STUDI DAN ANALISIS TEKNIK-TEKNIK PENDETEKSIAN STEGANOGRAFI DENGAN METODE LSB DALAM MEDIA GAMBAR

Arnold Nugroho Sutanto – NIM : 13507102

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if17102@students.itb.ac.id

Abstrak

Saat ini, telah terdapat berbagai cara dalam steganografi untuk menyembunyikan informasi dalam citra digital yang walaupun dengan adanya perubahan, tidak membawa dampak yang terlihat. Salah satu teknik yang paling umum digunakan adalah penggunaan metode LSB pada citra dijital 24-bit, 8-bit citra bewarna maupun hitam putih. Perubahan pada LSB dipercaya tidak dapat terdeteksi oleh karena *noise* yang akan selalu ada pada citra dijital.

Beberapa teknik telah ditemukan untuk melakukan serangan terhadap metode LSB ini untuk mendeteksi adanya pesan rahasia dalam gambar. Dalam makalah ini, kita akan membahas 3 teknik steganalisis yang sudah ada. Teknik pertama adalah visual attack oleh Wesfield yang memerlukan bantuan indra penglihatan manusia. Teknik berikutnya adalah uji statistik chi-square yang juga dikemukakan oleh Pitzmann dan Westfeld. Teknik ini berbasiskan analisis statistik dari *Paris of Values* (PoVs) yang bertukar saat penyisipan pesan pada gambar.

Steganalisis ketiga dinamakan sebagai metode RQP yang dikemukakan oleh Federich dkk untuk mendeteksi penyisipan LSB dalam gambar berwarna 24-bit. Sebagai kesimpulan, kita akan menentukan kelebihan dan kekurangan dari masing-masing teknik dan dengan begitu kita dapat mengukur sekaligus meningkatkan tingkat keamanan metode LSB untuk penyembunyian informasi dalam media gambar.

Kata kunci : Steganografi, Citra Dijital, metode LSB, Steganalisis, *Visual Attack*, uji chi-square, metode RQP.

1. PENDAHULUAN

Steganografi merupakan ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga pesan rahasia tersebut tidak dapat diketahui[1]. Steganografi dapat dianggap sebagai saudara gelap dari kriptografi. Kriptografi berfungsi mengacak pesan sehingga tidak dapat dimengerti sedangkan steganografi menyembunyikan pesan sehingga tidak terlihat[6]. Teknologi dijital memberikan cara yang baru dalam mengaplikasikan teknik steganografi, yang salah satunya adalah penyembunyian informasi dalam citra dijital. Saat ini, banyak perangkat lunak steganografi yang menggunakan penyisipan pesan pada Least Significant Bit (LSB) sebagai metode pilihan untuk menyembunyikan pesan dalam citra dijital.

2. TERMINOLOGI

2.1. Steganografi

Permodelan umum yang biasanya digunakan untuk menggambarkan steganografi adalah cerita tentang Alice yang ingin mengirimkaan pesan rahasia *p* ke Bob. Permasalahannya, Alice membutuhkan bantuan Wendy sebagai kurir dari pesan tersebut dan Alice tidak ingin Wendy curiga akan pesan rahasia yang dikirimkan. Untuk itu, Alice menyisipkan pesan *p* kepada objek pembungkus *c* untuk mendapatkan objek hasil steganografi *s*.
Tujuan dari steganografi ini adalah agar Wendy tidak dapat membedakan antara objek pembungkus *c* (objek tanpa rahasia) dengan objek steganografi *s* (objek dengan pesan rahasia terkandung di dalamnya). Pesan rahasia yang tertanam pada objek hasil steganografi dapat berupa hasil enkripsi atau teks biasa.

