STEGANOGRAFI DENGAN MENGUNAKAN TEKNIK DYNAMIC CELL SPREDING

Yosef Sukianto – NIM : 13506035

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
Email : if16035@students.if.itb.ac.id

Abstrak

Perkembangan komputer dan perangkat pendukung lainnya yang serba digital, telah membuat data-data digital semakin banyak digunakan. Disisi lain kemudahan tersebut telah memunculkan masalah di sekitar hak cipta dan hak kepemilikan materi digital. Teknik hidden message (steganografi), adalah suatu teknik yang mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain. Dengan kemampuan tersebut maka informasi hak cipta seperti identitas seorang pengarang, tanggal ciptaan, dan lain-lain dapat disisipkan/disembunyikan kedalam berbagai macam variasi jenis dokumen besar seperti: gambar, audio , video, text atau file biner.

Penelitian ini membahas steganografi dengan menggunakan Teknik Dynamic Cell Spreading yang merupakan teknik menyembunyikan /menyisipkan data dengan bantuan buffer memori sebagai media penggabungan. Teknik Dynamic Cell Spreading (DCS) merupakan steganografi dengan menggunakan model proteksi terhadap deteksi yang dikembangkan oleh Holger Ohmacht dengan konsep dasar yaitu menyembunyikan file pesan (semua data elektronik) kedalam media gambar (JPEG). Penyembunyian pesan dilakukan dengan cara menyisipkanya pada bit rendah LSB (Least Significant Bit) dari data pixel yang menyusun file tersebut menggunakan buffer memori sebagai media penyimpan sementara.

Kata kunci: *Dynamic cell Spreading, Least Significant Bit, steganography, cryptography, embedding, extracting.*

1. Pendahuluan

Adanya Internet sebagai sistem jaringan terluas yang menghubungkan hampir seluruh komputer di dunia, membuat semua komputer dapat dengan mudah untuk saling bertukar data. Dalam “dunia maya” ini, hampir segala jenis informasi dapat diperoleh, yang dibutuhkan hanyalah sebuah komputer yang terhubung dengan dunia maya ini (Internet).

Perkembangan komputer dan perangkat pendukung lainnya yang serba digital, telah membuat data-data digital semakin banyak digunakan. Terdapat sejumlah faktor yang membuat data digital (seperti audio, citra, video, dan teks) semakin banyak digunakan, antara lain:

a. Mudah diduplikasi dan hasilnya sama dengan aslinya,
b. Murah untuk penduplikasian dan penyimpanan,
c. Mudah disimpan untuk kemudian diolah atau diproses lebih lanjut,
d. Serta Mudah didistribusikan, baik dengan media disk maupun melalui jaringan seperti Internet.

Adanya berbagai kemudahan tersebut di sisi lain telah memunculkan masalah di sekitar hak cipta dan hak kepemilikan materi digital. Setiap materi digital yang menjadi bagian dari distribusi elektronik bersifat rentan terhadap pengkopian gelap dan pendistribusian gelap. Karena masalah itulah kemudian muncul sejumlah pemikiran tentang bagaimana cara melindungi hasil pekerjaan dalam bentuk materi digital serta cara-cara untuk mencegah aktivitas gelap serta teknik untuk melacak distribusi suatu dokumen elektronik.

Salah satu solusi adalah lewat teknik *hidden message (steganografi)*, yaitu suatu teknik yang mengijinkan para pengguna untuk menyembunyikan suatu pesan didalam pesan yang lain. Dengan steganografi adalah mungkin untuk menyembunyikan informasi hak cipta seperti identitas seorang pengarang , tanggal ciptaan , dan lain-lain, dengan cara menyisipkan / menyembunyikan informasi tersebut kedalam berbagai macam variasi jenis dokumen besar seperti: gambar, audio , video, text atau file biner.

