PENYEMBUNYIAN DAN PENGACAKAN DATA TEXT MENGGUNAKAN STEGANOGRAFI DAN KRIPTOGRAFI TRIPLE DES PADA IMAGE

Agus Prihanto, Suluh Sri Wahyuningsih
Jurusan Teknik Informatika, Fakutas Teknologi Informasi
Institut Teknologi Sepuluh Nopember - Surabaya
E-mail : guspri_inf@cs.its.ac.id, suluh@cs.its.ac.id

ABSTRAK

Telah umum diketahui bahwa kriptografi bersifat mengacak pesan sehingga tidak mudah dimengerti, sedangkan steganografi merupakan seni menyembunyikan pesan sehingga tidak terlihat. Pesan dalam cipherteks mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan steganografi tidak akan menimbulkan kecurigaan karena secara visual tidak kelihatan.

Banyak metode steganografi yang telah dikembangkan salah satunya adalah Least Bit Insertion (LSB) yaitu menyisipkan pesan pada bit terendah pada pixel image dengan memanfaatkan kelemahan mata manusia. Metode ini memiliki kelebihan yaitu sederhana, cepat dan mempunyai kapasitas penyisipan yang cukup besar namun mempunyai kelemahan mudah dideteksi pesannya sehingga kurang aman. Tujuan penelitian ini adalah mengatasi kelemahan metode LSB dengan menggabungkan teknik steganografi dan cryptografi Triple DES sehingga pesan yang tersisip lebih aman.

Kata Kunci:Steganografi,Kriptografi,Triple DES,LSB

1. Pendahuluan

Steganografi sebagai suatu seni penyembunyian pesan ke dalam pesan lainnya yang telah ada sejak sebelum masehi dan kini seiring dengan kemajuan teknologi jaringan serta perkembangan dari teknologi digital, steganografi banyak dimanfaatkan untuk mengirim pesan melalui jaringan Internet tanpa diketahui orang lain dengan menggunakan media digital berupa file gambar [1].

Walaupun steganografi dapat dikatakan mempunyai hubungan yang erat dengan kriptografi, tetapi metode steganografi sangat berbeda dengan kriptografi. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat. Pesan dalam cipherteks mungkin akan menimbulkan kecurigaan sedangkan pesan yang dibuat dengan steganografi tidak akan menimbulkan kecurigaan karena secara visual tidak kelihatan.

Ada beberapa metode steganografi untuk penyisipan pesan pada gambar yang pernah diteliti sebelumnya diantaranya adalah[3] :

- Least Significant Bit Insertion (LSB).
- Algorithms and Transformation.
- Redundant Pattern Encoding.
- Spread Spectrum method.

Pada penelitian ini digunakan metode penyisipan pesan pada LSB (Least Significant Bit Insertion) atau penyisipan pesan pada bit terendah. Metode LSB merupakan salah satu metode steganografi yang paling sederhana, cepat dan mempunyai kapasitas penyisipan yang cukup besar namun mempunyai kelemahan mudah dideteksi pesannya sehingga kurang aman.

Untuk mengatasi kelemahan pada metode LSB tersebut dalam penelitian ini dicoba untuk menggabungkan teknik steganografi, metode LSB, dan teknik kriptografi Triple DES untuk mengacak pesan dengan tujuan agar pesan lebih aman.

Format image yang digunakan dibatasi pada bitmap 24 bit dan penyisipan secara berurut pada pixel RGB.

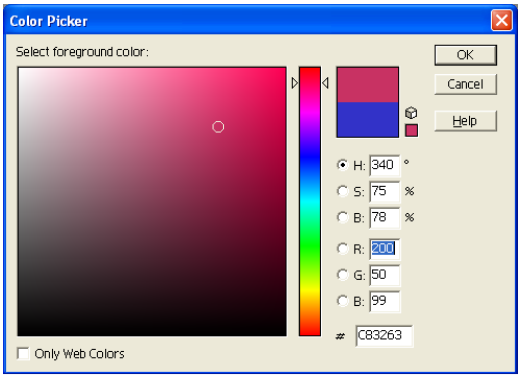
2. KONSEP BITMAP, TRIPLE DES . dan LSB

2.1 Bitmap

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*) [2].

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.

Berikut adalah contoh color pallete yang sering digunakan dalam pengolahan warna.



Gambar 1 : Color Pallete

2.2 Triple DES Cryptograghy

Triple DES merupakan kriptografi simetris dengan kunci encrypt dan decrypt message adalah sama. Triple DES merupakan penyempurnaan dari kriptografi DES sebelumnya[1].

