# *Hidden Messages* pada *Google Map Marker Images* Menggunakan Teknik Steganografi

Fredy Susanto[1],Pajar Saputra[2]

[1,2] *Magister Ilmu Komputer, Universitas Budi Luhur*

*Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260.*

*DKI Jakarta, Indonesia. Telp: 021-5853753*

[1]fredysusanto@gmail.com

[2]pajar.p109@gmail.com

**Abstrak− Teknik pencarian pada google sudah umum dipergunakan oleh semua kalangan, mesin pencari ini memberikan informasi semua hal yang dibutuhkan, termasuk informasi gambar dan peta. Pengkodean dengan Steganografi adalah penyisipan informasi ke dalam sebuah media seperti media gambar , suara maupun video. Penyampaian pesan di dalam google dapat memberikan informasi terhadap orang yang dituju pada media publik yang dienkripsi. Penyisipan informasi ke dalam gambar suatu lokasi pada *google map marker*, merupakan sebuah teknik penyampaian informasi kepada orang yang dituju ke dalam dimensi yang berbeda. Semua orang tidak akan mengira bahwa dalam gambar tersebut terdapat informasi rahasia yang dapat mencirikan tempat yang dituju tersebut.**

***Kata kunci* − google, steganografi, teks, gambar.**

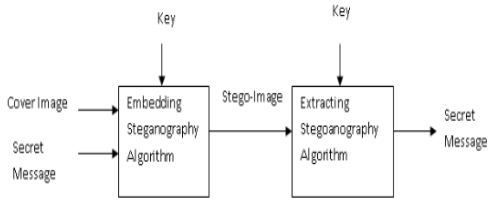
## I. PENDAHULUAN

Dalam ilmu komputer khususnya dalam ilmu informatika, penyampain pesan dari satu orang ke orang yang lainnya merupakan hal yang sudah sangat wajar. Namun saat ini, bagaimana pesan yang ingin disampaikan ke orang tersebut tidak diketahui oleh orang banyak dalam arti kata rahasia. Dalam ilmu komputer istilah peyampaian pesan ini ada beberapa cara. Diantaranya adalah metode kriptografi yang menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Yang kedua adalah metode steganografi penyembunyian data digital dalam berkas-berkas (*file*) komputer. Contohnya, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap *pixel* ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).

Pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi. Contohnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat di antara garis-garis yang kelihatan.

Di dalam tulisan ini *Hidden Messages* diimplementasikan ke dalam gambar yang di *share* secara publik menggunakan fasilitas *google map marker*, jika kita ingin mencari peta yang ingin dicari biasanya menggunakan *google map*. Aplikasi ini dapat menuntun kita ke lokasi yang ingin dituju. Biasanya pada lokasi yang dituju terdapat *marker*, biasanya berupa deskripsi dan gambar atau foto *real* dari tempat tersebut. Gambar atau foto *real* dari lokasi tersebut bisa disisipkan informasi tambahan yang sifatnya rahasia. Penyisipan informasi atau pesan rahasia tersebut dapat menggunakan metode steganografi.

Pada teknik steganografi metodeLSB (*Least Significant Bit*) paling sering digunakan untuk menyisipkan pesan rahasia pada gambar. *Bit* paling signifikan dari beberapa atau semuadari *byte* dalam Sebuah gambar berubah menjadi *bit* pesan rahasia. Bila menggunakan Gambar dengan warna 24-*bit* RGB, sedikit dari masing-masing komponen warna merah, hijau dan biru bisa digunakan. Dengan kata lain, satu piksel dapat menyimpan 3 *bit* pesan rahasia[1].




Gambar 1. Model Dasar Steganografi

Komponen

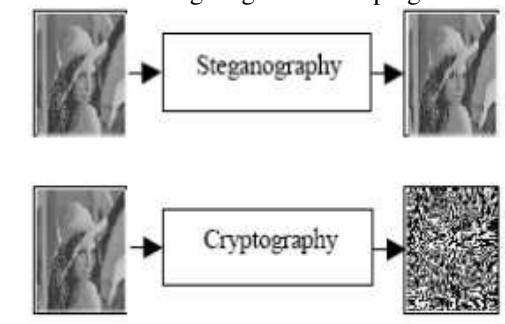
- *Secret Message*- Pesan yang akan tertanam
- *Cover Image*- Sebuah gambar dimana Pesan Rahasia akan tertanam.
- *Stego Image*- Gambar yang mengandung pesan rahasia.