Untuk itu penelitian ini akan di fokuskan pada konsep dasar yaitu untuk menyembunyikan data/dokumen elektronik khususnya dalam data

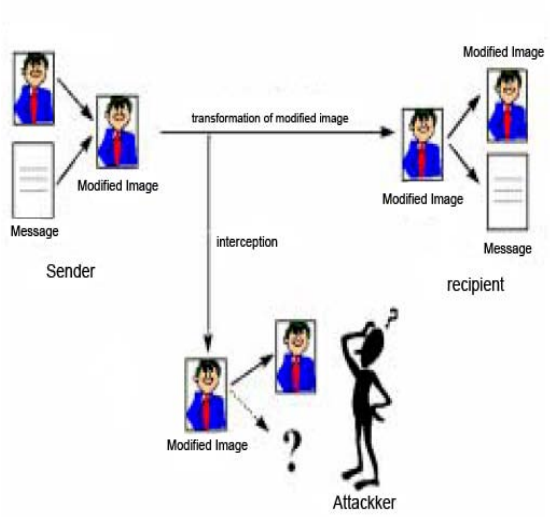
gambar. Teknik utama yang akan digunakan adalah steganografi dengan menggunakan Teknik Dynamic Cell Spreading (DCS).

2. Landasan Teori

2.1 Konsep Steganograf

Steganografi adalah ilmu pengetahuan dan seni dalam menyembunyikan komunikasi. Suatu sistem *steganografi* sedemikian rupa menyembunyikan isi suatu data di dalam suatu sampul media yang tidak dapat di duga oleh orang biasa sehingga tidak membangunkan suatu kecurigaan kepada orang yang melihatnya, Gambar 1 adalah ilustrasi dasar dari konsep steganografi.

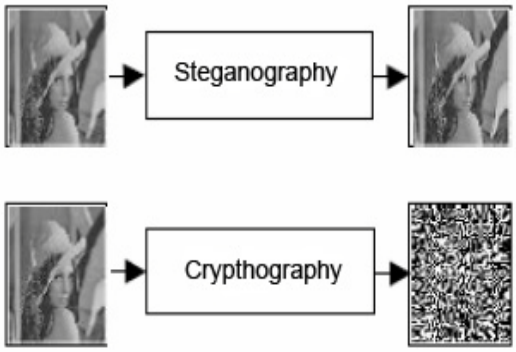
Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi *steganografi*. Sekarang, teknologi jaringan dan komputer menyediakan cara *easy-to-use* jaringan komunikasi untuk *steganografi.* Proses penyembunyian informasi di dalam suatu sistem *steganografi* dimulai dengan mengidentifikasi suatu sampul media yang mempunyai bit berlebihan (yang dapat dimodifikasi tanpa menghancurkan integritas media). Proses menyembunyikan (*embedding*) menciptakan suatu proses stego medium dengan cara menggantikan bit yang berlebihan ini dengan data dari pesan yang tersembunyi.



Gambar 1 ilustrasi steganography

2.2 Perbedaan Steganografi dengan Kriptografi

Steganography berbeda dengan cryptography, letak perbedaannya adalah pada hasil keluarannya. Hasil dari *cryptography* biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah - olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi), sedangkan hasil keluaran dari *steganography* memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses. Gambar 2 menunjukkan ilustrasi perbedaan antara steganografi dan kriptografi.



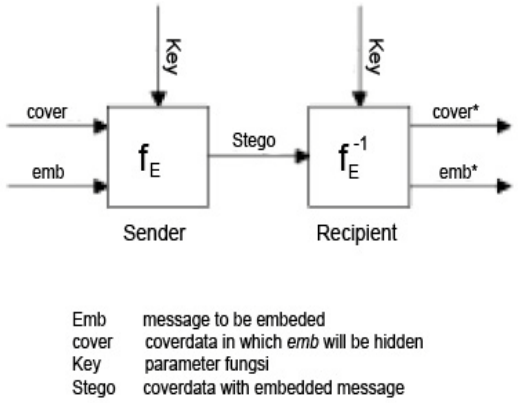
Gambar 2 Perbedaan steganography dengan Cryptography

