ANALISIS STEGANOGRAFI METODE *LEAST SIGNIFICANT BIT* (LSB) DENGAN PENYISIPAN SEKUENSIAL DAN ACAK SECARA KUANTITATIF DAN VISUAL

Erwin Yudi Hidayat[1], Khafiizh Hastuti[2]
[1,2]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jalan Nakula I No. 5-11, Semarang, 50131, (024) 3517261
E-mail : erwin@dsn.dinus.ac.id[1], afis@dosen.dinus.ac.id [2]

Abstrak

Penelitian ini bertujuan untuk melakukan analisis terhadap steganografi Least Significant Bit (LSB) yang mampu menyisipkan pesan secara sekuensial dan acak. Analisis dilakukan untuk mengetahui penyisipan yang manakah yang memiliki kemampuan paling baik. Secara kuantitatif, Peak Signal to Noise Ratio (PSNR) digunakan untuk mengukur kualitas citra. Sedangkan secara visual, steganalisis Enhanced LSB dimanfaatkan untuk mengetahui teknik mana yang mampu menyisipkan pesan tanpa mudah dideteksi. Hasil percobaan menunjukkan, penyisipan secara acak memiliki kemampuan lebih baik daripada penyisipan secara sekuensial.

Kata Kunci: *steganografi, acak, sekuensial, PSNR, Enhanced LSB*

Abstract

This research is aimed to analyze Least Significant Bit (LSB) steganography that able to embed message in sequence method as well as randomly. Analysis is conducted to investigate which embedding scheme has better performance. Quantitative analysis uses Peak Signal to Noise Ratio (PSNR) to measure image quality. Meanwhile Enhanced LSB steganalysis is utilized to examine which technique has higher imperceptibility. Result shows that random embedding method outperforms sequence embedding technique for both quantitative and visual means.

Keywords: *steganography, random, sequence, PSNR, Enhanced LSB*

1. PENDAHULUAN

Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet naik dari satu juta di tahun 1999 menjadi (prediksi) 12 juta di tahun 2004. Hasil survei PT Telkom Desember 2003 menunjukkan bahwa *e-mail* dan browsing adalah alasan utama 1.500 responden. Di antaranya 48,3 persen menggunakan internet untuk *e-mail* dan 35,1 persen untuk keperluan *browsing* [1].

Media internet dipilih karena kemudahan penggunaan dan efisiensi waktu yang diperlukan dalam pengiriman informasi. Kelemahan pengiriman informasi melalui media internet adalah pada masalah jaminan keamanan. Banyak orang mencoba mencuri informasi rahasia yang tidak menjadi haknya melalui media tersebut.

Peritel AS TJX Cos, Inc. pada tahun 2006 mengumumkan pencurian 45,7 juta informasi kartu kredit dan kartu debit milik para pelanggannya. Pencurian informasi tersebut berlangsung terus-menerus selama 18 bulan dan TJX baru mengetahuinya di tahun 2007 [2]. Di Indonesia pada tahun 2001, survei AC Nielsen mencatat bahwa Indonesia berada pada posisi keenam terbesar di dunia atau keempat di Asia dalam tindak kejahatan *cyber*.

Data ClearCommerce yang bermarkas di Texas, Amerika Serikat mencatatkan bahwa pada 2002 Indonesia berada di urutan kedua setelah Ukraina sebagai negara asal *carder* terbesar di dunia. Sementara itu, Verisign, perusahaan keamanan teknologi informasi dunia, mencatat bahwa Indonesia berada pada peringkat paling atas di dunia dalam hal persentase kejahatan penipuan perbankan di dunia [1].

Steganografi sebagai suatu seni penyembunyian pesan ke dalam media, banyak dimanfaatkan untuk mengirim pesan rahasia melalui internet agar tidak diketahui orang lain.

Penggunaan steganografi menjadi daya tarik banyak orang pada peristiwa penyerangan gedung *World Trade Centre* (WTC), 11 September 2001. Pada peristiwa tersebut 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" [3]. Isu lainnya menyebutkan bahwa teroris menyembunyikan pesan-pesannya dalam gambar-gambar porno di *website* tertentu.

