Teknik Penyembunyian Pesan Rahasia Pada Berkas Video

Mohamad Ray Rizaldy – NIM : 13505073

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15073@students.if.itb.ac.id

Abstrak

Makalah ini membahas bagaimana cara sederhana dalam steganografi untuk menyembunyikan pesan dalam sebuah berkas Video. Steganografi merupakan ilmu serta seni dalam menyembunyikan pesan yang sudah digunakan sejak zaman perang. Steganografi memungkinkan pesan rahasia bisa dikirim lewat jalur yang tidak aman sekalipun tanpa terdeteksi oleh pihak lain yang tidak berhak mendapatkannya. Steganografi terdiri beberapa komponen, yaitu *embedded message* yang akan disisipkan, *cover-object* yang digunakan sebagai pembungkus pesan rahasia, serta *stego-key*. *Stego-key* adalah kunci yang digunakan untuk membangkitkan posisi acak untuk meletakkan *embedded message* pada *cover-object*.

Ada beberapa metoda steganografi yang umum digunakan dalam menyisipkan pesan ke dalam suatu media. Metoda yang pertama adalah metoda manipulasi LSB. Ada juga metoda *spread spectrum*, lalu metoda *Discrete Cosine Transform* (DCT) dan *Wavelet Compression.*

Steganografi bisa menggunakan berbagai medium sebagai pembungkus pesannya. Medium tersebut bisa berupa teks, gambar, audio, maupun video. Ada banyak format video yang beredar dan sering kita gunakan menonton. Dari segala format video yang ada tersebut semua bisa dipakai sebagai *cover-object* untuk membungkus pesan rahasia di dalamnya. Karena video merupakan kumpulan dari gambar-gambar yang tersusun secara sekuensial, pada dasarnya teknik penyembunyian pesan rahasia pada berkas video sebagian besar mirip dengan penyisipan pesan pada berkas gambar biasa. Meski begitu umumnya hanya dua metoda yang biasa digunakan dalam penyisipan pesan pada video yaitu metoda DCT dan *Wavelet Compression.*

***Kata kunci** : steganografi, video, format, medium*

1. Pendahuluan

Komunikasi merupakan satu hal yang tak terpisahkan dari kehidupan manusia. Tiap manusia pasti membutuhkan komunikasi dengan manusia lainnya. Seiring berkembangnya teknologi, kini manusia dapat berkomunikasi melalui berbagai media digital. Di sisi lain, komunikasi melalui media digital ini mudah menyebar ke banyak pihak, meskipun pengguna komunikasi tidak menginginkannya.

Untuk mengatasi hal tersebut diperkenalkanlah teknologi kriptografi. Dengan teknik kriptografi pesan asli yang ingin dikirimkan (*plaintext*) diubah atau dienkripsi dengan suatu kunci menjadi suatu informasi acak yang tidak bermakna(*ciphertext*). Kunci yang hanya diketahui oleh pengirim dan penerima, kemudian bisa digunakan untuk mengembalikan *ciphertext* ke plaintext oleh penerima. Dengan begitu, orang lain yang tidak memiliki hak akses terhadap pesan tersebut tidak dapat mengetahui isi pesan sebenarnya, hanya mengetahui pesan acaknya saja.

Namun karena sifatnya yang acak itu, timbul suatu kecurigaan terhadap pesan yang dikirim. Karena terlihat pesan tersebut seperti tidak mempunyai arti, maka bisa saja pihak luar akan merusak pesan tersebut dengan tujuan agar penerima tidak mendapatkan pesan tersebut secara utuh. Untuk mengatasi masalah ini, dapat digunakan teknik lain yaitu teknik steganografi.

Menurut kabar, jaringan teroris di timur tengah menggunakan teknik ini dalam bertukar pesan. Medium yang dipakainya adalah medium audio visual. Bagaimana hal tersebut bisa dilakukan? Selanjutnya, dalam makalah ini akan dibahas

mengenai penggunaan steganografi untuk menyembunyikan pesan rahasia melalui medium audio visual.

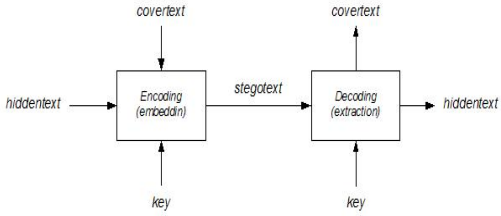
2. Steganografi

Steganografi merupakan ilmu sekaligus seni menyembunyikan sebuah pesan rahasia. Dalam steganografi, pesan rahasia disimpan sedemikian rupa dalam pesan lain sehingga tidak dapat dilihat secara kasat mata. Adapun beberapa medium yang digunakan untuk menyebunyikan pesan, termasuk di dalamnya medium gambar (visual), suara (audio) bahkan video (audio visual).