2.3 Dasar Penyembunyian (Embedding)

Tiga aspek berbeda di dalam sistem penyembunyian informasi bertentangan dengan satu sama lain yaitu: kapasitas, keamanan, dan ketahanan (*robustness*). Kapasitas adalah mengacu pada jumlah informasi yang dapat tersembunyi di dalam sampul media, keamanan adalah pencegahan bagi orang biasa yang tidak mampu untuk mendeteksi informasi tersembunyi, dan ketahanan adalah untuk modifikasi media stego sehingga dapat bertahan terhadap suatu *attack* yang dapat menghancurkan informasi tersembunyi.

Penyembunyian informasi biasanya berhubungan dengan *watermarking* dan *steganografi*. Tujuan utama sistem *watermarking* adalah untuk mencapai tingkat ketahanan yang lebih tinggi, sangatlah mustahil untuk menghilangkan suatu proses *watermarking* tanpa menurunkan tingkat kualitas objek data. steganografi, pada sisi lain, mengejar kapasitas dan keamanan tinggi, yang dimana sering diketahui bahwa informasi yang tersembunyi mudah diketahui. Bahkan modifikasi kecil kepada media stego dapat menghancurkannya.

Model dasar untuk *embedding* adalah sebagaimana pada Gambar 3.



Gambar 3 Model Dasar Embedding

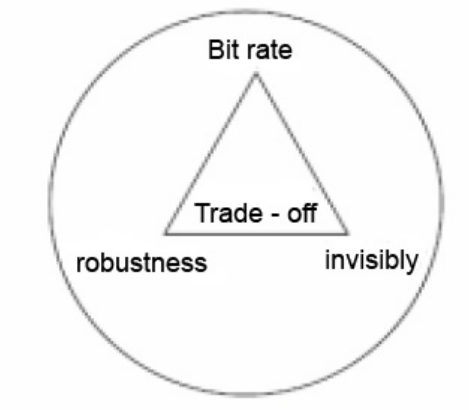
steganografi terbagi menjadi 2 buah model yaitu:

a. Proteksi terhadap deteksi untuk teknik penyembuyian data
   Proteksi model ini banyak digunakan di dalam dunia *steganografi* untuk piranti keamanan dalam suatu pengiriman dokumen melalui media internet atau yang lainnya. Proteksi ini mempunyai metode agar suatu file yang telah disisipi oleh data tidak dapat dideteksi oleh suatu program steganalisis sehingga hanya orang yang mempunyai program *steganografi* tertentu saja yang dapat menampilkan / ekstrakting data yang ada.
b. Proteksi terhadap kehilangan untuk teknik pemberian tanda tehadap data
   Proteksi model ini banyak digunakan di dalam media secure digital atau *steganografi* yang berfungsi sebagai penanda hak cipta (*copyright*) agar tidak dapat dimusnahkan maupun digandakan olah pihak yang tidak bertanggung jawab. Salah satu metode yang dapat digunakan adalah *watermarking*.

Watermarking merupakan suatu bentuk dari *steganografi* (ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain), dalam mempelajari teknik-teknik bagaimana penyimpanan suatu data (digital) kedalam data host digital yang lain (istilah host digunakan untuk data /sinyal digital yang ditumpangi). Parameter-parameter yang perlu diperhatikan dalam penerapan metoda *watermarking* adalah:

a. Jumlah data (*bitrate*) yang akan disembunyikan.
b. Ketahanan (*robustness*) terhadap proses pengolahan sinyal.
c. Tak terlihat (*invisibly*) atau output tidak berbeda dengan input awal.

Kesatuan dari ketiga parameter tersebut dikenal sebagai *trade-off* dalam watermarking. Gambar 4 menunjukkan ilustrasi trade-off dalam watermarking.



