Penggunaan Steganografi Pada Produk Motion Picture Yang Dijual Secara Online Untuk Melacak Pelaku Pembajakan.

Khairul Fahmi – 13507125

Teknik Informatika, Institut Teknologi Bandung
Jalan Ganesha 10
e-mail: if17125@students.if.itb.ac.id

ABSTRAK

Pembajakan produk adalah salah satu permasalahan terbesar di industry berbasis digital. Produk berupa software, gambar, video, music dibajak tiap saat oleh pihak-pihak yang tidak bertanggung jawab. Pembajakan ini dibantu dengan mudahnya distribusi produk hasil bajakan lewat bermacam media seperti lewat internet, dan *physical disk* yang sangat portable.
Transaksi pembelian video secara online sekarang sudah banyak diterapkan. *User* mendaftar di penyedia layanan kemudian melakukan pemesanan video.
Video yang dijual kepada user dapat diberi penanda khusus berisi identitas user yang melakukan pembelian. Tanda ini dapat digunakan untuk melacak sumber produk bajakan.
Pemberian penanda dapat dilakukan dengan teknik-teknik steganography.

Keyword : steganoraphy, pembajakan, video.

1. PENGANTAR

Pembelian video (movie) secara online sudah banyak dilakukan sekarang. Pada pembelian seperti ini pelanggan mendaftarkan diri pada penyedia layanan (seperti amazon.com, ebay.com). Untuk melakukan pembelian, pelanggan terlebih dahulu melakukan otentikasi lalu melakukan transaksi. Setelah selesai transaksi, penyedia layanan menyampaikan video yang dipesan kepada pelanggan.

Seorang pelanggan yang tidak bertanggung jawab bisa saja melakukan pembajakan video tersebut. Video digandakan dan disebarkan ke orang lain baik untuk komersial maupun sekedar berbagi dengan rekan-rekannya. Jika ini terjadi (sejauh ini kondisi ini benar) *movie industry* dunia pasti dirugikan. Jumlah penjualan video akan berkurang, pendapatan orang-orang yang bekerja di *movie industry* berkurang sehingga mungkin saja menurunkan gairah orang-orang untuk menyalurkan kreativitasnya di *movie industry*.

Banyak cara yang dapat ditempuh untuk mencegah mundurnya *movie industry* karena pembajakan. Salah satu caranya adalah dengan menghukum pelaku pembajakan, terutama sumbernya. Akan tetapi untuk mengungkap sumber pembajakan tersebut sangatlah susah. Orang-orang bisa saja tutup mulut karena diancam atau memang karena loyalitas atau karena hal lainnya. Pada persoalan ini kita bisa menggunakan steganoraphy.

Dengan asumsi bahwa video yang dibajak berasal dari video original yang diperoleh secara legal kita dapat melakukan penelusuran pelaku pembajakan. Pada saat pelaku melakukan pembelian video yang original sebuah identitas yang unik di-*embed* ke video. Identitas pembajak dapat diketahui dengan melihat identitas di video tersebut sehingga pelaku bisa dibuktikan bersalah dan dihukum dengan harapn akan membuat takut orang lain untuk melakukan pembajakan.

2. SEJARAH STEGANOGRAPHY

Steganography sering sulit dibedakan dengan cryptography karena kemiripan fungsi kedua bidang tersebut dalam hal melindungi informasi yang penting. Perbedaan antara kedua bidang adalah dalam hal cara melindungi informasi. Steganography menyamarkan informasi pada media lain sehingga orang tidak merasakan keberadaan informasi tersebut. Sementara itu cryptography melindungi data dengan cara mengubah informasi ke bentuk yang tidak bisa dibaca atau dimengerti oleh orang yang tidak berhak.