2.2. Citra Dijital

Dalam dunia dijital, sebuah citra merupakan array numerik yang merepresentasikan intensitas warna pada berbagai posisi titik (pixel)[6]. Citra dijital biasanya disimpan dalam data 24-bit atau 8-bit. Semua

variasi dari warna untuk sebuah pixel berasal dari 3 warna utama : merah, hijau, dan biru. Setiap warna utama ini direpresentasikan dengan 1 byte; citra 24 bit menggunakan 3 byte untuk merepresentasikan warna dari sebuah pixel. Misal, untuk warna putih pada suatu pixel direpresentasikan dengan 100 persen merah (11111111), 100 persen biru (11111111), dan 100 persent biru (11111111). Citra 24 bit ini akan memberikan tempat yang lebih luas untuk menyembunyikan informasi.

Ada 2 buah kompresi yang dilakukan pada citra dijital, *loseless* dan *lossly*[6]. Kompresi *lossless* memperbolehkan kita untuk melakukan rekonstruksi dari byte-byte pixel sebagai mana mestinya (tidak ada pengubahan). Contoh dari citra dengan kompresi *loseless* adalah GIF dan 8-bit BMP. Di lain pihak. kompresi *lossly* tidak mempertahakan keaslian integritas citra yang seharusnya sehingga hasil kompresinya hanya merupakan pendekatan dari citra tersebut. Hasil kompresi ini tentu saja dapat merusak pesan yang tersisipkan (misal JPEG).

Citra dijital yang paling baik digunakan adalah citra yang memiliki kapasitas luas untuk menyembunyikan informasi tetapi tetap menjaga integritas citra agar tidak merusak isi pesan yang ditanamkan. Oleh karena itu, citra yang sebaiknya dipilih adalah citra 24 bit dengan kompresi *loseless*.

2.3. Metode LSB

Penyisipan pada *least significant bit* meupakan pendekatan yang umum dan sederhana untuk menanamkan informasi pada file pembungkus. *Least significant bit* merupakan bit yang paling tidak berarti dalam suatu byte (misal 1000110**1**, LSB nya adalah **1**). Metode LSB akan mengganti LSB dari byte-byte pixel dalam citra dengan informasi yang ingin ditanamkan. Oleh karena citra merupakan salah satu objek multimedia yang sering memiliki representasi yang redundan, pengubahan LSB dari pixel-pixel ini tidak akan memperlihatkan degadrasi yang terlihat kasat mata.

Terdapat banyak teknik yang telah dibuat berdasarkan pada steganografi dengan metode LSB. Contoh dari teknik-teknik yang ada adalah *EzStego*, *S-Tools* dan *Steganos*[2]. Secara garis besar, teknik-teknik ini dapat kita kelompokkan sesuai dengan penyebaran penempatan pesan pada citra. Cara pertama adalah dengan penempatan secara teratur (mis. Sekuensial) seperti yang dilakukan oleh *EzStego* dan *Steganos*. Cara kedua, pesan disebarkan secara random pada pixel-pixel citra. Dengan cara kedua, kunci steganografi dibutuhkan sebagai *seed* untuk menghasilkan angka-angka acak sebagai posisi pixel tempat pesan disimpan.

2.4. Steganalisis

Steganalisis dibuat untuk menggagalkan tujuan utama dari steganografi untuk menyembunyikan informasi. Steganalisis merupakan seni dan ilmu untuk mendeteksi adanya informasi yang disembunyikan dalam suatu objek stego[4].

Steganalisis untuk metode LSB terdiri dari metode subjektif dan metode statistik. Metode subjektif memerlukan bantuan penglihatan manusia untuk menentukan bagian gambar yang dicurigai, oleh karena itu metode ini sering disebut sebagai Visual Attack. Metode statistik melakukan perhitungan matematis untuk menemukan properti dari gambar asli yang membedakan dengan gambar yang telah disisipi pesan. Meskipun secara kasat mata terlihat sama, citra hasil steganografi LSB memiliki perbedaan statistik properti yang cukup kuat dengan citra aslinya. Berikut akan dijelaskan 3 teknik yang telah dikemukakan.

