Nim : 1410651174
Nama : Muhammad Ghafur Hidayatullah
Tugas : Steganografi

Teknik Menyembuyikan Pesan Dengan Steganografi

A. Pengertian Steganografi

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 steganografi yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas.

Steganografi biasanya sering disalahartikan dengan kriptografi karenanya keduanya sama-sama bertujuan untuk melindungi informasi yang berharga. Perbedaan yang mendasar antara keduanya yaitu steganografi berhubungan dengan informasi tersembunyi sehingga tampak seperti tidak ada informasi tersembunyi sama sekali. Jika seseorang mengamati obyek yang menyimpan informasi tersembunyi tersebut, maka dia tidak akan menyangka bahwa terdapat pesan rahasia dalam obyek tersebut, dan karenanya dia tidak akan berusaha memecahkan informasi dari obyek tersebut.

Kata *steganografi* berasal dari bahasa Yunani, yaitu dari kata *Stegos* (*covered*/tersembunyi) dan *Graptos* (*writing*/tulisan). Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio, atau video. Teknik *Steganografi* ini telah banyak digunakan dalam strategi peperangan dan pengiriman sandi rahasia sejak jaman dahulu kala. Dalam perang Dunia II, teknik steganografi umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman, (Morkel, dkk, 2005).

Semakin pentingnya nilai dari sebuah informasi, maka semakin berkembang pula metode-metode yang dapat digunakan untuk melakukan penyisipan informasi yang didukung pula dengan semakin berkembangnya media elektronik. Berbagai macam media elektronik kini telah dapat digunakan untuk melakukan berbagai fungsi *steganografi* dengan berbagai macam tujuan dan fungsi yang diharapkan oleh penggunanya. Sebagai fungsi yang umum, *steganografi* digunakan untuk memberikan cap khusus dalam sebuah karya yang dibuat dalam format media elektronik sebagai identifikasi, (Johnson, dkk, 1998).

Dua teknik lain yang sangat erat kaitannya dengan steganografi adalah *watermarking* dan *fingerprinting*. Kedua teknik ini berfokus pada perlindungan hak cipta dengan menyisipkan informasi hak cipta pada media lain dan memberikan ijin kepada pihak ketiga untuk mengetahui keberadaan informasi yang disisipkan tersebut. Hal ini berbeda dengan steganografi yang menjaga informasi yang disisipkan pada media lain agar tidak terlihat oleh pihak ketiga. Jika ada pihak ketiga yang ingin meng*hack* isi informasi tersembunyi tersebut, maka tujuan mereka adalah berbeda. Jika pada *watermarking* dan *fingerprinting*, maka mereka berusaha menghilangkan informasi yang disisipkan, sedangkan jika pada steganografi, maka mereka berusaha sebatas mendeteksi keberadaan informasi tersembunyi, (Morkel , 2005).

B. Sejarah Steganografi

Seperti kriptografi, penggunaan *steganografi* sebetulnya telah digunakan berabad-abad yang lalu bahkan sebelum istilah *steganografi* itu sendiri muncul. Berikut adalah contoh penggunaan *steganografi* di masa lalu, (Munir, 2005):

- Steganografi sudah dikenal oleh bangsa Yunani. Herodatus, penguasa Yunani, mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Dalam hal ini, rambut budak dibotaki, lalu pesan rahasia ditulis pada kulit kepala budak. Ketika rambut budak tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya.
- Bangsa Romawi mengenal steganografi dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

3. Metode lain yang digunakan oleh masyarakat Yunani kuno adalah dengan menggunakan lilin sebagai media penyembunyi pesan mereka. Pesan dituliskan pada suatu lembaran, dan lembaran tersebut akan ditutup dengan lilin untuk menyembunyikan pesan yang telah tertulis. Pihak penerima kemudian akan menghilangkan lilin dari lembaran tersebut untuk melihat pesan yang disampaikan oleh pihak pengirim.

C. Kegunaan Steganografi

Seperti perangkat keamanan lainnya, *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 tag-notes untuk citra online. Terakhir, *steganografi* juga dapat digunakan untuk melakukan penyimpanan atas kerahasiaan informasi yang berharga, untuk menjaga data tersebut dari kemungkinan sabotasi, pencuri, atau dari pihak yang tidak berwenang.

Sayangnya, *steganografi* juga dapat digunakan untuk alasan yang ilegal. Sebagai contoh, jika seseorang telah mencuri data, mereka dapat menyembunyikan arsip curian tersebut ke dalam arsip lain dan mengirimkannya keluar tanpa menimbulkan kecurigaan siapapun karena tampak seperti email atau arsip normal. Selain itu, seseorang dengan hobi menyimpan pornografi, atau lebih parah lagi, menyimpannya dalam hard disk, mereka dapat menyembunyikan hobi buruk mereka tersebut melalui *steganografi*. Begitu pula dengan masalah terorisme, *steganografi* dapat digunakan oleh para teroris untuk menyamarkan komunikasi mereka dari pihak luar.

