Walisongo Journal of Information Technology, Vol. 1 No. 1 (2019): 75-90
DOI : http://dx.doi.org/10.21580/wjit.2019.1.1.4025

Steganografi Pada Digital Image Menggunakan Metode Least Significant Bit Insertion

Siti Nur'aini[1]
[1]Universitas Islam Negeri Walisongo Semarang

Abstract

Steganography is a way to hide messages or confidential data in a medium called a carrier file. In this study steganography is performed using the Least Significant Bit Insertion method, which is to replace the lowest bits of Red Green Blue (RGB) each pixel with the data bits that you want to insert. From the results of this study it can be seen that steganography can be performed by the Least Significant Bit Insertion method. This method causes the color difference between pixels that have not been pasted by messages and pixels that have been pasted by messages. The size of the change or degradation of color depends on the number of characters inserted. The more characters that are inserted the more visible color degradation that occurs. In using the Least Significant Bit Insertion method, it is necessary to consider the type of digital image format used, this is necessary to avoid the loss of messages when extracting. The best digital image format used is the 24-bit BMP because the BMP format is lossless compression.

Keyword: *Embedding, extracting, least significant bit, steganography.*

Abstrak

Steganografi adalah suatu cara untuk menyembunyikan pesan atau data rahasia di dalam suatu media yang disebut *carrier file*. Pada penelitian ini steganografi dilakukan dengan menggunakan metode *Least Significant Bit Insertion* yaitu mengganti bit yang paling rendah dari *Red Green Blue* (RGB) setiap *pixel* dengan bit data yang ingin disisipkan. Dari hasil penelitian ini terlihat bahwa steganografi dapat dilakukan dengan metode *Least Significant Bit Insertion*. Metode ini menyebabkan perbedaan warna antara *pixel* yang belum disisipi pesan dan *pixel* yang telah disisipi pesan. Besar kecilnya perubahan atau degradasi warna tersebut tergantung dari jumlah karakter yang disisipkan. Semakin banyak karakter yang disisipkan akan semakin terlihat degradasi warna yang terjadi. Pada penggunaan metode *Least Significant Bit Insertion* perlu dipertimbangkan jenis format *digital image* yang digunakan, hal ini diperlukan untuk menghindari hilangnya pesan pada waktu *extracting*. Format *digital image* yang paling baik digunakan adalah bmp 24-bit karena format bmp ini bersifat *lossless compression*.

Kata kunci*: Embedding, extracting, least significant bit, steganografi*.

ISSN 2715-0143 (online) ISSN 2714-9048 (print)
http://journal.walisongo.ac.id/index.php/jit/index

1. Pendahuluan

Saat ini internet sudah berkembang menjadi salah satu media yang paling populer di dunia. Karena fasilitas dan kemudahan yang dimilikinya maka internet untuk saat ini sudah menjadi barang yang tidak asing lagi. Sayangnya dengan berkembangnya internet dan aplikasi menggunakan internet, semakin berkembang pula kejahatan sistem informasi. Dengan berbagai teknik, banyak yang mencoba untuk mengakses informasi yang bukan haknya. Maka dari itu, sejalan dengan berkembangnya media internet ini harus juga diikuti dengan perkembangan pengamanan sistem informasi.

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak, salah satunya adalah teknik steganografi. Berbeda dengan teknik kriptografi, steganografi menyembunyikan pesan rahasia agar orang awam tidak menyadari keberadaan dari pesan yang disembunyikan. Teknik ini sering digunakan untuk menghindari kecurigaan orang dan menghindari keinginan orang untuk mengetahui isi pesan rahasia tersebut. Steganografi membutuhkan dua properti, yaitu media penampung dan data rahasia yang akan disembunyikan, media penampung steganografi dapat berupa *image*, *audio* maupun *video* (Munir, 2006).

Walaupun steganografi dapat dikatakan mempunyai hubungan erat dengan kriptografi, tetapi kedua metode ini sangat berbeda. Semua teknik steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganografi lebih dikonsentrasikan pada kerahasiaan komunikasinya bukan pada datanya.

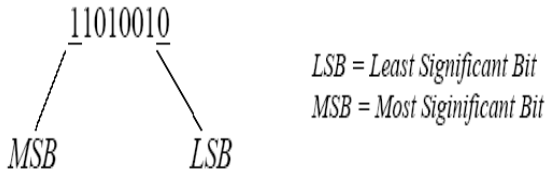
Dalam peristiwa penyerangan gedung WTC tanggal 11 September 2001 disebutkan oleh pejabat pemerintah dan para ahli dari pemerintahan AS yang tidak disebut namanya bahwa "para teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang chat sport, bulletin boards porno dan *website* lainnya". Isu lainnya menyebutkan bahwa teroris menyembunyikan pesan-pesannya dalam gambar-gambar porno di *website* tertentu. Dimana teknik penyembunyian pesannya disebutkan dengan menggunakan steganografi (Suyono, 2004). Hal ini membuktikan bahwa steganografi dapat digunakan untuk menyembunyikan pesan.

