STUDI METODE STEGANALISIS PADA *STEGOIMAGE*

Yosep Kurniawan – NIM : 13503059
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if13059@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang studi metode steganalisis. Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tidak dapat diketahui. Steganalisis adalah ilmu dan seni menemukan informasi yang tersembunyi pada pesan lain. *Stegoimage* adalah citra yang sudah berisi informasi yang disembunyikan. Dalam steganografi terdapat tiga kriteria yang perlu diperhatikan dalam memilih citra pelindung (*cover-image*) informasi dan metode untuk menyembunyikannya, yaitu *imperceptibility*: tidak dapat dipersepsi oleh indera manusia, *fidelity*: kualitas *cover-object* tidak jauh berubah akibat *embedded*, dan *recovery*: informasi yang disembunyikan harus dapat diungkapkan kembali. *Stegoimage* dapat dibentuk dengan menggunakan metode steganografi seperti LSB (*Least Significant Bit*) dan DCT (*Discrete Cosine Transform*).

Metode LSB dan DCT ini masing-masing memiliki kelebihan dan kekurangan. Pada metode LSB, *stegoimage* dapat dibentuk dengan mudah dan cepat namun *stegoimage* yang terbentuk tidak tahan terhadap perubahan dan informasi yang terdapat di dalamnya mudah terhapus atau diubah. Sedangkan pada metode DCT, *stegoimage* tahan terhadap perubahan, informasi yang disisipkan pun tidak mudah terhapus atau diubah, namun pembentukan *stegoimage*nya membutuhkan usaha yang lebih besar.

Pengertian steganalisis mengacu pada seni dan ilmu pengetahuan dalam membedakan antara *stego-object* dan *cover-object*. Dua metode steganalisis terhadap *stego-object* menggunakan metode LSB yang terkenal adalah steganalisis PoV (*Pair of Values*) yang dikenalkan oleh Westfeld dan Pfitzmann dan steganalisis RS (*Regular* dan *Singular*) yang dikenalkan oleh Fridrich. Selain itu, Farid dan Avcibas beserta kawan-kawannya mengusulkan metode steganalisis universal yang mampu medeteksi berbagai algoritma steganografi. Secara umum, terdapat beberapa metode steganalisis yang terkenal, yaitu steganalisis RS, PoV berbasis uji coba *Chi-Square*, *palette checking*, metode RQP, memeriksa kompatibilitas JPEG, analisis histogram, dan *universal blind detection.*

Kata kunci: steganografi, steganalisis, *stegoimage*, LSB, DCT, RS, PoV, analisis histogram, RQP.

1. Pendahuluan

Kriptografi mempunyai sejarah yang panjang. Bangsa Mesir 4000 tahun yang lalu telah menggunakan *hyroglyph* yang tidak standard. Namun kata *cryptography* sendiri berasal dari bahasa Yunani, yaitu κρυπτο (*hidden* atau *secret*) dan γραφη (*writing*), artinya *secret writing*. Kriptografi (definisi lama) adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi (definisi baru) adalah ilmu sekaligus seni untuk menjaga keamanan pesan (message) [Schneier, 1996]

Steganografi berasalah dari bahasa Yunani yaitu *steganos* yang artinya "*covered writing*" atau tulisan tersembunyi. Steganografi adalah ilmu dan seni menyembunyikan (*embedded*) informasi dengan cara menyisipkan pesan di dalam pesan lain.

Steganografi juga memiliki usia yang hampir sama dengan usia kriptografi. Steganografi telah dikenal oleh bangsa Yunani sejak Herodotus, seorang penguasa Yunani, mengirimkan pesan rahasia menggunakan kepala budak atau prajurit.

Steganografi terbagi menjadi beberapa zaman, yaitu ancient, renaissance, dan modern.

a. Ancient steganografi
   Ancient steganografi telah dikenal sejak zaman Herodotus (485-582 SM).
   Kemudian Pliny *the Elder* dengan *invisible ink* –nya.

b. Renaissance steganografi
   Renaissance steganografi dimulai sejak tahun 1518 oleh Johannes Trithemius yang menemukan cipher steganografi pada setiap huruf yang merepresentasikan sebuah kata. Tokoh lainnya yaitu Giovanni Battista Porta (1535-1615) yang menggunakan kulit telur sebagai *cover*

object dan pesan yang ditulis dapat dibaca setelah kulit telur dilepaskan.

c. Modern steganografi
Modern steganografi oleh Simmons pada tahun 1983 di USA.

