

TUGAS KULIAH
EC 5010
KEAMANAN SISTEM INFORMASI

VIDEO
STEGANOGRAPHY

Oleh :

NAMA : **HENRY**

NIM : 132 03 057



PROGRAM STUDI TEKNIK ELEKTRO
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

2006

DAFTAR ISI

DAFTAR ISI	1
BAB I PENDAHULUAN	2
1.1 Latar Belakang	2
1.2 Tujuan	2
1.3 Batasan	2
BAB 2 TEORI DASAR	3
2.1 Pendahuluan	3
2.2 Manfaat Steganography	4
2.3 Steganography pada Image	5
2.3.1 Least-Significant Bit Modification	6
2.3.2 Masking dan Filtering	7
2.3.3 Transformation	7
2.4 Steganography pada Video	10
BAB 3 VIDEO STEGANOGRAPHY TOOLS	12
3.1 Pendahuluan	12
3.2 Penggunaan MSU Stego Video	13
3.3 Performansi MSU Stego Video	19
BAB 4 PENUTUP	26
4.1 Kesimpulan	26
4.2 Saran	26
DAFTAR PUSTAKA	27

BAB I

PENDAHULUAN

1.1 Latar Belakang

Steganography merupakan salah satu cara untuk menyembunyikan suatu pesan / data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Steganography dapat digunakan pada berbagai macam bentuk data, yaitu image, audio, dan video. Sudah banyak artikel yang membahas steganography, tetapi kebanyakan membahas steganography pada image dan audio. Sudah banyak metode yang dilakukan untuk steganography pada image dan audio ini dan sudah banyak pula metode steganalysis yang digunakan untuk mendeteksinya. Steganography pada video menggabungkan steganography pada image dan audio, pada dasarnya video merupakan gabungan image yang “bergerak” dan audio, yang lebih sulit dideteksi.

1.2 Tujuan

Artikel ini membahas video steganography dan menjelaskan tentang video steganography sebagai salah satu cara yang sedang berkembang dalam menjaga keamanan suatu informasi.

1.3 Batasan

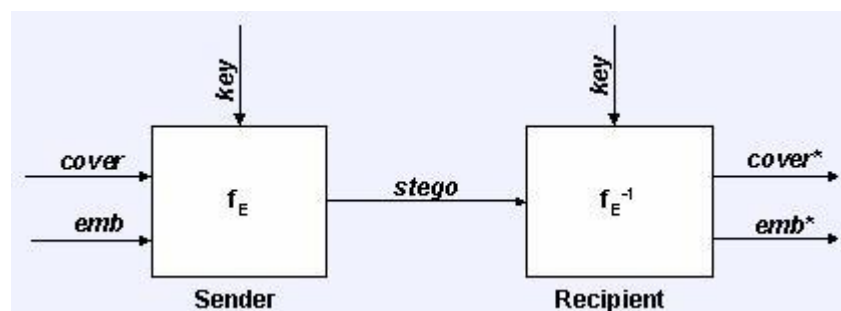
Dalam artikel ini, video steganography yang akan dibahas di sini adalah video steganography yang menyimpan pesan dalam video sebagai kumpulan image yang “bergerak” saja, tanpa audio.

BAB 2

TEORI DASAR

2.1 Pendahuluan

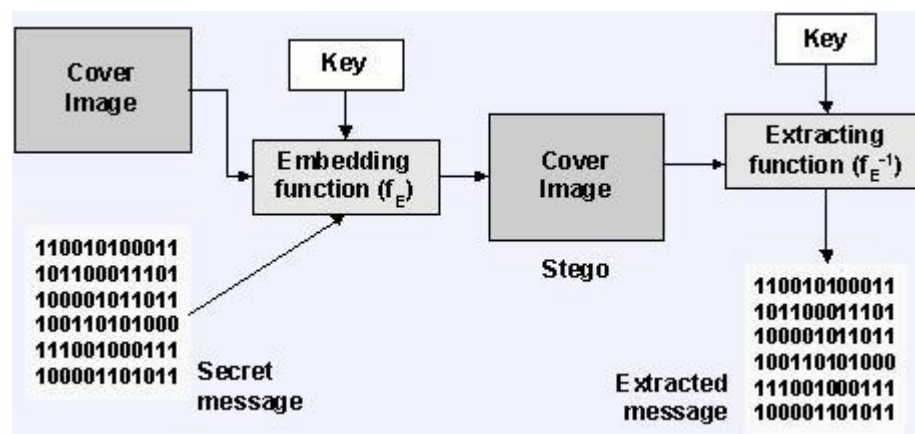
Steganography merupakan salah satu cara untuk menyembunyikan suatu pesan / data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Dalam bidang keamanan komputer, steganography digunakan untuk menyembunyikan data rahasia saat enkripsi tidak dapat dilakukan atau bersamaan dengan enkripsi. Jadi, walaupun enkripsi berhasil dipecahkan (decipher) pesan / data rahasia tetap tidak terlihat. Selain itu, pada cryptography pesan disembunyikan dengan “diacak” sehingga pada kasus-kasus tertentu dapat dengan mudah mengundang kecurigaan, sedangkan pada steganography pesan “disamarkan” dalam bentuk yang relatif “aman” sehingga tidak terjadi kecurigaan itu. Steganography dapat digunakan pada berbagai macam bentuk data, yaitu image, audio, dan video.



