TUGAS MAKALAH

STEGANOGRAPHY DAN TEKNIK WATERMARKING

Di Susun Oleh :

Muhammad Afdhol Sodiq

1410652005

PROGRAM TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2017

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Allah SWT yang telah memberikan rahmat serta karunia-Nya kepada kami sehingga kami berhasil menyelesaikan Makalah ini yang alhamdulillah tepat pada waktunya yang berjudul “Keamanan Multimedia”. Diharapkan Makalah ini dapat memberikan informasi kepada kita semua tentang membangun pendidikan yang berkarakter bagi anak usia dini.

Kami menyadari bahwa Makalah ini masih jauh dari sempurna, oleh karena itu kritik dan saran dari semua pihak yang bersifat membangun selalu kami harapkan demi kesempurnaan Makalah ini.

Akhir kata, kami sampaikan terima kasih kepada semua pihak yang telah berperan serta dalam penyusunan Makalah ini dari awal sampai akhir.Semoga Allah SWT senantiasa meridhai segala usaha kita.Amin.

Penulis

DAFTAR ISI

STEGANOGRAPHY

A. Definisi

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. **Kegunaan Steganografi**

Steganografi dapat digunakan untuk berbagai macam alasan, beberapa diantaranya untuk alasan yang baik, namun dapat juga untuk alasan yang tidak baik.Untuk tujuan legitimasi dapat digunakan pengamanan seperti citra dengan watermarking dengan alasan untuk perlindungan copyright.Digital watermark (yang juga dikenal dengan fingerprinting, yang dikhususkan untuk hal-hal menyangkut copyright) sangat mirip dengan steganografi karena menggunakan metode penyembunyian dalam arsip, yang muncul sebagai bagian asli dari arsip tersebut dan tidak mudah dideteksi oleh kebanyakan orang.

Steganografi juga dapat digunakan sebagai cara untuk membuat pengganti suatu nilai hash satu arah (yaitu pengguna mengambil suatu masukan panjang variabel dan membuat sebuah keluaran panjang statis dengan tipe string untuk melakukan verifikasi bahwa tidak ada perubahan yang dibuat pada variabel masukan yang asli). Selain itu juga, steganografi dapat digunakan sebagai tag-notes untuk citra online. Steganografi juga dapat digunakan untuk melakukan

perawatan atas kerahasiaan informasi yang berharga, untuk menjaga data tersebut dari kemungkinan sabotasi, pencuri, atau dari pihak yang tidak berwenang.

C. Teknik Steganografi

Tujuan dari teknik-teknik steganografi adalah menyembunyikan keberadaan pesan.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*.Model yang ditunjukkan pada Gambar 1 menunjukkan sistem steganografi yang umum digunakan pada gambar.Pesan rahasia disisipkan ke dalam medium menggunakan sebuah teknik steganografi tertentu untuk menghasilkan *stego-image* (*stego-object*).Keamanan dari steganografi ini bergantung pada kunci, yang hanya diketahui oleh pengirim dan penerima pesan.Dalam sistem steganografi yang kuat, hanya pihak yang memiliki kuncilah yang dapat melakukan ekstraksi pesan.Pemanfaatan kunci dalam melakukan penyisipan dan pengekstraksian pesan unik bagi setiap teknik steganografi.

Tujuan lainnya adalah membuat informasi yang disisipkan tidak dapat dibedakan dengan derau-derau acak lain yang ada dalam gambar. Secara umum, gambar yang memiliki lebih banyak detail akan memiliki lebih banyak derau. Contohnya, gambar langit biru yang bersih memiliki derau yang lebih sedikit dibandingkan dengan gambar stadion bola yang dipenuhi penonton.Untuk meningkatkan pengamanan, penggunaan steganografi dikombinasikan dengan kriptografi. Pesan yang akan disisipkan dienkripsi terlebih dahulu menggunakan metode kriptografi tertentu. Dalam menyisipkan informasi, ada beberapa faktor yang saling berkompetisi satu sama lain. Gambar 2 menunjukkan tiga faktor yang saling berkompetisi ini: *capacity*, *undetecability*, dan *robustness*.

Penyisipan informasi dengan jumlah yang lebih banyak dapat saja mengubah *cover-object* sehingga keberadaan informasi dapat dengan mudah dideteksi.Anti-deteksi adalah kemampuan untuk menghindari deteksi.Kekokohan adalah ukuran ketahanan teknik steganografi dalam menghadapi berbagai macam manipulasi terhadap medium.

D. Terminologi dalam Steganografi

Terdapat beberapa istilah yang berkaitan dengan steganografi.

Ø Hiddentext atau embedded message: pesan atau informasi yang disembunyikan.

Ø Covertext atau cover-object: pesan yang digunakan untuk menyembunyikan embedded message.

Ø Stegotext atau stego-object: pesan yang sudah berisi embedded message. Dalam steganografi digital, baik hiddentex atau covertext dapat berupa teks, audio, gambar, maupun video.

