Pengembangan Metode Pencegahan Serangan *Enhanced LSB*

Ikmal Syifai 13508003[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*if18003@students.if.itb.ac.id*

***Abstrak*—Makalah ini membahas metode pencegahan untuk serangan dengan metode *enhanced LSB*. Pada citra dengan kontras tinggi, serangan akan menyebabkan citra pembawa pesan sangat mudah dibedakan dari aslinya. Dari hasil percobaan, dapat disimpulkan bahwa metode pencegahan yang diusulkan berhasil.**

***Kata kunci*—steganografi, enhanced LSB, steganalisis.**

I. PENDAHULUAN

Steganografi berasal dari bahasa Yunani steganos yang berarti tersembunyi dan graphei yang berarti tulisan. Secara harfiah, steganografi adalah tulisan tersembunyi. Steganografi adalah seni untuk menyembunyikan pesan.

Hal yang membedakan antara steganografi dan kriptografi adalah steganografi hanya menyembunyikan. Agar pesan menjadi tidak terbaca atau tidak dapat dimengerti, digunakan enkripsi yang merupakan ranah ilmu kriptografi. Karena itu seringkali pesan dienkripsi terlebih dulu sebelum disembunyikan.

Media yang digunakan untuk menyembunyikan pesan terus berkembang sesuai teknologi. Penyembunyian pesan pada tahun 440 sebelum masehi menggunakan media kepala budak. Kepala budak digunduli kemudian pesan ditulis di kepalanya. Setelah tumbuh rambut, budak dikirim ke penerima pesan. Pesan tersebut dapat dibaca setelah budak digunduli kembali.

Saat era multimedia ini, pesan bisa disembunyikan di berbagai media mulai dari teks, gambar, hingga video. Makalah ini akan membahas metode penyembunyian pesan yang tahan akan serangan *enhanced LSB*.

Salah satu metode untuk menyembunyikan pesan pada gambar adalah penyembunyian bit pesan pada bit LSB (least significant bit) pembawa pesan.

Sebuah gambar mengandung informasi yang dapat diukur dengan satuan piksel. Sebuah gambar dengan lebar 800 piksel dan panjang 600 piksel mengandung 480.000 piksel.

Satu piksel pada gambar mempunyai panjang n-bit. Pada gambar 24-bit maka 1 piksel mempunyai panjang 24 bit. Dari 24 bit yang ada, masing-masing 8 bit dialokasikan untuk mengkodekan komponen RGB (Red Green Blue).

Sebagai ilustrasi, pada gambar 24 bit, satu piksel akan diwakili oleh deretan bit berikut:

10010011 10010100 10000101
R G B

Penyembunyian pesan dilakukan dengan mengubah bit terakhir (LSB) dari setiap piksel pembawa pesan dengan bit pesan. Misalkan pesan yang akan dikirim adalah KRIPTO. Enam huruf tersebut akan diubah menjadi 6 byte pesan yaitu:

K	:	0100 1011
R	:	0101 0010
I	:	0100 1001
P	:	0101 0000
T	:	0101 0100
O	:	0100 1111

Kemudian masing-masing bit pesan akan disisipkan pada bit terakhir dari bit pembawa pesan. Pada contoh ini 3 bit yang pertama kali akan disisipkan adalah bit 010 yang memulai huruf K. Tiga bit yang terakhir disisipkan adalah bit 111 yang mengakhiri huruf O.

Asumsikan gambar yang akan disisipi pesan adalah gambar 24-bit dan piksel pertama dari gambar tersebut adalah 10010011 10010100 10000101.

Piksel pertama dari pembawa pesan
10010011 10010100 10000101
Pesan yang disisipkan
111
Piksel pertama dari pembawa pesan setelah proses
10010010 10010101 10000100

Setelah proses penyembunyian pesan, gambar pembawa pesan tidak akan berubah secara visual. Persepsi yang dirasakan oleh manusia tidak bisa membedakan bit LSB yang diubah.

Dengan tidak mampunya persepsi manusia membedakan dua gambar di atas, maka serangan visual manusia tidak akan bisa memecahkan steganografi dengan metode pengubahan bit LSB. Karena itulah dikembangkan sebuah metode serangan enhanced LSB.

