Implemantasi steganografi menggunakan metode end of file (EOF) dalam pengamanan data (Studi kasus pada file AVI, MP3, dan JPEG)

Ari Dwi Cahyono[1)] dan Mohamad Yasin[2)]
E-mail: dwica.bond@gmail.com
Universitas Negeri Malang

Abstrak: Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Metode yang digunakan untuk menyembunyikan pesan rahasia adalah metode penyisipan pesan EOF (*End of File*). Steganografi metode *EOF (End of File)* menggunakan cara dengan menyisipkan data pada akhir file. Dalam metode *EOF* data yang disisipkan diberi tanda khusus sebagai pengenal awal dan pengenal akhir data tersebut. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. File hasil steganografi ini secara visual maupun suara tampak tidak berubah dibanding file sebelum disisipi data. Hanya saja ukuran dari file tersebut menjadi lebih besar. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut.

Kata kunci: Steganografi, EOF, Pesan Rahasia, File Media.

Dengan pesatnya perkembangan teknologi, berkembang pula ancaman terhadap keamanan informasi yang dikirimkan, terutama untuk informasi yang dirahasiakan. Keamanan pengiriman informasi dapat dilakukan dengan kriptografi dan enkripsi atau dengan menyembunyikan pesan informasi. Salah satu teknik penyembunyian informasi yang cukup terkenal adalah steganografi. Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui.

Teknologi komputer memberikan kontribusi baru dalam revolusi menyembunyikan pesan. Steganografi pada era informasi digital merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain. File media merupakan komponen penting pada proses penyembunyian informasi ini.

Teknik ini mempunyai beberapa metode yang sering digunakan. Salah satunya adalah *LSB (Least Significant Bit)* dan *EOF (End Of File)*. Teknik steganografi metode *EOF (End of File)* menggunakan cara dengan menyisipkan data pada akhir file. Dalam metode *EOF* data yang disisipkan diberi tanda khusus sebagai pengenal awal dan pengenal akhir data tersebut. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. File hasil steganografi ini secara visual maupun suara tampak tidak berubah dibanding file sebelum disisipi data. Hanya saja ukuran dari file tersebut menjadi lebih besar. Ukuran file yang telah disisipkan data sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam file tersebut.

Informasi adalah pengumpulan atau pengolahan data untuk memberikan pengetahuan atau keterangan (Bruch dan Strater, 1974:23). Secara umum informasi adalah data yang sudah diolah menjadi suatu bentuk lain yang lebih berguna yaitu pengetahuan atau keterangan yang ditujukan bagi penerima dalam

---

1. Ari Dwi Cahyono adalah mahasiswa jurusan Matematika FMIPA Universitas Negeri Malang
2. Mohamad Yasin adalah dosen jurusan Matematika FMIPA Universitas Negeri Malang

pengambilan keputusan, baik masa sekarang atau yang akan datang. Informasi juga bisa disebut sebagai hasil pengolahan atau pemrosesan data.

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi: (Renaldi Munir, 2004 : 209)

- *Fidelity*. Mutu media penampung tidak jauh berubah. Setelah penambahan data rahasia, media hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam media tersebut terdapat data rahasia.
- *Recovery*. Data yang disembunyikan harus dapat diiungkapkan kembali (*reveal*). Karena tujuan stegnografi adalah penyembunyian data, maka sewaktu-waktu data rahasia di dalam media penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

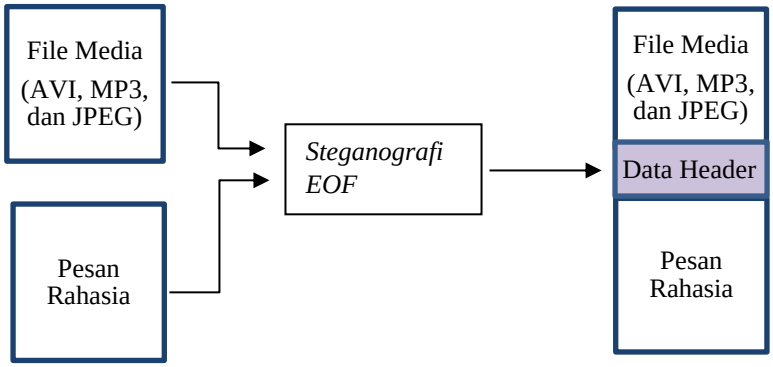
Terdapat beberapa istilah yang berkaitan dengan steganografi. (Renaldi Munir, 2006 : 304)