3. STEGANALISIS METODE LSB

3.1. Visual Attack

3.1.1. Keacakan LSB dari suatu citra

Terdapat asumsi umum yang mengatakan bahwa bit LSB pada citra dijital bersifat acak sehingga dapat dengan bebas dapat digantikan. Westfield dalam [2] memperlihatkan bahwa asumsi ini salah. Mesin memang tidak mungkin bisa membedakan antara bit yang acak dengan LSB dari suatu citra. Oleh karena itu, sebagai gantinya, dibutuhkan indra manusia untuk membedakan suatu konten dari suatu citra yang menjadi samar karena hanya berdasarkan LSB dari pixel-pixel nya. Berikut adalah contoh citra yang ditampilkan dalam untuk memperlihatkan ketidak acakan LSB.

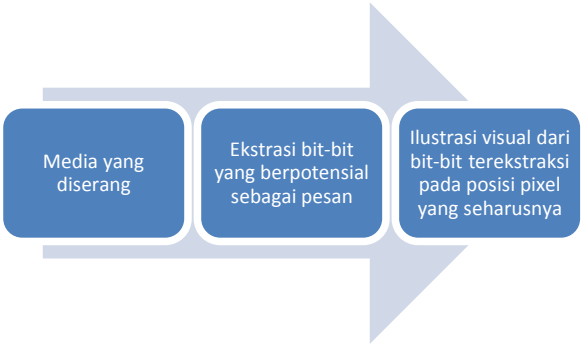
Gambar 1 Citra Asli Tanpa Pengubahan [2]

Gambar 2 LSB dari Gambar 1 dengan 0 disimbolkan hitam dan 1 disimbolkan putih [2]

Oleh karena LSB dapat menggambarkan isi dari citra, pengubahan LSB akan mengakibatkan kerusakan yang dapat dilihat oleh indra penglihatan manusia dengan membuang bagian dari citra yang digunakan untuk membungkus suatu pesan rahasia.

Struktur Algoritma dari Visual Attacks

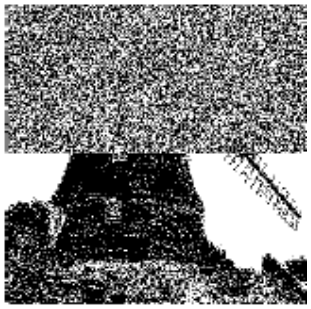
Ide dasar dari visual attack adalah melakukan penyaringan terhadap bagian dari bit-bit dari byte pixel yang digunakan untuk menyembunyikan pesan. Proses penyaringan untuk mendapatkan bit-bit dari persan tertanam bergantung pada teknik steganografi yang dilakukan. Secara umum, visual attack pada suatu citra akan mengikuti struktur seperti berikut[2]:



Gambar 3 Struktur Teknik Steganografi Visual Attack

Proses pengekstraksian bit-bit yang berpotensi disesuaikan dengan fungsi penanaman yang dilakukan pada bit-bit tersebut. Misal, EzStego menggunakan warna dari pixel, terdefinisikan oleh palet, untuk menentukan bit yang tertanam. Bit-bit hasil ekstraksi ini kemudian direpresentasikan secara visual untuk dapat menentukan ada tidaknya pesan rahasia dengan bantuan mata manusia. Berikut adalah contoh hasil penyaringan image dalam :

Gambar 4 Hasil ekstraksi dari citra yang tidak disisipi pesan [2]



Gambar 5 Hasil ekstraksi dari citra yang disisipi pesan 50% menggunakan EzStego [2]

Gambar di atas adalah contoh dari penempatan penanaman informasi secara sekuensial yang dilakukan oleh EzStego. Pada penyisipan informasi secara acakpun, visual attack dapat digunakan. Hanya saja, panjang pesan berpengaruh pada besarnya kerusakan gambar. Jika panjang pesan terlalu kecil dan penyisipan LSB nya acak, maka kerusakan gambar menjadi hampir tidak terlihat.

