TEKNOMATIKA, Vol.07, No.02, September 2017
P-ISSN : 2087-9571, E-ISSN : 2541-335X



# Enkripsi Teks Pesan dengan Menggunakan Metode Steganografi pada Binari *Image*

## MESSAGE TEXT ENCRYPTION USING STEGANOGRAPHY METHODS ON IMAGE BINARIES

**Suryati***
Universitas Indo Global Mandiri: Jln. Jenderal Sudirman No.03 Palembang
Jurusan Sistem Informasi, Universitas Indo Global Mandiri Palembang
e-mail: *buyaticute@gmail.com

**Abstrak**

Sejak muculnya teknologi internet sangat memungkinkan pertukaran data dari satu komputer ke komputer lain yang mempunyai jarak yang berjauhan bahkan antar negara, selama komputer tersebut terhubung dengan jaringan internet maka komputer tersebut dapat berkomunikasi. Pertukaran data atau pesan dapat berupa data teks ataupun data gambar, oleh sebab itu keamanan data yang yang dikirim perlu diperhatikan, apakah data atau pesan yang di terima sesuai dengan data atau pesan yang dikirim. Penyandian pesan sangat penting untuk keamanan data atau pesan. Hal ini dapat dilakukan dengan menggunakan *enkripsi* atau *steganography*. *Steganography* merupakan suatu metode untuk menyisipkan sebuah informasi rahasia dalam suatu objek media lain seperti gambar. Dalam *steganography* dikenal *data hiding* atau *data embedding* yaitu penyembunyian data yang nampak sangat familiar dengan *kriptografi*. Namun *data hiding* dalam *steganography* dan *kriptografi* sangat berbeda. Jika pada *kriptografi*, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan *steganography, ciphertext* dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaan data tersebut. Aplikasi penyandian pesan yang peneliti buat untuk menerapkan metode steganography. Metode ini membuktikan bahwa teknik penyembunyian pesan setelah melalui proses *embeding data,* maka hasil output berupa data atau pesan ini tidak mengalami penurunan kualitas. Sehingga tidak menimbulkan kecurigaan bahwa file data atau pesan tersebut sudah melalui proses *enkripsi* atau *steganography*.
**Kata kunci-***data hiding, steganography, image, LSB.*

**Abstract**

*The emergence of Internet technology allows exchanging data from one computer to another computer with a distance even apart between countries, as long as the computer is connected to the Internet network then the computer can communicate. The exchange of data or messages can be text data or image data, therefore the security of sent data needs to be noticed, whether the data or messages received is corresponding with the data or messages sent. Message encryption is essential for data or message security. This can be done using encryption or steganography. Steganography is a method to insert a secret information in another media object such as images. In steganography, data hiding or embedding data is data hiding that seems very familiar with cryptography. But the data hiding in steganography and cryptography is very different. In cryptography, the encrypted data (ciphertext) is still available, but in steganography, ciphertext can be hidden so that third parties do not know the existence of the data. The message encoding application that the researcher made is used to apply the steganography method. This method proves that the technique of concealing the message after going through data embeding process, then the output of data or this message does not decrease quality. Thus, did not arouse suspicion that the data file or message has been through the process of encryption or steganography.*
***Keywords**-data hiding, steganography, image, LSB.*

## 1. PENDAHULUAN

Keamanan sangat dibutuhkan pada saat kita bekerja melakukan aktifitas, agar kita dapat melakukan aktifitas dengan aman dan nyaman maka dibutuhkan suatu cara atau metode agar kita dapat berkerja dengan aman dan nyaman, Keamanan akan informasi pada era digital saat ini menjadi sebuah kebutuhan sangat penting dalam berbagai segi kehidupan. Suatu informasi akan sangat berharga apabila dapat berhubungan dengan aspek - aspek lain yang berhubungan dengan informasi, seperti pengambilan keputusan, keamanan, kepentingan umum, ataupun bisnis. Dimana informasi-informasi tersebut tentunya akan sangat berguna bagi pihak yang membutuhkan kepentingan keamanan akan informasi.

Penggunaan steganografi merupakan hal yang sangat penting dalam pengamanan pesan, hal ini menjadi daya tarik banyak orang setelah peristiwa penyerangan gedung WTC, pada tanggal 11 september 2001. Pada peristiwa tersebut disebutkan oleh ”pejabat pemerintahan dan ahli dari pemerintahan AS” yang tidak disebut namanya bahwa para ”Teroris” menyembunyikan peta-peta, foto-foto target dan juga pesan yang berupa perintah untuk aktivitas teroris di ruang *chat sport, bulletin boards* dan *website* lainnya. Isu lainnya menyebutkan bahwa teroris menyembunyikan pesan-pesannya dalam pornografi di *website* tertentu. Walaupun demikian, sebenarnya belum ada bukti nyata dari pernyataan tersebut di atas [1].

Metode dan media perantara yang digunakan dalam steganografi bermacam-macam, sesuai dengan perkembangan zaman. Pada zaman dahulu kala, teknik steganografi sederhana sudah banyak digunakan untuk merahasiakan pesan. Seperti Leonardo Da Vinci yang konon menyembunyikan pesan-pesan tertentu di balik karya-karya lukisannya. Seperti senyum misterius pada lukisan Monalisa yang kerap menjadi kontroversi di kalangan para ahli yang mencoba mengambil pesan tersirat dari Lukisan Monalisa tersebut [2].