Metode yang paling banyak digunakan untuk melakukan steganografi adalah *Least Significant Bit* (LSB). Penelitian mengenai steganografi teknik LSB pernah dilakukan oleh beberapa orang. Di antaranya [4], yang membahas steganografi LSB menggunakan media file gambar *Graphical Interchange Format* (gif). Penelitian serupa pernah dilakukan oleh [5] dan [6] melakukan penelitian ketahanan citra yang telah disisipi pesan menggunakan steganografi LSB, terhadap perubahan *brightness* dan kontras citra.

Namun demikian, steganografi LSB ini perlu diteliti, tentang bagaimana kemampuan metode sekuensial (berurutan) dan random (acak) dalam menyisipkan pesan. Untuk mengukur kemampuan tersebut, dibutuhkan alat ukur yang akan digunakan sebagai parameter analisis secara kuantitatif. Penulis menggunakan *Peak Signal to Noise Ratio* (PSNR), yang digunakan untuk mengetahui kualitas citra hasil steganografi.

Untuk mengetahui kemampuan metode sekuensial (berurutan) dan random (acak) digunakan analisis visual *Enhanced* LSB. Analisis ini memperlihatkan LSB dari tiap-tiap citra yang disisipi pesan, sehingga dapat terlihat perbedaan letak bit-bit pesan yang disisipkan.

2. STEGANOGRAFI

2.1 Least Significant Bit (LSB)

Terdapat dua langkah dalam sistem steganografi yaitu proses penyembunyian (*embedding*) dan ekstraksi data dari berkas penampung. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen citra dengan bit-bit data rahasia.

Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB).

Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan *byte* tersebut

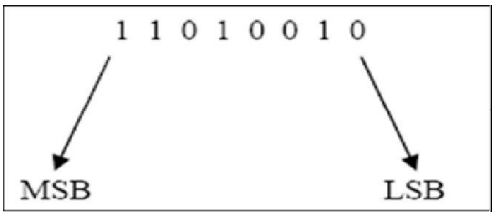
menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil.

Sebagai contoh, urutan bit berikut ini menggambarkan 3 piksel pada c*over-image* 24-bit.

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

Pesan yang akan disisipkan adalah karakter "A", yang nilai biner-nya adalah 10000011, maka akan dihasilkan *stegoimage* dengan urutan bit sebagai berikut:

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



Gambar 1. Contoh bit MSB dan LSB

2.2 Steganografi Metode LSB

Ada dua jenis teknik yang dapat digunakan pada metode LSB, yaitu secara sekuensial (berurutan) dan secara *random* (acak).

2.2.1 Sekuensial (Berurutan)

a) Teknik Penyembunyian Pesan (*embedding*)

Penyembunyian pesan secara sekuensial (berurutan) berarti pesan rahasia disisipkan secara berurutan dari data titik pertama yang ditemukan pada file gambar. Penyisipan dilakukan dari indeks (0,0), dari kiri ke kanan, baris per baris, sepanjang bit-bit pesan yang disembunyikan.

Algoritma penyisipan LSB sekuensial:

```
for i = 1,...,l(c) do
    si ← ci
end for
for i = 1 ...,l (m) do
    compute index ji where
    to store ith message bit
    sji ← cji <-> mi
end for
```

b) Teknik Pengungkapan Pesan (ekstraksi)

Ekstraksi pesan dilakukan dengan cara mengekstrak bit-bit LSB sebagaimana urutan proses penyisipan. Dimulai dari indeks (0,0), dari kiri ke kanan, baris per baris, sehingga diperoleh bit-bit LSB. Berdasarkan bit-bit tersebut, kemudian disusun ulang hingga diperoleh nilai bit pesan yang disisipkan.

Algoritma proses ekstraksi:

```
for i = 1,...,l(M) do
    compute index ji where
    the ith message bit is
    stored
    mi ← LSB (cij)
end for
```

2.2.2 Acak (*Random*)

a) Teknik Penyembunyian Pesan (*embedding*)

Acak berarti penyisipan pesan rahasia dilakukan secara acak pada gambar. Untuk melakukan penyisipan secara acak, bit-bit data rahasia tidak disipkan dengan mengganti *byte-byte* yang berurutan, namun dipilih susunan *byte* secara acak. Misalnya jika terdapat 50 *byte* dan 6 bit data yang akan disembunyikan, maka *byte* yang diganti bit LSB-nya dipilih secara acak, misalkan *byte* nomor 36, 5, 21, 10, 18, 49. Bilangan acak tersebut

dapat dibangkitkan dengan metode *pseudorandom number generator* (PRNG).

