Menyembunyikan File Kedalam File Gambar Menggunakan Metode Steganografi

Dedi Irawan[1], Pujianto[2]

Program Studi Ilmu Komputer, Fakultas Ilmu Komputer, Universitas Muhammadiyah Metro [1,2]
Jl. Gatot Subroto No. 100 Metro Lampung
dedi.mti@gmail.com [1], *pujilabkom@gmail.com* [2]

Abstract— ***The need for communication in the digital era at this time makes the insertion of information applicable to digital files / media such as images, video, audio and text. Steganography inserts a secret message in a file / media without anyone realizing that the media has a secret message. Steganography (information hiding) is a technique to hide secret messages on a media host or also called a media cover. Steganography comes from Greek which means "hidden writing". Used in various forms for thousands of years. Steganography method is a method that inserts information into other data without destroying the data. Of course, using this steganography will not arouse the suspicion of other parties who are not entitled to receive information.***

Abstrak— **Kebutuhan komunikasi di era digital pada saat ini membuat penyisipan informasi dapat diterapkan pada file/media digital seperti gambar, video, audio, dan teks. Steganografi menyisipkan pesan rahasia pada suatu file/media tanpa ada yang menyadari bahwa media tersebut memiliki sebuah pesan rahasia. Steganografi (*information hiding*) adalah sebuah teknik untuk menyembunyikan pesan rahasia pada sebuah host media atau disebut juga cover media. Steganografi berasal dari bahasa Yunani yang memiliki arti "menulis tersembunyi". Digunakan dalam beragam bentuk selama ribuan tahun. Metode Steganografi merupakan suatu metode yang menyisipkan informasi ke dalam data lainnya dengan tidak merusak data tersebut. Tentu saja dengan menggunakan steganografi ini tidak akan menimbulkan kecurigaan pihak lain yang tidak berhak menerima informasi.**

Keywords— **file kedalam file gambar, menyembunyikan file , menyembunyikan pesan, pesan rahasia, steganografi.**

I. Pendahuluan

Steganografi berawal dari bahasa Yunani yakni "steganos" yang mempunyai arti tersembunyi/menyembunyikan dan "graphy" yang artinya tulisan yang secara lengkap memiliki arti tulisan yang disembunyikan. Steganografi telah digunakan sejak sekitar 2.500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi sebagai alat. Catatan pertama tentang steganografi ditulis oleh Herodotus, yaitu seorang sejarawan Yunani. Herodatus mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Caranya dengan menuliskan pesan di atas kepala budak yang telah dibotaki, ketika rambut budak telah tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya.

Sedangkan penggunaan steganografi oleh bangsa Romawi dilakukan dengan menggunakan tinta tak-tampak (invisible ink) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Di era modern, teknik steganografi menjadi populer setelah kasus pemboman gedung WTC pada 11 September 2001 di Amerika Serikat. Pada saat itu, teroris menyembunyikan pesan-pesan kegiatan terornya dalam berbagai media yang dapat dijadikan penampung untuk menyembunyikan file seperti pada image, audio dan video. Pada peristiwa tersebut disebutkan bahwa para teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang chat sport, bulletin boards porno dan website lainnya.

A. Perbedaan Steganografi dengan Kriptografi

Ada beberapa perbedaan antara steganografi dengan kriptografi. Perbedaan terletak pada visibilitas pesan, pada kriptografi pihak ketiga dapat mendeteksi adanya data acak (chipertext), karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan, tetapi dapat dikembalikan ke bentuk semula.

Berbeda dengan kriptografi yang menjaga kerahasian pesan dengan cara mengubah bentuk (acak) pesan agar tidak dapat dipahami oleh orang lain yang menerimanya, steganografi merupakan suatu teknik penyembunyian pesan pada suatu medium. Perlu diperhatikan dalam steganografi, suatu pesan tidak harus diubah, tetapi pesan tersebut disembunyikan pada suatu medium agar pesan tersebut tidak terlihat.

Salah satu keuntungan steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian sehingga media penampung pesan tidak menimbulkan kecurigaan bagi pihak ketiga.

Gambar 1 dibawah ini menggambarkan ilustrasi perbedaan steganografi dengan kriptografi.

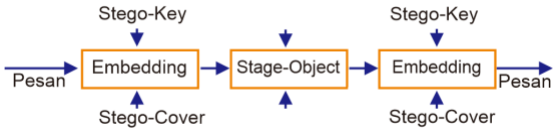
Gbr. 1 Perbedaan Steganografi dengan Kriptografi

B. Prinsip atau Cara Kerja Steganografi

Untuk dapat menyisipkan data yang akan disembunyikan membutuhkan dua unsur, yaitu:

a) Unsur pertama adalah media penampung seperti citra, suara, video dan sebagainya yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia.
b) Unsur kedua adalah pesan yang ingin disembunyikan yaitu media penampungnya berupa citra yang disebut cover-object dan citra yang telah disisipi pesan disebut stego-object.

