ORIGINAL ARTICLE

Steganografi Pada File Citra Bitmap 24 Bit Untuk Pengamanan Data Menggunakan Metode Least Significant Bit (LSB) Insertion

Setiana
Wayan Firdaus Mahmudy, (wayanfm@ub.ac.id)

Jurusan Matematika, FMIPA Universitas Brawijaya, Malang 65145

Abstrak

Steganografi adalah suatu ilmu dan seni menyembunyikan data pada suatu media. Steganografi tercipta sebagai salah satu cara yang digunakan untuk mengamankan data dengan cara menyembunyikannya dalam media lain agar "tidak terlihat". Penyisipan LSB dilakukan dengan memodifikasi bit terakhir dalam satu *byte* data. Dengan memodifikasi teknik penyisipan data serta menggabungkan teknik ini dengan fungsi hash dan kriptografi, maka akan dapat memberikan perlindungan data yang lebih optimal. Hasil akhir dari aplikasi ini berupa gambar stego yang telah memuat pesan yang disisipkan. Gambar stego mempunyai ukuran dan bentuk yang sama persis seperti media gambar aslinya. Meskipun bit-bit pixel media gambar sudah mengalami perubahan akibat penyisipan, namun perubahan itu tidak begitu signifikan, sehingga belum bisa dideteksi oleh mata manusia biasa.

Kata kunci: *Steganografi; Metode least signigicant bit insertion; lsb insertion; fungsi hash; kriptografi*

Abstract

Steganography is an art and science to hide data at one particular media. Steganography is created as one of ways used to protect data by hiding it in other media in order that they are "unseen". Modifying insertion data technique and also joining this technique with hash function and criptography, will be able to give protection of data more optimally. The final result of this application is in the form of picture of stego which contains inserted message. Stego images have size and form very similar to their original picture media. Although bits of pixel of media images have undergone changes due to insertion effect, the changes are not so significant, so that they can not yet be detected by ordinary human eyes.

Keywords: *Steganography; least signigicant bit insertion method; lsb insertion; hash function; kriptography*

1. PENDAHULUAN

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia (Wikipedia, 2006).

Sesungguhnya steganografi merupakan metode lama yang sudah dipakai oleh orang-orang Yunani kuno. Kata Steganografi berasal dari bahasa Yunani yang artinya tulisan tertutup atau tersembunyi (*covered letter*), yang meliputi berbagai cara komunikasi yang menyembunyikan pesan dengan sangat efisien. Pada awalnya metode ini berupa penggunaan tinta yang tidak nampak, pengaturan karakter, tanda tangan digital, saluran yang dikacaukan, dan spektrum komunikasi yang disebar. Dengan adanya teknologi digital maka muncul cara baru untuk sistem steganografi ini, yaitu dengan penyembunyian pesan dalam gambar digital.

Ada dua proses utama dalam steganografi yaitu penyisipan (*embedding*) dan penguraian (*extraction*) pesan *atau* informasi dalam media cover. *Embedding* merupakan proses menyisipkan

Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor*, vol. 2, no. 2, pp. 38-44.

pesan atau informasi ke dalam media cover, sedangkan *extraction* adalah proses menguraikan pesan yang tersembunyi dalam gambar stego. Pesan yang akan disembunyikan dalam sebuah gambar membutuhkan dua file. Pertama adalah gambar asli yang belum dimodifikasi yang akan menangani pesan tersembunyi, yang disebut gambar cover (*cover image*). File kedua adalah informasi pesan yang disembunyikan. Suatu pesan dapat berupa *plaintext*, *chipertext*, gambar lain, atau apapun yang dapat ditempelkan ke dalam bit stream. Ketika dikombinasikan, cover image dan pesan yang ditempelkan membuat gambar stego (*stego image*).

1.1 Steganografi vs Kriptografi

Steganografi dan kriptografi mempunyai prinsip kerja yang berbeda, meskipun keduanya mempunyai hubungan yang dekat dalam dunia keamanan data. Pada kriptografi menghasilkan sebuah chipertext dimana dengan itu seolah-olah dengan sengaja menunjukkan kepada orang lain bahwa ada sesuatu di dalamnya, namun tidak dapat diketahui maknanya. Namun dengan bentuk *chipernya*, justru akan membuat data tersebut terancam oleh usaha-usaha yang dilakukan oleh orang lain untuk dapat membongkarnya dengan tujuan dan atau alasan apapun.

