti atau diketahui secara langsung. *Steganography* memanfaatkan kekurangan-kekurangan indra manusia seperti mata dan telinga. Dengan kekurangan inilah maka teknik ini dapat diterapkan dalam berbagai media digital. Media *cover* merupakan data digital yang akan ditempeli dengan data yang akan disembunyikan atau sering disebut dengan stego medium. Berbagai media yang dapat digunakan sebagai cover dari data atau informasi yang akan disembunyikan dengan berbagai teknik *steganography*. Media yang dimaksudkan adalah media dalam bentuk file digital dengan berbagai format, antara lain :Images (bmp, gif, jpeg, tif, dll), Audio (wav, Mp3, dll), Video, Teks.

B. Teknik Watermarking

Teknik *Watermarking* merupakan bagian dari *steganografi* yang ditujukan untuk perlindungan hak cipta, tidak hanya dimaksudkan untuk menyembunyikan keberadaan pesan atau informasi, tapi lebih diarahkan untuk menjamin informasi dapat selamat dari beragam serangan yang dimaksudkan untuk menghancurkan *watermark.* Pada dasarnya, teknik *watermarking* adalah proses menambahkan kode identifikasi secara permanen ke dalam data *digital*. Kode identifikasi tersebut dapat berupa teks, gambar, suara, atau video. Selain tidak merusak data *digital* produk yang akan dilindungi, kode yang disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan seperti pengubahan, transformasi geometri, kompresi, enkripsi, dan sebagainya.

Keamanan di WWW dengan Enkripsi : Dalam upaya untuk menyediakan tingkat keamanan yang lebih tinggi, dapat didesain sedemikian rupa, sehingga setiap user memiliki kunci dekripsi masingmasing, kemudian dikirim ke server HTTP (Hyper Text Transfer Protocol) melalui CGI (Common Gateway Interface) pada server . Permintaan untuk informasi

yang tidak rahasia ke server akan diproses secara normal melalui mekanisme HTTP biasa, sedangkan permintaan untuk halaman web yang mengandung dokumen terenkripsi akan melalui prosedur khusus yang akan dijelaskan berikut ini. Gambar 13, menunjukan source code HTML dengan menyertakan suatu citra yang telah dienkripsi. Halaman web ini disimpan sebagai plaintext di server.

C. Digital Rights Management (DRM)

Digital Rights Management (DRM) adalah sebuah teknologi yang berkelas sehingga memungkinkan para pemegang hak cipta untuk mengontrol penggunaan media perangkat digital dari para pembajakan hak intelektual. Pemegang hak cipta biasanya berupa hak cipta perusahaan seperti musik, film, buku atau software. DRM digunakan untuk mengawasi bagaimana dokumen, seluruh program software digunakan. Ketika kerugian pada kualitas media analog yang tidak terhindarkan dan dalam beberapa kasus sekalipun selama penggunaan normal, beberapa file digital mungkin diduplikasi dalam jumlah yang tidak terbatas setiap kali dengan tanpa penurunan kualitas pada masing-masing duplikasinya.

DRM adalah suatu terminology yang melingkupi beberapa teknologi yang digunakan untuk menetapkan penjelasan pendahuluan akses kendali terhadap software, musik, film dan data digital lainnya. DRM menangani pendeskripsian, layering, analisis, valuasi, perdagangan dan pengawasan hak dalam segala macam aktivitas digital. **Digital Rights Management (DRM)** adalah suatu system yang ditujukan untuk mengatasi permasalahan yang terkait dengan pengaturan akses dan distribusi materi digital yang menjamin hak dan kewajiban antara pemilik (creator), penerbit (publisher) , penjual (seller) dan pengguna (consumer).

Topik utama dari DRM adalah berkaitan dengan lisensi digital. Bila seseorang membeli suatu materi digital, maka akan diberikan suatu lisensi yang terkait dengan hak dan kewajibannya. Dalam hal ini lisensi akan berbentuk file data digital yang berisi sejumlah aturan tentang penggunaan materi digital tersebut. Aturan dapat berupa sejumlah kriteria, misalnya : batas akhir penggunaan (expiration date), larangan untuk melakukan transfer ke media lain, ijin melakukan copy, dll. Kriteria tersebut dapat dikombinasikan sesuai dengan model bisnis yang disepakati, misalnya: meminjam (rental), mencoba (try before use), membayar per penggunaan (pay per use).

3. HASIL DAN PEMBAHASAN

A. Steganography

Terdapat beberapa istilah yang berkaitan dengan steganografi.

1) Hiddentext atau embedded message: pesan atau informasi yang disembunyikan.
2) Covertext atau cover-object: pesan yang digunakan untuk menyembunyikan embedded message.
3) Stegotext atau stego-object: pesan yang sudah berisi embedded message. Dalam steganografi digital, baik hiddentex atau covertext dapat berupa teks, audio, gambar, maupun video.