- *Key*-Data tambahan yang diperlukan untuk proses *embedding* dan *extracting*.
- *Embedding Steganography Algorithm*- Algoritma Steganografi yang digunakan untuk menanamkan pesan rahasia pada gambar.
- *Extracting Steganography Algorithm*- Fungsi Invers dari *embedding*, dimana digunakan untuk mengekstrak pesan tertanam (pesan rahasia) dari gambar stego [2].

## II. TINJAUAN STUDY

### A. Perbedaan Steganografi dengan Kriptografi

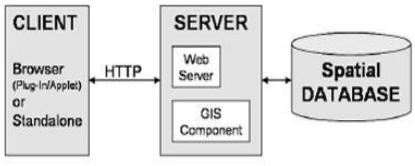
*Steganography* berbeda dengan *cryptography*, letak perbedaannya adalah pada hasil keluarannya. Hasil dari *cryptography* biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi), sedangkan hasil keluaran dari steganography memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses [3]. Gambar dibawah ini menunjukkan ilustrasi perbedaan antara steganografi dan kriptografi.




Gambar 2. Perbedaan Steganografi dan Kriptografi

### B. Peta Digital dalam GIS

Bentuk umum arsitektur dari peta di web dapat dilihat pada gambar berikut :




Gambar 3. Peta Digital dalam GIS

Pada gambar di atas, interaksi *client* dengan server berdasarkan skenario *request* dan respon. Web browser mengirim request ke web server. Karena web server tidak memiliki kemampuan merespon peta, maka request berkaitan dengan pemrosesan peta akan diteruskan oleh web server ke server aplikasi dan map server. Hasil dari pemrosesan akan dikembalikan lagi melalui server web, terbungkus dalam bentuk file HTML atau applet[4].

### C. Permasalahan

1) Bagaimanakah menyembunyikan pesan atau informasi pada gambar tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari gambar semula ?

2) Bagaimanakah penyampaian pesan tersembunyi dari lokasi suatu tempat menggunakan fasilitas publik tanpa diketahui ataupun dicurigai oleh pengguna publik ?

### D. *Literatur Riview*

Banyak penelitian yang sebelumnya dilakukan mengenai metode steganografi dan *Geografical Information System*. Dalam upaya pengembangan kedua hal tersebut, perlu dilakukan studi pustaka sebagai salah satu dari penerapan metode penelitian. Diantaranya adalah mengindentifikasi kesenjangan (*identify gaps*), menghindari pembuatan ulang (*Reventing The Wheel*), mengidentifikasi metode yang pernah dilakukan, meneruskan penelitian sebelumnya, serta mengetahui orang lain yang spesialisasi dan area penelitiannya sama di bidang ini. Beberapa *literature review* tersebut adalah sebagai berikut :

1) Penelitian yang dilakukan oleh Ermadi Satriya Wijaya, Yudi Prayudi dariJurusan Teknik Informatika, Fakultas Teknologi Industri,Universitas Islam Indonesia pada jurnal Media Informatika, Vol. 2, No. 1, Juni 2004, 23-38 ISSN: 0854-4743 berjudul " Konsep *Hidden Masagge* dengan teknik *steganografi dynamic cell spreading* ". Penelitian ini membahas Proses penyembunyian atau Proses penyembunyian atau steganografi mempunyai berbagai macam bentuk metode juga implementasi program. Pada alamat website www.1ecs.com pada bagian *steganography tools* (*hidden message*) terdapat sejumlah link untuk *download software* steganografi.

2) Penelitian yang dilakukan oleh Deny Wiria Nugraha, Jurusan Teknik Elektro, Fakultas Teknik, Universitas Tadulako pada Jurnal Ilmiah Foristek Vol. 2, No. 1, Maret 2012 dengan judul "Perancangan Sistem Informasi Geografis Menggunakan Peta Digital", Setelah dilakukan perancangan sistem informasi geografis menggunakan peta digital[5].

3) Penitian yang dilakukan oleh Thiyagarajan P, Prasanna Venkatesan V, Aghila G, (2012) pada CDBR-SSE Lab Department of Computer Science, Pondicherry University dengan judul "*Stego-Image Generator* (SIG) - *Building Steganography Image Database*". Yang berisi *There are numerous tools available either in free or licensed version in the Internet for the production of Stego-Images. Mother of all Steganography algorithms in spatial domain is Least Significant Bit (LSB) algorithm. Our proposed SIG tool uses the LSB algorithm combined with choice in selecting the no of LSB bits to be replaced, choice in selecting the colour channel, choice in selecting the no of rows to be affected. In table 1 the proposed SIG tool is compared with various Stego-Tools against various parameters*[6].