Untuk melakukan teknik steganografi setidaknya ada 4 properti :

1. *Embedded message* : pesan yang ingin disembunyikan.
2. *Cover Object* : pesan lain yang digunakan untuk menyembunyikan *embedded message*.
3. Stego-*Object* : pesan baru yang sudah berisi *embedded message*
4. *Stego-key* : kunci yang digunakan untuk menyisipkan dan mengekstraksi *embedded message*.

Adapun skema penyisipan dan pengekstrasian *embedded message* ditunjukkan pada gambar



Gambar 1 Skema penyisipan dan ekstraksi pesan pada steganografi

2.1 Kriteria Steganografi

Dalam steganografi ada beberapa kriteria utama yang yang digunakan dalam menilai kualitas steganografi. Kriteria-kriteria tersebut yaitu :

1. ***Imperceptible***, semakin pesan rahasia tidak dapat dipersepsi semakin bagus stego-*object*.
2. ***Fidelity***, mutu *cover-object* tidak jauh berubah dibanding sebelum dimasukan *embedded message*.
3. ***Recovery***, tak ada gunanya jika pesan rahasia tidak dapat diekstrak dari stego-*object*. Oleh karenanya suatu stego-*object* yang bagus adalah yang bisa diekstrak kembali menjadi pesan.
4. ***Capacity***, merupakan besar data yang bisa disisipkan dalam sebuah *cover*, dibandingkan dengan besarnya *cover* itu sendiri. Kapisitas penyimpanan ini juga sering disebut sebagai payload.
5. ***Robustness***, kriteria ini tidak terlalu diutamakan karena tujuan utama dari steganografi adalah penyembunyian pesan sehingga tak terdeteksi.

2.2 Teknik Steganografi

Ada beberapa teknik yang bisa digunakan dalam menyisipkan pesan dalam suatu *cover object*. Teknik-teknik tersebut dibagi menjadi dua domain sebagai berikut :

1. *Spatial Domain*, caranya adalah memodifikasi langung nilai *byte* dari *cover-object*, dimana nilai *byte* merupakan representasi dari intensitas/warna tiap pixel.
2. *Transform Domain*, memodifikasi hasil transform sinyal dalam ranah frekuensi.

2.2.1 Metoda Pengubahan LSB

Metoda ini adalah bagian dari teknik spatial domain. Metoda LSB (*Least Significant Bit*) merupakan salah satu bentuk yang paling sederhana dalam steganografi. LSB adalah bit paling kanan. Pengubahan terhadap bit ini tidak akan berpengaruh dalam persepsi auditori atau visual.

Sebagai contoh pada penyisipan pesan pada file gambar 24-bit. Gambar 24-bit berarti pada tiap pixelnya mengandung 24-bit informasi warna. Pixel mengandung 3 X 3*byte* terdiri dari 1 *byte* warna merah, 1 *byte* warna biru dan 1 *byte* sisanya warna hijau.

- *Embedded message* yang ingin disisipkan misalnya adalah bit 010
- Sisipkan pada sebuah pixel berwarna merah yang bernilai 00110011-10100010-11100010
- Ganti tiap LSB dengan bit pada *embedded message*.
- Hasilnya adalah pixel yang bernilai 00110010-10100011-11100010. Pixel

tersebut tetap berwarna merah dengan sedikit perubahan intensitas warna yang tak terdeteksi oleh mata.

Dengan metoda LSB ini untuk setiap *cover object* gambar 24-bit berukuran 256 X 256 pixel besar pesan yang bisa disisipkan adalah sebesar 24567 *byte*.

Teknik sederhana seperti di atas bisa diperkuat dengan cara mengubah pola penyembunyian data. Bit-bit data *embedded message* tidak disisipkan pada *byte-byte cover* secara berurutan, namun dipilih susunan *byte* secara acak.

Untuk membuat susunan tersebut diperlukan sebuah pembangkit bilangan acak-semu yang disebut sebagai *pseudo-random number generator* (PRNG). Generator ini memerlukan sebuah umpan atau seed untuk mulai membangkitkan. Seed inilah yang berlaku sebagai kunci atau *stego-key*.