D. Media Steganografi

Hampir semua file digital dapat digunakan untuk steganografi, tetapi format yang paling cocok adalah yang mempunyai nilai bits redundancy tinggi. Bit Redudancy adalah bit yang dapat dirubah tanpa merubah banyak karakteristik file secara keseluruhan. File gambar dan suara adalah yang memenuhi syarat ini, sehingga banyak periset steganografi yang telah menggunakan media tersebut.

1). Citra (Image)

File Citra pada komputer merupakan *array* bilangan yang merepresentasikan nilai intensitas cahaya yang bervariasi (*pixel*). Kumpulan *pixel-pixel* inilah yang membentuk suatu citra. Citra yang sering digunakan umum adalah citra 24 bit dan citra 8 bit (256 *colors*), (Johnson, 1998).

Table 1.1 Jenis Citra dilihat dari ukuran bitnya.

Jumlah Bit	**Keterangan**
1	binary-valued image (0 – 1)
8	gray level (0 – 255)
16	high color (216)
24	224 true color
32	true color (232)

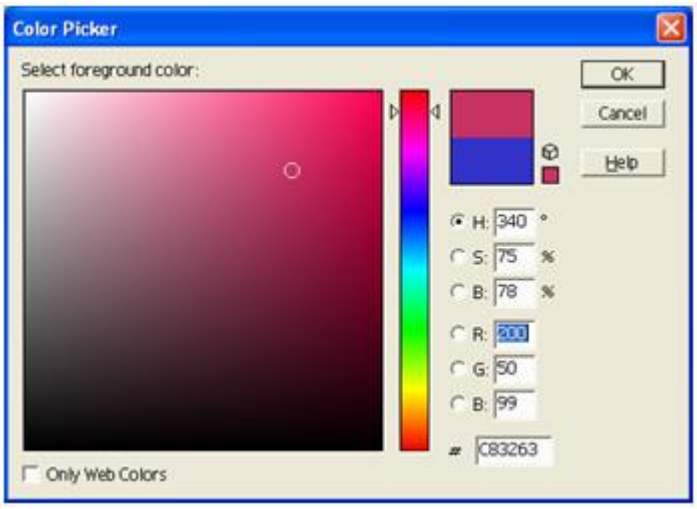
Format gambar digital memiliki 2 parameter:

- spatial resolution : pixels x pixels
- color encoding : bits / pixel

Misal: terdapat gambar berukuran 100 pixels x 100 pixels dengan color encoding 24 bits dengan R=8 bits, G=8 bits, B=8 bits per pixel, maka color encoding akan mampu mewakili 0 .. 16.777.215 (mewakili 16 juta warna), dan ruang disk yang dibutuhkan = 100 * 100 * 3 byte (karena RGB) = 30.000 bytes = 30 KB atau 100 * 100 * 24 bits = 240000 bits.

Pada steganografi, citra yang biasa digunakan adalah citra 24 bit, karena citra tersebut dapat menyediakan space yang besar untuk disisipi oleh data. *Pixel* penyusun citra ini tersusun atas 3 warna primer yaitu merah, hijau, dan biru (RGB). Masing-masing warna primer tersusun atas 1 *byte* data. Untuk citra 24 bit berarti menggunakan *3 bytes per pixel* untuk merepresentasikan nilai warna *pixel*. *3 bytes* data ini dapat berupa hexadesimal, desimal, atau biner.

Gambar 1 adalah contoh color pallete yang sering digunakan dalam pengolahan warna.



Gambar 1 Color Pallete

2). Media Gambar Terkompresi dan pengaruhnya pada steganografi

Ketika bekerja dengan gambar bit depth tinggi, maka file size gambarnya akan menjadi terlalu besar untuk berada di standar halaman internet. Agar dapat menampilkan gambar dengan ukuran yang wajar, gambar tersebut harus diberi teknik-teknik tertentu. Teknik ini menggunakan rumus matematika untuk menganalisa data gambar dan menghasilkan gambar dengan ukuran file lebih kecil. Proses ini disebut dengan kompresi, (Morkel, dkk, 2005).

Dua jenis kompresi gambar adalah *lossless* dan *lossy*. Keduanya memperkecil ukuran file tetapi menghasilkan sesuatu yang berbeda. Hal ini tentunya dapat mengganggu karena gambar tersebut mengandung informasi yang hendak kita kirimkan. Lain halnya bila informasi itu tidak dikompresi.

