

Perancangan Aplikasi Penyisipan Pesan Pada Pixel Citra Menggunakan Metode End Of File

Mahrizal Masri¹⁾, Mahyuzar Masri²⁾, Helma Widya³⁾, Dedek Yuhendri⁴⁾,
Muhamamd Ihsan Fauzi⁵⁾

^{1,3,4)}Dosen Teknik Informatika – ITM, ²⁾Dosen Teknik sIPIL – ITM,

⁵⁾Alumni Teknik Informatika - ITM

Abstrak

Salah satu format digital yang sering dijumpai pada computer adalah citra digital atau sering disebut dengan file image. Seiring dengan semakin banyaknya pengguna citra digital, maka proses pengolahan citra digital juga semakin berkembang seperti penyisipan tesk pada citra digital dengan teknik Steganography. Teknik steganography dapat dimanfaatkan untuk beberapa hal contohnya seperti dapat mengirim pesan rahasia tanpa terlihat oleh orang lain. Format citra digital yang digunakan adalah JPG, PNG, dan BMP. Hasil dari implementasi program ini adalah pesan yang telah disisipkan tidak terlihat oleh kasat mata dan kualitas citra digital tidak berubah. Aplikasi yang dibuat dapat mengembalikan isi pesan secara utuh yang sebelumnya telah dilakukan proses encode, disarankan untuk dikembangkan lebih lanjut dengan menambahkan proses cryptography untuk meningkatkan keamanan pesan sebelum di sisipkan ke media.

Kata Kunci : Steganography, EOF (End Of File), Citra Digital, MatlabR2012.

I. PENDAHULUAN

Steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan atau data rahasia di dalam suatu media penampungnya sehingga orang lain tidak menyadari adanya pesan didalam media tersebut. Dalam bidang keamanan komputer, steganografi digunakan untuk menyembunyikan data rahasia. Mode warna RGB adalah model warna yang aditif yang dapat dikombinasikan untuk membuat warna yang lainnya. Sistem warna RGB terdiri dari tiga bagian yang utama, yaitu Red, Green, dan Blue. Model warna RGB didasarkan pada sistem koordinat kartesius. (R.C. Gonzales dan R.E. Woods, Digital Image Processing, 2nd ed. Upper Saddle River, NJ: Prentice-Hall, 2008).

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 yang akan disisipkan ditempatkan diakhir pixel citra.

II. TINJAUAN PUSTAKA

2.1. Steganography

Jubilee Enterprise dalam 13 Ancaman PC dan Cara Mengatasinyapengertian dan definisi istilah steganografi adalah paduan antara seni dan ilmu pengetahuan yang mempelajari cara menuliskan pesan tersembunyi. Isi maupun arti pesan hanya

bisa diterjemahkan oleh pembuat dan orang yang berhak menerima pesan.

Donovan Artz dalam jurnalnya Digital Steganography: Hiding Data within Data Steganografi adalah sebuah cara menyimpan informasi dalam suatu teknik penyembunyian keberadaan dari informasi itu.

Jadi di simpulkan bahwa Steganografi (*Steganography*) seni dan ilmu menulis atau menyembunyikan pesan dengan suatu cara sehingga selain sender dan receiver, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata steganografi (*steganography*) berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan graphein, yang artinya menulis, sehingga kurang lebih artinya adalah menulis sesuatu yang tersembunyi atau terselubung. Penggunaan steganografi antara lain bertujuan untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi dan melindungi hak cipta suatu produk. Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi ciphertext dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya. Steganografi membutuhkan dua poperti 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. 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 (Martono, 2013).

2.2. Pengertian Citra Digital

Menurut Linggar “Dalam Teori Dan Profesi Kehumasan Serta Aplikasinya, 2000:69: Bahwa citra humas yang ideal ialah kesan yang benar, yakni sepenuhnya berdasarkan pengalaman, pengetahuan serta pemahaman atas kenyataan yang sesungguhnya.