TABEL I
STEGO IMAGE GENERATOR

| S.No | Tools | Input Such As Channel, Number of LSB to be Replaced in Cover Image | Format | Number of Stego-Images Produced on per Cover Image |
|---|---|---|---|---|
| 1 | S-Tools | No | BMP | 1 |
| 2 | Camera Shy | No | JPEG | 1 |
| 3 | Steganos | No | BMP | 1 |
| 4 | Steghide | No | BMP | 1 |
| 5 | Info Stego | No | BMP, JPEG, PNG | 1 |
| 6 | SIG (Stego Image Generator) | Yes | All format expect compressed image format | 63 |

4) Penelitian oleh Jhoni Verlando Purba, Marihat Situmorang, Dedy Arisandi , Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Sumatera Utara dengan judul "Implementasi Steganografi Pesan Text Ke Dalam File *Sound* (.Wav) Dengan Modifikasi Jarak Byte Pada Algoritma *Least Significant Bit* (LSB)" pada jurnal Jurnal Dunia Teknologi Informasi Vol. 1, No. 1, (2012) 50-55, Steganografi data berupa pesan text atau informasi data ke dalam media audio dapat diimplementasikan menggunakan metode modifikasi *Least Significant Bit* yaitu dengan mengkonversikan setiap nilai–nilai bit data kedalam nilai–nilai bit media audio, Ukuran dari daya tampung media audio tidak mempengaruhi seberapa besar jumlah data yang dapat disembunyikan.

5) Penelitian oleh Hendra Bunyamin, Andrian, Fakultas Teknologi Informasi, Universitas Kristen Maranatha, Jurnal Informatika, Vol. 5, No. 2, Desember 2009: 107 – 117 dengan judul "Aplikasi Steganography pada File dengan Menggunakan Teknik *Low Bit Encoding* dan *Least Significant Bit*" bahwa Setiap pengujian file mengalami perubahan yang berbeda-beda. Pada file gambar yang telah mengalami *steganography* akan mengalami perubahan kontras pada gambar, gambar akan tampak lebih terang. Untuk Pengujian file media, file media akan mengalami kerusakan pada audio.Kerusakan yang dimaksud adalah adanya *noise* pada audio.

6) Penelitian yang dilakukan oleh Hendrikus Zebua, Setia Wirawan, pada Jurusan Teknik Informatika Universitas Gunadarma (2010) dengan Judul "Implementasi Steganografi Pada Berkas Audio Wav Untuk Penyisipan Pesan Gambar Menggunakan Metode *Low Bit Coding*" bahwa Dengan semakin berkembangnya teknologi informasi dan telekomunikasi, maka perhatian pada tingkat keamanan akan menjadi semakin penting. Salah satunya adalah tingkat kemanan pengiriman data atau informasi. Peningkatan keamanan pengiriman data dapat dilakukan dengan menggunakan steganografi. Steganografi adalah teknik menyembunyikan pesan ke dalam sebuah media pembawa (*carrier*)[7].

## III. PEMBAHASAN

Pada pembahasan ini penulis menggunakan bantuan *software* aplikasi untuk penyisipan informasi kedalam *image*, yakni dengan matlab. Hasil konversi *image* pada matlab adalah berbentuk matrik, dengan bantuk matrik tersebut dapat dihasilkan berupa grafik yang pengukurannya atau penggambarannya melalui bantuan aplikasi yang disebut histrogram. Penulis mengunakan diagram *flowchart* sebagai pendefisinian pemrograman. Seperti pada gambar dibawah ini. Sehingga *image* yang akan dikonvert atau digabungkan ke dalam sebuah teks dapat terdefisinikan. Pada tulisan ini *image* yang digunakan bitmap. Bitmap adalah representasi dari citra grafis yang terdiri dari susunan titik yang tersimpan di memori komputer. Dikembangkan oleh Microsoft dan nilai setiap titik diawali oleh satu *bit* data untuk gambar hitam putih, atau lebih bagi gambar berwarna.Ukuran sebenarnya untuk **n**-bit ($2^n$ warna) *bitmap* dalam *byte*dapat dihitung : ukuran file BMP