Prinsip atau Cara Kerja Steganografi dapat dilihat pada gambar 2 dibawah ini.



Gbr. 2 Prinsip atau cara kerja steganografi

Secara umum, terdapat dua proses didalam steganografi, yaitu proses embedding untuk menyisipkan pesan ke dalam cover-object dan proses decoding untuk ekstraksi pesan dari stego-object. Kedua proses ini mungkin memerlukan kunci rahasia yang dinamakan stego-key agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

C. Kriteria dan Aspek dalam Steganografi

Penyembunyian data rahasia ke dalam media digital mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data diantaranya adalah:

a) Fidelity
Yaitu mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
b) Robustness
Yaitu data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, penambahan noise, perbesaran gambar, pemotongan (cropping), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
c) Recovery
Yaitu data yang disembunyikan harus dapat diungkapkan kembali (recovery). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

D. Jenis-jenis Teknik Steganografi

Berdasarkan teknik steganografi yang digunakan terdapat tujuh jenis teknik steganografi, yaitu sebagai berikut (Ariyus, 2009):

a) Injection
Merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut embedding.
b) Substitusi.
Data normal digantikan dengan data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.
c) Transformasi Domain
Teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada transform space.
d) Spread Spectrum
Merupakan teknik pentransmisian menggunakan pseudo-noise code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwith) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima,

sinyal dikumpulkan kembali menggunakan replika pseudo-noise code tersinkronisasi.

e) Statistical Method
Teknik ini disebut juga skema steganographic 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.

f) Distortion
Metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.

g) Cover Generation
Metode ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan.

II. METODE PENELITIAN

Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya:

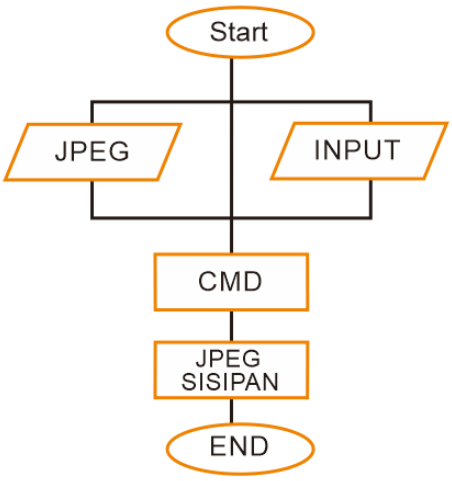
- ✓ Format gambar
  bitmap bmp, gif, pcx, jpeg, dll.
- ✓ Format audio
  wav, mid, mp3, dll.
- ✓ Format lain : teks file, html, pdf, doc, dll.

Metode Steganografi merupakan suatu metode yang menyisipkan informasi ke dalam data lainnya dengan tidak merusak data tersebut. Tentu saja dengan menggunakan steganografi ini tidak akan menimbulkan kecurigaan pihak lain yang tidak berhak menerima informasi.

Analisis Kebutuhan dan Perancangan

Sistem steganografi yang dibahas akan di fokuskan kepada bagaimana cara membangun suatu sistem steganografi pada citra digital file gambar yang efisien dan untuk mengeksploitasi keterbatasan sistem penglihatan manusia. Sistem ini terdiri dari dua buah sub sistem yaitu:

a) Sistem penyisipan
Berfungsi untuk melakukan proses penyembunyian pesan berupa file ke file citra digital gambar, seperti pada gambar 3 dibawah ini.



Gbr 3. FlowChart Penyisipan Gambar

b) Sistem pengekstrakkan
berfungsi untuk melakukan pengekstrakkan file untuk memeperoleh pesan yang telah disisipkan ke dalam file gambar tersebut. Komponen pada sistem pengekstrakkan ini terdapat komponen untuk membuka File pesan yang berada pada gambar, seperti pada gambar 4 dbawah ini.

Gbr. 4 FlowChart Pengekstrak Gambar

Permasalahan

Steganografi mempunyai kelebihan dalam aspek penyembunyian pesan di mana pesan yang disembunyikan tidak terlihat kasat mata berupa kode tertentu seperti kriptografi, dikarenakan dalam steganografi pesan dititipkan pada suatu gambar. Permasalahannya bagaimana agar pesan tersebut dapat dititipkan pada gambar tanpa terlihat berkurangnya kualitas dari gambar tersebut, dan metode apa yang tepat agar pesan yang dititipkan tidak mengurangi kualitas gambar.

