Implementasi Penyembunyian Pesan Teks pada Citra Gif dengan menggunakan Metode End Of File

Samlyot Hutasoit
STMIK Budi Darma Medan, JL. Sisingamangaraja Np. 338 Simpang Limun Medan
Email: Samlyothutasoit@gmail.com

Abstrak

Seiring dengan berkembangnya kejahatan dalam sistem informasi, dengan berbagai tehnik pengambilan informasi secara illegal. Untuk itu ada tuntutan yang semakin besar untuk menciptakan suatu sistem penyampaian informasi yang terjamin keamanannya. Salah satunya adalah dengan steganografi. Steganografi merupakan suatu metode untuk menyisipkan informasi rahasia dalam suatu objek atau media lain. Dengan steganografi, informasi disembunyikan sedemikian rupa sehingga tidak diketahui keberadaannya, yang dikenal dengan istilah informasi hiding. Metode ini berbeda dengan metode kriptografi, yang menyandikan informasi yang ada sehingga tidak dapat dibaca tanpa mengetahui kunci atau sandi yang digunakan, namun keberadaannya tetap diketahui dan tidak disembunyikan. Proyek akhir ini dikembangkan dengan menggunakan Microsoft Visual Basic, mengimplementasikan metode steganografi End Of File (EOF) untuk menyembunyikan suatu informasi ke dalam file multimedia. File multimedia yang digunakan adalah file citra, sebagai media pembawa informasi rahasia. Penggunaan teknologi steganografi ini diharapkan dapat meningkatkan keamanan dalam penyampaian informasi, agar informasi-informasi penting akan terlindungi dan tersamarkan keberadaannya dalam file citra digital.

Kata kunci : Steganografi, Pesan teks, Citra digital, End Of File

Abstract

Along with the development of crime in information systems, with various techniques for illegal information retrieval. For this reason, there is an increasing demand to create a system for delivering information that is guaranteed to be safe. One of them is with steganography. Steganography is a method for inserting confidential information in an object or other media. With steganography, information is hidden in such a way that its whereabouts are unknown, known as hiding information. This method is different from the cryptographic method, which encodes the information available so that it cannot be read without knowing the key or password used, but its existence is still known and not hidden. This final project was developed using Microsoft Visual Basic, implementing the End of File (EOF) steganography method to hide information into multimedia files. The multimedia file used is an image file, as a carrier for confidential information. The use of steganography technology is expected to increase security in the delivery of information, so that important information will be protected and camouflaged its existence in digital image files.

Keywords: Steganography, Text messages, Digital imagery, End of File

1. PENDAHULUAN

Seiring berkembangnya dunia komputer semakin bertambah pula kejahatan dalam sistem informasi, dengan berbagai tehnik pengambilan informasi secara illegal yang berkembang, banyak yang mencoba untuk megakses informasi yang bukan haknya. Dengan

hal itu, perlu mengembangkan pengamanan dalam sistem informasi yang berada dalam media komputer tersebut [1].

Berbagai macam teknik yang digunakan untuk melindungi informasi yang dirahasiaakan dari orang yang tidak berhak telah banyak dilakukan dalam upaya mengamankan suatu data penting dengan menggunakan sistem kriptografi yang melakukan enkripsi sebelum data tersebut di tranmisikan. Tindakan pengamanan menggunakan cara tersebut ternyata dianggap belum cukup dalam mengamankan suatu data karena adanya peningkatan kemampuan komputasi [2].

Maka untuk itu dilakukan tehnik steganografi yaitu menyembunyikan teks rahasia agar orang awam tidak menyadari keberadaan teks yang disembunyikan.Teknik ini sering digunakan untuk menghindari dari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi teks rahasia tersebut.Caranya dengan menyembunyikan teks rahasia tersebut dalam suatu wadah penampung informasi dengan sedemikian rupa sehingga keberadaan teks rahasia yang ditempel tidak terlihat. Wadah penampung teks tersebut dapat berbentuk berbagai jenis file seperti multimedia digital seperti citra, audio dan video.Dalam penelitian ini, peneliti membuat analisis steganografi merupakan solusi dari permasalahan tersebut. Dengan penggunaan teknik ini, saya memamfaatkan kelemahan indera manusia sehingga data informasi tidak jatuh pada orang-orang yang tidak berhak dan dapat kita sembunyikan didalam media digital yang kita punya[3], [4].

