Steganografi Menggunakan Teknik Substitusi LSB pada Peta Vektor Digital

Rita Wijaya (13509098)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509098@std.stei.itb.ac.id

***Abstract*—Steganografi digital merupakan seni dalam menyembunyikan informasi digital. Steganografi dapat diimplementasikan pada berbagai media. Salah satu media steganografi yang dapat dimanfaatkan adalah peta vektor digital. Pada makalah ini, akan dipelajari teknik steganografi pada peta vektor digital. Teknik steganografi menggunakan teknik substitusi LSB ini akan diterapkan dan diukur kinerjanyanya terhadap akurasi peta vektor berbentuk *shapefile*. Perbandingan akurasi peta diukur menggunakan rumus PSNR pada peta vektor digital. Berdasarkan nilai perbandingan PSNR yang diperoleh, akan dilakukan analisis terhadap kinerja teknik steganografi ini.**

Index Terms*—PSNR, *shapefile*, *steganografi*, substitusi *LSB

I. PENDAHULUAN

Komunikasi telah menjadi kebutuhan utama dalam hidup. Perkembangan teknologi informasi seperti Internet dan *smartphone* menjadikan komunikasi digital semakin diminati orang-orang. Namun, kemudahan berkomunikasi ini tidak dijamin keamanannya. Ancaman akan adanya pihak tidak diinginkan di tengah-tengah komunikasi pasti selalu ada. Kebutuhan akan keamanan berkomunikasi inilah yang melahirkan berbagai teknik melindungi informasi, salah satunya steganografi.

Steganografi digital memungkinkan suatu pesan rahasia dibungkus ke dalam media lain sehingga pesan sebenarnya tidak terlihat. Hanya pihak yang terlibat dalam komunikasi saja yang mengetahui bahwa pesan tersebut ada dan dapat membuka isinya. Berkas gambar, audio, dan video merupakan media yang populer digunakan sebagai media steganografi. Namun, media steganografi tidak terbatas pada berkas-berkas tersebut saja. Peta digital juga dapat dimanfaatkan sebagai media steganografi.

Salah satu metode yang umum digunakan dalam steganografi adalah teknik modifikasi LSB. Selanjutnya, pada makalah ini akan dipelajari teknik steganografi dengan metode LSB pada peta vektor digital. Teknik tersebut akan diterapkan pada peta vektor digital berbentuk *shapefile* dan diukur kinerjanya terhadap peta awal.

II. LANDASAN TEORI

A. Steganografi

Steganografi adalah seni dan ilmu menyembunyikan pesan dengan cara apa pun sehingga orang lain selain penerima pesan tidak mencurigai adanya pesan tersembunyi. Kata steganografi sendiri berasal dari bahasa Yunani yang berarti tulisan yang tertutup. Terdapat beragam metode yang dapat digunakan dalam steganografi, antara lain penggunaan tinta yang tidak terlihat, penyusunan ulang huruf-huruf penyusun pesan, dan *microdots* [1].

Meskipun sama-sama bertujuan melindungi pesan, steganografi berbeda dengan kriptografi. Dalam kriptografi, pesan diubah dalam bentuk yang tidak dapat dimengerti, namun tidak menyembunyikan fakta bahwa pesan itu ada. Sedangkan dalam steganografi, kita berusaha menyembunyikan keberadaan pesan supaya tidak menarik perhatian.

Teknik steganografi dapat dibagi menjadi 3 jenis berdasarkan media yang digunakannya[2], yaitu:

1. Steganografi fisik (*physical steganography*)
   Steganografi fisik ini telah digunakan secara luas sejak zaman kuno. Steganografi fisik melakukan manupulasi terhadap benda fisik untuk menyembunyikan pesan. Contoh steganografi jenis ini adalah penulisan pesan di kertas menggunakan tinta yang tidak terlihat, penulisan pesan di kayu yang kemudian ditutupi dengan lilin dan penulisan pesan di balik perangko.
2. Steganografi digital (*digital steganography*)
   Steganografi digital adalah seni menyembunyikan data di dalam data. Dengan teknik ini, data rahasia dapat disembunyikan di balik gambar, teks, atau audio yang direpresentasikan dalam data biner.
3. Steganografi tercetak (*printed steganography*)
   Hasil dari steganografi digital dapat juga berupa dokumen yang tercetak. Ukuran huruf dan karakteristik dokumen dapat dimanupulasi untuk membawa pesan rahasia. Seseorang yang mengetahui teknik penyembunyiannya dapat membaca kembali pesan yang disembunyikan.

