Studi dan Perbandingan Steganografi Metode EOF(End of File) dengan DCS(Dynamic Cell Spreading)

Adiputra Sejati

13507105
Teknik Informatika Institut Teknologi Bandung
e-mail: if17105@students.if.itb.ac.id; adiputra.sejati@yahoo.com

ABSTRAK

Seiring dengan perkembangan teknologi komunikasi dan informasi yang berkembang, penggunaan perangkat komputer menjadi sangat sering digunakan. Hal ini menyebabkan data-data digital semakin banyak digunakan. Para ahli jaman dahulu telah mengembangkan ilmu untuk mengamankan pengiriman pesan melalui data digital, contoh yang kita kenal adalah kriptografi dan steganografi. Steganografi adalah sebuah teknik yang digunakan dalam penyembunyian pesan dalam sebuah pesan. Steganografi merupakan sebuah ilmu yang sudah ada sejak jaman dahulu yang digunakan untuk menghindari ancaman-ancaman dari penyadapan, interupsi, modifikasi maupun fabrikasi. Dengan teknik ini diharapkan dapat menyembunyikan pesan maupun data digital(image,audio,video, dan lain-lain) yang penting dari kriptanalis attack. Makalah ini akan membahas tentang steganografi dengan metode EOF (*End of File*) dan DCS (*Dynamic Cell Spreading*) dalam menyembunyikan pesan rahasia. Tehnik *End of File* merupakan teknik steanografi dengan menyisipkan data akhir file. Sedangkan teknik *Dynamic Cell Spreading* adalah suatu teknik dengan metode menyembunyikan /menyisipkan data dengan bantuan buffer memori sebagai madia penggabungan. Dengan studi ini diharapkan kita dapat lebih mengerti bagaimana cara menyembunyikan pesan dengan menggunakan steganografi.

Kata kunci: *Kriptografi, Steganografi, Kriptanalis attack, End of File, Dynamic Cell Spreading*

1. PENDAHULUAN

Teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Sebagai contoh perkembangan jaringan internet yang memungkinkan orang untuk saling bertukar data melalui jaringan internet tersebut. Seiring dengan perkembangan tersebut, kejahatan teknologi komunikasi dan informasi juga turut berkembang, seperti yang sering kita dengar adalah *hacker*, *cracker* dan sebagainya. Ancaman-ancaman tersebut bisa berupa interupsi, penyadapan, modifikasi maupun fabrikasi. Dengan berkembangnya ilmu pengetahuan, masalah masalah tersebut dapat ditangani dengan menggunakan ilmu-ilmu yang sudah ada sejak jaman dahulu, seperti kriptografi dan steganografi. Steganografi adalah sebuah tehnik yang digunakan dalam penyembunyian pesan didalam sebuah pesan. Perkembangan steganografi ini menjadi salah alternatif pengamanan dalam komunikasi data di jaringan internet. Berbeda dengan teknik kriptografi, kalau kriptografi, kecurigaan terhadap pesan yang disamarkan mudah dikenali karena pesan disamarkan dengan cara mengubah pesan yang asli menjadi seolah-olah tidak terbaca. Sedangkan steganografi lebih mengurangi kecurigaan karena pesan yang disamarkan disembunyikan dalam file. Satu hal yang juga cukup menghebohkan dunia pada tanggal 11 september 2001 adalah peristiwa penyerangan gedung WTC. Diberitakan bahwa para ”teroris” menyembunyikan peta-peta dan foto-foto target dan juga pesan yang berupa perintah untuk aktivitas teroris di ruang *chat sport, bulletin boards* dan *website* lainnya.

Oleh karena itu penulis akan membahas dua buah metode yang dapat digunakan di dalam steganografi yaitu EOF(*End of File*) dan DCS(*Dynamic Cell Spreading*). Dengan studi tentang steganografi ini diharapkan bisa mengerti perbedaan penggunaan kedua teknik diatas(EOF dan DCS) dalam steganografi.