Dengan mempertimbangkan penelitian yang menyatakan bahwa metode *End Of File* dapat sebagai cara untuk menyisipkan pesan ke dalam citra, dengan hal itu maka akan dilakukan proses penyembunyian dengan menggunakan metode *End Of File*. Metode *End Of File*merupakan salah satu teknik yang menyisipkan pesan pada akhir file dan pengembangan dari pada metode *LSB* [3].

2. LANDASAN TEORI

2.1 Steganografi

Steganografi merupakan seni untuk menyembunyikan pesan didalam media digital sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan diadalam media tersebut. Kata steganografi (*steganography*) berasal dari bahasa yunani steganos, yang artinya "tersembunyi/terselubung", dan graphein, "menulis" sehingga kurang lebih artinya "menulis (tulisan) terselubung"[5].

Dalam bidang keamanan komputer, steganografi digunakan untuk menyembunyikan data rahasia saat enkripsi tidak dapat dilakukan atau bersamaan dengan enkripsi.jadi, walaupun enkripsi berhasil dipecahkan (*decipher*)pesan atau data rahasia tetap tidak terlihat. Selain itu, pada kriptografi pesan disembunyikan dengan "diacak" sehingga pada kasus-kasus tertentu dapat dengan mudah mengundang kecurigaan, sedangkan pada steganografi pesan "disamarkan" dalam bentuk yang relatif "aman" sehingga tidak terjadi kecurigaan itu. Seperti yang terjadi pada peristiwa penyerangan gedung WTC tanggal 11 september 2001 disebut oleh "pejabat pemerintah dan para ahli dari pemerintahan AS" yang tidak disebut namanya 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". Isu lainnya menyebutkan bahwa teroris menyembunyikan pesan-pesannya dalam gambar-gambar porno di website tertentu.Walaupun demikian sebenarnya belum ada bukti nyata dari pernyataan-pernyataan tersebut di atas [1], [2].

2.2 Metode End Of File (EOF)

Teknik yang digunakan pada digital *watermarking*beragam tetapi secara umum teknik ini menggunakan *redundantbits*sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitive

sehingga pesan tersebut tidak ada perbedaan yang terlihat atau yang terdengar. Teknik EOF atau *End Of File* merupakan salah satu teknik yang digunakan dalam Steganografi. Teknik ini menggunakan cara dengan menyisipkan data pada akhir *file*[6].

Jaminan keamanan yang dihasilkan metode EOF *(End Of File)* dapat memberikan keamanan yang lebih terjamin untuk melindungi suatu pesan teks didalam citra digital. Karena dengan metode penyisipan yang menyebar bit-bit *watermark* mengganti posisi LSB *(Least Significant Bit)* dari citra dan dimulai di akhir dari piksel citra tersebut. Maka dengan metode ini pesan yang disembunyikan didalam citra akan lebih sulit terdeteksi keberadaannya.

Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran *file* yang telah disisipkan data sama dengan ukuran *file* sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam *file* tersebut. Dalam teknik ini, data disisipkan pada akhir *file* dengan diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut.

Stego File = Nilai Decimal teks +
Nilai Decimal Gambar

keterangan :
+ : Metode *end of file*

Misalkan pada sebuah citra skala keabuan 6x6 piksel disisipkan disisipkan pesan yang berbunyi "#aku", kode ASCII dari pesan tersebut adalah :

35 97 107 117

Misalkan matriks tingkat derajat keabuan citra sebagai berikut:

196 10 97 182 101 40
67 200 100 50 90 50
25 150 45 200 75 28
176 56 77 100 25 200
101 34 250 40 100 60
44 66 99 125 190 200

Kode decimal pesan disisipkan di akhir citra, sehingga citra menjadi:

196 10 97 182 101 40
67 200 100 50 90 50
25 150 45 200 75 28
176 56 77 100 25 200
101 34 250 40 100 60
44 66 99 125 190 200
35 97 107 117

Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. Tidak dapat dipersepsi *(impercepbility)*
   Keberadaan data rahasia tidak dapat dipersepsi oleh indera manusia.Jika pesan disisipkan kedalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli saat dilihat dengan mata.
2. Ketepatan*(Fidelity)*
   Kualitas citra penampung tidak jauh berubah setelah penyisipan data rahasia.Pengamat tidak mengetahui kalau didalam citra tersebut terdapat data rahasia.
3. Kapasitas *(Capacity)*
   Berhubungan dengan jumlah informasi yang dapat disisipkan kedalam media penampung.