Seiring perkembangan teknologi informasi, steganografi digital juga mengalami perkembangan yang pesat. Secara umum, terlepas dari media yang digunakan,

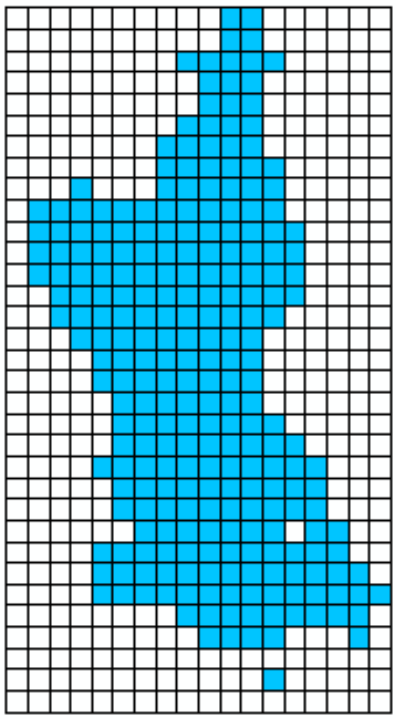
proses steganografi digital terdiri dari langkah-langkah berikut.

1. Identifikasi bits yang redundan dalam media perantara. Bits redundan adalah bits yang dapat dimodifikasi tanpa mengurangi kualitas media perantara.
2. Memilih subset bits redundan untuk ditimpa dengan data dari pesan rahasia

B. Peta Digital

Terdapat dua jenis model data yang digunakan untuk menyimpan data geografis [3], yaitu:

1. Model data raster
   Model data raster membagi suatu area menjadi kotak-kotak kecil berukuran sama. Informasi dari setiap kotak kecil kemudain disimpan dalam bentuk matriks. Contoh model data raster dapat dilihat pada Gambar 1. Biasanya model daata raster digunakan untuk menyimpan informasi berupa ketinggian tanah, keasaman tanah, atau kedalaman air.



Gambar 1. Representasi model data raster (sumber: http://www.extension.org/sites/default/files/w/4/4c/21999 39046_f3bf66d23f_o.gif)

2. Model data vektor
   Model data vektor memodelkan suatu area sebagai objek-objek geometris, seperti titik, garis, dan poligon. Titik mewakili suatu lokasi spesifik, seperti pusat kota atau terminal bis. Garis dapat mewakili fitur linear seperti jalan, pipa air, atau jalur kereta api. Sedangkan poligon mewakili bentuk yang lebih kompleks seperti batas negara atau pulau. Contoh model data raster dapat dilihat pada Gambar 2. Dalam GIS, model data vektor umumnya digunakan untuk menyimpan informasi jalan dan daerah vegetasi tumbuhan.

Model data raster dan vektor memiliki kelebihan dan kekurangannya masing-masing. Oleh sebab itu, kedua model data tersebut digunakan bersama untuk membentuk suatu peta. Setiap informasi spesifik disimpan sebagai satu lapisan peta. Tumpukan lapisan informasi inilah yang biasa kita lihat sebagai satu peta utuh.

C. Teknik Substitusi LSB

Teknik steganografi yang paling paling sederhana sekaligus paling populer adalah teknik substitusi LSB. Teknik ini mengganti bit terakhir dari media steganografi dengan bit dari pesan [4]. Secara umum, cara kerja teknik subtitusi ini adalah sebagai berikut. Misalkan kita memiliki informasi pada media seperti:

10110101
10010111
10000100
00110001
01100001
10110101
01100110
10110101

Kemudian, kita akan menyisipkan pesan “00100101” pada deretan informasi awal yang ada. Maka, setiap bit pesan akan disubstitusi satu per satu pada informasi awal. Setelah dilakukan proses substitusi, informasi media akan berubah menjadi sebagai berikut.

1011010**0**
1001011**0**
1000010**1**
0011000**0**
0110000**0**
1011010**1**
0110011**0**
1011010**1**

Supaya tidak menyebabkan perubahan besar, penggantian bit ini hanya boleh dilakukan pada informasi yang sifatnya redundan dan memiliki toleransi terhadap perubahan kecil. Informasi yang memiliki toleransi ini misalnya informasi warna pada bitmap gambar atau frekuensi pada data audio. Perubahan kecil pada warna gambar tidak dapat dideteksi oleh mata manusia. Frekuensi audio yang bergeser kecil juga tidak dapat terdeteksi oleh pendengaran biasa.