Gambar1 Steganographic System

Gambar 1 menunjukkan sebuah sistem steganography umum dimana di bagian pengirim pesan (**sender**), dilakukan proses embedding (f_E) pesan yang hendak dikirim secara rahasia (**emb**) ke dalam data cover sebagai tempat

meyimpannya (**cover**), dengan menggunakan kunci tertentu (**key**), sehingga dihasilkan data dengan pesan tersembunyi di dalamnya (**stego**). Di bagian penerima pesan (**recipient**), dilakukan proses extracting (f_E^{-1}) pada **stego** untuk memisahkan pesan rahasia (**emb**) dan data penyimpan (**cover**) tadi dengan menggunakan kunci yang sama seperti pada proses embedding tadi. Jadi hanya orang yang tahu kunci ini saja yang dapat mengekstrak pesan rahasia tadi. Proses tadi dapat direpresentasikan secara lebih jelas pada gambar 2 di bawah.



Gambar2 Graphical Version of a Steganographic System

Steganography bukan merupakan hal yang baru. Steganography sudah dikenal sejak zaman Romawi dan Yunani kuno. Misalnya, pesan ditulis di kepala budak lalu menunggu sampai tumbuh cukup rambut untuk menutupi pesan tersebut sebelum ia dikirim kepada orang yang dituju dimana rambutnya akan dicukur sehingga pesan itu terlihat.

2.2 Manfaat Steganography

Steganography adalah sebuah pisau bermata dua, ia bisa digunakan untuk alasan-alasan yang baik, tetapi bisa juga digunakan sebagai sarana kejahatan. Steganography juga dapat digunakan sebagai salah satu metode watermarking pada image untuk proteksi hak cipta, seperti juga digital watermarking (fingerprinting). Steganography juga dapat digunakan sebagai pengganti hash.

Dan yang terutama, seperti disebutkan sebelumnya, steganography dapat digunakan untuk menyembunyikan informasi rahasia, untuk melindunginya dari pencurian dan dari orang yang tidak berhak untuk mengetahuinya. Sayangnya, steganography juga dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain, yang tidak berhak, tanpa ada yang curiga. Steganography juga dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan yang lain.

Sehubungan dengan keamanan sistem informasi, steganography hanya merupakan salah satu dari banyak cara yang dapat dilakukan untuk menyembunyikan pesan rahasia. Steganography lebih cocok digunakan bersamaan dengan metode lain tersebut untuk menciptakan keamanan yang berlapis. Sebagai contoh steganography dapat digunakan bersama dengan enkripsi. Windows dan Unix juga menggunakan steganography dalam mengimplementasikan hidden directory.

2.3 Steganography pada Image

Seperti dikatakan sebelumnya, pada dasarnya video merupakan image-image dalam frame-frame yang “bergerak”. Jadi, sebelum membahas tentang video steganography akan dibahas lebih dulu tentang image steganography secara singkat.

Sekarang ini, image steganography sudah sangat populer. Sudah banyak metode yang digunakan untuk melakukannya. Untuk menyembunyikan pesan di dalam image tanpa mengubah tampilan image, data cover perlu dimodifikasi pada bagian area yang “noisy” dengan banyak variasi warna, sehingga modifikasi yang terjadi tidak akan terlihat. Berikut akan dibahas beberapa metode yang digunakan pada image steganography.

2.3.1 Least-Significant Bit Modification

Cara paling umum untuk menyembunyikan pesan adalah dengan memanfaatkan Least-Significant Bit (LSB). Walaupun banyak kekurangan pada metode ini, tetapi kemudahan implementasinya membuat metode ini tetap digunakan sampai sekarang.

Metode ini membutuhkan syarat, yaitu jika dilakukan kompresi pada stego, harus digunakan format lossless compression, karena metode ini menggunakan bit-bit pada setiap piksel pada image. Jika digunakan format lossy compression, pesan rahasia yang disembunyikan dapat hilang.

