PENERAPAN STEGANOGRAFI METODE END OF FILE (EOF) DAN ENKRIPSI METODE DATA ENCRYPTION STANDARD (DES) PADA APLIKASI PENGAMANAN DATA GAMBAR BERBASIS JAVA PROGRAMMING

Article · March 2014

CITATIONS
6

READS
5,342

2 authors:

Yayuk Anggraini
Universitas Budi Luhur
1 PUBLICATION **6** CITATIONS
SEE PROFILE

Dolly Shaka
Universitas Budi Luhur
5 PUBLICATIONS **8** CITATIONS
SEE PROFILE

KNSI2014-346

PENERAPAN STEGANOGRAFI METODE *END OF FILE* (EOF) DAN ENKRIPSI METODE *DATA ENCRYPTION STANDARD* (DES) PADA APLIKASI PENGAMANAN DATA GAMBAR BERBASIS JAVA PROGRAMMING

Yayuk Anggraini[1], Dolly Virgian Shaka Yudha Sakti[2]

[1,2]Magister Ilmu Komputer, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753 ext.303, Fax. 5853489
yayuk.anggraini@budiluhur.ac.id, dolly.virgianshaka@budiluhur.ac.id

Abstrak

Terdapat beberapa cara untuk menangani masalah keamanan data rahasia yang dikirimkan melalui internet, diantaranya adalah menggunakan teknik kriptografi dan steganografi. Steganografi merupakan ilmu dan seni penyembunyian informasi/pesan pada suatu media sedemikian rupa sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan karena file terlihat mencurigakan. Teknik Steganografi yang penulis gunakan adalah End Of File (EOF). Teknik EOF menggunakan cara menambahakan data atau file pada akhir file image. Untuk teknik ini, data atau file yang akan disembunyikan besar ukurannya dapat melebihi dari ukuran file image. Data yang disembunyikan tersebut akan disisipkan pada akhir file sehingga tidak akan mempengaruhi gambar. Aplikasi steganografi ini juga dilengkapi dengan fungsi kriptografi Data Encryption Standard (DES) pada saat penyisipan data yang berfungsi sebagai kode pembangkit dan mengenkripsi data, agar keamanan suatu data dalam file lebih terjaga dan terlindungi dari pihak yang tidak berhak mengetahui data tersebut. Jogjack Factory outlet merupakan usaha dagang yang bergerak dibidang fashion. Selain menjual, Factory Outlet ini mendesain dan memproduksi sendiri barang dagangannya. Desain yang dikirim sangat rahasia dan tidak boleh diterima oleh pihak lain. Dengan dikembangkan sebuah sistem dengan mengimplementasikan sistem keamanan data menggunakan steganografi dengan algoritma metode end of file (EOF) dan enkripsi data standard (DES) berbasis Java Programming diharapkan dapat melindungi data rahasia perusahaan agar tidak mudah terbaca oleh orang yang tidak berkepentingan.

Kata Kunci: *Steganografi, End of File, EOF, Data Encryption Standard, DES*

Pendahuluan

Pencurian data melalui media internet saat ini sangat marak dilakukan, karena mudah dilakukan oleh penyadap dan banyak pelaku bisnis yang masih belum menyadarinya, sehingga dengan mudah dan tanpa pikir panjang mengirim data penting melalui internet, salah satunya mengirim data melalui email. Persaingan pasar industri yang sangat pesat saat ini memungkinkan tiap perusahaan yang sedang bersaing melakukan hal yang tidak wajar dan melakukan kecurangan, yaitu dengan menyadap data-data yang dikirim melalui internet tersebut, sehingga memungkinkan mereka untuk mencontek atau mengambil hak paten, hal tersebut yang membuat persaingan menjadi tidak sehat karena saling menjatuhkan sesama kompetitor. Untuk itu dibutuhkan aplikasi penunjang yang dapat membuat data tidak bisa disadap, bahkan tidak menarik perhatian dari para pencuri tersebut, aplikasi yang dimaksud tersebut yaitu aplikasi Steganografi.

Steganografi adalah sebuah teknik penyembunyian pesan rahasia, yang biasanya sebuah pesan yang disisipi (diekstrak) kedalam suatu media sebagai pembawa pesan.

Menurut Dony Ariyus [1] dalam bukunya yang berjudul Keamanan Multimedia :

"Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) didalam file-file lain yang mengandung teks, image, bahkan audio tanpa

menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari file semula. Metode ini termasuk tinta yang tidak tampak, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar. Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi"

Keuntungan bagi perusahaan adalah perusahaan mampu merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari orang-orang yang berpotensial mencurinya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan. Pokok permasalahan yang dihadapi adalah:

Desain rahasia dan tidak boleh diketahui orang lain. Sehingga aplikasi ini ditujukan untuk mengamankan data yang ingin dikirimkan.

Desain yang dibuat harus dikirim ke tempat produksi melalui email sehingga mudah terjadi pencurian data. Jika desain tersebar luas perusahaan mengalami kerugian.