Steganografi berasal dari bahasa yunani steganos, yang artinya 'tersembunyi/terselubung', dan graphein, 'menulis' sehingga kurang lebih artinya "tulisan terselubung". Steganografi merupakan seni untuk menyembunyikan pesan di dalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Salah satu proses penyembunyian pesan rahasia

dalam sistem steganografi dapat dilakukan dengan menggunakan *digital image*. *Digital image* ini di sebut sebagai *file* induk (*carrier file*) dan *digital image* yang akan digunakan adalah format bmp 24-bit. Sedangkan *image* yang telah disisipi pesan disebut *stego-image*. Metode yang digunakan untuk menyembunyikan pesan yaitu dengan *Least Significant Bit Insertion.* Steganografi pada *digital image* digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada *carrier file*. Sehingga dengan keterbatasan tersebut manusia tidak akan mencurigai bahwa *digital image* tersebut telah disisipi pesan rahasia (Sellars, 2009).

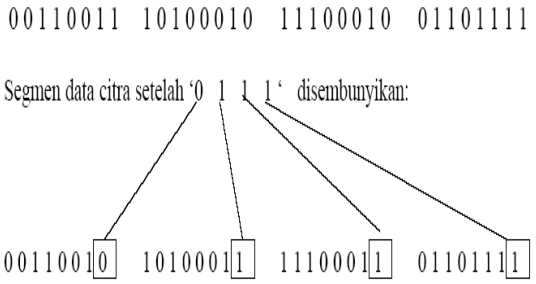
2. Metode

Metode yang digunakan dalam penelitian ini adalah *Least Significant Bit* (LSB) *Insertion* merupakan pendekatan yang sederhana untuk menyembunyikan pesan di dalam suatu *carrier file*. Metode ini diterapkan pada format *image* seperti bmp. Prinsip kerja dari metode ini yaitu mengganti LSB dari RGB setiap *pixel* dengan bit pesan. *Stego-image* yang dihasilkan nantinya akan terlihat sama dengan gambar sebelum disisipkan karena dalam proses penggantiannya dilakukan pada bit LSB sehingga tidak akan nampak perbedaan yang signifikan pada *pixel* tersebut. Untuk metode LSB *insertion* harus digunakan *digital image* yang bersifat *lossless compression* hal ini dilakukan untuk menghindari hilangnya pesan yang tersimpan dalam *stego-image* karena proses kompresi. (Bender, 1996)



Gambar 2

Susunan bit pada sebuah *Byte*



Gambar 3

Proses Penyembunyian pesan dengan Metode *LSB Insertion*

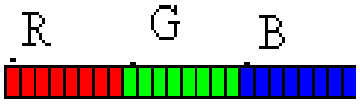
Pada gambar 3 ditunjukan bagaimana proses penyisipan pesan yang dilakukan pada LSB dimana 00110011 10100010 11100010 01101111 merupakan bit dari *carrier file* dan 0111 merupakan bit data pesan yang ingin disembunyikan. Dari gambar 3 perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut menyatakan

warna merah, maka perubahan satu bit LSB tidak kelihatan perubahan warna merah tersebut secara berarti dan tidak tampak mata. Agar data tersebut aman sebelum disembunyikan dapat dienkripsi terlebih dahulu (Wijaya, 2004).

3. Kerangka Teori

3.1 *Image Digital*

Bagi sebuah komputer, sebuah *image* adalah sebuah kumpulan angka-angka yang merepresentasikan intensitas cahaya pada bermacam-macam *pixel* (titik). *Digital image* biasanya disimpan dalam 24-bit atau 8-bit. 24-bit d*igital image* menyediakan tempat yang lebih untuk menyembunyikan informasi. Semua variasi warna untuk tiap *pixel* terdiri dari dari 3 warna dasar yaitu RGB. 3 warna dasar yang dijadikan patokan warna secara universal (*primary colors*). Dengan basis RGB, kita bisa mengubah warna ke dalam kode-kode angka sehingga warna tersebut akan tampil universal di manapun di seluruh dunia ini. Setiap warna dasar direpresentasikan dengan 1 *byte,* 24 *bit gambar* menggunakan 3 *bytes* per *pixel* untuk merepresentasikan nilai warna.



Gambar 1

Susunan RGB pada tiap *pixel*

Untuk warna merah murni direpresentasikan dengan: 11111111 00000000 00000000. Untuk hijau murni direpresentasikan dengan: 00000000 11111111 00000000, dan untuk biru murni direpresentasikan dengan: 00000000 00000000 11111111. Dari uraian di atas dapat dilihat bahwa informasi dari warna biru berada pada bit 0 sampai bit 7, dan informasi warna hijau berada pada bit 8 sampai dengan bit 15, sedangkan informasi warna merah berada pada bit 16 sampai dengan bit 23 (Batara, 2008).