Sejak ditemukan, teknik LSB telah mengalami berbagai perkembangan. Beberapa modifikasi yang dapat dilakukan terhadap teknik LSB antara lain:

1. Substitusi bit tidak dilakukan secara sekuensial.
2. Substitusi tidak hanya dilakukan terhadap 1 bit, namun beberapa bit sekaligus.
3. Bit yang diubah tidak hanya bit terakhir, melainkan bit pada posisi tertentu.

D. PSNR (Peak Signal to Noise Ratio)

PSNR digunakan untuk mengukur kualitas media yang

telah mengalami perubahan secara kuantitatif. PSNR dapat dimodifikasi sesuai media yang digunakan. Pada peta vektor, rumus PSNR yang dapat digunakan adalah:

$$\text{PSNR} = 20 \log_{10}\left(\frac{MAX(V_{x,y})}{RMSE}\right), \quad (1)$$

$$\text{RMSE} = \sqrt{\sum\left(\left(V_{x,y} - V_{x,y}^{d}\right)^2 / \left(V_{x,y}^2\right)\right)} \quad (2)$$

dengan $V_{x,y}$ adalah koordinat awal dari suatu titik, dan $V_{x,y}^{d}$ adalah koordinat setelah perubahan [5]. PSNR memiliki satuan *decibel* (dB). RMSE adalah nilai rata-rata pergeseran titik. Peta yang identik akan memiliki nilai RMSE 0. Semakin besar perbedaan kedua peta, semakin tinggi nilai RMSE. Akibatnya, semakin kecil nilai PSNR yang dimiliki. Semakin tinggi nilai PSNR yang dimiliki, semakin bagus kualitas peta yang dihasilkan.

III. Algoritma Steganografi pada Peta Vektor Berbentuk Shapefile

A. Peta Vektor

Sebuah peta vektor terdiri dari data spasial, data atribut, dan data tambahan berupa index atau deskripsi tambahan. Data spasial menggambarkan objek geografis di dunia nyata. Gambar dari data spasial suatu peta vektor dapat dilihat pada Gambar 2. Data atribut mendeskripsikan properti dari peta seperti nama, kategori, dan informasi lainnya. Data atribut menyimpan informasi penting dan tidak dapat diubah, begitu juga dengan data tambahan. Oleh sebab itu, data atribut dan data tambahan jelas tidak dapat digunakan sebagai lokasi penyisipan pesan. Satu-satunya data yang dapat dimanfaatkan sebagai lokasi penyisipan pesan adalah data spasial. Data spasial memiliki menyimpan informasi koorrdinat yang dapat dimanipulasi untuk disisipi pesan [5].

Gambar 2. Representasi model data vektor (sumber: http://www.extension.org/sites/default/files/w/4/4c/21999 39046_f3bf66d23f_o.gif)

Salah satu format peta vektor yang populer digunakan oleh aplikasi GIS (*Geographic Information System*) adalah *shapefile*. Format teknis dari *shapefile* ini terdefinisi pada [6]. *Shapefile* sesungguhnya terdiri dari beberapa berkas. Tiga berkas utama penyusun sebuah *shapefile* berekstensi *.shp, *.shx, dan *.dbf. Selain ketiga berkas utama tersebut, *shapefile* dapat diikuti berkas pilihan lainnya berupa *.prj, *.sbn, *.sbx, *.fbn, *.fbx, *.ain, *.aih, *.ixs, *.mxs, *.atx, *.shp.xml, atau *.cpg.

Berkas yang paling penting dari *shapefile* adalah *.shp. Berkas ini yang menyimpan data spasial dari peta. Berkas *.shp ini memiliki *header* sepanjang 100 *byte* yang menjelaskan tentang *shapefile* itu sendiri. Tipe bentuk suatu geometri tersimpan pada *header* utama berkas dan *header* tiap *record*. Terdapat 14 tipe bentuk yang telah terdefinisi hingga saat ini seperti yang dijabarkan padaTabel 1.