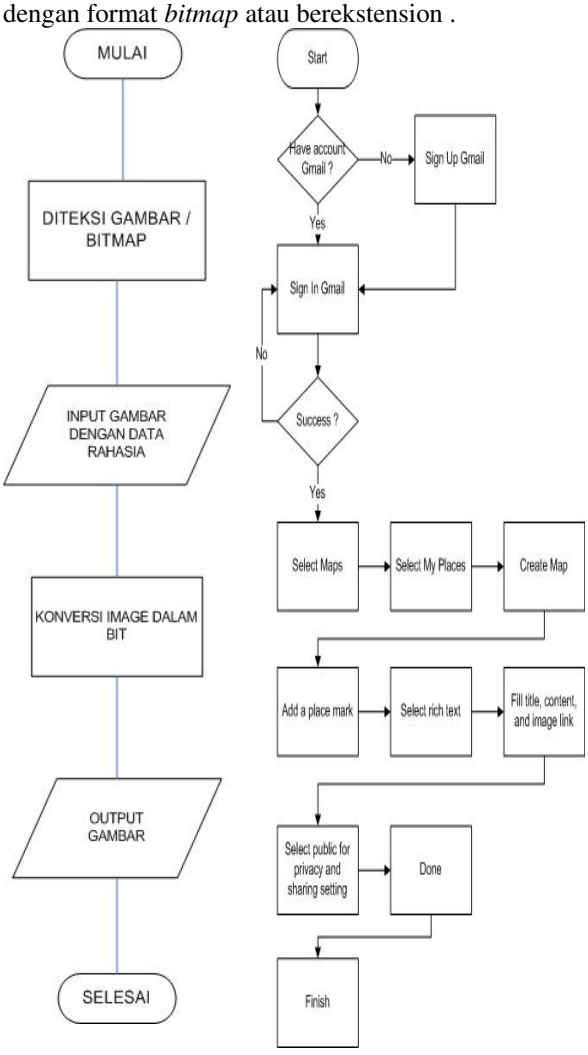
$$\approx 54 + 4 \cdot 2^n + \frac{lebar \cdot tinggi \cdot n}{8},$$

dimana tinggi dan lebar dalam pixel.

Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam gambar ini

ditampilkan, ditunjukkan dengan jumlah baris dan kolom, contohnya 1024x768. Untuk menampilkan citra *bitmap* pada monitor atau mencetaknya pada printer, komputer menterjemahkan *bitmap* ini menjadi *pixel* (pada layar) atau titik tinta (pada printer). Beberapa *format filebitmap* yang populer adalah BMP, PCX dan TIFF.

Pada gambar dibawah ini dijelaskan skema *flowchart* sistem untuk memasukan *image* , proses penyisipan gambar serta image hasil keluarannya. Gambar yang digunakan dalam sistem ini tentunya dengan format *bitmap* atau berekstension .




Gambar 4. Skema Flowchart Pemrograman Steganografi dan Flowchart Google *Map Marker*

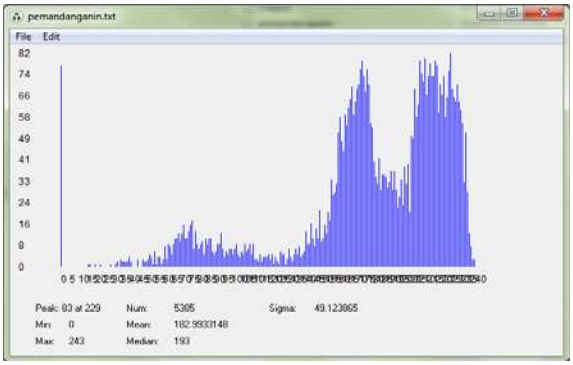
## IV. ANALISA DAN HASIL

Penulis memberikan analisa berupa inputan proses serta *output* yang dihasilkan. Pada percobaan ini penulis memasukan *image* view suatu danau, kemudian melalui program aplikasi steganografi image tersebut disisipi teks yang sudah dalam format *file*. Di dalam proses tersebut *image* diolah berupa matrik dan matrik tersebut disisipi text yang berupa format file.txt. Setelah diolah maka hasil keluaran proses juga berupa file *image*. Hasil *image* yang didapat bentuknya hampir sama atau tidak berbeda dengan image asli atau image awal. Penulis menggunakan *tools* mengujian untuk melihat perbedaan ini. Karena secara visual atau sekilas mata kedua objek tersebut hampir sama tidak ada yang berbeda. *Tools* yang digunakan adalah aplikasi Histogram.