Bilangan acak dibangkitkan dengan PRNG kriptografi. *Pseudorandom Number Generator* kriptografi sebenarnya adalah algoritma kriptografi yang digunakan untuk enkripsi. PRNG dibangun dengan algoritma *hash Message Digest 5* (MD5). Tujuan dari enkripsi adalah menghasilkan sekumpulan bilangan acak yang sama untuk setiap kunci enkripsi yang sama. Bilangan acak dihasilkan dengan cara memilih bit-bit dari sebuah blok data hasil enkripsi

Algoritma penyisipan LSB *random*:

```
for i = 1...,l(c) do
   s_i ← c_i
end for
generate random sequence
k_i using seed k
n ← k_1
for i = 1,...,l(m) do
   s_n ← c_n ↔ m_i
   n ← n + k_i
end for
```

b) Teknik Pengungkapan Pesan (ekstraksi)

Data yang disembunyikan di dalam citra dapat dibaca kembali dengan cara pengungkapan (*reveal* atau *extraction*). Posisi *byte* yang menyimpan bit data dapat diketahui dari bilangan acak yang dibangkitkan oleh PRNG. Karena algoritma kriptografi yang digunakan menggunakan kunci pada proses enkripsi, maka kunci yang sama digunakan untuk membangkitkan bilangan acak. Bilangan acak yang dihasilkan sama dengan bilangan acak yang dipakai pada waktu penyembunyian data. Dengan demikian, bit-bit data rahasia yang bertaburan di dalam citra dapat dikumpulkan kembali.

Algoritma proses ekstraksi:

```
generate random sequence k_i
using seed k
   n ← k_1
   for i = 1,...,l(m) do
        m_i ← LSB(c_n)
        n ← n + k_i
   end for
```

c) Penggunaan Kunci

Pesan yang disisipkan akan melalui proses pengacakan terlebih dahulu, sehingga proses ekstraksi nantinya juga harus diurutkan kembali. Kedua proses ini menggunakan kunci, yaitu sebagai *seed* dalam pembangkitan deretan bilangan acak yang menjadi pengatur letak pesan. Pesan diubah ke dalam bentuk biner, dan pengacakan atau pengurutan dilakukan dengan mengubah letak biner tersebut.

Deretan bilangan acak ini memakai algoritma *Linear Congruential Generator* (LCG). Nilai *seed* dibangkitkan melalui fungsi MD5 dari *string* kunci, yang menjadi sebuah bilangan dengan ukuran 128-bit.

Jumlah bilangan acak yang dihasilkan adalah sebanyak biner pesan, dan proses pengurutan akan memakai deretan yang sama untuk mengembalikannya menjadi pesan yang asli.

2.3 Kriteria Steganografi

Kriteria yang harus diperhatikan dalam penyembunyian data tersebut di adalah [7]: 1) *Fidelity*. Mutu citra penampung tidak jauh berubah. 2) *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali. 3)

Imperceptibility. Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi.

2.4 *Peak Signal to Noise Ratio* (PSNR)

Peak Signal to Noise Ratio adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut, dalam satuan desibel (dB). Semakin besar parameter PSNR semakin mirip dengan citra asli.

$$PSNR = 10 . log \left(\frac{MAX_i^2}{MSE}\right) = 20. log \left(\frac{MAX_i}{\sqrt{MSE}}\right)$$

$$MSE = \frac{1}{mn} \sum_{i}^{m} \sum_{j}^{n} \left| I_{(i,j)} - K_{(i,j)} \right|^2$$

(1)

dengan MSE = nilai *Mean Square Error* dari citra tersebut; m = panjang citra (dalam piksel); n = lebar citra (dalam piksel), (i,j) = koordinat masing-masing piksel; I = nilai intensitas citra asli; K = nilai intensitas citra setelah disisipi pesan (*stegoimage*)

