Studi dan Analisis Mengenai Teknik Steganalisis Terhadap Pengubahan LSB Pada Gambar: *Enhanced LSB* dan *Chi-square*

Paul Gunawan Hariyanto (13504023)
Teknik Informatika ITB, Bandung 40132, e-mail: if14023@students.if.itb.ac.id

Abstract – *Pemakaian ilmu steganografi pada media gambar sampai saat ini masih terus berkembang, dan belum ditemukan algoritma yang benar-benar kuat yang dapat menghindarkan terdeteksinya pesan rahasia yang disembunyikan. Hal ini dikarenakan untuk tiap algoritma steganografi yang dibuat, terdapat juga teknik steganalisis yang secara spesifik dikembangkan untuk melawan algoritma tersebut. Makalah ini khusus membahas teknik steganalisis pada gambar bitmap 24-bit yang memakai algoritma pengubahan LSB (Least Significant Bit) gambar, yang merupakan algoritma yang paling sederhana dalam steganografi pada media gambar. Jenis steganalisis yang dibahas adalah secara visualisasi (visual attack) dan secara statistic (statistical attack).*

Kata Kunci*: steganografi, steganalisis, pengubahan LSB, gambar.*

1. PENDAHULUAN

Sebelum masuk ke pokok permasalahan, berikut akan dijelaskan mengenai bagaimana file gambar *bitmap*, LSB, dan steganografi dengan pengubahan LSB.

1.1. Format gambar *bitmap*

Pada jenis gambar *bitmap*, informasi gambar disimpan secara utuh dan tidak mengalami kompresi apapun. Di awal file, terdapat *header* yang merupakan informasi umum seperti besar ukuran file, jumlah bit yang dipakai pada tiap *pixel*, serta panjang dan lebar gambar tersebut. Setelah itu, warna untuk masing-masing titik (*pixel*) ditampilkan berurut dari bawah kanan ke kiri atas, dan untuk tiap *pixel*-nya mengandung sejumlah bit yang berupa besarnya kandungan warna dasar merah (*Red/R*), hijau (*Green/G*), dan biru (*Blue/B*).

1.2. LSB (*Least Significant Bit*)

LSB adalah bit yang memiliki porsi paling kecil dari kumpulan bit tersebut, atau dapat dianggap sebagai bit yang terletak di paling kanan. Contohnya, LSB dari 8-bit berikut adalah bit yang digarisbawahi: 1100101<u>0</u>. LSB memiliki arti penting karena perubahan nilai dari LSB tidak membawa pengaruh yang signifikan.

1.3. Steganografi dengan pengubahan LSB

Perubahan LSB pada gambar sangat sulit untuk diketahui secara kasat mata, sehingga cocok untuk menjadi media dalam steganografi. Dengan mengubah nilai-nilai LSB gambar sesuai dengan pesan rahasia yang diinginkan, mata manusia tidak akan dapat menemukan perbedaan antara gambar yang asli dengan yang sudah dimasukkan pesan [3].

Pada gambar *bitmap* 24-bit, tiap *pixel*-nya mengandung 24-bit kandungan warna atau 8-bit untuk masing-masing warna dasar (R, G, dan B), dengan kisaran nilai kandungan antara 0 (00000000) sampai 255 (11111111) untuk tiap warna. Perubahan LSB ini pada gambar jenis ini hanya akan merubah 1 nilai dari 256 nilai, sehingga gambar hasil steganografi akan sulit dibedakan dengan gambar yang asli.

Kapasitas maksimum pesan yang dapat ditampung adalah *panjang gambar x lebar gambar x 3 bit* (1). Sebagai contoh, desktop umum berukuran 1.024 *pixel* x 768 *pixel*, jadi ukuran pesan maksimum pada gambar dengan ukuran tersebut adalah 2.359.296 bit, atau sebanyak 294.912 karakter (1 karakter = 1*byte* atau 8 bit).

Ada dua jenis teknik steganografi yang dapat digunakan pada gambar *bitmap*, yaitu penyisipan pesan secara sekuensial dan secara acak. Sekuensial berarti pesan rahasia disisipkan secara berurutan dari data titik pertama yang ditemukan pada file gambar, yaitu titik pada pojok kanan bawah gambar. Sedangkan acak berarti penyisipan pesan rahasia dilakukan secara acak pada gambar, dengan umpan masukan kata kunci.