Tabel 1. Nilai ID dan bentuk yang terdefinisi pada *shapefile*

No	Nilai ID	Bentuk
1	0	Null
2	1	Point
3	3	Polyline
4	5	Polygon
5	8	MultiPoint
6	11	PointZ
7	13	PolylineZ
8	15	PolygonZ
9	18	MultiPointZ
10	21	PointM
11	23	PolylineM
12	25	PolygonM
13	28	MultiPointM
14	31	MultiPatch

Masing-masing tipe bentuk memiliki *header* dan format *record* yang berbeda-beda. Selain tipe Null, setiap tipe bentuk memiliki satu kesamaan yaitu informasi bentuknya tersusun dari titik-titik. Setiap titik memiliki nilai absis dan ordinat yang bertipe *double* (*signed 64-bit IEEE double-precision floating point number*). Pada steganografi dengan media peta vektor, informasi koordinat titik inilah yang dimanfaatkan untuk menyisipkan informasi. Suatu peta biasanya tersusun dari banyak titik dan perubahan jarak kecil pada titik sulit dideteksi dengan penglihatan biasa. Selain itu, setiap peta memang memiliki toleransi kesalahan terhadap jarak pengukuran [5]. Oleh sebab itu, informasi berupa lokasi titik ini dianggap sebagai posisi yang cocok untuk menyisipkan pesan rahasia.

B.Algoritma Penyisipan Pesan

Pada bagian ini akan dijelaskan teknik penyisipan pesan pada data spasial peta vektor. Pertama-tama, simpan informasi berupa panjang pesan yang akan disispkan sebagai *header* pesan. *Header* yang menyimpan informasi panjang pesan ini dilakukan supaya penerima peta tetap dapat membaca pesan tanpa mengetahui panjang pesan. Sebelum penyisipan dimulai kita harus memastikan bahwa peta cukup untuk menampung seluruh pesan. *Header* pesan dapat disesuaikan dengan kebutuhan. Apabila tipe pesan telah terdefinisi pada *header*, maka pembaca pesan tidak perlu mengetahui tipe pesan saat pembacaan. Namun, apabila tipe pesan tidak terdefinisi pada *header*, maka pembaca harus mengetahui tipe pesan untuk membaca pesan hasil ekstraksi.

Berikut langkah-langkah penyisipan pesan pada peta vektor:

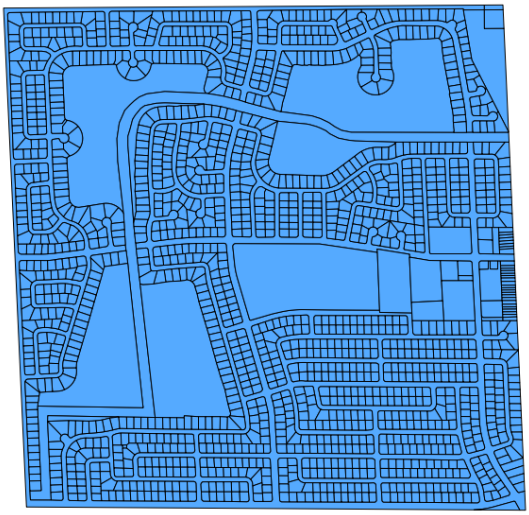
1. Hitung jumlah titik yang ada pada peta cover
2. Hitung panjang pesan (termasuk *header*) yang akan disisipkan
3. Apabila jumlah titik pada peta tidak cukup untuk menampung seluruh pesan, terminasi proses penyisipan.
4. Baca dan salin kembali *header* utama peta
5. Untuk setiap *record* yang ada pada peta, lakukan langkah berikut:
   a. Baca dan salin kembali *header record*
   b. Berdasarkan informasi tipe bentuk yang telah dibaca, cari posisi *record* yang menyimpan nilai titik
   c. Untuk setiap titik yang ada pada suatu *record*, lakukan substitusi LSB pada absis dan ordinat dengan pesan hingga seluruh pesan berhasil disisipkan.

Informasi selain posisi titik disalin sama persis seperti keadaan awal. Setelah melalui proses penyisipan informasi tersebut, maka pada peta vektor akan tersimpan sebuah pesan rahasia. Untuk membaca kembali pesan tersebut, seseorang harus mengetahui pasti format pesan dan cara penyisipan dilakukan. Pada bagian berikutnya akan dijelaskan teknik pembacaan kembali pesan yang telah disispkan.