2.6 Kriteria Kualitas Citra Dilihat dari PSNR

Tabel 1: Nilai PSNR kriteria kualitas citra

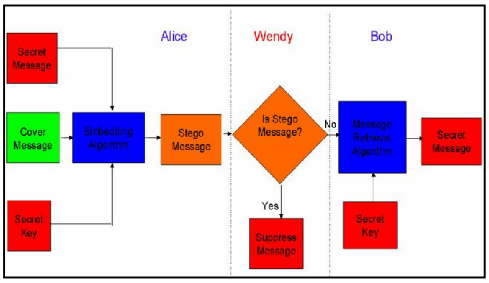
Nilai PSNR	Kualitas Citra
60 dB	*Excellent*, tanpa derau
50 dB	*Good*, terdapat sejumlah derau tapi kualitas citra masih bagus
40 dB	*Reasonable*, terdapat butiran halus atau seperti salju di dalam citra
30 dB	*Poor picture*, terdapat banyak derau
20 dB	*Unusable*

Kriteria kualitas citra dapat dilihat dari nilai PSNR [1], seperti pada tabel 1 di atas.

2.7 Steganalisis *Enhanced* LSB

Pada dasarnya, *Enhanced* LSB merupakan metode untuk mendeteksi adanya pesan rahasia di dalam sebuah media, yang disebut dengan steganalisis Pengertian steganalisis mengacu pada seni dan ilmu pengetahuan dalam membedakan antara *stego-object* dan *cover-object*. Dalam hal ini, steganalisis membedakan antara citra asli yang berisi pesan yang tersembunyi dan citra penutup yang digunakan untuk menyembunyikan pesan. Hal penting yang menjadi bahasan utama dalam steganalisis adalah mengetahui ada atau tidaknya pesan yang disisipkan pada suatu objek.

Ide yang mendasari teknik *Enhanced* LSB adalah menghilangkan seluruh bagian gambar sampai hanya terlihat bagian-bagian yang mungkin disisipi pesan, sehingga akan dihasilkan suatu gambar baru yang terlihat secara kasat mata apabila ada data lain di dalamnya. Hal ini berarti metode steganalisis secara visual membutuhkan bantuan manusia untuk menyelesaikan prosesnya.



Gambar 2. Proses Steganalisis Secara Umum

Algoritma ini dikemukakan oleh Andreas Westfeld. Proses utama dari metode *enhanced LSB* akan dijelaskan sebagai berikut: setiap piksel memiliki tiga buah komponen yaitu *Red*, *Green*, *Blue*. Setiap komponen direpresentasikan oleh satu *byte*, setiap *byte* memiliki sebuah bit LSB. Apabila

bit LSB tersebut adalah 1, maka semua bit pada *byte* tersebut diganti dengan bit 1 sehingga nilai *byte* tersebut adalah 11111111 (biner) atau 255 (desimal).

Sedangkan, apabila bit LSB tersebut adalah 0, maka semua bit pada *byte* tersebut diganti dengan bit 0 sehingga nilai *byte* tersebut adalah 00000000 (biner) atau 0 (desimal) [20]. Misalnya terdapat sebuah piksel dengan komposisi *byte* sebagai berikut:

Tabel 2: Komposisi Byte

BLUE	GREEN	RED
1010010**1**	1001110**0**	1110011**1**

Maka setelah mengalami *enhanced LSB*, *byte* di atas akan menjadi:

Tabel 3: Komposisi Byte Setelah Enhanced LSB

BLUE	GREEN	RED
11111111	**00000000**	**11111111**

Setelah melalui proses penyaringan, maka citra pada bagian gambar yang tidak disisipi pesan akan mendekati bagian gambar semula. Sedangkan bagian gambar yang mengandung pesan rahasia akan menjadi ”rusak” setelah disaring. Dengan demikian, dari gambar yang dihasilkan setelah penyaringan, mata manusia dapat dengan mudah membedakan apakah pada gambar tersebut terdapat pesan rahasia atau tidak.