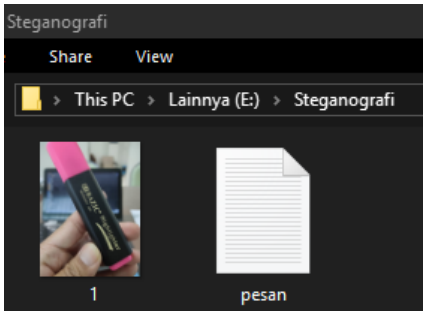
III. *HASIL DAN PEMBAHASAN*

Steganografi yang dibahas adalah menyembunyikan file/data di dalam citra digital. Meskipun demikian, penyembunyian data dapat juga dilakukan pada wadah berupa suara digital, teks, ataupun video. Penyembunyian file/data rahasia ke dalam citra digital tidak akan mengubah kualitas citra tersebut. Adapun langkah-langkah melakukannya sebagai berikut:

PENYISIPAN GAMBAR

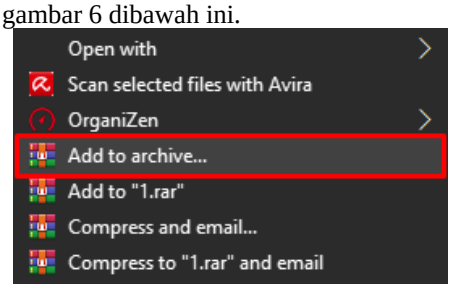
a) Membuat Folder

Buatlah Folder, misalkan folder Steganografi dan siapkan file kedalam direktori yang sama. Seperti pada gambar 5 dibawah ini.



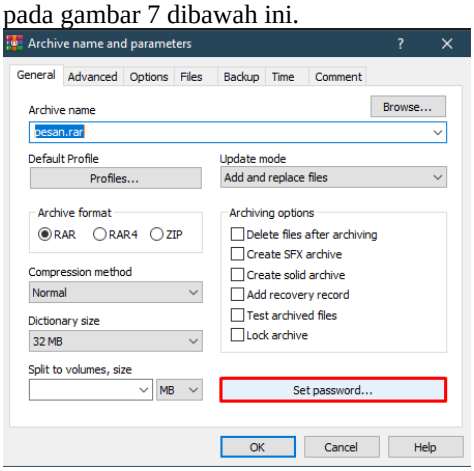
Gbr 5. Folder Steganografi

b) Kompres file yang akan disisipkan, klik kanan -> Add to archieve, seperti pada gambar 6 dibawah ini.



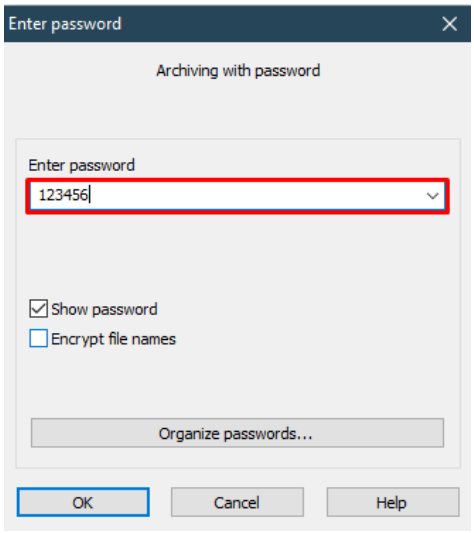
Gbr 6. Add to archieve

c) Pada dialog "Archieve name dan parameters", klik St password untuk membuat password terlebih dahulu, seperti pada gambar 7 dibawah ini.



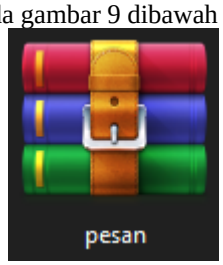
Gbr 7. Set Password

d) Isikan password, seperti pada gambar 8 dibawah ini.



Gbr 8. Set password

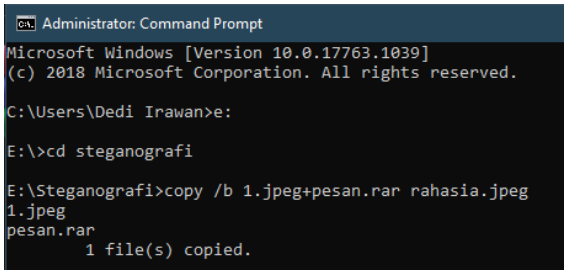
e) File yang akan disembunyikan akan muncul dalam file baru yaitu pesan.rar, seperti pada gambar 9 dibawah ini.



Gbr 9. File baru

f) Selanjutnya jalan tools CMD,

g) Pada dialog Command Prompt, isikan command menuju kealamat direktori pada point a diatas, seperti pada gambar 10 dibawah ini.