Era digital yang merambah kehidupan manusia modern dan telah berhasil membawa perubahan dalam implementasi teknik *steganografi*. Penyembunyian pesan tak lagi dilakukan lewat lukisan kanvas ataupun lewat kertas, titik-titik rahasia di suatu majalah ataupun cara-cara konvensional lainnya yang mana di zaman sekarang ini, pesan rahasia disembunyikan di dalam suatu file teks, gambar, vidio, atau bahkan audio. Walaupun *steganografi* dapat dikatakan mempunyai hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda. *Kriptografi* mengacak pesan sehingga pesan tersebut tidak dapat di mengerti, sedangkan *steganografi* menyembunyikan pesan sehingga pesan tersebut tidak dapat terlihat [3].

Penelitian ini membahas tentang bagaimana pembuatan sebuah aplikasi program *Steganografi* yang dapat memberikan kemudahan dalam penyembunyian pesan, yaitu yang berupa teks, ke dalam sebuah image/gambar digital. Agar tidak terjadi kesalahan persepsi dan tidak meluasnya pokok bahasan, Maka pembahasan masalah dalam penelitian ini ruang lingkupnya dibatasi meliputi : Pesan rahasia yang disembunyikan berupa pesan dalam bentuk teks dan Media yang digunakan untuk menyembunyikan pesan yaitu media gambar dalam bentuk format file bitmap 24 bit.

Tujuan dari penelitian ini adalah membuat aplikasi yang dapat menyembunyikan pesan rahasia ke dalam suatu file gambar, agar pesan rahasia tersebut hanya dapat dibuka oleh orang yang kita kehendaki. Peneliti tidak menemukan penelitian dengan judul yang sama seperti judul penelitian yang dibuat oleh peneliti. Namun penulis mengangkat beberapa penelitian sebagai referensi dalam memperkaya bahan kajian pada penelitian peneliti. Berikut merupakan penelitian terdahulu berupa beberapa jurnal terkait dengan penelitian yang peneliti lakukan. Siti Rohayah dkk menghasilkan Aplikasi yang dapat menyisipkan data dalam bentuk video dan suara [4], sedangkan penelitian yang dibuat oleh Jhoni Verlando Purba dkk yang berjudul Implementasi Steganografi Pesan *Text* Ke Dalam *File Sound* (.Wav) Dengan modifikasi Jarak *Byte* pada Algoritma *Least Significant Bit* (Lsb). Mengimplementasikan metode steganografi ke dalam *file* suara dengan jarak *byte* [5], pada penelitian yang di buat oleh Ghazali Moenandar , Wirawan, Eko Setijadi yaitu menganalisa Kualitas Citra Pada Steganografi Untuk Aplikasi E-

Government.menghasilkan kualitas citra yang lebih baik setelah dilakukan penyembunyian pesan [6].

## 2. METODE PENELITIAN

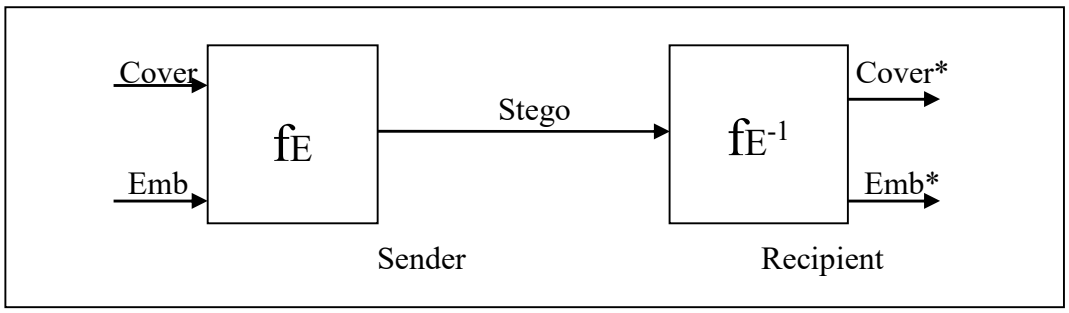
Metode penelitian berhubungan erat dengan prosedur, teknik, alat, serta desain penelitian yang digunakan. Desain penelitian harus cocok dengan pendekatan penelitian yang dipilih. Prosedur, teknik, serta alat yang digunakan dalam penelitian harus cocok pula dengan metode penelitian yang ditetapkan. Metode penelitian menggambarkan rancangan penelitian yang meliputi prosedur atau langkah-langkah yang harus ditempuh, waktu penelitian, sumber data, serta dengan cara apa data tersebut diperoleh dan diolah/dianalisis. Dalam prakteknya terdapat sejumlah metode yang biasa digunakan untuk kepentingan penelitian.

Steganografi (S*teganography*) adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi berasal dari Bahasa Yunani, yaitu "steganos" yang artinya "tulisan tersembunyi (*covered writing*)". Steganografi termasuk ke dalam *security through obscurity*. Steganografi biasa digunakan oleh teroris, intelijen, atau militer dalam menyampaikan pesan sehingga tidak diketahui orang lain. 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. Penggunaan steganografi antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi dan melidungi 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. 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 *ciphertext* menimbulkan kecurigaan bahwa pesan tersebut merupakan pesan rahasia.

