Layanan Steganografi dengan Metode End ff File untuk Pengamanan Pesan Elektronik

Faiz Muqorrir Kaffah
faiz@uninus.ac.id

Abstract

Desktop-based applications are still widely used for users in their daily work. Because computer users who want to secure files and send them to others use the file delivery facility on email, but not all file files can be sent via mail including system files with the format .ade, .adp, .bat, .chm, .cmd, .com , .cpl, .exe, .hta, .ins, .isp, .jar, .jse, .lib, .lnk, .mde, .msc, .msp, .mst, .pif, .scr, .sct, . shb, .sys, .vb, .vbe, .vbs, .vxd, .wsc, .wsf, .wsh. With steganography using the end of file algorithm, the file system insertion is carried out so that it can send system files on sending mail files. Therefore, the end of file algorithm is the choice in helping the optimization of system file insertion. Based on the tests carried out, the application can insert a system file that is blocked by mail to the cover file in the form of an image, without changing the physical appearance of the cover image file or the system file that is inserted, so that system files can be sent via file delivery in mail. Then the election results can be used as a reference and direction to users in sending files to mail in the form of system files without any rejection of blocked files.

Keyword: Steganografi, End of file, Penyisipan, File, Mail

Pendahuluan

Dengan perkembangan teknologi terutama dibidang internet, maka berkembang pula kebutuhan manusia terutama kebutuhan akan informasi. Berbagai ancaman dalam dunia maya seperti hacker, cracker, carder membuat orang khawatir akan keamanan informasi yang dikirimnya[1]. Oleh karena itu maka diperlukanlah sesuatu pengamanan data yang akan menjamin keamanan dan keutuhan data ketika data tersebut dikirim maupun diterima. salah satu teknologi internet yang paling sering digunakan yaitu pada layanan surat electronik atau biasa yang kita kenal dengan sebutan email. salah satunya mail yang merupakan salah satu layanan surat elektronik gratis buatan dari google dengan layanan surat elektronik berbasis web terbesar dengan 425 juta pengguna aktif di seluruh dunia[2].

File-File yang dikirim melalui pesan mail terkadang tidak semua jenis file dapat dikirim dikarnakan dari pihak mailnya ada beberapa jenis file yang dilarang dalam

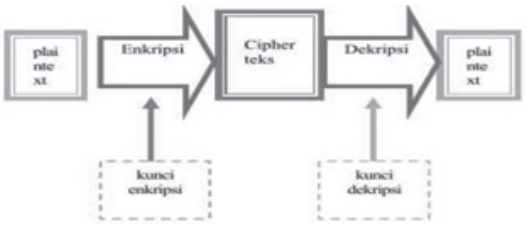
mengirim atau menerima jenis file berikut .ade, .adp, .bat, .chm, .cmd, .com, .cpl, .exe, .hta, .ins, .isp, .jar, .jse, .lib, .ink, .mde, .msc, .msp, .mst, .pif, .scr, .sct, .shb, .sys, .vb, .vbe, .vbs, .vxd, .wsc, .wsf, .wsh.. Pesan berisi jenis file tersebut akan dikembalikan ke pengirim secara otomatis. Mmail tidak akan menerima jenis file tersebut walau dikirim dalam bentuk zip. Sebagai langkah pengamanan guna mencegah kemungkinan terkena virus, mail tidak mengizinkan mengirim atau menerima file berisi program. File semacam itu bisa berisi kode berbahaya yang dapat mengunduh perangkat lunak berbahaya ke komputer. Selain itu,mail tidak mengizinkan untuk mengirim atau menerima file rusak, yaitu file yang tidak berfungsi dengan baik [3].

Teknik EOF atau End Of File merupakan salah satu metode yang dapat diimplementasikan dalam steganografi. Metode ini digunakan dengan cara menambahkan data atau pesan rahasia pada akhir file[4]. Sehingga menghasilkan aplikasi yang dapat menyembunyikan file dengan baik dan menutup kecurigaan dari pihak mail.