Gambar 4 Trade-off dalam watermarking

2.4 Konsep Teknik Dynamic Cell Spreading

Teknik Dynamic Cell Spreading (DCS) merupakan steganografi dengan menggunakan model proteksi terhadap deteksi yang dikembangkan oleh Holger Ohmacht dengan konsep dasar yaitu menyembunyikan file pesan (semua data elektronik) kedalam media gambar (JPEG). Penyembunyian pesan dilakukan dengan cara menyisipkanya pada bit rendah LSB (Least Significant Bit) dari data pixel yang menyusun file tersebut menggunakan buffer memori sebagai media penyimpan sementara.

Dalam proses penggabungan (stego) antara file gambar dengan teks, untuk file bitmap 24 bit maka setiap pixel (titik) pada gambar tersebut akan 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 kita dapat menyisipkan 3 bit data. Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Sedangkan representasi biner huruf A adalah 10000011. Dengan menyisipkannya pada data pixel diatas maka akan dihasilkan:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001001 00100111 11101001)

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 bahkan ketiga.

Proses penggabungan file gambar dengan data elektronik hampir sama tetapi lebih kompleks karena membutuhkan media memori sebagai perantara untuk menghitung jumlah keseluruhan bit yang terdapat didalam file gambar maupun didalam data elektronik yang akan diembedding sehingga memudahkan proses embedding itu sendiri.

Penghitungan aritmatika dalam melakukan embedding maupun extracting ini menggunakan perintah *assembler* karena menyangkut bit-bit yang terdapat didalam memori.

Proses *embedding* dalam *Teknik* DCS mempunyai beberapa tahapan proses yaitu:

a. Membuat *registry address* untuk mempersiapkan tempat penyimpan memori sementara guna proses dalam penghitunggan LSB (*Least Significant Bit)* pada gambar maupun data yang akan digabungkan (*embed*).
b. Konversi JPEG ke dalam bitmap dalam arti format gambar JPEG yang merupakan format kompresi gambar dirubah atau di unkompres agar mempermudah dalam penghitunggan dan penempatan data.
c. Mengkalkulasikan jarak antar bit yang ada pada file gambar agar mempermudah penghitunggan dan penyisipan bit data yang akan dimasukkan.
d. Mengalokasikan memori untuk menampung bit gambar pada saat proses *steganografi* akan dijalankan.
e. Mengkopi bitmap ke dalam buffer memori.
f. Mendapatkan ukuran input byte file yaitu sama dengan proses pada gambar yang dimana untuk mengetahui besar dari data yang akan digabungkan ke dalam gambar.
g. Mengkopi buffer memori ke bentuk bitmap mengubah kembali dari memori menjadi file gambar.

Proses *ekstrakting* dalam *Teknik* DCS mempunyai beberapa tahapan proses yaitu:

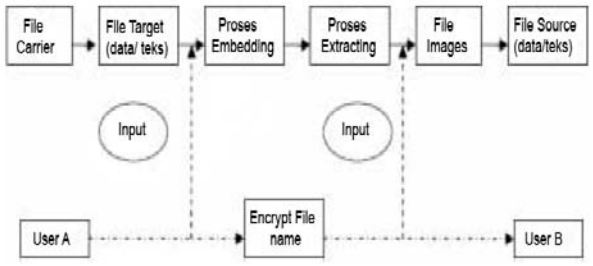
a. Membuat registry address untuk mempersiapkan tempat penyimpan memori sementara guna proses dalam penghitunggan LSB (*Least Significant Bit)* pada gambar maupun data yang akan dipisahkan (*extract*).
b. Mengkalkulasikan variabel yang ada pada media pembawa pesan dalam hal ini adalah file gambar yang berformat bmp.
c. Mengalokasikan ukuran memori yang akan digunakan dalam proses.
d. Mengcopy bitmap ke dalam buffer memori.
e. Ekstrak ukuran file pembawa bertujuan untuk menghitung dan mengembalikan kembali ukuran file pembawa ke dalam ukuran yang semula sebelum disisipkan file lain.
f. Mengkalkulasikan variabel yang ada menghitung kembali setelah proses ekstrak dilewati.
g. Ekstrak file bertujuan untuk mengambil data dalam file gambar yang telah dihitung dan disiapkan dalam memori sebelumnya sehingga proses dapat berjalan dengan cepat.