Menurut Ruslan “Dalam Bukunya Manajemen Humas Dan Manajemen Komunikasi Dan Aplikasi, 1998:63: Menyebutkan bahwa landasan citra berakar dari: “Nilai-nilai kepercayaan yang konkritnya diberikan secara individual dan merupakan pandangan atau persuasi. Serta terjadinya proses akumulasi dari individu-individu tersebut akan mengalami suatu proses cepat atau lambat untuk membentuk suatu opini publik yang lebih luas dan abstrak yaitu sering dinamakan citra atau image.

Jadi di simpulkan bahwa Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra terbagi 2 yaitu ada citra yang bersifat analog dan ada citra yang bersifat digital. Citra analog adalah citra yang bersifat kontinu seperti gambar pada monitor televisi, foto sinar X, hasil CT scan dll. Sedangkan pada citra digital adalah citra yang dapat diolah oleh komputer (T,Sutoyo et al. 2009).

2.3. Metode EOF (*End Of File*)

Metode EOF (*End Of File*) merupakan salah satu teknik yang menyisipkan data pada akhir file. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sama dengan ukuran file sebelum disisipkan data ditambah dengan ukuran data yang disisipkan kedalam file tersebut. Dalam teknik EOF, data yang disisipkan diakhir file diberi tanda khusus sebagai pengenal start dari data tersebut dan pengenal akhir dari data tersebut (Yayuk Anggrain, 2014).

Metode EOF (*End Of File*) merupakan 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 akhir file, maka sistem akan berhenti melakukan pembacaan pada file tersebut. Prinsip kerja EOF menggunakan karakter / symbol khusus penanda yang diberikan pada setiap akhir file (Yayuk Anggrain, 2014).

EOF menggunakan karakter yang berbeda sebagai penanda awal penyisipan pesan dan penanda akhir penyisipan pesan. Metode EOF menggunakan kelemahan indera manusia yang tidak sensitive sehingga seakan-akan tidak ada perbedaan terlihat antara sebelum atau sesudah pesan disisipkan (Yayuk Anggrain, 2014).

Sebagai Contoh, akan disisipkan sebuah pesan berjumlah 150 karakter pada sebuah citra digital dengan dimensi 300 x 300 pixel. Maka akan

ditempatkan pada baris ke 301 sampai selesai sesuai dengan panjang dari pesan yang akan disisipkan, Berikut gambar citra yang disisipi pesan dengan citra yang tidak disisipi pesan (Yayuk Anggrain, 2014).

Adapun algoritma dari metode EOF (*End Of File*) ini adalah sebagai berikut:

1. Baca informasi file, tentukan dimana posisi terakhir file.
2. Tandai posisi ctrl-z (penanda) sebagai awal baris penyisipan pesan.
3. Sisipkan pesan dimulai dari posisi ctrl-z (penanda) hingga akhir pesan.
4. Sisipkan ctrl-z (penanda) kedua pada akhir pesan.

Teknik EOF tidak mengubah isi awal dari file yang disisipi. Sebagai contoh, jika kita menyisipkan sebuah pesan kedalam sebuah dokumen, isi dari dokumen tidak akan berubah. Ini yang menjadi salah satu keunggulan metode EOF dibandingkan dengan metode steganografi yang lain. Karena disisipkan pada akhir file, pesan yang disisipkan tidak akan bersinggungan dengan isi file, hal ini menyebabkan integrasi data dari file yang disisipi tetap terjaga.

III. METODE PENELITIAN

3.1 Metode Pengumpulan Data

Dalam melakukan penelitian ini, dibutuhkan data pendukung berupa teori serta contoh kasus yang penulis kumpulkan dari beberapa sumber. Adapun metode pengumpulan data yang penulis lakukan adalah berupa teori mengenai steganografi teks dalam media citra digital dan cara kerja metode *End of File* (EOF) yang dikumpulkan dari sumber buku bacaan serta jurnal penelitian.

3.2 Analisa Sistem

Dalam perancangan perangkat lunak penyisipan teks ke dalam citra digital menggunakan metode EOF ini, dilakukan analisa terhadap cara kerja metode EOF dalam menyisipkan ke dalam teks dan membaca teks yang disisipkan di dalam teks.