3.2. Metode RQP

Fridrich dalam [3] mengemukakan penanaman pesan pada suatu citra tidak akan memperlihatkan properti yang rusak jika total warna yang ada hampir sama dengan jumlah piksel yang ada pada citra. Akan tetapi, setelah melakukan berbagai observasi, Fridrich menemukan bahwa jumlah warna yang ada pada citra true-color (hasil dari scanning dan kamera dijital) biasanya jauh lebih kecil daripada jumpah piksel pada citra tersebut. Rasio dari jumlah warna dan jumlah piksel diperkirakan sekitar 1:2 untuk hasil scan berkualitas tinggi sampai 1:6 untuk gambar JPEG atau hasil rekaman video.

Hasil observasi ini sangat penting karena dengan begitu berarti banyak citra memiliki palet yang relatif kecil. Setelah penyisipan dengan LSB, palet yang baru akan memiliki fitur yang membedakan, akan terdapat banyak pasangan dari warna yang sangat berdekatan. Adanya banyak pasangan warna yang

berdekatan adalah indikasi dari penggunaan LSB untuk steganografi pada citra tersebut.

Ide ini sebenarnya sudah dikenalkan oleh Johnson dan Jajodia [6]. Akan tetapi, sifat ini dianggap hanya dapat diaplikasikan hanya pada citra yang menggunakan palet yang kecil seperti GIF dan PNG yang memiliki 256 warna maksimumnya. Metode RQP ini memungkinkan penggunaan ide yang sama untuk melakukan serangan terhadap citra true-color dengan ukuran palet yang besar.

Konsep

Metode RQP mengajukan pengujian adanya pesan rahasia pada citra 24-bit dengan ide sebagai berikut[3]. Kita andaikan banyaknya warna dalam sebuah citra sebagai U sedangkan P adalah jumlah pasangan warna yang berdekatan yang merupakan himpunan bagian dari U. Kita dapat mengatakan bahwa 2 warna dekat jika $|R1-R2| \leq 1, |G1-G2| \leq 1$, dan $|B1-B2| \leq 1$. Persamaan ini menghasilkan $(R1-R2)2+(G1-G2)2+(B1-B2)2 \leq 3$. Total pasangan warna yang ada :

$$\binom{U}{2} \geq P.$$

Persamaan 1 Perbandingan nilai P dan U [3]

Maka rasio antara pasangan warna terdekat dengan total pasangan warna:

$$R = \frac{P}{\binom{U}{2}},$$

Persamaan 2 Perhitungan nilai Rasio (R) [3]

Penanaman pesan pada suatu citra, akan meningkatkan nilai R (nilai P meningkat lebih besar dari nilai U). Permasalahan yang terjadi adalah, kita tidak dapat mendapat nilai R yang seharusnya dari suatu citra (oleh karena variasi nilai U) sebagai acuan untuk mengetahui ada tidaknya pesan yang disisipkan.

Setelah melakukan observasi, Fridrich menemukan bahwa suatu citra yang tidak dilakukan metode LSB, kemudian dilakukan penyisipan pesan dengan metode ini, akan mengalami peningkatan nilai R secara signifikan. Berbeda dengan citra yang merupakan stego-object hasil kriptografi LSB, citra ini tidak mengalami perubahan nilai R setelah dicoba disisipkan pesan tertanam.

Oleh karena hal ini, Fridrich mengemukakan untuk melakukan perbandingan peningkatan nilai R yang terjadi setelah citra dilakukan metode LSB. Langkah pendeteksiannya :

1. Hitung nilai R awal dari citra yang akan diuji.
2. Lakukan penyisipan LSB dengan pemilihan pixel secara acak
3. Lakukan perhitungan nilai P' dan U' untuk mendapatkan nilai R' yang baru dari citra yang sudah disisipi.

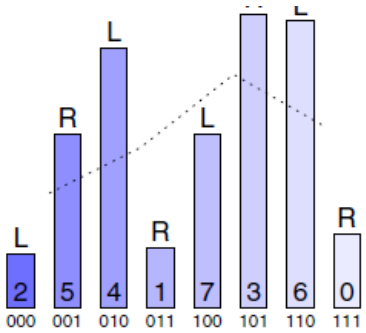
Jika suatu citra memiliki pesan rahasia berukuran cukup besar di dalamnya, maka akan diharapkan R bernilai hampir sama dengan R'. Jika citra tersebut tidak dilakukan pengubahan LSB maka diharapkan nilai R'>R.