2. LANDASAN TEORI

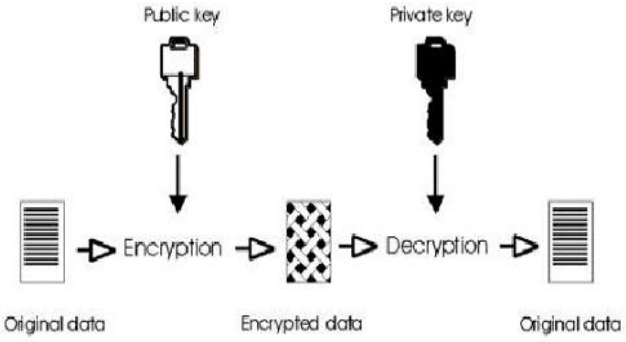
2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, yang terdiri dari dua kata yaitu kripto dan graphia. Kripto berarti rahasia(*secret*) sedangkan graphia berarti tulisan(*writing*). Sehingga kriptografi bisa diartikan sebagai “tulisan yang dirahasiakan”. Dalam kamus *hacker* (Ariyus, 2005), kriptografi diartikan sebagai ilmu yang mempelajari penulisan secara rahasia. Secara umum kriptografi adalah

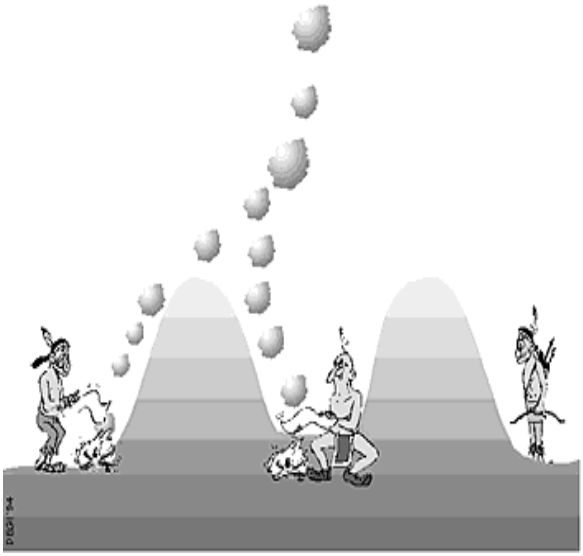
ilmu dan seni untuk menjaga kerahasiaan pesan. Selain itu, kriptografi juga bisa diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentifikasi data. Tidak semua aspek keamanan informasi dapat ditangani olej kriptografi.

Dalam sebuah algoritma kriptografi, terdapat tiga unsur yaitu :

- Enkripsi, yaitu proses mengubah plaintext menjadi *ciphertext*
- Dekripsi, yaitu mengubah ciphertext menjadi *plaintext*
- Kunci, merupakan *key* yang digunakan untuk proses enkripsi maupun proses dekripsi.



Gambar 1. Skema alrian proses pada metode Kriptografi



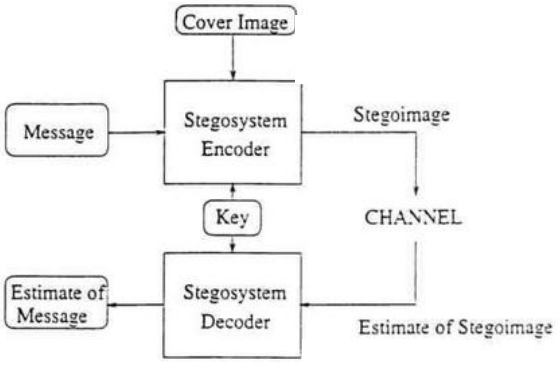
Gambar 2. Ilustrasi serangan dari yang ada pada Kriptografi

2.2 Steganografi

Secara umum steganografi tujuannya hampir sama dengan kriptografi, yaitu untuk menjaga kerahasiaan pesan. Tetapi steganografi menyembunyikan pesan dalam suatu sampul berupa media digital lainnya yang tidak akan tampak atau diduga oleh orang biasa, hal ini tidak menimbulkan kecurigaan kepada orang yang melihatnya. Jadi steganografi secara khusu adalah suaut ilmu, teknik dan seni bagaimana menyembunyikan data rahasia didalam sebuah media digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang lain.