Teknik ini dapat digunakan untuk menyisipkan pesan yang ukurannya sesuai dengan kebutuhan. Ukuran *file* yang telah disisipkan pesan sama dengan ukuran *file* sebelum disisipkan pesan ditambah dengan ukuran pesan yang disisipkan ke dalam *file* tersebut. Dalam teknik ini, pesan disisipkan pada akhir *file* dengan diberi tanda khusus sebagai pengenal awal dari pesan tersebut dan pengenal akhir dari data tersebut. Agar tidak menimbulkan kecurigaan, tetap harus dipertimbangkan agar pesan yang disisipkan tidak terlalu mengubah ukuran dan bentuk fisik citra pada saat ditampilkan.

3.2.1 Penerapan Metode End Of File (EOF)

Proses *embedding* atau penyisipan pesan menggunakan algoritma *End of File* adalah sebagai berikut :

1. Pilih *file* gambar yang akan disisipi.
2. Baca nilai warna pada *file* citra.
3. Inputkan teks atau pesan yang akan menjadi media di dalam citra penampung.
4. Tambahkan penanda “#” di akhir teks .
5. Ubah pesan dan penanda kedalam bentuk desimal sesuai kode ASCII.

Proses *extraction* atau pengambilan pesan rahasia dari media menggunakan algoritma *End of File* adalah sebagai berikut :

1. Pilih *file* gambar yang telah disisipkan (*stego image*).
2. Baca nilai *stego image* yang terdapat pada akhir *file* citra.
3. Ambil pesan rahasia tersebut yang terdapat pada *stego image*, yaitu di awal dan di akhir penanda “#”

Contoh proses penyisipan pesan dengan algoritma EOF adalah seperti berikut:

1. Pilih *file* gambar yang akan disisipkan pesan, misalnya :



Gambar 1. Citra Penampung

2. Kemudian kita ambil cuplikan *pixel* dari citra penampung dalam bentuk matriks berukuran 7x7 dalam bentuk desimal:

Tabel 1. Nilai pixel citra penampung 7x7 dalam bentuk desimal

| | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|
| R:255 | R:255 | R:255 | R:255 | R:255 | R:255 | R:255 |
| G:255 | G:255 | G:255 | G:255 | G:255 | G:255 | G:255 |
| B:255 | B:255 | B:255 | B:255 | B:255 | B:255 | B:255 |
| R:255 | R:255 | R:255 | R:255 | R:255 | R:255 | R:255 |
| G:255 | G:255 | G:255 | G:255 | G:255 | G:255 | G:255 |
| B:255 | B:255 | B:255 | B:255 | B:255 | B:255 | B:255 |
| R:255 | R:255 | R:255 | R:255 | R:255 | R:255 | R:255 |
| G:255 | G:255 | G:255 | G:255 | G:255 | G:255 | G:255 |
| B:255 | B:255 | B:255 | B:255 | B:255 | B:255 | B:255 |
| R:255 | R:255 | R:255 | R:255 | R:255 | R:255 | R:255 |
| G:255 | G:255 | G:255 | G:255 | G:255 | G:255 | G:255 |
| B:255 | B:255 | B:255 | B:255 | B:255 | B:255 | B:255 |

3. Kemudian pesan rahasia yang akan disisipkan adalah “#IHSAN#” yang jika direpresentasikan kedalam bentuk ASCII menjadi :

Tabel 2. Pesan dalam bentuk ASCII

| Karakter | Desimal |
|----------|---------|
| # | 35 |
| I | 105 |
| H | 104 |
| S | 115 |
| A | 97 |
| N | 110 |
| # | 35 |

4. Penyisipan data akan bertambah sebanyak 1 byte, pada algoritma *End of File* inipenyisipan dilakukan dalam bentuk decimal. Maka penyisipan diletakkan pada akhir baris *cover image* seperti pada Tabel 3.3.