3. Perancangan dan Implementasi

3.1 Design dan Rancangan Aplikasi

Aplikasi steganografi yang akan dibangun dirancang untuk bisa diakses oleh komputer yang memiliki mikroprosesor 32 bit ke atas dan memiliki cache memory dengan sistem operasi berbasis windows yaitu Microsoft Windows XP. Untuk mendukung hal itu dipilihlah bahasa pemrograman berorientasi object.

Blok diagram dari program implementasi secara umum dengan menggunakan Teknik DCS diperlihatkan pada Gambar 5. Pertama-tama yang dilakukan adalah membuat registry address untuk mempersiapkan tempat penyimpan memori sementara di dalam sistem operasi yang kemudian menginisialisasi data asli. Data ini akan digabungkan dengan file gambar menggunakan Teknik DCS kemudian hasilnya akan di tampilkan, dari data yang telah diembedding akan dikembalikan ke data asli dengan proses ekstraksi.

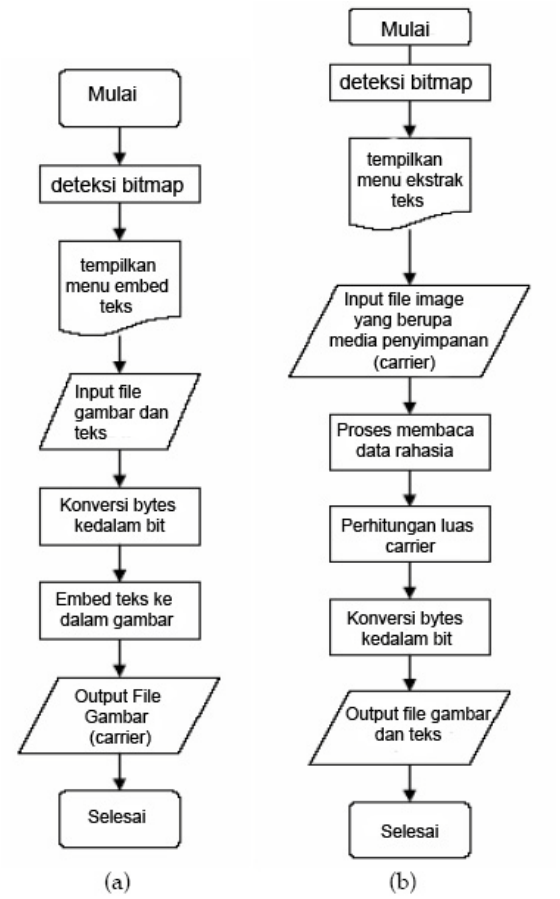


Gambar 5 Rancangan Program

Aplikasi untuk Teknik DCS ini akan dibuat menjadi beberapa fungsi, antara lain:
a. Embed file
b. Embed teks
c. Ekstrak file
d. Ekstrak teks
e. Proses Tahapan

Gambar 6 menunjukkan algoritma untuk proses embedding.

Teknik DCS mempunyai prosedur utama dalam proses embedding maupun ekstrakting yaitu dalam procedure *Copy bitmap to buffer* dan procedure *Copy buffer to bitmap*. Procedure *Copy bitmap to buffer* digunakan hanya sekali dalam setiap proses sedangkan prosedure *Copy buffer to bitmap* digunakan pada saat embedding file. Proces embedding dan ekstrakting pada dasarnya adalah sama hanya pada proses ekstrakting ada beberapa prosedur yang tidak dipanggil.



