APLIKASI STEGANOGRAFI PADA CITRA BERFORMAT BITMAP DENGAN MENGGUNAKAN METODE *END OF FILE*

Mukharrom Edisuryana[*)], R. Rizal Isnanto, and Maman Somantri

Jurusan Teknik Elektro, Universitas Diponegoro Semarang
Jl. Prof. Sudharto, SH, Kampus UNDIP Tembalang, Semarang 50275, Indonesia

[*)]*E-mail:edisuryana09@gmail.com*

Abstrak

Meningkatnya perkembangan komunikasi data mengakibatkan aspek keamanan dan kerahasiaan informasi menjadi sangat penting.Informasi yang bersifat rahasia rentan dicuri oleh orang yang tidak berhak.Pengamanan data dapat dilakukan dengan menerapkan teknik kriptografi dan steganografi.Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita atau informasi.Sedangkan steganografi adalah ilmu dan seni menyembunyikan pesan ke dalam suatu wadah.Wadah dapat berupa gambar, berkas audio, atau berkas video.Kedua teknik tersebut dapat digabungkan sehingga menghasilkan sistem keamanan data yang tinggi. Dalam penelitian ini diimplementasikan teknik kriptografi dan steganografi pada citra berformat bitmap dengan menggunakan metode End Of File (EOF).Kriptografi berfungsi untuk mengacak pesan asli (plaintext) dan mendapatkan pesan acak/tersandi (ciphertext) sebelum disisipkan ke dalam citra.Metode kriptografi yang digunakan adalah Caesar Cipher dan Zig-zag Cipher.Aplikasi dibuat dengan menggunakan perangkat MATLAB R2008a.Aplikasi berbasis GUI dan berjalan pada sistem operasi Windows. Berdasarkan penggunaan aplikasi, didapatkan hasil bahwa pesan yang disisipkan dengan metode End Of File (EOF) menghasilkan garis baris baru di akhir citra asli. Semakin banyak pesan yang disisipkan akan semakin banyak pula garis yang muncul. Pembatasan pesan adalah cara agar citra yang disisipi pesan tidak jauh berubah. Manipulasi citra stego dapat dilakukan dengan syarat tidak mengganggu piksel pesan yang disisipkan berada.

Kata kunci : kriptografi, steganografi, citra, EOF

Abstract

Advancement of data communication making security and confidentiality of the information to be very important. Confidential information is vulnerable to be stolen by unauthorized person. Data security can be done by applying cryptography and steganography techniques. Cryptography is the science and art to keep confidentiality of news or information. While steganography is the science and art of hiding messages into a container. The container can be an image, audio file, or video file. Both techniques can be combined to produce a system with high level security data.
In this final project will be implemented cryptography and steganography technique on a bitmap image with End Of File (EOF) method. Cryptography is used to randomized the original messages (plaintext) and generate a random messages/encrypted (ciphertext) before inserted into image. The cryptography methods used in this final project are Caesar Cipher and Zig-zag Cipher. The application created using MATLAB R2008a. The application is based on GUI and running on Windows operating system. Based on application usage, showed that message is inserted using End Of File (EOF) method generate a new line at the end of original image. The more messages that are inserted into an image, more new line will appear. Limiting the messages is the way to maintain the generated image from changing to much. Stego image manipulation can be done with the requirement of not changing pixel where the message is inserted.

Keywords : cryptography, steganography, image, EOF

1. Pendahuluan

Berkembangnya ilmu pengetahuan dalam dunia informatika memungkinkan pengamanan data dari ancaman yang ada. Sebagai contoh adalah kriptografi, yaitu ilmu yang digunakan untuk menjaga keamanan dari pihak yang tidak memiliki hak akses terhadap suatu data, baik data berupa *e-mail*, dokumen, maupun berkas pribadi[8]. Namun disisi lain kriptografi dapat menimbulkan kecurigaan pada orang yang membaca data terenkripsi. Kecurigaan ini dapat memicu orang untuk memecahkan enkripsi tersebut walau membutuhkan waktu yang cukup lama. Teknik lain sebagai upaya pengamanan data adalah steganografi.

Steganografi adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang.Perkembangan steganografi dengan beberapa metode yang ada menjadi alternatif pengamanan dalam pertukaran data dalam internet.Steganografi berbeda dengan kriptografi. Kriptografi akan menyamarkan suatu pesan menjadi sesuatu yang sulit dibaca atau dimengerti. Karakter aneh atau susunan huruf yang sulit dibaca tersebut dapat mengundang kecurigaan orang.Sedangkan steganografi lebih cenderung untuk mengurangi kecurigaan orang karena pesan yang dirahasiakan disembunyikan dalam suatu media. Media penampung dapat berupa berkas audio[13], video[5], citra[10][15], dan lain sebagainya.

Tujuan dari penelitian ini adalah untuk menghasilkan algoritma dan penerapan program steganografi metode *End of File* (EOF) dengan perangat MATLAB R2008a serta menguji tingkat perubahan yang dialami citra yang telah disisipkan pesan di dalamnya.

