Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018
SENSITEK 2018
STMIK Pontianak, 12 Juli 2018

Penerapan Metode End Of File Terhadap Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar

Risang Nur Bagas Barakaallah[1)], **Irfan Suparman Putra**[2),] **Sandi Supriansah**[3)]

Mahasiswa Jurusan Teknik Informatika STMIK PONTIANAK[1, 2, 3)]
Jl. Merdeka Barat No.374, Tengah, Pontianak Kota, Tengah, Pontianak Kota, Kota Pontianak,
Kalimantan Barat 78116, Indonesia
Telp. (0561) 735555, web www.stmikpontianak.ac.id
e-mail: risangbara@gmail.com

Abstrak

Steganografi merupakan ilmu dan seni yang mempelajari cara penyembunyian informasi pada suatu media sedemikian rupa sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Pengguna pertama (pengirim pesan) dapat mengirim media yang telah disisipi informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh pengguna kedua (penerima pesan).Penerima pesan dapat mengekstraksi informasi rahasia yang ada di dalamnya. Pengiriman pesan untuk menyampaikan informasi sering dilakukan oleh banyak manusia dalam kemajuan teknologi saat ini. Sehingga penelitian ini dilakukan untuk menghindari terjadinya pencurian maupun sabotase informasi pesan yang dilakukan antara dua belah pihak dan tidak terbaca oleh orang yang tidak diinginkan. Metode end of file dapat dijadikan salah satu media transmisi untuk menyembunyikan informasi rahasia berupa pesan teks. Karakteristik metode end of file yang mampu penampung lebih banyak data atau pesan sehingga memungkinkan dapat menyisipkan lebih banyak pesan yang akan disisipkan..Tapi akan akan tetap ditentukan ukuran panjang pesan ynag akan disisipkan agar tidak mempengaruhi ukuran atau citra penampung yaitu image(citra) tersebut.

Kata kunci: *End of File, Steganografi, Citra*

1. Pendahuluan

Perkembangan dunia teknologi informasi yang sangat pesat akhir-akhir ini berpengaruh dalam segala aspek kehidupan. Salah satunya yaitu dalam pengamanan informasi yang bersifat rahasia. Kerahasiaan informasi merupakan suatu aspek yang penting. Informasi yang sifatnya rahasia perlu disembunyikan agar tidak diketahui olehorang yang tidak berhak.
Steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan atau data rahasia didalam suatu media penampungnya sehingga orang lain tidak menyadari adanya pesan didalam media tersebut. Dalam bidang keamanan komputer, steganografi digunakan untuk menyembunyikan data rahasia.
Ada dua buah proses dalam steganografi yakni proses penyisipan pesan dan proses ekstraksi pesan. Proses penyisipan pesan membutuhkan masukan media penyisipan, pesan yang akan disisipkan dan kunci. Keluaran dari proses penyisipan ini adalah media yang telah berisi pesan. Proses ekstraksi pesan membutuhkan masukan media yang telah berisi pesan. Keluaran dari proses ekstraksi pesan adalah pesan yang telah disisipkan. Metode *End Of File* ini mempunyai kelebihan dapat menyembunyikan pesan dalam jumlah yang tidak terbatas dan pesan yag akan disisipkan ditempatkan diakhir file citra.

Steganografi berasal dari bahasa Yunani yaitu stegos yang berarti penyamaran dan graphia yang berarti tulisan. Steganografi digunakan untuk menyembunyikan informasi rahasia ke dalam suatu media sehingga keberadaan pesan tersebut tidak diketahui oleh orang lain.Steganografi bertujuan untuk menghilangkan kecurigaan dengan cara enyamarkan pesan tersebut. Menurut (Rinaldi, 2006),[6] ada beberapa hal yang diperlukan untuk menyembunyikan pesan yaitu:
1. Algoritma Penyisipan (Embeding Algorithm). Algoritma ini digunakan untuk menyisipkan suatu pesan yang disembunyikan ke dalam suatu data yang akan dikirim. Proses penyisipan ini diproteksi oleh sebuah key-word sehingga hanya orang-orang yang mengetahui key-word ini yang dapat membaca pesan yang disembunyikan tersebut.
2. Fungsi Detektor (Detector Function). Fungsi Detektor ini adalah untuk mengembalikan pesan-pesan yang disembunyikan tersebut.
3. Carrier Document. Merupakan dokumen yang berfungsi sebagai media yang digunakan untuk menyisipkan informasi. Dokumen ini dapat berupa file-file seperti file audio,video atau citra(gambar).
4. Key. Merupakan kata kunci yang ikut disisipkan kedalam dokumen berguna dan dipakai sebagai proses verifikasi sewaktu informasi akan ditampilkan atau diuraikan.
5. Secret Message/ Plaintext. Merupakan pesan rahasia yang akan disisipkan kedalam carrier document. Pesan inilah yang tidak ingin terlihat dan terbaca oleh orang yang tidak berkepentingan.