Gambar 6(a) embedding text (b) extracting teks

Procedure *Copy bitmap to buffer* bertujuan untuk merubah dari bentuk bitmap yang kemudian diterjemahkan ke dalam bahasa assembler untuk mendapatkan data keseluruhan bit dari gambar yang telah ditransfer pada buffer memori. Prosedur ini digunakan dalam proses embedding maupun extracting.

```
procedure Copy_Bitmap_n_Buffer(Bitmap:
TBitmap);
var
  Goal: pointer;
  Height_M, Width_M, Column, Line: longint;
  Source: ByteArray;
begin
  Goal:= pGoal;
  Height_M:= Height-1;
  Width_M:= Width_Byte-1;
  for Line:= 0 to Height_M do
  begin
     Source:= Bitmap.ScanLine[Line];
     for Column:= 0 to Width_M do
     asm
        push eax
        push ebx
        push ecx
        mov eax, [Source]
        mov ebx, [Goal]
        mov cl, [eax]
        mov [ebx], cl
        inc [Goal]
        inc [Source ]
        pop ecx
        pop ebx
        pop eax
     end;
  end;
end;
```

Procedure *Copy buffer to bitmap* bertujuan untuk merubah bentuk dari nilai bit yang telah diproses assembler pada buffer memori ke dalam bentuk file bitmap. Prosedur ini hanya digunakan satu kali saja pada saat proses embedding dilakukan.

```
Procedure Copy_Buffer_n_Bitmap(oitmap:
TBitmap);
var
  Goal: pointer;
  Column, Line: longint;
  Source: ByteArray;
begin
  Goal:= pGoal;
  for Line:= 0 to Height-1 do
  begin
     Source:= Bitmap.ScanLine[Line];
     for Column:= 0 to Width_Byte-1 do
     asm
       push eax
       push ebx
       push ecx
       mov eax, [Goal]
       mov ebx, [Source]
       mov cl, [eax]
       mov [ebx], cl
       inc [Goal]
       inc [Source]
       pop ecx
       pop ebx
       pop eax
     end;
  end;
end;
```

3.2 Implementasi Hasil

Karena implementasi program *stganografi* dengan Teknik DCS ini bersifat study/pembelajaran , maka berapa hal yang dijadikan sebagai batasan dalam implementasi adalah :

a. Untuk embedding file format gambar yang digunakan adalah JPEG atau berekstensi *.jpg, dalam hal ini format

gambar yang berekstensi lain belum dapat digunakan.

b. Untuk hasil dari embedding dapat dipastikan menjadi format gambar Bitmap atau berekstensi *.bmp, tidak dapat menggunakan format gambar yang berekstensi lain.

Steganografi merupakan teknik menyebunyikan suatu data atau teks di dalam file yang lain sehingga untuk hasil akhir dari proses *steganografi* tidaklah berbeda jauh dengan file aslinya, karena bila terjadi perbedaan akan dapat menimbulkan kecurigaan terhadap user lain yang tidak berhak menerima file yang dimodifikasi tersebut.

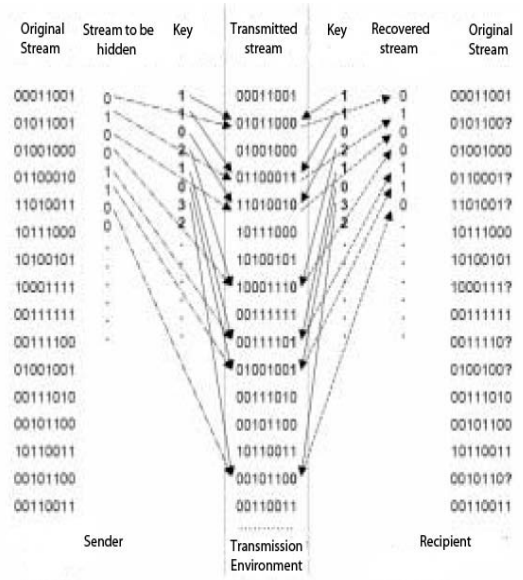
Dalam Teknik DCS hasil dari proses *steganografi* tidak berbeda jauh dengan file aslinya, perbedaan utama adalah pada format file yaitu sebelum proses berekstensi *.jpg dan setelah proses penyisipan menjadi beresktensi *.bmp.