Penulisan penelitian ini memiliki batasan pada permasalahan berikut :

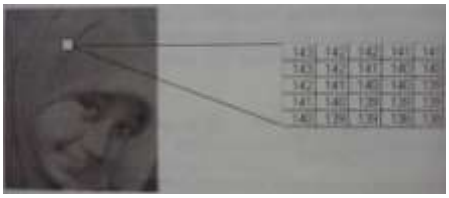
1. Penyembunyian pesan rahasia dilakukan dengan metode *End of File* (EOF).
2. Berkas atau pesan rahasia yang disembunyikan berupa teks (ekstensi *.txt).
3. Citra yang digunakan sebagai citra pembawa atau citra stego merupakan citra warna dalam format bitmap (ekstensi *.bmp).
4. Tidak mmbahas tentang teknik kompresi citra.
5. Aplikasi berjalan pada Sistem Operasi Windows 7 Profesional 32 bit, dibuat dengan menggunakan perangkat MATLAB R2008a.
6. Pengujian tingkat perubahan citra yang telah disisipkan data dengan bantuan perangkat lunak ACDSee Pro 4. Pengujian dilakukan dengan variasi pengubahan ukuran *(resize),* pemotongan citra (*cropping*), pemberian efek pada citra (efek *Sunspot*), pengaburan citra *(bluring),* dan perputaran citra (*rotation).*

2. Metode

2.1 Citra Digital

Citra digital dapat dinyatakan sebagai suatu fungsi dua dimensi *f(x,y),* dengan *x* maupun *y* adalah posisi koordinat sedangkan f merupakan amplitudo pada posisi *(x,y)* yang sering dikenal sebagai intensitas atau *grayscale*[11].

Resolusi piksel merupakan perhitungan jumlah piksel dalam sebuah citra digital. Sebuah citra dengan tinggi *N* piksel dan lebar *M* piksel berarti memiliki resolusi sebesar *N x M*[10]. Citra digital *N x M* mempunyai *NM* buah piksel.Citra keabuan (*grayscale*) merupakan citra yang hanya memiliki satu nilai kanal pada setiap pikselnya, dengan kata lain nilai bagian *RED = GREEN = BLUE*.Jumlah warna pada citra keabuan adalah 256, karena citra keabuan jumlah bitnya adalah 8, sehingga jumlah warnanya adalah $2^8 = 256$, nilainya berada pada jangkauan 0-255.



Gambar 1.Contoh citra digital aras keabuan[11]

Citra berwarna (*color images*) dikenal dengan nama citra spectral, karena warna pada citra disusun oleh tiga komponen warna yang disebut komponen RGB, yaitu merah (*red*), hijau (*green*), dan biru (*blue*).Jumlah warna untuk citra RGB adalah dengan mengalikan jumlah pada masing-masing komponennya, jumlah dari tiap komponennya R=256 (8bit), G=256 (8bit), dan B=256 (8bit). Jumlah warna RGB adalah sejumlah $2^8 * 2^8 * 2^8 = 256 \times 256 \times 256 = 16777216$. Sehingga jumlah byte yang diperlukan untuk berkas citra jenis RGB adalah 3 kali ukuran berkas citra jenis skala keabuan (*gray scale*)[11].

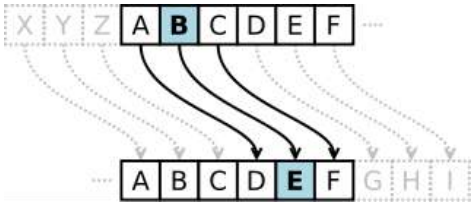
Gambar 2. Contoh citra digital RGB[11]

Berkasbitmap (*.bmp) merupakan format berkascitra yang tidak mengalami proses kompresi, sehingga kualitas gambar yang dihasilkan baik dari pada berkas citra dengan format lain.

2.2 Kriptografi

Kriptografi adalah ilmu yang digunakan untuk menjaga keamanan dari pihak yang tidak memiliki hak akses terhadap suatu data, baik data berupa *e-mail*, dokumen, maupun berkas pribadi[16].Pada PENELITIAN ini digunakan 2 (dua) metode kriptografi, yaitu metode *Caesar Cipher* dan *Zig-zag Cipher*. *Caesar Cipher* juga dikenal sebagai *shift cipher*, sandi geser, kode Caesar, atau pergeseran Caesar. Sandi ini termasuk dalam sandi substitusi dimana setiap huruf dalam pesan asli (*plaintext*) diganti dengan huruf yang berselisih angka tertentu dalam

alfabet[17].Analogi Caesar Cipher dapat ditunjukkan pada Gambar 3.



Gambar 3. Analogi *Caesar Cipher*[17]

Contoh Caesar Cipher :
Pesan asli *(plaintext)*: "we will meet at mid nigth"
Kunci = 11
Berarti dari kalimat di atas akan mendapatkan angka dari setiap huruf sebagai berikut:

22 4 22 8 11 11 12 4 4 19 0 19 12 8 3 13 8 6 7 19

Cara mendapatkan pesan tersandi (*ciphertext*) dengan kunci 11 yaitu dengan menambahkan setiap nilai dari pesan asli (*plaintext*) dengan kunci 11 maka akan didapatkan:

7 15 7 19 22 22 23 15 15 4 11 4 23 19 14 24 19 17 18 4

Jika lebih dari 20 setelah ditambah dengan kunci maka akan dikurangi dengan 26 seperti 22+11= 33 – 26 = 7. Setelah diubah menjadi huruf akan mendapatkan pesan tersandi (*ciphertext*) :

"HPHTWWXPPELEXTOYTRSE"

Metode *Caesar Cipher* yang digunakan menggunakan prinsip modulo 26.