Pada jurnal sebelumnya [7] membahas tentang keamanan data menggunakan steganografi dengan metode End Of File (EOF) yang dibuat tanpa menggunakan enkripsi. Hal ini membuat pesan yang dikirim belum sepenuhnya aman, karena pesan yang disembunyikan merupakan file asli tanpa enkripsi, hal ini memungkinkan jika file dapat terbuka maka pesan dapat langsung dibaca oleh pihak yang tidak berhak atas pesan tersebut.

Dengan ditambahkannya enkripsi pada penyisipan pesan steganografi, maka pesan yang akan dikirim lebih terjaga kerahasiaannya, karena sebelum pesan disembunyikan, pesan tersebut sudah di-enkrip terlebih dahulu agar suatu saat jika pesan tersebut berhasil dibuka oleh orang yang tidak berhak, maka dia tidak akan dapat mengerti isi pesan tersebut.

Adapun masalah yang dapat dipecahkan adalah sebagai berikut:

Mengamankan desain rahasia yang tidak boleh diketahui orang lain

Menghindari terjadinya pencurian data

Desain aman dan perusahaan tidak mengalami kerugian dari pencurian desain.

Landasan Teori

Sebelum membahas lebih dalam baiknya kita mempelajari beberapa teori dasar berikut:

Dasar Penyembunyian (*Embed*)

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 [9].

Citra Digital

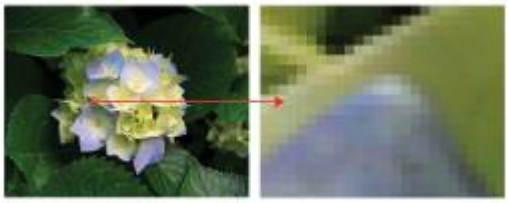
Citra menurut kamus Webster adalah suatu representasi atau gambaran, kemiripan, atau imitasi dari suatu objek atau benda, contohnya yaitu foto seseorang dari kamera yang mewakili orang tersebut, foto sinar *X-thorax* yang mewakili gambar bagian tubuh seseorang dan lain sebagainya.

Citra yang terlihat merupakan cahaya yang direfleksikan dari sebuah objek. Sumber cahaya tersebut akan menerangi objek, objek kemudian akan memantulkan kembali sebagian dari berkas cahaya tersebut dan pantulan cahaya lalu ditangkap oleh alat-alat optik, seperti mata manusia, kamera, scanner, dan sensor satelit, kemudian direkam. Citra sebagai keluaran dari suatu sistem perekaman data dapat bersifat optic berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan.

Citra digital adalah data yang ditampilkan dalam bentuk gambar sehingga memiliki arti tertentu. Sebuah citra digital menyimpan data berupa bit yang dapat dimengerti oleh manusia dengan visualisasi bit tersebut pada kanvas menjadi gambar. Pengolahan yang dapat dilakukan terhadap citra digital antara lain adalah menampilkan bentuk gambar, melakukan perubahan terhadap gambar

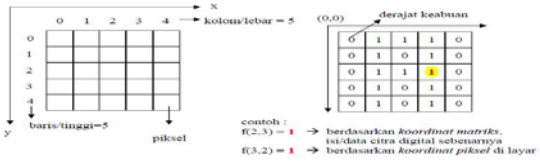
(image editing), dan mencetakan citra digital ke atas media berupa kertas.

Citra digital terdiri dari pixel-pixel berukuran kecil yang membentuk sebuah bentuk gambar yang dapat dilihat oleh mata manusia. Kepadatan *pixel-pixel* yang ada dalam gambar ini disebut dengan resolusi. Semakin besar resolusi sebuah citra *digital* maka kualitas gambar dari citra *digital* tersebut semakin baik. Gambar dibawah ini menunjukkan *pixel-pixel* yang ada dalam sebuah gambar.



Gambar 1: *Pixel* pada citra digital

Citra *digital* merupakan fungsi intensitas cahaya *f(x,y)*, dimana *x* dan *y* merupakan koordinat spesial dan fungsi tersebut pada setiap titik *(x,y)* merupakan tingkat kecemerlangan atau intensitas cahaya citra pada titik tersebut. Citra *digital* adalah suatu matriks dimana indeks baris dan kolomnya menyatakan suatu titik pada citra tersebut dan elemen matriksnya yang disebut sebagai elemen gambar atau *pixel* menyatakan tingkat keabuan pada titik tersebut. Indeks baris dan kolom *(x,y)* dari sebuah *pixel* dinyatakan dalam bilangan bulat (*integer*). Sebuah *pixel* merupakan sampel dari pemandangan yang mengandung intensitas citra yang dinyatakan dalam bilangan bulat. Untuk menunjukkan lokasi suatu *pixel*, koordinat (0,0) digunakan untuk posisi kiri atas dalam bidang citra, dan koordinat (m-1,n-1) digunakan untuk posisi kanan bawah dalam citra berukuran m x n *pixel* dimana m adalah kolom dan n adalah baris. Untuk menunjukkan tingkat pencahayaan suatu *pixel*, seringkali digunakan bilangan bulat yang besarnya delapan bit dengan lebar selang nilai 0-255 dimana 0 untuk warna hitam, 255 untuk warna putih, dan tingkat abu-abu berada di antara nilai 0 dan 255.