Jika digunakan image 24 bit color sebagai cover, sebuah bit dari masing-masing komponen Red, Green, dan Blue, dapat digunakan sehingga 3 bit dapat disimpan pada setiap piksel. Sebuah image 800 x 600 piksel dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia. Misalnya, di bawah ini terdapat 3 piksel dari image 24 bit color :

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

jika diinginkan untuk menyembunyikan karakter A (10000001b) dihasilkan :

(00100111 11101000 11001000)

(00100111 11001000 11101000)

(11001000 00100111 11101001)

dapat dilihat bahwa hanya 3 bit saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif.

Jika digunakan image 8 bit color sebagai cover, hanya 1 bit saja dari setiap piksel warna yang dapat dimodifikasi sehingga pemilihan image harus dilakukan

dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada citra. Akan lebih baik jika image berupa image grayscale karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia.

Proses ekstraksi pesan dapat dengan mudah dilakukan dengan mengekstrak LSB dari masing-masing piksel pada stego secara berurutan dan menuliskannya ke output file yang akan berisi pesan tersebut.

Kekurangan dari metode modifikasi LSB ini adalah bahwa metode ini membutuhkan "tempat penyimpanan" yang relatif besar. Kekurangan lain adalah bahwa stego yang dihasilkan tidak dapat dikompres dengan format lossy compression.

2.3.2 Masking dan Filtering

Teknik masking dan filtering ini biasanya dibatasi pada image 24 bit color atau image grayscale. Metode ini mirip dengan watermark, dimana suatu image diberi tanda (marking) untuk menyembunyikan pesan rahasia. Hal ini dapat dilakukan, misalnya dengan memodifikasi luminance beberapa bagian dari image. Walaupun metode ini akan mengubah tampilan dari image, dimungkinkan untuk melakukannya dengan cara tertentu sehingga mata manusia tidak melihat perbedaannya.

Karena metode ini menggunakan aspek image yang memang terlihat langsung, metode ini akan lebih "robust" terhadap kompresi (terutama lossy compression), cropping, dan beberapa image processing lain, bila dibandingkan dengan metode modifikasi LSB.

2.3.3 Transformation

Metode yang lebih kompleks untuk menyembunyikan pesan pada image ini

dilakukan dengan memanfaatkan Discrete Cosine Transformation (DCT) dan Wavelet Compression.

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

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

di mana $C(x) = 1/\sqrt{2}$ saat x sama dengan 0 dan $C(x) = 1$ saat x sama dengan 1. Setelah koefisien-koefisien diperoleh, dilakukan proses kuantisasi sebagai berikut :

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

dengan $Q(u,v)$ adalah 64-elemen dari tabel kuantisasi.

Sebagai contoh, berikut merupakan algoritma sederhana untuk menyembunyikan pesan di dalam image 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

Walaupun image yang dikompresi dengan lossy compression akan menimbulkan kecurigaan karena perubahan LSB akan terlihat jelas, pada metode ini hal ini tidak

akan terjadi karena metode ini terjadi di domain frekuensi di dalam image, bukan pada domain spasial, sehingga tidak akan ada perubahan yang terlihat pada cover image.

Wavelet Compression adalah salah satu cara kompresi data yang cocok digunakan untuk kompresi image, audio, dan video. Tujuannya adalah untuk menyimpan data dalam “ruang” yang sekecil mungkin dalam sebuah file, karenanya hilangnya informasi tertentu memang sudah diharapkan akan terjadi, kompresi ini merupakan contoh lossy compression. Sama seperti DCT, wavelet compression juga berbasis pada domain frekuensi. Keuntungannya, wavelet compression lebih baik dalam merepresentasikan daerah transien, contohnya image bintang pada langit malam. Artinya, elemen dari data yang transien akan direpresentasikan dalam jumlah informasi yang lebih kecil daripada yang terjadi pada transformasi lain, seperti pada DCT. Kerugiannya, wavelet compression kurang baik digunakan pada data yang bersifat periodik dan smooth.

Metode yang dilakukan pada wavelet compression akan dijelaskan sebagai berikut. Pertama-tama, dilakukan wavelet transform yang akan menghasilkan koefisien sesuai dengan jumlah piksel pada image 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 dengan

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

dimana $a = 2^{-j}$ disebut binary dilation atau dyadic dilation, dan $b = k2^{-j}$ disebut binary position atau dyadic position. Setelah koefien wavelet diperoleh, koefisien ini dapat dikompresi dengan mudah karena informasi terkonsentrasi secara statistik pada beberapa koefisien tertentu saja. Prinsip ini disebut dengan

transform coding. Setelah itu, koefisien-koefisien tadi dikuantisasi, baru kemudian di-encode dengan entropy encoding dan/atau run length encoding.

