TEKNIK KEAMANAN MULTIMEDIA

Dian Damara[1] (127006164)

[1]Jurusan Teknik Informatika, Fakultas Tenik, Universitas Siliwangi Tasikmalaya
dian.damara@student.unsil.ac.id

Abstrak

Pesatnya perkembangan teknologi informasi menjadikan semakin banyak pembajakan yang terjadi. Banyak konten dgital yang diakses secara illegal. Di dalam dunia bisnis konten digital, seharusnya konten illegal harus di proteksi dan di pastikan keamanan terjaga sampai konten tersebut sampai ke konsumennya. Sehingga untuk mengatasi permasalan ini, dibutuhkan suatu teknik pengamanan data. Teknik pengamanan data multimedia yang umum digunakan adalah *Cryptography* , *Steganography* dan *Watermarking*. *Cryptography* adalah teknik yang menyandikan data untuk mengamankan datanya. *Steganography* adalah teknik pengamanan data dengan menyamarkan datanya. Sedangkan *Watermarking* adalah teknik pengamanan data dengan menyembunyikan data ke dalam data lain.

Kata kunci : *Cryptography , Multimedia, Steganography, Watermarking*

1. PENDAHULUAN

Perkembangan teknologi informasi, secara tidak langsung berpengaruh terhadap bidang komunikasi data, dimana bidang komunikasi data ini menjadi jalur transmisi bagi data informasi yang mengalir dan menjadi penghubung dari satu orang ke orang lain. Hal tersebut memungkinkan berbagai lapisan masyarakat, termasuk para cracker atau penjahat lainnya dapat mengakses berbagai computer hingga merusak datanya. Oleh karena itu, keamanan data sangat penting demi menghindari kejahatan yang dapat mengakibatkan data hilang atau rusak.

Berdasarkan latarbelakang diatas, maka dalam penelitian ini dapat dirumuskan teknik-teknik pengamanan data seperti *Cryptography* , *Steganography* dan *Watermarking.*

Tujuan dari penelitian ini adalah untuk menjelaskan teknik mengamankan data berbasis multimedia menggunakan *Cyrptography, Steganography* dan *Watermarking.*

2. LANDASAN TEORI

Multimedia

Multimedia secara sederhana merupakan suatu media yang tidak hanya terdiri dari teks. Namun secara lengkap, multimedia dapat diartikan sebagai gabungan dari dua atau lebih media termasuk teks, gambar, audio, video dan animasi.

Multimedia terdiri dari beberapa bentuk media dasar yang saling terintegrasi dan mengandung suatu pesan tertentu.

Berikut bentuk-bentuk media, pada dasarnya terdiri dari 4 (empat) bentuk, yaitu:

- Text (.doc, .txt, .pdf dan sebagainya)
- Image (.jpg, .gif, .png, .tiff, .bmp dan sebagainya)
- Audio (.mp3, .wav, .au, dan sebagainya)
- Video (.avi, .dat, .mov dan sebagainya)

Keempat bentuk tersebut, masuk kedalam elemen multimedia yang pentig bagi produk multimedia.

3. METODE PENELITIAN

Metode penelitian yang digunakan adalah metode litertur, dimana pengumpulan data yang dilakukan dengan cara menganalisa dan mempelajari data- data yang diperlukan dari jurnal-jurnal referensi yang berkaitan.

4. HASIL DAN PEMBAHASAN

Kriptografi

Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data, adalah suatu bidang ilmu dan seni (*art and science*) yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data data dari akses oleh orang-orang atau pihak-pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. Bidang ilmu Kriptografi ini, semula hanya popular dibidang militer dan bidang intelijen untuk menyandikan pesan-pesan panglima perang kepada pasukan yang berada di garis depan, akan tetapi seiring dengan semakin berkembangnya teknologi, terutamanya teknologi informasi dan semakin padatnya lalu lintas informasi yang terjadi tentu saja semakin menuntut adanya suatu komunikasi data yang aman, bidang ilmu ini menjadi semakin penting.