Perbedaan antara keduanya adalah[1]

- Steganografi dapat dianggap pelengkap kriptografi (bukan pengganti).
- Steganografi: menyembunyikan *keberadaan* (*existence*) pesan.
  Tujuan: untuk menghindari kecurigaan *conspicuous*)
- Kriptografi: menyembunyikan *isi* (*content*) pesan
  Tujuan: agar pesan tidak dapat dibaca

Steganography pada dasarnya bekerja dengan memanfaatkan persepsi manusia. Indera manusia

tidak terlatih untuk melihat informasi yang di simpan di medium steganoraphy.

2.1. Sejarah

Steganography berasal dari bahasa Yunani Steganós (Covered) dan Graptos (Writing). Steganography secara teknis berarti pesan yang ditutupi atau pesan yang tersembunyi.

Catatan tertua mengenai penggunaan steganografi tercatat pada masa Yunani kuno. Pada saat itu, penguasa Yunani, Histiaues, sedang ditawan oleh Raja Darius di Susa. Histiaeus ingin mengirim pesan rahasia kepada menantunya, Aristagoras, di Miletus. Untuk itu, Histiaeus mencukur habis rambut budaknya dan menatokan pesan rahasia yang ingin dikirim di kepala budak tersebut. Setelah rambut budak tadi tumbuh cukup lebat, barulah ia dikirim ke Miletus.

Cerita lain masih juga berasal dari zaman Yunani kuno. Medium tulisan pada saat itu adalah papan yang dilapisi lilin dan tulisan ditulisi di papan tersebut. Demeratus, perlu memberitahu Sparta bahwa Xerxes bermaksud untuk menginvasi Yunani. Agar pesan yang dikirimnya tidak diketahui keberadaannya, Demeratus melapisi lagi papan tulisannya dengan lilin. Papan tulisan yang terlihat masih kosong inilah yang dikirim ke Sparta.

Tinta yang tidak nampak merupakan salah satu metode yang populer dalam bidang steganografi. Bangsa Romawi telah menggunakan tinta yang tidak nampak ini untuk menulis pesan di antara baris-baris pesan yang ditulis dengan tinta biasa. Tinta yang tidak nampak ini dapat terbuat dari sari jeruk atau susu. Ketika dipanaskan, warna tinta yang tidak tampak akan menjadi gelap dan tulisannya akan menjadi dapat terbaca. Tinta yang tidak tampak ini juga digunakan dalam Perang Dunia II.

Mayoritas penggunaan steganography adalah pada system yang menggunakan objek multimediaseperti gambar, audio, dan video. Sebagai cover media.

Steganography dibedakan jadi lima jenis berdasar objeknya.

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography
- Protocol Steganography

Steganography: ilmu dan seni menyembunyikan (*embedded*) informasi dengan cara menyisipkan pesan di dalam pesan lain [1].

Steganografi digital: steganografi pada data digital dengan menggunakan komputer digital

3. TEKNIK

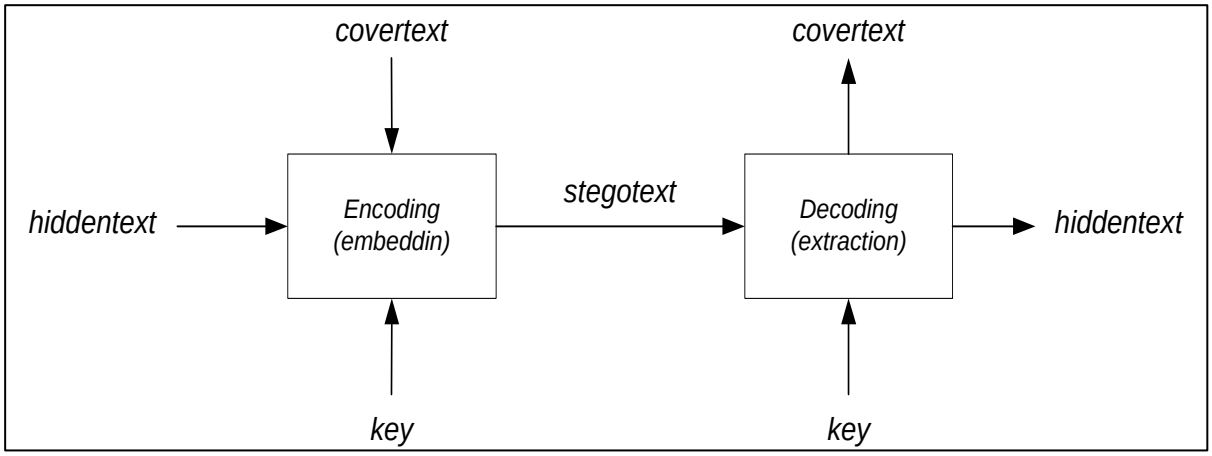
Dalam steganography terdapat beberapa term yang sering disebut properti steganography[1]