4. Tidak terdeteksi *(Undetecability)*
   Kemampuan untuk menghindari deteksi oleh indera manusia maupun analisis statistic.
5. Pemulihan *(Recovery)*
   Data yang disembunyikan harus dapat diungkapkan kembali *(reveal)*.

Dalam melakukan proses steganografi, ada beberapa faktor yang saling berkompetisi satu sama lain, artinya saat salah satu faktor ditingkatkan maka kemungkinan faktor lain akan mengalami penurunan[7].

2.3 Citra GIF

Graphics interchange format atau sering disingkat GIF adalah sebuah format berkas citra yang diperkenalkan pada tahun 1987 oleh CompuServe untuk menggantikan format RLE yang hanya menampilkan gambar dengan warna hitam dan putih saja.

GIF adalah salah satu format berkas citra yang paling sering ditemui di dunia digital hal ini terjadi karena format ini berukuran relative kecil. Sebagai contoh untuk cira yang sama, berkas dengan format GIF dapat berukuran lebih kecil jika dibandingkan format JPG.

Hal ini disebapkan karena file GIF hannya menggunakan 256 palet warna. Sehingga tentunya ukuran file akan lebih kecil. Namun 256 falet warna tersebut tidak mutlak hanya 256 warna tertentu.Namun warna tersebut dapat dipilihdari 24-bit palet warna RGB. Sehingga dengan singkat kata dapat disimpulkan bahwa berkas dengan format GIF akan membuang palet warna yang tidak diperlukan dan mengambil hannya 256 palet warna yang diperlukan.

Ukuran palet sebesar 256 warna adalah standar GIF'89 dan 87.Beberapa versi dari GIF sekarang telah dapat menampilkan warna dengan lebih dari 256 warna.GIF dengan format GIF'89 dan GIF'87 dapat dibedakan dari hider file [3], [8].

Menurut sebuah sumber saat ini 3 format file yang digemari adalah JPG, GIF dan juga PNG. Format PNG memang sekarang ini merupakan format yang dinilai lebih favorit ketimbang format lainnya namun format GIF tetap merupakan salah satu format yang umum digunakan.Karena salah satu kelebihan format ini adalah adanya dukungan untuk penampilan gambar bergerak.

Namun format GIF bukan merupakan format yang tidak memiliki kekurangan.Akibat dari jumlah warna yang hannya 256 warna saja maka format ini jarang sekali digunakan untuk citra fotografi.Karena seringkali citra fotografi menggunakan warna yang lebih dari 256 warna. Sehingga jika citra fotografi direprentasikan dalam format GIF akan mengalami penurunnan kualitas yang banyak.

2.4 Citra Keabuan/*grayscale*

Citra yang menggunakan gradasi warna abu-abu yang merupakan kombinasi antara hitam dan putih. Setiap warna didalam citra berskala keabuan dinyatakan dengan sebuah nilai bulat antara 0 dan 255 (untuk yang aras keabuanya sama dengan 256) dan nilai tersebut disebut sebagai intensitas[9].

3. HASIL DAN PEMBAHASAN

Teknik *End Of File (EOF)* merupakan salah satu teknik yang digunakan dalam steganografi. Teknik menggunakan cara dengan menyisipkan data pada akhir *file.* Jaminan keamanan yang dihasilkan metode *End Of File* dapat memberikan keamanan yang lebih terjamin untuk melindungi suatu pesan teks.

Misalkan data berupa text **"RAHASIA1"** akan disisipkan kedalam gambar. Jika direpresentasikan ke dalam decimal kata **"RAHASIA1"** ini menjadi

Tabel 1 ASCII Perubahan dari Character ke Decimal

Character	Decimal
R	82
A	65
H	72
A	65
S	83
I	73
A	65
1	49

Disini terdapat pixel 8x8 *grayscale* tempat untuk penyisipan pesan teks dan setiap pixel tersebut akan dicari nilai decimal nya supaya lebih gampang untuk penyisipan pesan teks tersebut. *Grayscale image* terdiri dari warna hitam, abu-abu dan putih , *grayscale* menunjukkan jumlah warna yang ada dalam satu citra. Biasanya *grayscale* image disebut gambar hitam putih dan memiliki 8 bit warna.