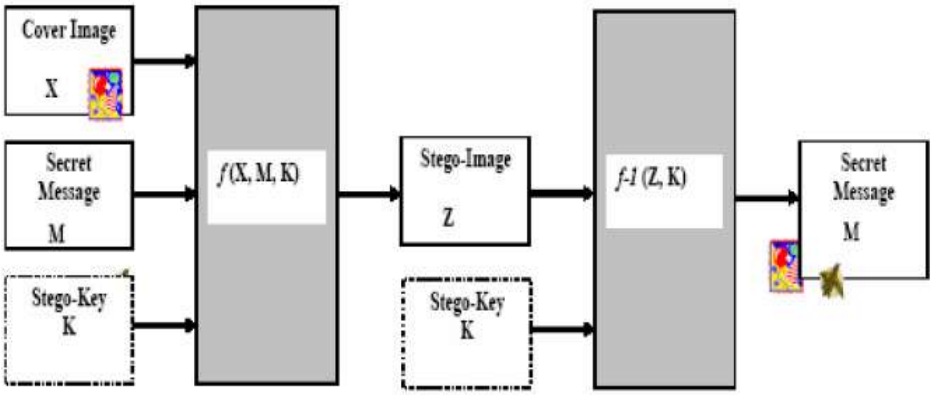
Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi, yaitu:

1) **Impercepbility**. Keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
2) **Fidelity**. Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.
3) **Recovery**. Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan

Istilah yang sering digunakan dalam teknik steganografi:

1) Carrier file : file yang berisi pesan rahasia tersebut
2) Steganalysis : proses untuk mendeteksi keberadaanpesan rahasia dalam suatu file
3) Stego-medium : media yang digunakan untuk membawa pesan rahasia

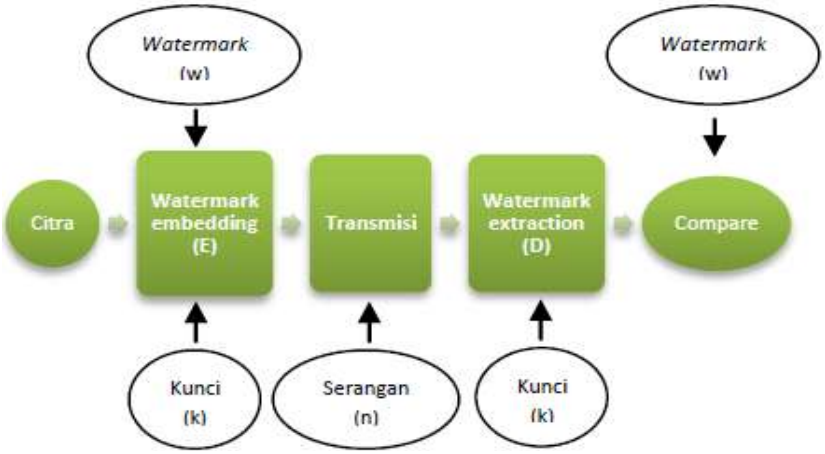
4) Redundant bits : sebagian informasi yang terdapat di dalam file yang jika dihilangkan tidak akan menimbulakn kerusakan yang signifiakan (setidaknya bagi indera manusia)
5) Payload : informasi yang akan disembunyikan



Gambar 2. Model sistem steganografi

B. Watermarking

Skema *watermarking* pada citra dapat digambarkan melalui bagan di bawah ini :



Gambar 3. Model sistem Steganografi

Bagan tersebut menunjukkan skema dalam sebuah proses penyisipan *watermark* pada citra *digital* sekaligus pengujian ekstraksi *watemark*. Terlihat bahwa terjadi serangan pada sebuah citra, kemudian *watermark* diekstraksi. Dari hasil ekstraksi *watermark* inilah nantinya akan diketahui apakah citra tersebut telah dimanipulasi. Jika memang citra tersebut telah dimanipulasi oleh pihak-pihak tertentu, maka *watermark* yang diekstraksi akan rusak. Dalam *watermarking,* terdapat dua proses yang cukup penting, yaitu enkripsi dan dekripsi. Enkripsi dalam hal ini berarti proses penyisipan pesan atau informasi ke dalam suatu citra *digital*.

Teknik penyisipan *watermark* ke dalam sebuah citra dapat dibedakan berdasarkan ranah penyisipannya, yaitu :

1) Ranah spasial

Penyisipan *watermark* dilakukan dengan melakukan pengubahan bit-bit data secara langsung pada data spasial citra penampungnya. Contohnya adalah penyisipan *watermark* pada LSB (*Least Significant Bit*).

2) Ranah frekuensi

Penyisipan *watermark* dilakukan dengan cara melakukan transformasi pada data penampung, kemudian perubahan dilakukan terhadap koefisien transformasinya. Contohnya adalah penyisipan *watermark* di ranah frekuensi dengan terlebih dahulu melakukan transformasi DCT (*Discrete Cosine Transform*).

3) Ranah *feature*

Penyisipan *watermark* dilakukan dengan menggunakan *feature point extraction* untuk menentukan daerah yang akan disisipi *watermark.* Metode ini termasuk metode baru di bidang *watermarking.* Namun, penyisipan *watermark* tetap dilakukan pada ranah spasial dan ranah frekuensi.