- *Embedded message* (*hiddentext)*: pesan yang disembunyikan.
- *Cover-object* (*covertext):* pesan yang digunakan untuk menyembunyikan *embedded message*.
- *Stego-object* (*stegotext):* pesan yang sudah berisi pesan *embedded message*.
- *Stego-key*: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stegotext.

Selain itu steganography yang bagus harus memiliki kriteria seperti[1]

- *Imperceptible* - Keberadaan pesan rahasia tidak dapat dipersepsi.
- *Fidelity* - Mutu *cover-object* tidak jauh berubah akibat *embedded.*
- *Recovery* - Data yang disembunyikan harus dapat diungkapkan kembali.
- *Robustness* – Tahan terhadap segala macam *stegobreak*.

Informasi bisa disembunyikan di dalam objek multimedia menggunakan berbagai teknik yang cocok. Sebagai cover object, bisa digunakan image,



audio or video file.

Secara umum teknik yang digunakan adalah:

- *Spatial (time) domain.* Memodifikasi langsung nilai *byte* dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna *pixel* atau amplitudo)
- *Tranform domain.* Memodifikasi hasil transformasi sinyal dalam ranah frekuensi.

Berdasarkan cover media teknik yang digunakan akan berbeda oleh spesialisasi dua metode yang generic diatas.

Secara umum metode *spatial domain* tidak robust jika dilakukan manipulasi terhadap *stego-object.*

Metode *transform domain* menyediakan hasil yang lebih robust[1]

Sinyal dalam ranah spasial/waktu diubah ke ranah frekuensi dengan menggunakan transformasi seperti

- *DCT* (*Discrete Cosine Transform*),
- *DFT* (*Discrete Fourier Transform*), dan
- *DWT* (*Discrete Wavelet Trabform*)

Penyisipan pesan dilakukan pada koefisien tranformasi. Keuntungannya adalah kokoh (*robust*) terhadap manipulasi pada *stego-object*.

Untuk tiap-tiap komponen warna sebuah image menggunakan *discrete cosine transform* (DCT) untuk mentransformasikan blok image menjadi koefisien DCT.

$$C(p,q)=\alpha_p\alpha_q\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}I(m,n)\cos\frac{\pi(2m+1)p}{2N}\cos\frac{\pi(2n+1)q}{2N}$$

Salah satu algoritma untuk melakukan encoding dari covertext dan pesan menjadi *stego-object* adalah seperti pada gambar berikut

```
Input: message, shared secret, cover
image
Output: stego image
initialize PRNG with shared secret
permutate DCT coefficients with PRNG
determine k from image capacity
calculate code word length n←2k – 1
while data left to embed do
  get next k-bit message block
  repeat
    G←{n non-zero AC coefficients}
    S←k-bit hash f of LSB in G
    S←s xork-bit message block
    if s != 0 then
       decrement absolute value of
       DCT coefficient Gs
       insert Gs into stego image
    end if
   until s = 0 or Gs ≠ 0
  insert DCT coefficients from into
  stego image
end while
```

3.1. Text Steganography

Menyembunyikan informasi di *plaintext* dapat dilakukan dengan bermacam cara[4]. Misalnya dengan melakukan modifikasi layout teks, menggunakan tiap karakter ke-N atau mengubah jumlah *white space* setelah baris atau antara kata-kata. Cara lain adalah meletakan informasi rahasia di cover media public seperi Koran, buku menggunakan sebuah kode yang terdiri dari kombinasi nomor halaman, nomor baris dan nomor karakter.