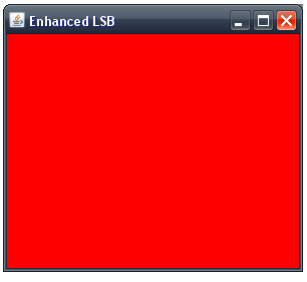
Enhanced LSB adalah serangan dengan mengubah bit pada kanal warna sesuai bit LSBnya. Sebagai ilustrasi, diasumsikan piksel berikut adalah piksel dari gambar pembawa pesan 10010010 10010101 10000100.

Piksel pembawa pesan
10010010 10010101 10000100
Piksel pembawa pesan setelah proses
00000000 11111111 00000000

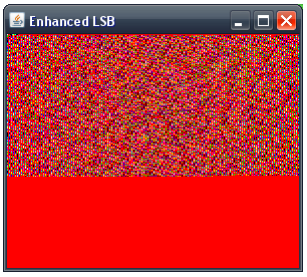
Pada gambar dengan kontras tinggi, serangan akan membuat gambar pembawa pesan menjadi berbeda dengan gambar aslinya. Dengan perbandingan ini, steganalis dapat memastikan bahwa ada pesan yang disembunyikan. Selanjutnya steganalis dapat menghancurkan pesan hanya dengan mengganti bit LSB dari tiap kanal warna RGB.

Gambar 1 Gambar tanpa pesan

Gambar 2 Gambar dengan pesan



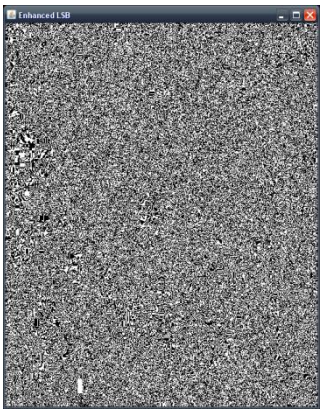
Gambar 3 Serangan enhanced LSB terhadap gambar tanpa pesan



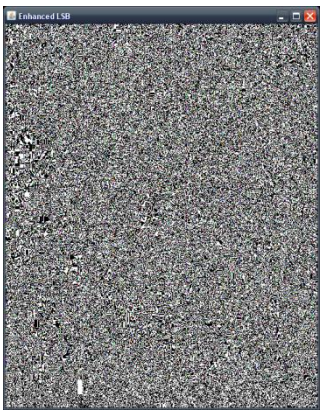
Gambar 4 Serangan enhanced LSB terhadap gambar dengan pesan

Gambar 5 Gambar tanpa pesan

Gambar 6 Gambar dengan pesan



Gambar 7 Serangan enhanced LSB terhadap gambar tanpa pesan



Gambar 8 Serangan enhanced LSB terhadap gambar dengan pesan

Gambar 1-8 memberi ilustrasi bagaimana serangan enhanced LSB dilakukan. Namun demikian, dapat dilihat bahwa serangan tersebut tidak dapat dilakukan untuk gambar dengan kontras rendah.

II. METODE YANG DIAJUKAN

Ada beberapa pengetahuan yang dijadikan dasar metode yang diajukan ini:

1. Penyembunyian pesan dilakukan dengan pengubahan bit LSB.
2. Serangan dilakukan dengan metode enhanced LSB yaitu mengubah bit selain LSB sesuai bit LSBnya.

Dengan pengetahuan di atas diajukan dua buah metode untuk mencegah serangan tersebut, yaitu:

1. Penyembunyian pesan dilakukan dengan mengubah bit ke 7 (sebelum LSB) dari tiap kanal RGB.
2. Penyembunyian pesan dilakukan dengan mengubah bit ke 7 (sebelum LSB) dari kanal RGB secara bergantian.

Metode 1 dapat diilustrasikan sebagai berikut. Asumsikan gambar yang akan disisipi pesan adalah gambar 24-bit dan piksel pertama dari gambar tersebut adalah 10010011 10010100 10000101.