3. EKSPERIMEN

Pesan yang disisipkan ke dalam citra memiliki prosentase 10%, 20%, 30%, 40%, dan 50% dari kapasitas maksimum pesan yang dapat ditampung oleh citra. Citra *udinus.bmp* pada gambar 3 mampu disisipi pesan sebanyak 400x400x3= 480.000 bit, atau 480.000 : 8 = 60.000 *byte* (60 KB). Dengan ukuran 60 KB, maka 10% dari kapasitas maksimum pesan yang dapat disisipkan sebanyak 6 KB (*pesan10.txt*). Dua puluh sampai 50% secara berturut-turut adalah 12 KB (*pesan20.txt*), 18 KB (*pesan30.txt*), 24 KB (*pesan40.txt*), dan 32 KB (*pesan50.txt*). *Stegoimage* yang disisipi pesan-pesan tersebut disajikan dalam tabel 2.

Gambar 3. Citra asli *udinus.bmp*

Tabel 4: *Stegoimage* hasil penyisipan sekuensial dan *random* pada *udinus.bmp*

No	Pesan disisipkan		*Stegoimage sekuensial*	*Stegoimage random*
	Nama	Prosentase		
1	*pesan10.txt* (6 KB)	10 %	*udinus10seq.bmp*	*udinus10ran.bmp*
2	*pesan20.txt* (12 KB)	20 %	*udinus20seq.bmp*	*udinus20ran.bmp*
3	*pesan30.txt* (18 KB)	30 %	*udinus30seq.bmp*	*udinus30ran.bmp*
4	*pesan40.txt* (24 KB)	40 %	*udinus40seq.bmp*	*udinus40ran.bmp*
5	*pesan50.txt* (30 KB)	50 %		

			udinus50seq.bmp	*udinus50ran.bmp*

Untuk mengetahui kemampuan steganografi LSB secara sekuensial dan acak, dihitung dengan mencari nilai PSNR dari *stegoimage* yang terbentuk. Dari perhitungan yang dilakukan dengan menggunakan kakas *LSB Insertion*, diperoleh nilai PSNR untuk tiap-tiap *stegoimage* yang dihasilkan. Hasil perhitungan tersebut disajikan dalam tabel 3.

Jika dilihat, secara kasat mata tidak menampakkan adanya perbedaan yang jelas, di mana letak pesan-pesan disisipkan ke dalam citra. Untuk itu dilakukan analisis visual steganalisis *Enhanced LSB*, guna menampilkan LSB citra secara keseluruhan. Gambar-gambar yang menampilkan LSB dari citra *stegoimage*, dapat dilihat pada tabel 4.

Tabel 3: Nilai PSNR dari *stegoimage udinus.bmp*

No	Hasil penyisipan sekuensial		Hasil penyisipan *random*	
	Stegoimage	PSNR	*Stegoimage*	PSNR
1	 *udinus10seq.bmp*	57.693	 *udinus10ran.bmp*	61.948
2	 *udinus20seq.bmp*	51.886	 *udinus20ran.bmp*	55.395
3	 *udinus30seq.bmp*	48.416	 *udinus30ran.bmp*	51.473
4	 *udinus40seq.bmp*	45.990	 *udinus40ran.bmp*	48.502
5	 *udinus50seq.bmp*	44.086	 *udinus50ran.bmp*	46.111

Tabel 4: *Stegoimage* dari *udinus.bmp* dan gambar *Enhanced LSB*-nya

No	Metode penyisipan sekuensial		Metode penyisipan *random*	
	Stego image	*Enhanced LSB*	*Stego image*	*Enhanced LSB*
1	 *udinus10seq.bmp*	 *udinus10seq_LSB.bmp*	 *udinus10ran.bmp*	 *udinus10ran_LSB.bmp*
2	 *udinus20seq.bmp*	 *udinus20seq_LSB.bmp*	 *udinus20ran.bmp*	 *udinus20ran_LSB.bmp*
3	 *udinus30seq.bmp*	 *udinus30seq_LSB.bmp*	 *udinus30ran.bmp*	 *udinus30ran_LSB.bmp*
4	 *udinus40seq.bmp*	 *udinus40seq_LSB.bmp*	 *udinus40ran.bmp*	 *udinus40ran_LSB.bmp*
5	 *udinus50seq.bmp*	 *udinus50seq_LSB.bmp*	 *udinus50ran.bmp*	 *udinus50ran_LSB.bmp*

4. HASIL DAN PEMBAHASAN

4.1 Perhitungan PSNR

Percobaan dilakukan menggunakan citra *udinus.bmp* yang memiliki ukuran 400x400 piksel. Sementara pesan yang disisipkan ke dalam citra tersebut adalah *pesan10.txt, pesan20.txt, pesan30.txt, pesan40.txt*, dan *pesan50.txt*.