2.2.2 Metoda *Spread Spectrum*

Metoda lain yang merupakan bagian dari transform domain adalah metoda *spread spectrum*. Definisi dari *spread spectrum* sendiri adalah teknik pentransmisian dengan menggunakan *pseudo-noise-code*. *Code* ini bersifat independen terhadap data pesan dan berfungsi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.

Steganografi dengan metoda *spread spectrum* salah satu caranya adalah dengan menempatkan data *embedded message* pada keseluruhan *cover-object*.

Untuk melakukan penyisipan, data pesan diubah dulu menjadi gangguan semu (*pseudo-noise*). Gangguan semu ini kemudian disisipkan ke dalam *cover-object* menjadi *stego-object*. Ada tiga kunci yang digunakan dalam metoda ini. Kunci pertama digunakan untuk mengenkripsi informasi. Kunci kedua digunakan untuk membangkitkan gangguan semu. Dan kunci ketiga digunakan untuk memasukan dan menyebarkan data yang telah dimodulasi ke dalam *cover-object* sedemikian rupa sehingga penyisipan informasi sesedikit mungkin mempengaruhi *cover-object*.

2.2.3 Metoda *Discrete Cosine Transform*ation

Metoda ini dikenal cukup rumit. Untuk menyembunyikan pesan pada sebuah berkas gambar, diperlukan *Discrete Cosine Transform*ation (DCT).

DCT digunakan terutama pada berkas gambar JPEG, untuk mentransformasikan blok 8x8 pixel yang berurutan dari gambar menjadi 64 koefisien DCT. Setiap koefisien DCT F(u,v) dari blok 8x8 pixel gambar f(x,y) dihitung sebagai berikut :

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * cos\frac{(2x+1)u\pi}{16} cos\frac{(2y+1)v\pi}{16}\right]$$

Dengan C(x) =1/√2 jika x=0 dan C(x)=1 jika x=1.

Usai koefisien-koeifisen diperoleh, dilakukan proses kuantisasi :

$$F^{Q}(u,v) = \left\lfloor \frac{F(u,v)}{Q(u,v)} \right\rfloor$$

Dengan Q(u,v) adalah 64 elemen tabel kuantisasi.

Berikut Algoritma penyembunyian pesan dalam berkas JPEG :

```
Input : pesan, cover image
Output : stego
while (masih ada data untuk di-embed)
do
   ambil koefisien DCT selanjutnya
   dari cover image (DCT)

   if koefisien < nilai treshold then
        ambil bit selanjutnya dari
        pesan

        ganti bit koefisien DCT dengan
        bit pesan tersebut
   end if
   masukkan DCT ke stego (invers DCT)
end while
```

2.2.4 Metoda *Wavelet Compression*

Wavelet Compression adalah salah satu cara kompresi data yang cocok digunakan untuk

kompresi gambar, audia dan video. Tujuannya adalah menyimpan data dalam berkas yang sekecil mungkin. Dengan metoda ini hilangnya informasi tertentu memang sudah diharapkan terjadi.

Sama dengan DCT, *Wavelet Compression* juga termasuk dalam domain frekuensi (transform). Bedanya, wavelet lebih baik dalam merepresentasikan daerah transien, contohnya gambar bintang pada langit malam. Artinya elemen dari data yang transien akan direpresentasikan dalam jumlah informasi yang lebih kecil. Sayangnya metoda ini justru kurang baik pada data yang bersifat periodik dan halus.

Dalam wavelet, yang pertama kali dilakukan adalah transformasi yang akan menghasilkan koefisien sesuai dengan jumlah pixel padal gambar sebagai berikut :

$$[W_\psi f](a,b) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} \overline{\psi\left(\frac{x-b}{a}\right)} f(x)dx$$

Koefisien wavelet c_{jk} diperoleh :

$$c_{jk} = [W_\psi f](2^{-j}, k2^{-j})$$

Dengan a=2-j. a disebut sebagai binary dilation. Juga b=k2-j dan disebut sebagai binary position. Jika c_{jk} diperoleh, koefisien ini dapat dikompresi dengan mudah karena informasi terkonsentrasi secara statistik pada beberapa koefisien tertentu saja. Hal ini disebut dengan transform coding.

Koefisien-koefisien tersebut kemudian dikuantisasi, lalu diencode dengan entropi encoding dan/atau run length encoding.

