J. Pilar Sains 6 (2) 2007

ISSN 1412-5595

STEGANOGRAFI DENGAN METODE PENGGANTIAN LEAST SIGNIFICANT BIT (LSB)

Astried
Jurusan Matematika FMIPA UNRI
Kampus Bina Widya Km 12,5. Simpang Baru Pekanbaru
Universitas Riau

Abstract

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. Least Significant Bit method (LSB) is one of steganography method to hiding data by changing bit LSB in segment of image with secret data bit. The changing image can be applied without humanly visible degradation

Keywords : Image, Least Significant Bit,, Steganography, degradation.

Pendahuluan

Perkembangan teknologi digital serta internet saat ini telah memberi kemudahan untuk melakukan akses serta mendistribusikan berbagai informasi dalam format digital. Beberapa faktor yang membuat data digital (seperti audio, citra, video dan text) banyak digunakan antara lain (Supangkat, et al, 2000) :

- Mudah diduplikasi dan hasilnya sama dengan aslinya
- Murah untuk penduplikasian dan penyimpanan
- Mudah disimpan dan kemudian untuk diolah atau diproses lebih lanjut
- Mudah didistribusikan, baik dengan media disk maupun melalui jaringan internet

Namun kemudahan tersebut sering kali digunakan secara "negative", dimana data digital yang dikirim melalui internet dapat disadap dan diubah oleh pihak lain. Salah satu cara yang dikenal untuk melindungi data digital adalah kriptografi. Kriptografi adalah suatu seni atau ilmu mengamankan pesan, dimana pesan rahasia diamankan dengan proses enskripsi dari *plaintext* menjadi *chipertext*. Sebaliknya, untuk mengubah *chipertext* ke pesan rahasia yang asli (*plaintext*) dilakukan proses deskripsi. Masalah yang timbul adalah bahwa enkripsi hanya akan mengubah bentuk dari

melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar-benar acak (tetapi dapat dikembalikan ke bentuk semula) dan berbeda dengan aslinya, sedangkan teks yang dienkripsi menjadi bentuk teks yang acak yang tentunya akan menimbulkan kecurigaan akan data teks tersebut sehingga dengan mudah dapat disimpulkan bahwa teks tersebut merupakan hasil enkripsi dari sebuah data sehingga dapat dipecahkan dengan metode-metode tertentu.

Selain dengan kriptografi sebuah data dapat disembunyikan dengan menggunakan metode steganografi. Steganografi adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang. Steganografi membutuhkan dua property yaitu wadah (media) penampung dan data rahasia yang akan disembunyikan (Munir, 2004).

Bahan dan Metoda

Steganografi

Steganografi merupakan seni untuk menyembunyikan pesan di dalam media lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu pesan di dalam media tersebut. Kata "steganography" berasal dari kata Yunani "steganos" yang berarti "terlindungi", dan "graphein" yang berarti "menulis" (Paulus, Nataliani, 2007).

Steganography berbeda dengan *cryptography*. Letak perbedaannya adalah pada proses penyembunyian data dan hasil akhir dari proses tersebut. *Cryptography Steganography* menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum

dan setelah proses penyembunyian hampir sama.

Teknologi steganografi sudah dikenal ribuan tahun yang lalu, pada tahun 480 sebelum masehi, seorang berkebangsaan Yunani yaitu Demaratus mengirimkan pesan kepala polis Sparta yang berisi peringatan mengenai penyerangan Xerxes yang ditunda. Teknik yang digunakan adalah dengan menggunakan meja yang telah diukir kemudian diberi lapisan lilin untuk menutupi pesan tersebut, dengan begitu pesan dalam meja dapat disampikan tanpa menimbulkan kecurigaan oleh para penjaga (Thana, 2008)

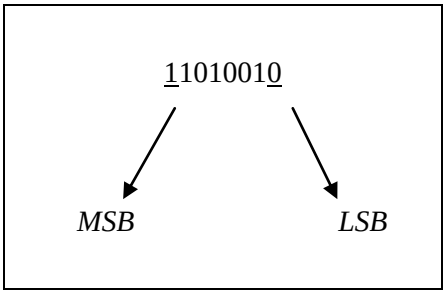
Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut.Kriteria yang harus diperhatikan dalam penyembunyian data adalah (Thana, 2008):

- *Fidelity*. Mutu citra penampung tidak jauh berbeda. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
-
- *Robustness*. Data yang disembunyikan harus tahan (*robust*) terhadap berbagai operasi manipulasi yang dilakukan pada citra penampung, seper
- ti pengubahan kontras, penajaman, pemampatan, rotasi, perbesaran gambar, pemotongan (*cropping*), enskripsi dan sebagainya. Bila pada citra penampung dilakukan operasi-operasi pengolahan citra tersebut, maka data yang disembunyikan seharusnya tidak rusak (tetap valid jika diekstraksi kembali)
- *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali.