Dalam MATLAB, fungsi modulo dapat dilakukan dengan menuliskan fungsi '*mod*' atau '*rem*'. x merupakan pesan asli yang akan disandikan dan kunci yang digunakan pada saat enkripsi sama dengan kunci dekripsi.

Pada metode *Zig-zag Cipher* pada prinsipnya pesan yang akan dikirimkan ditulis per baris sebanyak baris yang ditentukan (sesuai dengan nilai n-nya). Sebelumnya karakter disusun dalam posisi baris dan kolom dengan urutan penyusunan :

1. baris ke-1 dengan penyusunan karakter dengan menggunakan jeda ke-1 = 2*n baris-2 dan jeda 2 = 0.
2. baris ke-2 dengan penyusunan karakter menggunakan jeda ke-1 yang sebelumnya dikurangi 2 dan jeda ke-2 dengan sebelumnya menambah nilai jeda ke-2 dengan 2, demikian seterusnya sampai baris ke-n. Ilustrasi :

Plaintext = $a_1a_2a_3a_4\ldots a_n$
Dikirim menggunakan metode zig-zag:n baris

Pesan yang akan dikirimkan ditulis per baris dari pola :

a_1 a_{n+3} dst
a_2 a_{n+2}
… a_{n+1}
a_n

Sehingga pesan tersandi (*ciphertext*) menjadi = a_1 a_{n+3} a_2 a_{n+2} … a_{n+1} a_n.

2.3 Steganografi

Steganografi (*steganography*) adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang.Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video[7].

Ada beberapa metode yang dapat digunakan untuk menyisipkan suatu pesan, diantaranya adalah[2]:

1. Metode LSB (*Least Significant Bit*)

Metode ini bekerja dengan cara mengganti bit terakhir dari masing-masing piksel dengan pesan yang akan disisipkan.LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekurangannya adalah pesan/data yang akan disisipkan terbatas, sesuai dengan ukuran citra. Selain itu, kualitas citra akan sedikit berubah setelah mengalami proses penyisipan pesan. Namun perubahan yang sedikit itu biasanya tidak nampak oleh mata.

2. Metode *End of File* (EOF)

Metode ini merupakan metode pengembangan LSB.Dalam metode ini pesan disisipkan diakhir berkas.Pesan yang disisipkan dengan metode ini jumlahnya tidak terbatas.Akan tetapi efek sampingnya adalah ukuran berkas menjadi lebih besar dari ukuran semula. Ukuran berkas yang terlalu besar dari yang seharusnya, tentu akan menimbulkan kecurigaan bagi yang mengetahuinya. Misalnya pada sebuah citra skala keabuan 6x6 piksel 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 biner 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[7] [4] :

1. Tidak dapat dipersepsi (*Impercepbility*)

Keberadaan data rahasia tidak dapat dipersepsi oleh indera manusia.Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli saat dilihat dengan mata.Begitu pula dengan suara, telinga haruslah mendapati tidak ada perbedaan antara suara asli dan suara yang telah disisipi.

2. Ketepatan (*Fidelity*)

Kualitas citra penampung tidak jauh berubah setelah penyisipan data rahasia.Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

3. Kapasitas (Capacity)

Berhubungan dengan jumlah informasi yang dapat disisipkan ke dalam media penampung.

4. Ketahanan (*Robustness)*

Data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung.

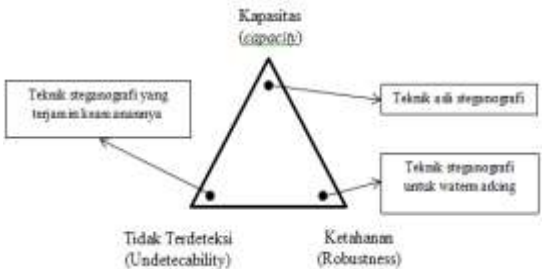
5. Tidak terdeteksi (*Undetecability*)

Kemampuan untuk menghindari deteksi oleh indera manusia maupun analisis statistik.

6. Pemulihan (*Recovery)*

Data yang disembunyikan harus dapat diungkapkan kembali (*reveal*).

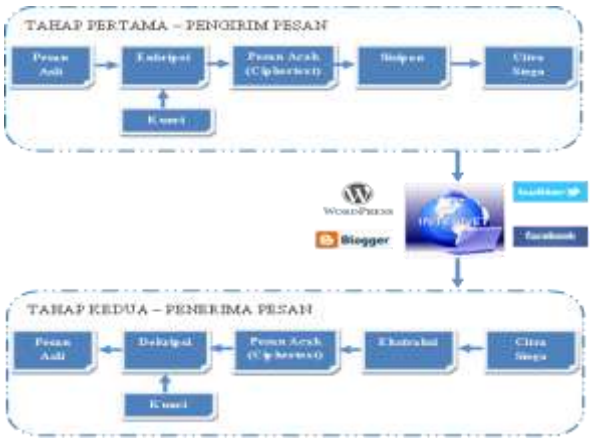
Dalam melakukan proses steganografi, ada beberapa faktor yang saling berkompetisi satu sama lain (*trade-off*), artinya saat salah satu faktor ditingkatkan maka kemungkinan faktor lain akan mengalami penurunan. Faktor yang saling berkompetisi tersebut dapat ditunjukkan pada Gambar 4.