Algoritma dari metoda ini sebagai berikut :

```
Input : pesan, cover image
Output : stego
while (masih ada data untuk di-embed)
do
   ambil koefisien wavelet
   selanjutnya dari cover image
   (wavelet transform)

   if koefisien < nilai treshold then
        ambil bit selanjutnya dari
        pesan

        ganti bit koefisien wavelet
        dengan bit pesan tersebut dan
        kompresi
        (Wavelet Compression)
   end if

   masukkan koefisien tadi ke stego
   (invers wavelet transform)
end while
```

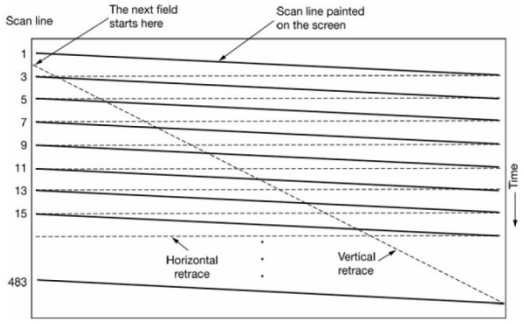
3. Video

Video secara sederhana diartikan sebagai kumpulan suatu gambar yang disusun sedemikian rupa sehingga gambar-gambar terlihat bergerak.

Pada mata manusia, ketika suatu objek masuk ke retina, butuh waktu beberapa milidetik hingga terbentuk sebuah gambaran di dalam otaknya. Hal ini menyebabkan jika ada sekumpulan gambar yang berubah dengan kecepatan lebih dari 50 gambar/detik, mata tidak bisa menangkapnya sebagai suatu gambar yang bergerak secara diskrit. Dari konsep inilah video kemudian dibuat.

3.1 Video Analog

Pada video analog, yang berwarna hitam putih misalnya, gambar dua dimensi yang terbentuk merupakan hasil representasi intensitas tembakan sinar electron dari ujung layar ke ujung lainnya yang terekam secara cepat oleh kamera. Sinar electron ini berpindah secara perbaris di layar. Tiap barisnya dikenal dengan istilah scan line. Setiap sekali rekamannya disebut satu bingkai (frame).



Gambar 2 Pola perekaman sinar untuk video NTSC

Untuk video yang berwarna pola perekamannya juga mirip dengan yang terjadi pada monokrom (hitam-putih) . Hanya saja pada video berwarna digunakan tiga penembak sinar yang bergerak secara bersamaan. Masing-masing penembak sinar mewakili warna merah, hijau dan biru, dengan suatu intensitas tertentu.

3.2 Video Digital

Mirip dengan video analog, representasi sederhana dari video digital adalah urutan dari

bingkai (frame). Tiap bingkainya terdiri dari jala-jala kecil *picture elements* yang dikenal dengan pixel.

Untuk menciptakan gerakan yang halus sebuah video digital harus menampilkan minimal 25 bingkai setiap detiknya. Tapi hingga saat ini monitor komputer sudah bisa melakukan perekaman hingga 75 kali atau lebih dalam sedetik. Saking cepatnya, monitor harus menggunakan perekaman progresif dengan menggambarkan ulang bingkai yang sama 1 sampai 3 untuk menghilangkan kedipan pada monitor.

3.3 Kompresi Berkas Video

Amat sangat besar ukuran datanya untuk memanipulasi sebuah berkas multimedia. Untuk itulah perlu adanya kompresi. Untuk berkas video ada dua jenis kompresi yang akan dijelaskan disini.

Dalam kompresi dikenal dua istilah yaitu encoding dan decoding. Encoding adalah memadatkan berkas multimedia menjadi data terkompresi. Sedangkan decoding adalah proses sebaliknya yang dilakukan oleh setiap pengguna yang ingin menonton video. Biasanya proses encoding bisa jauh lebih lama dibandingkan dengan proses decodingnya.

3.3.1 Standar Kompresi JPEG

Standar JPEG (Joint Photographic Experts Group) digunakan unuk kompresi gambar yang memiliki corak yang kontinu. Kompresi JPEG ini cukup kompleks dan sifatnya simetrik, sehingga waktu decodingnya sama lamanya dengan saat encoding.

3.3.2 Standar Kompresi MPEG

Standar MPEG (Motion Picture Experts Group) awalnya digunakan untuk memadatkan video berkualitas broadcast sampai 4 hingga 6 Mbps sehingga bisa masuk ke kanal broadcast NTSC maupun PAL.