Pada Triple DES pengenkripsian pesan dilakukan sebanyak tiga kali. Enkripsi ini dapat dicapai dengan beberapa cara. Sebagai contoh, pesan dapat dienkripsi dengan kunci 1, dekripsi dengan kunci 2 (pada dasarnya enkripsi yang lain), dan dienkripsi lagi dengan kunci 1:

[E{D(M,K1),K2},K1]

Enkripsi Triple DES dengan cara ini dikenal sebagai DES-EDE2. Jika tiga enkripsi dijalankan menggunakan dua kunci, dikenal sebagai DES-EEE2:

[E{E[E(M,K1)],K2},K1]

Sama dengan diatas:

[E{E[E(M,K1)],K2},K3]

Persamaan terakhir menggambarkan enkripsi Tripel DES-EEE3 dengan tiga kunci yang berbeda dan merupakan bentuk yang paling aman dari Triple DES.

2.3 Least Significant Bit Insertion (LSB)

Metode LSB 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[3].

Contoh penyisipan huruf A pada bitmap 24 bit pixel dengan data raster original adalah sebagai berikut :

```
00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001
```

Sedangkan representasi biner ASCII huruf A adalah :

```
100000111.
```

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

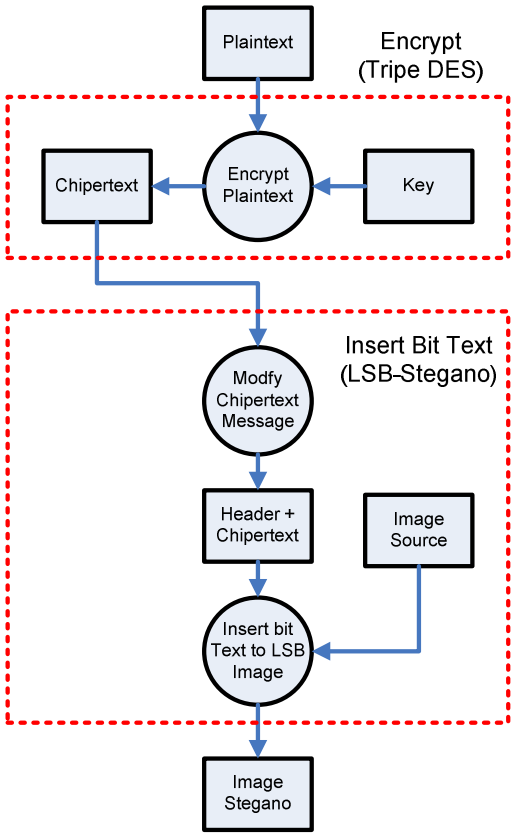
dengan metoda ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga.

3. PERENCANAAN SISTEM

Pada penelitian ini dibuat sebuah program steganografi dengan kriptografi Triple DES menggunakan bahasa pemrograman Delphi 7.

Pada program ini terdiri dari 2 bagian utama yaitu :

3.1 Enkripsi dan Penyisipan Bit



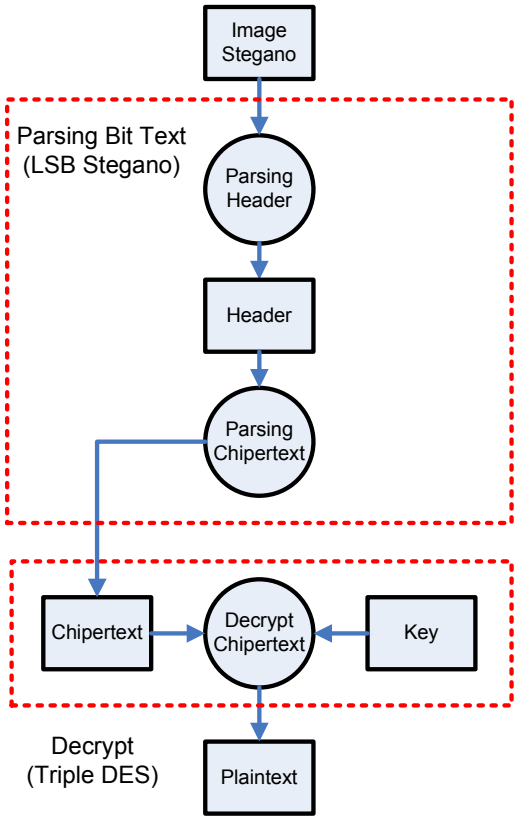
Gambar 2 : Diagram Aliran Proses Enkripsi dan Penyisipan

Blok ini bertugas untuk mengenkripsi pesan dan chipertext yang dihasilkan kemudian disisipkan pada LSB pixel image source sehingga dihasilkan image stegano.