Tabel 3.3 Nilai pixel setelah pesan disisipkan

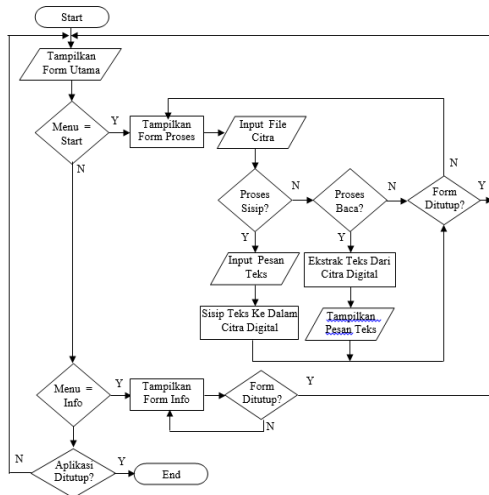
| | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|
| R=255 | R=255 | R=255 | R=255 | R=255 | R=255 | R=255 |
| G=255 | G=255 | G=255 | G=255 | G=255 | G=255 | G=255 |
| B=255 | B=255 | B=255 | B=255 | B=255 | B=255 | B=255 |
| R=255 | R=255 | R=255 | R=255 | R=255 | R=255 | R=255 |
| G=255 | G=255 | G=255 | G=255 | G=255 | G=255 | G=255 |
| B=255 | B=255 | B=255 | B=255 | B=255 | B=255 | B=255 |
| R=255 | R=255 | R=255 | R=255 | R=255 | R=255 | R=255 |
| G=255 | G=255 | G=255 | G=255 | G=255 | G=255 | G=255 |
| B=255 | B=255 | B=255 | B=255 | B=255 | B=255 | B=255 |
| R=255 | R=255 | R=255 | R=255 | R=255 | R=255 | R=255 |
| G=255 | G=255 | G=255 | G=255 | G=255 | G=255 | G=255 |
| B=255 | B=255 | B=255 | B=255 | B=255 | B=255 | B=255 |
| R=255 | R=255 | R=255 | R=255 | R=255 | R=255 | R=255 |
| G=255 | G=255 | G=255 | G=255 | G=255 | G=255 | G=255 |
| B=255 | B=255 | B=255 | B=255 | B=255 | B=255 | B=255 |
| R=35 | R=105 | R=97 | R=35 | R=0 | R=0 | R=0 |
| G=35 | G=104 | G=110 | G=35 | G=0 | G=0 | G=0 |
| B=35 | B=115 | B=0 | B=35 | B=0 | B=0 | B=0 |

3.3 Rancangan Penelitian

Dalam perancangan perangkat lunak penyisipan teks ke dalam citra digital menggunakan metode EOFini, tahapan perancangan yang dilakukan terbagi menjadi dua bagian, yaitu rancangan proses serta rancangan antarmuka program.

3.3.1 Rancangan Proses

Berdasarkan hasil analisa sistem yang dilakukan, dirancang sebuah alur proses yang akan digunakan dalam perancangan aplikasi. Adapun bentuk rancangan *flowchart* proses pengambilan keputusan pada sistem yang dirancang ini seperti terlihat pada Gambar 2.



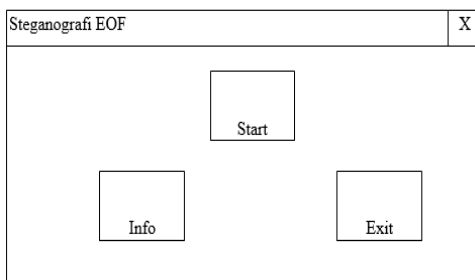
Gambar 2. Flowchart proses kerja

3.3.2 Rancangan Antarmuka

Setelah merancang proses kerja perangkat lunak yang akan dirancang, selanjutnya dilakukan perancangan terhadap antarmuka perangkat lunak ini. Dalam perancangan ini, penulis merancang tiga form yang dapat digunakan pengguna untuk berinteraksi dengan perangkat lunak yang dirancang.