Tinjauan Teori

Steganografi

Steganografi merupakan salah satu teknik yang sampai saat ini masih digunakan untuk mengamankan informasi. Adapun jenis-jenis steganografi yang dikategorikan berdasarkan ketidaknampakannya yaitu invisibile dan visible, sedangkan dari media yang digunakan, steganografi dapat dibedakan menjadi 6 yaitu antara lain teks steganografi, image steganografi, audio steganorafi, video steganografi, dan protocol steganografi[4]. Berikut merupakan bagan proses steganografi secara umum.



Gambar 1. Proses Steganografi [5]

Steganografi berasal dari Bahasa yunani, yaitu *steganos* yang artinya tulisan tersembunyi *covered writing*. Steganografi sangat kontras dengan kriptografi. Jika kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, maka steganografi menutupi keberadaan pesan. Steganografi dapat dipandang sebagai kelanjutan kriptografi dan dalam prakteknya pesan rahasia dienkripsi terlebih dahulu, kemudian cipherteks disembunyikan didalam media lain sehingga pihak ketiga tidak menyadari keberadaan. Pesan rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti aslinya.[5]

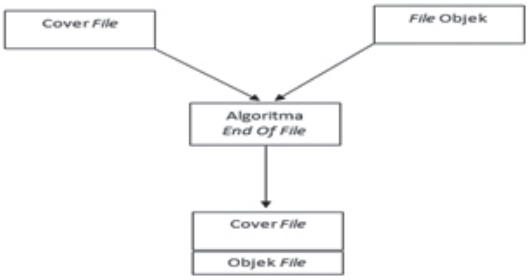
Steganografi membutuhkan dua property yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa sebuah artikel, gambar, daftar barang, kode program, atau pesan lain.[6]

Keuntungan Steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan bagi pihak ketiga. Ini berbeda dengan kriptografi dimana sphersteks menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia [6].

Algoritma End of File

Metode EOF merupakan sebuah metode yang diadaptasi dari metode penanda akhir file (*end of file*) yang digunakan oleh sistem operasi windows. 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[3]. Secara umum media steganografi (file yang akan disisipi data) memiliki struktur.



Gambar 2. Proses steganografi End Of File

File

Kata *file* diambil dari bahasa Inggris yang artinya data atau berkas, namun lebih spesifiknya file adalah kumpulan bermacam-macam informasi yang berhubungan dan juga tersimpan di dalam *secondary storage*. Secara konsep file mempunyai beberapa tipe, tipe tersebut ada yang berupa data dari *numeric*, *character* dan *binary*. Namun ada juga file yang bertipe program.

Biasanya, suatu file yang berada dalam komputer disimpan didalam suatu folder. Masing-masing file mempunyai ekstensinya sendiri-sendiri tergantung dari jenis file tersebut. Ekstensi file merupakan tanda yang membedakan jenis-jenis dari sebuah file. Berikut contoh dan jenis file beserta ekstensinya[7]:

1. System: com, sys, tmp, bak, bat, dan exe.
2. Video: mpeg, mpg, 3gp, avi, dan fly.
3. Dokumen: doc, odt, xls, ods, pdf, dan html.
4. Suara: mp3, midi, rm, dan wav.
5. Gambar : gif, jpg, jpeg, png, tif, dan tiff.

E-mail

Electronic mail (surat elektronik), sering disebut e-mail atau email, merupakan metode Store and Forward dari menulis, mengirim, menerima dan menyimpan surat melalui sebuah sistem komunikasi elektronik[8].