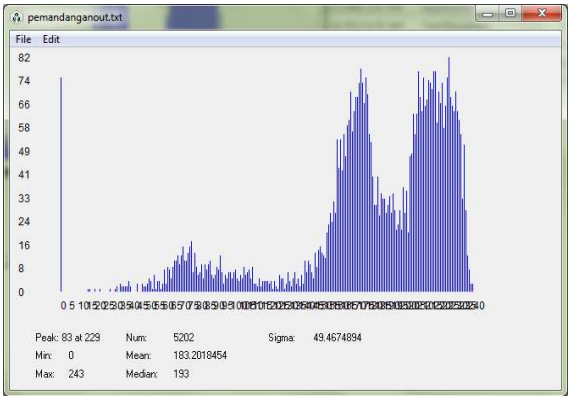

Gambar 5. Isi Teks Sisipan

Gambar diatas adalah pesan atau informasi yang ingin disisipi dalam image, pesan tersebut ditulis dalam fomat teks dalam aplikasi Notepad.Sehingga pesan atau informasi ini dapat secara rapi tertulis, jika pesan atau informasinya banyak dalam artian kata-katanya banyak juga tidak terpengaruh pada sistem.

Gambar 6. Sebelah Kiri *Image* Awal, Kanan *Image* Hasil




Gambar 7. Skema Grafik Input Image pada Histogram




Gambar 8. Skema Grafik Output *Image* pada Histogram

Pada Gambar 9 dibawah ini adalah penerapan sebenarnya pada aplikasi *google map marker,* pada gambar view danau Situ Bulakan di daerah Tangerang telah disisipi sebuah informasi pada teks.


Gambar 9. Skema Penerapan pada *Google Map Marker*

## V. KESIMPULAN

Dalam penyajiannya *System Steganografi* adalah suatu sistem yang dapat mengaplikasikan suatu penyisipan pesan rahasia ke dalam suatu gambar yang dalam hal ini adalah dengan format Bitmap. Dasar dari penyisipan pesan rahasia dalam suatu gambar digital adalah penggantian *rendundantbit* pada LSB(*Least Significant Bit*) dengan data pesan rahasia. Dalam percobaan penyisipan pesan rahasia dalam gambar menggunakan MatLab, proses penyisipan maupun ekstraksi akan menghasilkan *cover image* yaitu gambar asli yang belum disisipi pesan, dan *stego image* yaitu gambar asli yang sudah disisipi pesan rahasia tanpa merubah kwalitas gambar asli secara visual. Setelah *stego image* dihasilkan maka proses berikutnya adalah mem-publish *stego image* tersebut ke dalam fasilitas publik dengan menggunakan layanan *google map marker*. Sehingga detail *view* yang berisi *stego image* dari lokasi tersebut dapat di *extact* informasinya yang bersifat rahasia oleh pengguna yang mengerti terdapat pesan rahasia di dalamnya dan juga mempunyai *key* untuk membukanya, tanpa sepengetahuan ataupun kecurigaan pengguna publik.

## REFERENSI

[1] Verlando Purba Jhoni, Situmorang Marihat, Arisandi Dedy, (2012), *Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (Lsb).* Jurnal Dunia Teknologi Informasi. Universitas Sumatra Utara.

[2] Bunyamin Hendra, Andrian, (2009), *Aplikasi Steganography pada File dengan Menggunakan Teknik Low Bit Encoding dan Least Significant Bit.Jurnal Informatika.* Jurusan Teknik Informatika. Unversitas Kristen Maranatha

[3] Satriya Wijaya, Ermadi. , Prayudi Yudi (2004) *Konsep Hidden Message Menggunakan Teknik Steganografi Dynamic Cell Spreading*.Jurnal Media Informatika.Universitas Islam Indonesia.

[4] Ruslan Nuryadin, (2005) Panduan Menggunakan MapServer.

[5] Wiria Nugraha Deni (2012) *Perancangan Sistem Informasi Geografis Menggunakan Peta Digital.* Jurnal Ilmiah Foristek. Universitas Tadulako.

[6] Thiyagarajan P, Prasanna Venkatesan V, Aghila G (2012), *Stego-Image Generator (SIG) - Building Steganography Image Database.* DBR-SSE Lab Department of Computer Science, Pondicherry University.

[7] Zebua Hendrikus, Wirawan Setia, (2010), *Implementasi Steganografi Pada Berkas Audio Wav Untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding*, Jurusan Teknik Informatika. Universitas Gunadarma