Tabel 2 Matriks Media Penampung (gambar cover.GIF)

36	36	19	19	22	36	22	22
22	29	36	13	13	36	13	13
22	22	36	13	29	19	18	19
22	22	22	13	24	13	36	36
13	13	13	22	29	29	13	22
22	22	13	29	32	24	22	22
22	22	13	24	34	32	36	36
22	22	22	13	13	13	22	22

Tabel 3 Hasil Penyisipan

36	36	19	19	22	36	22	22
22	29	36	13	13	36	13	13
22	22	36	13	29	19	18	19
22	22	22	13	24	13	36	36
13	13	13	22	29	29	13	22
22	22	13	29	32	24	22	22
22	22	13	24	34	32	36	36
22	22	22	13	13	13	22	22
82	**65**	**72**	**65**	**83**	**73**	**65**	**49**

Kode decimal pesan disisipkan di akhir citra, sehingga citra menjadi seperti yang di atas. Bit yang diboldkan adalah bit data yang disisipkan kedalam citra digital dengan metode EOF, penyisipan bit data ini tidak akan memberi pengaruh besar pada perubahan nilai bit citra sehingga citra awal dan citra hasil tidak akan terlihat perubahan yang mencolok.

4. ALGORITMA DAN IMPLEMENTASI

Algoritma adalah urutan langkah-langkah logis untuk menyelesaikan suatu masalah yang disusun secara sistematis, dan algoritma program merupakan bentuk dasar dari perintah-perintah yang akan di-*coding*-kan kedalam setiap form yang telah dirancang pada tahap implementasi sistem. Adapun bentuk algoritma tersebut adalah sebagai berikut :

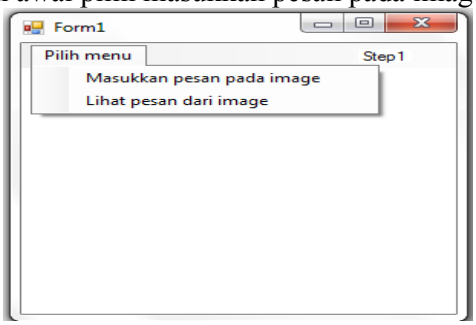
4.1 Algoritma Penyisipan Pesan

Input : **X** ⟵ Pesan teks
Y ⟵ Gambar (*image*)
Output : **Z** ⟵ Stego file (Citra berisi pesan)

Proses : X = Nilai decimal teks
Y = Nilai decimal gambar
Z = X + Y
End

4.2 Implementasi

Pada Tampilan Menu Masukkan pesan pada image/Lihat pesan dari image berfungsi untuk pemilihan penyisipan pesan teks pada gambar atau mengekstrak gambar yang telah disisipi teks. Untuk langkah awal pilih masukkan pesan pada image, seperti pada gambar 1

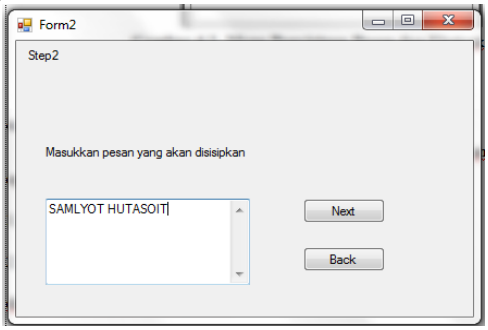


Gambar 1 Menu Penyisipan Pesan dan Ekstrak Pesan

Pada menu inilah kita mengisi teks yang akan disisipi pada gambar. Pada menu ini ada 2 option tombol yaitu :

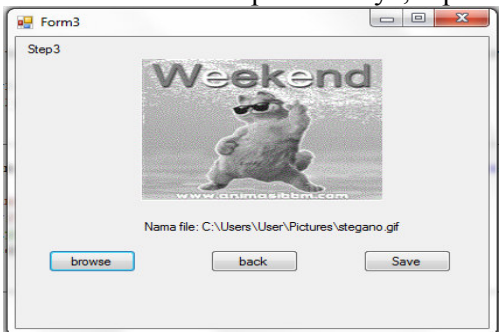
1. Back : Berfungsi untuk kembali ke menu sebelumnya
2. Next : Berfungsi untuk lanjut ketahap berikutnya.