Piksel pertama dari pembawa pesan
10010011 10010100 10000101
Pesan yang disisipkan
111
Piksel pertama dari pembawa pesan setelah proses
10010011 10010110 10000111

Pseudocode dari algoritma metode 1:

```
//jika carrier mampu menampung pesan
if(carrier.length/8>message.length){
        //untuk setiap bit pesan ..
        for(i=0;i<message.length;i++){
        //.. sisipkan di bit ke-7 tiap kanal
        if(i%3=0){
        carrier[i].r[6]=message[i];
        carrier[i].g[6]=message[i+1];
        carrier[i].b[6]=message[i+2];
        }
        else{
        continue;
        }
        }
}
```

Dengan demikian, saat steganalis mengubah bit selain LSB sesuai dengan bit LSBnya maka hasilnya tidak akan berbeda dengan gambar asli yang diserang. Dengan hasil seperti itu steganalis tidak akan mengetahui perbedaan antara gambar dengan dan tanpa pesan.

Metode 2 menggunakan cara yang hampir sama tetapi mengubah bit ke 7 dari kanal RGB secara bergantian. Hal ini ditujukan agar kualitas gambar tidak terlalu buruk. Asumsikan gambar yang akan disisipi pesan adalah gambar 24-bit dan piksel pertama, kedua, dan ketiga dari gambar tersebut adalah 10010011 10010100 10000101, 10111011 10110110 10101101, dan 10010111 11010100 10110100.

Tiga piksel pertama dari pembawa pesan
10010011 10010100 10000101
10111011 10110110 10101101
10010111 11010100 10110100
Pesan yang disisipkan
111
Tiga piksel pertama dari pembawa pesan setelah proses
10010011 10010100 10000101
10111011 10110110 10101101
10010111 11010100 10110110

Pseudocode dari algoritma metode 2:

```
//jika carrier mampu menampung pesan
if(carrier.length/24>message.length){
        //untuk setiap bit pesan ..
        for(i=0;i<message.length;i++){
        //.. sisipkan di bit ke-7 bergantian
        switch(i%3){
        case0:
        carrier[i].r[6]=message[i];break;
        case1:
        carrier[i].g[6]=message[i];break;
        case2:
        carrier[i].b[6]=message[i];break;
        }
        }
}
```

Dari dua metode di atas, ada dua faktor yang akan diuji, yaitu:

1. Berhasil tidaknya pencegahan serangan dengan metode enhanced LSB.
2. Kualitas gambar yang dihasilkan dengan metode yang diajukan

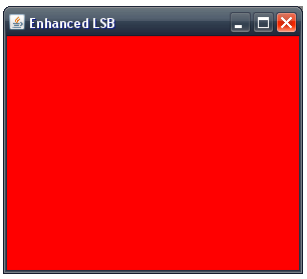
Penelitian dilakukan dengan menggunakan dua gambar, yaitu gambar kotak berwarna merah dan gambar grayscale dari seorang artis. Kedua gambar ini diambil dari chapman.edu yang menggunakannya sebagai objek percobaan steganografi.

Dalam penelitian ini digunakan cerita pendek yang ditulis oleh Ernest H. berjudul "Elephant" sebagai pesan yang disembunyikan. Pesan ini berukuran sekitar 7700 byte.

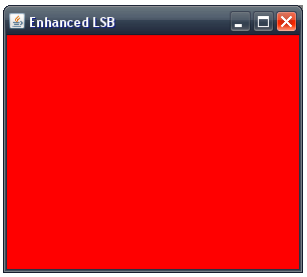
Setelah pesan disembunyikan dengan metode yang diajukan, gambar pembawa pesan diserang dengan metode enhanced LSB.

III. HASIL PENELITIAN

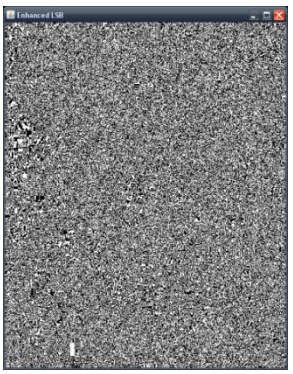
Dari dua metode yang diajukan, berikut adalah gambar dari hasil serangan. Gambar 9-12 menggunakan metode 1 sedangkan gambar 13-16 menggunakan metode 2.