Steganografi dan kriptografi merupakan seni dan teknik yang dapat digunakan untuk melakukan pengamanan data digital. Namun keduanya tidaklah sama. Pada kriptografi, suatu data digital diamankan dengan cara mengenkripsi data tersebut dan menghasilkan sebuah data yang berupa sandi, secara visual data tersebut masih dapat terlihat atau diketahui, hanya saja data tersebut menjadi tidak dapat dimengerti. Berbeda dengan steganografi yang tujuannya adalah menyembunyikan data ke dalam sebuah media yang lain, sehingga data tersebut tidak terlihat.

Pada aplikasi steganografi modern, kehadiran steganografi bukanlah untuk menggantikan kedudukan kriptografi. Bahkan steganografi diciptakan untuk dapat memperkuat dan menambah satu lapis pertahanan keamanan data digital.

1.2 Enkripsi dan Fungsi Hash

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. Encryption berasal dari bahasa yunani *kryptos* yang artinya tersembunyi atau rahasia.

Fungsi *hash* adalah fungsi yang menerima masukan *string* yang panjangnya sembarang, lalu mentransformasikannya menjadi *string* keluaran yang panjangnya tetap (*fixed*) (umumnya berukuran jauh lebih kecil daripada ukuran *string* semula).

Persamaan fungsi *hash*:

$h = H(M)$
M = pesan ukuran sembarang
h = nilai *hash* (*hash value*) atau pesan-ringkas (*message-digest*)

Salah satu contoh algoritma fungsi hash Kriptografi adalah MD5. Fungsi ini sering digunakan pada pengecekan data password dikarenakan fungsi ini dapat mengubah bentuk string ke bentuk hash string yang unik. Ini dapat digunakan sebagai data security yang tidak mudah untuk ditebak. . Bentuk unik ini terdiri dari 32-karakter bilangan heksadesimal (Kusumawati, 2005).

1.3 Least Significant Bit (LSB)

Least significant bit (LSB) adalah posisi bit dalam bilangan biner yang mempunyai nilai 1 (Wikipedia, 2006). Least significant digit dari sebuah bilangan desimal adalah angka yang berada pada posisi paling kanan.

Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor*, vol. 2, no. 2, pp. 38-44.

1.4 Metode Least Significant Bit (LSB) Insertion

Penyisipan LSB dilakukan dengan memodifikasi bit terakhir dalam satu *byte* data. Bit yang diganti adalah LSB karena perubahan pada LSB hanya menyebabkan perubahan nilai *byte* satu lebih tinggi atau satu lebih rendah. Misalkan data yang diubah adalah warna hijau, maka perubahan pada LSB hanya menyebabkan sedikit perubahan yang tidak dapat dideteksi oleh mata manusia.

Seperti kita ketahui untuk file bitmap 24 bit maka setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner `00000000` sampai `11111111`. Dengan demikian pada setiap *pixel* file bitmap 24 bit kita dapat menyisipkan 3 bit data. Contohnya huruf A dapat kita sisipkan dalam 3 pixel, misalnya data raster original adalah sebagai berikut:

```
(00100111   11101001   11001000)
(00100111   11001000   11101001)
(11001000   00100111   11101001)
```

Sedangkan representasi biner huruf A adalah `10000011`. Dengan menyisipkan-nya pada data pixel diatas maka akan dihasilkan:

```
(00100111   11101000   11001000)
(00100110   11001000   11101000)
(11001001   00100111   11101001)
```

Terlihat hanya empat bit rendah yang berubah, untuk mata manusia maka tidak akan tampak perubahannya. Secara rata-rata dengan metode ini hanya setengah dari data bit rendah yang berubah, sehingga bila dibutuhkan dapat digunakan bit rendah kedua bahkan ketiga.

1.5 LSB Insertion Menggunakan Pixel Yang Tidak Berurutan

Bit-bit data rahasia tidak digunakan mengganti pixel yang berurutan, namun dipilih susunan pixel secara acak. Misalnya jika terdapat 20 pixel dan 6 bit data yang akan disembunyikan, maka *pixel* yang diganti bit *LSB*-nya dipilih secara acak, misalkan pixel nomor 1, 3, 6, 7, 10, 14. Parameter yang digunakan sebagai acuan untuk menuju pixel berikutnya adalah 2 bit *lsb* dari komponen warna *blue* dari pixel yang sedang ditempati. Penggunaan metode ini akan mengurangi daya tampung gambar, karena tidak semua pixel dipakai untuk menyembunyikan pesan. Prosedur penyembunyian bit data secara *random pixel* adalah sebagai berikut:

- Tentukan f(x,y). f(x,y) adalah pixel dengan posisi koordinat x,y.
- Dapatkan nilai byte dari komponen warna Blue (B) dari f(x,y).
- Dapatkan 2 lsb dari B dengan n = B AND $(11)_2$
- Tambahkan nilai n ke x. f'(x,y) = f'(x+n, y)

```
     R            G            B
(00100110     11101001   110010 10)  2 digit LSB
.{pixel ini tdk dipakai}            dari B
.{pixel ini tdk dipakai}            sebagai
(00100110     11001000   11101001)  acuan ke
                                    pixel
                                    berikutnya.
```

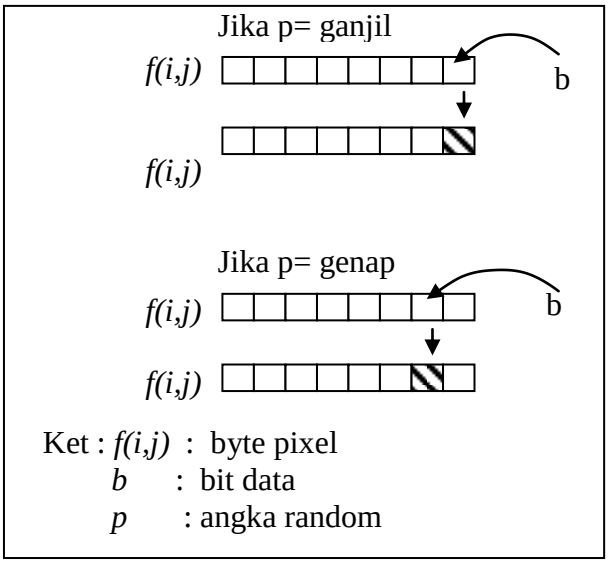
1.6 LSB Insertion secara random LSB

Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor*, vol. 2, no. 2, pp. 38-44.

Bit LSB yang dipakai untuk menampung bit data tidak selalu LSB bit pertama, tetapi juga memakai LSB bit kedua. Penerapan metode ini dilakukan bersamaan dengan pembangkitan angka random dari sebuah fungsi random generator sebagai acuan untuk penyisipan.

Prosedur penyembunyian data menggunakan bit LSB yang berbeda (*random lsb*) adalah sebagai berikut:

- Bangkitkan *p (pseudorandom number).*
- Lakukan proses penyembunyian dengan cara menyisipkan 1 bit data dengan aturan seperti berikut:
  - jika p adalah bilangan ganjil, sisipkan 1 bit data b pada LSB (bit pertama)
  - jika p adalah bilangan genap, sisipkan 1 bit data b pada LSB (bit kedua) .



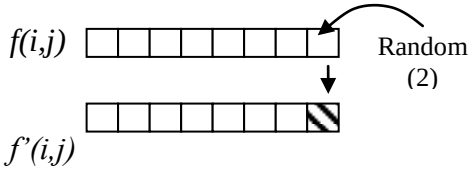
Gambar 1 Penyembunyian 1 bit data pada LSB yang berbeda

Untuk membangkitkan angka-angka random, digunakan sebuah fungsi pembangkit bilangan acak dengan rumus : $X_n = (7X_{n-1} + 11) \bmod 17$.

1.7 Modifikasi seluruh LSB

Metode tambahan berikutnya adalah *modify all* atau mengubah seluruh *lsb* gambar yang bertujuan untuk menyamarkan posisi pesan yang disembunyikan dalam gambar. Dengan mengubah seluruh *lsb* dalam gambar akan menimbulkan kesan bahwa seolah-olah seluruh pixel dalam gambar memuat bit-bit data, padahal hanya tempat-tempat tertentu saja yang disisipi pesan. Prosedur untuk mengubah seluruh lsb dalam gambar adalah sebagai berikut :

- Tentukan *f(i,j), byte pixel* pada gambar.
- Ubah 1 bit LSB dengan nilai 0 atau 1 secara random.