Gambar 4 Faktor yang saling berkompetisi (*trade-off*)[4]

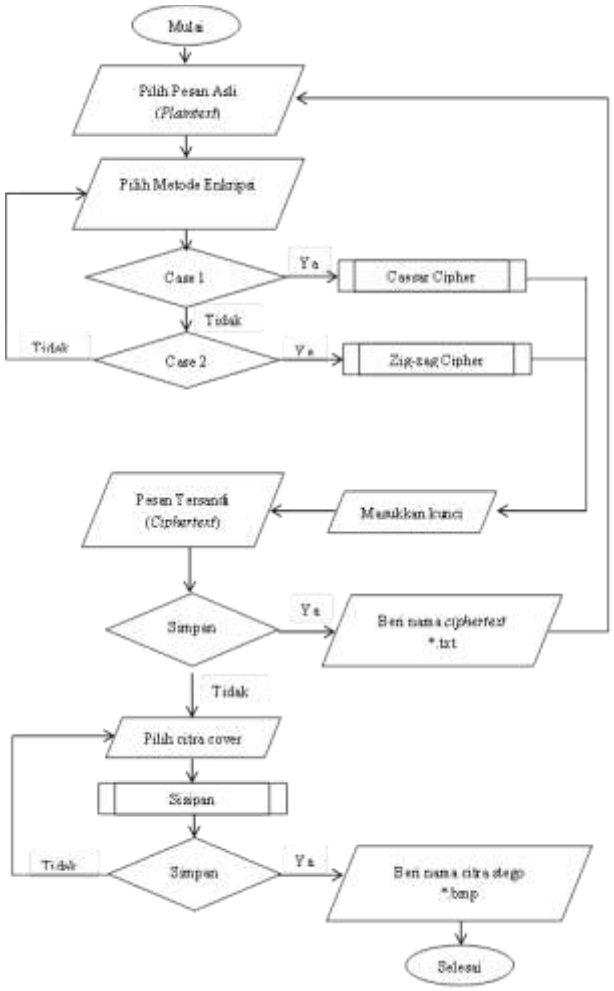
2.4 Perancangan Sistem

Terdapat 2 (dua) tahap dalam perancangan sistem ini.Tahap pertama yaitu tahap yang dilakukan oleh seorang pengirim pesan rahasia. Pengirim yang akan mengirimkan pesan terlebih dahulu melakukan penyandian (enkripsi) terhadap pesan yang dimilikinya. Keluaran dari tahap ini adalah berupa pesan acak yang telah tersandikan dengan menggunakan metode *Caesar Cipher* atau dengan metode *Zig-zag Cipher*.Selanjutnya pengirim melakukan penyisipan pesan acak ke dalam citra. Proses ini dinamakan proses sisipan. Dalam proses ini diperoleh citra stego yang sudah termuat pesan acak di dalamnya.Tahap kedua adalah tahap yang dilakukan oleh penerima pesan rahasia. Penerima yang telah menerima citra stego dapat mendeteksi pesan yang ada di dalamnya dengan proses ekstraksi. Setelah pesan berhasil dipisahkan dari citra stego, penerima harus menerjemahkan (dekripsi) agar pesan acak yang dimiliki dapat dimengerti maknanya. Dalam proses dekripsi ini penerima harus mengetahui kunci rahasia yang sebelumnya telah ditentukan oleh pengirim. Bagan umum dari sistem steganografi yang akan dibangun dapat ditunjukkan pada Gambar 5.



Gambar 5 Bagan umum sistem

Alur sistem yang dilakukan pengirim dapat dilihat pada diagram alir seperti ditunjukkan pada Gambar 6.



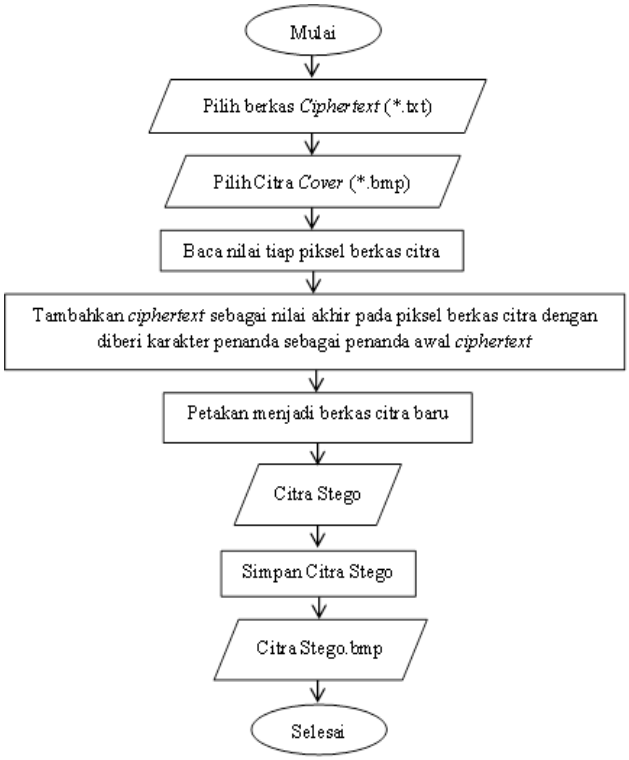
Gambar 6 Bagan alir gambaran umum pengirim

Metode *Caesar Cipher* yang digunakan menggunakan prinsip modulo 26. Secara matematis dapat dituliskan sebagai berikut[19] :

cipher = rem ((x+kunci-97,26)+97)(3.1)