*S*teganografi yang dibahas di sini adalah penyembunyian data di dalam citra digital. Meskipun demikian, penyembunyian data dapat juga dilakukan pada wadah berupa suara digital, teks, ataupun video. Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. 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.
2. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung. Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
3. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*)

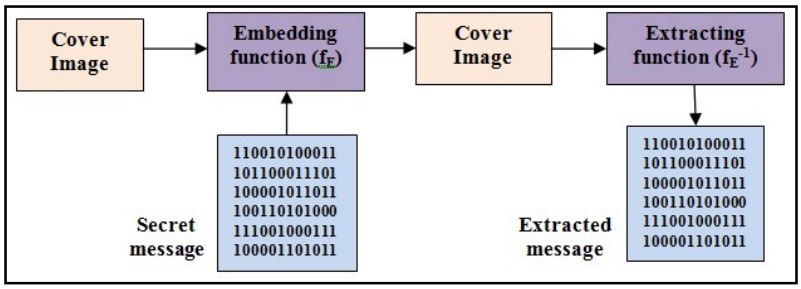
Tiga aspek berbeda didalam sistem penyembunyian informasi bertentangan dengan satu sama lain yaitu: kapasitas, keamanan, dan ketahanan. Kapasitas adalah mengacu pada jumlah informasi yang dapat tersembunyi di dalam sampul media, keamanan adalah pencegahan bagi orang biasa yang tidak mampu untuk mendeteksi informasi tersembunyi, dan ketahanan adalah untuk modifikasi media stego sehingga dapat bertahan terhadap suatu *attack* yang dapat menghancurkan informasi tersembunyi [7].




Gambar 1. Cara kerja Steganografi secara umum

$f_E$ : *Embedding* (Penggabungan berkas *cover* dengan berkas pesan ).
$f_E^{-1}$ : *Extracting* (Pengambilan berkas pesan dari berkas *cover*).
Cover : Berkas data yang akan disisipkan informasi *(carrier).*
Emb : Pesan yang akan disisipkan.
Stego : Berkas *cover* yang sudah berisi pesan.

Diistilahkan sebagai *embedded message* (*hiddentext*), datanya bisa berupa file, image, teks, dan lain-lain. Data yang dijadikan media untuk menyembunyikan pesan disebut *cover medium (covertext)*. *Cover medium* yang telah ditambahkan pesan rahasia dengan steganografi disebut *stego-data (stegotext)*. Pada keadaan yang ideal, siapapun yang melakukan *scan* terhadap data tersebut tidak akan mengetahui bahwa data tersebut mengandung data lain yang rahasia sehingga pengambilan data hanya dapat dilakukan oleh penerima yang berhak. Proses tadi dapat direpresentasikan secara lebih jelas pada gambar 2 sebagai berikut:




Gambar 2. *Graphical Version of a Steganographic System*

**Jenis Citra**

Nilai Suatu Pixel memiliki nilai dalam suatu rentang tertentu, dari nilai minimum sampai nilai maksimum. Citra dengan penggambaran seperti ini digolongkan ke dalam citra integer, berikut adalah jenis- jenis citra berdasarkan nilai pixelnya [8].

1) Citra Biner
   Citra yang hanya memiliki 2 kemungkinannilai pixel yaitu hitam dan putih. Hanya dibutuhkan 1 bit untuk mewakili nilai setiap pixel dari citra biner.
2) Citra *Grayscale*
   Citra digital yang hanya memiliki satu nilai kanal pada setiap pixelnya, dengan kata lain nilai bagian *RED=GREEN=BLUE.*
3) Citra Warna(8 bit)
   Setiap pixel dari citra warna (8 bit) hanya diwakili oleh 8 bit dengan jumlah warna maksimum yang dapat digunakan adalah 256 warna.
4) Citra Warna(16 bit)

Citra warna 16 bit (biasa disebut sebagai citra *highcolor*) dengan setiap pixelnya diwakili dengan 2 *byte memory* (16 bit).

5) Citra Warna(24 bit)
Setiap pixel dari citra warna 24 bit diwakili dengan 24 bit sehingga total 16.777.216variasi warna.

**Teknik Steganografi**

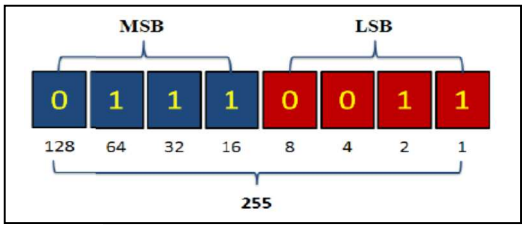
Secara teknik penyembunyiannya dapat dipisahkan dan dianalisa untuk mengetahui apa yang terjadi dalam keseluruhan proses. Hal tersebut dikategorikan dalam enam kategori steganografi [9] yaitu:

1) Sistem Substitusi
Sistem steganografi substitusi menggantikan *bit-bit* yang tidak perlu dari suatu media dengan *bit-bit* dari pesan rahasia. Beberapa teknik steganografi yang ada menggunakan metode *Least Significant Bit*(LSB) untuk memproses pesan rahasianya.
2) Teknik *Domain Transform*
Pada dasarnya teknik ini menyembunyikan data pesan dalam ”ruang transform” dari suatu sinyal. Contoh algoritma yang tergolong teknik ini adalah steganografi pada domain DCT *(Discrete Cosine Transform).*
3) Teknik *Spread-Spectrum*
Dalam *spread spectrum* yang langsung, aliran informasi yang ditransmisikan dibagi menjadi potongan-potongan kecil. Setiap potongan ditempatkan sebagai kanal frekuensi dari spektrum.
4) Metode Statistik
Dengan teknik ini data di *encoding* melalui pengubahan beberapa informasi statistic dari berkas *cover.* Berkas *cover* di bagi dalam blok-blok dimana setiap blok tersebut menyimpan satu piksel informasi rahasia yang disembunyikan. Jika piksel yang ditemukan pada suatu blok untuk menyimpan data adalah piksel T maka tidak dilakukan perubahan nilai piksel, jika sebaliknya maka dilakukan perubahan nilai piksel. Meskipun secara teoritis mungkin untuk dilakukan, pada kenyataannya teknik ini agak sulit untuk diimplementasikan.
5) Teknik Distorsi
Metode steganografi ini membuat perubahan dalam obyek media untuk menyembunyikan informasi. Pesan rahasia didapatkan kembali jika algoritma yang dibandingkan berubah, berbeda dengan aslinya. informasi yang disembunyikan disimpan berdasarkan distorsi sinyal.
6) Metode Penurunan Media
Secara khusus obyek media dipilih untuk menyembunyikan pesan, namun sebenarnya metode ini membuat/menurunkan sebuah media yang digunakan untuk menyembunyikan informasinya.

Pada sistem substitusi, terdapat beberapa metode yang bias diterapkan untuk beberapa tipe media, di antaranya adalah metode *Least Significant Bit* (LSB).

**Metode *Least Significant Bit* (LSB)**

Pada sebuah rangkaian informasi terdapat penggolongan-penggolongan bit berdasarkan urutan dan pengaruhnya dalam byte. Secara garis besar, dalam rangkaian informasi terdapat 2 golongan bit, yaitu *Most Significant Bit* (MSB) dan *Least Significan Bit* (LSB).




sumber: Agus, dkk, Gambar 3. Representasi Biner

*Most Significant Bit* merupakan reprsentasi 4-bit yang memiliki pengaruh besar pada sebuah rangakain informasi, artinya adalah akan terjadi perubahan yang drastis apabila bit-bit ini dimodifikasi. Sementara *Least Significant Bit* merupakan representasi 4-bit yang paling sedikit memiliki pengaruh apabila bit-bit tersebut dimodifikasi dan tidak akan terjadi perubahan yang drastis, sehingga kemungkinan terjadinya kecurigaan manusia terhadap bit-bit LSB yang dimodifikasi sangat kecil. Dengan demikian, semakin kekanan, bit-bit tersebut makin kecil pengaruhnya terhadap keutuhan data yang dikandung. Oleh sebab itu, 4-bit terakhir tersebut yang dimodifikasi dan dijadikan tempat pelekatan sebuah informasi digital steganografi [10].

Teknik LSB dilakukan dengan memodifikasi bit-bit yang tergolong bit-bit LSB pada tiap byte pada sebuah *file* yang digunakan sebagai *carrier file,* atau dengan kalimat yang lain dengan cara mengganti bit-bit LSB dengan bit-bit informasi yang ingin dilekatkan. Proses penggantian bit ini disebut dengan proses *encoding/ embedding.* Setelah semua bit informasi tersebut menggantikan bit LSB *carrier file* tersebut, maka informasi telah berhasil dilekatkan pada *carrier file* dan *output*-nya disebut dengan *Stego File* [10].

Apabila suatu informasi yang dilekatkan tersebut ingin dibuka *(ekstract)* kembali, maka bit-bit LSB yang ada pada *stego file* akan diambil satu per satu dan dikembalikan lagi atau disatukan kembali sehingga menjadi sebuah informasi atau disebut dengan *decoding/ retrieving (*Alfebra dan Asep, 2009*)* [10]. Berikut ini adalah standar *flowchart* dari metode LSB yang digunakan untuk menyisipkan informasi dan mengekstraknya setelah suatu informasi disisipkan pada media penampungnya [10].

## 3. HASIL DAN PEMBAHASAN

### Analisis Kebutuhan Sistem

Analisis merupakan tahapan awal dalam perancangan sistem untuk mengidentifikasi masalah dan kebutuhan-kebutuhan dalam pembangunan sebuah sistem. Dalam pembangunan aplikasi enkripsi pesan *text* dengan metode steganografi pada binary *images* ini, dilakukan analisis terhadap kegiatan yang berkaitan dengan aplikasi, yaitu alur cerita yang menjelaskan tahapa-tahapan sistem yang berjalan. Aplikasi enkripsi pesan teks yaitu sebuah perangkat lunak untuk menyembunyikan pesan ke dalam sebuah gambar tanpa membuat curiga orang yang tidak berhak mengakses/membuka gambar yang berisi pesan rahasia tersebut.

### Kebutuhan Sistem

Pembangunan aplikasi ini membutuhkan analisis dari kebutuhan sistem yang akan dibangun. Kebutuhan sistem aplikasi enkripsi pesan text dengan metode steganografi pada binary *images* ini meliputi:

a) *Input* / masukan
   *User* melakukan pemilihan untuk enkripsi atau deskripsi.
b) Proses
   Setelah *user* memilih antara enkripsi dan deskripsi yang diinginkan maka secara otomatis sistem akan mengeksekusi ke perintah selanjutnya.
c) *Output* / keluaran
   *User* mendapatkan hasil dari proses yang di inginkan tadi.