Ke dalam *udinus.bmp*, masing-masing pesan tersebut disisipkan. Penyisipan sekuensial pertama dilakukan dengan menyembunyikan *pesan10.txt* ke dalam *udinus.bmp*. setelah pesan disisipkan, terbentuklah *stegoimage* dan diberi nama *udinus10seq.bmp*.

Dengan menggunakan pesan yang sama, penyisipan secara acak dilakukan. Untuk menyisipkan *pesan10.txt* ini kata kunci yang digunakan adalah `secret`. Kata kunci ini berfungsi sebagai masukkan pada pambangkitan bilangan acak PRNG, untuk menentukan piksel di mana pesan akan disisipkan. Untuk selanjutnya, percobaan penyisipan secara acak dilakukan dengan kata kunci ini.

Pengukuran PSNR kemudian dilakukan terhadap masing-masig *stegoimage*. Nilai PSNR pada *udinus10seq.bmp* sebesar 57.6936 dB dan *udinus10ran.bmp* sebesar 61.9485 dB. Mengacu pada tabel 2.8, *udinus10seq.bmp* yang terletak pada interval 50-60 dB masuk ke dalam kriteria *good* yang artinya terdapat sejumlah derau tapi kualitas citra masih bagus. Sedangkan *udinus10ran.bmp* dengan PSNR >60 dB termasuk kriteria e*xcellent*, yaitu tanpa derau.

Percobaan ke-dua, ke-tiga, ke-empat, dan ke-lima menggunakan cara serupa dengan percobaan pertama. Hasil penyisipan secara sekuensial dan acak, beserta nilai PSNR selengkapnya disajikan pada tabel 3. Pada penyisipan acak selanjutnya, kata kunci secret juga dimanfaatkan.

Pengukuran PSNR pada percobaan ke-dua yang dilakukan menujukkan kedua *stegoimage* termasuk kriteria *good*. Meski demikian, *stegoimage* hasil penyisipan secara acak menunjukkan angka yang lebih tinggi, 55.3954 untuk *udinus20ran.bmp* dan 51.8863 untuk *udinus20seq.bmp.*

Percobaan ke-tiga menujukkan kedua *stegoimage* termasuk dalam kriteria yang berbeda. Citra *udinus30seq.bmp* dengan PSNR 48.4165 termasuk kriteria *reasonable*, artinya terdapat butiran halus atau seperti salju di dalam citra. Sedangkan *udinus30ran.bmp* dengan PSNR 51.4737 termasuk kategori *good*.

Percobaan ke-empat menujukkan kedua *stegoimage* termasuk dalam kriteria *reasonable*, artinya terdapat butiran halus atau seperti salju di dalam citra. Namun demikian, *udinus40ran.bmp* memiliki nilai PSNR 48.5029, lebih tinggi dari *udinus40seq.bmp* yang hanya 45.9907.

Pengukuran PSNR pada percobaan terakhir yang dilakukan juga menujukkan kedua *stegoimage* termasuk dalam kriteria *reasonable*, artinya terdapat butiran halus atau seperti salju di dalam citra. Namun demikian, *udinus50ran.bmp* memiliki nilai PSNR 46.1115, lebih tinggi dari *udinus50seq.bmp* yang hanya 44.0863.

4.2. Hasil Steganalisis *Enhanced* LSB

Untuk membedakan di mana letak bit-bit pesan disisipkan ke dalam citra *udinus.bmp*, dilakukan steganalisis *Enhanced LSB* menggunakan *bmp2EnhancedLSB*. Percobaan ini dilakukan pada seluruh *stegoimage* yang dihasilkan menggunakan cara sekuensial maupun acak.