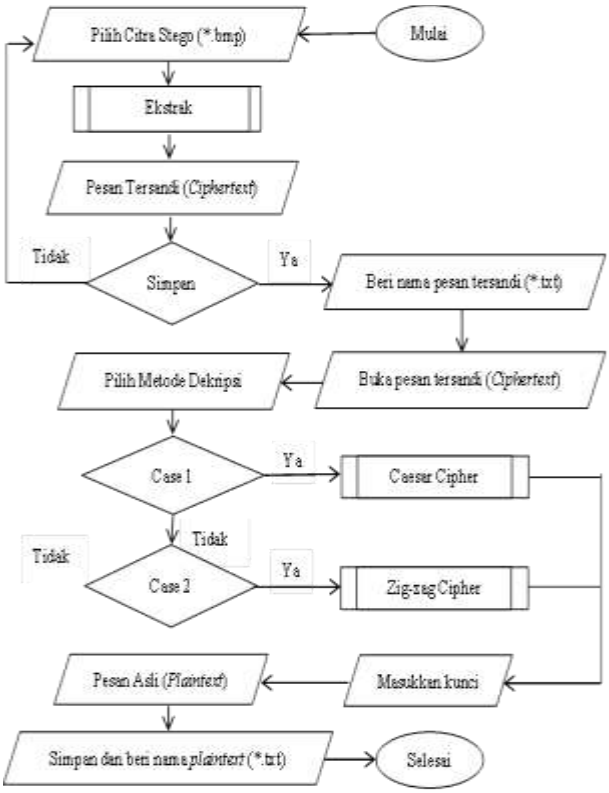
Dalam MATLAB, fungsi modulo dapat dilakukan dengan menuliskan fungsi '*mod*' atau '*rem*'. x merupakan pesan asli yang akan disandikan dan kunci yang digunakan pada saat enkripsi sama dengan kunci dekripsi.*Caesar Cipher* terbatas pada penyandian huruf alfabet dari 'a' hingga 'z' dimana dalam ASCII berada pada posisi 97 sampai 122.Mengurangkan 97 diterjemahkan ke dalam kisaran 0 sampai 25 (0 sebagai 'a' hingga 25 sebagai 'z').Kunci digunakan sebagai pergeseran dan mengambil sisanya pada pembagian dengan bilangan 26 melalui fungsi '*rem*' (modulo 26).Menambah 97 diterjemahkan kembali pada kisaran 97 sampai 122.

Pada metode *Zig-zag Cipher p*esan yang mengandung spasi bisa langsung dilakukan enkripsi, namun dengan syarat kunci yang dipilih harus lebih besar atau sama dengan 2 (dua) hingga maksimal panjang karakter pesan. Misal pada pesan 'bismillah, sukses'.Pesan tersebut terdapat 17 karakter.Sehingga kunci yang dipilih harus berada pada rentang 2 sampai dengan 17.Tidak boleh kurang dari 2 ataupun lebih dari 17**.**Kombinasi antara *cipher* substitusi (*Caesar Cipher*)dan *cipher* transposisi (*Zig-zag Cipher*) akan memperoleh *ciphertext* baru yang lebih kuat (super) dari pada hanya menggunakan satu *cipher* saja. Keadaan *ciphertext* yang seperti ini disebut dengan *Super Enkripsi*[3]. Bagan alir dari Sisipandapat dilihat pada Gambar 7.



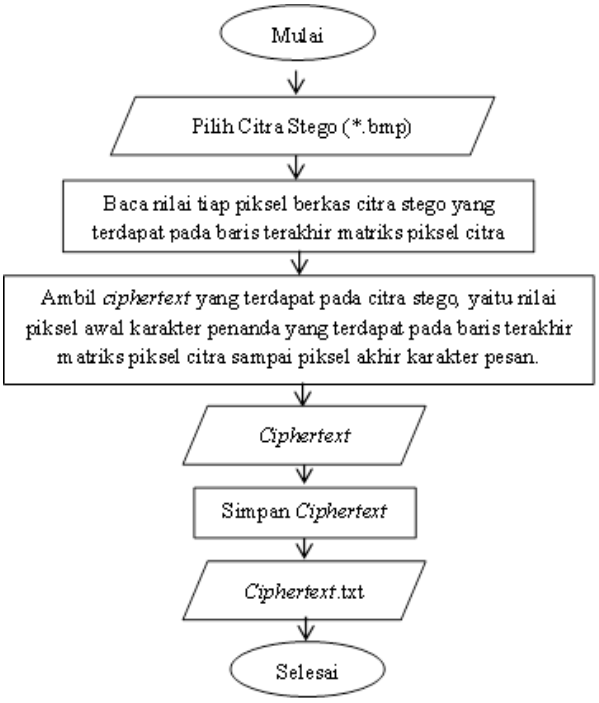
Gambar 7 Bagan alir Sisipan

Alur sistem yang dilakukan oleh penerima dapat dilihat pada diagram alir seperti ditunjukkan pada Gambar 8.



Gambar 8 Bagan alir gambaran umum penerima

Bagan alir dari Ekstrakdapat dilihat pada Gambar 9.