1. Rancangan Form Utama

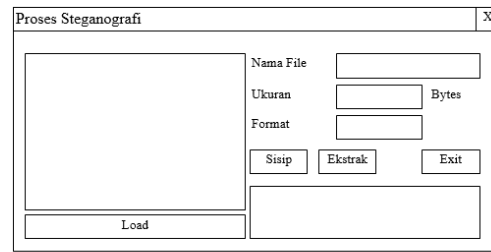
Form Utama adalah form yang dirancang untuk menampilkan pilihan menu dan menerima inputan pilihan menu dari pengguna. Gambar 3.2 menunjukkan bagaimana bentuk rancangan form Utama yang digunakan di dalam aplikasi yang dirancang.



Gambar 3. Rancangan Form Utama

2. Rancangan Form Proses

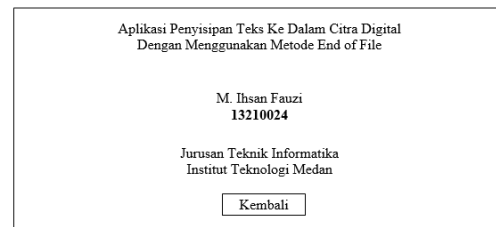
Form Proses adalah form yang dirancang untuk menerima inputan spesifikasi komponen *smartphone* yang dipilih pengguna dalam mencari varian *smartphone* yang diinginkan serta menampilkan hasil pilihan varian *smartphone* dari proses pencarian yang dilakukan. Gambar 4 menunjukkan bagaimana bentuk rancangan form Proses yang digunakan di dalam aplikasi yang dirancang.



Gambar 4. Rancangan Form Proses

3. Rancangan Form Info

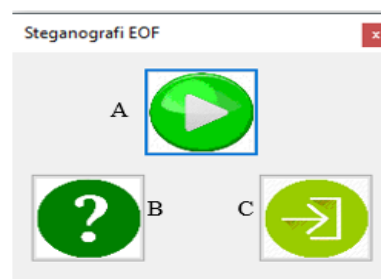
Form Info merupakan tampilan yang dirancang untuk menampilkan informasi mengenai perancang aplikasi penyisipan teks ke dalam citra digital dengan menggunakan metode EOF ini. Gambar 5 menunjukkan bagaimana bentuk rancangan form Info yang digunakan di dalam aplikasi yang dirancang.



Gambar 5. Rancangan Form Info

4. Implementasi Perangkat Lunak

Tampilan pertama program begitu dijalankan adalah seperti Gambar 6.



Gambar 6. Tampilan Form Utama

Gambar 6 Merupakan Form Utama dari aplikasi Penyisipan Pesan Menggunakan Metode EOF, terlihat pada gambar 4.1 ada tiga buah tombol yaitu:

1. Tombol A ini berfungsi untuk masuk ke form utama.
2. Tombol B ini berfungsi untuk masuk ke form info penulis.
3. Tombol C ini berfungsi untuk keluar dari aplikasi.

Tampilan Form Info

Untuk pengujian pertama penulis akan menekan tombol info dan akan mengeluarkan hasil seperti gambar dibawah ini.



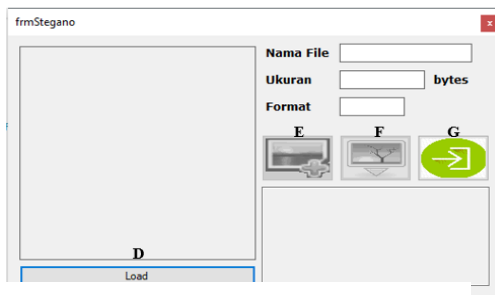
Gambar 4.2 Form Info Penulis

Gambar 7. Form Info penulis

Gambar 7 merupakan form yang menampilkan informasi mengenai penulis dan informasi lainnya dan berikutnya adalah menekan tombol yang digunakan untuk menampilkan form penyisipan pesan.

Tampilan Proses Penyisipan Pesan

Setelah menekan tombol tersebut akan muncul form penyisipan pesan seperti Gambar 8.