1. *Hiddentext* atau *embedded message*: pesan atau informasi yang disembunyikan.
2. *Covertext* atau *cover-object*: pesan yang digunakan untuk menyembunyikan *embedded message*.
3. *Stegotext* atau *stego-object*: pesan yang sudah berisi *embedded message*.

Dalam steganografi digital, baik *hiddentext* atau *covertext* dapat berupa teks, audio, gambar, maupun video. Steganografi dengan menggunakan metode *EOF (End of File)* lebih mudah dan efektif digunakan karena tempat penyisipan di akhir file media dan tidak merusak kualitas file media, namun terlihat perbedaan pada ukuran file stego yang dihasilkan, sehingga akan mudah dicurigai apabila ukuran pesan yang akan disisipkan terlalu besar atau lebih besar dari file media yang akan dibuat untuk tempat penyisipan pesan (Krisnawati, 2008:2). Agar kekurangan tersebut dapat tertutupi maka dianjurkan ukuran file pesan proporsional dengan ukuran file media.

PEMBAHASAN

Menurut Rachmawanto (2010) dengan metode *EOF*, secara umum media steganografi (file yang akan disisipi data) memiliki struktur seperti ini:



Gambar 1. Proses Steganografi metode EOF

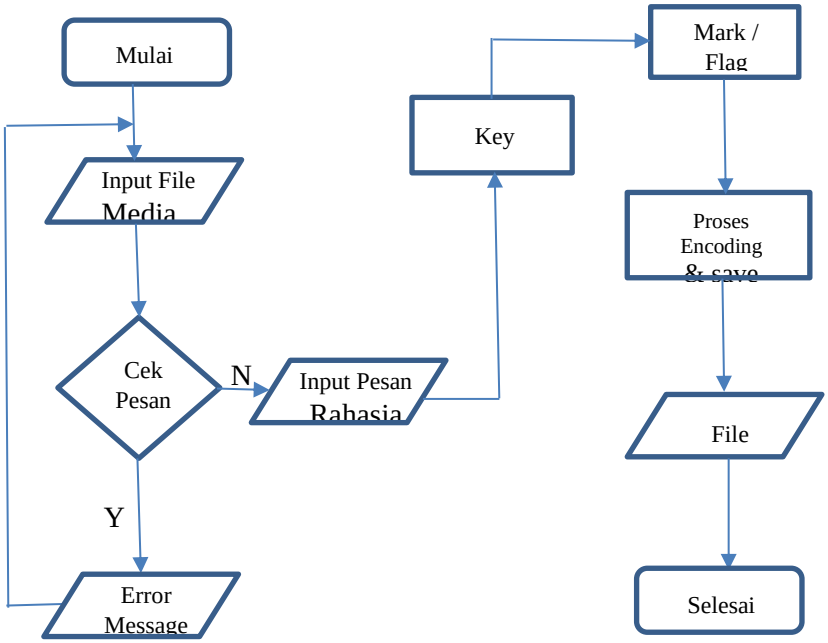
Algoritma proses penyisipan metode *EOF* dapat dituliskan sebagai berikut:

1. Inputkan pesan yang akan disisipkan
2. Ubah pesan menjadi kode desimal
3. Inputkan file media yang akan disisipi pesan
4. Dapatkan kode desimal file media
5. Tambahkan kode desimal pesan sebagai kode desimal diakhir file media
6. Simpan file hasil penyisipan

Algoritma penguraian pesan metode *EOF* dapat dituliskan sebagai berikut:

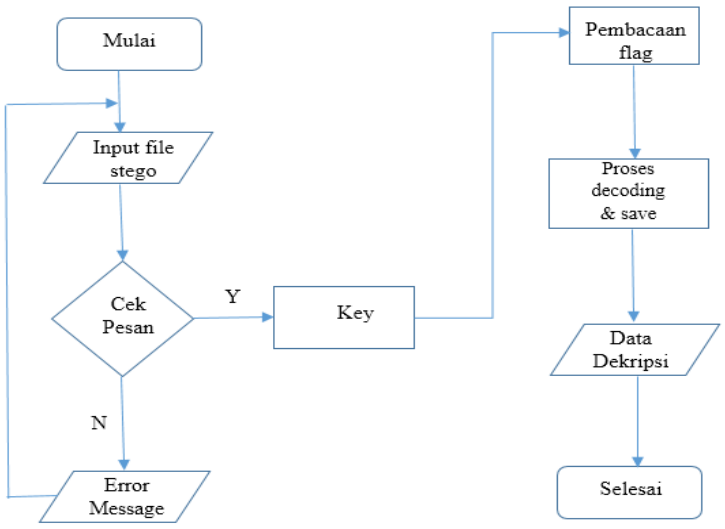
1. Inputkan file media yang sudah mengandung pesan (file stego)
2. Dapatkan penanda pesan rahasia
3. Dapatkan nilai desimal setelah penanda pesan
4. Ubah nilai tersebut menjadi karakter pesan

Proses yang terjadi dalam penyisipan pesan dengan metode *EOF* adalah dengan mendapatkan nilai atau letak piksel terakhir dari file media, berikan sebuah tanda pengenal start dari pesan rahasia dan tambahkan pesan ke file media (Antonio, 2013). Proses penyisipan pesan dengan metode *EOF* dapat dilihat pada Gambar 2.



Gambar 2. Diagram alir penyisipan pesan metode EOF

Proses penguraian pesan dengan metode *EOF* (*End of File*) dapat dilihat pada Gambar 3.3.



Gambar 3. Diagram alir penguraian pesan metode EOF

HASIL IMPLEMENTASI PROGRAM

Dalam program ini akan dijalankan dengan percobaan menggunakan file yang berektensi .avi, .mp3, dan .jpeg. Ketiga tipe file tersebut akan disisipi dengan suatu pesan rahasia yang berupa file txt. Dan file media yang akan digunakan adalah masing-masing :

- File avi : file avi yang digunakan yaitu Detective Conan.avi
- File mp3 : file mp3 yang digunakan yaitu Sheila On 7 - Buat Aku Tersenyum.mp3
- File jpeg : file jpeg yang digunakan yaitu AC-Milan.jpeg

Hasil dari penyisipan proses steganografi dengan metode *EOF* pada file Detective Conan.avi adalah file avi baru (Detective Conan.avi) yang telah disisipi file TXT pesan rahasia. Ukuran file setelah disisipi pesan rahasia sedikit lebih besar, yaitu 233 MB (244.971.516 bytes) dibanding ukuran file aslinya yaitu 233 MB (244.970.800 bytes). Meskipun terdapat perbedaan ukuran file tetapi secara kasat mata tidak terlalu mencolok untuk dilihat, sebab dalam perancangan program ini penulis sudah memberi batasan-batasan untuk tipe dan ukuran file yang akan dioperasikan. Sehingga kualitas file video setelah mengalami proses penyisipan file pesan rahasia tidak mengalami perubahan dibanding file sebelumnya.

Kita dapat melihat contoh perubahan byte sebelum dan sesudah disisipi file txt, seperti pada tabel berikut :