E. 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

Beberapa istilah yang sering digunakan dalam teknik steganografi:

Ø Carrier file : file yang berisi pesan rahasia tersebut

Ø Steganalysis : proses untuk mendeteksi keberadaanpesan rahasia dalam suatu file

Ø Stego-medium : media yang digunakan untuk membawa pesan rahasia

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

Ø Payload : informasi yang akan disembunyikan Cara yang harus dilakukan saat menggunakan digital watermarking adalah menghapus file asli dari carrier file. Karena jika tidak bila dilakukan perbandingan dengan berbagai cara, perbedaan antara keduanya dapat diketahui sehingga pesan dapat diketahui oleh orang lain. Walaupun sekarang tanpa file asli beberapa jenis steganografi dapat diktahui, caa ini merupakan cara yang harus dilakukan untuk setidaknya mengurangi kemungkinan untuk dilakukannya perbandingan.

B. Teknik Watermarking

1. Kegunaan Watemarking

Ada 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* digunakan sebagai metoda untuk menyembunyikan label hak cipta pada data *digital* atau sebagai bukti autentik kepemilikan atas dokumen *digital* tersebut.

Ø 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.

Ø *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.

Ada tiga tahap utama dalam proses watemarking :

§ mengintegrasikan watermark pada citra (embedding)

§ 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).

§ proses ekstraksi watermark dari dokumen yang akan diuji.

2. Syarat-syarat Sebuah Digital Watemarking yang Ideal

Untuk mendapatkan suatu teknik digital watemarking yang baik, maka teknik tersebut harus dapat memenuhi kondisi adalah : Elemen dari suatu data digital dapat secara langsung dimanipulasi dan informasi dapat ditumpangkan ke dalam data digital tersebut Penurunan kualitas dari data digital setelah dibubuhkan watermark, dapat seminimal mungkin.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. Label hak cipta yang unik mengandung informasi pembuatan, seperti nama, tanggal, dan sebagainya, atau sebuah kode hak cipta seperti halnya ISBN (International Standard for Book Notation) pada buku-buku. Watermark tidak dapat diubah atau dihapus (robustness) secara langsung oleh orang lain atau dengan menggunakan software pengolahan sinyal sampai tingkatan tertentu. Watemarking yang diberikan lebih dari satu kali dapat merusak data digital aslinya. Cara ini dilakukan supaya orang lain tidak dapat melakukan pelabelan berulang terhadap data yang telah dilabel. Sampai saat ini, belum ada teknik watemarking yang dapat memenuhi seluruh kriteria di atas.

Metode audio watermarking yang sering dikaji dapat dibagi menjadi :

a. Domain waktu

Metode ini bekerja dengan cara mengubah data audio dalam domain waktu yang akan disisipkan watermark. Contohnya dengan mengubah LSB (Least Significant Bit) dari data tersebut. Secara umum metode ini rentan terhadap proses kompresi, transmisi dan encoding. Beberapa teknik algoritma yang termasuk dalam metode ini adalah:

a) Compressed-domain watermarking : Pada teknik ini hanya representasi data yang terkompresi yang diberi watermark. Saat data di uncompressed maka watermark tidak lagi tersedia.

b) Bit dithering: Watermark disisipkan pada tiap LSB, baik pada representasi data terkompresi atau tidak. Teknik ini membuat derau pada sinyal.

c) Amplitude modulation: Cara ini membuat setiap puncak sinyal dimodifikasi agar jatuh ke dalam pitapita amplitudo yang telah ditentukan

d) Echo hiding: Dalam metode ini salinan-salinan terputus-putus dari sinyal dicampur dengan sinyal asli dengan rentang waktu yang cukup kecil. Rentang waktu ini cukup kecil sehingga amplitudo salinannya cukup kecil sehingga tidak terdengar.

b. Domain frekuensi

Metode ini bekerja dengan cara mengubah spectral content dalam domain frekuensi dari sinyal. Misalnya dengan cara membuang komponen frekuensi tertentu atau menambahkan data sebagai derau dengan amplitudo rendah sehingga tidak terdengar. Beberapa teknik yang bekerja dengan metode ini:

a) Phase coding : Bekerja berdasarkan karakteristik sistem pendengaran manusia (Human Auditory System) yang mengabaikan suara yang lebih lemah jika dua suara itu datang bersamaan. Secara garis besar data watermark dibuat menjadi derau dengan amplitudo yang lebih lemah dibandingkan amplitudo data audio lalu digabungkan

b) **Frequency band modification :**Informasi *watermark* ditambahkan dengan cara membuang atau menyisipkan ke dalam pita-pita (*band*) *spectral* tertentu.

c) Spread spectrum : Dalam metode ini, sinyal yang membawa data *watermark* dimodulasikan ke dalam derau pita lebar (*wideband noise*) setelah sebelumnya di multiplikasi dengan suatu*pseudorandom sequence*.