Iswahyudi, Setyaningsih(2012) meneliti tentang Pengamanan Kunci Enkripsi Citra ada Algoritma Super Enkripsi Menggunakan Metode End Of File. Keamanan informasi menjadi isu yang sangat penting dalam penyimpanan dan transmisi data. Salah satu pengamanan tersebut menggunakan teknik kriptografi yang dimana melakukan penyamaran pesan asli yang akan dikirimkan menjadi pesan yang tidak beraturan atau tidak dapat dimengerti maupun dibaca. Algoritma yang dikembangkan pada penelitian ini menggunakan konsep symmetric cryptosystem yang dimana sangat menekankan pada kerahasiaan unci yang digunakan untuk proses enkripsi dan dekripsi. Sehingga sistem ini sering disebut sebagai secret-key cryptography dimana merupakan bentuk riptografi yang lebih tradisional, sebuah kunci tunggal digunakan untuk proses enkripsi dan dekripsi. Pengirim maupun penerima saling memiliki kunci yang sama, namun masalah utama yang dihadapi adalah bagaimana pengirim dan penerima menyetujui kunci rahasia tanpa ada orang lain yang mengetahuinya. ehingga diusulkan sebuah cara untuk mengoptimalkan keamanan pada kunci yang digunakan. Teknik yang diusulkan adalah mengadopsi dari konsep steganografi menggunakan metode end of file.

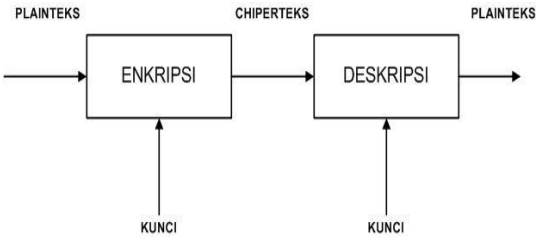
Wasino, Rahayu (2012) meneliti tentang Implementasi Steganografi Teknik End Of File dengan enkripsi Rijndael. Keamanan uatu data yang rahasia merupakan suatu tindakan yang bertujuan untuk mengamankan data tersebut dari gangguan pihak lain yang tidak bertanggung jawab terhadap kerahasiaan data. Sehingga diperlukannya suatu teknik dalam proses pengamanan pesan rahasia saat proses pengiriman pesan tersebut sesuai tujuan. Teknik steganografi sangat sesuai dalam melakukan pengamanan pesan dengan menggunakan algoritma End Of File yang merupakan suatu teknik dengan cara menambahkan data atau pesan rahasia pada akhir file dan pesan yang akan disisipkan tidak terbatas sesuai keinginan namun disesuaikan dengan media penampung sehingga tidak mengalami perubahan ukuran citra penampung yang sangat signifikan dan dapat memberikan kecurigaan bagi pihak ketiga. Kemudian pesan yang akan disisipkan nanti akan dilakukan proses enkripsi yaitu teknik kriptografi, hal ini dilakukan untuk menambah pengaman data dengan menggunakan algoritma Rijndael.

Rumusan Masalah

1. Bagaimana menyisipkan pesan teks pada gambar?
2. Bagaimana menerapkan metode end of file untuk menyisipkan pesan teks kedalam gambar?
3. Bagaimana merancang aplikasi steganografi untuk menyisipkan pesan teks ke dalam gambar?

2. Pembahasan

Secara umum program steganografi ini mempunyai fungsi untuk menyembunyikan informasi berupa pesan teks dibalik data citra, Dalam hal ini media yang digunakan adalah citra digital dan harus menjadi perhatian bahwa dalam proses modifikasi media penampung tidak boleh terlalu mencolok atau dengan kata lai secara kasat mata, perubahan pada citra penampung yang telah termodifikasi tidak terlalu terlihat,agar suatu kerahasiann dari informasi yang ada dalam file citra digital tetap terjaga (integrity). Tanpa key ini orang yang tidak mengetahui kuncinya, tidak akan bisa membuka dan mengambil informasi yang terkandung dalam image penampung. Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia didalam suatu informasi lainya (Ariyus, 2008).