Steganografi membutuhkan dua properti, yaitu media penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra (gambar), suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video, Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi *ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya. Proses *embedding* atau sering kita sebut penyembunyian pesan ini dilakukan dengan cara menciptakan suatu proses stego medium dengan cara menggantikan atau menyisipkan bit-bit dari sampul media dengan bit-bit dari pesan yang disembunyikan.

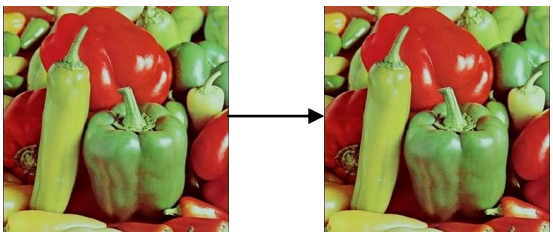
Pada jaman dahulu teknik steganografi ini menggunakan tinta yang tak terlihat untuk menyampaikan pesan. Tetapi pada jaman sekarang, karena data yang ada kebanyakan merupakan data digital, teknologi jaringan dan komputer sudah menyediakan cara yang mudah digunakan untuk menyembunyikan pesan dengan teknik ini.



Gambar 3. Aliran proses yang ada pada Steganografi

2.3 Perbedaan Steganografi dan Kriptografi

Pada dasarnya steganografi dan kriptografi memiliki tujuan yang sama yaitu menyembunyikan pesan. Tetapi kedua metode ini memiliki perbedaan, perbedaannya terletak pada hasil keluaran enkripsi dari kedua metode tersebut. Hasil enkripsi dari kriptografi biasanya berupa data yang jauh berbeda dari bentuk aslinya dan biasanya data yang dihasilkan sangat berantakan sehingga tidak dapat dibaca dan diketahui apa isi informasi dari data tersebut. Tetapi dengan adanya data yang tidak beraturan tersebut atau biasa kita sebut *ciphertext* itu, kriptanalis akan tahu bahwa ada pesan tersimpan dalam data-data tersebut. Berbeda dengan kriptografi, teknik steganografi menghasilkan keluaran yang memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut biasanya terletak pada indera manusia, biasanya terletak pada indera penglihatan dan pendengaran. Tetapi apabila menggunakan komputer atau perangkat digital lainnya, dapat dilihat dan dibedakan dengan jelas antara kondisi sebelum enkripsi atau biasa kita sebut *plaintext* dan kondisi setelah enkripsi yang biasa kita sebut *ciphertext*.