3.3. Uji Chi-Square

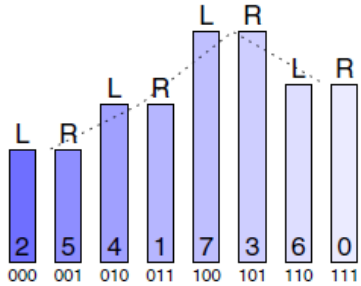
Penggantian least significant bit hanya akan mengubah nilai dari suatu warna menjadi suatu warna lain yang hanya berbeda pada LSB nya. Misal, pada byte 10010011, penggantian LSB hanya akan mengubahnya menjadi 2 nilai yaitu 10010011 dan 10010010. Pasangan nilai yang hanya berbeda pada LSB nya inilah yang disebut *Pair of Values* (PoVs). Frekuensi dari setiap nilai PoV ini akan cenderung sama jika bit yang digunakan untuk menggantikan bit LSB didistribusikan secara merata[2]. Hal ini inilah yang akan menjadi dasar untuk melakukan pendeteksian stego-image.

Hal yang penting adalah mendapatkan frekuensi yang diharapkan secara teori setelah dilakukan perubahan steganografi pada citra. Frekuensi ini tentu saja tidak dapat diambil dari citra yang akan diuji, karena mungkin citra tersebut sudah dilakukan perubahan dengan operasi steganografi.

Secara teori, frekuensi distribusi yang diharapkan adalah rata-rata dari 2 frekuensi dalam sebuah PoV. Hal ini dapat disimpulkan karena pengubahan LSB hanya akan menambah salah satu nilai dari PoV dan mengurangi nilai lain dalam PoV tersebut. Oleh karena itu, jumlah dari frekuensi dalam suatu PoV akan selalu sama, baik sebelum atau sesudah ditanami pesan rahasia.



Gambar 6 Frekuensi masing-masing PoVs pada citra asli [2]



Gambar 7 Frekuensi masing-masing PoVs pada *stego-image*[2]

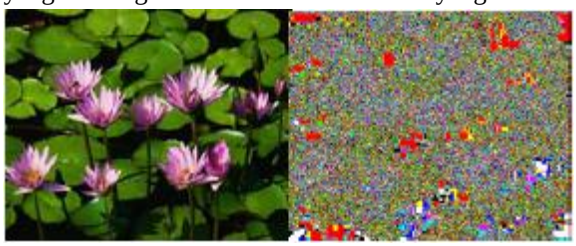
Derajat kesamaan antara frekuensi distribusi pada citra yang diuji dengan frekuensi yang diharapkan secara teori (rata-rata dari jumlah 2 frekuensi dalam satu PoV) merupakan pengukur dari probabilitas terjadinya penyisipan pesan.

4. ANALISIS

4.1. Analisis Visual Attack

Visual Attack yang dikemukakan oleh Westfeld mempunyai 1 asumsi yang krusial, yaitu bahwa LSB dari citra yang diserang tidaklah acak tetapi membentuk suatu pola yang samar-samar dari gambar yang dibentuknya. Asumsi ini krusial karena hal ini menjadi dasar dari teknik visual attack. Jika suatu citra ternyata memiliki LSB yang acak, maka Visual Attack tidak dapat diterapkan.

Keacakan dari LSB ditentukan oleh kontras dari latar belakang dengan gambar utamanya[4]. Gambar yang memiliki nilai kontras rendah tidak bisa diserang dengan teknik steganalisis ini. Citra hasil kamera dijital atau hasil scanning merupakan contoh citra yang kemungkinan besar memiliki LSB yang acak.



Gambar 8 Citra dengan kontras yang tinggi (R), Hasil enhanced LSB (salah satu teknik Visual Attack) (L) [4]

Teknik steganalisis ini juga membutuhkan indra penglihatan manusia untuk mendeteksi ada tidaknya pesan tertanam sehingga pendeteksian tidak dapat dilakukan secara otomatis. Otomatisasi ini penting karena citra pada zaman modern ini yang harus ditelusuri sangatlah banyak untuk dapat menemukan citra yang benar-benar disisipi pesan rahasia.