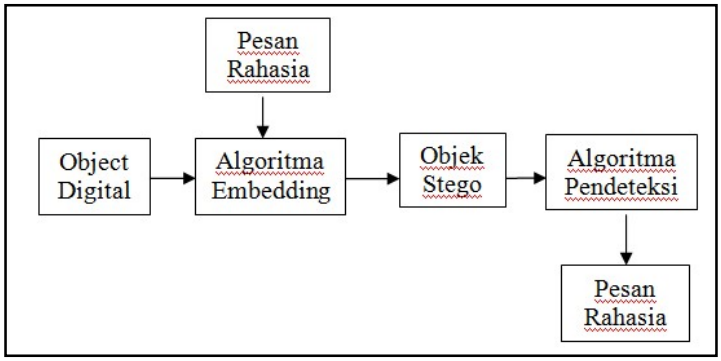
### Batasan Perancangan Sistem

Agar pembahasan tidak menyimpang dari permasalahan, maka pembahasan hanya difokuskan pada pesan teks dengan format gambar BMP.

### Perancangan Umum

Apabila dilihat secara umum program Steganografi ini berfungsi untuk menyembunyikan informasi data digital dibalik informasi digital lainnya. Untuk menyembunyikan informasi, dibutuhkan suatu media sebagai sarana untuk menampung informasi, media yang digunakan dalam penulisan ini adalah objek digital berupa *file* gambar. Setelah menentukan media yang

digunakan, barulah pesan rahasia dapat disisipksn kedalamnya, untuk menampung pesan rahasia ke dalam objek digital tentunya membutuhkan suatu algoritma yang dapat memodifikasi objek digital sehingga menghasilkan objek digital baru yang berisi pesan tersembunyi, yang disebut dengan istilah *algoritma embedding*, dengan catatan bahwa dalam proses modifikasi perubahan yang terjadi antara media asli dengan hasil modifikasi media tidak boleh terlalu mencolok atau bahkan secara kasat mata perubahan yang terjadi tidak terlihat [11]. Untuk lebih jelasnya lihat pada gambar di bawah ini:



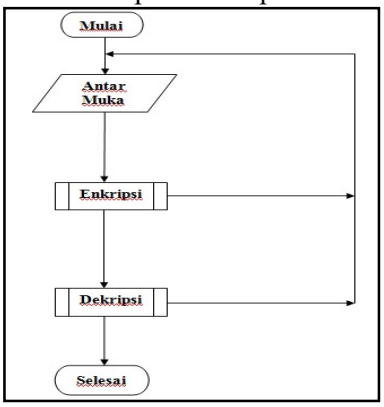

Gambar 4. Skema Metode Steganografi

Setelah menghasilkan *objek stego* yang berupa *file* gambar, lalu pengirim mengirimkan *objek stego* ini ke penerima, Untuk mengambil pesan rahasia yang terkandung di dalam *objek stego* dibutuhkan algoritma pendeteksi yang diberikan oleh pengirim. Algoritma pendeteksi ini merupakan kebalikan dari algoritma *embedding*, bila algoritma *embedding* digunakan untuk menyisipkan pesan rahasia ke dalam *file* gambar, maka algoritma pendeteksi digunakan untuk mengambil pesan rahasia dari *file* gambar.

### 3.1 Perencanaan Perancangan Sistem

**Proses Menu Utama**

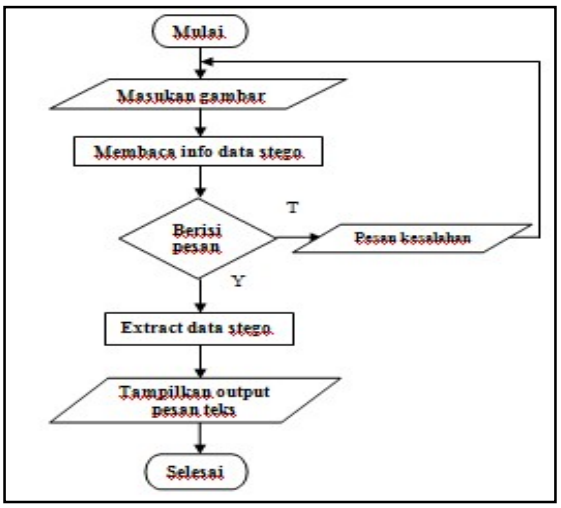
Proses ini berlangsung saat user ingin melakukan pemilihan proses enkripsi dan deskripsi.




Gambar 5. Diagram Alir Menu Utama

Proses *Enkripsi* Data

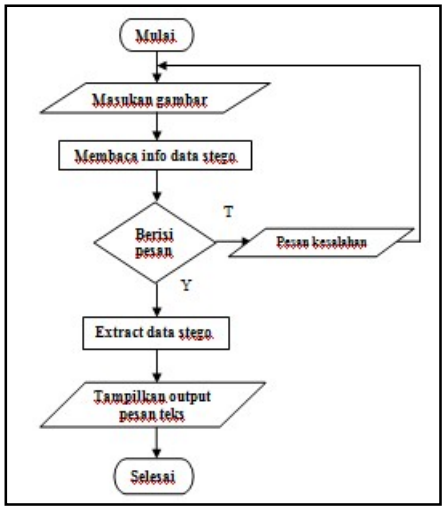
Proses ini berlangsung saat user ingin melakukan *encoding* (menyembunyikan) data ke dalam suatu media.