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
0e99f400	30	30	64	63	00	00	00	00	1c	34	88	0e	07	00	00	00
0e99f410	30	31	77	62	10	00	00	00	2c	34	88	0e	9b	02	00	00
0e99f420	30	30	64	63	00	00	00	00	d0	36	88	0e	92	0a	00	00
0e99f430	30	31	77	62	10	00	00	00	6a	41	88	0e	9b	02	00	00
0e99f440	30	30	64	63	00	00	00	00	0e	44	88	0e	17	01	00	00
0e99f450	30	31	77	62	10	00	00	00	2e	45	88	0e	9c	02	00	00
0e99f460	30	30	64	63	00	00	00	00	d2	47	88	0e	07	00	00	00
0e99f470	30	31	77	62	10	00	00	00	e2	47	88	0e	07	00	00	00
0e99f480	30	30	64	63	00	00	00	00	f2	47	88	0e	e6	0c	00	00
0e99f490	30	30	64	63	00	00	00	00	e0	54	88	0e	13	01	00	00
0e99f4a0	30	30	64	63	00	00	00	00	fc	55	88	0e	07	00	00	00
0e99f4b0	30	30	64	63	00	00	00	00	0c	56	88	0e	68	16	00	00
0e99f4c0	30	30	64	63	00	00	00	00	7c	6c	88	0e	99	01	00	00
0e99f4d0	30	30	64	63	00	00	00	00	1e	6e	88	0e	07	00	00	00
0e99f4e0	30	30	64	63	00	00	00	00	2e	6e	88	0e	56	05	00	00
0e99f4f0	30	30	64	63	00	00	00	00	8c	73	88	0e	c4	00	00	00
0e99f500	30	30	64	63	00	00	00	00	58	74	88	0e	07	00	00	00
0e99f510	30	30	64	63	00	00	00	00	68	74	88	0e	0b	13	00	00
0e99f52f	30	30	64	63	00	00	00	00	7c	87	88	0e	fc	01	00	00
0e99f530	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..
0e99f540	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..

Gambar 4. Byte File Sebelum Disisipi Pesan

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
0e99f400	30	30	64	63	00	00	00	00	1c	34	88	0e	07	00	00	00
0e99f410	30	31	77	62	10	00	00	00	2c	34	88	0e	9b	02	00	00
0e99f420	30	30	64	63	00	00	00	00	d0	36	88	0e	92	0a	00	00
0e99f430	30	31	77	62	10	00	00	00	6a	41	88	0e	9b	02	00	00
0e99f440	30	30	64	63	00	00	00	00	0e	44	88	0e	17	01	00	00
0e99f450	30	31	77	62	10	00	00	00	2e	45	88	0e	9c	02	00	00
0e99f460	30	30	64	63	00	00	00	00	d2	47	88	0e	07	00	00	00
0e99f470	30	31	77	62	10	00	00	00	e2	47	88	0e	07	00	00	00
0e99f480	30	30	64	63	00	00	00	00	f2	47	88	0e	e6	0c	00	00
0e99f490	30	30	64	63	00	00	00	00	e0	54	88	0e	13	01	00	00
0e99f4a0	30	30	64	63	00	00	00	00	fc	55	88	0e	07	00	00	00
0e99f4b0	30	30	64	63	00	00	00	00	0c	56	88	0e	68	16	00	00
0e99f4c0	30	30	64	63	00	00	00	00	7c	6c	88	0e	99	01	00	00
0e99f4d0	30	30	64	63	00	00	00	00	1e	6e	88	0e	07	00	00	00
0e99f4e0	30	30	64	63	00	00	00	00	2e	6e	88	0e	56	05	00	00
0e99f4f0	30	30	64	63	00	00	00	00	8c	73	88	0e	c4	00	00	00
0e99f500	30	30	64	63	00	00	00	00	58	74	88	0e	07	00	00	00
0e99f510	30	30	64	63	00	00	00	00	68	74	88	0e	0b	13	00	00
0e99f520	30	30	64	63	00	00	00	00	7c	87	88	0e	fc	01	00	00
0e99f530	05	31	32	33	34	35	00	00	00	00	00	00	00	00	00	00
0e99f54f	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0e99f550	5c	f5	99	0e	94	02	00	00	4e	00	00	00	4a	41	4d	41
0e99f560	4e	20	45	44	41	4e	0d	0a	0d	0a	0d	0a	50	61	6e	63
0e99f570	65	6e	20	61	6d	65	6e	61	6e	67	69	20	6a	61	6d	61
0e99f580	6e	20	65	64	61	6e	2c	0d	0a	73	69	6e	67	20	6f	72

Gambar 5. Byte File Sesudah Disisipi Pesan

Pada proses *decoding* ini akan diuraikan file stego (file media yang telah tersisipi pesan rahasia) Detective Conan.avi sebagai inputan. Sebelumnya pilih terlebih dahulu tab *decoding* pada program. Setelah proses *decoding* telah dilakukan dan berhasil, maka file txt tersebut dapat dibaca pada lokasi folder yang telah ditentukan sebelumnya.