Berikut adalah blok proses yang terlibat dalam Enkripsi dan Penyisipan bit :

- **Encrypt Plaintext** berfungsi untuk merubah pesan plaintext menjadi chipertext (input : *plaintext, key* dan output : *chipertext*).
- **Modify Chipertext Message** berfungsi menambahkan header pada chipertext. Header berisi tentang informasi panjang karakter chipertext dan didefinisikan mengambil tempat sebanyak 6 karakter. (input : *chipertext* dan output : *header+chipertext*).
- **Insert bit to LSB Image** berfungsi menyisipkan ASCII bit chipertext yang telah diberi header ke dalam LSB Byte RGB pixel image (input : *image, header+chipertext* dan output : *image stegano*).

3.2 Parsing Bit dan Dekripsi



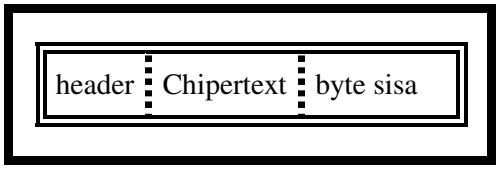
Gambar 3 : Diagram Aliran Proses Parsing dan Dekripsi

Blok ini bertugas mem-parsing message (header+chipertext) yang telah terembed dalam image stegano dan mendekripsi chipertext yang telah didapatkan sehingga didapatkan plaintextnya kembali.

Berikut adalah blok proses yang terlibat dalam Parsing Bit dan Dekripsi :

- **Parsing Header** berfungsi untuk mendapatkan string header dari message terembed (input : *image stegano* dan ouput : *string header*).
- **Parsing Chipertext** berfungsi untuk mendapatkan chipertext yang terembet. Hal Ini dilakukan dengan menscanning LSB Byte RGB pixel image secara urut sepanjang informasi ukuran header yang didapatkan sebelumnya (input : *image stegano, header* dan output : *chipertext*).
- **Decrypt Chipertext** berfungsi untuk mendaptkan kembali pesan asli/plaintextnya (input : *chipertext, key* dan output : *plaintext*).

Image Stegano yang di hasilkan akan mempunyai susunan byte pixel seperti yang terdapat pada gambar 4.



Gambar 4 :Susunan Byte Pixel Image Stegano

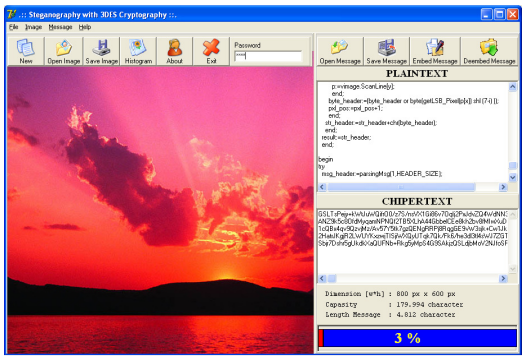
Pada gambar 4 di atas, header berisi informasi dari panjang chipertext dan telah didefinisikan dengan mengambil tempat sebanyak 6 karakter. Informasi header tersebut diperlukan agar scanning yang dilakukan hanya pada bit LSB dari karakter chipertext yang telah disisipkan saja dan tidak dilakukan scanning bit LSB pada seluruh gambar. Jika tidak ada informasi panjang chipertext pada header berarti tidak ada pesan yang terembed.

4. UJI COBA DAN HASILNYA

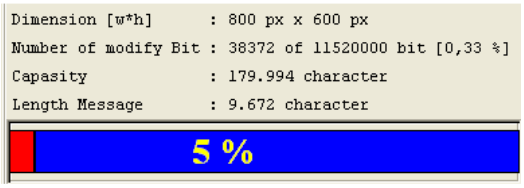
Gambar 5 menunjukkan Interface program Steganografi dan Cryptografi Tiple DES yang dibuat menggunakan Delph7. Dalam aplikasi ini terdapat 2 fungsi utama yaitu embed dan deembed message.

Dalam penelitian ini diambil sampel source image berukuran 800 x 600 pixel berformat bitmap 24 bit dan data masukan berupa teks dengan panjang pesan setelah dienkripsi = 9.672 karakter atau sekitar 5 % dari capasitas maximum (179.994 karakter).

Kemudian setelah dilakukan penyisipan bit ASCII message ke LSB Byte RGB Pixel image di dapatkan perubahan bit sebesar 38.372 bit atau sekitar 0,33 % dari bit total (11.520.000 bit). Berikut adalah capture gambar informasi yang didapatkan dari uji coba sesuai dengan data yang telah disebutkan di atas.