Setelah dilakukan proses embedding dengan data (berupa dokumen) maka akan dihasilkan file kasar (*noise*). Kemudian dilakukan proses akhir penyamaran data dan menghasilkan file gambar berupa format Bitmap.

4. Analisis Hasil

Proses penyembunyian atau *steganografi* mempunyai berbagai macam bentuk metode juga implementasi program. Aplikasi Teknik DCS yang dibangun menggunakan gabungan antara bahasa visual dengan bahasa pemrograman assembler. Penggabungan tersebut dilakukan untuk prosedur dan fungsi dari perintah pengaksesan memori, manajemen memori, kalkulasi variabel, kalkulasi jarak antar bit, conversi bitmap ke dalam buffer memori maupun perintah sebaliknya conversi buffer memori ke dalam bitmap menjadi satu perintah tunggal yang diakses dari prosedur utama.

Teknik DCS merupakan suatu teknik s*teganografi* yang menerapkan metode embedding data dengan menggunakan LSB (*Least Significant Bit*). Penggunaan metode embedding data dengan menggunakan LSB dilakukan dengan mempersiapkan suatu arus bit, kemudian menetapkan LSB dari cover sesuai dengan nilai dari file kedua atau data yang akan dibawa. Jarak antara dua bit tersembunyi yang berurutan menjadi banyaknya contoh dari metode ini dan dikendalikan dengan suatu nilai acak.



Gambar 7 Skema LSB

Pada Gambar 7 dijelaskan tentang mekanisme dasar penggunaan LSB. Pengirim memodifikasi arus bit yang asli menggunakan kunci rahasia. Dengan panah yang berlanjut dapat diuraikan posisi di mana bit yang tersembunyi nantinya yang akan disisipi (*embed*). Arus bit yang baru diperoleh dari arus bit yang asli, tetapi dimodifikasi menurut nilai-nilai yang menyangkut arus bit untuk tersembunyi (lihat panah disela yang diberi titik). Sebagai contoh, jika jarak adalah 2, kita biarkan dua bytes tanpa perubahan dan menyisipkan bit rahasia seperti LSB dari byte ketiga. Jika jarak adalah 0, maka kita memodifikasi byte yang pertama dengan mengubah LSB dan seterusnya. Penerima menggembalikan bit yang tersembunyi menggunakan kunci yang bersama, yang memberikan posisi dari embedding bit (lihat panah berlanjut), dan mengekstraknya (lihat yang disela-sela panah).

Nilai-Nilai dari jarak antara bit tersembunyi yang berurutan haruslah antar dua nilai-nilai ekstrim. Nilai yang minimal pada umumnya 0, tetapi nilai yang maksimal harus dengan tepat memilihnya. Jika panjang bit dari file gambar cukup panjang, maka tidak ada masalah. Tetapi jika panjangnya tidak memenuhi syarat yang ada, atau mempunyai suatu arus bit file gambar yang pendek, maka pengirim harus mengambil beberapa ukuran untuk meyakinkan bahwa semua bit yang tersembunyi akan masuk ke dalam arus bit pada file gambar. Ketika menggunakan arus bit, sama seperti sedang berbicara ditelepon, pengirim tidak mengetahui ketika kapan percakapan akan diakhiri. Oleh karena itu, harus berhati-hati waspada dan membuat rata-rata jarak yang sangat pendek agar pada saat semua bit rahasia selesai disisipkan tidak sampai tertulis sebelum diakhir file. Dalam beberapa hal, ini

bukanlah suatu tugas gampang, sebab jika jarak antara bit yang tersembunyi yang tidak seragam didistribusikan, maka karakter statistik dari noise tidaklah menghilang (pada umumnya noise yang teracak mempunyai distribusi interval bersifat exponen panjangnya).