Gambar 9 Bagan alir Ekstrak

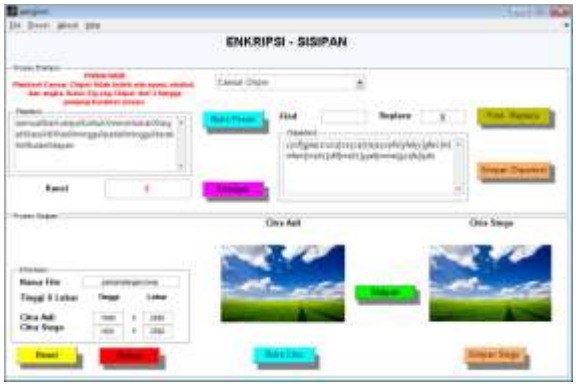
3. Hasil dan Analisa

Program dibagi menjadi 2 (dua) bagian utama, yaitu program GUI Enkripsi - Sisipan dan GUI Ekstrak - Dekripsi. GUI Enkripsi - Sisipan digunakan oleh seorang pengirim untuk menyandikan pesan asli agar pesan yang nantinya akan disisipkan berubah menjadi karakter acak yang susah dimengerti. Selanjutnya karakter acak akan disisipkan dalam citra berformat bitmap dengan metode *End of* File (EOF) untuk menghasilkan citra stego.

GUI Ekstrak - Dekripsi digunakan oleh seorang penerima untuk mengambil kembali pesan/karakter acak yang berada dalam citra stego. Pesan yang berhasil dipisahkan akan didekripsikan untuk menghasilkan pesan asli yang dapat dimengerti maknanya.

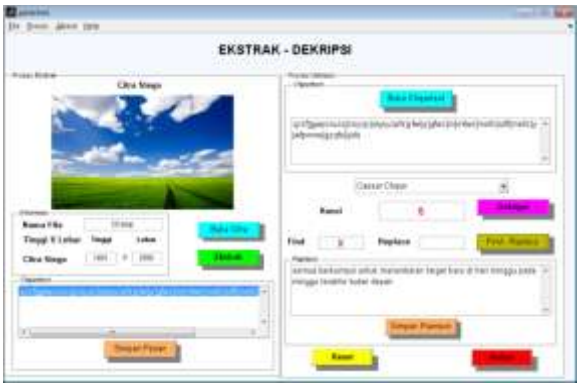
Seorang pengirim harus memastikan metode enkripsi apa yang akan digunakan beserta kuncinya. Metode dan kunci yang digunakan enkripsi nantinya akan digunakan kembali pada saat seorang penerima pesan melakukan dekripsi.

Tampilan dari cara mengenkripsi pesan asli (*plaintext*) untuk mendapatkan pesan tersandi (*ciphertext*) dan menyisipkannya ke dalam suatu citra bitmap dapat dilihat pada Gambar 10.



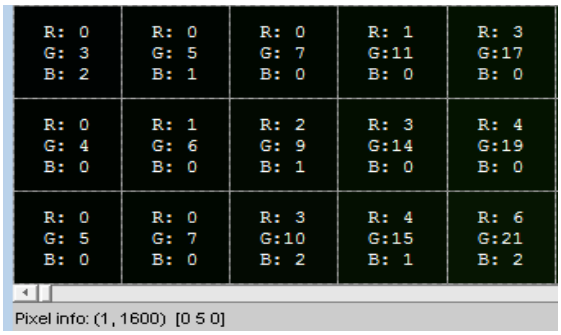
Gambar 10 Tampilan pengujian penyisipan pesan dengan enkripsi *Caesar Cipher*

Tampilan dari cara mengekstraksi pesan dari citra stego hingga proses dekripsi untuk mendapatkan pesan asli (*plaintext*) dapat dilihat pada Gambar 11.

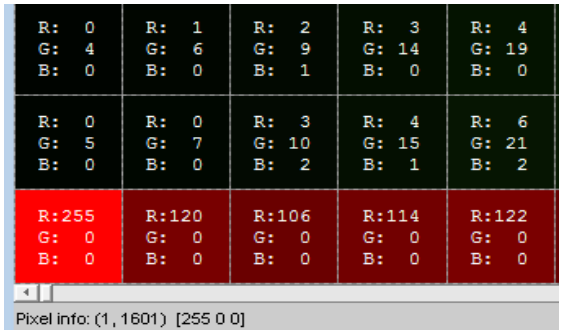


Gambar 11 Tampilan pengujian ekstrak pesan dandekripsi *Caesar Cipher*

Citra asli dengan citra *stego* merupakan citra yang sama. Namun terdapat sedikit perbedaan diantara keduanya.Perbedaan itu dapat ditunjukkan pada piksel akhir citra Gambar 12 dan Gambar 13.



Gambar 12 Piksel citra asli sebelum penyisipan



Gambar 13 Piksel citra stego setelah penyisipan

Ciri dari citra stego dengan metode *End of File* (EOF) adalah terdapat tambahan baris berupa garis-garis pada baris paling bawah piksel citra. Jika dilihat pada piksel citra stego, maka akan terlihat tambahan piksel baru yang mengisi kanal merah (*Red*) di akhir baris piksel citra asli. Baris ini mengandung pesan yang disipkan pada saat proses sisipan steganografi dengan metode *End of File* (EOF).

Pada program ini dilengkapi juga menu About dan Help. Halaman menu About berisikan informasi tentang sistem dan pembangun sistem (*programmer*), sedangkan menu Help merupakan halaman yang berisikan panduan dalam menggunakan sistem.