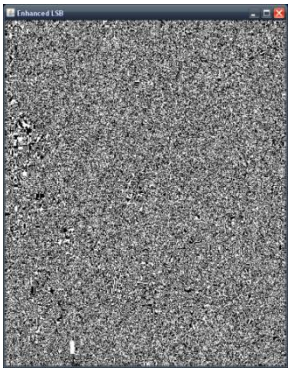
Gambar 9 Serangan enhanced LSB terhadap gambar tanpa pesan (metode 1)



Gambar 10 Serangan enhanced LSB terhadap gambar dengan pesan (metode 1)



Gambar 11 Serangan enhanced LSB terhadap gambar tanpa pesan (metode 1)

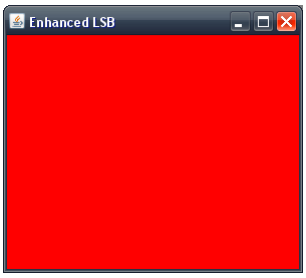


Gambar 12 Serangan enhanced LSB terhadap gambar dengan pesan (metode 1)

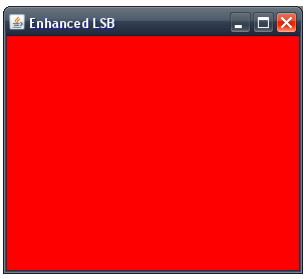
Dapat dilihat bahwa tidak ada perbedaan secara visual antara gambar 9-10 dan gambar 11-12. Pada metode modifikasi LSB, gambar dengan kontras tinggi akan tampak berbeda jika diserang dengan enhanced LSB. Dengan metode yang diajukan (metode 1), tidak tampak perbedaan antara gambar dengan pesan dan gambar tanpa pesan.

Sama seperti metode modifikasi LSB, gambar grayscale atau dengan kontras rendah tidak bisa dideteksi apakah disisipi pesan atau tidak. Dengan menggunakan metode 1, steganalis tidak akan mampu menentukan gambar mana yang mengandung pesan.

Metode 1 mempunyai kelebihan yaitu mampu menampung pesan lebih banyak dibanding metode 2. Tetapi kualitas gambar yang dihasilkan lebih buruk karena memodifikasi lebih banyak bit.

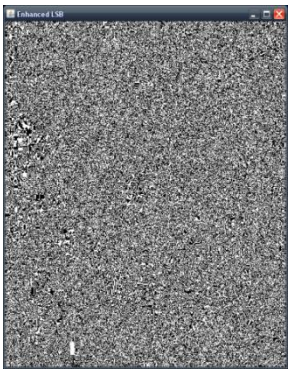


Gambar 13 Serangan enhanced LSB terhadap gambar tanpa pesan (metode 2)



Gambar 14 Serangan enhanced LSB terhadap gambar dengan pesan (metode 2)

Gambar 15 Serangan enhanced LSB terhadap gambar tanpa pesan (metode 2)



Gambar 16 Serangan enhanced LSB terhadap gambar dengan pesan (metode 2)

Gambar 13-16 menampilkan hasil serangan enhanced LSB terhadap gambar dengan metode 2. Tidak ada perbedaan yang terlihat secara vidual antara gambar dengan pesan dan tanpa pesan. Untuk gambar grayscale juga tidak ada perubahan, tetap tidak bisa dibedakan.

Dibanding dengan metode 1, metode 2 menghasilkan kualitas gambar yang lebih baik karena hanya menggunakan bit sejumlah 1/3 dari bit yang digunakan metode 1. Namun demikian, kapasitas pesan yang mampu ditampung menjadi kecil karena setiap piksel hanya bisa membawa 1 bit pesan.

IV. SIMPULAN

Ada dua simpulan yang bisa diambil dari hasil penelitian:

1. Metode 1 mampu menampung pesan lebih banyak dengan gambar yang sama dibanding metode 2.
2. Metode 2 mampu menghasilkan kualitas gambar yang lebih baik dibanding metode 1.

Karena itu penggunaan metode yang diajukan harus memperhatikan kebutuhan, jika dibutuhkan metode untuk menampung pesan lebih banyak, maka gunakan metode 1. Jika ingin menghasilkan kualitas gambar yang lebih baik, maka gunakan metode 2.

V. SARAN

Dari simpulan di atas, ada beberapa pengembangan yang dapat dilakukan:

1. Pengembangan metode dengan kualitas gambar dan kemampuan menampung pesan yang minimal sama dengan metode modifikasi LSB.
2. Pengembangan metode serangan enhanced LSB yang bisa digunakan untuk gambar grayscale atau kontras rendah.

REFERENSI

R. Munir, Steganografi http://www1.chapman.edu/~nabav100/ImgStegano/screenshots.html diakses tanggal 24 Maret 2013.

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
ttd

Ikmal Syifai
13508003