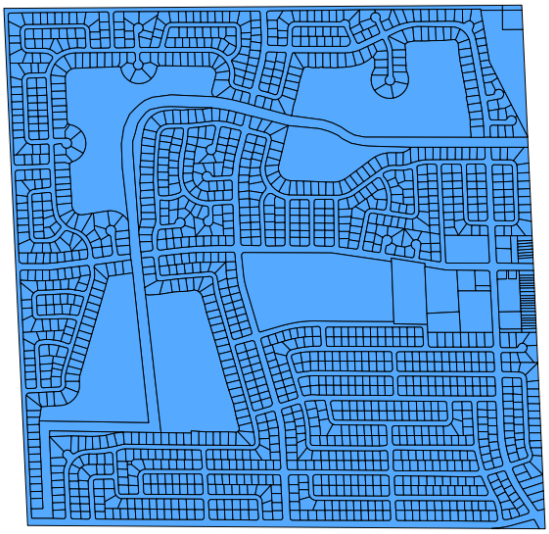
C. Algoritma Pembacaan Pesan

Pesan yang telah disembunyikan menggunakan teknik steganografi tentu harus dapat dibaca kembali. Secara umum, proses pembacaan hanya akan membaca kembali bit-bit pesan yang sebelumnya disisipkan. Setiap algoritma penyisipan memiliki teknik pembacaan tersendiri. Algoritma penyisipan di atas memiliki algoritma pembacaan pesan sebagai berikut.

1. Baca *header* utama peta untuk mengetahui tipe bentuk peta
2. Untuk setiap *record* yang ada pada peta, lakukan langkah berikut:
   a. Baca *header record*
   b. Berdasarkan informasi tipe bentuk setiap *record*, cari posisi *record* yang menyimpan nilai titik
   c. Untuk setiap titik yang ada pada suatu *record*, baca dan simpan nilai bit terakhir dari absis dan ordinat titik
3. Berdasarkan string biner yang telah terbaca, baca *header* pesan untuk mengetahui panjang pesan. Kemudian, simpan pesan sebanyak panjang pesan yang sebenarnya menjadi pesan semula.



(a) Peta awal (sumber: http://www.emapsplus.com/mwh/downloadshape.htm)



(b) Peta berisi pesan

Gambar 3. Perbandingan peta sebelum dan setelah pesan disisipkan

Header pesan yang dibaca dapat disesuaikan dengan *header* yang didefinisikan saat penyisipan. Informasi yang terdapat pada *header* dapat disesuaikan dengan format yang telah disepakati. Apabila tipe pesan terdefinisi pada *header*, maka pesan yang terbaca dapat disimpan kembali sesuai tipe tersebut. Namun, apabila tipe pesan tidak terdefinisi pada *header*, maka pembaca pesan perlu mengetahui pasti tipe pesan untuk setiap peta

yang berasosiasi. Untuk meningkatkan keamanan informasi pada peta, lebih baik informasi berupa tipe pesan tidak disimpan pada *header*. Namun, informasi tambahan tersebut juga memiliki efek positif, yaitu untuk mempermudah proses pembacaan pesan. Seseorang tidak perlu mengingat tipe pesan yang bersangkutan setiap pembacaan pesan dari peta.

IV. IMPLEMENTASI DAN PENGUJIAN

Teknik steganografi pada peta vektor digital di atas kemudian diimplementasikan menggunakan bahasa pemrograman Java. Program ini menerima masukan berupa berkas *.shp sebagai media steganografi dan 1 berkas lainnya sebagai pesan yang akan disembunyikan. Program ini kemudian akan menyembunyikan suatu pesan tersebut ke dalam peta. Setelah pesan berhasil disembunyikan, peta berisi pesan akan dibandingkan kembali dengan peta awal dengan perbandingan PSNR. Berikutnya, program dapat membaca kembali pesan yang telah disembunyikan dengan menggunakan algoritma pembacaan pesan.

Pada implementasi ini, *header* pesan dialokasikan sepanjang 32 bit untuk menyimpan panjang pesan dalam *byte*s. Karena ekstensi pesan tidak disimpan sebagai *header* pesan, pesan hasil pembacaan harus diketahui formatnya menyimpan dan membuka kembali pesan tersebut. Pada implementasi yang dilakukan kali ini, pesan tersembunyi berhasil dibaca kembali secara utuh untuk setiap pengujian. Peta awal dan peta berisi pesan terlihat sama dan tidak dapat dibedakan melalui observasi visual.

Salah satu peta hasil pengujian teknik steganografi ini dapat dilihat pada Gambar 3. Gambar 3 (a) merupakan peta awal yang akan disisipkan pesan, sedangkan Gambar 3 (b) merupakan peta yang telah berisi pesan tersembunyi. Meskipun keduanya terlihat sama, sebagian titik pada peta sebenarnya telah mengalami perubahan. Untuk mengetahui seberapa besar perubahan yang diakibatkan, peta berisi pesan dibandingkan kembali terhadap peta awalnya dengan menghitung nilai PSNR. Hasil pengujian dapat dilihat padaTabel 2.