Program *steganografi* dengan menggunakan teknik lain belum tentu dapat mengekstrak hasil dari embedding Teknik DCS. Hal ini disebabkan Teknik DCS memiliki keamanan yang variatif, juga untuk menyisipkan data baik berupa file maupun teks, cara penyisipannya menggunakan nilai penghitungan panjang ukuran nama file serta besar kecilnya ukuran file yang akan dimasukkan ke dalam media penyimpan (*carrier*) serta menghitung jarak antar bit yang ada pada media penyimpan (*carrier*) itu sendiri.

Teknik DCS mempunyai kelebihan pada tingkat keamanannya dengan belum adanya *steganalisis* yang mampu untuk memecahkan keamanan Teknik DCS. Keamanan tersebut didapat karena dalam melakukan sistem penggabungan atau penyisipan data berupa file, data dipecah dan kemudian dimasukkan ke dalam bentuk binary RGB melalui proses pengukuran memory eksternal dalam sebuah komputer sehingga digunakan perintah assembler untuk menyisipkannya.

Kekurangan di Teknik DCS sebenarnya kelemahan umum yang ada pada model embedding. Kelemahan ini timbul karena bentuk ouput file tidak dapat menyerupai aslinya sehingga saat dilakukan pengiriman melalui internet maupun pertukaran data dibutuhkan waktu yang banyak karena besarnya hasil output ukuran file embedding.

5. Kesimpulan

Dengan solusi steganografi, maka pada prinsipnya masalah yang terkait dengan hak cipta dan kepemilikan dapat dipecahkan, hal ini mengacu pada sifat dasar steganografi yaitu menyembunyikan pesan. Namun demikian steganografi bukan solusi tunggal untuk menyelesaikan masalah tersebut, watermarking dan cryptografi dapat pula dijadikan sebagai solusi bersama untuk mengatasi masalah hak cipta dan kepemilikan.

Teknik DCS merupakan proses *embedding* dengan menggunakan metode LSB. Implementasi program dilakukan dengan menggunakan bahasa pemrograman tingkat rendah yaitu assembler.Teknik DCS mempunyai cara menejemen alokasi memori yang cukup baik dalam melakukan proses *embedding* maupun *ekstrakting*, sehingga tidak memboroskan pemakaian memori yang ada.

Dalam program *steganografi* ini terjadi perubahan besar dalam hal ukuran file, yaitu sebelum proses embedding dengan setelah proses embedding. Pada masa mendatang perlu kiranya dilakukan penelitian lanjutan dengan menggabungkan Teknik DCS dengan algoritma kompresi file sehingga ukuran file hasil proses staganografi akan lebih kecil atau minimal sama dengan file aslinya

5. Daftar Pustaka

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

[2] Anonim (1998). *Modul Praktikum Assembler*. Laboratorium Jaringan Komputer, Jurusan Teknik Informatika, Universitas Islam Indonesia.

[3] Ohmacht, H. (2001). *Stegano Project*. Diakses pada 27 Maret 2009 dari http://www.holger-ohmacht.de.

[4] Provos, N., Honeyman, P. (2003). Hide and Seek: An Introduction to Steganography. *IEEE Computer Society.*

[5] Suhono, Supangkat, H., Juanda, K. Watermarking Sebagai Teknik Penyembunyian Hak Cipta Pada Data Digital. *Jurnal Departemen Teknik Elektro,* Institut Teknologi Bandung.

[6] Zöllner, J. et al. Modeling the Security of Steganographic System. *Journal of Dresden University of Technology*.