1.4. Pemakaian aplikasi, gambar, dan data

Ada beberapa aplikasi yang dipakai dalam membantu pembuatan makalah ini, begitu juga dengan gambar yang menjadi media penyimpanan pesan, serta data

yang menjadi pesan rahasia yang disembunyikan dalam gambar.

1.2.1 Aplikasi yang dipakai

Terdapat dua program berbeda yang mengaplikasikan kedua teknik diatas yang digunakan pada makalah ini, yaitu InPlainView (http://www.softpile.com/Utilities/Encryption/Download_05300_1.html) dan The Third Eye (http://cs.uic.edu/%7Espopuri/tte/tte.zip). Keduanya merupakan aplikasi gratis, dan dapat di-*download* lewat internet. Aplikasi InPlainView memakai cara sekuensial, dengan atau tanpa pemakaian kata kunci, sedangkan The Third Eye memakai cara acak yang mengharuskan pengguna memasukkan kata kunci.

Untuk menghasilkan gambar *enhanced LSB*, penulis membuat sendiri program berdasarkan algoritma yang didapat. Dan gambar grafik *chi-square* didapat dari internet [4].

1.2.2 Gambar yang dipakai

Ada dua buah gambar yang dipakai dalam analisis, yaitu gambar logo Institut Teknologi Bandung edisi lama, dan sebuah gambar fotografis acak yang didapat dari internet yang dipotong dan diperkecil. Gambar pertama mewakili analisis untuk gambar kontras tinggi, dan gambar kedua mewakili untuk gambar kontras rendah.

1.2.3 Data yang dipakai

Pesan atau data rahasia yang disembunyikan pada gambar adalah teks dari halaman web di situs http://kur2003.if.itb.ac.id, dengan berukuran 1.513 *bytes*.

2. ANALISIS

Steganalisis bertujuan untuk mengetahui apakah terdapat pesan rahasia di dalam suatu media, yang dalam makalah ini adalah citra/gambar. Dengan memenuhi tujuan tersebut, steganalisis dapat dikatakan berhasil.

Teknik steganalisis yang akan dibahas adalah secara visualisasi, yaitu dengan metode *enhanced LSB*, sebuah teknik menggambarkan sesuai dengan nilai LSB-nya saja. Sedangkan teknik kedua adalah secara statistik, yaitu metode *Chi-square*, sebuah teknik analisa jumlah frekuensi dari warna pixel yang berdekatan (Pair of Values).

Kedua metode ini dapat dipakai pada gambar yang diperiksa saat itu saja, dan tidak harus membandingkannya dengan gambar yang asli yang belum diisi pesan. Apabila pada analisis terdapat perbandingan gambar, hal itu hanya merupakan keperluan analisis pada makalah ini saja.

2.1. Steganalisis secara visualisasi

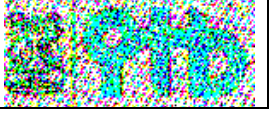
Ide yang mendasari teknik ini adalah menghilangkan seluruh bagian gambar sampai hanya terlihat bagian-bagian yang mungkin disisipi pesan, sehingga akan dihasilkan suatu gambar baru yang terlihat secara kasat mata apabila ada data lain di dalamnya. Hal ini berarti metode steganalisis secara visualisasi tetap membutuhkan bantuan manusia untuk menyelesaikan prosesnya. Metode yang dibahas adalah *enhanced LSB* [1].

2.1.1 Penjelasan gambar *enhanced LSB*

Ditemukan oleh Andreas Westfeld, yang kemudian menyatakan bahwa LSB pada suatu gambar tidaklah benar-benar acak, tetapi juga ikut menggambarkan gambar tersebut. Caranya adalah menentukan nilai dari tiap-tiap titik sesuai dengan nilai pada LSB-nya; jika LSB sama dengan 1, maka nilai seluruh bit juga dijadikan 1 (atau 255 pada desimal), dan jika nilai LSB sama dengan 0, maka nilai seluruh bit juga dijadikan 0 (atau 0 pada desimal) [1].

2.1.2 Contoh untuk gambar kontras tinggi

Tabel 1 merupakan contoh perbandingan yang gambar asli (kolom kiri) dengan *enhanced LSB*-nya (kolom kanan). Pada nomor 1, gambar masih belum disisipi pesan apapun. Sedangkan pada nomor lainnya, gambar tersebut sudah disisipi file lain dengan menggunakan kedua aplikasi di atas; cara penyisipan pada gambar nomor 2 dan 3 adalah sekuensial, dan cara penyisipan pada gambar nomor 4 adalah acak dengan masukan kata kunci.