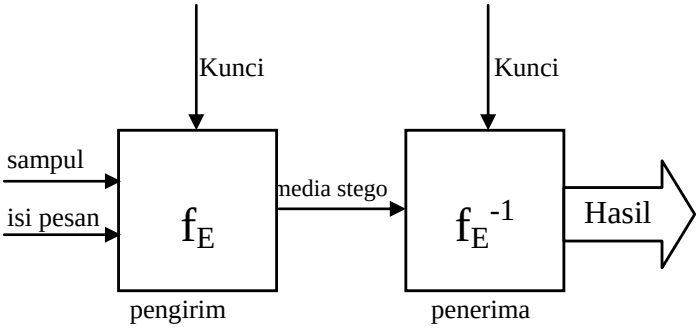


Gambar 4. Contoh Steganografi pada gambar

Gambar 5. Contoh Kriptografi pada gambar

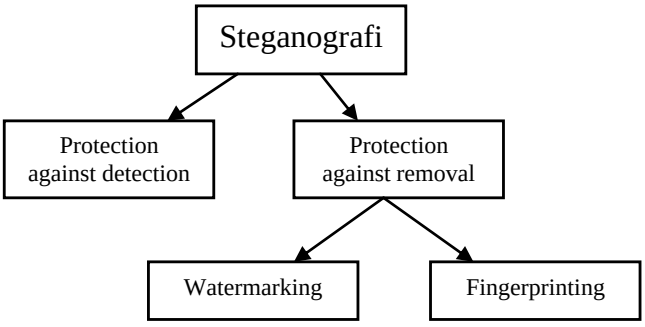
2.4 Sistem Penyembunyian pada Steganografi

Dalam sistem penyembunyian, ada tiga aspek yang berbeda dan saling bertentangan, yaitu : kapasitas, kemanan, dan ketahanan. Kapasitas adalah jumlah informasi yang dapat disembunyikan dalam media penampung. Jadi kapasitas data yang dapat disisipkan tergantung pada besar kapasitas media penampung/media sampul. Sedangkan keamanan adalah pencegahan bagi orang awam untuk mendeteksi adanya pesan maupun informasi tersembunyi. Ketahanan adalah kemampuan untuk menahan serangan(*attack*) yang dapat menemukan maupun menghancurkan informasi tersembunyi yang tersimpan dari suatu media sampul. 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. Sedangkan steganografi, mengejar kapasitas dan keamanan tinggi, yang dimana sering diketahui bahwa informasi yang tersembunyi mudah diketahui. Bahkan modifikasi kecil kepada media stego dapat menghancurkannya (Provos, 2003).



Gambar 6. Model dasar embedding pada Steganografi

2.4.1 Pembagian pada Steganografi



Gambar 7. Pembagian Steganografi

Pada gambar diatas dapat dilihat bahwa proteksi dalam steganografi terbagi menjadi dua jenis/model yaitu :

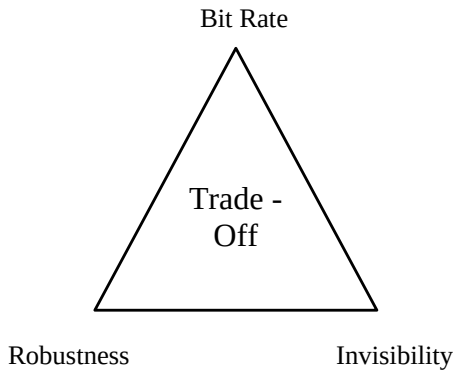
- *Protection* aginst *detection*

Model proteksi ini banyak digunakan dalam dunia maya sebagai security tools dalam suatu pengiriman data atau dokumen melalui internet atau media lainnya. Proteksi ini mempunyai metode agar suatu file/media sampul yang telah disisipi data tidak dapat dideteksi oleh steganalisis, sehingga data yang dikirimkan aman sampai orang yang ditujukan.

- *Protection against removal*

Model proteksi ini banyak digunakan dalam media digital security. Biasanya model ini berfungsi sebagai penanda hak cipta (*copyright*) agar tidak dapat dihilangkan maupun diganti oleh pihak-pihak lain yang tidak bertanggung jawab. Pada metode ini terdapat dua metode yang dapat digunakan, yaitu watermarking dan fingerprinting.

Watermarking merukpakan satu bentuk metode dari steganografi dalam mempelajari teknik-teknik bagaimana penyimpanan suatu data digital kedalam data sampul digital yang lain. Parameter-parameter yang ada dalam penerapan metode watermarking adalah jumlah data yang disembunyikan (*bit rate*), ketahanan terhadap proses pengolahan sinyal(robustness), tak terlihat atau output tidak berbeda dengan input awal(*invisibilty*).



Gambar 8. Trade-off dalam watermarking

3 Teknik Steganografi End of File

Teknik yang digunakan pada digital watermarking beragam tetapi secara umum teknik ini menggunakan redundant bits sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitive sehingga pesan tersebut tidak ada perbedaan yang terlihat atau yang terdengar.

Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut. Dalam teknik ini, data disisipkan pada akhir file dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut.

3.1 Implementasi Metode EOF pada DOS Text File

Peletakkan pesan rahasia yang digunakan pada DOS ini menggunakan EOF sebagai pengkalkulasian EOF melalui informasi direktori. Pembacaan file berbasiskan DOS membaca file hingga karakter Ctrl-Z yang dapat disebut elemen dari EOF. Prinsip penggunaan Ctrl-Z ini adalah pembatas antara *covertext*(media sampul) dengan pesan rahasia yang disispkan. Jadi apabila kita membuka file teks dengan binary pada DOS kemudian kita gabungkan dengan sebuah teks secara eksplisit setelah Ctrl-Z, maka pesan tersebut akan tersembunyi dibelakang EOF.

Steganografi pada DOS ini akan membaca seluruh karakter seluruh file di sampul media kemudian menulis karakter EOF Ctrl-Z. Setelah itu barulah program menulis pesan rahasia tersebut.

Contohnya:

Media Sampul : Halo bagaimana kabarmu disana

File yang disisipkan : bunuh pangeran jam 7

Maka bila dibuka pada mode biner akan menjadi

Halo bagaimana kabarmu bunuh pangeran jam 7

Tetapi apabila dibuka pada command prompt tidak akan diperlihatkan file yang disisipkan.

```
main(argc,argv)
     int    argc;
     char  *argv[];
{
  int bit;
  long count=0l;
  FILE *masukan;
  if ( argc == 2 )
    {
          infl = fopen(argv[1],"rb");
          if ( infl != NULL )
            {
while((byte=getc(masukan)) != EOF )
               {
                count++;
                putc(byte,stdout);
               }
                close(masukan);
            }
          else
            {
               printf("\n Tidak dapat
membuka file yang dimasukkan... \n\n");
            }
     }
  else
    {
```

```
        printf("\n Silahkan masukkan
file \n");
    }
}


main(n,params)
  int i;
  char *karakter[];
{
  FILE *berkas,*data;
  int ch=0;
  if ( i == 3 )
    {
      berkas   =   fopen(   karakter[1],
"ab"
);
      berkas   =   fopen(   karakter[2],
"rb"
);
      if ( berkas != NULL && data
!= NULL )
        {
          fseek(berkas, 0, 2);
          putc(26,berkas);
          while ( (ch = getc(data))
!= EOF )
            {
                  putc(ch,berkas);
            }
        }
      else
        {
          printf("\n Berkas yang
dimasukkan tidak dapat dibuka \n");
        }
      fclose(data);
      fclose(file);
      }
  else
    {
      printf("\n Format yang benar
adalah :\n lappend <file appended
to>");
      printf("<file to append>\n");
    }
}
```

Gambar 9. Penggalan Algoritma untuk mencari Ctrl-Z dan untuk menulis file yang akan disisipkan

4 Teknik Dynamic Cell Spreading

Teknik *Dynamic Cell* Spreading adalah sebuah teknik steganografi yang menggunakan metode protection against detection dengan konsep dasar menyembunyikan pesan digital ke dalam media gambar. Penyembunyian pesan dilakukan dengan menyisipkan pada bit rendah LSB(*Least Significant* B*i*t) dari pixel-pixel yang menyusun file tersebut menggunakan buffer memori yang digunakan sebagai media penyimpanan sementara.