Pada dasarnya, analisis *Enhanced LSB* merupakan suatu teknik steganalisis untuk mendeteksi ada atau tidaknya pesan di dalam LSB citra. Teknik ini mengandalkan kejelian indra penglihatan manusia guna membedakan

mana gambar yang disisipi pesan atau tidak. Citra yang disisipi pesan mungkin saja menampilkan pola-pola tertentu, apabila LSB citra diperlihatkan. Namun, pola-pola itu bisa saja tidak dikenali mata manusia karena kemampuannya yang terbatas.

Gambar 4 berikut ini menampilkan tiga buah citra yang dua di antaranya telah disisipi pesan dengan steganografi metode LSB. Satu citra disisipi pesan secara acak, sedang satu citra yang lain secara sekuensial, dan sisanya adalah citra yang tidak disisipi pesan.

Gambar 4. Perbandingan citra asli dan dua citra yang telah disisipi pesan

Namun, kondisi tersebut akan berbeda, jika ketiga citra di atas diperlihatkan LSB-nya saja seperti pada gambar berikut:

Gambar 5. Citra Enhanced LSB dari gambar 4

Terlihat pada gambar bagian tengah di atas memiliki sejumlah data asing yang semestinya tidak dimiliki oleh gambar, seperti yang tertera pada gambar sebelah kiri. Gambar yang berada di tengah yang memakai steganografi LSB secara sekuensial dapat langsung didentifikasi bahwa gambar *Enhanced LSB*-nya memiliki pesan, karena mengandung suatu pola yang terletak di atas gambar. Lebih jauh lagi, kemungkinan besar pola tersebut dibentuk dari penyisipan berupa karakter alfanumerik, karena pada pola terdapat garis-garis vertikal teratur. Keteraturan itu dibentuk karena kode *byte* dari huruf dan angka memiliki beberapa awalan bit yang sama, sehingga terlihat seperti membentuk pola.

Sedangkan pada gambar paling kanan yang menggunakan steganografi LSB secara acak. Keberadaan pesan dalam gambar tidak begitu terlihat karena tidak membentuk pola seperti pada gambar tengah. Kata kunci dipakai sebagai masukan untuk mengacak letak bit-bit dari pesan, sehingga terlihat menyebar ke seluruh gambar.

Secara jelas, hasil percobaan untuk menghasilkan gambar *Enhanced LSB* terdapat pada tabel 4. Berikut adalah uraian penjelasan yang lebih rinci dari hasil percobaan tersebut.

Percobaan pertama dilakukan dengan menggunakan *pesan10.txt* sebesar 6 KB. Penyisipan secara sekuensial menyebabkan LSB piksel pertama dengan indeks (0,0) sampai dengan piksel ke-16.000 berisi pesan tersebut. Pada *udinus10seq_LSB.bmp* terlihat munculnya pola teratur pada sebagian kecil bagian atas citra tersebut. Menggunakan pesan dengan besar yang sama, penyisipan secara acak tidak membuat adanya pola yang nampak pada *udinus10ran_LSB.bmp.*

Citra *udinus20seq_LSB.bmp*, yang disisipi *pesan20.txt* secara sekuensial nampak terlihat pola teratur pada bagian atas gambar. Pesan sebesar 12 KB atau 12.288 *byte* tersebut secara urut disisipkan dari piksel pertama index (0,0) sampai piksel ke-32.000 pada citra. Sedangkan pada *udinus20ran_LSB.bmp* tak menampakkan adanya pola seperti

gambar sebelumnya. Hal ini disebabkan karena *pesan20.txt* yang disisipkan secara acak terletak pada bit-bit LSB yang tidak urut. Tidak adanya pola teratur yang nampak pada *udinus20ran_LSB.bmp*, akan mengurangi kecurigaan manusia terhadap adanya pesan yang disisipkan

Percobaan yang dilakukan dengan menyisipkan *pesan30.txt*, juga menampakkan hasil yang hampir serupa pada percobaan sebelumnya. Citra *udinus30seq_LSB.bmp* manampakkan adanya pola tertentu pada sebagian gambar bagian atas. Pesan sebesar 18 KB tersebut disisipkan dari piksel pertama index (0,0) sampai piksel ke-48.000. Sedangkan penggunaan kata kunci secret pada penyisipan secara acak, membuat bit-bit *pesan30.txt* tersebar tidak berurutan.