No.	Gambar biasa	Gambar *enhanced LSB*
1		
2		
3		
4		

Tabel 1. Perbandingan antara gambar biasa dengan gambar *enhanced LSB-nya*. (1) Gambar asli, (2) Gambar tersisipi pesan dengan cara

sekuensial, (3) Gambar tersisipi pesan dengan cara sekuensial, memakai kata kunci, (4) Gambar tersisipi pesan dengan cara acak

Terlihat pada tabel di atas bahwa beberapa gambar di kolom kanan memiliki sejumlah data asing yang semestinya tidak dimiliki oleh gambar, seperti yang tertera di gambar nomor 1.

Pada gambar nomor 2 di Tabel 1 yang memakai steganografi secara sekuensial, dapat langsung diidentifikasi bahwa gambar *enhanced LSB*-nya memiliki pesan, karena mengandung suatu pola yang terletak di bawah 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/angka memiliki beberapa awalan bit yang sama, sehingga terlihat seperti membentuk pola.

Dan pada gambar nomor 3 yang menggunakan masukan kata kunci, pola tersebut masih muncul walaupun terlihat lebih acak. Hal ini disebabkan aplikasi yang dipakai pada makalah, yaitu InPlainView, menggunakan enkripsi XOR biasa antara pesan dan kata kunci yang berulang. Hasilnya adalah suatu karakter acak, sehingga gambar pola tersebut juga acak. Meskipun demikian, gambar *enhanced LSB* tetap memperlihatkan adanya data pada gambar tersebut.

Sedangkan pada gambar nomor 4 yang menggunakan steganografi secara acak, keberadaan pesan dalam gambar masih dapat terdeteksi walaupun pola tersebut lebih merata. Kata kunci dipakai sebagai masukan untuk mengacak letak bit-bit dari karakter tersebut, sehingga terlihat menyebar ke seluruh gambar.

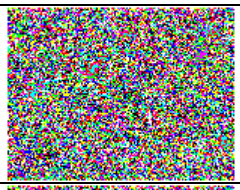
Steganalisis memakai gambar *enhanced LSB* terbilang berhasil, karena gambar steganografi secara sekuensial dan acak dapat diketahui. Akan tetapi, keberhasilan ini agaknya didukung atas tingginya kontras gambar yang dipakai. Contoh pada Tabel 1 memakai gambar yang yang memiliki warna latar yang jelas, sehingga steganalis dapat memprediksi seperti apa gambar *enhanced LSB* yang seharusnya. Untuk gambar yang nilai kontrasnya rendah, seperti gambar fotografis, teknik steganalisis dengan cara ini akan mengalami kesulitan.

2.1.3 Contoh untuk gambar kontras rendah

Contoh steganalisis dengan fotografis dapat dilihat pada Tabel 2. Gambar *enhanced LSB* pada gambar nomor 1 sudah mengalami pengacakan, walaupun gambar tersebut adalah gambar asli. Pola ini tidak berbeda dengan gambar nomor 4, yang secara kasat mata menghasilkan pola yang mirip dan tidak dapat diketahui adanya suatu pesan rahasia dalam gambar.

Sedangkan pada gambar nomor 2, yang menggunakan penyisipan secara sekuensial, pesan rahasia tersebut disisipkan dengan utuh sehingga timbul pola teratur pada bagian bawah gambar. Hal ini dapat menimbulkan kecurigaan akan adanya pesan pada gambar. Pemasukan kata kunci pada gambar nomor 3 berhasil mengaburkan pola tersebut, dan mata manusia akan sulit untuk menemukan adanya suatu pola.

Dan pada gambar nomor 4, yaitu steganografi secara acak, gambar *enhanced LSB* tidak dapat membantu menemukan suatu pola karena pesan tersebut disisipkan dengan menyebarkan bit-bit karakter ke seluruh gambar.

No.	Gambar biasa	Gambar *enhanced LSB*
1		
2		
3		
4		

Tabel 2. Perbandingan antara gambar biasa (fotografis), dengan gambar *enhanced LSB-nya*. (1) Gambar asli, (2) Gambar tersisipi pesan dengan cara sekuensial, tanpa kata kunci, (3) Gambar tersisipi pesan dengan cara sekuensial, memakai kata kunci, (4) Gambar tersisipi pesan dengan cara acak

2.2. Steganalisis secara statistik

Ide yang mendasari metode ini adalah membandingkan distribusi frekuensi pada gambar

dengan suatu contoh distribusi lain yang secara teori adalah gambar yang telah disisipi pesan. Metode yang dibahas adalah teknik *chi-square*.