Contoh Text Steganography

Lupakan asal rumor itu, jaga agar matamu sehat atau turunkan ubanmu

Covertext:

upakan sal umor tu aga aga atamu ehat tau turunkan banmu

Hiddentext:

Lari jam satu

Stegotext:

Lupakan asal rumor itu, jaga agar matamu sehat atau turunkan ubanmu

Dengan mengirimkan pesan dalam bentuk stegotext di atas kecurigaan orang akan berkurang atau hilang sama sekali.

3.2. Image Steganography

Untuk menyembunyikan informasi dalam image, cara yang umum digunakan antara lain :

3.2.1. Least significant bit insertion

LSB adalah cara paling umum digunakan dalam steganography untuk melakukan *embedding* informasi pada cover media. Pada metode ini LSB dari bytes diganti dengan bit-bit pesan. Teknik ini bagus digunakan pada image, audio dan video karena mata dan telinga manusia tidak terlalu peka terhadap perbedaan yang sangat kecil pada cover media. Bagi mata manusia, image hasil proses LSB insertion akan terlihat identik dengan *covertex*[2, 5].

Misalkan penyisipan pada citra 24-bit.
Setiap *pixel* panjangnya 24 bit (3 x 3 *byte*, masing-masing komponen *R* (1 *byte*), *G* (1 *byte*), dan *B* (1 *byte*))

```
00110011 10100010 11100010
```

(misal *pixel* berwarna merah)

Misalkan *embedded message*: 010

Encoding:

```
00110010 10100011 11100010
```

(*pixel* berwarna "merah berubah sedikit", tidak dapat dibedakan secara visual dengan citra aslinya)

Jika pesan = 10 bit, maka jumlah *byte* yang digunakan = 10 *byte*

Contoh susunan *byte* yang lebih panjang:

```
00110011 10100010 11100010
10101011 00100110

10010110 11001001 11111001
10001000 10100011
```

Pesan yang akan disisipkan :

```
1110010111
```

Hasil penyisipan pada bit *LSB*:

```
00110011  10100011   11100011
10101010  00100110

10010111  11001000   11111001
10001001  10100011
```

Ukuran data yang akan disembunyikan bergantung pada ukuran *cover-object*.

Citra 24-bit:
ukuran 256 × 256 *pixel* = 65536 *pixel.*

Setiap *pixel* berukuran 3 *byte* (komponen *RGB*), berarti ada
65536 × 3 = 196608 *byte*.

Setiap 1 *byte* menyembunyikan satu bit di *LSB*-nya, maka ukuran data yang dapat disembunyikan:
196608/8 = 24576 *byte*

Untuk memperkuat teknik penyembunyian data, bit-bit data rahasia tidak digunakan mengganti *byte-byte* yang berurutan, namun dipilih susunan *byte* secara acak.

Pembangkit bilangan acak-semu (*PRNG*: *pseudo-random number generator*) digunakan untuk membangkitkan bilangan acak.

Umpan (*seed*) untuk bilangan acak berlaku sebagai kunci (*stego-key*).

Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan, maka maka *byte* yang diganti bit *LSB*-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49.

3.2.2. Masking and filtering

Metode masking and filtering biasanya digunakan pada image 24 bit grey scale. Caranya adalah dengan mengubah luminance. Masking lebih robust dibandingkan LSB insertion jika terhadap covertext dilakukan compression, cropping, and image processing.