Kompresi *lossy* menghasilkan gambar dengan ukuran file lebih kecil dengan cara menghilangkan beberapa data gambar dari aslinya. Kompresi ini menghilangkan detail-detail yang terlalu kecil bagi penglihatan mata, sehingga menghasilkan aproksimasi yang dekat dengan gambar aslinya walaupun bukan duplikat yang sama persis. Contoh format file yang menggunakan teknik kompresi ini adalah JPEG (*Joint Photographic Experts Group*), (Morkel, dkk, 2005).

Lain halnya dengan kompresi *lossless* yang dapat dikembalikan ke pesan aslinya. Kompresi ini tidak pernah memindahkan informasi apapun dari gambar aslinya dan sebagai gantinya menggunakan rumus matematika tertentu untuk menyimpan datanya. Integritas gambar aslinya tetap dipertahankan dan gambar yang telah dikompresi, bitnya tetap sama bit demi bit dengan gambar aslinya. Format gambar yang paling sering digunakan untuk jenis kompresi ini adalah GIF (Graphic Interchange Format) dan BMP 8-bit.

Kompresi memerankan peran yang sangat penting dalam memilih Algoritma yang tepat untuk steganografi. Kompresi *lossy* menghasilkan gambar dengan ukuran file lebih kecil, tetapi juga meningkatkan kemungkinan bahwa informasi yang tersimpan di dalamnya hilang karena data gambar yang tak terlihat akan dibuang. Kompresi *lossless* berusaha

untuk mempertahankan gambarnya tanpa ada kemungkinan untuk hilang bagian gambarnya tetapi ukuran filenya tidak berubah banyak.

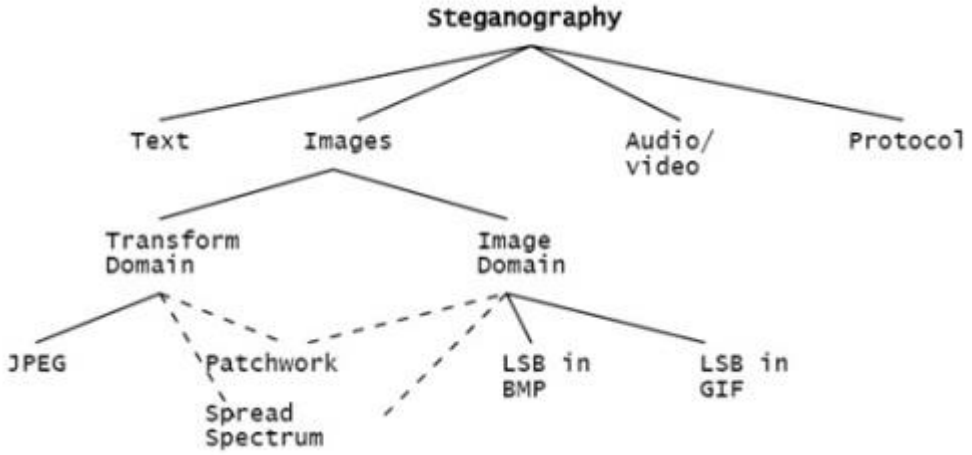
E. Teknik Steganografi Pada Gambar

Teknik steganografi gambar dapat dibagi menjadi dua bagian: *spatial domain* dan *transform / frekuensi domain*. Pada *spatial domain* informasi dimasukkan kedalam tiap pixel satu persatu. Sementara itu, pada *transform domain*, gambar ditransformasikan terlebih dulu kemudian informasi baru dimasukkan ke gambar.

Teknik steganografi pada *spatial domain* menggunakan metoda *bit-wise* yang menggunakan penyisipan bit dan noise manipulation. Format gambar yang paling cocok untuk cara ini adalah tipe *lossless*. Namun, cara ini sangat bergantung kepada format gambarnya, (Morkel, dkk, 2005).

Steganografi pada *transform domain* melibatkan manipulasi algoritma dan transformasi gambar. Metoda ini menyembunyikan informasi pada area yang lebih signifikan pada cover image dan membuat hasilnya jadi lebih baik. Cara ini juga tidak tergantung pada format gambar. Informasi yang disisipkan juga dapat bertahan walaupun menggunakan kompresi *lossy* maupun *lossless*.

Gambar 2 adalah skema image steganografi dan penggolongan berdasarkan domainnya.



Gambar 2 Skema penggolongan Steganografi berdasarkan domainnya

F. Kriteria Steganografi yang Bagus

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah, (Munir, 2005) :

1. *Fidelity*. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

2. *Robustness*. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, rotasi,

perbesaran gambar, pemotongan (*cropping*), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.

3. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

G. Teknik Steganografi Least Significant Bit Insertion (LSB)

Least Significant Bit Insertion merupakan salah satu metode steganografi yang yang paling sederhana, cepat dan mempunyai kapasitas penyisipan yang cukup besar (*ditunjukkan dalam table 2.1*). LSB insertion menggunakan cara menyisipkannya pada bit rendah atau bit paling kanan (LSB) pada data pixel yang menyusun file tersebut. Untuk file bitmap 24 bit, setiap pixel (titik) pada gambar 1 terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian pada setiap pixel file bitmap 24 bit dapat disisipkan 3 bit data, (Prihanto, 2009).

Contoh penyisipan huruf A pada bitmap 24 bit pixel dengan data raster biner gambar asli ditunjukkan oleh Gambar 3 :

00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101001

Gambar 3 Data raster biner gambar asli

Sedangkan representasi biner ASCII huruf A adalah :

100000111

Gambar 4 Representasi biner ASCII huruf A

Dengan menyisipkannya pada data pixel diatas maka akan dihasilkan :

00100111 **11101000** 11001000

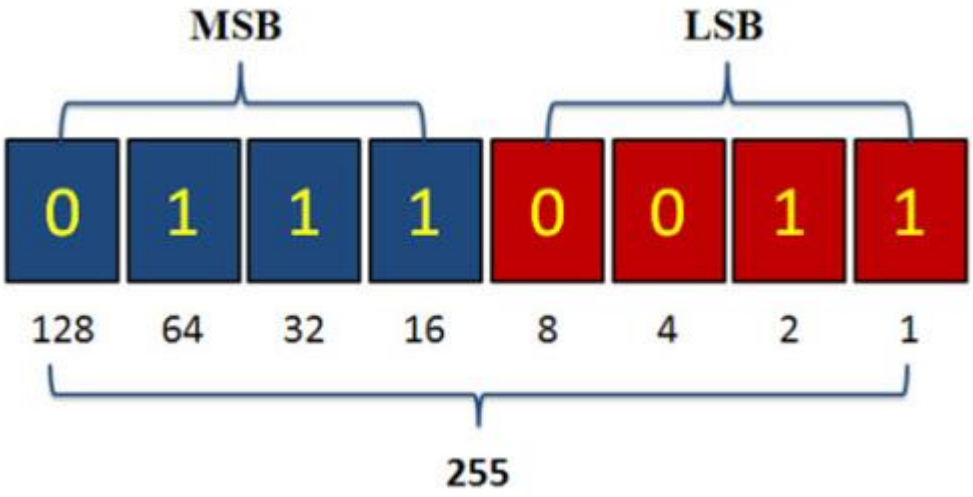
00100110 11001000 **11101000**

11001001 00100111 11101001

Gambar 5 Data raster biner gambar asli setelah disisipi data biner ASCII huruf A

Terlihat hanya empat bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metoda ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua dan seterusnya, namun sebaiknya tidak melebihi 4 bit LSB (Habes, 2006), karena semakin banyak bit LSB yang

digunakan maka gambar akan semakin banyak mengalamai perubahan layaknya terkena noise.



Gambar 6 Representasi Biner 4-LSB

Gambar di atas merupakan representasi biner 1 byte (8 bit), bagian yang berwarna biru merupakan MSB (*Most Significant Bit*) sedangkan yang merah merupakan LSB (*Least Significant Bit*). Kita dapat menyisipkan pada bagian yang berwarna merah. Jika kita rekontruksi ulang contoh sebelumnya dengan menggunakan penyisipan multi LSB 4 bit, maka untuk penyisipan huruf A sekarang hanya membutuhkan 2 bytes binary warna. Untuk lebih jelasnya ditunjukkan contoh raster 2 byte gambar aslinya seperti pada Gambar 7.

00100111 11101001

Gambar 7 Data raster biner 2 byte gambar asli

Sedangkan representasi biner ASCII huruf A adalah :

100000111

Gambar 8 Representasi biner ASCII huruf A

Dengan menyisipkannya pada data pixel diatas maka akan dihasilkan :

0010**1000** 1110**0111**

Gambar 9 Data raster 2 byte gambar asli setelah disisipi data biner ASCII huruf A

Download contoh program

Download materi

Praktikum

A. Menyisipkan file kedalam gambar

1. buka program stegano

1. Pilih icon open=>image source

2. pilih icon embed file (pilih file doc anda)

3. simpan image yang yang sudah berisi file

4. Tutup program

B. mengekstrak file yang tersembunyi

1. buka program stegano

1. Pilih icon open=>image stegp

2. pilih icon deembed file

3. file telah kembali, selesai

Alamat

https://cogierb201.wordpress.com/2012/05/08/teknik-menyembuyikan-pesan-dengan-steganografi/