Gambar 6. Diagram Alir *Enkripsi* Data

Proses *Dekripsi* Data

Proses ini berlangsung saat *user* ingin melakukan *decoding* (pengekstrakan) data dari berkas stego.




Gambar 7. Diagram Alir *Dekripsi* Data

Dari diagram alir menu utama di atas, dapat dijelaskan langkah-langkah proses sebagai berikut: setelah memulai sistem (*start*),selanjutnya tampilan *form* antar muka akan muncul. Lalu *user* melakukan pilihan untuk memilih enkripsi atau dekripsi, jika memilih enkripsi, maka tampilan *form* enkripsi akan muncul. Jika memilh dekripsi maka tampilan *form* deskripsi akan muncul, jika tidak memilih keduanya maka keluar (*Exit*).

**Tahap *Enkripsi* Data**

Dari diagram alir *encoding* di atas, dapat dijelaskan langkah-langkah proses sebagai berikut: setelah memulai sistem (*start*), selanjutnya *user* melakukan input untuk Gambar (*carrierimage)*, kemudian program menghitung maksimal data gambar yang disisipkan. Selanjutnya *user* melakukan input untuk pesan, kemudian program menghitung maksimal data pesan yang disisipkan. Jika data pesan ≤ data gambar maka program melakukan penyisipan (enkripsi). Lalu simpan hasil penyisipan. Jika tidak, kembali ke awal (*input* gambar). Jika data

pesan ≥ data gambar maka kembali ke proses awal yaitu: input gambar/*input* pesan. Jika telah terpenuhi semua proses maka selesai. Dari proses ini, akan dihasilkan *stego file*.

**Tahap *Dekripsi* Data**

Dari diagram alir *decoding* di atas, dapat dijelaskan langkah-langkah proses sebagai berikut: setelah memulai sistem (*start*), selanjutnya user melakukan input untuk Gambar (*carrierimage)*, kemudian program membaca info stego, setelah itu program akan mengextract gambar yang berisi pesan tersebut, jika gambar berisi pesan maka tampil output pesan, jika gambar tidak berisi pesan maka tampil pesan kesalahan kembali ke proses awal (*input* gambar). Jika telah terpenuhi semua proses maka selesai.

**Fungsi-Fungsi pada Tahap Enkripsi dan Dekripsi Data**

Pada bagian ini akan dijelaskan fungsi-fungsi apa saja yang diperlukan untuk menunjang jalannya proses pada tahap *encoding* data. Berikut ini merupakan potongan variabel yang akan digunakan pada *form* Tulis Pesan:

```
                                    ...
Type DataPixel = Array [0..1000, 0..1000] of integer;
var
        frmTulisPesan: TfrmTulisPesan;
        MaxChar, InfoBaris, InfoKolom, tinggi, lebar, PanjangText : integer;
        NamaFile : string;
        hdc1 : hdc;
        Awal, Selesai : TDateTime; …
```

Gambar 8. Variabel yang Akan digunakan pada *Form* Tulis Pesan

Pada *Form encoding* tersebut setelah menulis pesan rahasia selanjutnya pengguna tinggal menekan tombol *encoding* yang kemudian proses penyembunyian pesan dimulai. Dalam modul program ini terdapat 4 proses utama yaitu cek fleck, sisip fleck, sisip pesan dan sisip lokasi yang dilakukan secara berurutan. Fleck adalah tanda di dalam file gambar berupa deretan 3 karakter yaitu @#$. Sebelum disisipi pesan, *file* gambar diperiksa dahulu oleh program apakah terdapat fleck di dalamnya, jika program menemukan fleck maka di dalam *file* gambar tersebut juga terdapat pesan rahasia. Pendeteksian fleck ini terdapat pada proses cek fleck .

```
…
for i:=0 to 7 do
begin
merah:=GetRValue(getpixel(ImageFile.Canvas.Handle,i,0));
hijau:=GetGValue(getpixel(ImageFile.Canvas.Handle,i,0));
biru:=GetBValue(getpixel(ImageFile.Canvas.Handle,i,0));
CekBiner:=CekBiner+(biner(biru))[8]+(biner(hijau))[8]+(biner(merah))[8];
end;
…
huruf1:=chr(decimal(copy(CekBiner,1,8)));
huruf2:=chr(decimal(copy(CekBiner,9,8)));
huruf3:=chr(decimal(copy(CekBiner,17,8)));
fleck:=huruf1+huruf2+huruf3;
```

Gambar 9. Cek fleck

Jika program tidak menemukan fleck di dalam *file* gambar setelah proses cek fleck selesai maka program akan meneruskan proses selanjutnya yaitu proses sisip fleck. Proses sisip fleck ini berfungsi untuk memberi tanda pada gambar bahwa gambar ini sudah mengandung pesan.

```
…
        Screen.Cursor:=CrHourGlass;
        fleck:='@#$';
        BinerFleck:='';
        n:=1;
          for i:=1 to 3 do
          …
```

Gambar 10. Sisip fleck

Setelah proses sisip fleck selesai, kemudian program akan melanjutkan proses selanjutnya yaitu proses sisip pesan.

```
…
        pesan:=memoTulisPesan.Lines.Text;
        BinerPesan:='';
        PanjangText:=length(memoTulisPesan.Lines.Text);
            for i:=1 to PanjangText do
            begin
                BinerPesan:=BinerPesan+biner(ord(pesan[i]));
        end;
                n:=1;
                for j:=1 to ImageFile.Height-1 do
        begin
for i:=0 to ImageFile.width-1 do
…
```