Proses penggabungan file gambar dengan teks untuk file bitmap 24 bit maka setiap pixel pada gambar tersebut akan terdiri dari susunan warna-warna dasar(*Red*, *Green*, *Blue*) yang masing-masing disusun oleh bilangan 8 bit dari 0 sampai 255 yang dapat ditulis juga dalam format bilangan biner dari 00000000 sampai 11111111. Oleh karena itu, pada setiap pixel file bitmap 24 bit, kita dapat menyisipkan 3 bit data. Contohnya kita akan menyisipkan sebuah huruf A disebuah data, data raster originalnya adalah

11101001	00010100	10100010
00100101	10101010	11010111
11100100	11100101	11111001

Huruf A dalam biner adalah 10000111. Dengan menyisipkan pada data raster diatas dengan metode LSB maka data yang dihasilkan adalah

11101001	00010100	10100010
00100100	10101010	11010111
11100101	11100101	11111001

Dari contoh diatas dapat diketahui hanya dua bit rendah yang berubah dari data raster originalnya, bila dilihat oleh manusia maka data tersebut tidak akan tampak perubahannya. Dari penelitian yang ada, metode ini rata-rata hanya akan mengubah setengah bit rendah dari data raster awal. Sehingga apabila dibutuhkan dapat menggunakan bit rendah kedua atau ketiga.

Sedangkan proses penggabungan file gambar dengan data elektronik hampir sama dengan penggabungan dengan teks tetapi pada penggubungan dengan data elektronik akan lebih kompleks karena membutuhkan memori perantara untuk menghitung jumlah bit keseluruhan yang ada dalam file gambar maupun dalam media elektronik yang akan disisipkan. Hal ini dilakukan agar dapat memudahkan proses penyembunyian pesan(*embedding*) tersebut.

Dalam proses perhitungan aritmatika, pada proses embedding maupun proses extracting menggunakan perintah assembler. Hal ini dikarenakan proses tersebut menggunakan bit-bit yang ada dalam memori.

Proses-proses penyembunyian(*embedding*) dalam teknik *Dynamic Cell Spreading* adalah:

- Membuat re*g*istry *address* yang akan digunakan untuk menyimpan memori sementara yang digunakan dalam proses perhitungan *Least Significant Bit* pada gambar maupun data digital yang akan disisipkan.

- Mengkonversi gambar JPEG ke dalam bitmap. Hal ini digunakan untuk menekstrak gambar agar dapat lebih mudah dalam penghitungan dan penempatan data.
- Menghitung jarak antar bit yang ada pada file gambar. Hal ini berfungsi untuk mempermudah penghitunggan dan penyisipan bit data yang akan dimasukkan.
- Mengalokasikan memori untuk menampung bit gambar pada saat proses steganografi akan dijalankan.
- Mengkopi bitmap ke dalam *buffer* memori.
- Mendapatkan ukuran data yang akan digabungkan ke dalam gambar.
- Mengkopi *buffer* memori ke bentuk *bitmap* mengubah kembali dari memori menjadi file gambar.

Proses-proses ekstraksi dalam teknik *Dynamic Cell Spreading* adalah:

- Membuat registry address yang akan digunakan untuk menyimpan memori sementara yang digunakan dalam proses perhitungan *Least Significant Bit* pada gambar maupun data digital yang akan dipisahkan.
- Mengkalkulasikan variabel yang ada pada media pembawa pesan.
- Mengalokasikan ukuran memori yang akan digunakan dalam proses.
- Mengkopi bitmap ke dalam *buffer* memori.
- Mengekstrak ukuran file pembawa pesan bertujuan untuk menghitung dan mengembalikan kembali ukuran file pembawa pesan(media sampul) ke dalam ukuran yang semula sebelum disisipkan file lain.
- Mengkalkulasikan variabel yang ada menghitung kembali setelah proses
- Mengekstrak file yang bertujuan untuk mengambil data dalam file gambar yang telah dihitung dan disiapkan dalam memori sebelumnya sehingga proses dapat berjalan dengan cepat.

4.1 Implementasi DCS

Pada pengimplementasian menggunkan teknik DCS ini pertama-tama membuat registry address sesuai dengan teori yang telah dijelaskan pada bab sebelumnya. Registry address ini dipergunakan untuk menyimpan memori sementara dalam sistem yang kemudian digunakan untuk menginisialisasi data asli. Data ini kemudian disisipkan dengan file gambar menggunakan teknik ini dan hasilnya akan ditampilkan. Data yang telah disembunyikan akan dapat dikembalikan lagi ke data asli.