4.2. Analisis metode RQP

Asumsi yang digunakan oleh metode RQP adalah jumlah warna dari suatu citra, jauh lebih kecil daripada jumlah pixelnya. Asumsi ini tampaknya tidak bisa diterapkan pada semua citra. Fridrich mengatakan dalam makalah terbarunya[newest], bahwa metode RQP hanya bisa diterapkan pada citra yang memiliki jumlah warna kurang dari 30% dari jumlah pixel. Metode ini juga tidak dapat diterapkan pada citra hitam-putih.

Anggapan bahwa scanner dan kamera dijital menghasilkan citra yang memiliki rasio perbandingan jumlah warna dan jumlah pixel yang kecil, tampaknya semakin tidak berlaku. Perkembangan teknologi dalam dunia dijital menghasilkan warna yang semakin detail sehingga jumlah warna yang dihasilkan semakin sebanding dengan jumlah pixel dari citra tersebut.

Metode ini akan sangat cocok digunakan untuk media citra yang dikompresi secara *lossly*(mis. JPEG). Kompresi lossly akan mengurangi jumlah warna yang unik untuk mendapatkan citra dengan ukuran yang lebih kecil.

4.2. Analisis metode uji chi square

Batasan yang dimiliki oleh uji chi square adalah bahwa metode ini mengasumsikan pesan disebarkan secara merata pada citra (mis. Sekuensial). Padahal, seperti yang telah diketahui, metode LSB yang telah diterapkan melakukan dapat melakukan pemilihan pixel yang disisipinya baik secara teratur (mis. EzStego) atau acak (mis. S-Tools). Oleh karena hal ini, uji chi square yang diterapkan untuk citra yang telah disisipi menggunakan teknik LSB dengan pemilihan pixel acak memberikan hasil deteksi yang kurang dapat dipercaya tergantung pada rasio panjang pesan yang disisipkan dan kapasitas citra. Jika lebih dari 50% dari LSB citra dirusak, meskipun dengan teknik LSB acak, uji chi square akan memberikan hasil deteksi yang dapat dihandalkan.

4.3. Analisis kualitas citra sebagai objek pembungkus

Berdasarkan analisis yang telah dilakukan terhadap ketiga teknik steganalisis yang telah disebutkan, kita dapat menyimpulkan sifat dari suatu citra yang baik sebagai objek pembungkus (memiliki sekuritas tinggi untuk menyembunyikan pesan yang ditanamkan). Berikut adalah keempat sifat yang harus dimiliki suatu citra :

1. Memiliki kontras yang tinggi antara gambar utama dengan latar belakang
   Sifat ini dimiliki untuk menanggulangi serangan secara visual attack.

2. Merupakan hasil dari pengambilan citra dengan kamera dijital/scanner
   Hal ini dimaksudkan agar didapatkan suatu citra yang memiliki LSB yang benar-benar acak.
3. Memiliki jumlah warna unik yang sebanding dengan jumlah pixelnya.
   Setidaknya suatu citra memiliki jumlah warna lebih dari 50% dari jumlah pixelnya. Hal ini dilakukan untuk menanggulangi serangan metode RQP.
4. Penyisipan pesan pada citra sebaiknya menggunakan teknik pemilihan pixel acak.
   Penggunaan perangkat lunak seperti S-Tools yang melakukan penempatan pesan secara acak lebih direkomendasikan daripada EzStego (sekuensial).

Pesan yang ditanamkan pada citra juga sebaiknya tidak melebihi batas kapasitas maksimum yang dimiliki citra tersebut (agar tidak mudah terdeteksi). Chandramouli and Memon [8] melakukan anilisis dari steganografi LSB dan menemukan persamaan dari batas atas kapasitas maksimum untuk penyisipan LSB secara umum agar tidak terdeteksi.