Gambar 1. Skema Proses Enkripsi dan Deskripsi

Metode End Of File merupakan salah satu teknik yang menyisipkan pesan pada akhir file dan pengembangan dari pada metode LSB. Adapun langkah-langkah encoding menggunakan metode End of File adalah sebagai berikut :

1. Proses encoding dimulai dengan pesan yang akan disisipkan. Pesan diubah kedalam bentuk biner dengan representasi 1 atau 0.
2. Kemudian disisipkan angka 1 didepan rangkaian biner tersebut.langkah selanjutnya rangkaian biner tersebut dikonversikan menjadi bilangan decimal dan menghasilkan sebuah bilangan yang dinamakan dengan m
3. Menghitung jumlah warna yang terdapat pada berkas RGB yang menjadi objek steganografi.dan akan menghasilkan sebuah bilangan.Bilangan tesebut dinamakan dengan n, maka apabila m>n!-1 maka pesan yang akan disisipkan berukuran terlalu besar sehingga proses penyisipan tidak dapat dilakukan.
4. Warna dalam palet warna diurutkan sesuai dengan urutan yang “natural”.Setiap warna dengan format RGB dikonversikan kedalam bilangan integer dengan aturan (Merah * 5536 + Hijau * 256 + Biru). Kemudian diurutkan berdasarkan besar bilangan integer yang mewakili warna tersebut.

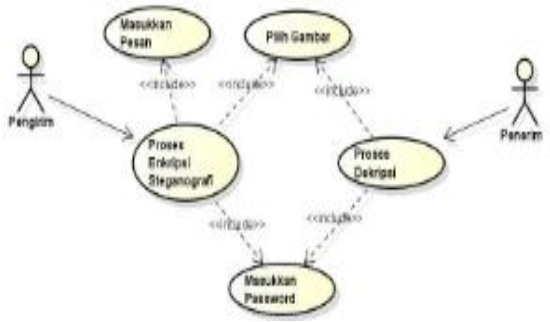
5 Setelah itu lakukan proses iterasi terhadap variable i dengan nilai i adalah dari 1 sampai n. Setiap warna dengan urutan n – i dipindahkan ke posisi baru yaitu m mod i , kemudian m dibagi dengan i.

6. Kemudian palet warna yang baru hasil iterasi pada langkah ke – 4 dimasukkan kedalm palet warna berkas

RGB. Apabila ada tempat yang diisi oleh dua buah warna, maka warna sebelumnya yang menempati tempat tesebut akan digeser satu tempat ke samping.
7. Apabila ternyata besar dari palet warna yang baru lebih kecil dari 256 maka palet warna akan diisi dengan warna terakhir dari palet warna sebelumnya.
8. Kemudian berkas RGB akan dikompresi ulang dengan palet warna yang baru, untuk menghasilkan berkas yang baru dengan ukuran dan gambar yang sama, namun telah disisipi pesan.

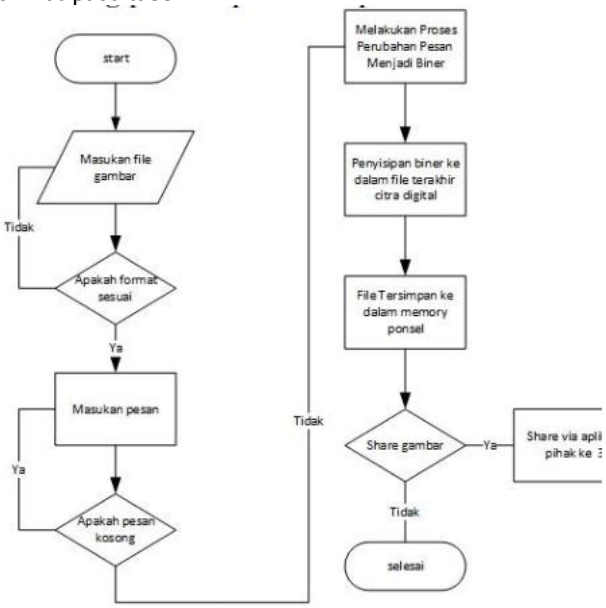
Adapun langkah - langkah proses *decoding* atau mengekstrak pesan dari citra RGB yang telah disisipi pesan dengan metode *End Of File* adalah sebagai berikut:
1. Masukkan nomor sesuai dengan posisi setiap warna pada palet warna citra RGB yang telah disisipkan pesan
2. Warna diurutkan berdasarkan konversi RGB ke nilai integer dengan rumus: (Merah * 65536 + Hijau * 256 + Biru).
3. *m* diberi nilai 0
4. Iterasi variabel *i* dari *i+1* sampai *n-1*. m=m*(n-1) + posisi warna ke *i* iterasi variabel *j* dari *i* +1 sampai n-1
jika posisi warna ke *j* > nilai posisi warna ke-i, maka posisi warna ke *i* dikurangkan 15. Setelah nilai *m* diperoleh, maka nilai *m* dikonversikan kebilangan binari untuk memperoleh pesan asli kembali.