2.2.1 Penjelasan mengenai *chi-square*

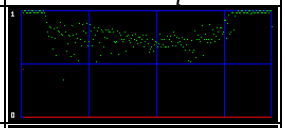
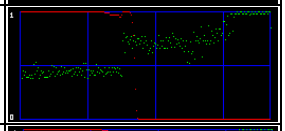
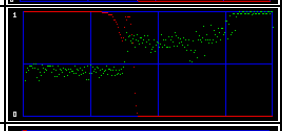
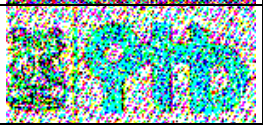
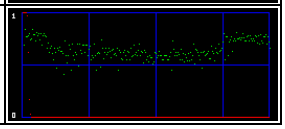
Gagasan ini juga dikemukakan oleh Andreas Westfeld, yaitu bahwa gambar yang telah disisipi pesan akan memiliki frekuensi yang relatif sama antara *Pair of Values* (PoV) yang bersangkutan [2].

PoV adalah pasangan titik yang hanya berbeda di LSB-nya saja, seperti 00000000 dan 00000001. Misalkan terdapat suatu gambar yang hanya memiliki kedua warna tersebut, dengan distribusi sebesar 70 dan 30 masing-masing titik. Setelah disisipi pesan, frekuensi tersebut akan berubah mendekati 50 dan 50, karena jumlah PoV pasti berjumlah tetap, dan jumlah dari tiap-tiap PoV akan cenderung menjadi sama.

Metode ini bekerja dengan melakukan perbandingan *chi-square* test antara dua buah statistik distribusi frekuensi, yang pertama adalah statistik pada gambar sebenarnya, dan yang kedua adalah statistik dengan PoV sama yang diprediksi akan dimiliki oleh gambar tersebut jika ada pesan yang disisipi. Apabila kedua statistik ini sama, atau terdapat suatu bagian yang sama, maka kemungkinan besar terdapat suatu pesan dalam gambar.

2.2.2 Contoh untuk gambar kontras rendah

Berikut adalah contoh *chi-square* dengan menggunakan gambar pada Tabel 1.

No.	Gambar *enhanced LSB*	Hasil *chi-square*
1		
2		
3		
4		

Tabel 3. Perbandingan antara gambar *enhanced LSB* dari Tabel 1, dengan grafik hasil *chi-square*. (1) Gambar asli, (2) Gambar tersisipi pesan dengan cara sekuensial, (3) Gambar tersisipi pesan dengan cara sekuensial, memakai kata kunci, (4) Gambar tersisipi pesan dengan cara acak

Kotak-kotak biru yang berada pada latar dalam grafik menunjukkan besarnya data gambar, yaitu 1 kotak akan menunjuk 1 *kilobyte* data, dari kiri ke kanan. Kemudian garis merah adalah hasil dari *chi-square* test; jika menunjuk angka 1 berarti terdapat kesamaan antar kedua statistik, sehingga besar kemungkinan bahwa gambar yang bersangkutan memiliki pesan tersembunyi. Terakhir, titik-titik hijau yang tersebar pada grafik adalah nilai rata-rata dari LSB. 1 kotak biru mengandung 64 titik hijau, dimana 1 titik hijau adalah rata-rata untuk 16 *bytes*. Jika titik tersebut terletak di tengah dan mendekati angka 0.5, terjadi kesamaan jumlah PoV dan mungkin terdapat pesan rahasia di dalam gambar.