Sedangkan jenis *image* yang paling baik untuk menyembunyikan pesan adalah *digital image* dengan format bmp 24-bit. Alasannya adalah karena format bmp ini adalah jenis d*igital image* yang paling besar ukurannya dan secara otomatis menjadikan kualitas gambarnya menjadi yang paling tinggi. Jika suatu gambar mempunyai resolusi dan kualitas yang tinggi maka untuk melakukan proses penyembunyian pesan akan lebih mudah. Selain itu *image* dengan tipe bmp bersifat *lossless* sehingga dalam penyembunyian pesan dapat menggunakan metode *LSB insertion*. (Suyono, 2004).

3.2 Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia

didalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui (Munir, 2006). Pengertian lain dari steganografi adalah ilmu, teknik atau seni menyembunyikan pesan rahasia (*hidding message*) atau tulisan rahasia (*covered writing*), menjadikan pesan tersebut tidak terbaca orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi awalnya dari bahasa Yunani yakni "*steganos*" yang artinya tersembunyi/menyembunyikan dan "*graphy*" yang artinya tulisan yang secara lengkap memiliki arti tulisan yang disembunyikan. Dalam buku *Histories of Herodatus steganografi* dengan media kepala budak yaitu dengan cara kepala budak dibotaki kemudian ditulisi pesan dan rambut budak tersebut dibiarkan tumbuh selanjutnya budak baru dikirim. Ditempat penerima kepala budak pembawa pesan tersebut digundul supaya pesan dapat terbaca. Pemakaian tinta tak-tampak (*invisible ink*), tinta dibuat dari campuraan sari buah, susu dan cuka. Tulisan diatas kertas bisa dibaca dengan memanaskan kertas tersebut (Darmawan, 2003).

Pada perang dunia II adalah periode pengembangan teknik – teknik baru steganogafi. Pada awal Perang Dunia II walaupun masih digunakan teknik tinta yang tak terlihat, namun teknik – teknik baru mulai dikembangkan seperti menulis pesan rahasia ke dalam kalimat lain yang tidak berhubungan langsung dengan isi pesan rahasia tersebut, kemudian teknik menulis pesan rahasia ke dalam pita koreksi karbon mesin ketik, dan juga teknik menggunakan pin berlubang untuk menandai kalimat terpilih yang digunakan dalan pesan, teknik terakhir adalah microdots yang dikembangkan oleh tentara Jerman pada akhir Perang Dunia II. Dari contoh-contoh steganografi konvensional tesebut dapat dilihat bahwa semua teknik steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganogafi lebih dikonsentrasikan pada kerahasiaan komunikasinya bukan pada datanya (Wijaya, 2004).

Cara kerja atau prinsip dari steganografi adalah dengan menggunakan dua unsur untuk menyisipkan suatu pesan atau data yang ingin disembunyikan. Unsur pertama adalah media penampung seperti citra, suara, video, dan lain sebagainya yang tidak membuat curiga bahwa ada pesan rahasia dalam media tersebut. Unsur kedua adalah pesan yang hendak disembunyikan (Husni, 2010).

4. Pembahasan

4.1 *Embedding* Pesan

Pada proses ini yang pertama kali dilakukan adalah menyediakan *carrier file* yaitu *digital image* dengan format bmp 24-bit. Pesan yang disisipkan berupa teks yang diinputkan melalui keyboard. Sebelum dilakukan

penyisipan pesan, *carrier file* diperiksa apakah sudah terdapat pesan yang telah disembuyikan atau belum. Jumlah karakter yang bisa disisipkan tergantung dari ukuran *image*. Semakin besar ukuran *image* maka semakin banyak pula karakter pesan yang bisa disisipkan. Untuk menyisipkan 1 karakter diperlukan 3 *pixel*. Dimana dengan perhitungan sebagai berikut: 1 karakter direpresentasikan dengan 8 bit biner. Sedangkan 1 *pixel* terdiri dari 24 bit. Sehingga 1 *pixel* mampu menampung 3 bit dari karekter yang akan disisipkan. Perhitungan untuk karakter maksimal yang dapat disisipkan adalah:

(width * (height – 1) * 3) / 8.....(1)

Jadi jika ada sebuah *digital image* dengan ukuran 300x250 *pixel* dapat digunakan untuk menyisipkan karakter sebanyak 28012 karakter. Pada persamaan (1) untuk *height* harus dikurangi 1. Hal ini disebabkan karena harus disediakan 1 *pixel* untuk menyimpan kode tertentu yang menunjukkan bahwa suatu *digital image* sudah terisi pesan atau belum.