Gambar 5 : Inteface Program



Gambar 6 : Informasi Hasil Uji Coba

Untuk menghitung kapasitas maximum chipertext yang dapat disisipkan dalam sebuah image bitmap, maka dalam program ini digunakan rumus :

M = (3 x w x h) / 8 – msg_header

Dengan :

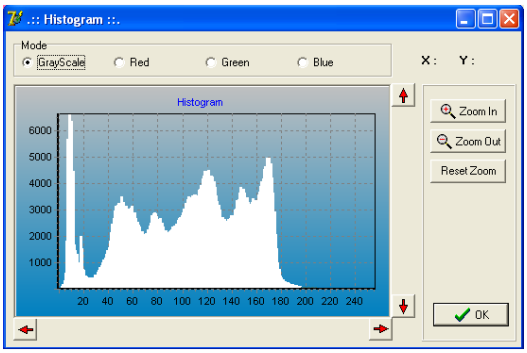
M = Maximum karakter

W = lebar gambar

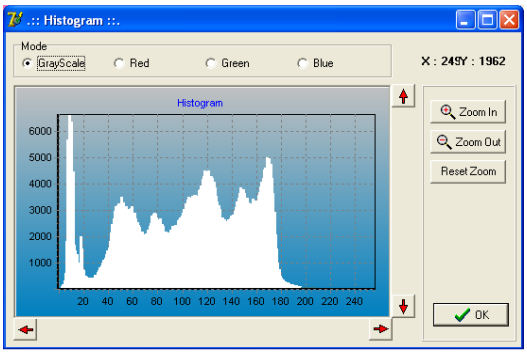
H = tinggi gambar

Msg_header = panjang header (6 karakter).

Setelah dilakukan analisa dengan histogram penyebaran warna sebelum dan sesudah penyisipan pesan, diperoleh hasil histogram yang hampir sama (tidak nampak perbedaan yang berarti) seperti ditunjukkan pada gambar 7 dan gambar 8. Hal ini diperkuat juga dengan informasi pada gambar 6 yaitu untuk number of modify bit (jumlah perubahan bit) sebesar 0,33 % terhadap bit total.



Gambar 7 : Histogram sebelum penyisipan.



Gambar 8 : Histogram setelah penyisipan.

Dari pengamatan terhadap enkripsi data menggunakan tiple DES diperoleh hasil bahwa perubahan kecil pada karakter plaintext maupun key akan merubah secara drastis chipertext yang dihasilkan. Hal ini dapat terlihat dari hasil ujicoba berikut ini :

- **Percobaan 1**

  Plaintext : Bunuh Bossmu
  Key : kila
  Chipertext : VzPHEgneaEPwkuWZ

- **Percobaan 2**

  Plaintext : Bunuh Bossmu
  Key : kili
  Chipertext : 33ehCar2EauIRyiB

Hal tersebut terjadi karena Triple DES menggunakan fungsi hash dalam proses pengenkrpsian-nya. Kenyataan ini akan menambah tingkat keamanan data meskipun message yang terembed telah berhasil didapatkan dan tidak mudah untuk mendapatkan pesan plaintext kembali karena pesan yang terembed telah di acak menggunakan enkripsi Triple DES.

5. KESIMPULAN DAN SARAN

1. Kesimpulan

- Program steganografi yang dibuat menggunakan metode Least Bit insertion (LSB) ini mepunyai capasitas yang tinggi yaitu : M = (3 x w x h) / 8 – msg_header. Pada penelitian ini digunakan image dengan ukuran 800 x 600 pixel sehingga diperoleh kapasitas maximum sebesar 179.994 karakter.
- Setelah dilakukan analisa perbandingan terhadap histogram dari image source dan image hasil stegano diperoleh histogram yang hampir sama dengan nilai perbedaan sebesar 0,33 % terhadap bit total image (number of modify LSB), sehingga sulit dibedakan antara gambar asli dengan gambar hasil steganonya dan dengan demikian tidak menimbulkan kecurigaan.
- Pesan yang disisipkan ke image lebih aman karena pesan yang disisipkan berupa chipertext hasil dari enkripsi Triple DES dan bukan plaintext secara langsung.

2. Saran

Untuk meningkatkan kapasitas message stegano dapat dilakukan dengan :

- Menggunakan lebih dari 1 pixel LSB (bit kedua, ketiga dari LSB).
- Mengkompres message sebelum disisipkan.

6. DAFTAR PUSTAKA

- [1] William Stallings, Cryptography and Network Security, Fourth Edition
- [2]http://en.wikipedia.org/wiki/Color_histogram.htm.
- [3]Nova Hadi Lestriandoko dan Sandra Yuwana, Pemanfaatan Color-Frequency Citra Digital untuk Menyembunyikan Data Digital, Proceeding Seminar Nasional Pascasarjana 2006, ITS, Agusus 2006.