Perancangan suatu sistem memerlukan alur proses kerja dari suatu perangkat lunak yang akan dirancang. Perancangan alur tersebut menggunakan Use Case Diagram. Use case diagram merupakan an salah satu diagram dalam bahasa pemodelan UML yang dapat menggambarkan kegiatan yang dilakukan oleh actor secara garis besar, dan hubungan antara actor dengan setiap kegiatan (actor–use case) atau hubungan antara kegiatan (use case–use case). Gambaran atau model dari pembuatan penelitian ini dapat dilihat pada gambar 2.



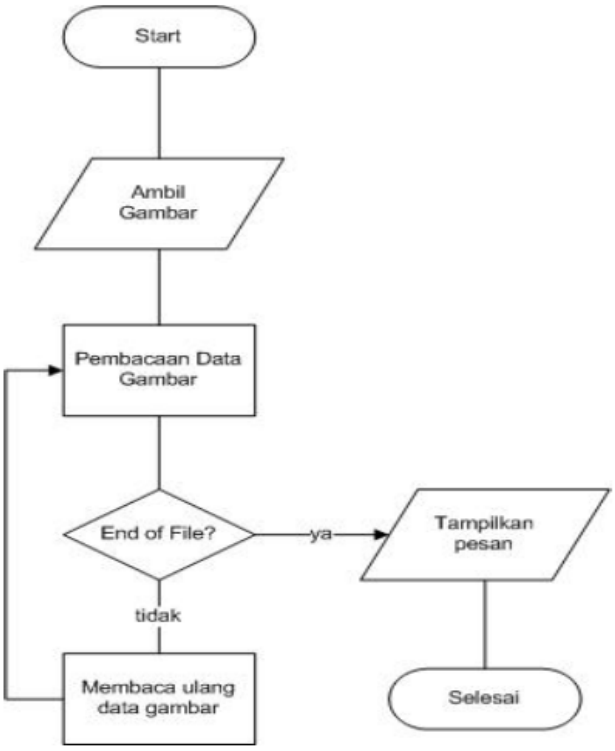
Gambar 2 Usecase Diagram

Perancangan alur proses deskripsi memiliki tahap yang harus digambarkan terlebi dahulu. Perancangan alur tersebut dilakukan dengan membuat flowchart. Pada peroses penyisipan pesan tersebut memiliki tahap enkripsi yang biasa disebut proses *Encoding* pesan. Pada proses *Encoding* pesan dimulai dari menginputkan gambar yang dapat diambil dari kamera secara langsung maupun gambar yang sudah ada pada gallery, kemudian proses *Encoding* dimulai dengan membaca nilai file suatu gambar setelah itu pesan yang akan disisipkan dibaca nilai nya dalam bentuk decimal. Kemudian nilai tersebut dimasukkan diakhir suatu file image tersebut. Hasil output file image disimpan ke lokasi yang telah ditentukan. Flowchart *Encoding* pesan dapat dilihat pada gambar 3 berikut dan proses embedding pesan dapat dilihat pada tabel 1



Gambar 3. Flowchart Encoding Pesan
Tabel 1 Proses Ecoding

Proses selanjutnya dilakukan pada client dengan cara mengekstrakting pesan yang telah dikirim. Pada proses extracting pesan dimulai dari menginputkan gambar hasil steganografi yang dimana diambil nilai derajatnya berupa bilangan decimal, dan mencari nilai akhir sebuah file dimana pesan rahasia dapat dibaca dalam bentuk bilangan decimal setelah itu konversi dalam standar kode ASCII yang menghasilkan pesan yang dapat dibaca oleh penerima. Flowchart ektraksi pesan dapat dilihat pada gambar.