Contoh penyisipan karakter Z yang direpresentasikan 01011010 *pada carrier file*:

00001011 11111000
11110100

11100001 10110000
10101111

01010000 10111111
01010010

Maka *stego-image* yang dihasilkan adalah sebagai berikut:

00001010 11111001
11110100

11100001 10110001
10101110

01010001 10111110
01010010

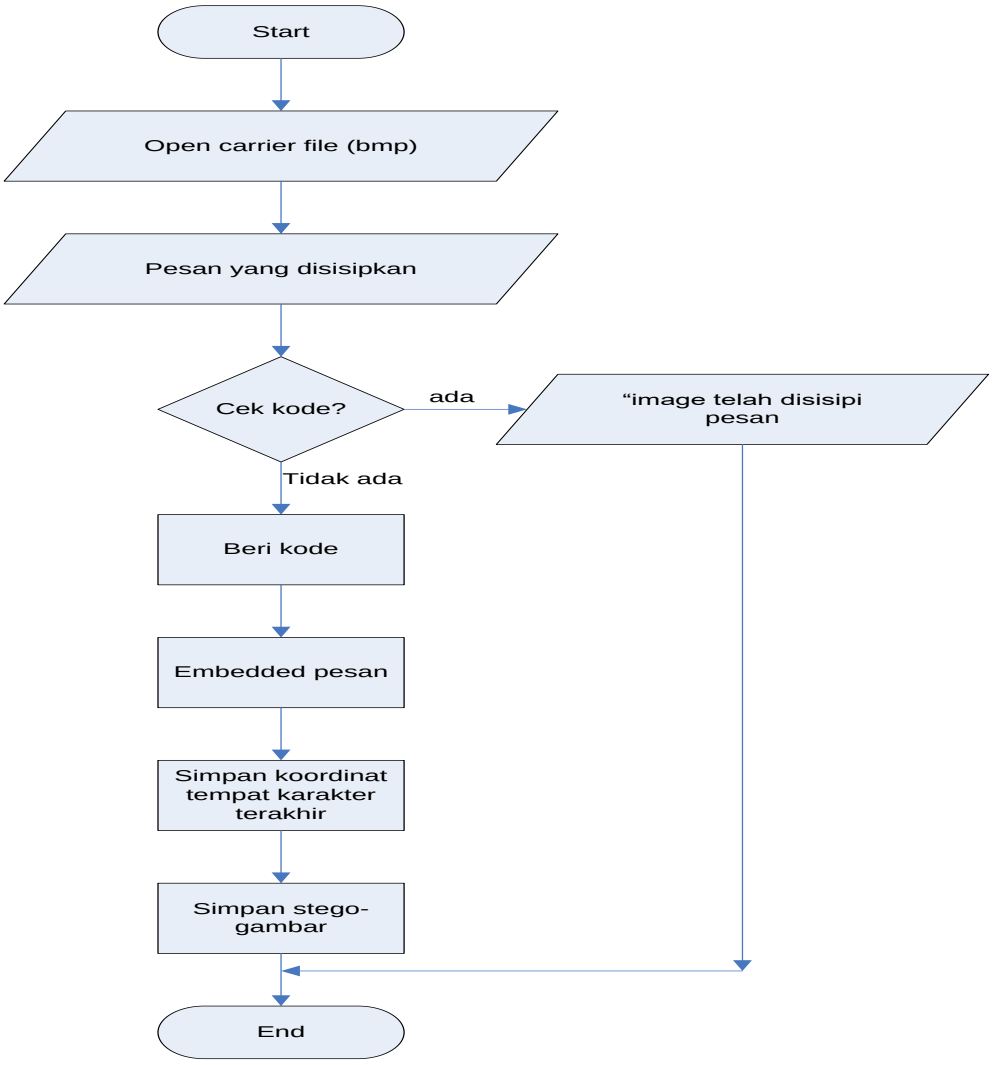
Pada bit-bit yang digarisbawahi adalah LSB dari masing-masing komponen RGB. Sedangkan yang dicetak tebal adalah LSB yang mengalami perubahan. Setelah pesan disisipkan. Maka langkah berikutnya adalah menyisipkan koordinat *pixel* dimana karakter terakhir disisipkan. Informasi lokasi ini berguna agar dalam proses *extracting* pesan rahasia dari *image* bisa tepat dalam mengambil bit-bit biner.