E-mail mengawali sejarah Internet, bahkan merupakan komponen penting dalam perkembangan internet. 1961 MIT mendemonstrasikan *Compatible Time-Sharing System* (CTSS). *Multiple user login* ke IBM 7094 dari terminal dial-up, dan menyimpan file secara online ke disk. Memberikan bentuk baru untuk user dalam berbagi informasi. 1965 *multiple user* dari *time-sharing mainframe computer* dapat saling berkomunikasi. 1966 E-mail berkembang cepat menjadi network e-mail, mengizinkan user saling bertukar surat antar komputer yang berbeda. 1969 Jaringan komputer ARPANET memberikan kontribusi terhadap pengembangan e-mail. (Transfer antar system email yang sukses). 1971 Ray Tomlinson memperkenalkan penggunaan tanda @ untuk memisahkan nama user dan komputer. ARPANET secara signifika meningkatkan popularitas dari e-mail, dan membuatnya menjadi killer app dari ARPANET.Format E-mail e-mail terdiri dari dua bagian besar:

- *Header* — Terstruktur menjadi beberapa fields seperti summary, sender, receiver, dan informasi lain mengenai e-mail tersebut.
- *Body* — isi surat sebagai teks yang tak terstruktur, juga berisi signature block di akhir Header dipisahkan dari Body dengan sebuah Email baris kosong[8].

Metode Pengembangan Sistem

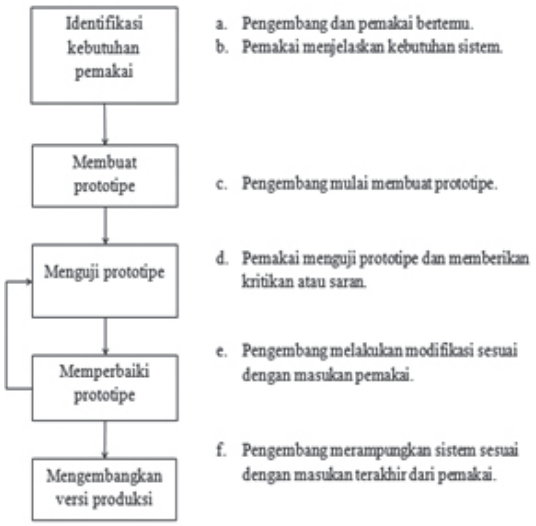
Untuk menyelesaikan masalah yang dihadapi, pengembangan sistem yang

akan dirancang berupa model prototipe, yang merupakan suatu metode dalam pengembangan sistem yang menggunakan pendekatan untuk membuat sesuatu program dengan cepat dan bertahap sehingga segera dapat dievaluasi oleh pemakai. Secara garis besar, sasaran prototipe adalah sebagai berikut[9]:

1. Mengurangi waktu sebelum pemakai melihat sesuatu yang konkret dari usaha pengembangan sistem.
2. Menyediakan umpan balik yang cepat dari pemakai kepada pengembang.
3. Membantu menggambarkan kebutuhan pemakai dengan kesalahan yang lebih sedikit.
4. Meningkatkan pemahaman pengembang dan pemakai terhadap sasaran yang seharusnya dicapai oleh sistem.
5. Menjadikan keterlibatan pemakai sangat berarti dalam analisis dan desain sistem.

Tahapan analisis kebutuhan ini merupakan tahapan yang dilakukan untuk menganalisa sistem secara lebih detail baik proses, prosedur dan fungsi sesuai dengan data-data yang telah dikumpulkan, analisa sistem terbagi dalam beberapa tahapan yaitu:

1. Analisa Requirement sistem, tahapan dimana kebutuhan (*requirement*) kebutuhan sistem didefinisikan sesuai data-data fungsi dan proses yang terjadi pada sistem sebelumnya.
2. Analisa Proses, tahapan ini dilakukan untuk menganalisa proses-proses detail yang terjadi sesuai dengan transaksi update dan delete.
3. Analisa Data, tahapan ini merupakan tahapan untuk menganalisa data-data berupa report, dokumen, memo, rekap yang berhubungan dengan flow ataupun transaksi proses yang terjadi pada kegiatan. Sistem metode perancangan yang digunakan ialah metode terstuktur.
4. Analisa Modul Sistem, tahapan ini dilakukan setelah tahapan sebelumnya selesai dilakukan.