Gambar 2 Mengubah 1 bit LSB dengan nilai random 0 atau 1

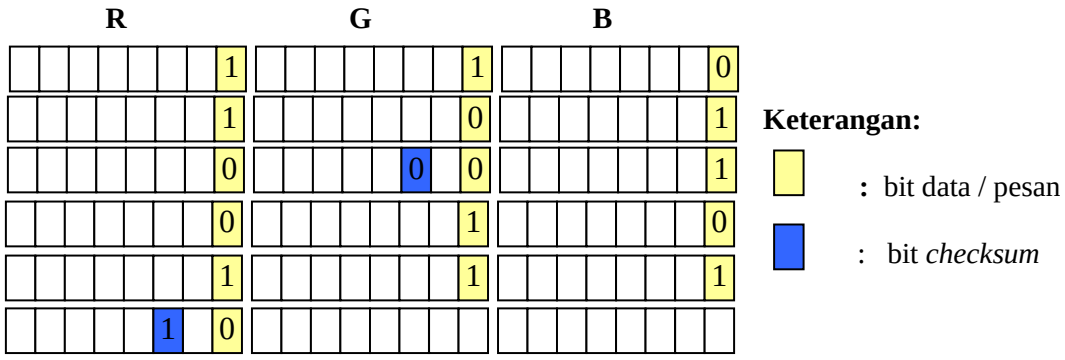
Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor,* vol. 2, no. 2, pp. 38-44.

1.8 Validitas Data

Salah satu kelemahan metode LSB insertion adalah tidak tahan terhadap pengubahan (modifikasi) terhadap *cover object***,** karena kesalahan satu bit saja akan menghasilkan hasil yang berbeda pada waktu penguraian (*extraction*).

Untuk menjaga integritas (keaslian) isi arsip terhadap perubahan, misalnya karena serangan virus atau terjadi manipulasi terhadap gambar, maka harus dilakukan otentikasi data. Caranya adalah dengan menghitung *jumlah* bit yang bernilai 1 untuk setiap penyisipan 1 byte data. Jika jumlah bit bernilai ganjil, simpan nilai 1 pada LSB ke 3, di tempat terakhir penyisipan dat per bytenya. Jika sebaliknya maka yang disimpan adalah nilai 0. Pada saat penguraian, nilai tersebut akan diperiksa untuk menentukan apakah data yang diperoleh masih sama atau sudah berubah. Posisi bit yang digunakan untuk checksum adalah seperti gambar berikut :

Misalkan bit data : 101 0100 1010 1110



Gambar 3. Penempatan bit checksum

2. METODE PENELITIAN

Pada tahap pertama penelitian ini diuji coba pada sebuah gambar. Ini dilakukan untuk menguji kebenaran program komputer yang telah disusun. Pada tahap kedua, citra yang sudah berisi pesan diberi noise untuk melihat validitas data. Pada tahap kedua ini dapat diketahui bahwa telah terjadi perubahan pada gambar.

3. HASIL DAN PEMBAHASAN

Pada pengujian ini menggunakan media gambar dengan format BMP dengan kedalaman warna gambar sebesar 24 bpp, resolusi 400 x 322 dan ukuran 378 Kb . Sedangkan data yang disisipkan dalam gambar adalah file teks dengan ukuran sebesar 11 Kb.

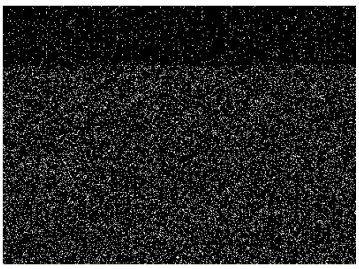
gambar asli
(400 x 322)

file teks
berukuran 11
kb

gambar stego
(400 x 322)

Dari proses penyisipan pesan diatas, dihasilkan sebuah gambar stego yang ukurannya sama persis dengan gambar aslinya sebelum disisipkan pesan. Ukuran resolusi, kedalaman warna dan besar kapasitasnya sama persis, keduanya mempunyai resolusi 400 x 322 dengan kedalaman warna 24 bpp dan kapasitasnya 378 Kb.

Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor,* vol. 2, no. 2, pp. 38-44.



Pixel yang berubah

Posisi pesan dalam gambar

Warna hitam menandakan pixel yang berubah. Hampir seluruh pixel mengalami perubahan nilai warna. Karena pada saat proses penyisipan juga menggunakan option Modify All, maka pixel yang tidak ditempati oleh pesan juga berubah.

Contoh perubahan nilai pada pixel adalah sebagai berikut:

Koordinat		Sebelum			Sesudah		
x	y	R	G	B	R	G	B
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
98	1	56	106	165	56	107	164
99	1	59	106	164	59	106	164
100	1	57	107	164	57	105	164
101	1	57	107	164	57	107	164
102	1	56	107	164	56	105	164
103	1	57	107	164	57	106	165
105	1	57	107	165	57	105	164
106	1	57	107	165	57	105	165
108	1	57	106	165	57	106	167
112	1	56	106	165	56	106	165
114	1	56	107	164	56	107	164
115	1	57	106	164	57	107	164
116	1	57	106	164	57	106	166
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Terlihat ada beberapa nilai byte pixel yang tidak berubah, dikarenakan nilai bit karakter sama dengan nilai LSB pada pixel gambar.