dapat dilihat seperti pada gambar 2



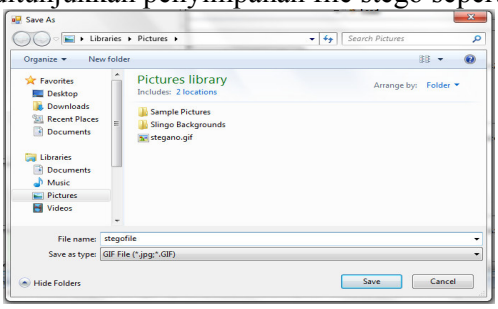
Gambar 2 Tampilan Penyisipan Pesan Pada Image

Pada Tampilan Pemilihan gambar, pilih browse untuk memilih gambar pembawa pesan yang akan disisip kemudian klik next untuk step berikutnya, seperti pada gambar 3.



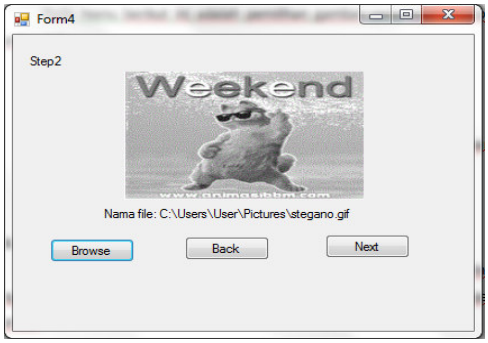
Gambar 3 Menu Pemilihan Document

Pada tampilan ini ditunjukkan penyimpanan file stego seperti pada gambar 4



Gambar 4 Menu Penyimpanan Hasil

Pada menu berikut ini adalah pemilihan gambar yang telah disisipi pesan teks. Seperti pada gambar 5



Gambar 5 Menu pemilihan gambar yang telah disisipi pesan teks

5 KESIMPULAN

Steganografi merupakan tehnik yang bagus dalam pengamanan file maupun pesan teks rahasia. Berdasarkan perancangan yang dilakukan, maka dapat di tarik kesimpulan :

1. Menggunakan metode *End Of File* maka akan mempermudah proses penyembunyian pesan teks pada citra GIF karna nilai decimal teks disisipkan diakhir nilai decimal gambar dan tanpa ada perubahan yang signifikan terhadap kualitas citra.
2. Dengan adanya aplikasi pemograman Visual Basic 2008 membuat pengguna lebih mudah untuk melakukan penyembunyian pesan teks pada citra GIF.

DAFTAR PUSTAKA

[1] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
[2] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.
[3] A. Suhendra, "Steganografi Pada Citra Terkompresi Metode Huffman," *MEANS (Media Inf. Anal. dan Sist.*, vol. 1, no. 2, pp. 33–39, Dec. 2016.
[4] T. Limbong, "Pengujian Kriptografi Klasik Caesar Chipper Menggunakan Matlab," *no. Sept.*, vol. 2017, 2015.
[5] A. M. Hasibuan, "Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone," *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 1, pp. 29–35, Jun. 2017.
[6] S. Maharani, I. Maula, and Z. Arifin, "STEGANOGRAFI VIDEO MENGGUNAKAN METODE END OF FILE (EOF)," *SCAN - J. Teknol. Inf. dan Komun.*, vol. 11, no. 3,

pp. 49–56, 2016.

[7] Martono and Irawan, "Penggunaan Steganografi Dengan Metode End of File (EOF) Pada Digital Watermarking - Neliti," *urnal TICOM*, 2013. [Online]. Available: https://www.neliti.com/publications/93689/penggunaan-steganografi-dengan-metode-end-of-file-eof-pada-digital-watermarking. [Accessed: 14-Dec-2019].

[8] T. Sutojo, E. Mulyanto, V. Suhartono, and O. K. I. D. W. I. NURHAYATI, "Teori Pengolahan Citra Digital."

[9] P. B. N. Simangunsong, "Peningkatan Kualitas Citra Pada Studio Photography Dengan Menggunakan Metode Gaussian Filter," *J. Tek. Inform. UNIKA St. Thomas*, vol. 3, no. 1, pp. 59–63, 2018.