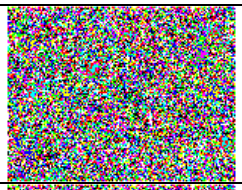
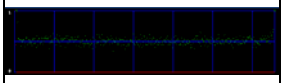
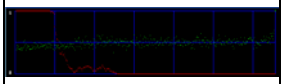
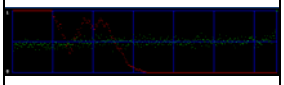
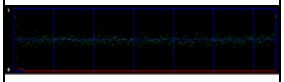
Grafik pada gambar nomor 1 Tabel 2 memperlihatkan bahwa titik-titik hijau berada di angka 1 pada sedikit bagian di awal, kemudian agak menurun selama bagian tengah gambar, kemudian kembali naik ke angka 1. Hasil itu dapat dijelaskan melalui gambar *enhanced LSB*, yaitu titik hijau yang menunjuk angka 1 pada bagian awal dan akhir grafik adalah beberapa baris bagian atas dan bawah gambar, yang hanya berwarna putih. Dan garis merah pada grafik secara konsisten berada di angka 0. Ini berarti jumlah PoV tidak relatif sama, sehingga kemungkinan tidak ada pesan pada gambar ini.

Sedangkan pada grafik di gambar nomor 2, titik-titik hijau terlihat patah setelah melalui kotak kedua; bagian pertama cenderung berkumpul di angka 0.5, dan bagian kedua menyebar di bagian atas. Garis merah juga mengikuti pola ini, yaitu bagian pertama berada pada angka 1, dan bagian kedua berada pada angka 0. Hal ini menunjukkan bahwa kemungkinan terdapat pesan yang disisipi dalam gambar, dengan ukuran sekitar 1.5 *kilobyte*.

Gambar pada nomor 3 tidak menunjukkan perubahan yang signifikan terhadap nomor 2, karena kata kunci yang dimasukkan hanya dipakai untuk melakukan operasi XOR terhadap pesan. Nilai PoV yang didapat tetap menjadi sama, dan keberadaan pesan dapat terdeteksi.

Pada gambar nomor 4, hasil *chi-square* test dapat dikatakan gagal. Grafik menunjukkan bahwa *chi-square* test menyatakan gambar tersebut mengandung pesan yang berukuran sangat kecil, atau dianggap tidak ada pesan. Kumpulan titik hijau tidak berkumpul pada garis 0.5, dan kisaran nilainya masih tersebar. Hal ini mungkin disebabkan karena steganografi secara acak ini menyebarkan bit-bit pesan, sehingga nilai PoV tidak menjadi sama pada suatu tempat melainkan menyebar.

2.2.3 Contoh untuk gambar kontras tinggi
Perhatikan Tabel 4 di bawah ini.

No.	Gambar *enhanced LSB*	Hasil *Chi-square*
1		
2		
3		
4		

Tabel 4. Perbandingan antara gambar *enhanced LSB* dari Tabel 2, dengan grafik hasil *chi-square*. (1) Gambar asli, (2) Gambar tersisipi pesan dengan cara sekuensial, (3) Gambar tersisipi pesan dengan cara sekuensial, memakai kata kunci, (4) Gambar tersisipi pesan dengan cara acak

Pada gambar nomor 1 di atas, terlihat bahwa analisis *chi-square* dapat dengan baik memeriksa gambar yang dimaksud, dimana garis merah yang menghitung kesamaan jumlah PoV dapat menunjuk ke angka 0 dari awal hingga akhir, walaupun penyebaran titik hijau sudah berada pada kisaran angka 0.5.

Untuk gambar nomor 2, hasil analisis *chi-square* menunjukkan adanya kemungkinan pesan, yang diperlihatkan oleh nilai garis merah yang berada pada angka 1 selama 1 *kilobyte* pertama, dan kemudian turun ke angka 0. Jadi, keberadaan data tersembunyi dapat terdeteksi.

Hasil yang sama ditunjukkan pada gambar nomor 3, dimana grafik juga menunjukkan adanya pesan dalam gambar. Namun panjang data yang dideteksi adalah sekitar 2 sampai 3 *kilobyte*. Berbeda dengan grafik nomor 2, yang masih dianggap akurat karena baru menyentuh angka 0 di sekitar 1.5 *kilobyte*.

Namun metode *chi-square* kembali gagal, dimana garis merah hanya menunjuk angka 0 dari awal hingga akhir data. Untuk gambar jenis ini, teknik steganalisis lagi-lagi gagal dalam mendeteksi pesan dapat disembunyikan oleh teknik steganografi secara acak.

3. HASIL DAN PEMBAHASAN

Tabel 5 dan 6 menunjukkan hasil dari analisis yang dilakukan pada bagian sebelumnya, dimana Tabel 5 menunjuk pada gambar dengan kontras tinggi, dan Tabel 6 menunjuk pada gambar dengan kontras rendah.