Gambar 4 Flowchart Decoding Pesan

Pengimplementasian dari metode End Of File tersebut dapat diterjemahkan kedalam bahasa pemrograman secara bertahap. Tahapan yang harus diproses kedalam bahasa pemrograman adalah sebagai berikut :

Tahapan Encoding 1)

1. Input pesan = T THEN
   Input kunci = U THEN
   Proses enkripsi = T + U mod 96 = L
2. IF pesan = T THEN Ubah pesan kebiner
3. Sisipkan angka 1 pada rangkaian biner untuk mendapatkan nilai M = 1+ biner AND ubah pesan ke decimal
4. ELSE IF nilai decimal pesan> 6! – 1 THEN Proses penyisipan tidak dapat dilakukan
5. ELSE IF akan diurutkan THEN Dikonversikan kebilangan integer = (merah * 65536 + hijau * 256 + biru) THEN diurutkan berdasarkan nilai integer
6. ELSE IF iterasi variabel *i* = 1 n THEN Warna urutan n – i dipindahkan keposisi baru THEN *m* mod *i*
7. ELSE IF warna indeks = warna indeks sama THEN Warna indeks = bergeser 1 x ke indeks berikutnya THEN Indeks palet warna dimasukkan kecitra RGB
8. Output proses encoding
   Pesan telah disisipkan kedalam berkas RGB = " selesai "

Tahapan yang dilakukan saat decoding :

1. Input proses encoding pesan THEN
   Cari nilai m = dapatkan plantext
2. IF palet warna diketahui THEN
   Diberi nomor sesuai posisinya
3. ELSE IF nilai natural ditampilkan THEN
   Diurutkan = nilai integer terkecil AND m = 0
4. ELSE IF iterasi variabel i dari 0 5 THEN
   m = 0 (6 – 1) + posisike- i AND
   iterasi variabel j dari i + 1 sampai 5
5. ELSE IF nilai warna ke j > nilai posisi warna ke- i THEN
   Posisi warna ke- i - 1
6. Output proses decoding
   Di dapat pesan asli = plantext =" Selesai "

Ketika akan menginputkan Menu utama seperti pada gambar dibuat agar mudah untuk digunakan,form ini dilengkapi tahapan proses pengambilan *gambar* dan menyimpan *gambar*. Disini akan dimulai dengan proses penyisipan pesan (*encoding*). Berikut keterangan dari menu *file* yang terdapat pada menu bar.

3. Kesimpulan

Berdasarkan hasil dari penelitian maka dapat dihasilkan simpulan sebagai berikut :

1. Steganografi dengan menggunakan metode End of File (EOF) dapat menyisipkan informasi kedalam media citra digital pada bagian akhir file gambar
2. Dengan adanya perangkat lunak steganografi yang dikembangkan berdasarkan metode End Of File , maka data-data penting dapat diamankan (dienkripsi).

Daftar Pustaka

[1]. Dewobroto, "Visual Basic 6.0" Penerbit PT.Gramedia Jakarta, Bab 1, Hal 2, 2004.

[2]. D. Darwis, 2015., *Implementasi Steganografi pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding*., Program Studi Ma Magister Ilmu Komputer Universitas Budi Luhur Jakarta. Jurnal Expert. ISSN : 20885555

[3]. Krisnawati, 2008. Metode Least Significant Bit (LSB) dan End Of File (EOF) untuk Menyisipkan Teks Ke Dalam Citra Grayscale. Jurnal UPN "Veteran" Yogyakarta
[4]. O.D. Nurhayati, 2010. Keamanan Multimedia, Program Studi S1 Sistem Komputer: Universitas Diponegoro.
[5]. Y. Aditya, A. Pratama, A. Nurlifa, 2010. Studi Pustaka Untuk Steganografi Dengan Beberapa Metode. Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010). Yogyakarta, 19 Juni 2010. ISSN: 1907-5022.
[6]. S. Sembiring, 2013. Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File. Jurnal Pelita Informatika Budi Darma, volume : iv, nomor:2