Pengujian citra stego dilakukan dengan berbagai macam manipulasi.Citra stego yang digunakan merupakan citra yang disisipi pesan sebanyak 92 karakter.Manipulasi pengubahan ukuran citra (*resize*) dengan dua puluh kali pengujian mendapatkan hasil yang buruk.Manipulasi citra stego dengan pengubahan ukuran citra (*resize*) akan mengakibatkan pesan yang disisipkan di dalam citra akan hancur sehingga pada proses ekstraksi, pesan tidak dapat dimunculkan kembali/tidak dapat dipulihkan seperti semula.

Manipulasi pemotongan citra (*cropping*) dilakukan dengan empat kali pengujian, yaitumanipulasi pemotongan setengah bagian atas, setengah bagian kanan, setengah bagian bawah, dan setengah bagian kiri. Berdasarkan hasil pengujian, diketahui bahwa apabila pemotongan dilakukan pada daerah yang mengandung pesan maka pesan yang terdapat di dalam citra stego tersebut tidak akan dapat terdeteksi/tidak dapat dimunculkan kembali. Namun apabila pemotongan citra dilakukan di luar daerah yang mengandung pesan, maka tidak akan ada masalah. Pesan masih tetap utuh dan dapat dimunculkan kembali.

Manipulasi pemberian efek *Sunspot* pada dasarnya adalah citra diberikan cahaya terang seperti adanya sebuah matahari yang menyinari.*Sunspot* diletakkan pada berbagai posisi dengan tingkat kecerahan yang berbeda dan akan diamati apakah terdapat perubahan pada pesan yang disisipkan pada citra.Berdasarkan hasil pengujian, manipulasi yang diberikan dekat dengan posisi pesan disisipkan mengakibatkan pesan menjadi rusak sehingga tidak dapat dimunculkan kembali. Efek manipulasi ini akan berbeda-beda tergantung dari panjang pesan yang disisipkan dan posisi manipulasi yang diberikan. Jadi apabila ingin memberikan efek pada citra stego, pastikan agar tidak mengganggu piksel citra stego yang pengandung pesan rahasia.

Manipulasi pengaburan citra (*bluring*) dilakukan dengan beberapa metode.Metode pengaburan (*bluring*) tersebut diantaranya adalah pengaburan (*bluring*) tipe *Gaussian,* pengaburan (*bluring*) tipe *Linear,* pengaburan (*bluring*) tipe *Radial,* pengaburan (*bluring*) tipe *Spread,* dan pengaburan (*bluring*) tipe *Zoom.*Berdasarkan hasil pengujian diketahui bahwa citra stego sangat aman apabila diberikan manipulasi pengaburan tipe *Radial Counter-Clockwise* pada sumbu(0,0) untuk kuantitas 1 hingga 100 dan tipe *Zoom in* pada segala sumbu untuk kuantitas 1 hingga 1000.

Manipulasi perputaran citra (*rotation*) dilakukan sebanyak tiga kali, yaitu diputar sejauh 90^0 ke kiri, 90^0 ke kanan, dan 180^0. Berdasarkan hasil pengujian, dapat diketahui bahwa citra stego tidak boleh diberikan manipulasi perputaran (*rotation*) karena akan merusak pesan yang disisipkan di dalamnya. Pesan tidak terdeteksi karena piksel penyusun citra yang sebelumnya disisipkan berubah tempat, sehingga pada saat proses ekstrak sistem mengecek piksel citra yang tidak terdapat pesan.

Pengujian citra stego di internet dilakukan dengan pengunggahan citra ke *Facebook*, *Twitter*, dan blog. Setelah diunggah, citra akan diunduh kembali dan akan menjalani proses ekstrak untuk mengetahui pesan yang sebelumnya disisipkan akan rusak atau tidak.

Berdasarkan hasil pengujian dalam mengunggah citra stego pada jejaring sosial *Facebook*, dapat diketahui bahwa format dari citra yang diunggah akan lebih efektif jika menggunakan PNG. Ukuran berkas citra bitmap yang sangat besar mengakibatkan proses pengunggahan (*upload*) yang cukup lama. Namun pada saat berkas citra diunduh kembali, terjadi perubahan format dan ukuran pada citra. Format apapun yang diunggah pada *Facebook* akan secara otomatis dimampatkan menjadi format JPEG. Oleh karena itu, baik format bitmap ataupun PNG yang diunggah dan diunduh kembali, tidak dapat dilakukan proses ekstrak karena pesan yang disisipkan ke dalam citra menjadi rusak.

Lain halnya dengan *Twitter*, mikro blog ini tidak dapat menerima format citra bitmap untuk diunggah.Citra berformat bitmap yang digunakan harus diubah ke dalam format lain yang merupakan kompresi tak berugi/*lossless*(PNG). Apabila format bitmap diubah menjadi JPEG, pesan di dalam citraakan rusak karena JPEG merupakan kompresi berugi/*lossy*.Hal lain yang dimiliki oleh *Twitter* adalah format citra PNG yang diunggah akan tetap sama pada saat diunduh kembali. Sehingga pesan yang berada di dalam citra akan aman dan dapat diekstrak kembali.

Pengujian pada blog *wordpress* menunjukkan format citra bitmap tidak dapat diunggah.Pada format PNG tidak ada masalah saat proses pengunggahan dan pengunduhan kembali. Pesan yang disisipkan pada citra stego dapat diekstrak kembali setelah diunduh dari blog.