3.2.3. Redundant Pattern Encoding

Teknik ini melakukan redundant pattern encoding, yang merupakan salah satu teknik spread spectrum. Cara kerjanya adalah dengan menyebarkan informasi ke semua bagian covertext(scatered). Teknik ini membuat hasil steganoraphy jadi lebih tahan terhadap cropping dan rotation[2, 4].

3.2.4. Encrypt and Scatter

Cara ini menggunakan teknik spread spectrum dan frequency hopping yaitu dengan cara menyebar informasi diseluruh gambar pada 8 channel dalam jumlah yang acak yang di-*generate* oleh window size sebelumnya dan data channel sebelumnya. Channel lalu di-*swap* kemudian dirotasi dan dikombinasikan satu sama lain. Tiap channel merepresentasikan satu bit.

3.3. Audio Steganography

Pada teknik ini, informasi disembunyikan pada file audio.Metode yang umum digunkan adalah

- LSB coding
- Parity coding
- Phase coding
- Spread spectrum
- Echo hiding

3.3.1. LSB coding

Pengubahan LSB dapat digunakan karena telinga manusia tidak akan bisa mendeteksi perubahan yang sangat kecil pada audio. Selain itu dapat juga dilakukan dengan memanfaatkan keadaan bahwa manusia hanya mendengarkan suara pada range frekuensi tertentu. Melakukan encoding informasi

dalam frekuensi diatas range tersebut membuat pesan tidak bisa dideteksi oleh telinga manusia keberadaannya.

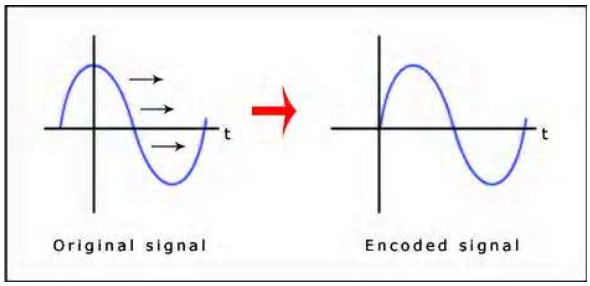
3.3.2. Parity coding

Pada parity coding, signal dipisahkan jadi region of sample dan melakukan encoding tiap bit dari informasi pada parity bit dari region sample.

3.3.3. Phase coding

Phase coding memiliki kelebihan dibanding cara lainnya karena phase coding tidak membuat noise pada hasil steganography. Phase coding berdasarkan fakta bahwa perubahan phase dari suara tidak sejelas noise pada telinga manusia. Efek dari perubahan phase tidak terlalu terdengar terasa di telinga dibanding efek dari noise.

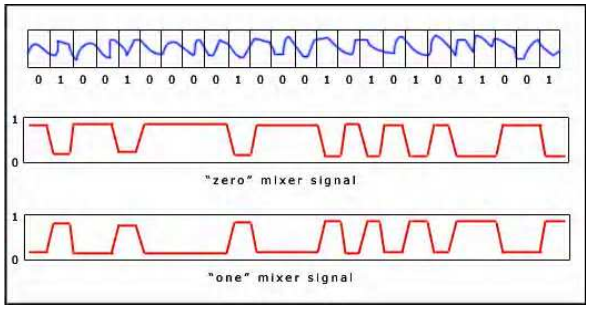
Teknik ini melakukan encoding bit-bit pesan dengan cara melakukan shifting phase pada spectrum sinyal digital menghasilkan suara yang tidak relative terdengar.



3.3.4. Echo hiding

Informasi di-*embed* ke dalam suara dengan melakukan *echo* ke signal diskrit. Seperti metode spread spectrum cara ini memberi kelebihan pada transmisi data yang besar dan robust dibanding metode yang menimbulkan noise.

Signal dipecah jadi blok, tiap blok dilakukan echo satu bit pesan kemudian blok digabungkan kembali membentuk sinyal akhir hasil proses steganography.