Berikut merupakan algoritma sederhana untuk menyembunyikan pesan di dalam image dengan menggunakan wavelet compression:

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

Proses ekstraksi pesan dengan menggunakan metode transformasi ini dilakukan dengan melakukan transformasi pada stego untuk memperoleh koefisien transformasi image. Pilih koefisien yang nilainya lebih kecil dari nilai treshold. Ekstrak bit data yang sesuai dengan koefisien ini dan tulis ke output file yang akan berisi pesan tersebut.

2.4 Steganography pada Video

Seperti dikatakan sebelumnya, video merupakan kumpulan dari image yang “bergerak”, jadi sebagian besar metode yang digunakan pada image steganography dapat digunakan pada video steganography. Dapat dikatakan bahwa video steganography merupakan turunan dari image steganography. Pada video steganography ini, yang umum digunakan adalah metode transformasi baik

menggunakan Discrete Cosine Transform maupun Wavelet Compression. Hal ini dikarenakan modifikasi LSB akan menghasilkan stego yang berukuran sangat besar sedangkan metode masking dan filtering akan mengubah tampilan visual dari video secara langsung.

Untuk menyembunyikan pesan pada cover video, prinsipnya sama seperti pada image steganography. Pertama-tama dilakukan transformasi pada masing-masing frame image cover video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai treshold tertentu. Koefisien tersebut akan diganti dengan bit-bit data pesan yang akan disembunyikan. Setelah seluruh pesan di-embed, koefisien tadi ditransformasi balik untuk menghasilkan stego video.

Untuk mengekstrak pesan dari stego video, prinsipnya juga sama seperti pada image steganography. Pertama-tama dilakukan transformasi pada masing-masing frame image stego video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai treshold tertentu. Koefisien tersebut akan merupakan bit-bit data pesan yang telah disembunyikan dan akan ditulis ke file output yang berisi pesan yang disembunyikan tersebut.

Keuntungan dari video steganography adalah banyaknya data yang dapat disembunyikan di dalamnya, serta fakta bahwa video merupakan “streams” dari image-image menyebabkan adanya distorsi pada salah satu frame image tidak akan dilihat dengan mudah dengan mata manusia. Akan tetapi, semakin banyak data pesan yang disembunyikan, bukan hal yang mustahil jika perubahan pada video menjadi semakin mudah terlihat.

BAB 3

VIDEO STEGANOGRAPHY TOOLS

3.1 Pendahuluan

Tools yang digunakan untuk melakukan video steganography sangat terbatas untuk sekarang ini. Satu-satunya tools yang saya temukan adalah MSU Stego Video yang dapat didownload di alamat berikut :

http://www.compression.ru/video/stego_video/src/msu_stegovideo_exe.zip

Software ini menggunakan metode transformasi menggunakan DCT dalam menyimpan data pesan dalam video. Saat program ini dibuat, beberapa codecs yang sedang populer dianalisis dan sebuah algoritma dipilih untuk menjamin kecilnya jumlah data yang hilang setelah kompresi.

Beberapa keunggulan dari software ini :

- distorsi yang relatif kecil pada stego video yang dihasilkan.
- pesan dapat diekstrak dari stego video untuk menguji apakah pesan yang tersimpan sesuai dengan apa yang diinginkan (tidak ada informasi yang hilang)
- informasi diproteksi dengan menggunakan passcode.
- unik (karena belum ada software lain yang serupa)
- freeware

Sayangnya, software ini memiliki beberapa batasan, yaitu cover video dan stego video harus dalam format .avi sedangkan pesan yang ingin disembunyikan harus berupa text file (.txt). Selain itu, software ini belum dapat menghasilkan video yang ada audio-nya.

3.2 Penggunaan MSU Stego Video

Setelah mendownload zip dari alamat yang disebutkan sebelumnya dan mengekstrak isi dari zip tersebut, software MSU Stego Video dapat langsung digunakan tanpa diinstall terlebih dulu dengan menjalankan MSU_stego_video.exe

Berikut ini merupakan langkah-langkah penggunaan software ini :

- Hiding Information

1. Pilih mode



Saat menjalankan software ini, kita harus memilih mode yang diinginkan, apakah hendak menyimpan informasi dalam video (embedding) atau mengekstrak informasi dari video (extracting). Disini kita memilih mode “embedding” dengan klik ”Hide file in video” dan kemudian klik next.