3. Watemarking pada WWW 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. *Watemarking* dapat digabungkan ke dalam sistem enkripsi-dekripsi dalam salah satu dari dua cara berikut :

Ø **Browser-based watermarking** : Metoda ini akan secara langsung menggunakan *Java applet* untuk menerapkan *watemarking* pada citra. Kompleksitas pada pemodelan *Java* ini adalah tidak tersedianya kontrol yang bagus untuk menampilkan warna dengan *applet* yang ada. Oleh karena itu, teknik *watemarking* yang didasarkan pada penggunaan pemetaan warna untuk mengkodekan watermark tidak dapat diterapkan.

Ø CGI-based **watermarking** : Mekanisme ini akan menambahkan watermark pada dokumen sebelum dienkripsi dan dikirim ke browser. Pada pendekatan berdasarkan CGI, proses watemarking dilakukan di server, sehingga lebih rumit dan proses komputasi akan lebih berat lagi. *Watemarking* pada level-CGI juga memastikan bahwa proses tidak dapat digagalkan oleh serangan yang disebabkan oleh proses dekripsi berbasis bahasa pemrograman *Java*. Jadi, kekurangan teknik ini hanyalah terletak pada beban komputasi yang cukup besar di sisi *server*.

Mengapa perlu watermarking ?

Berikut adalah masalah yang melatarbelakangi munculnya *watermarking*.

Ø Masalah kepemilikan. Pemalsuan atas kepemilikan produk digital seringterjadi. Foto digital, misalnya, tidak memiliki suatu label atau informasi pengidentifikasi yang melekat pada foto tersebut. Apabila ada klaim dari pihak lain yang juga mengaku sebagai pemilik sah atas foto digital tersebut, pemilik foto yang asli tidak dapat memberikan bantahan karena memang ia tidak memiliki bukti otentik yang menandakan kepemilikan.

Ø Masalah pelanggaran hak cipta. Penggandaan yang tidak berizin atas produk digital dapat merugikan pemiliknya sebab pemilik produk digital tidak memperoleh royalti apapun terhadap penggandaan ilegal tersebut.

Ø Masalah keaslian. Produk digital mudah diubah. Perubahan tersebut dapat berupa rekayasa terhadap produk yang asli, baik perubahan yang dapat dipersepsi maupun tidak. Perubahan yang timbul dapat menyebabkan informasi penting yang terdapat di dalam produk digital hilang. Kriptografi biasa saja tidak dapat menyelesaikan masalah-masalah di atas. Meskipun produk-produk digital dienkripsi, menggunakan algoritma RSA sekalipun, cukup sekali saja diperlukan dekripsi produk-produk digital tersebut. Setelah enkripsi dihilangkan, produk-produk digital tadi dapat langsung diperbanyak dan disebarkan tanpa perlu melakukan dekripsi lagi. Selain itu, tidak terdapat jejak yang dapat menunjukkan bahwa seseorang bertanggung jawab atas penyebaran produk digital ataupun otentikasi mengenai hak seseorang atas produk digital tersebut.

BAB III
KESIMPULAN

Sebuah peranan sangat penting dalam system keamanan Multimedia ,dalam teknik watermakerting serta steganography, menyimpulakan bahwa hanya dalam mengandalkan teknik keamanan yang sederhana saja untuk membangun sebuah keamanan yang ideal dalam sebuah multimedia. Beberapa teknik steganography bisa dikombinasikan untuk menghasilkan tingkat keamanan yang lebih tinggi. Selain itu, proteksi pada sisi hardware dan operating system teknik watermarketing dibutuhkan untuk mendukung aplikasi serta keamanan multimedia Dari studi literatur yang dilakukan penulis dan dari hasil percobaan watemarking menggunakan tool Digimarc Demo Version, teknik watemarking yang ada sampai saat ini semuanya menambahkan tanda watermark pada seluruh bagian citra digital.

Keterbatasan manusia pada indera penglihatan dapat dimanfaatkan, terutama pada perubahan warna yang sangat sedikit dan perubahan kecil pada intensitas gambar. Penulis berkesimpulan bahwa dengan memberikan perubahan kecil pada warna di sebagian daerah berintensitas sangat rendah dari suatu citra digital (watemarking parsial), maka akan diperoleh citra yang sudah diberi tanda yang memiliki fidelity yang sangat baik, yaitu tingkat degradasinya tidak dirasakan oleh pengamatan manusia. Bila teknik ini diterapkan dengan menggunakan Java Script untuk menyisipkan informasi dekoder untuk menerjemahkan dokumen terenkripsi di WWW, maka tentunya keamanan di internet dapat lebih ditingkatkan lagi.

Sumber : http://rhyoeozonit29tugaskuliah.blogspot.co.id/2013/11/contoh-makalah-multimedia-steganography.html