Teknik DCS memiliki prosedur utama dalam proses penyembunyian maupun pengekstrakan, yaitu dalam proses mengkopi *bitmap* ke *buffer* dan proses mengkopi *buffer* ke *bitmap*. Prosedur mengkopi dari *bitmap* ke *buffer* digunakan sekali di setiap proses dan prosedur mengkopi *buffer* ke *bitmap* digunakan pada saat embedding file.

Prosedur mengkopi *bitmap* ke *buffer* bertujuan untuk merubah dari bentuk bitmap yang kemudian diubah ke bahasa assembly untuk mendapatkan keseluruhan bit dari gambar yang telah didapat dari *buffer* memori.

```
Procedure CopyBitmapToBuffer(Bitmap:
  TBitmap);
var Hasil: pointer;
Panjang, Lebar, Kolom, Baris: longint;
Source: ByteArray;
begin
      Hasil:= pHasil;
      Panjang:= Height-1;
      Lebar:= Width_Byte-1;
      for Baris:= 0 to Panjang do
      begin
      Source:= Bitmap.ScanBaris[Baris];
       for Kolom:= 0 to Lebar
       do
             asm
             push eax
             push ebx
             push ecx
             mov eax, [Source]
             mov ebx, [Hasil]
             mov cl, [eax]
             mov [ebx], cl
             inc [Hasil]
             inc [Source ]
             pop ecx
             pop ebx
             pop eax
      end;
end;
end;
```

Gambar 10. Algoritma untuk mengkopi dari Bitmap ke Buffer

Prosedur mengkopi *buffer* to *bitmap* digunakan untuk merubah bentuk dari nilai bit dari proses assembler pada *buffer* memory ke bentuk file *bitmap*.

```
Procedure CopyBuffeToBitmap(Bitmap:
TBitmap);
var Hasil: pointer;
Kolom, Baris: longint;
Source: ByteArray;
begin
      Hasil:= pHasil;
      for Baris:= 0 to Height-1 do
      begin
      Source:= Bitmap.ScanBaris[Baris];
      for Kolom:= 0 to Width_Byte-1
      do
```

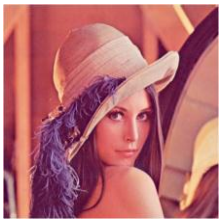
```
                asm
                push eax
                push ebx
                push ecx
                mov eax, [Hasil]
                mov ebx, [Source]
                mov cl, [eax]
                mov [ebx], cl
                inc [Hasil]
                inc [Source]
                pop ecx
                pop ebx
                pop eax
        end;
end;
end;
```

Gambar 11. Algoritma untuk mengkopi dari Buffer ke Bitmap

Steganografi merupakan teknik menyembunyikan suatu data didalam file lain sehingga pada hasil akhir proses steganografi tidak berbeda jauh dengan file aslinya, karena bila terjadi perbedaan akan dapat menimbulkan kecurigaan terhadap orang lain yang tidak berhak menerima file yang telah dimodifikasi tersebut.

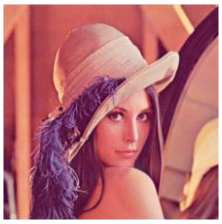
Contoh

Gambar awal :

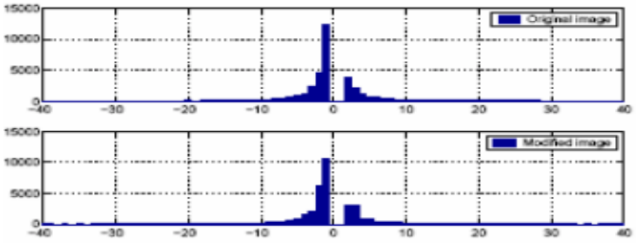


Isi pesan :
Sebuah file.txt

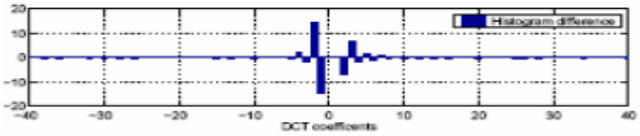
Gambar hasil setelah disispi text :



