ISSN: 1978-5569

KEAMANAN DATA DENGAN MENGIMPLEMENTASIKAN *STEGANOGRAPHY*

GATOT SUSILO, M.KOM

STMIK BINA PATRIA

ABSTRACT

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

Keyword: Steganography

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. *Steganography* dapat digunakan pada berbagai macam bentuk data, yaitu *image, audio,* dan *video*. 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.

Steganografi bukanlah pengganti kriptografi. Keduanya saling melengkapi satu sama lain. Untuk dapat mencapai maksud penggunaannya steganografi harus

memenuhi beberapa kriteria tertentu. Lebih jauh lagi, untuk dapat diaplikasikan sebagai *watermarking*, ada kriteria lain yang harus dipenuhi, selain kriteria steganografi.

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan di dalam pesan lain sehingga keberadaan pesan yang pertama tidak diketahui. Steganografi berasal dari bahasa Yunani steganos yang berarti tulisan tersembunyi. Steganografi sangat kontras dengan kriptografi. Kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, sedangkan steganografi menutupi keberadaan pesan. Steganografi dapat dipandang sebagai kelanjutan dari kriptografi. Dalam prakteknya, pesan dienkripsi terlebih dahulu, kemudian disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaan pesan. Steganografi membutuhkan dua properti, yaitu pesan dan media penampung. Media penampung yang umumnya digunakan sekarang dapat berupa teks, suara, gambar, atau video. Sedangkan pesan yang disembunyikan dapat berupa teks, gambar, atau pesan lainnya. Keuntungan penggunaan steganografi adalah memungkinkan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim. Ini membuat pihak ketiga tidak menyadari keberadaan pesan. Sebaliknya, penggunaan kriptografi akan menarik kecurigaan pihak ketiga bahwa ada sesuatu yang disembunyikan dalam pesan yang sedang dikirim. Steganografi juga memiliki kelemahan. Tidak seperti kriptografi, steganografi memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan. Akan tetapi, kelemahan ini sedikit demi sedikit dapat diatasi seiring dengan perkembangan teknik-teknik dalam melakukan steganografi.

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi, yaitu:

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.*

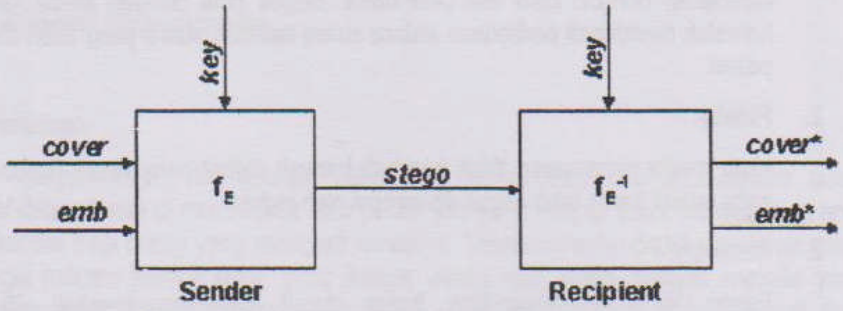
   Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.

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.

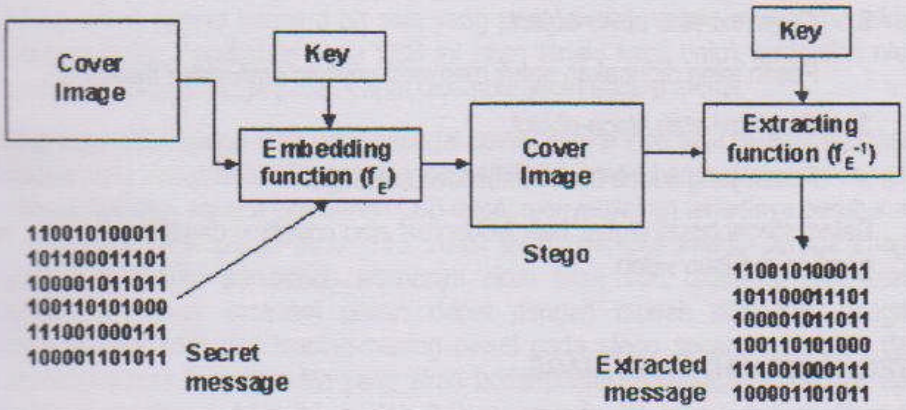
Catatan tertua mengenai penggunaan steganografi tercatat pada masa Yunani kuno. Pada saat itu, penguasa Yunani, Histiaues, sedang ditawan oleh Raja Darius di

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. Steganografi terus berkembang selama abad kelima belas dan keenam belas. Pada masa itu, banyak penulis buku yang enggan mencantumkan namanya karena takut akan kekuatan penguasa pada saat itu. Pengembangan lebih jauh lagi mengenai steganografi terjadi pada tahun 1883 dengan dipublikasikannya kriptografi militer oleh Auguste Kerckhoffs. Meskipun sebagian besar berbicara mengenai kriptografi, Kerckhoffs menjabarkan beberapa deskripsi yang patut dicatat ketika merancang sebuah sistem steganografi. Lebih jauh lagi, Les Filigranes, yang ditulis oleh Charle Briquet di tahun 1907,merupakan sebuah kamus sejarah dari *watermark*, salah satu wujud pengaplikasian steganografi. Dengan adanya komputer, steganografi memperoleh kemajuan yang sangat pesat. Penyembunyian pesan memasuki era baru berkat adanya komputer.