Gambar 2 Gambar Posisi Letak *Pixel*

Steganografi

Steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia sehingga selain orang yang dituju, orang lain tidakakan menyadari keberadaan dari pesan rahasia tersebut. Steganografi membutuhkan dua bagian yang sangat penting yaitu berkas atau media penampung dan data rahasia yang akandisembunyikan. Steganografi berfungsi untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi, dan juga dapat melindungi hak cipta dari suatu produk. Data rahasia yang disembunyikan dapat diungkapkan kembali sama seperti aslinya tanpa merusak media *file* dan pesannya.

Salah satu teknik Steganografi yang biasa dipakai adalah metode *End Of File*(EOF). Teknik ini tidak jauh beda dengan teknik*Least Significant Bit* (LSB). Jika LSB menambahkan data *file* pada akhir bit-nya, maka EOF langsung menambahkan data diakhir fileimage, dan sebelum pesan diberi penanda yang berupa karakter/simbol. Untuk teknik ini dapat menambahkan data atau *file* yang akan disembunyikan lebih dari ukuran*fileimage*. Data yang disembunyikan tersebut akan disisipkan pada akhir *file* sehingga tidak mempengaruhi gambar.

Enkripsi

Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi (*encryption*) atau *enciphering*.[6]

Enkripsi juga dapat diartikan sebagai cara untuk mengamankan data/informasilebih lanjutnya yaitu untuk melindungi informasi sensitif selama transmisi dan penyimpanan.

Algoritma kriptografi atau sering disebut dengan cipher adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi [8]. DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok.

Bahasa Pemrograman Java

Java adalah bahasa pemrograman berorientasi objek yang dikembangkan oleh Sun Microsystems sejak tahun 1991. Bahasa ini dikembangkan dengan model yang mirip dengan bahasa C++ dan Smalltalk, namun dirancang agar lebih mudah dipakai dan ber-platform independent, yaitu dapat dijalankan di berbagai jenis sistem operasi dan arsitektur komputer. Bahasa ini juga dirancang untuk pemrograman di internet sehingga dirancang agar aman dan portabel.

Pemrograman berorientasi objek adalah teknik untuk mengorganisasi program dan dapat dilakukan dengan hampir semua bahasa pemrograman. Namun Java telah mengimplementasikan berbagai fasilitas agar seorang pemrogram dapat mengoptimalkan teknik pemrograman berorientasi objek. Selain itu, *Java* juga memiliki fasilitas perpustakaan (*library*) yang luas untuk memudahkan pemrogram membuat aplikasi yang diinginkan.

Metodologi Penelitian

Metodologi yang digunakan dalam penulisan ini adalah sebagai berikut:

Eksplorasi dan Studi Pustaka

Merupakan tahapan untuk mempelajari literature-literatur yang ada berupa buku (*textbook*), jurnal dan artikel ilmiah, maupun *website* yang berkaitan dengan steganografi, dokumen citra dan metode *EOF*.

Analisis masalah

Merupakan tahapan untuk mengidentifikasi permasalahan yang akan dikaji. Dalam hal ini batasan ditentukan dari suatu bidang pengetahuan dan masalah yang akan dikaji, pakar yang akan terlibat sebagai narasumber dan tujuan yang relevan sesuai dengan judul tugas akhir ini.

Perancangan perangkat lunak

Merupakan tahapan untuk membuat desain, deskripsi dan spesifikasi terhadap steganografi yang akan diimplementasikan.

Implementasi perangkat lunak

Merupakan tahapan untuk pengecekan aplikasi steganografi yang telah dibuat berdasarkan hasil perancangan perangkat lunak.

Pengujian hasil implementasi

Merupakan tahapan untuk menjalankan aplikasi steganografi dengan data masukan yang telah ditentukan dan melakukan evaluasi terhadap performansi perangkat lunak.

Pembahasan

Ulasan Singkat Organisasi

Jogjack *Factory Oulet* merupakan usaha dagang yang bergerak dibidang *fashion*. Selain menjual, Factory Outlet ini mendesain dan memproduksi sendiri barang dagangannya. Ada banyak jenis pakaian yang ditawarkan dengan desain-desain yang menarik dan terbaru. Jogjack yang berkantor pusat di Jakarta ini mempunyai tempat produksi di Bandung, karena bahan produksinya lebih mudah dicari dan lebih murah. Produsen pengerjaan desain dikerjakan di Jakarta, setelah itu desain dikirim ke Bandung untuk diproduksi.