4.4. Studi perbandingan dengan metode steganalisis lainnya

Pada [5], Fridrich dkk mengemukakan metode RS yang lebih mangkus dari metode RQP. Metode RS ini dikatakan sanggup untuk mendeteksi pesan yang pendek dan ditanamkan secara acak, tersebar pada citra. Avcibas, Memon dan Sankur [9] memberikan sebuah teknik umum dari steganalysis untu citra yang bekerja pada berbagai variasi teknik penyisipan, tidak terbatas pada metode LSB.

Dari studi banding ini, kita dapat katakan bahwa ketiga teknik steganalisis yang telah dibahas sebelumnya bukanlah teknik yang paling mangkus yang ada sekarang. Oleh karena itu, meskipun kita telah memilih teknik penyisipan LSB dan pemilihan citra yang dapat bertahan terhadap serangan-serangan yang telah dibahas sebelumnya, pendeteksian dengan teknik steganalisis lainnya masih sangat dimungkinkan.

5. KESIMPULAN

Ketiga steganalisis yang telah dibahas memiliki kelemahan masing-masing yang dapat membuat *stego-image* dapat bertahan terhadap serangan. Visual Attack yang dikemukakan Westfield tidak dapat mendeteksi pesan tertanam pada citra dengan kontras rendah atau dengan LSB yang acak.

Keakurasian pendeteksian metode RQP sangat bergantung pada rasio jumlah warna dengan jumlah pixelnya. Rasio maksimum yang dapat dideteksi oleh metode ini adalah saat jumlah warna pada citra tidak melebihi 30% dari jumlah pixelnya.

Uji Chi Square memiliki kemampuan mendeteksi pesan rahasia jika pesan tersebut disisipkan secara merata pada citra. Metode ini dapat mendeteksi penyisipan pesan acak hanya jika panjang dari pesan sebanding dengan jumlah pixel dari citra (merusak lebih besar dari 50% pixel citra). Berdasarkan kelemahan-kelemahan ini, kita dapat melakukan pemilihan terhadap citra pembungkus, teknik penyisipan LSB, dan panjang maksimum pesan, agar dapat bertahan dari serangan ketiga teknik ini.

Ada beberapa steganalisis lain yang telah dikembangkan dan memberikan solusi yang lebih mangkus dari ketiga teknik ini. Meskipun begitu, penggunaan metode LSB pada media citra dalam steganografi masih merupakan salah satu cara yang handal. Hal ini dikarenakan jumlah citra yang sangat banyak dan tersebar pada jaringan internet (sebagai sarana penyimpanan) sehingga akan sangat sulit untuk menemukan setgo-image dari sebegitu banyak citra yang ada.

SUMBER REFERENSI

[1] Munir, Rinaldi. (2006). Diktat Kuliah IF5054 Kriptografi.

[2] A. Westfeld and A. Pfitzmann, (1999) "Attacks on Steganographic Systems", *Proc. 3rd Information Hiding Workshop*, Dresden, Germany.

[3] J. Fridrich, R. Du, and L. Meng, (2000) “Steganalysis of LSB Encoding in Color Images”, *ICME 2000*, New York City.

[4] Anneria, Yulia (2008) “Program Steganalisis Metode LSB pada Citra dengan Enhanced LSB, Uji Chi-Square, dan RS-Analysis”

[5] J. Fridrich, M. Goljan and R. Dui, (2001) ”Reliable Detection of LSB steganography in Color and Grayscale Images,” *Proc. of the ACM Workshop on Multimedia and Security*.

[6] N. F. Johnson and S. Jajodia,(1998) “Steganalysis of Images Created Using Current Steganography Software.” *Proc. 2nd Information Hiding Workshop*, Portland, OR, April 1998.

[7] Johnson, Neil F. and Jajodia, Sushil. (1998) “Steganography: Seeing the Unseen.” *IEEE Computer*.

[8] R. Chandramouli and N. Memon, (2001) ”Analysis of LSB Based Image Steganography Techniques.”

[9] I. Avcibas, N. Memon and B. Sankur, (2001) ”Steganalysis Using Image Quality Metrics