Gambar 8. Tampilan Form Utama

Pada Gambar 8 merupakan Aplikasi Penyisipan Pesan Pada Citra Digital Menggunakan Metode End Of File, di form ini terdapat 4 tombol yaitu;

1. Tombol D untuk mengload gambar yang akan di sisipkan pesan.
2. Tombol E untuk memasukkan tesk yang akan disisipkan.
3. Tombol F untuk membaca pesan yang telah disisipkan.
4. Dan terakhir tombol C yang berfungsi untuk kembali ke form sebelumnya.

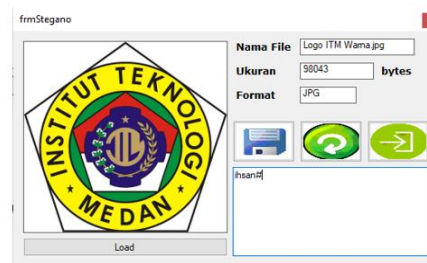
Kemudian untuk menjalankan aplikasi ini dengan cara menekan tombol Load, tombol tersebut berfungsi mengload gambar yang akan disisipkan pesan. Contoh penulis akan memasukkan logo Institut Teknologi Medan untuk disisipkan pesan ke dalam gambar tersebut dan hasilnya sebagai berikut:



Gambar 4.4 Load Gambar yang akan disisipkan

Gambar 9. Load gambar yang akan disisipkan

Pada Gambar 9, gambar berhasil di Load. Untuk melakukan penyisipan pesan maka tekan tombol memasukkan pesan, setelah menekan tombol tersebut, penulis akan memasukkan kata Ihsan# untuk disisipkan dan akan terlihat seperti berikut:



Gambar 4.5 Proses Penyisipan Pesan

Gambar 10. Proses penyisipan pesan

Gambar 10 adalah proses penyisipan pesan, setelah itu silahkan tekan tombol simpan untuk menyimpan pesan ke dalam gambar.

Setelah tombol simpan ditekan, terdapat tiga pilihan format gambar yang dapat disave dan pilih lokasi gambar akan disave. Penulis akan memilih format gambar JPG dan membuat nama gambar tersebut menjadi Logo ITM dan menekan tombol Save. Pesanpun berhasil disisipkan pada gambar tersebut.

Tampilan Proses Ekstraksi Pesan

Selanjutnya penulis akan membaca pesan yang telah disisipkan sebelumnya. Cara yang dilakukan untuk membaca pesan yang telah disisipkan dengan cara menload gambar yang sudah penulis simpan sebelumnya.

Pengaruh yang akan terjadi pada gambar ialah:

1. Size yang akan bertambah sesuai panjangnya pesan yang disisipkan. Semakin panjang pesan yang disisipkan, maka semakin besar pula size gambarnya.
2. Terdapat garis lurus berwarna hitam horizontal di akhir gambar.

Pembuktian Metode End Of File

Penulis membuktikan metode end of file telah diterapkan dan pesan telah disisipkan ke dalam gambar dengan menggunakan Aplikasi Matlab dengan cara sebagai berikut:

1. Open Mantab R12



Gambar 4.9 Aplikasi Matlab

2. Setelah terbuka, Pilih APPS > Image Viewer
3. Kemudian Pilih File > Open, dan masukan gambar yang telah di sisipkan pesan.
4. Setelah itu Pilih Tools > Pixel Region.
5. Scrol hingga kebawah, maka kode RGB di pixel paling bawah telah berubah dari ASCII ke DEX

IV. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Dengan diselesaikannya penelitian ini yang mencakup Aplikasi Penyisipan Pesan Pada Citra Digital Menggunakan Metode End Of File maka kesimpulannya sebagai berikut:

1. Aplikasi yang penulis buat mampu untuk menyembunyikan pesan kedalam citra digital dengan baik. Hasil dari proses *encode* menjadi pesan tersembunyi kedalam citra tanpa mendapatkan perubahan yang berarti, hanya saja jika ukuran file kecil akan terdapat garis lurus horizontal di akhir gambar.
2. Aplikasi yang dibuat dapat membaca pesan secara utuh yang sebelumnya telah dilakukan proses *encode*.