Dengan menggunakan *pesan40.txt*, penyisipan dilakukan melalui dua cara. Pada penyisipan secara sekuensial, pesan sebesar 24 KB tersebut disisipkan dari piksel pertama index (0,0) sampai piksel ke-64.000. Pola pada *udinus40seq_LSB.bmp* yang nampak terlihat menjadi lebih terlihat dari percobaan sebelumnya. Dengan menggunakan kata kunci secret yang sama, bit-bit *pesan40.txt* diletakkan secara acak sehingga tidak membentuk pola pada *udinus40ran_LSB.bmp*.

Percobaan terakhir dilakukan dengan menggunakan *pesan50.txt* sebesar 30 KB. Penyisipan secara sekuensial menyebabkan LSB piksel pertama dengan indeks (0,0) sampai dengan piksel ke-80.000 berisi pesan tersebut. Pola yang nampak pada *udinus50seq_LSB.bmp* menutupi separuh dari citra asli, karena pesan yang disisipkan berukuran 50% dari kapasitas maksimum *udinus.bmp*. Meskipun menggunakan pesan dengan besar yang sama, penyisipan secara acak tidak membuat adanya pola yang nampak pada *udinus50ran_LSB.bmp*.

5. KESIMPULAN

Dari penelitian yang telah dilakukan, maka dapat diambil kesimpulan bahwa nilai PSNR dari *stegoimage* dengan penyisipan pesan steganografi metode LSB secara *random* (acak) lebih tinggi dibandingkan penyisipan pesan secara sekuensial (berurutan).

Gambar *Enhanced LSB* yang dihasilkan dari *stegoimage* dengan penyisipan secara sekuensial menunjukkan pola teratur pada citra. Sedangkan pada gambar *Enhanced LSB* dari *stegoimage* yang dihasilkan dengan penyisipan secara *random*, pola tersebut tidak tampak.

Munculnya pola tertentu pada gambar *Enhanced LSB* memudahkan mata manusia untuk menangkap adanya pesan yang disembunyikan pada suatu citra. Dengan nilai PSNR lebih tinggi dan tidak munculnya pola tertentu pada gambar *Enhanced LSB*, dapat dikatakan bahwa kemampuan penyisipan pesan pada metode steganografi LSB secara *random* (acak) lebih baik daripada penyisipan secara sekuensial (berurutan).

DAFTAR PUSTAKA

[1] Hidayat, E. Y., (2009). *Analisis Steganografi Metode* Least Significant *Bit (LSB) dengan Penyisipan Sekuensial dan Acak Secara Kuantitatif dan Visual*. Laporan Tugas Akhir Fakultas

Ilmu Komputer. Universitas Dian Nuswantoro

[2] Hidayat, R., (2007). *Waspadai Pencurian Data*. http://rudihd.wordpress.com/2007/04/10/waspadai-pencurian-data/; diakses pada 12 Juli 2013

[3] Sinaga, Y. A., (2008). *Program Steganalisis Metode LSB pada Citra dengan Enhanced LSB, Uji Chi-Square, dan RS-Analysis.* Institut Teknologi Bandung

[4] Iswahyudi, (2008). *Teknik Steganografi pada Pembuatan Pesan Digital yang Dirahasiakan*. Laporan Tugas Akhir Fakultas Ilmu Komputer. Universitas Dian Nuswantoro

[5] Karima, A., (2008). *Pengukuran tingkat ketahanan (Robustness) metode LSB terhadap kontras pada steganografi*. Laporan Tugas Akhir Fakultas Ilmu Komputer. Universitas Dian Nuswantoro

[6] Supriyanto, C., (2009). *Uji ketahanan (Robustness) metode LSB terhadap brightness pada steganografi*. Laporan Tugas Akhir Fakultas Ilmu Komputer. Universitas Dian Nuswantoro

[7] Munir, R., (2004a). *Diktat Kuliah IF5054 Kriptografi: Steganografi dan Watermarking*. Institut Teknologi Bandung.