Desain yang dikirim sangat rahasia dan tidak boleh diterima oleh pihak lain. Selama ini pengiriman desain dilakukan melalui internet, namun yang terjadi banyak pengguna internet yang mengalami pencurian data yang dilakukan oleh oknum yang tidak bertanggung jawab. Fatalnya lagi jika file tersebut berisi dokumen yang berisi desain sebuah produk yang tidak boleh disebarluaskan, hal tersebut akan membuat perusahaan rugi besar karena desain tersebut akan ditiru oleh perusahaan lain dan hak patennya jatuh ke tangan mereka. Untuk itu penulis berniat untuk mengimplementasikan teknik steganografi ke Jogjack *Factory Oulet*

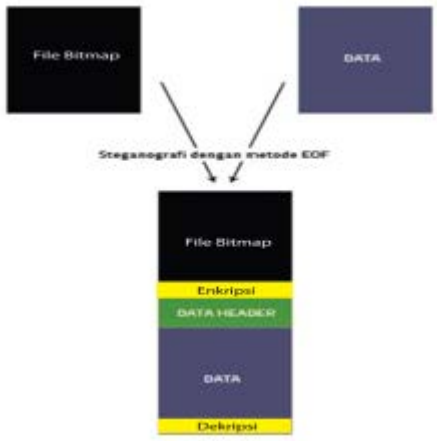
Metode *End of File* (EOF)

Metode *End of File* (EOF) merupakan salah satu teknik yang menyisipkan data pada akhir *file*[2]. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran *file* sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam *file* tersebut. Dalam teknik EOF, data yang disisipkan pada akhir*file* diberi tanda khusus sebagai pengenal *start* dari data tersebut dan pengenal akhir dari data tersebut.

Metode EOF merupakan sebuah metode yang diadaptasi dari metode penanda akhir *file* (*end of file*) yang digunakan oleh sistem operasi *windows*[3]. Dalam sistem operasi windows, jika ditemukan penanda EOF pada sebuah file, maka sistem akan berhenti melakukan pembacaan pada file tersebut. Prinsip kerja EOF menggunakan karakter/simbol khusus yang diberikan pada setiap akhir file. Karakter/simbol ini biasanya digunakan pada sistem operasi DOS untuk menandakan akhir dari sebuah penginputan data. Dengan berkembangnya sistem operasi windows, penggunaan karakter seperti ini dikembangkan untuk menandakan akhir dari sebuah file.

Dari metode yang telah penulis baca, metode End Of File(EOF) dengan Least Significant Bit (LSB) tidak begitu banyak perbedaan dalam alur algoritmanya, namun terdapat perbedaan yaitu pada pesan yang disisipi dan output. Pada metode LSB, pesan yang disisipi ukurannya harus lebih kecil dari citra yang akan disisipi, tetapi lain halnya pada metode EOF ukuran pesan yang akan disisipi bisa lebih besar dari ukuran citranya. Pada metode LSB citra yang telah disisipi pesan *(hidden text)*tidak terlalu mempengaruhi ukuran citranya, tetapi akanmempengaruhi kualitas citranya. Sedangkan pada metode EOF, kualitas citra setelah disisipi pesantidak berubah, tetapi akan mengubah ukuran citranya. Misalkan kita memiliki citra asal yang berukuran 150x200 *pixel*. Pesan yang disisipkan ada 422 karakter. Ukuran citra setelah disisipkan menjadi 153x200, dengan kata lain 422 karakter yang ada memakan tempat sebanyak 3 baris.

Dengan metode EOF, secara umum media steganografi (*file* yang akan disisipi data) memiliki struktur seperti gambar ini:



Gambar 3: Konsep EOF pada steganografi

Metode Enkripsi *Data Encryption Standard* (DES)

Data Encryption Standard (DES) adalah suatu blok cipher (salah satu bentuk enkripsi rahasia bersama) yang dipilih oleh National Bureau of Standar sebagai seorang pejabat *Federal Information Processing Standard* (FIPS) untuk Amerika Serikat pada tahun 1976 dan yang kemudian dinikmati secara luas yang digunakan internasional [4]. Hal ini didasarkan pada algoritma kunci simetris yang menggunakan 56-bit key. Algoritma awalnya diklasifikasikan kontroversial dengan elemen desain, kunci yang relatif pendek panjang, dan kecurigaan tentang National Security Agency (NSA) backdoor [5]. DES akibatnya datang di bawah pengawasan intens akademis yang memotivasi pemahaman modern dan blok cipher kriptoanalisis mereka.

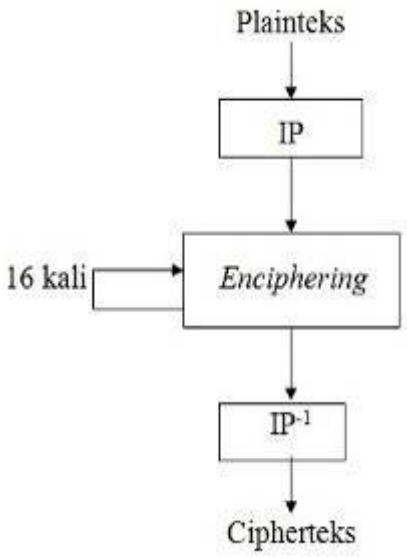
DES termasuk ke dalam sistem *kriptografi* simetri dan tergolong jenis *cipher*blok. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit *plainteks* menjadi 64 bit *cipherteks* dengan menggunakan 56 bit kunci internal (*internal key*) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

Skema global dari algoritma DES adalah sebagai berikut:

Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).