Gbr 10. Command Prompt

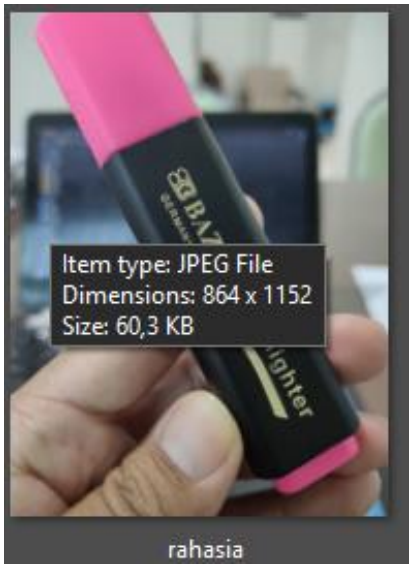
h) Apabila berhasil maka akan ada file baru dengan nama rahasia.jpeg dan ukurannya bertambah, seperti pada gambar 11 dibawah ini.

Gbr 11. File Baru Rahasia

File rahasia.jpeg yang baru dibuat dengan perintah di command prompt didalamnya sudah ditambahkan file/data rahasia dari file pesan.txt

Sekilas file rahasia.jpeg hanya sebatas file jpeg biasa yang mirip seperti file 1.jpeg. Berikut ini adalah perbandingan perbedaan ukuran gambar sebelum dan sesudahnya, seperti pada gambar 12 dan 13 dibawah ini.

Gbr 12. Sebelum Steganografi

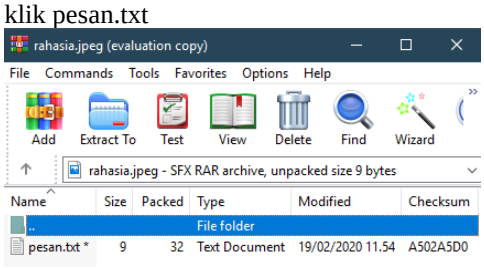


Gbr 13. Sesudah Steganografi

MENGEKSTRAK GAMBAR

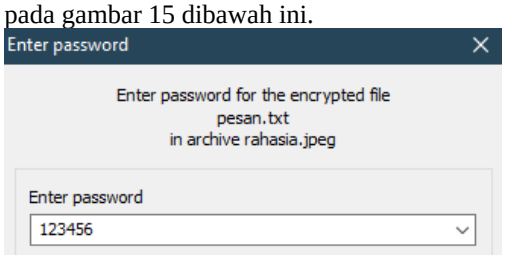
Bagaimana cara mengakses file rahasia.jpeg yang baru dibuat:

a) Klik kanan pada gambar rahasia.jpeg -> Open With -> Winrar archiever.
b) Pada dialog seperti gambar 14 dibawah ini, klik pesan.txt



Gbr 14. Pesan.txt

c) Isikan password pada file pesan.txt, seperti pada gambar 15 dibawah ini.



Gbr 15. Mengisikan Password

d) Jika password yang diisikan benar maka file akan terbuka, seperti pada gambar 16 dibawah ini.

Gbr 16. File berhasil dibuka

IV. KESIMPULAN

Kesimpulan dari penulisan ini adalah sebagai berikut:

a) Metode Steganografi menyembunyikan pesan file kedalam file gambar yang merupakan pembungkus pesan file.
b) File yang sudah terselubung dalam proses encode menjadi file gambar dengan ukuran file yang lebih besar namun tidak merubah komposisi fisik gambar.
c) Dalam penelitian ini digunakan Command Prompt untuk memberikan command dan format file yang disembunyikan dikompresi dengan aplikasi Winrar. Format gambar dalam ekstensi jpeg. Hasil encode dalam format gambar berekstensi jpeg.
d) Hasil pemisahan file ter-encode (decode) dalam bentuk file terkompresi berekstensi rar yang isinya adalah file gambar dan pesan file asli dengan ukuran tetap.

e) Efektivitas steganografi dalam pengiriman pesan file rahasia cukup kompeten dalam dunia keamanan komputer, mengingat secara kasat mata file dalam bentuk file (gambar) biasa yang tidak terkira tersimpan pesan rahasia di dalamnya.

Referensi

[1] Agung Sulistyanto, "Aplikasi Steganografi dengan Metode LSB dan Enkripsi Pesan dengan Pembangkitan Bilangan Acak ," Laboratorium ICT Terpadu Universitas BUDI LUHUR, Juli 2015.
[2] Dony Ariyus, "Kriptografi keamanan data dan komunikasi," Graha Ilmu, Juli 2017.
[3] Pulung Nurtantio Andono, T Sutojo, Muljono, "Pengolahan Citra Digital," Andi Offset, 2015.
[4] (2018) Cornell University. [Online]. Available: https://arxiv.org/abs/1806.03618
[5] Harun Mukhtar, "Kriptografi untuk keamanan data," Deeppublish, November 2018.
[6] (2020) Repository DINUS. [Online]. Available: http://dinus.ac.id/repository/docs/ajar/SteganoGraphy.pptx