4.2 *Extracting*

Pada proses *extracting* yang perlu dilakukan pertama kali adalah memeriksa keberadaan kode. Jika terdapat kode tertentu maka dapat dipastikan bahwa *digital image* tersebut mempunyai pesan di dalamnya. Langkah berikutnya adalah mengambil koordinat terakhir dimana karakter disimpan, hal ini diperlukan untuk menghindari pengambilan bit pada koordinat yang kurang tepat. Informasi lokasi ini berguna agar dalam

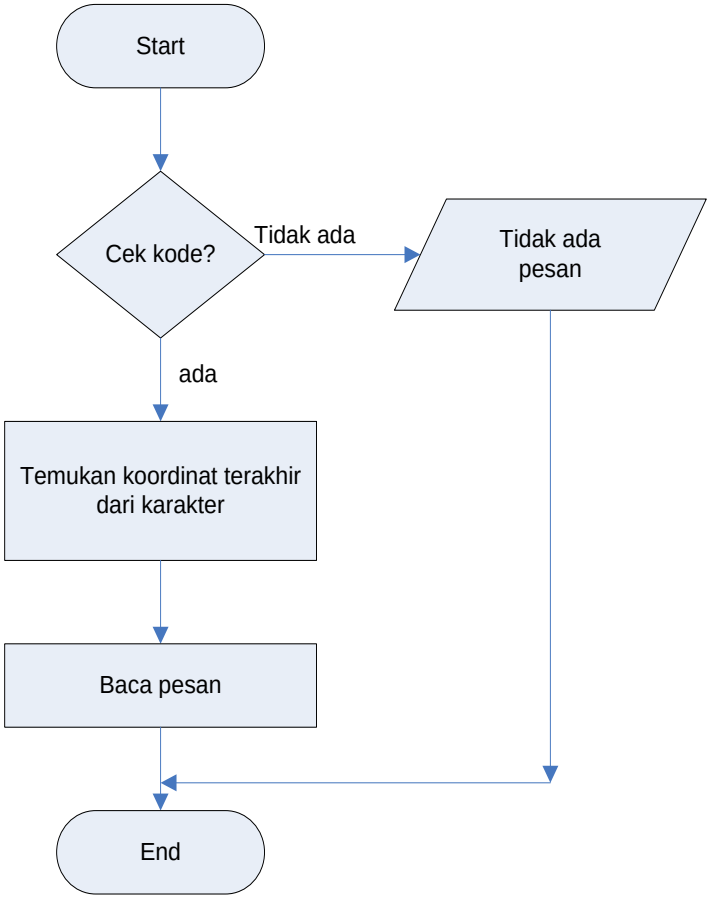
proses *extracting* pesan rahasia dari *stego-image*, program bisa tepat dalam mengambil bit-bit biner pesan, sehingga program bisa berhenti ketika bit-bit biner pesan telah habis diambil.

Informasi koordinat ini berfungsi sebagai pembatas dalam *looping* pada proses ambil pesan, sehingga ketika sampai pada koordinat terakhir proses *extracting* bisa berhenti. Adapun diagram alir secara umum ditunjukkan pada gambar 5.



Gambar 4

Diagram alir proses embedding pesan secara umum



Gambar 5

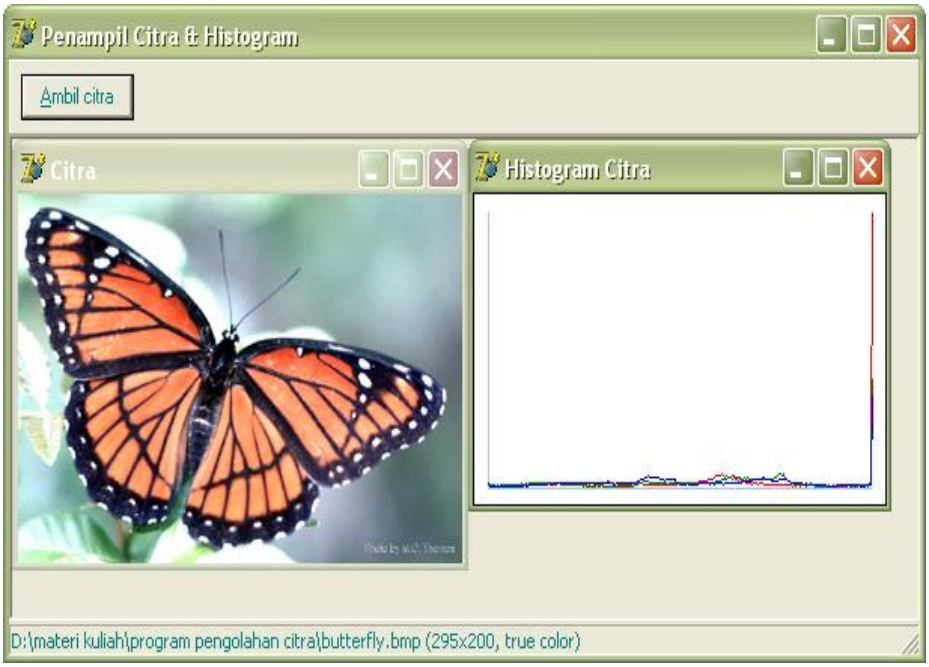
Diagram alir proses *extracting* secara umum

4.3 Pengujian

Pengujian menggunakan 3 *digital image* dengan format bmp 24-bit yang berbeda dan pesan yang berbeda pula. Sebelum proses *embedding* dan setelah proses *embedding* akan diperiksa bagaimana histogram dari masing-masing *image*. Histogram ini digunakan untuk mengetahui tingkat RGB dari masing-masing *pixel*.