Hasil permutasi awal kemudian di-*enciphering* sebanyak 16 kali (16 putaran).Setiap putaran menggunakan kunci internal yang berbeda.

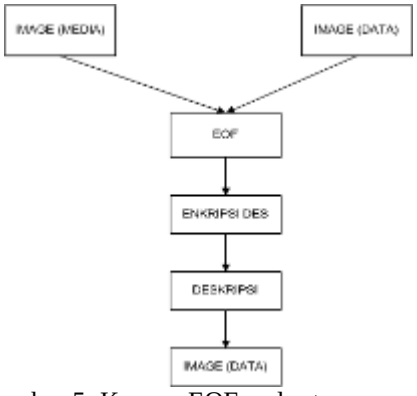
Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok *cipherteks*.



Gambar 4:Skema Global Algoritma DES

Struktur *File* Steganografi dengan Metode*End of File*(EOF) dan Enkripsi DES

Dengan metode EOF, secara umum media steganografi (*file* yang akan disisipi data) memiliki struktur seperti gambar ini:



Gambar 5: Konsep EOF pada steganografi

Pada gambar 5, dapat dijabarkan sebagai berikut :

Terdapat satu media dalam bentuk *file* citra, *file* tersebut kemudian digunakan untuk meng-*embed* data yang akan disisipkan.

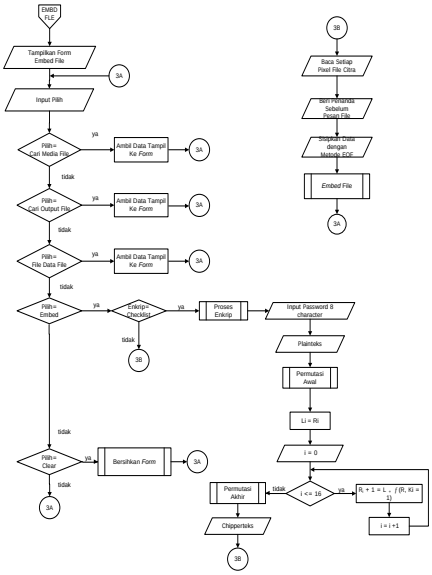
Selanjutnya dilakukan proses enkripsi pada data dan media file. Sedangkan enkripsi adalah proses mengacak data sehingga tidak dapat dibaca oleh pihak lain atau mengubah *plainteks* menjadi *chiperteks*. Adapun data *header* digunakan untuk membedakan media dengan data yang disisipkan.

Setelah proses enkripsi dilakukan, untuk membuka data yang telah disisipkan maka diperlukan adanya proses dekripsi. Sedangkan dekripsi adalah proses untuk mengubah *chiperteks* menjdi *plainteks*/data asli.

Flowchart

Flowchart Embed File

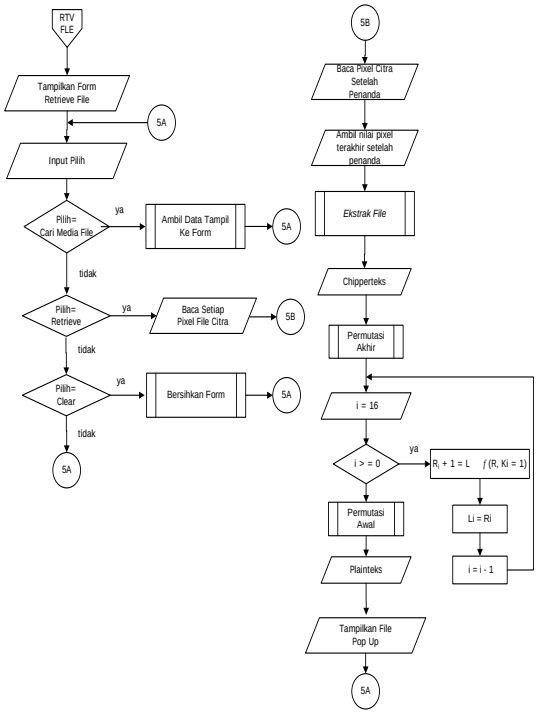
*Flowchart*berikut merupakan gambaran alur proses *Embed File*, *Form* ini terdapat fasilitas proses menyembunyikan pesan yang berupa *file* citra *bitmap*. Urutan proses yang akan dilalui pada *Form Embed File* digambarkan dengan *Flowchart* berikut ini:



Gambar 6: *Flowchart EmbedFile*

Flowchart Retrieve File

Flowchart berikut merupakan gambaran alur proses *Retrieve file*, *Form* ini terdapat fasilitas proses ekstrak pesan yang berupa *file* citra *bitmap*. Urutan proses yang akan dilalui pada *Form Retrieve File*digambarkan dengan *Flowchart*berikut ini:



Gambar 7: *FlowchartRetrieveFile*

Algoritma

Algoritma *Form Login*

Algoritma ini menjelaskan bagaimana berjalannya login aplikasi. Di bawah ini dijelaskan jika *username* dan *password* yang dimasukkan benar, maka user dapat membuka menu utama administrator.