Sampai saat ini steganografi telah banyak digunakan untuk berbagai keperluan tertentu dengan metode-metode yang beragam salah satunya adalah metode penggantian Least Significant Bit (LSB).

Metode LSB (least significant bit)

Metode penggantian LSB merupakan salah satu metode steganografi yang di gunakan untuk menyembunyikan data dimana penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia. Susunan bit setiap pixel terdiri dari MSB (Most Significant bit) dan LSB (least significant bit). Bit citra yang cocok untuk diganti adalah bit LSB, karena penggantian hanya mengubah nilai *byte* tersebut satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya, sehingga perubahan satu bit LSB tidak mengubah warna tersebut secara berarti, dan mata manusia tidak dapat membedakan perubahan yang kecil ini. gambar 1 menunjukkan susunan bit pada sebuah *byte*



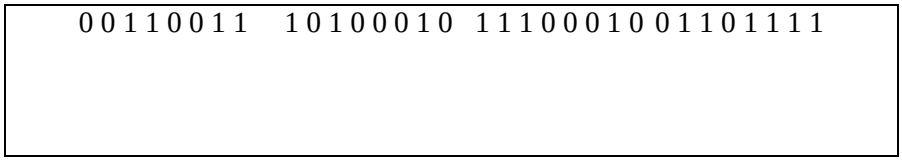
Gambar 1. susunan bit pada sebuah *byte*

Keterangan :

LSB = *Least Significant Bit*

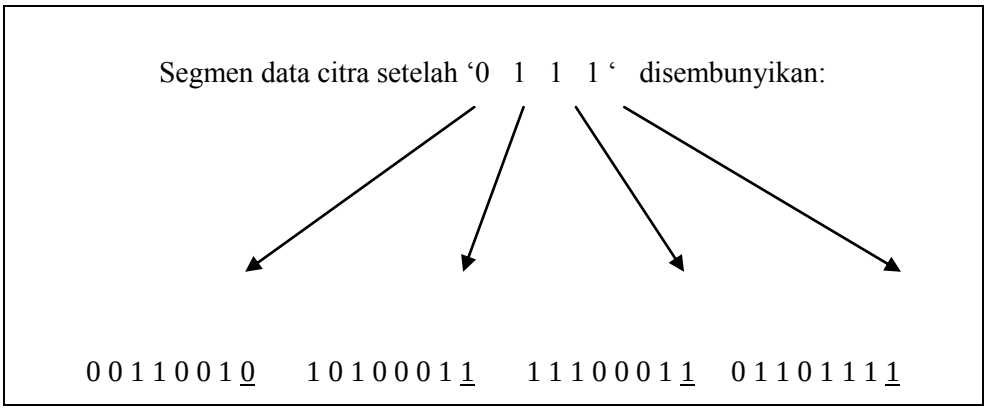
MSB = *Most Siginificant Bit*

Misalkan segmen pixel-pixel citra sebelum penambahan bit-bit rahasia seperti yang ditunjukkan pada gambar 2.



Gambar 2. Segmen pixel-pixel citra sebelum penambahan bit-bit watermark

Misalkan data rahasia (yang telah dikonversi ke sistem biner) adalah 0111. Setiap bit dari data rahasia menggantikan posisi LSB dari segmen data citra seperti yang ditunjukkan pada gambar 3.



Gambar 3. Segmen citra setelah penyisispan pada LSB

Algoritma Steganografi ini bekerja dalam domain waktu. Domain waktu memodifikasi nilai byte dari media yang akan disisipinya Citra yang digunakan sebagai media yang akan disisipkan data rahasia merupakan citra berwarna 24 bit, dimana setiap pikselnya terdiri atas susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit dari 0 sampai 255 dalam format biner dari 00000000 sampai 11111111.

Pada proses penyisipan data rahasia, langkah awalnya setiap piksel dari citra akan diubah kedalam bentuk biner untuk mendapatkan bit terendahnya. Langkah berikutnya, mengubah data rahasia yang akan disisipkan menjadi bit-bit biner. Setelah itu mengganti setiap bit rendah dengan bit data rahasia.