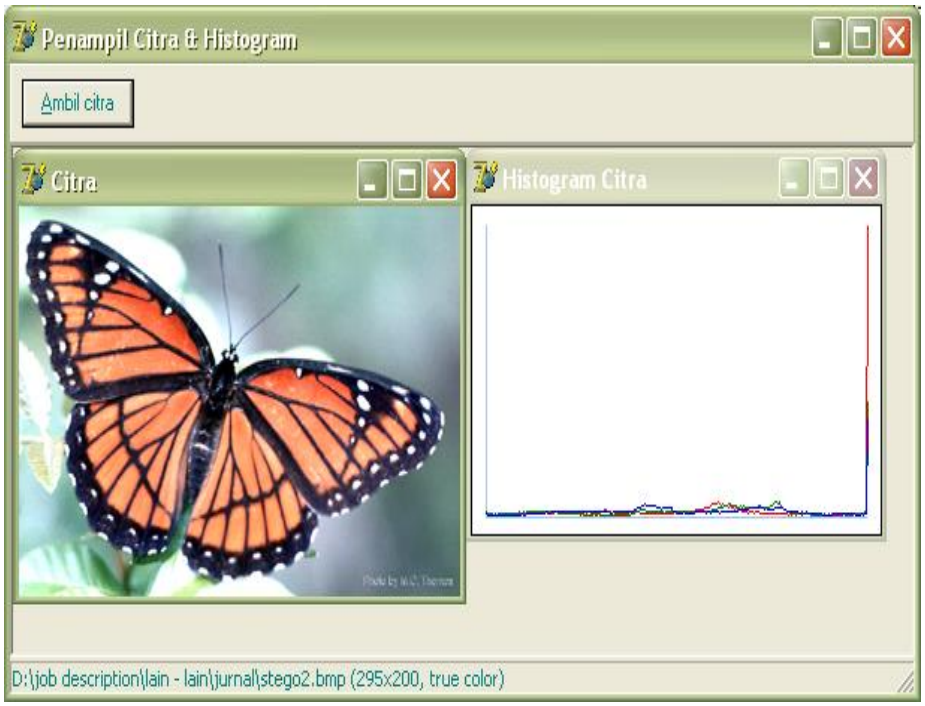
Image 1 adaah *digital image* dengan ukuran 295x200 *pixel*. Image pada gambar 6 berfungsi sebagai *carrier file*. Adapun pesan yang ingin

disembunyikan adalah: "*lihat perbedaannya*", yaitu sebanyak 18 karakter. Sedangkan pada gambar 7 adalah image 1 setelah proses *embedding*. Dari hasil gambar dan histogram yang ada pada gambar 6 dan gambar 7, dapat diketahui bahwa tidak terjadi degradasi warna. Sehingga orang awam yang melihat *image* tersebut tidak akan menyadari adanya pesan yang disembunyikan pada image tersebut.