C. Digital Rights Management (DRM)

Sistem DRM dibangun dengan menyatukan teknologi keamanan dalam satu bundel system end-to-end yang melayani kepentingan dan kebutuhan pemilik, distributor, pengguna dan pihak terkait lainnya. Dalam membangun DRM diperlukan dua arsitektur kritis yang perlu dipertimbangkan. **Pertama** adalah arsitektur fungsional yang melingkupi modul atau komponen tingkat tinggi yang secara bersama-sama akan membentuk system end-to-end. **Kedua** adalah aristektur informasi yang melingkupi pemodelan entitas-entitas dalam DRM dan hubungan antara entitas-entitas tersebut.

1) Arsitektur Fungsional Kerangka kerja keseluruhan DRM dapat dimodelkan dalam tiga area bahasan:

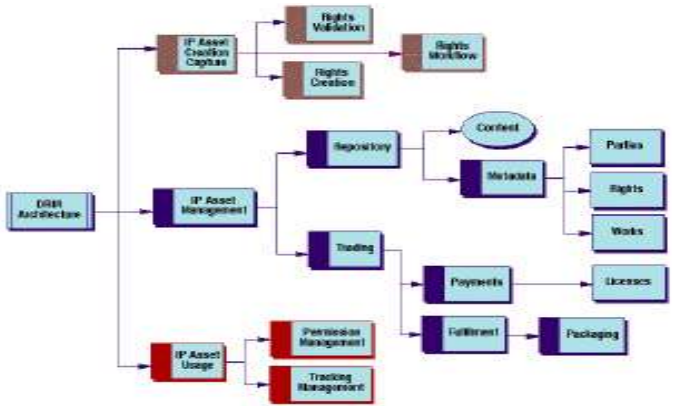
a) Intellectual Propierty (IP) Asset Creation and Capture: yakni suatu cara untuk mengelola pembuatan/kreasi suatu konten sedemikian hingga mudah untuk diperjual-belikan.

b) IP Asset Management: yakni suatu cara untuk mengelola dan memperjual-belikan konten. Termasuk di dalamnya menerima suatu konten dari creator/pembuat kedalam suatu sistem manajemen asset. IP Asset Usage: yakni bsuatu cara untuk mengelola penggunaan konten pada saat pertama kali diperjual-belikan. Termasuk di dalamnya mendukung kendala-kendala yang terjadi pada perdagangan konten dalam suatu system desktop /software tertentu.

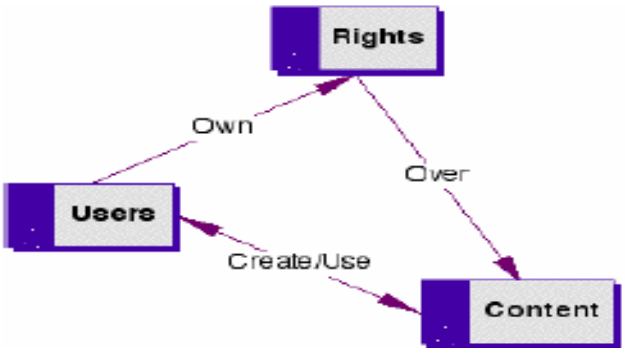
2) Arsitektur Informasi Arsitektur ini berhubungan dengan bagaimana cara agar entitas-entitas yang ada dibuat modelnya dalam kerangka kerja keseluruhan DRM berikut hubungan/relasi di antaranya. Bahasan yang penting mengenai kebutuhan yang diperlukan untuk membangun model Informasi DRM yakni:

a) Pemodelan entitas- entitas
b) Pengidentifikasi dan Pemaparan entitas- entitas
c) Pengekspresian pernyataan hak-hak.

Berikut adalah skema dua arsitektur kritis DRM:



Gambar 4: Arsitektur Fungsional DRM



Gambar 5: Arsitektur Informasi DRM Model Entitas Inti

4. PENUTUP

Penggunaan teknik tersebut diharapkan dapat memberikan perlindungan terhadap suatu file sehingga dapat mengamankan file dari orang – orang yang tidak berhak memiliki file tersebut. Sekalipun seseorang dapat mengambil file tersebut dapat diketahui keaslian dari file yang didapatkan tersebut sehingga tidak ada pihak yang merasa dirugikan.

5. DAFTAR PUSTAKA

Lu, Zhe-Ming; Wei-Min Zheng; Jen-Shyang Pan. 2006. ***Multipurpose Image Watermarking Method Based on Mean-removed Vector Quantization****. Journal of Information Assurance and Security, vol. 1, p.33-42. China : Harbin Institute of Technology Shenzhen Graduate School, Visual Information Analysis and Processing Research Center.*

Ide.B, Th.2005, ***Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi,*** *http://one.indoskripsi.com/judul-skripsi/teknik-informatika/implementasi-pengamanan-basis-data-dengan-teknik-enkripsi-0,*

Ohmacht, H. (2001). ***Stegano Project.*** *Diakses pada 23 Februari 2004 dari http://www.holger-ohmacht.de.*