Gambar 3. Mekanisme pengembangan sistem dengan prototipe.

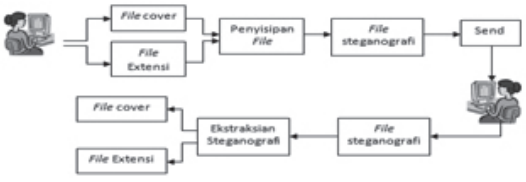
Analisa Modul Sistem ini, dilakukan analisa pembagian terhadap modul-modul dan sub-modul yang menggunakan proses dan data yang telah didefinisikan sebelumnya.

Metode Penelitian

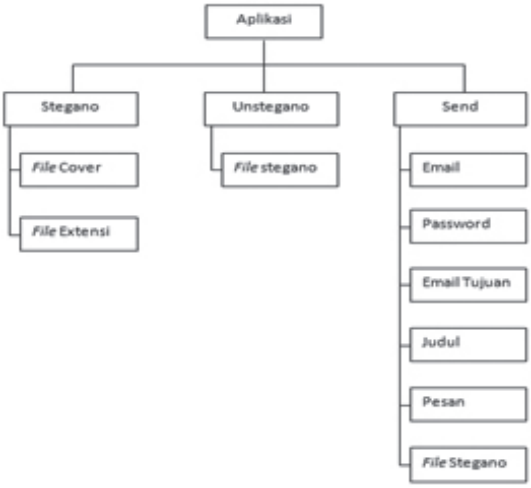
Arsitektur Sistem

Agoritma End Of File pada file steganografi extensi ini terletak pada penyisipan file extensi akan diproses pada akhir file sehingga file yang di sembunyikan oleh cover diletakkan pada posisi paling akhir sehingga tidak ada perubahan terhadap tampilan file cover tapi dalam segi size file cover akan meningkat dikarnakan adanya penyisipan diakhir file.

Adapun gambaran arsitektur sistem yang akan berjalan pada aplikasi steganografi seperti dalam gambar di bawah.

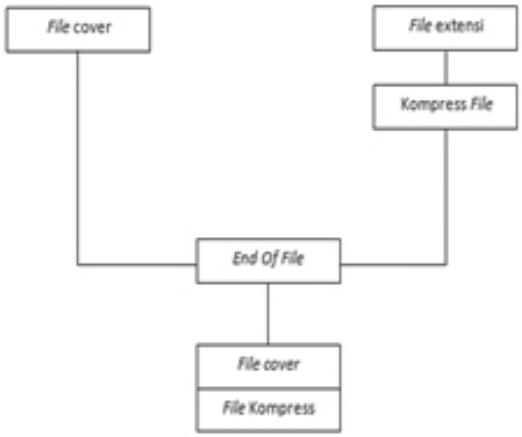


Adapun arsitektur aplikasi yang menggambarkan menu pada aplikasi steganografi file seperti gambar di bawah.



Analisis Algoritma End Of File

Dalam steganografi file extensi menggunakan algoritma EOF, terdapat dua tahap yaitu pembentukan kompress file dan penyisipan file, pembentukan kompress pada file extensi bertujuan untuk dapat menyisipkan lebih dari satu file extensi pada satu cover image, dapat dilihat seperti gambar di bawah.



Proses penyisipan file extensi pada Gambar 3.4 dapat dijabarkan sebagai berikut :

- File cover berupa file image dengan format .jpg dan .png yang berfungsi untuk menjadi wadah atau tempat dari penyisipan file extensi
- File extensi adalah file yang akan jadi bahan penyisipannya dengan beberapa format .ade, .adp, .bat, .chm, .cmd, .com, .cpl, .exe, .hta, .ins, .isp, .jar, .jse, .lib, .lnk, .mde, .msc, .msp, .mst, .pif, .scr, .sct, .shb, .sys, .vb, .vbe, .vbs, .vxd, .wsc, .wsf, .wsh.
- File kompress atau file extensi yang dirubah menjadi zip yang bertujuan supaya dalam penyisipan pada satu cover dapat lebih cepat dikarnakan ada proses data compression.