1. Tampilkan Menu Utama,

Disable menu Embed dan Retrieve

2. Input Pilih

3.if Pilih=*File* then

4. Input Pilih

5. if Pilih=Login then

6.Tampilkan Form Login

7.Input Username dan

Password

8.Input Pilih

9.if Pilih=Login then

10.proses Cek UserName dan Password

11.if UserName=username & Password=password then

12.Menuju Menu Utama

13.else

14.Tampilkan Pesan Gagal Login

15.lanjut ke baris 6

16.end if

17.else if Pilih=Close then

18.lanjut ke baris 2

19.else

20.lanjut ke baris 6

21.end if

22.else if Pilih=Keluar then

23.selesai

24.else

25.lanjut ke baris 2

26.end if

27. else if Pilih=About then

28.Tampilkan About

29. lanjut ke baris 2

30. else if Pilih=Help then

31.Tampilkan Help

32. lanjut ke baris 2

33. else

34.lanjut ke baris 2

35. end if

Algoritma Menu Utama

Algoritma ini menjelaskan proses berjalannya Menu Utama. Di bawah ini dijelaskan terdapat beberapa pilihan menu di menu utama, diantaranya Menu *File*, Menu *Embed*, Menu *Retrieve*, Menu *About* dan Menu *Help*.

Tampilkan Menu Utama,
Enable Menu Embed dan Retrieve
Input Pilih
If Pilih=Embed then
Tampilkan Menu Embed
Input Pilih
if Pilih=Embed File Then
Menuju ke Form Embed File
Else
Menuju ke baris 2
End if
Else if Pilih=Retrieve then
Tampilkan Menu Retrieve
Input Pilih
If Pilih=Retrieve File then
Menuju ke baris 2
Else
Menuju ke Form Retrieve File
End if
Else if Pilih=About then

```
Tampilkan Form About
Menuju ke Baris 2
Else if Pilih=Help then
Tampilkan Form Help
Menuju ke Baris 2
Else
Menuju ke Baris 2
End if
```

Algoritma *Embed File*

Algoritma di bawah ini menjelaskan proses berjalannya form *Embed File* pada program aplikasi steganografi metode EOF. Untuk urutan proses yang lebih jelas dapat dilihat di bawah ini.

```
Tampilkan Form Embed File
Input Pilih
If Pilih=Cari Media File then
Proses Ambil Data Tampil Ke Form
Menuju ke baris 2
Else if Pilih=Cari Output File then
Proses Ambil Data Tampil Ke Form
Menuju ke baris 2
Else if Pilih=Data File then
 Proses Ambil Data Tampil Ke Form
 Menuju ke baris 2
 Else if Pilih=Embed then
 Input Media File
 if pilih enkrip=checklist
 Proses enkrip
 Planteks
 Proses Permutasi Awal
            Li = Ri
            i = 0
         if i <= 16
             Ri + 1 = L  +   f (R, Ki = 1)
             i = i +1
 Menuju ke baris 20
 Else Proses Permutasi Akhir
 Chippertext
 Menuju ke baris 20
 Baca Setiap Pixel File Citra
 Beri Penanda Sebelum Pesan File
 Sisipkan Pesan File
 Proses Embed File
 End if
 Else if Menuju ke baris 27
 End if
 Else if Pilih=Clear then
 Proses Bersihkan Form
 Menuju ke baris 2
 Else
 Menuju ke baris 2
 End if
```

Algoritma *Retrieve File*

Algoritma di bawah ini menjelaskan proses berjalannya form *Retrieve File* pada program aplikasi steganografi metode EOF. Untuk urutan proses yang lebih jelas dapat dilihat di bawah ini.