4.2 Saran

Adapun saran yang dapat disampaikan dalam pengembangan sistem ini untuk masa yang akan datang sebagai berikut:

1. Aplikasi ini dapat dikembangkan lebih lanjut dengan menambahkan proses *cryptography* untuk pengacakan pesan sebelum di *encoe* ke media untuk meningkatkan keamanan pesan.
2. Untuk pengembangan lebih lanjut, aplikasi ini dapat digunakan metode selain EOF (*End Of File*), sehingga dapat dibandingkan kelemahan dan kelebihan dari masing masing metode tersebut.

DAFTAR PUSTAKA

- [1.] Arfiyah, 2013, *Perbandingan Teknik Steganografi Dengan Metode First-Of-File, End-Of-File Dan Kombinasi First-Of-File Dan End-Of-File Pada File Bitmap*, Universitas Sumatra Utara.
- [2.] Christopher Lee, 2014, *Buku Pintar Pemrograman Visual Basic 2010*, Jakarta : Elex Media Komputindo.
- [3.] Michael Sitorus, 2016, *Aplikasi Keamanan Data dengan Teknik Steganografi Menggunakan Metode End Of File*. ISSN: 2477-5894.

- [4.] Mukharrom Edisuryana, R. Rizal Isnanto, Maman Somantri: *Aplikasi Steganografi pada Citra Berformat Bitmap Dengan Menggunakan Metode End Of File*, Universitas Diponegoro Semarang.
- [5.] Martono, Irawan, 2014, *Penggunaan Steganografi dengan Metode End Of File (EOF) Pada Digital Watermarking*. Universitas Budi Luhur.
- [6.] Michael Sitorus, 2016, *Aplikasi Keamanan Data dengan Teknik Steganografi Menggunakan Metode End Of File*. ISSN: 2477-5894.
- [7.] Mukharrom Edisuryana, R. Rizal Isnanto, Maman Somantri: *Aplikasi Steganografi pada Citra Berformat Bitmap Dengan Menggunakan Metode End Of File*, Universitas Diponegoro Semarang.
- [8.] Martono, Irawan, 2014, *Penggunaan Steganografi dengan Metode End Of File (EOF) Pada Digital Watermarking*. Universitas Budi Luhur.
- [9.] Putra Darma, 2010, *Pengolahan Citra Digital*, Yogyakarta : ANDI.
- [10.] Rahmad Zainul Abidin, *Penerapan Metode Steganografi End Of File Untuk Menyisipkan Pesan File Pada Gambar Digital*, Universitas Yudharta Pasurua
- [11.] Rinaldi Munir, *Pengolahan Citra Digital*, Bandung : Informatika Bandung.
- [12.] Rahmad Zainul Abidin, *Penerapan Metode Steganografi End Of File Untuk Menyisipkan Pesan File Pada Gambar Digital*, Universitas Yudharta Pasurua.
- [13.] Rinaldi Munir, *Pengolahan Citra Digital*, Bandung : Informatika Bandung <http://informatika.stei.itb.ac.id/~rinaldi.munir>
- [14.] Yogie Aditya, Andhika Pratama dan Alfian Nurlifa, 2010, *Studi Pustaka Untuk Steganografi dengan Beberapa Metode*, Yogyakarta. ISSN: 1907-5022.
- [15.] Yayuk Anggraini, Dolly Virgian Shaka Yudha Sakti, 2014, *Penerapan Steganografi Metode End Of File (EOF) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Mengamanan Data Gambar Bermasis Java Programming*, Universitas Budi Luhur.
- [16.] Yogie Aditya, Andhika Pratama dan Alfian Nurlifa, 2010, *Studi Pustaka Untuk Steganografi dengan Beberapa Metode*, Yogyakarta. ISSN: 1907-5022.
- [17.] Yayuk Anggraini, Dolly Virgian Shaka Yudha Sakti, 2014, *Penerapan Steganografi Metode End Of File (EOF) Dan Enkripsi Metode Data Encryption Standard (Des) Pada Aplikasi Mengamanan Data Gambar Bermasis Java Programming*, Universitas Budi Luhur.