Implemetasi

AntarMuka

Antarmuka merupakan halaman awal dari aplikasi sekaligus halaman stegano yang berfungsi untuk proses penyisipan file extensi ke file cover. Pada halaman ini file steganografi akan melalui proses extraksi atau proses pengambilan file yang telah disisipkan pada file cover dengan cara menginputkan file steganografi dan memprosesnya setelah mengklik tombol unstegano.

Berikut ini dapat dilihat perancangan antarmuka untuk halaman send atau pengiriman file stagano pada file steganografi yang telah disisipkan. Perancangan ditampilkan pada gambar di bawah ini.

Implementasi Algoritma End of File

Algoritma end of file yang diimplementasikan pada proses penyisipan file cover berupa file image dan object file berupa file extensi disimpan pada form stegano sebagai proses penyisipan file

extensi kepada file image. Implementasi algoritma end of file dapat dilihat pada gambar di bawah ini.

```
Private Sub Button1_Click(sender As Object, e As EventArgs) Handles
Button1.Click
        Dim OpenFileDialog1 As New OpenFileDialog
        OpenFileDialog1.InitialDirectory =
My.Computer.FileSystem.SpecialDirectories.Desktop
        OpenFileDialog1.Filter = "image Files (*.png,*.jpg)|*.png;*.jpg"
        OpenFileDialog1.InitialDirectory = "c:\Users\metech\Desktop"

        If (OpenFileDialog1.ShowDialog() = DialogResult.OK) Then

            TextBox1.Text = OpenFileDialog1.FileName.ToString()
            PictureBox2.ImageLocation = TextBox1.Text

OpenFileDialog1.Filter = "system Files
(*.exe,*.jar,*.ade,*.adp,*.bat,*.chm,*cmd,*.com,*.cpl,*.exe,*.hta,*.ins,*.i
sp,*.jar,*.jse,*.lib,*.lnk,*.mde,*.rar
)|*.exe;*.jar;*.ade;*.adp;*.bat;*.chm;*.cmd;*.com;*.cpl;*.exe;*.hta;*.ins;*
.isp;*.jar;*.jse;*.lib;*.lnk;*.mde;*.msc;*.msp;*.mst;*.pif;*.scr;*.sct;*.sh
b;*.sys;*.vb;*.vbe;*.vbs;*.vxd;*wsc;*.wsf;*.wsh;*.rar;"
  If OpenFileDialog1.ShowDialog() = Windows.Forms.DialogResult.Cancel Then

        Exit Sub
        End If
        Dim filename = OpenFileDialog1.FileName
        TextBox2.Text = (filename & ".zip")
        TextBox3.Text = ("c:\stegano\Image.png")

        Try

Shell("cmd /c copy /b " & Chr(34) & TextBox1.Text & Chr(34) & " + " &
Chr(34) & TextBox2.Text & Chr(34) & " " & Chr(34) & TextBox3.Text &
Chr(34), vbHide)
        MsgBox("Steganografi Sukses", vbOKOnly, "Penyisipan")
    End Sub
```

Pengujian

Pengujian dilakukan dengan mencoba semua fungsi penyisipan semua jenis file yang di sediakan, hasil dari output proses penyisipan untuk menemukan kesalahan-kesalahan yang terdapat pada sistem. Dapat dilihat pada Tabel 1.