1. Tampilkan Form Retrieve *File*
2. Input Pilih
3. If Pilih=Cari Media *File*
4. Proses Ambil Data Tampil Ke Form
5. Menuju ke baris 2
6. Else if Pilih=Retrieve then
7. Baca Setiap Pixel *File* Citra
8. Baca Pixel Citra Setelah Penanda
9. Ambil nilai pixel terakhir setelah penanda
10. Proses Ekstrak *File*

11. Chipper
12. Proses Permutasi Akhir
13. i = 16
14. if i > = 0
15. $R_i + 1 = L \oplus f$ (R, Ki = 1)
16. Li = Ri
17. i = i - 1
18. Menuju ke baris 13
19. Else if Proses Permutasi Awal
20. Plainteks
11. Tampilkan *File*

Pop Up

12. Menuju ke baris

2

13. end if

13. Else if

Pilih=Clear then

14. Proses

Bersihkan Form

15.Menuju ke baris

2

16. Else

17.Menuju ke baris

2

18. End if

Tampilan Layar

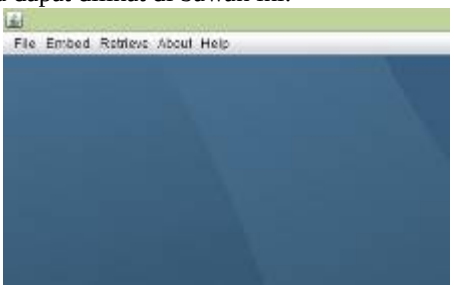
Tampilan Layar *Form Login*

Pada aplikasi ini ketika kita jalankan program maka akan langsung menuju halaman Menu Utama hanya ada tiga menu yang dipakai yaitu Menu *File*, Menu *Help* dan *About*. Yang harus dilakukan untuk dapat menggunakn semua menu utma adalah dengan *login* pada *form file login* di menu utama. Pada proses ini dilskuksn pengecekan *username* dan *password* yang berguna untuk keamanan aplikasi dan mengaktifkan Menu *Embed* dan Menu *Retrieve*. Berikut ini adalah tampilan Form Login tersebut. Tamilan selengkapnya dapat dilihat pada gambar di bawah ini :

Gambar 8: Tampilan Layar *Form Login*

Tampilan Layar Menu Utama

Setelah login berhasil dilakukan maka akan muncul tampilan menu utama yang menu-menunya sudah di *enable*, seperti Menu *Embed* dan Menu *Retrieve*. Dan jika kursor diarahkan ke menu *Embed* maka akan keluar sub menu *Embed Message* dan *Embed File*. Dan jika kursor diarahkan ke Menu *Retrieve* maka akan keluar sub menu *Retrieve Message* dan *Retrieve File*. Tampilan program menu utama dapat dilihat di bawah ini:



Gambar 9: Tampilan Layar Menu Utama

Tampilan Layar *Form Embed File*

Pada Form *Embed File*,user dapat melakukan *embed* pesan berupa file citra. Cara menjalankannya nya dengan masukkan file yang akan menjadi medianya kedalam media file. Lalu letakkanlah ke folder yang diinginkan ke dalam output file, kemudian pilihlah file yang ingin di sisipkan kedalam File Embed. Jika ingin di enkrip ceklis *Encrypt* dan masukkan delapan karakter *password*. Tampilan program menu *Embed File* dapat dilihat di bawah ini:

Gambar 10: Tampilan Layar *Form Embed File*

Gambar11 : Tampilan Layar Pesan Dialog *Embed File*

Tampilan Layar *Form Retrieve File*

Ketika file media sudah dipilih maka akan muncul informasi mengenai *Master File*, *Steganograph*, *Contains* dan *Requested Operation*. Tampilan program menu *Retrieve File* dapat dilihat di bawah ini:

Gambar 12 : Tampilan Layar *Form Retrieve File*

Gambar13 : Tampilan LayarPesan Dialog*Retrieve File*

Tampilan Layar *Form About*

Pada menu ini *user* dapat mengetahui sekilas tentang program aplikasi steganografi ini.Tampilan program form *About* dapat dilihat di bawah ini:

Gambar 14 : Tampilan Layar Pesan *Form About*

Tampilan Layar *Form Help*

Pada menu ini *user* diberikan penjelasan/panduan mengenai tata cara menjalankan program ini, sehingga lebih mudah ketika dijalankan.

Gambar 15 :Tampilan Layar *Form Help*

Experimental Result

Evaluasi program merupakan salah satu hal yang perlu dilakukan dalam setiap pengembangan aplikasi guna menganalisa dan mengetahui hasil yang telah dicapai oleh aplikasi yang dikembangkan tersebut. Demikian juga pada aplikasi steganografi yang dikembangkan ini, maka dilakukan evaluasi program untuk menganalisa hasil yang dicapai pada aplikasi ini. Dan dalam evaluasi tersebut ditemukan beberapa kelebihan dan kekurangan program yang dilihat dari beberapa kondisi dan situasi. Adapun kelebihan dan kekurangan pada aplikasi yang dikembangkan adalah sebagai berikut:

a. Kelebihan Program:
   1) Perbandingan waktu dalam untuk tehnik EOF lebih cepat dibanging tehnik lain.
   2) File citra yang dihasilkan dari aplikasi dengan tehnik EOF ini menghasilkan file yang relatif kecil dibanding tehnik steganografi lain.
   3) Program dapat dengan mudah dioperasikan oleh admin, karena memiliki user interface (tampilan antar muka) yang baik dan user friendly.
   4) Dapat dioperasikan di komputer yang memiliki spesifikasi rendah karena program aplikasi ringan ketika dijalankan.
   5) Tidak memerlukan databases.
   6) Integritas data dari file yang disisipi tetap dapat terjaga.

b.Kekurangan Program:
   1) Aplikasi ini tidak dapat menerjemahkan isi file citra digital yang telah dilakukan suatu perubahan yang disebabkan oleh pihak lain, seperti proses editing oleh perangkat lunak, cropping, maupun resizing image.
   2) File yang bisa disisipkan hanya berupa file citra digital.
   3) Media file yang telah disisipi pesan maupun file citra, ukuran file akan menjadi lebih besar.
   4) Ukuran file citra yang dihasilkan dari aplikasi ini masih relatif besar.