2. Pilih file



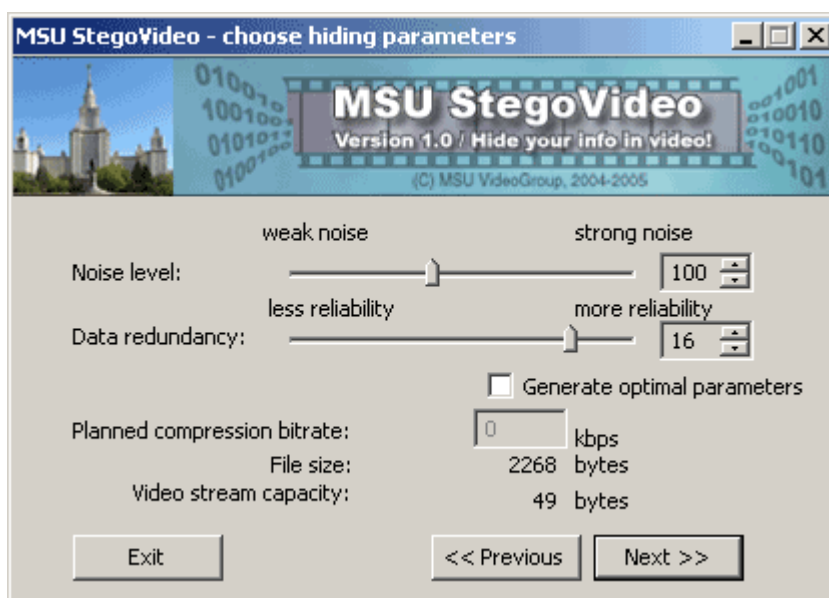
Di sini kita memilih file mana yang hendak disembunyikan (.txt, text file berukuran kecil direkomendasikan), file cover video tempat menyembunyikan file tadi, serta output stego video. (Kedua file video harus dalam format .avi)

3. Pilih mode kompresi



Di sini kita men-check box jika output video akan dikompres dan membiarkannya jika tidak. (catatan : informasi dapat hilang setelah kompresi, jangan menggunakan bitrate yang terlalu rendah, dianjurkan 800 kbps)

4. Pilih hiding parameter



Noise level – menentukan distorsi pada output stego video, kurangi jika distorsi terlalu tinggi, 100 direkomendasikan

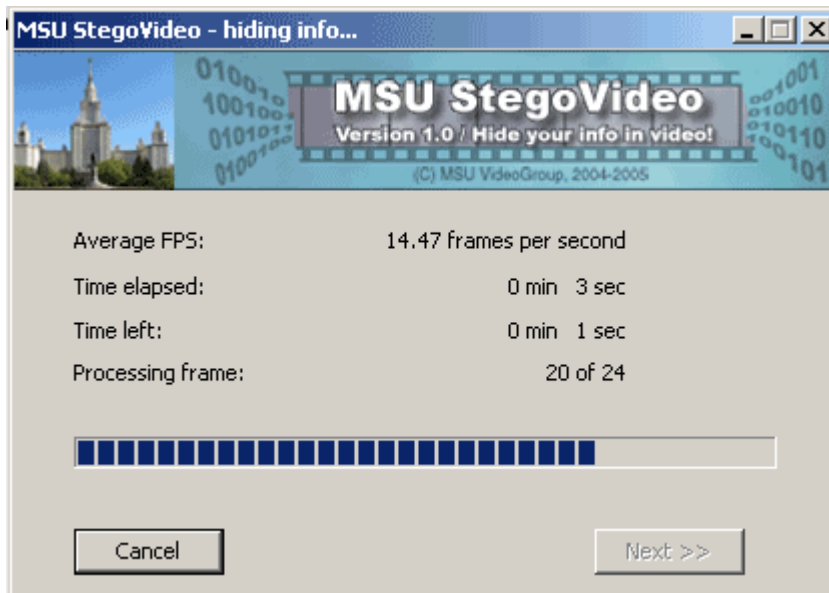
Data redundancy – meningkatkan data redundancy akan mengurangi jumlah data yang akan di-embed ke dalam setiap frame dan mengurangi kemungkinan terjadinya eror.

Kita juga dapat meng-generate optimal parameter secara otomatis, di sini kita diharuskan mengisi planned compression bitrate