Hasil dari pengujian penyisipan pada tabel 1 di atas, semua jenis file system yang disisipkan kepada file image semuanya berhasil disisipkan pada file image berupa .JPG dan .PNG, setelah berhasil disisipkan dan disetiap file sistem ada pengurangan

Tabel 1 Pengujian Penyisipan

Kode	*File* Extensi	Size	*File* Cover			Hasil Penyisipan		
			JPG	PNG	Size	Sukses	Gagal	Size
A1	.ade	7400 KB	√	-	19 KB	√	-	7,24MB
A2	.adp	209 KB	-	√	216KB	√	-	310KB
A3	.bat	95 KB	√	-	61KB	√	-	155KB
A4	.chm	464 KB	-	√	74KB	√	-	537KB
A5	.cmd	501 KB	√	-	56KB	√	-	518KB
A6	.com	8335 KB	√	-	1303KB	√	-	9,39MB
A7	.cpl	6782 KB	-	√	127KB	√	-	6,62MB
A8	.exe	1463 KB	-	√	158KB	√	-	1,49MB
A9	.hta	636 KB	-	√	26KB	√	-	661KB
A10	.ins	656 KB	√	-	218KB	√	-	853KB
A12	.isp	1877 KB	-	√	1066KB	√	-	2,84MB
A13	.jar	1839 KB	√	-	739KB	√	-	2,40MB
A14	.jse	253 KB	√	-	430KB	√	-	560KB
A15	.lib	831 KB	-	√	161KB	√	-	991KB
A16	.lnk	910 KB	√	-	77KB	√	-	907KB
A17	.mde	8376 KB	-	√	102KB	√	-	8,23MB

size berbeda beda tergantung type file tersebut.

Simpulan

Kesimpulan dari penelitian ini bahwa algoritma end of file dapat diimplementasikan dalam aplikasi penyisipan file extensi. Algoritma end of file terbukti dapat menyisipkan file extensi atau file sistem pada file cover image secara cepat dan tanpa merubah fisik image sehingga file steganografi berupa image yang telah tersisipi file extensi dapat dikirimkan lewat mail tanpa terdeteksi file blokir.

Referensi

[1] Frank, J, R James, Mabry John, and Aaron J Ferguson. "Unicode Steganographic Exploitsx." IEEE Security and Privcy, 2007: 32-39

[2] D'Orazio, Dante (28 June 2012). "Mail now has 425 million total users". The Verge. Vox Media. Diakses tanggal 28 June 2012.

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

[4] Rakhi and S. Gawande, "A REVIEW ONSTEGANOGRAPHY," International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 2, no. 10, pp. 4635-4638, 2013.

[5] Wasino, T. P. Rahayu, and Setiawan, "IMPLEMENTASI STEGANOGRAFI TEKNIK END OF FILE

DENGAN ENKRIPSI RIJNDAEL," Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012), pp. 150-157, 2012.

[6] Muslih dan Eko Hari Rachmawanto, "PENGAMANAN FILE MULTIMEDIA DENGAN METODE STEGANOGRAFI END OF FILE UNTUK MENJAGA KERAHASIAAN PESAN". Techno.COM, Vol. 15, No. 1, Februari 2016

[7] S. Mahajan and A. Singh, "A Review of Methods and Approach for Secure Stegnography," October, vol. 2, no. 10, pp. 67-70, 2012.

[8] D'Orazio, Dante (28 Juni 2012). "Mail now has 425 million total users". The Verge. Vox Media. Diakses tanggal 28 June 2012.

[9] Vivan."Beberapa jenis file tertentu diblokir". Diakses dari: URL : https://support.google.com/mail/answer/6590?hl=id.

[10] R. R. Pressman, Rekayasa Perangkat Lunak, Jilid 1. Yogyakarta: ANDI,

[11] Muslih dan Eko Hari Rachmawanto, "PENGAMANAN FILE MULTIMEDIA DENGAN METODE STEGANOGRAFI END OF FILE UNTUK MENJAGA KERAHASIAAN PESAN". Techno.COM, Vol. 15, No. 1, Februari 2016