Gambar 11. Sisip Pesan

Kemudian setelah proses sisip pesan ini selesai, program akan melanjutkan proses terakhir dalam modul program enkripsi yaitu proses sisip lokasi. Proses sisip lokasi ini adalah proses memasukkan informasi tempat baris dan kolom terakhir dimana pesan rahasia disisipkan di dalam *file* gambar. Informasi lokasi ini berguna agar dalam proses pemisahan pesan rahasia dari *file* gambar, program bisa tepat dalam mengambil bit-bit biner pesan yang telah habis diambil oleh program.

```
…
        InfoBaris:=j;
        BinerBaris:=biner16(InfoBaris);
                n:=1;
                for x:=8 to 15 do
…
begin
inc(z);
biru:=GetBValue(getpixel(ImageFile.Canvas.Handle,x,0));
hijau:=GetGValue(getpixel(ImageFile.Canvas.Handle,x,0));
merah:=GetRValue(getpixel(ImageFile.Canvas.Handle,x,0));
BinerHijau:=biner(hijau);
BinerMerah:=biner(merah);
delete(BinerHijau,8,1);
delete(BinerMerah,8,1);
BinerHijau:=BinerHijau+BinerBaris[n];
BinerMerah:=BinerMerah+BinerBaris[n+1];
HijauBaru:=decimal(BinerHijau);
MerahBaru:=decimal(BinerMerah);
n:=n+2;
setpixelV(ImageFile.Canvas.Handle,x,0,RGB(MerahBaru,HijauBaru,biru));
end;
```

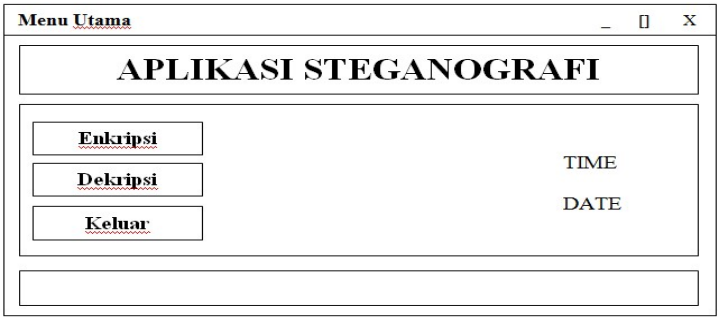
```
//sisip_kolom
InfoKolom:=i;
BinerKolom:=biner16(InfoKolom);
n:=1;
for x:=16 to 23 do
begin
inc(z);
biru:=GetBValue(getpixel(ImageFile.Canvas.Handle,x,0));
hijau:=GetGValue(getpixel(ImageFile.Canvas.Handle,x,0));
merah:=GetRValue(getpixel(ImageFile.Canvas.Handle,x,0));
BinerHijau:=biner(hijau);
BinerMerah:=biner(merah);
delete(BinerHijau,8,1);
delete(BinerMerah,8,1);
BinerHijau:=BinerHijau+BinerKolom[n];
BinerMerah:=BinerMerah+BinerKolom[n+1];
HijauBaru:=decimal(BinerHijau);
MerahBaru:=decimal(BinerMerah);
n:=n+2;
setpixelV(ImageFile.Canvas.Handle,x,0,RGB(MerahBaru,HijauBaru,biru));
end;
```

Gambar 12. Sisip lokasi

**Rancangan *User Interface***

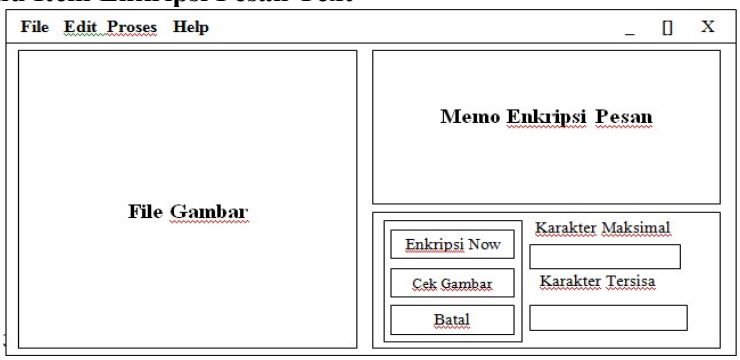
Sesuai dengan algoritma dan *flowchart* dari aplikasi enkripsi pesan *text* dengan metode steganografi pada binary images, dibuatlah tampilan-tampilan yang bertujuan untuk memudahkan *end user* untuk menjalankan aplikasi ini.