5. Simpan Passcode



6. Proses Embedding Informasi



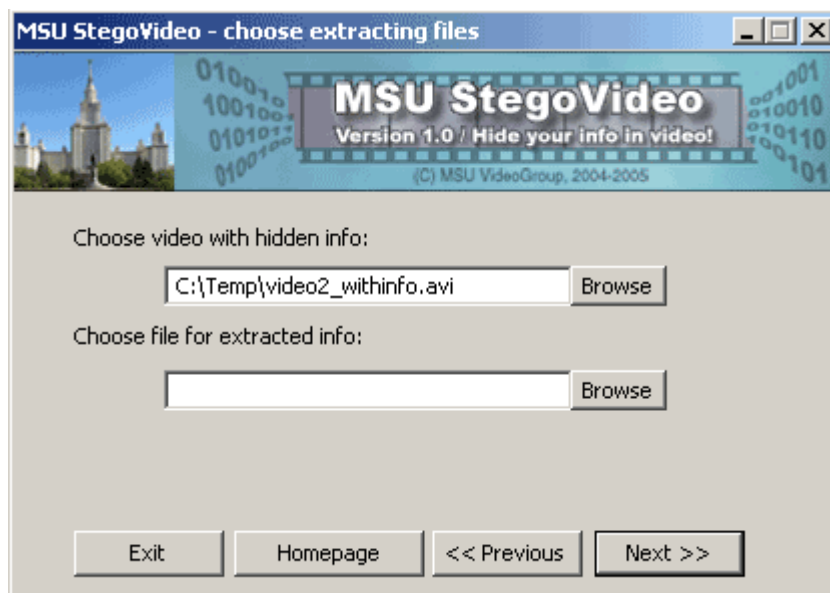
- Extracting Information

1. Pilih mode



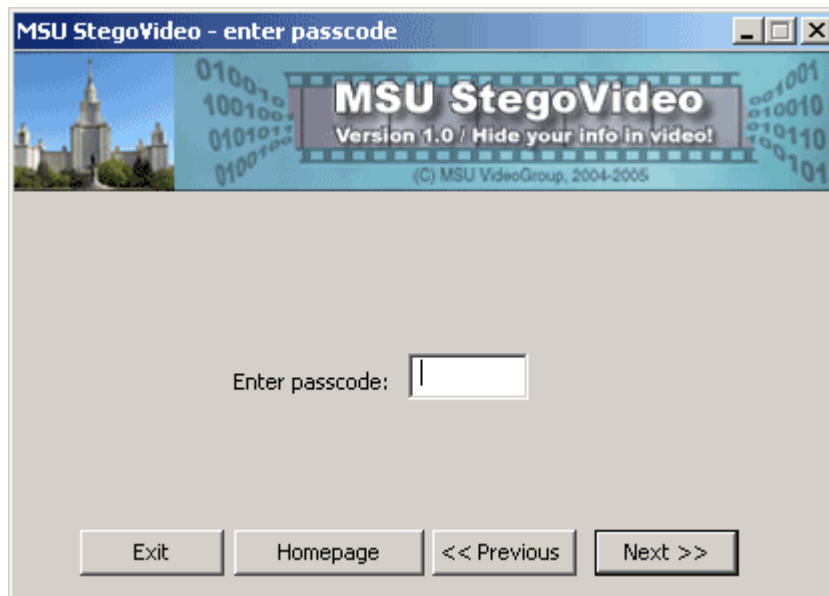
Saat menjalankan software ini, kita harus memilih mode yang diinginkan, apakah hendak menyimpan informasi dalam video (embedding) atau mengekstrak informasi dari video (extracting). Disini kita memilih mode "extracting" dengan klik "Extract file from video" dan kemudian klik next.

2. Pilih file

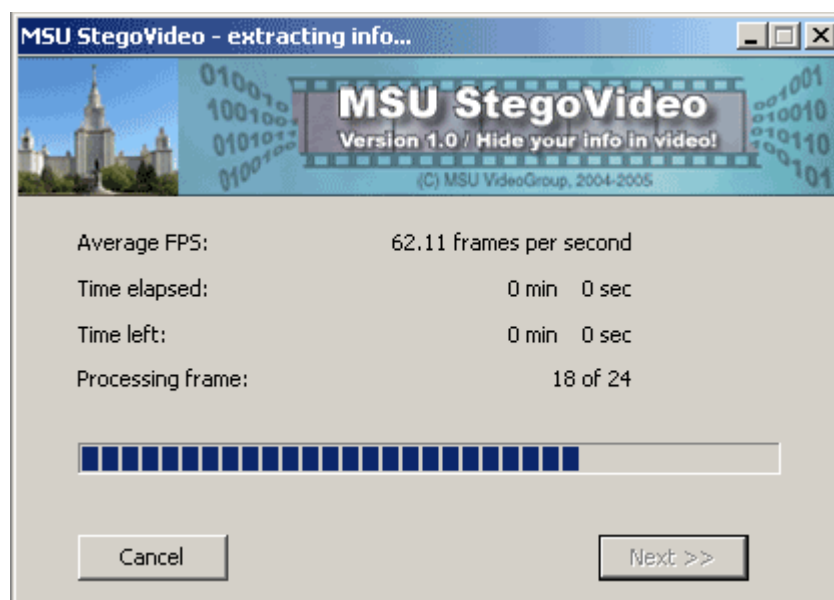


Di sini kita memilih file stego video yang akan diproses untuk mengekstrak data yang sudah di-embed ke dalamnya serta file output tempat hasil ekstrak akan disimpan. (Video berekstensi .avi, file output berekstensi .txt)