Pada tahap kedua, gambar diberi noise berupa garis seperti berikut :

Gambar dengan noise

Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor,* vol. 2, no. 2, pp. 38-44.

Pada saat aplikasi penguraian dijalankan, ada sebuah pesan yang memberi informasi bahwa telah terjadi kerusakan atau perubahan pada bit data. Data rahasia tetap bisa dibuka tetapi sudah tidak valid lagi.

Banyak maksimal pesan yang dapat disisipkan dalam gambar adalah ((Img.Width * Img.Height - 1) * 3 / 8) sedangkan jika dilakukan secara random pixel maka daya tampung gambar sebesar ((img.width * img.height-1) * 3 / 8 / 4).

Berdasarkan hasil perhitungan, besarnya daya tampung gambar terhadap pesan adalah sebesar 37,49%. Misalkan gambar dengan ukuran 400 x 322 dapat menampung pesan sebesar 48299 byte.

4. KESIMPULAN

- Dengan aplikasi Steganografi yang sudah dibuat, mampu mengamankan data dengan cara menyembunyikannya pada gambar dengan format bitmap (*.bmp) 24 bit.
- Perubahan warna pixel gambar yang dihasilkan akibat penyisipan bit-bit pesan dalam aplikasi ini masih belum dapat dideteksi oleh mata manusia biasa.
- Banyak maksimal pesan yang dapat disisipkan dalam gambar adalah ((img.width * img.height-1) * 3 / 8), sedangkan jika dilakukan secara random pixel maka daya tampung gambar sebesar ((img.width * img.height-1) * 3 / 8 / 4).
- Kerusakan data akibat noise dapat diketahui, tetapi tidak dapat diperbaiki.

.

DAFTAR PUSTAKA

1. Gonzalez, Rafael C. , Woods, Richard E.. Digital Image Processing Second Edition, Prentice Hall. 2002.
2. Irianto. 2004. Embedding Pesan Rahasia dalam Gambar. http://budi.insan.co.id/courses/ec7010/2004-2005/irianto-report.pdf. Tanggal akses: 14-02-2006.
3. Kurniawan, Yusuf. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Informatika. Bandung. 2004.
4. Kusumawati, Ratih. Fungsi md5() pada PHP. http://www.sony-ak.com/articles/4/php_md5_function.php. Tanggal akses: 2-04-2006.
5. Mohanty, Saraju P. 1999. Digital Watermarking : A Tutorial Review. http://www.cs.unt.edu/~smohanty/research/Reports/ MohantyWatermarkingSurvey1999.pdf. Tanggal akses: 22-02-2006.
6. Munir, Rinaldi. Pengolahan Citra Digital: dengan pendekatan algoritmik. Informatika. Bandung. 2004.
7. Petitcolas,fabien a.p. 2006. Mp3stego. http://www. petitcolas.net/fabien/steganography/mp3stego/ index.html . Tanggal akses: 4-04-2006.
8. Sukmawan, Budi. 2002. Steganografi. http:// bdg.centrin.net.id/~budskman/stegano.htm. Tanggal akses: 4-04-2006.
9. Soplanit, Susani. Penyembunyian Kunci Enkripsi Citra Pada Cipher-image. http://telecom.ee.itb.ac.id/tssa2004/papers/sudah %20didownload%20panitia/Camera-Ready_Paper-CKBA-KeysHide.doc--Susany%20Soplanit Fakultas Teknologi Informasi Universitas Tarumanagara. Jakarta Barat. Tanggal akses: 14-02-2006.
10. Wohlgemuth, Sven. 2002. Steganography and Watermarking. http://www.informatika.org/~rinaldi/Kriptografi/20020108SteganographyWatermarking.4on1.pdf . Tanggal akses: 4-03-2006.
11. Wikipedia. Steganography. http://en.wikipedia.org/wiki/ steganography. Tanggal akses: 4-03-2006.
12. Wikipedia. Least significant bit http://en.wikipedia. org/wiki/Least_significant_bit. Tanggal akses: 4-03-2006.

Setiana & Mahmudy, WF 2006, 'Steganografi pada file citra bitmap 24 bit untuk pengamanan data menggunakan metode least significant bit (LSB) insertion', *Kursor,* vol. 2, no. 2, pp. 38-44.