**Rancangan Menu Utama**



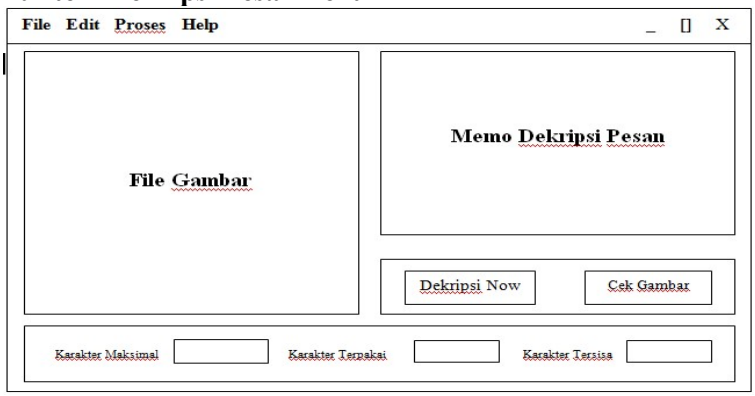

Gambar 13. Menu Utama

**Rancangan Menu Item Enkripsi Pesan Text**



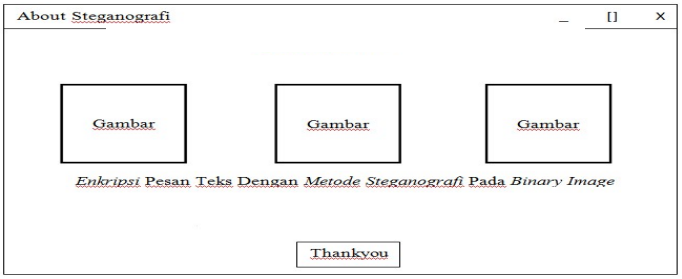

Gambar 14. *Form* Enkripsi

**Rancangan Menu Item Dekripsi Pesan Text**



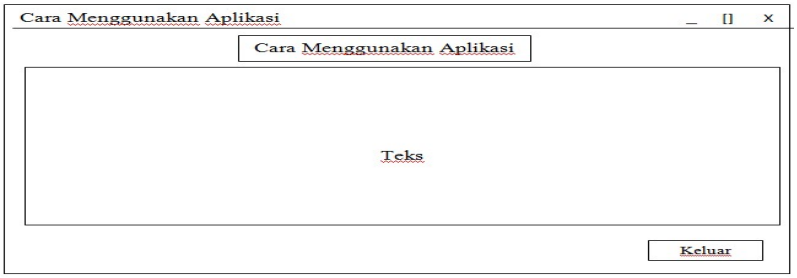

Gambar 15. *Form* Dekripsi

**Rancangan *About***




Gambar 16. *Form About*

**Rancangan *Instruksi***




Gambar 17. *Form* Instruksi

## 4. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian ini adalah pada Proses enkripsi dan dekripsi pesan teks bahwa banyak karakter yang disisipkan ke gambar tidak mempengarui piksel dan ukuran gambar, juga proses dekrpsi pesan teks berhasil diekstrak kembali dan pengguna aplikasi dapat membaca isi dari pesan rahasia tersebut. *User* yang menggunakan aplikasi *enkripsi* pesan teks dengan metode *steganografi* pada *binary image* ini dapat menyembunyikan pesan rahasia berupa file teks ke dalam file citra digital, tanpa diketahiu seseorang secara kasat mata, dengan menggunakan metode LSB (*Least Significant Bit*) yang diimplementasikan pada bahasa pemrograman Borlan Delphi 7.0

## UCAPAN TERIMA KASIH

Peneliti mengucapkan terimakasih kepada Allah SWT, yang telah memberikan kesehatan dan semangat sehingga selesainya penulisan penelitian ini.

## DAFTAR PUSTAKA

[1] Wahyono, Teguh. 2010. Pengolahan Citra: Penerbit Gava Media, Yogyakarta.
[2] Munir, Rinaldi. 2004. Pengolahan Citra Digital dengan Pendekatan algoritmik: Penerbit Informatika Bandung Yogyakarta.
[3] Johnson Neil F., S. Jajodia. 1998. Steganalysi Of Images Created Using Current Steganography Sofware: Penerbit ACM Press New York.
[4] Rohayah Siti , Sasmito Wiro Ginanjar, Somantri Oman. Jan 2015 Aplikasi Steganografi Untuk Penyisipan Pesan JURNAL INFORMATIKA Vol. 9, No. 1. Politeknik Harapan Bersama Tegal .
[5] Purba Verlando Jhoni, Situmorang Marihat, Arisandi Dedy. 2012. 50-55. Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan modifikasi Jarak Byte Pada Algoritma Least Significant Bit (Lsb). JURNAL DUNIA TEKNOLOGI INFORMASI Vol. 1, No.1.

[6] Moenandar Ghazali, Wirawan, Setijadi Eko. 2012. Analisa Kualitas Citra Pada Steganografi Untuk Aplikasi E-Government.Prosiding Seminar Nasional Manajemen Teknologi XV. Program Studi MMT-ITS, Surabaya.

[7] Suhono Harso Supangkat. 2000. Teknologi Informasi dan Ekonomi Digital: Persiapan Regulasi di Indonesia,Jurussan Teknik Elektro, Institut Teknologi Bandung

[8] Darma Putra, 2009. Pengolahan Citra Digital, Penerit Andi Yogyakarta.

[9] Bender W, Gruhl D, Norimoto N, Lu A. 1996. Techniques For Data Hiding. fBA'f Systems Journ(1135: 325-326)

[10] Ardhyana, Alfebra Stavia., Asep Juarna. 2008. Aplikasi Steganografi pada MP3 Menggunakan Teknik LSB. Teknik Informatika, Teknik Industri Universitas Gunadarma, 2008.

[11] Maulana, Basuki, Dwi Kurnia., Nadhori, Isbat Uzzin, Ahmad Mansur. 2009. DataHiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit, Jurnal Teknik Informatika