3. Masukkan Passcode



4. Proses Extracting Informasi



3.3 Performansi MSU Stego Video

Untuk melihat performansi dari software ini saya mencoba beberapa hal :
Isi file data yang akan di-embed adalah sebagai berikut:

This is a Test :

JuST WaNNa SaY

HaPPy BiRTHDaY

To YoU

WiSH YoU aLL tHE BeST

GoD BLeSS YoU aLWaYS

CU LaTeRz

TaKe CaRe :p

Noise level 100, Data redundancy 16 , compressed (1)

Cover Video



Stego Video



Ukuran file 14.659 MB

File hasil ekstraksi stego video :

This is a Test :

JuST WaNNa SaY

HaPPy BiRTHDaY

To YoU

WiSH YoU aLL tHE BeST

GoD BLeSS YoU aLWaYS

CU LaTeRz

TaKe CaRe :p

Noise level 60, Data redundancy 16 , compressed (2)

Cover Video



Stego Video



Ukuran file 14.265 MB

File hasil ekstraksi stego video :

This is a Test :

JuST WaNNa SaY

HaPPy BiRTHDaY

To YoU

WiSH YoU aLL tHE BeST

GoD BLeSS YoU aLWaYS

CU LaTeRz

TaKe CaRe :p

Noise level 100, Data redundancy 3 , compressed (3)

Cover Video

Stego Video



Ukuran file 14.291 MB

File hasil ekstraksi stego video :

@ 9 憎鱗^L 2 ???

JuST WaNNa SaY

HaPPy BiRTHDaY

To YoU

WiSH YoU aLL tHE BeST

GoD BLeSS YoU aLWaYS

CU LaTeRz

TaKe CaRe :p

Analisis

Baik pada (1), (2), maupun (3) dilakukan kompresi pada output stego video. Jika tidak dilakukan kompresi, file stego video dapat berukuran sampai 200 MB, dan hal ini tentu sangat tidak diinginkan.

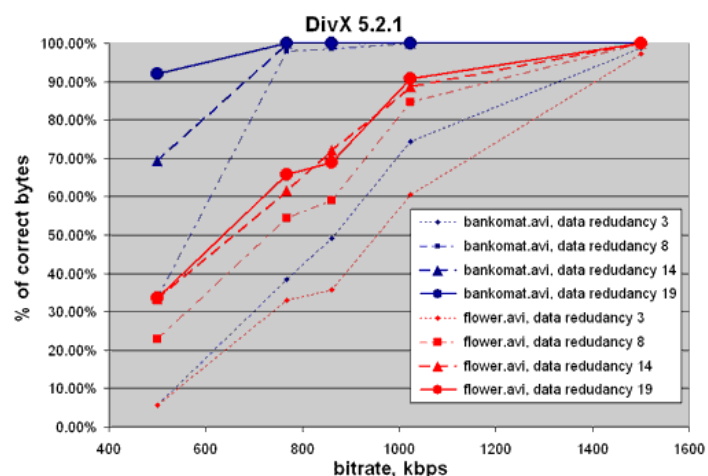
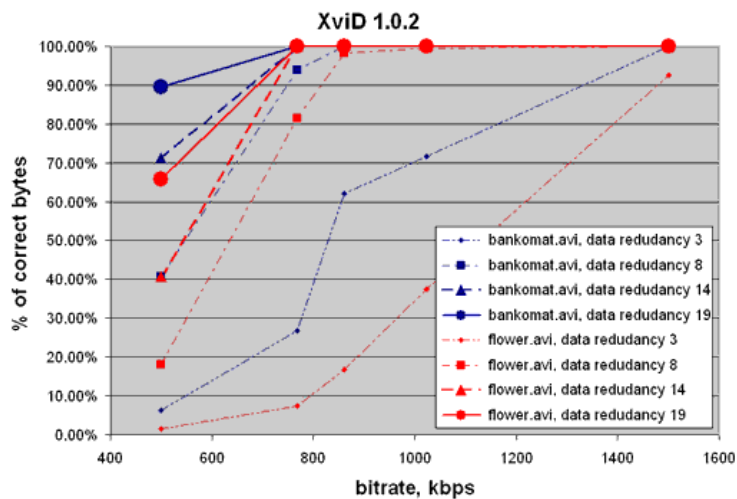
Perbedaan (1) dan (2) terletak pada besar Noise level-nya, jika dilihat pada output secara langsung tidak terlihat perbedaan yang mencolok pada output stego video. Tetapi bila dilihat secara lebih mendetail, hasil stego video pada (2) jauh lebih tajam daripada pada (1), seperti disebutkan sebelumnya, distorsi akan lebih kecil jika noise level lebih kecil.