3.4 Format Video

Sekarang ini banyak sekali format-format untuk berkas video yang beredar. Berikut ini adalah format-format yang sering digunakan :

- ASF (Advanced System Format) : dibuat Microsoft sebagai standar audio/video streaming format. Contoh ASF lain adalah WMA dan WMV dari Microsoft. ASF memiliki MIME ”type application/vnd.ms-asf”
- MOV (Quick Time) : dibuat oleh Apple supaya dapat lintas antar platform. Saat ini format MOV banyak digunakan untuk transmisi data di internet
- MPEG-1 : beresolusi 352 X 240 pixels dan hanya mensupport perekaman video secara progresif.
- MPEG-2 : menunjang format gambar yang salin terjalin dan sering digunakan pada HDTV maupun DVD video disc
- MPEG-4 : digunkana untuk streaming, CD distribution, dan broadcast television. Format ini mendukung terciptanya digital right management.
- DivX : diciptakan oleh DivX inc. Terkenal karena ukuran filenya kecil.

4. Steganografi Video

Pada dasarnya steganografi digital adalah menyisipkan bit-bit pesan pada sebuah *cover object*. *Cover object* bisa merupakan berkas apa saja baik berkas teks, berkas gambar, audio sampai visual. Jadi bisa disimpulkan semua berkas video juga bisa disisipkan *embedded message*.

Setiap berkas video terdiri dari bingkai-bingkai, dimana setiap bingkai merupakan sebuah gambar. Karena itu sebagaian besar metoda yang digunakan dalam steganografi gambar dapat digunakan pada steganografi video.

Dalam gambar setiap titik yang bertetanggaan biasanya berwarna hampir sama bahkan sama persis. Jika kita menggambil satu titik sembarang pada gambar, kita akan menemukan bahwa warna pada titik sebelahnya berkorelasi secara spasial.

Begitu juga yang terjadi pada video. Pada video terpadat korelasi sejenis. Hal ini karena bingkai yang berdekatan sering kali sangat mirip.

Pada penyisipan pesan ke dalam berkas video, metoda yang umum digunakan adalah metoda transformasi baik DCT maupun *Wavelet Compression*. Metoda modifikasi LSB tidak

dilakukan karena akan menghasilkan berkas stego yang berukuran sangat besar.

Langkah-langkah yang bisa ditempuh untuk menyembunyikan pesan pada *cover object* dengan bentuk video adalah sebagai berikut :

- Pilah video menjadi bingkai-bingkai gambar.
- Lakukan transformasi baik DCT maupun *Wavelet Compression* sehingga menghasilkan koefisien-koefisien yang akan dipilih berdasarkan suatu nilai treshold.
- Ganti koefisien tersebut dengan bit-bit data pesan yang akan disisipkan.
- Setelah seluruh pesan disisipkan, koefisien sebelumnya ditransformasi balik untuk menghasilkan stego-*object*.

Sebaliknya untuk mengekstraksi pesan dari sebuah stego *object* berbentuk video dilakukan cara berikut :

- Pilah video menjadi bingkai-bingkai gambar.
- Transformasi gambar untuk mendapatkan koefisien yang akan dipilih berdasarkan nilai treshold.
- Koefisien yang didapat merupakan bit-bit pesan yang telah disembunyikan.
- Tulis bit-bit tersebut ke file output untuk mendapatkan pesannya.

Sama halnya dengan gambar besarnya ukuran pesan yang dimasukkan juga akan berpengaruh terhadap kualitas video yang menjadi *cover-object*. Semakin besar ukuran pesan yang disisipkan semakin terlihat perubahan yang terjadi pada video.

5. Kesimpulan

1. Semua berkas video bisa dijadikan pembungkus atau *cover object* untuk menyisipkan pesan rahasia.
2. Tidak ada berkas video yang khusus dipakai untuk menyisipkan pesan
3. Ada beberapa metoda yang digunakan dalam steganografi, namun yang umum digunakan untuk menyisipkan pesan ke dalam berkas video adalah metoda *Discrete Cosine Transform* dan *Wavelet Compression*.
4. Karena video merupakan kumpulan dari gambar-gambar, penyisipan pesan ke dalam berkas video mirip halnya dengan penyisipan pesan ke dalam berkas gambar.

DAFTAR PUSTAKA

[1] Kim, Sung Min. (2007). Image Analysis and Recognition. Springer Berlin Heidelberg.

[2] Piva, Alesandro. (2008). Multimedia Services in Intelligent Environments. Springer Berlin Heidelberg.

[3] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[4] Antonie.(2005).Multimedia. *http://lecturer.ukdw.ac.id/anton/multimedia.php*. Tanggal akses: 2 April 2004 pukul 20:00.

[5] Liu, Bin. (2006). Multimedia Content Representation, Classification and Security. Springer Berlin Heidelberg.

[6] Tanenbaum, Andrew. (2003). Modern Operating System. Pearson Education International.