3.4. Video Steganography

Video pada dasarnya merupakan kombinasi beberapa image dengan audio. Teknik yang digunakan untuk melakukan penyisipan pesan pada video merupakan kombinasi teknik pada image dan audio. Kelebihan yang dipunyai video sebagai cover media adalah kapasitas pesan yang dapat disisipkan sangat besar.

4. IMPLEMENTASI

Berangkat dari fakta-fakta yang telah disebutkan, penggunaan steganography pada pelacakan pelaku pembajakan pada motion picture (movie atau film) dapat dilakukan sebagai berikut.

1. Menyediakan sistem penjualan yang terotentikasi. Semua pelanggan yang membeli sebuah film harus melakukan otentikasi terlebih dahulu. Untuk melakukan otentikasi, tiap pelanggan harus terlebih dahulu mendaftar.
2. Melakukan penyisipan identitas pelanggan yang melakukan pembelian yang unik dengan menggunakn metode steganography yang paling cocok.
3. Melakukan pemantauan pada film bajakan yang beredar kemudian melakukan ekstraksi identitas yang sudah disisipkan sebelumnya.
4. Mengidentifikasi pelaku atau sumber pembajakan berdasarkan identitas hasil ekstraksi.
5. Melakukan proses hukum yang tepat.

5. PEMBAHASAN

Untuk melakukan implementasi penggunaan steganography pada pelacakan pelaku pembajakan pada motion picture (movie atau film) banyak hal yang harus diperhatikan. Hal pertama adalah kebutuhan bahwa user harus melakukan otentikasi. Selama ini pola penjualan film pada system terotentikasi tidaklah terlalu besar. Pembelian film masih dilakukan dengan datang ke retailer, pesan, bayar, terima barang. Dengan system seperti ini penyisipan identitas untuk tiap barang yang dijual tidak mungkin dilakukan.

Akan tetapi dengan melihat perkembangan gaya hidup, teknologi dan faktor lainnya, transaksi pada suatu portal dengan mode terotentikasi dimasa yang akan datang akan semakin banyak digunakan. Jadi implementasi menjanjikan dilakukan jika melihat trend tersebut.

Pertimbangan kedua adalah kemungkinan bahwa identitas yang disisipkan akan hilang. Hal ini mungkin terjadi jika seseorang melakukan pengubahan pada content video. Seseorang bisa saja melakukan *ripping* pada video atau melakukan kompresi video atau pengubahan lain yang bisa saja menyebabkan

identitas yang disisipkan tidak bisa diekstraksi. Jika ini terjadi maka system akan gagal sama sekali.

Salah satu cara untuk mencegah ini terjadi adalah dengan menggunakan teknik steganography yang robust terhadap proses pengubahan content. Metode LSB tentu saja tidak cocok digunakan untuk encoding. Jika misalnya pada LSB kita menyimpan semua informasi identitas pada bit ke-8 pada tiap byte dan seseorang melakukan kompresi dengan membuang 2 bit atau 1 bit LSB tiap-tiap byte maka identitas akan hilang. Pemilihan metode encoding yang tepat sangat dibutuhkan disini. Salah satu metode adalah dengan menggunakan STEM[3].

Jika implementasi berjalan sesuai harapan, pelaku pembajakan dapat dilacak dan diproses semestinya. Konsekuensinya adalah angka pembajakan dapat berkurang drastis. Untuk produk digital lainnya seperti software, music, dan games dapat digunakan metode yang sama.

REFERENCES

[1] Munir, Rinaldi. *Diktat Kuliah Kriptografi*. 2006. Bandung: Institut Teknologi Bandung.

[2] Johnson, N. F. and Jajodia, S. *Exploring* Steganography: *Seeing The Unseen*.1998.

[3] Buchanan, J. Michael, *Creating Robust Form Of* Steganography, Thesis. 2004

[4] Krenn, Robert. Steganography *and Steganalysis*.

[5] Alain C. Brainos II. A Study Of Steganography And The Art Of Hiding Information

Bandyopadhyay, Samir K. *A Tutorial Review on* Steganography. 2008