Perbedaan (1) dan (3) terletak pada besar data redundancy-nya, jika dilihat pada output secara langsung juga tidak terlihat perbedaan yang mencolok pada output stego video, karena memang data redundancy lebih berpengaruh pada penyimpanan informasi yang di-embed. Terlihat bahwa pada (3) hasil

ekstraksi file dari stego video terdapat error. Hal ini sesuai dengan yang disebutkan sebelumnya bahwa data redundancy yang kecil akan menyebabkan kemungkinan terjadinya error lebih besar.

Selain ada tidaknya proses kompresi, ukuran frame dan codec juga menentukan ukuran output stego video. Selain itu, ukuran dari frame dan codec, bersama dengan nilai data redundancy akan menentukan kualitas dari penyimpanan informasi yang nantinya akan diekstrak dari stego video.

Selain itu bitrate yang digunakan juga mempengaruhi keberhasilan penyimpanan informasi. Berikut ini perbandingan persentase byte yang berhasil disimpan dengan bitrate yang digunakan saat menggunakan codec XviD 1.0.2 dan DivX 5.2.1.



Sebagai tambahan, saya juga mencoba untuk menyembunyikan file .mid, walaupun file berhasil disimpan dalam stego video, tetapi saat diekstrak, hasil filenya menjadi tidak berguna (tidak bisa dijalankan). Saya juga mencoba mengekstrak file dengan menggunakan passcode yang salah, tetapi bila passcode tidak benar maka proses ekstraksi file tidak akan dilakukan. Dari sini keamanan software ini dalam menjaga kerahasiaan informasinya sudah cukup baik.

BAB 4

PENUTUP

4.1 Kesimpulan

Steganography adalah cara yang menarik dan efektif dalam menyembunyikan pesan rahasia dan telah digunakan selama berabad-abad. Metode-metode untuk “memperlihatkan” pesan yang disembunyikan (disebut steganalysis) sudah cukup banyak, tetapi yang sulit adalah menyadari digunakannya steganography itu dan kunci yang diperlukan untuk ”membuka” pesan yang ada. Teknologi yang digunakan sederhana tetapi pelacakannya cukup sulit. Karenanya, steganography masih digunakan dalam menjaga keamanan suatu informasi dan diterapkan dalam banyak hal-hal sampai sekarang.

Video steganography merupakan turunan dari image steganography. Metode yang digunakan di sini adalah metode transformasi dengan menggunakan Discrete Cosine Transform dan Wavelet Compression. Software yang ada untuk melakukan video steganography untuk sekarang masih sangat minim dan masih belum bisa menggabungkannya dengan audio steganography.

4.2 Saran

Pengembangan metode dan software video steganography harus lebih ditingkatkan melihat banyak keuntungan dari video steganography, terutama untuk menggabungkan image steganography dan audio steganography untuk menghasilkan video steganography yang jauh lebih baik.

DAFTAR PUSTAKA

1. Hyperdictionary. *Discrete Cosine Transform*
—Available at <http://www.hyperdictionary.com/computing/discrete+cosine+transform>
2. Hyperdictionary. *Fast Fourier Transform*
—Available at <http://www.hyperdictionary.com/computing/fast+fourier+transform>
3. *Introduction to Steganography*.
—Available at <http://www.infosyssec.com/infosyssec/Steganography/>
4. Johnson, Neil F. 1995. *Steganography* . Center for Secure Information
—Systems, George Mason University
—Available at <http://www.jitc.com/stegdoc/steg1995.html>
5. Krenn, Robert . *Steganography and Steganalysis*
—Available at <http://www.krenn.nl/univ/cry/steg/article.pdf>
6. Mangarae, Aelphaeis. 2006. *Steganography FAQ* . zone-h.org
—Available at [http://www.infosecwriters.com/text_resources/pdf/](http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf)
—[Steganography_AMangarae.pdf](http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf)
7. MSU Stego Video software and manual
—Available at <http://www.compression.ru/video/>
8. Potdar, Vidyasagar, Elizabeth Chang . *Visible Invisible: Ciphertext as a*
—*Steganographic Carrier*. School of Information System, Curtin University

—of Technology

—Available at <http://www.fit.cbs.curtin.edu.au/~potdarv/pubications/INC2.pdf>

9. Westphal, Kristy. 2003 *Steganography Revealed*

—Available at <http://www.securityfocus.com>

10. Wikipedia – The Free Encyclopedia . *Discrete Cosine Transform*

—Available at http://en.wikipedia.org/wiki/Discrete_cosine_transform.htm

11. Wikipedia – The Free Encyclopedia . *Steganography*

—Available at <http://en.wikipedia.org/wiki/steganography.htm>

12. Wikipedia – The Free Encyclopedia . *Wavelet Compression*

—Available at http://en.wikipedia.org/wiki/Wavelet_compression.htm