PSNR pada setiap pengujian dihitung menggunakan rumus (1) dan (2). Nilai PSNR dari setiap pengujian cukup tinggi dengan nilai di atas 250. Hal ini berarti akurasi peta yang berisi pesan tidak bergeser terlalu jauh dan secara umum masih dapat digunakan. Meskipun demikian, peta hasil steganografi tidak direkomendasikan untuk digunakan oleh aplikasi yang memerlukan ketelitian tinggi. Teknik ini juga memiliki kelemahan lain yaitu pesan yang disisipkan tidak dapat berukuran terlalu besar. Hal ini disebabkan karena modifikasi hanya dilakukan terhadap 1 bit terakhir dari nilai absis dan ordinat sehingga daya tampung pesan kecil. Apabila substitusi dilakukan terhadap lebih dari 1 bit sekaligus, maka daya tampung pesan akan bertambah lebih dari 2 kali lipatnya.

Teknik ini masih dapat dikembangkan. Apabila ingin memperbesar daya tampung peta, maka jumlah bit yang disubstitusi dapat diperbanyak hingga batasan tertentu. Apabila pesan dikompresi sebelum penyisipan dilakukan, maka ukuran pesan dapat dikurangi. Algoritma steganografi ini juga dapat dimodifikasi supaya pesan yang dapat disisipkan bisa berjumlah lebih dari 1.

Tabel 2. Hasil pengujian teknik steganografi pada peta vektor

No	Ukuran *shapefile*	Ukuran pesan	PSNR
1	412 KB	79 *bytes*	398.6705336247941
2	413 KB	2.16 KB	369.87115112946015
3	440 KB	12 KB	282.11290518458304
4	102 KB	1 KB	282.8775053273776
5	1.239 KB	5.31 KB	273.9988938101392
6	166 KB	1.46 KB	279.4305307820415
7	31.733 KB	2.69 KB	274.26042963086576
8	31.733 KB	21.45 KB	256.1813282461196
9	31.733 KB	43.0 KB	250.12581543103715
10	2.009 KB	178 *bytes*	297.57037368474784

V. KESIMPULAN

Steganografi dapat meningkatkan keamanan suatu pesan dengan cara menyembunyikan keberadaan pesan. Peta vektor digital dapat digunakan sebagai media steganografi. Teknik substitusi LSB untuk steganografi dapat diaplikasikan juga pada media peta vektor digital. Berdasarkan nilai PSNR hasil perbandingan peta awal dan peta berisi pesan, teknik steganografi LSB pada peta vektor ini dinilai memiliki kinerja yang cukup baik. Peta hasil steganografi ini tidak dapat dibedakan dengan peta awal dengan observasi visual. Peta berisi pesan tetap dapat dipergunakan seperti biasa, namun tidak direkomendasikan untuk penggunaan yang memerlukan akurasi tinggi. Teknik ini juga memiliki kelemahan yaitu daya tampung pesannya lebih kecil dibandingkan dengan substitusi blok bit. Daya tampung peta dapat diperbesar dengan menambah jumlah bit yang diperbolehkan untuk disubstitusi. Berkas pesan juga dapat dikurangi ukurannya dengan cara dikompresi terlebih dahulu.

DAFTAR REFERENSI

[1] B. Rahardjo, Keamanan Sistem Informasi Berbasis Internet, Bandung: PT Indocisc, 2005.

[2] D. E. Walia and P. Jain, "An Analysis of LSB & DCT based Steganography," *Global Journal of Computer Science and Technology,* vol. 10, 2010.

[3] A. Silberschatz, H. F. Korth and S. Sudarshan, Database System Concepts, 6th ed., New York: McGraw-Hill, 2011.

[4] V. K. Sharma and V. Shrivastava, "A Steganography Algorithm for Hiding Image in Image by Improved LSB Substitution by Minimize Detection," *Journal of Theoritical and Applied Information Technology*, 2012.

[5] X. Niu, C. Shao and X. Wang, "A Survey of Digital Vector Map Watermarking," *International Journal of Innovative Computing*, vol. 2, December 2006.

[6] Environmental Systems Research Institute, Inc., "ESRI Shapefile Technical Description - An ESRI White Paper," 1998.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Maret 2013

Rita Wijaya (13509098)