Secara kasat mata tidak dapat terlihat hasil steganografi. Tetapi apabila dilihat dengan menggunakan histogram akan terlihat perbedaannya



Gambar 12. Perbandingan Steganografi dengan Histogram



Gambar 13. Perbedaan sebelum dan sesudah disisipi file pada Histogram

5. Analisis

Teknik *End of File* merupakan suatu teknik yang menggunakan tanda pengenal untuk memisahkan awal dan akhir dari file yang ingin disisipkan. Pada implementasi EOF pada text file di DOS, Ctrl-Z digunakan sebagai penanda akhirfile sekaligus penanda dimana file yang disisipkan mulai ditulis.

Pada teknik *Dynamic Cell Spreading* menerapkan metode embedding data dengan menggunakan *Least Significant* Bit. Dimana penggunaan LSB ini dilakukan dengan mempersiapkan suatu arus bit, kemudian menetapkan LSB dari sampul media yang sesuai dengan nilai dari kedua file yang akan disatukan. Jarak antara dua bit tersembunyi yang berurutan menjadi banyaknya contoh dari metode ini dan dikendalikan melalui suatu nilai acak.

Teknik *Dynamic Cell Spreading* memiliki kelebihan pada tingkat keamanannya, sampai saat ini belim ada steganalisis yang mampu memecahkan keamanan dengan menggunakan teknik ini. Keamanan dari teknik ini didapat karena pada proses melakukan penggabungan atau penyisipan data, data dipecah dahulu kemudian dimasukkan ke dalam bentuk binary RGB(*Red*,*Green*, *Blue*) melalui proses pengukuran memory eksternal dan menggunakan perintah assembly untuk menyisipkannya.

Kelemahan dari teknik *Dynamic Cell Spreading* ini ada pada model *embedding*. Kelemahan ini didapat dari bentuk outpt file yang jika disisipkan file yang besar akan tidak menyerupai media sampulnya, sehingga steganalisis akan curiga dengan file tersebut.

6. KESIMPULAN

Dengan adanya steganografi, pengiriman pesan dengan menyisipkan pada sebuah media sampul akan lebih aman dan tidak mudah menimbulkan kecurigaan dari pada dengan menggunakan kriptografi. Dengan menggunakan teknik ini jika dikaitkan dengan hak cipta dan kepemilikan maka hak cipta akan dapat terjaga dengan baik.

Menurut analis diatas, teknik DCS lebih aman dari pada teknik EOF karena teknik EOF menggunakan penanda pada akhir file sehingga dapat dengan mudah dideteksi. Dibandingkan dengan teknik EOF, teknik DCS menggunakan teknik LSB. Implementasi program dilakukan dengan menggunakan bahasa tingkat rendah yaitu bahasa assembly. Dan juga teknik DCS mempunyai cara manajemen alokasi memori yang cukup baik dalam melakukan *embedding* dan ekstaksi sehingga tidak memboroskan memori.

7. REFERENSI

[1] Suhono, Supangkat, H., Juanda, K. (2000). Watermarking Sebagai Teknik Penyembunyian Hak Cipta Pada Data Digital. Jurnal Departemen Teknik Elektro, Institut Teknologi Bandung.

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

[2] http://www.digimarc.com/watermarking/>. Digimarc Corporation. June 2004. Diakses pada 24 Maret 2010 pukul 19.30

[3] Ohmacht, H. (2001). Stegano Project. http://www.holger-ohmacht.de. Diakses pada 24 Maret 2010 pukul 19.45

[4] http://journal.uii.ac.id/index.php/media-informatika / article /viewFile/3/3. Diakses pada 24 Maret 2010 pukul 20.00