Jenis	*Enhanced LSB*	*Chi-square*
Sekuensial, tanpa kata kunci	Berhasil	Berhasil
Sekuensial, dengan kata kunci	Berhasil	Berhasil
Acak, dengan kata kunci	Berhasil	Gagal

Tabel 5. Ringkasan dari hasil analisa yang dilakukan untuk gambar dengan kontras tinggi

Pada Tabel 5, metode *enhanced LSB* telah berhasil mendeteksi pesan rahasia tersembunyi pada gambar dengan penyisipan data secara sekuensial maupun acak. Hal ini sangat didukung karena adanya faktor manusia yang membantu memeriksa akan adanya suatu pola asing yang muncul pada gambar *enhanced LSB*.

Metode *Chi-square* hanya berhasil pada penyisipan data secara sekuensial, dimana kesamaan jumlah PoV dapat dideteksi dengan mudah sehingga keberadaan pesan di dalamnya juga dapat diketahui. Metode ini gagal menganalisa gambar penyisipan data secara acak, karena pengubahan bit-bit dari pesan disebarkan secara merata ke seluruh gambar sehingga tidak menyamakan jumlah PoV. Inilah sebabnya kenapa hanya steganografi sekuensial yang dapat dideteksi.

Pada Tabel 6, metode *enhanced LSB* hanya berhasil mendeteksi penyisipan data secara sekuensial yang tidak menggunakan kata kunci, karena bit-bit pada karakter langsung disisipkan pada gambar sehingga gambar *enhanced LSB* akan menunjukkan pola yang teratur pada suatu bagian gambar. Sedangkan penggunaan kata kunci pada metode sekuensial akan

mengacak bit-bit tersebut, sehingga pola tersebut tidak lagi teratur dan dapat membaur dengan gambar aslinya.

Jenis	*Enhanced LSB*	*Chi-square*
Sekuensial, tanpa kata kunci	Berhasil	Berhasil
Sekuensial, dengan kata kunci	Gagal	Berhasil
Acak, dengan kata kunci	Gagal	Gagal

Tabel 6. Ringkasan dari hasil analisa yang dilakukan untuk gambar dengan kontras rendah

Namun metode *chi-square* dapat mendeteksi pesan pada penyisipan pesan sekuensial dengan kata kunci, karena jumlah PoV yang dihasilkan masih menjadi relatif sama walaupun bit-bit yang disisipkan diacak terlebih dahulu.

Tetapi pada penyisipan data secara acak, bit-bit pesan tidak lagi disisipkan pada suatu bagian tertentu, melainkan menyebarkan bit demi bit pada seluruh bagian gambar sehingga sehingga hampir tidak mungkin dapat dibedakan oleh mata manusia. Kedua metode tidak dapat mendeteksi keberadaan pesan dengan steganografi acak ini.

4. KESIMPULAN

Kesimpulan yang didapat pada studi ini antara lain:

1. Steganalisis dengan metode *enhanced LSB* maupun metode *chi-square*, dapat dengan mudah mendeteksi pesan pada gambar steganografi dengan penyisipan data secara sekuensial.

2. Pemilihan metode steganalisis dipengaruhi juga oleh tinggi/rendahnya kekontrasan gambar yang ingin diperiksa; metode *enhanced LSB* lebih berhasil digunakan pada gambar dengan kontras tinggi daripada metode *chi-square*, sedangkan metode *chi-square* lebih berhasil digunakan pada gambar dengan kontras rendah daripada metode *enhanced LSB*.

3. Metode steganalisis *enhanced LSB* dan *chi-square* sama-sama tidak dapat mendeteksi keberadaan pesan dalam gambar kontras rendah, seperti gambar fotografis.

4. Metode steganalisis *enhanced LSB* dan *chi-square* tidak membutuhkan gambar asli pada saat proses.

DAFTAR REFERENSI

[1] A. Westfeld, A. Pfitzmann, “Attacks on Steganographic Systems”, Department of Computer Science - Dresden University of Technology, 2000, Dresden, Germany.

[2] R. Chandramouli, M. Kharrazi, N. Memon, Image Steganography and Steganalysis:Concepts and Practice, 2004, Berlin, pp. 41-44.

[3] R. Munir, “Kriptografi”, Sekolah Teknik Elektro dan Informatika - Institut Teknologi Bandung, Bandung, 2006.

[4] http://www.guillermito2.net/stegano/, diakses pada tanggal 22 Oktober 2007.