ANALISIS PROGRAM

Program yang dibuat adalah dengan menggunakan metode steganografi *end of file*. Tehnik ini menggunakan tanda pengenal untuk memisahkan awal dan akhir file yang akan disisipkan. Hasil proses penyisipan pesan adalah file media

dalam pembahasan ini menggunakan file bertipe avi, mp3, dan jpeg yang telah tersisipi pesan rahasia bertipe teks (txt).

Kualitas file hasil sisipan pesan rahasia akan tampak mirip dari segi tampilan, suara, ataupun video dari file aslinya. Hanya saja apabila lebih detail diteliti lagi akan terlihat perbedaan pada sisi ukuran file sebelum dan sesudah disisipi pesan rahasia. Oleh karenanya penulis memberi batasan-batasan file yang akan digunakan dalam proses penyisipan. Dengan memanfaatkan kelemahan manusia dalam menganalisa secara detail, tidak akan tampak secara kasat mata kekurangan program dengan metode ini. Karena file sisipan yang digunakan bertipe teks (txt) yang mempunya ukuran file relatif kecil dan file media yang digunakan berukuran proporsional dengan ukuran pesan rahasia yang akan disisipkan.

KESIMPULAN DAN SARAN

Kesimpulan

Steganografi merupakan teknik penyembunyian pesan rahasia dengan menyisipkan pesan rahasia pada media lain sebagai pengalih perhatian. Secara garis besar aplikasi program Steganografi adalah aplikasi untuk menyembunyikan pesan yang berupa *cover-text* ke dalam file media yang bertipe avi, mp3, dan jpeg (*encoding*) dan proses pengekstrakan atau mendekripsi pesan rahasia yang berupa *cover-text.* Berdasarkan aplikasi yang dibuat dan uji coba yang telah dilakukan dapat ditarik kesimpulan sebagai berikut :

1. Pesan rahasia berupa teks disembunyikan ke dalam file media avi, mp3, dan jpeg dengan menggunakan proses steganografi metode *End of File (EOF)* dan menghasilkan file stego yang berupa file avi, mp3, dan jpeg yang telah berisi pesan rahasia di dalamnya.
2. *Decoding* yaitu proses pengambilan atau penguraian pesan rahasia dengan cara mengambil pesan rahasia yang berupa teks dari file stego.
3. Aplikasi steganografi dapat meningkatkan keamanan pesan rahasia dengan cara menyembunyikan pesan rahasia tersebut ke dalam file lain sebagai pengalih perhatian.

Proses *encoding* dan *decoding* dalam aplikasi dibuat secara sederhana dan mudah untuk dioperasikan.

Saran

Selain kelebihan-kelebihan dari aplikasi yang telah dibuat dan diuji cobakan, program ini juga masih mempunyai kelemahan, salah satunya adalah besar file pesan rahasia yang berukuran kecil. Beberapa saran sebagai pengembangan dan perbaikan aplikasi yang telah dibuat dalam skripsi ini diantaranya adalah :

1. File pesan rahasia hendaknya bisa berukuran besar sehingga pesan rahasia yang dikirimkan bisa lebih banyak.
2. File pesan rahasia hendaknya tidak hanya berbentuk teks. Sebagai contoh file audio, image, atau video.
3. Pada aplikasi yang dibuat tidak adanya operasi untuk memainkan atau membuka file hasil steganografi.
4. File hasil steganografi tidak dapat diekstrak atau diuraikan apabila terjadi pengubahan ukuran atau pemotongan file media hasil steganografi.

DAFTAR PUSTAKA

Bruch dan Strater. 1974. *Information System : Theory and Practice*, California : Hamilton Publishing Company.

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

Munir, Rinaldi. 2006. *Steganografi*. Informatika: Bandung

Qureshi, Waheed. 2000, *Steganography and Steganalysis.* (Online), www.giac.org/paper/gsec/2151/steganography-steganalysis/103664. Tanggal akses 29-11-2013.