Comparison

Setelah aplikasi ini selesai dibuat, dilakukan ujicoba terhadap penyisipan file gambar untuk

membandingkan aplikasi steganografi yang dibuat tanpa enkripsi [7] dengan aplikasi yang telah diberi enkripsi ini. Ujicoba dilakukan menggunakan aplikasi winrar.

Pengujian pertama dilakukan pada aplikasi steganografi EOF yang tidak memiliki enkripsi. Setelah file gambar berhasil disisipkan file lain, file gambar tersebut dicoba dibuka dengan menggunakan aplikasi winrar, dan terlihat ada file lain di dalam file gambar tersebut.

Lalu pengujian dilakukan pada aplikasi yang telah dibuat dari penelitian ini. Setelah file gambar berhasil disisipkan file lain, file gambar tersebut dicoba dibuka menggunakan aplikasi winrar, dan ternyata tidak terlihat ada file lain di dalam file gambar tersebut.

Penutup

Berdasarkan analisa yang telah dilakukan terhadap permasalahan-permasalahan yang ditemui, maka dapat ditarik kesimpulan dan saran yang mungkin diperlukan untuk pengembangan sistem ketahap yang lebih kompleks.

Kesimpulan

Adanya progam aplikasi steganografi, proses pertukaran informasi khususnya melalui *email* sehingga desain yang tidak boleh diketahui orang lain menjadi aman.

Terhindar dari tindak pencurian data dan perusahaan tidak mengalami kerugian.

Pada sistem ini, data rahasia akan di*embed*, kemudian hasilnya akan disembunyikan ke dalam suatu *file* gambar citra digital sehingga tidak akan muncul kecurigaan pihak lain dan keamanan dan kerahasiaan pesan tetap terjaga.

Pada metode *End of File*, data yang telah di *embed*akan disisipkan pada nilai akhir *file* gambar, sehingga akan menambah ukuran *file.*

Program ini berhasil menyisipkan dan mengekstraksi pesan rahasia dengan baik karena pesan yang didapatkan isinya sama, tanpa ada perubahan dengan pesan yang disisipkan.

Besar ukuran berkas hasil steganografi adalah hasil penambahan besar ukuran berkas pesan rahasia dengan ukuran berkas penampung.

Saran

Selain menarik beberapa kesimpulan, ada beberapa saran-saran yang mungkin bisa dijadikan pertimbangan dalam pengembangan sistem, antara lain :

Sistem ini dapat dikembangkan lebih lanjut dengan menambahkan pilihan *file* gambar berformat lain sebagai medianya, seperti format wav, Mp3, mkv, dan lain-lain.

Perlunya perbaikan program aplikasi, dengan menambahkan kompresi, sehingga pesan yang disampaikan bisa diatur ukurannya.

Menghilangkan tanda-tanda yang mencurigakan terhadap *file* hasil steganografi, seperti pada saat *file* dilihat dari *properties* nya.

Daftar Pustaka:

[1] Ariyus, Dony., 2006, Keamanan Multimedia. Yogyakarta: Penerbit ANDI.

[2] Jok, Rival., Steganografi dengan metode End of File. http://www.cenadep.org/2012/05/18 /steganography-dengan-metode-eof/ (diakses 20 Mei 2013).

[3] Sejati, Adiputra. , 2007, Studi dan Perbandingan Steganografi Metode EOF(End of File) dengan DCS(Dynamic Cell Spreading), Bandung.

[4] Menezes, J. Alfred, Paul C. Van Oorschot, Scott A.Vanstone. 1996. Handbook of Applied Cryptography. CRC Press.

[5] NIST. 2004. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, (online).

[6] Hardjianto, Mardi, Materi Perkuliahan Security Computer – Cryptography, Pasca Sarjana Universitas Budi Luhur Jakarta.

[7] Faruq, Ahmad, 2013, Implementasi Sistem Keamanan Data Dengan Menggunakan Tehnik Steganografi Metode End Of File(EOF) Berbasis Java Programing, Universitas Budi Luhur Jakarta.

[8] B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design," *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), Springer-Verlag, 1996, pp. 121-144.

[9] Provos, Neils, & Honeyman, Peter. (2003), “Hide and Seek: An Introduction to Steganography” IEEE Security and Privacy, May/June 2003; IEEE Computer Society.