Dalam teknologi informasi, telah dan sedang dikembangkan cara-cara untuk menangkal berbagai bentuk serangan semacam penyadapan dan pengubahan data yang dikirimkan. Salah satu cara yang ditempuh mengatasi masalah ini ialah dengan menggunakan kriptografi yang menggunakan transformasi datasehingga data yang dihasilkan tidak dapat dimengerti oleh pihak yang tidak berhak mengakses. Transformasi ini memberikan solusi pada dua macam masalah keamanan data, yaitu masalah privasi (*privacy*) dan keotentikan (*authenticatioan*). Privasi mengandung arti bahwa data yang diinginkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Adapun tujuan sistem kriptografi adalah sebagai berikut:

a) Convidentiality
Yaitu memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.

b) Massage Integrity
Yaitu memberikan jaminan untuk tiap bagian bahwa pesan tidak akan mengalami perubahan dari saat data dibuat atau dikirim sampai dengan saat data tersebut dibuka.

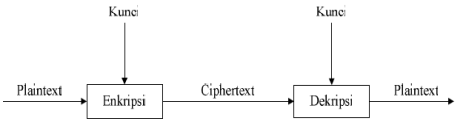
c) Non-repudiation
Yaitu memberikan cara untuk membuktikan bahwa suatu dokumen datang dari seseorang apabila ia mencoba menyangkal memiliki dokumen tersebut.

d) Authentication
Yaitu memberikan dua layanan. Pertama mengidentifikasikan keaslian suatu pesan dan memberikan jaminan keotentikannya. Kedua untuk menguji identitas seseorang apabila ia akan memasuki sebuah sistem.

Berikut Algoritma kriptografy dilihat berdasarkan kunci yang dipakai, dapat dibedakan atas dua golongan, yaitu :

1. Kunci Simetris

Kunci Simetris adalah jenis kriptografi yang paling umum digunakan. Kunci untuk membuat pesan yang di sandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia ciphertext.



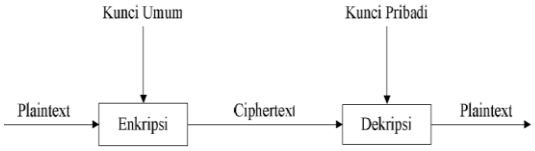
Gambar 1. Proses Enkripsi-Deskripsi Kunci Simetris

Algoritma kriptografi simeteris dibagi menajdi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*).

Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok). Kelebihan algoritma simetris ini adalah kecepatan proses enkripsi dan deskripsinya yang jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahan algoritma ini adalah permasalahan distribusi kunci (*key distribution*).

2. Kunci Asimetris

Kunci asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan yang satu lagi untuk deskripsi. Semua orang yang mendapatkan kunci public dapat menggunakannya untuk mengenkripsikan suatu pesan, data ataupun informasi, sedangkan hanya satu orang saja yang memiliki rahasia tertentu dalam hal ini kunci privat untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.



Gambar 2 . Proses Enkripsi-Deskripsi Kunci Asimetris

Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun diantara mereka tidak ada kesepakatan mengenai keamanan data terlebih dahulu maupun saling tidak mengenal satu sama lainnya.

Berikut beberapa kekurangan dari teknik Kriptografi :

- Setiap pasang pengguna membutukhan kunci yang berbeda, dan itu akan sangat sulit mengingat kunci yang sangat banyak secara aman dan ini akan menimbulkan kesulitan dalam hal menajamen kunci.
- Perlu adanya kesepakatan untuk jalur yang khusus untuk kunci, ini akan menimbulkan masalah baru karena untuk menentukan jalur yang aman untuk kunci lumayan sulit.
- Ada kemungkinan kunci dapat ditebak oleh pihak yang tidak bertanggung jawab.

Dan berikut kelebihannya :

- Waktu proses enkripsi dan den deskripsinya relative cepat
- Karena kecepatan itu, teknik ini bisa digunakan pada system secara real-time contohnya dapat digunakan pada keamanan saluran telepon digital.

Steganografi

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

Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas - berkas (*file*) komputer.

Contohnya, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya). Pada umumnya, pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi.

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas-berkas lain yang mengandung teks, *image*, bahkan *audio* tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas semula. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

Beberapa metode steganografi yang biasanya digunakan, yaitu:

1. Modifikasi LSB (Least Significant Bit)
   Dasar dari metode ini adalah pengetahuan akan bilangan biner atau bilangan basis 2, yang hanya terdiri dari ’1’ dan ’0’. Kedua bilangan yang menjadi dasar dari kerja komputer ini sering disebut dengan istilah bit. Susunan dari beberapa bit akan membentuk suatu informasi. Istilah yang umum dikenal adalah byte, yaitu kumpulan delapan bit data. Dalam satu byte data, bit yang paling berpengaruh terhadap informasi yang dikandungnya biasanya adalah bit paling awal/paling kiri. Bit inilah yang dinamakan Most Significant Bit (MSB). Semakin ke kanan, bit-bit tersebut semakin kecil pengaruhnya terhadap keutuhan data yang dikandung. Bit paling akhir/paling kanan inilah yang dinamakan Least Significant Bit (LSB).
   Teknik Steganografi modifikasi LSB dilakukan dengan memodifikasi bit-bit yang tergolong LSB pada setiap byte dalam sebuah file.
   Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit-bit informasi lain yang ingin disembunyikan.
   Contohnya pada file bitmap 24 bit, pesan dapat disimpan pada LSB tiap komponen penyusun warna (merah, hijau, biru). Maka untuk tiap pixel pada file bitmap 24 bit, dapat disimpan informasi sebanyak 3 bit. Teknik ini termasuk cukup sederhana, namun terkadang kualitas dari file yang ditumpanginya sedikit banyak akan terpengaruh. Misalnya untuk file bitmap 24 bit di atas, warnanya akan sedikit berubah meskipun mungkin tidak akan dapat disadari oleh mata manusia normal.
2. Algorithms and Transformation.
   Algoritma compression adalah metode steganografi dengan menyembunyikan data dalam fungsi matematika.
   Dua fungsi tersebut adalah Discrete Cosine Transformation (DCT) dan Wavelet Transformation. Fungsi DCT dan Wavelet yaitu mentransformasi data dari satu tempat (domain) ke tempat (domain) yang lain. Fungsi DCT yaitu mentransformasi data dari tempat spatial (spatial domain) ke tempat frekuensi (frequency domain).
3. Redundant Pattern Encoding
   Redudant Patrrern Encoding adalah menggambar pesan kecil pada kebanyakan gambar.
   Keuntungan dari metode ini adalah dapat bertahan dari cropping (kegagalan). Dan kerugiaannya adalah tidak dapat menggambar pesan yang lebih besar.
4. Spread Spectrum method
   Spread Spectrum steganografi terpencar-pencar sebagai pesan yang diacak (encrypted) melalui gambar (tidak seperti dalam LSB).
   Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu crypto-keydan stego-key.
   Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses image (gambar).

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang

menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi.

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.

Kekurangan dan kelebihan steganografi jika dibandingkan dengan criptografi adalah :

Kekurangan :

- Memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan.

Kelebihan :

- Memungkinakan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim.

Watermarking

Watermark merupakan proses untuk mencantumkan sebuah informasi rahasia di dalam sebuah gambar, yang mana informasi rahasia tersebut sebenarnya juga merupakan bagian dari gambar itu.

Berbagai tujuan yang ingin dicapai dari penggunaan watemarking, sebagai suatu teknik penyembunyian data pada data digital lain yaitu**:**

- Tamper-proofing : *Watemarking* digunakan sebagai alat indikator yang menunjukkan apakah data *digital* yang asli telah mengalami perubahan dari aslinya (mengecek integritas data).
- Feature Location : *Watemarking* sebagai alat identifikasi isi dari data *digital* pada lokasi-lokasi tertentu, misalnya penamaan suatu objek tertentu dari beberapa objek yang ada pada suatu citra *digital*.
- Annotation/caption : *Watermark* berisi keterangan tentang data *digital* itu sendiri, misalnya pada *broadcast monitoring* pada penayangan iklan di stasiun TV. Selain itu, *watermark* juga dapat digunakan untuk mengirimkan pesan rahasia.
- Copyright-Labeling : *Watemarking* di gunakan sebagai metoda untuk menyembunyikan label hak cipta pada data *digital* atau sebagai bukti autentik kepemilikan atas dokumen *digital* tersebut.

Berikut beberapa jenis dari *Watermarking :* Secara garis besar, ada dua jenis watermarking:

1. Robust watermarking : Jenis watermark ini tahan terhadap serangan (attack), namun biasanya watermark yang dibubuhi ke dokumen masih dapat ditangkap oleh indera penglihatan atau pendengaran manusia.
2. *Fragile watermarking :* Jenis *watermark* ini akan mudah rusak jika terjadi serangan, namun kehadirannya tidak terdeteksi oleh indera manusia. Jika diinginkan untuk membuat suatu algoritma yang dapat mengimplementasikan *watemarking* yang memiliki *fidelity* yang tinggi (adanya *watermark* tidak disadari oleh pengamatan manusia) maka hasilnya akan semakin rentan terhadap serangan.