Gambar 6

Image 1 sebelum proses *embedding*

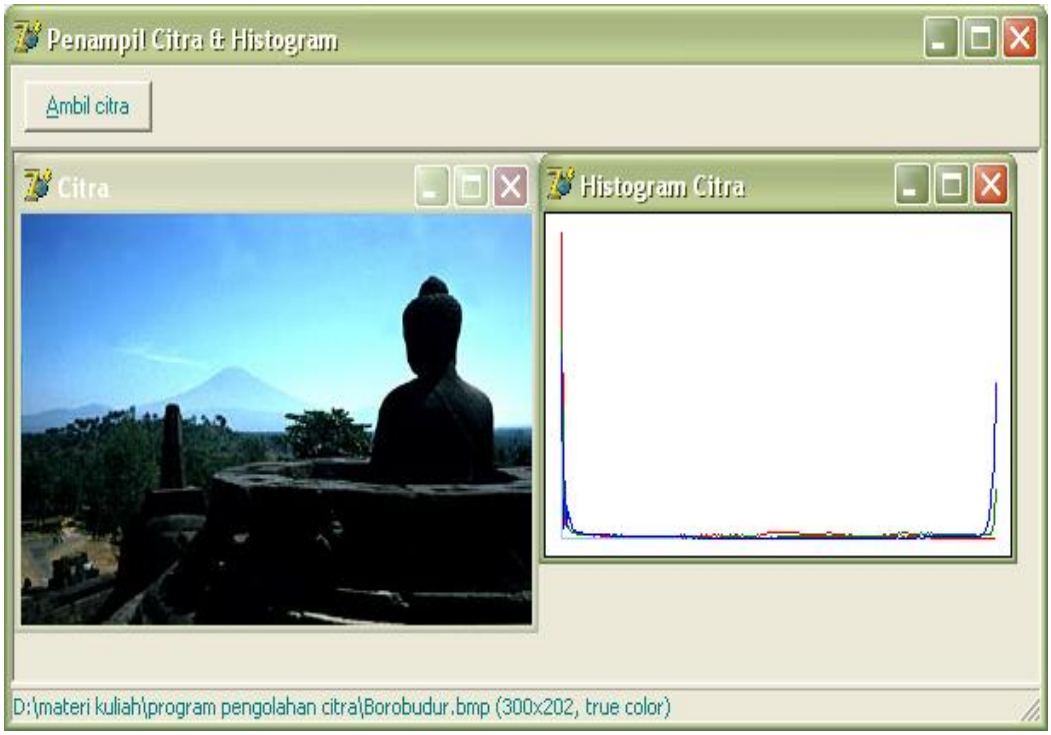


Gambar 7

Image 1 setelah proses *embedding*

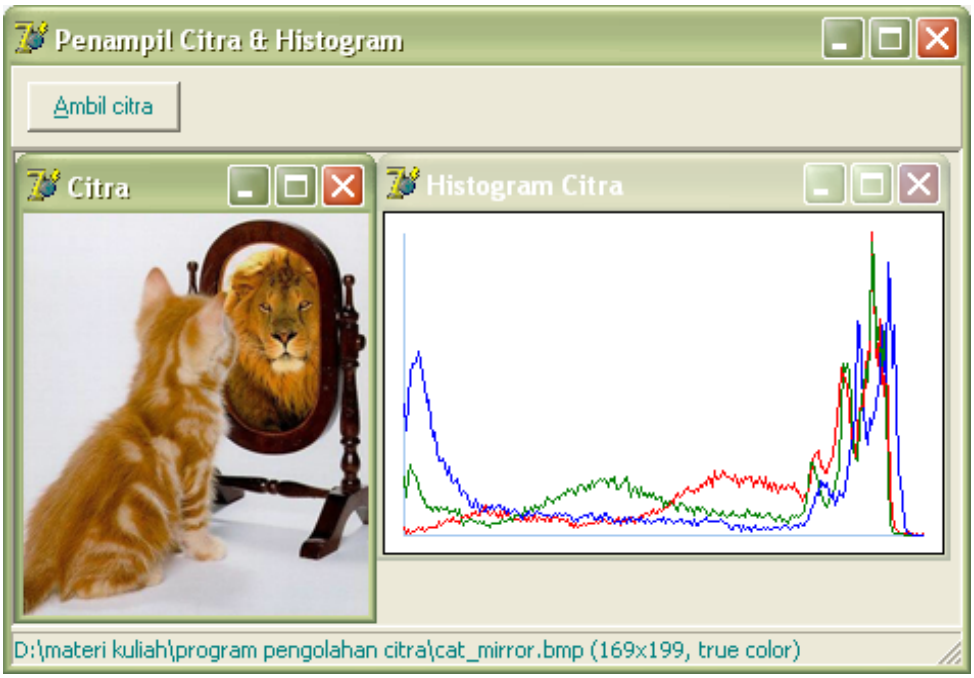
Image 2 berukuran 300x202 *pixel*. *Image* pada gambar 8 berfungsi sebagai *carrier file*. Pesan yang disisipkan sebanyak 5778 karakter. Sedangkan pada gambar 9 adalah *image* 2 setelah disisipi pesan. Dari *carrier file* dan *stego-image* serta histogram yang dihasilkan dari masing-masing *image*, dapat diketahui bahwa terjadi degradasi warna pada bagian atas *stego-image*. Karena terjadi degradasi warna tersebut menyebabkan kecurigaan pada orang yang melihatnya.

Image 3 dengan ukuran 169x199 *pixel*. *Image* pada gambar 10 tersebut berfungsi sebagai *carrier file*. Pesan tersebut sebanyak 12548 karakter. Sedangkan pada gambar 10 adalah *image* 2 setelah dilakukan proses *embedding*. Dari *carrier file* dan *stego-image* serta histogram yang dihasilkan dari masing-masing *image*, dapat diketahui bahwa terjadi degradasi warna pada seluruh bagian *stego-image*.