Pada *blogger* terdapat sedikit perbedaan.Blog ini mendukung format citra bitmap maupun PNG.Kedua format dapat diunggah pada blog.Namun, untuk format bitmap pada saat diunduh kembali, citra stego mengalami perubahan piksel yang mengakibatkan pesan di dalam citra menjadi rusak.Lain halnya pada citra stego berformat PNG.Format ini aman untuk dilakukan pengunggahan dan pengunduhan kembali. Pesan yang disisipkan pada citra juga tidak akan rusak sehingga dapat diekstrak kembali.

4. Kesimpulan

Pada tahap Enkripsi dengan metode *Caesar Chiper* perlu diperhatikan karakter pesan dan karakter pengganti spasi agar tidak saling tumpang tindih.

Steganografi dengan menggunakan metode *End of File* tidak merusak kualitas dari citra asli/citra *cover*, sehingga citra asli dengan citra stego nampak mirip dan sulit dibedakan secara kasat mata.

Steganografi dengan menggunakan metode *End of File* mengakibatkan ukuran citra yang disisipi pesan mengalami penambahan ukuran tinggi (*Height*) dan ukuran berkasnya (*file size*).

Jumlah maksimal karakter pesan yang dapat disisipkan pada citra tergantung dari ukuran lebar citra (w*idth*), semakin besar ukuran lebar citra maka karakter pesan yang dapat disisipkan akan semakin banyak.

Manipulasi citra stego dapat dilakukan dengan syarat tidak boleh mengganggu piksel pesan yang disisipkan berada.

Pengunggahan citra stego di internet dan proses pengunduhan kembali dengan menggunakan citra berformat bitmap menunjukkan hasil yang kurang memuaskan karena beberapa media (*Twitter, Wordpress*) tidak mendukung format bitmap.

Pesan yang berada dalam citra stego akan tetap aman dan dapat dimunculkan kembali jika proses pengunggahan pada media (*Twitter, Wordpress, Blogger*) menggunakan citra berformat PNG.

Adapun saran yang dapat diberikan adalah algoritma kriptografi dan teknik steganografi yang digunakan pada sistem ini dapat dikembangkan lebih lanjut agar lebih aman dalam pengiriman pesan dan tahan terhadap manipulasi yang dilakukan.

Program dapat dikembangkan agar dapat menampung berkas rahasia lain seperti citra, audio, video, dan format teks yang lain seperti format pdf atau doc.

Steganografi dengan metode *End of File* (EOF) dapat diimplementasikan oleh bahasa pemrograman lain sehingga dapat diaplikasikan pada perangkat bergerak seperti telepon pintar (*smart phone*).

Referensi

[1]. Aditya, Y., A. Pratama, dan A. Nurlita, *Studi Pustaka untuk Steganografi dengan Beberapa Metode*, Jurnal , Fakultas Teknologi Industri UII, 2010.

[2]. Arhami, M., dan A. Desiani, *Pemrograman MATLAB*, ANDI, Yogyakarta, 2005.

[3]. Hallim, A., *Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik*, Skripsi S-1, PENS-ITS, Surabaya, 2010.

[4]. Hidayatno, A., *Steganografi dan Watermarking – Pengolahan Citra Digital*, Teknik Elektro Universitas Diponegoro.

[5]. Ihsan, A.A., *Aplikasi Steganografi pada Berkas Video MP4 dengan Menggunakan Bahasa Pemrograman Java*, Skripsi S-1, Universitas Diponegoro, Semarang, 2012.

[6]. Krisnawati, *Metode Least Significant Bit (LSB) dan End Of File (EOF) untuk Menyisipkan Teks Ke Dalam Citra Grayscale*, Jurnal, Jurusan Manajemen Informatika AMIKOM, 2008.

[7]. Munir, R., *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Informatika, Bandung, 2004.

[8]. Nurhayati, O.D., *Multimedia*, Program Studi S1 Sistem Komputer Universitas Diponegoro.

[9]. Paulus, E., dan Y. Nataliani, *Cepat Mahir GUI Matlab*, ANDI, Yogyakarta, 2007.

[10]. Praditya, D., *Aplikasi Steganografi Berbasis GUI dengan Metode Pengganti LSB*, Skripsi S-1, Universitas Diponegoro, Semarang, 2010.

[11]. Purnomo, M.H., dan A. Muntasa, *Konsep Pengolahan Citra Digital dan Ekstraksi Fitur*, Graha Ilmu, Yogyakarta, 2010.

[12]. Putra, D., *Pengolahan Citra Digital*, ANDI, Yogyakarta, 2010.

[13]. Raharjo, A.S., *Implementasi Steganografi pada Berkas MP3*, Skripsi S-1, Universitas Diponegoro, Semarang, 2009.

[14]. Sigit, dkk, *Step by Step Pengolahan Citra Digital*, ANDI, Yogyakarta, 2005.

[15]. Wandani, H., *Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem*, Skripsi S-1, Universitas Sumatera Utara, Medan.

[16]. Yusuf, V.R., *Aplikasi Enkripsi dan Dekripsi Menggunakan Algoritma Rijndael*, Skripsi S-1, Universitas Diponegoro, Semarang.

[17]. ---, *Caesar Chiper*, http://en.wikipedia.org/wiki/Caesar_cipher, diakses pada Mei 2013.

[18]. ---, *Kriptografi*, http://id.wikipedia.org/wiki/Kriptografi, diakses pada Mei, 2013.

[19]. ---, *Practical Workbook: Information Theory*, 4th edition, Department of Computer & Information System Engineering NED University of Engineering & Technology, Karachi, Pakistan, 2012.