Dalam proses watermarking, terdapat tiga tahap utama berikut :

1. Mengintegrasikan watermark pada citra (embedding)
2. Serangan terhadap citra yang telah dibubuhi watermark, baik yang disengaja (misalnya dikompresi, dipotong sebagian, di-filter, dan sebagainya) ataupun yang tidak disengaja (misalnya disebabkan oleh noise atau gangguan dalam saluran transmisi data).
3. Proses ekstraksi watermark dari dokumen yang akan diuji.

Untuk mendapatkan suatu teknik digital watemarking yang baik, maka teknik tersebut harus dapat memenuhi kondisi. Elemen dari suatu data digital dapat secara langsung dimanipulasi dan informasi dapat ditumpangkan ke dalam data digital tersebut.

Watermark dapat dideteksi dan diperoleh kembali meskipun setelah data digital diubah sebagian, dikompresi, ataupun di-filter. Struktur dari watermark membuat penyerang sulit untuk mengubah informasi yang terkandung di dalamnya. Proses untuk membubuhkan watermark dan mendeteksinya cukup sederhana. Jika watermark dihapus, maka kualitas dari data digital yang ditumpanginya akan berkurang jauh atau bahkan rusak sama sekali. Informasi watermark yang diselipkan dalam isi data digital dapat dideteksi ketika dibutuhkan.

Teknik ini sangat baik digunakan untuk melindungi hak cipta.

Penggunaan watermarking pada beberapa media:

- *Watermarking* pada video digital harus sedemikian rupa sehingga peralihan gambar dari satu frame ke frame lainnya harus tetap baik dan tidak terlihat dimodifikasi. Karena video digital ukurannya relatif besar daripada citra, maka watermark yang disisipkan dapat lebih banyak.
- Khusus watermarking pada data audio, kehati-hatian perlu dilakukan pada perancangan algoritma watermarking-nya, karena suara lebih sensitif daripada gambar. Hal ini berarti suara digital lebih mudah rusak bila ditambahkan watermarking.
- Watermarking pada dokumen teks menggunakan metode yang berbeda daripada 3 media lainnya. Salah satunya dengan menyisipkan spasi antara dua buah kata atau antara dua buah kalimat di dalam dokumen.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil dan pembahasan diatas, maka dapat disimpulkan bahwa keamanan multimedia sangat penting.

Ada banyak teknik keamanan data, tetapi yang umum digunakan adalah *cryptography*, *steganography* dan *watermarking.*

Dari hasil analisa dan melihat kekurangan dan kelebihan dari masing-masing teknik, teknik yang baik digunakan untuk pengamanan data adalah *steganography*. Tetapi, seringkali *steganography* dan *cryptography* digunakan secara bersaman ini bisa menjamin keamanan pesan rahasianya.

Banyak yang mengatakan bahwa teknik *watermarking* itu adalah bagian dari *steganography*, tetapi hasil dari analisis *watermarking* hanya mirip saja dengan *steganography* (dilihat dari tekniknya). Dalam *steganography* yang penting adalah isi di dalam karyanya (karya rusak tidak masalah, hanya isi didalamnya harus benar-benar aman) . Sedangkan *watermarking* karyanya yang harus tetap terjaga dengan baik.

Untuk menjaga data tetap aman dan hak cipta tetap terjaga baiknya gunakan teknik *steganography* dan *watermaking.*

DAFTAR PUSTAKA

1. Solihin, Achmad, *Digital watermarking untuk melindungi informasi multimedia*,
2. Hidayat Eka Wahyu, 2011, *Metode Pengembangan Perangkat Lunak Berbasis Multimedi*, Forum Penelitian, 7(1) : 97-102
3. Arifin Rian, Oktaviana Lucky Tri, *Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB,*
4. Setiawan Rahmansyah Budi, *Penggunaan Kriptografy dan Steganografy Berdasarkan Kebutuhan dan Karakteristik Keduany,*
5. Tarbudhi, *Membangun Aplikasi Keamanan Transmisi Data Multimedia Menggunakan Kriptografi Algoritma Data Encryption Standard (DES),*
6. Utomo Prasetyo Tri, *Stegongrafi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Onlie*
7. Nurhayati Oki Dwi, *Keamanan Multimedia*, Semarang : Universitas Dipenogoro
8. Munir Rinaldi, 2004, *Steganografi dan Watermarking*, Bandung : Institute Teknologi Bandung
9. Hidayat Eka Wahyu, *Sistem Multimedia*, Tasikmalaya : Universitas Siliwangi