Steganographic System

Gambar di atas menunjukkan sebuah sistem *steganography* umum dimana di bagian pengirim pesan *(sender)*, dilakukkan proses *embedding* (fE) 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)*, dilakukkan 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 di bawah.



Graphical Version of a Steganographic System

MANFAAT STEGANOGRAFI

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, 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*.

Terdapat beberapa istilah yang berkaitan dengan steganografi, yaitu :

1. *Hiddentext* atau *embedded message*.

   Pesan atau informasi yang disembunyikan.

2. *Covertext* atau *cover-object*.

   Pesan yang digunakan untuk menyembunyikan *embedded message*.

3. *Stegotext* atau *stego-object*.

   Pesan yang sudah berisi embedded message.

Dalam steganografi digital, baik *hiddentext* atau *covertext* dapat berupa teks, audio, gambar, maupun *video*.

STEGANOGRAPHY PADA *IMAGE*

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*.

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 :

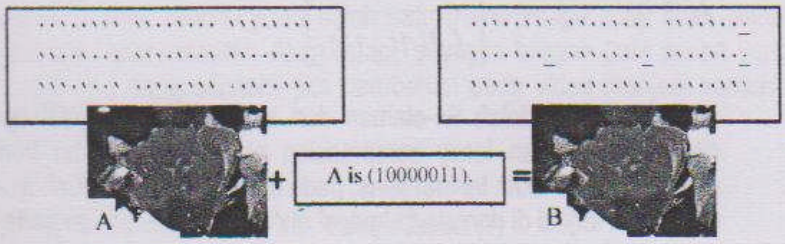
(00100111 11101000 11001000)

(00100110 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 dikompress dengan format *lossy compression.*



Contoh LSB

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.

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 metransformasikan 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/√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. 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*.

STEGANOGRAPHY PADA VIDEO

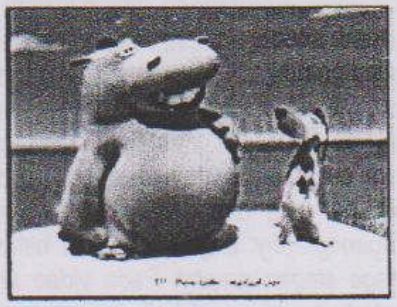
Video merupakan kumpulan dari *image* yang "bergerak", jadi sebagian besar metode yang digunakan pada *image steganography* dapat digunakan pada *video steganography*. Dapat dikatakan bahwa *video steganography* merupakan turunan dari *image steganography*. Pada *video steganography* ini, yang umum digunakan adalah metode transformasi baik menggunakan *Discrete Cosine Transform* maupun *Wavelet Compression*. Hal ini dikarenakan modifikasi LSB akan mengasilkan 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.

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

Cover Video

Stego Video



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

PENUTUP

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*.

DAFTAR PUSTAKA

- Johnson, N.F. & Jajodia, S., *"Steganalysis of Images Created Using Current Steganography Software"*, Proceedings of the 2nd Information Hiding Workshop, April 1998
- Kruus, Peter, Caroline Scace, Michael Heyman, dan Mathew Mundy. *A Survey of Steganographic Techniques for Image Files*. 2002. Advanced Security Research Journal – Network Associates Laboratories, Network Associates, Inc.
- Marvel, Lisa M., Charles G. Boncelet, dan Charles T. Retter. *Spread Spectrum Image Steganography*. 1999. IEEE Transaction on Image Processing.
- Morkel, T., JHP. Eloff, dan MS. Olivier. *An Overview of Image Steganography*. Pretoria: Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria.
- Stefan Hettzl, *"A Survey of Steganography"*, January 2002.
- Venkatraman, S., Abraham, A. & Paprzycki, M., *"Significance of Steganography on Data Security"*, Proceedings of the International Conference on Information Technology: Coding and Computing, 2004
- https://home.zhaw.ch/~rema/publications/als.pdf
- www.waset.org/pwaset/v24/v24-66.pdf
- www.martinolivier.com/open/stegoverview.pdf
- www.ksu.edu.sa/sites/Colleges/ComputerSciences/Documents/NITS/ID162.pdf