Algoritma Penyisipan

1. Langkah-langkah untuk menyisipkan data paa media penampung:
   mengubah setiap piksel gambar asli menjadi raster data dengan cara sebagai berikut :

   Baca Pixel → RGB → Raster data(Bil.biner) → LSB → bit rendah (0 atau 1)

2. mengubah data rahasia (bertipe karakter) menjadi bit-bit

   Baca Pesan → karakter → bil ASCII (bil.desimal) → bit pesan (bil.biner)

3. Menganti setiap bit rendah dengan bit data rahasia.
   Jika bit rendah = bit data rahasia, maka raster data tidak berubah. Jika bit rendah lebih kecil dari bit data rahasia, maka raster data ditambah 1. Jika bit rendah lebih besar dari bit data rahasia, maka raster data dikurangi 1.
4. menulis pixel yang baru sesuai dengan raster data :

   raster data → RGB → Pixel

contoh :

Pesan rahasia : hati-hati…..
Pesan berikut ini merupakan contoh dari penyandian pesan dalam bentuk teks

Gambar Asli : donald.jpg

Tabel 1. Contoh Metode Penyisipan

Pixel	Gambar Asli RGB (Red)	Raster Data	Bit Rendah	Bit Pesan (Huruf ‘h’)	Hasil	Gambar Stego RGB (Red)
[1,1]	46	00101110	0	0	00101110	46
[2,1]	39	00100111	1	1	00100111	39
[3,1]	36	00100100	0	1	00100101	37
[4,1]	29	00011101	1	0	00011100	28
[5,1]	21	00010101	1	1	00010101	21
[6,1]	30	00011110	0	0	00011110	30
[7,1]	46	00101110	0	0	00101110	46
[8,1]	47	00101111	1	0	00101110	46

Algoritma Ekstraksi

Langkah-langkah untuk ekstraksi data:

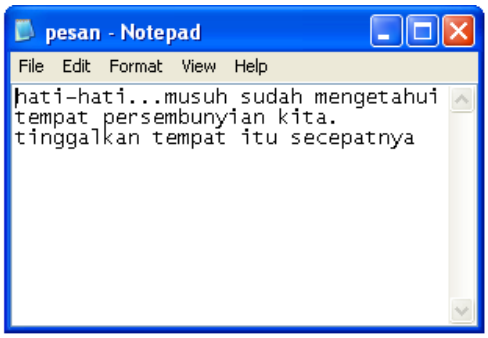
1. Setiap pixel stego image (citra yang sudah disisipi pesan) diubah menjadi raster data agar memperoleh bit rendah. Prosesnya sama dengan tahap pertama pada proses penyisipan.
2. Bit rendah setiap pixel dikumpulkan hingga terbentuk bit stream. Arah bacanya adalah atas ke bawah dan kiri ke kanan. Setiap 8 bit stream mempresentasikan sebuah karakter, Setelah semua bit stream diubah menjadi karakter, akan diperoleh pesan tersembunyinya diantara kumpulan karakter.

Tabel 2. Contoh Metode Ekstraksi

Pixel	Gambar Stego RGB (Red)	Raster Data	Bit rendah	Bit Stream	Hasil
[1,1]	46	00101110	0	01101000	h
[2,1]	39	00100111	1		
[3,1]	37	00100101	1		
[4,1]	28	00011100	0		
[5,1]	21	00010101	1		
[6,1]	30	00011110	0		
[7,1]	46	00101110	0		
[8,1]	46	00101110	0		

Sebagai contoh ilustrasi, Gambar 4(a) adalah citra dengan format file jpg yang akan digunakan sebagai media untuk menampung/menyembunyikan sebuah data. Sedangkan gambar 4(b) merupakan data yang akan disisipkan/disembunyikan pada media penampung.

(a) Citra penampung



(b) Data yang disembunyikan

Gambar 4. Citra penampung dan data yang di sembunyikan

Dengan menggunakan algoritma penyisipan, maka data akan disisipkan ke dalam citra penampung. Gambar 5 merupakan citra yang sudah disisipkan data, yang disebut dengan stego image.

Gambar 5. Stego Image

Kesimpulan

Steganografi adalah teknik menyembunyikan data rahasia didalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui oleh orang.

Metode Penggantian LSB merupakan metode penyembunyian data yang paling sederhana. Penggantian LSB dilakukan dengan memodifikasi bit terakhir dalam satu byte data, yang menyebabkan nilai byte menjadi satu lebih tinggi atau satu lebih rendah. Perubahan pada satu bit LSB hanya menyebabkan sedikit perubahan yang tidak dapat dideteksi oleh mata manusia

Daftar Pustaka

Supangkat, S, H., Kuspriyanto., dan Juanda., 2000, *Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital*, Majalah Ilmiah Teknik Elektro. Vol 6. No.3.

Munir, R., 2004, *Pengolahan Citra Digital Dengan Pendekatan Algoritmik*, Informatika , Bandung.

Thana, S.M, 2008, *Steganografi pada Citra Digital Dengan FAST FOURIER TRANSFORM*, Tesis S2, Ilmu Komputer UGM, Yogyakarta

Paulus, E., dan Nataliani, Y., 2007, *GUI Matlab*, Andi Offset, Yogyakarta