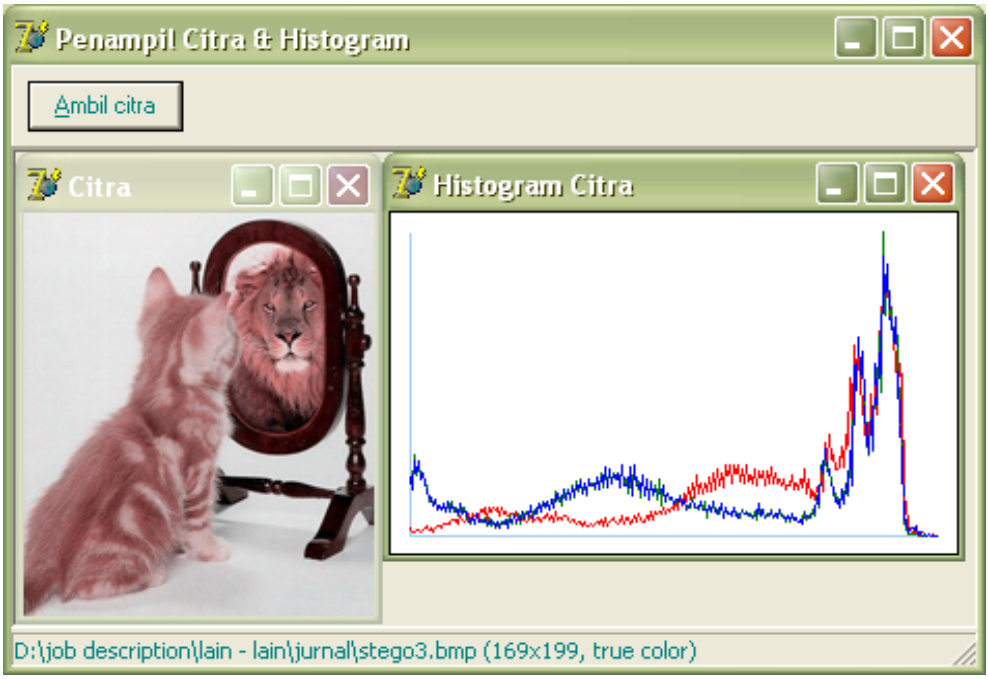
Gambar 8 : *Image* 2 sebelum proses *embedding*

Gambar 9 : *Image* 2 setelah proses *embedding*



Gambar 10

Image 3 sebelum proses *embedding*



Gambar 11

Image 3 setelah proses *embedding*

Tabel 1

Hasil pengujian

Image	**Ukuran (pixel)**	**Karakter Max**	**Karakter terpakai**	**sisa**
Image 1	295x200	22014	18	21996
Image 2	300x202	22612	5778	16834
Image 3	169x199	12548	12546	2

Tabel 1 menunjukkan informasi yang dihasilkan oleh program steganografi dengan berbagai ukuran *image* sebagai *carrier file* dan banyaknya pesan yang disisipkan. Pada image 1 *space* tersisa yang tidak disisipi pesan sangat banyak yaitu sebesar 21996, sedangkan pada image 3 *space* yang tersisa hanya 2. Dari 3 hasil pengujian dengan berbagai ukuran *carrier file* dan jumlah karakter yang disisipkan terlihat bahwa steganografi dapat dilakukan dengan metode LSB *insertion.* Metode ini menyebabkan adanya perubahan warna pada *carrier file.*

7. Kesimpulan

Berdasarkan hasil penelitian terlihat bahwa steganografi dapat dilakukan dengan menggunakan *carrier file* berupa *digital image* berformat bmp 24-bit dengan metode LSB *insertion*. Metode LSB *insertion* mengubah RGB setiap *pixel* dengan bit pesan. Metode ini menyebabkan adanya perubahan atau degradasi warna pada *carrier file*. Besar kecilnya perubahan atau degradasi warna tersebut tergantung dari jumlah karakter yang disisipkan. Semakin banyak karakter yang disisipkan akan semakin terlihat degradasi warna yang terjadi. Hal ini dapat menimbulkan kecurigaan sehingga untuk ke depan perlu dikembangkan metode atau algoritma steganografi yang lebih meminamalisir degradasi warna tersebut.

DAFTAR PUSTAKA

Batara, S. (2008). Studi Steganografi dalam File Mp3.

Bender. (1996). *Techniques For Data Hiding*. IBM Systems Journal.

Darmawan. (2003). *Steganography Sebuah Pendekatan Baru dalam Pengamanan Data*.

Husni. (2010). *Keamanan komputer*. Universitas Trunojoyo.

Munir, R. (2006). *Diktat Kuliah Kriptografi*. Institut Teknologi Bandung.

Sellars, D. (2009). *An Introduction to Steganography*.

Suyono. (2004). *Penyerangan Pada Sistem Steganografi Dengan Menggunakan Metode Visual Attacks dan Statistical Attacks*.

Wijaya, E. S. (2004). Konsep Hidden Message Menggunakan Teknik Steganografi. *Media Informatika*, *2*.

This page intentionally left blank.