Steganografi juga banyak digunakan pada negara-negara yang menerapkan sensor ketat terhadap informasi atau di negara di mana enkripsi pesan terlarang. [5]

Jika penggunaan kriptografi memunculkan kecurigaan orang ketiga terhadap pesan yang dikirimkan, maka dengan menggunakan steganografi kecurigaan ini menjadi tidak ada. Orang ketiga akan menganggap bahwa pesan yang dikirimkan tidak mengandung makna apa-apa. Hingga akhirnya pesan itu sampai pada orang yang dituju, maka pesan rahasia yang terdapat di dalamnya itu baru dapat diketahui.

Pada steganografi, rasa curiga itu ditekan sedemikian sehingga orang yang tidak berkepentingan tidak akan mengetahui keberadaan pesan rahasia dari pesan tersebut. Berbeda halnya pada kriptografi, pesan dienkripsi sedemikian sehingga pesan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Orang yang tidak berkepentingan ini harus memecahkan kunci dan algoritma yang digunakan untuk mengenkripsi pesan tersebut jika ia ingin mengetahui isi pesan tersebut.

Seni untuk menemukan ada atau tidaknya pesan rahasia dalam suatu pesan disebut dengan steganalisis. Steganalisis dapat dilakukan terhadap pesan berupa plainteks, suara, gambar, video, dan media digital lainnya. Steganalisis memiliki beragam tujuan, seperti steganalisis untuk mengetahui pesan rahasia yang disembunyikan, steganalisis untuk mengetahui ada atau tidaknya pesan, steganalisis untuk menguji kehandalan algoritma steganografi. Selain itu, ada juga serangan terhadap steganografi yang bertujuan untuk menghancurkan pesan rahasia yang tersembunyi dalam pesan.

Dalam dunia kriptografi, metode steganalisis memiliki peranan yang kurang lebih sama dengan metode kriptanalisis. Steganalisis dapat digunakan untuk menguji suatu algoritma steganografi, apakah algoritma tersebut handal atau tidak. Selain itu, steganalisis juga dapat digunakan oleh penjaga penjara untuk mendeteksi adanya pesan rahasia atau tidak dalam suatu pesan yang dikirimkan oleh tahanan.

2. Terminologi

a. *Embedded message(hiddentext)*: pesan yang disembunyikan

b. *Cover-object(covertext)*: pesan yang digunakan untuk menyembunyikan *embedded message*.

c. *Stego-object (stegotext)*: pesan yang sudah berisi pesan *embedded message*.

d. *Stego-key*: kunci yang digunakan untuk menyisipkan pesan dan mengekstraksi pesan dari *stegotext*.

e. *Steganografer*: orang yang merancang metode steganografi.

f. *Steganalyst*: orang yang berusahan untuk memecahkan metode steganografi dengan menggunakan berbagai metode steganalisis.

3. Metode Steganografi

Terdapat banyak metode untuk menyembunyikan informasi dalam suatu citra. Metode ini beragam dari LSB (*Least Significant Bit*) atau metode penyisipan *noise*, algoritma manipulasi citra dan kompresi, dan pengubahan properti citra seperti *luminance*. Teknik penyisipan data ke dalam *cover-object* dapat dilakukan dalam dua macam ranah:

1. Ranah spasial (waktu)

   Teknik ini mengubah langsung nilai *byte* dari *cover-object* (nilai *byte* dapat merepresentasikan intensitas/warna pixel atau amplitudo). Contoh metode yang tergolong ke dalam teknik ini adalah metode LSB (*Least Significant Bit*).

2. Ranah *transform*

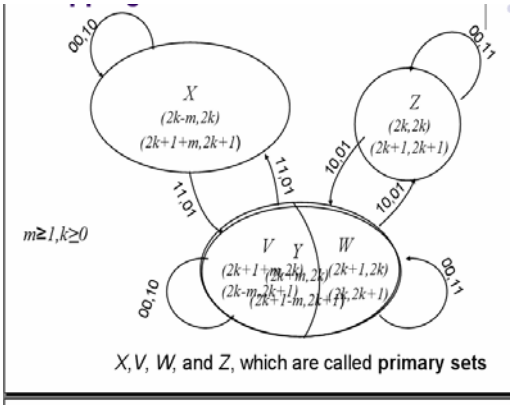
   Teknik ini memodifikasi langsung hasil transformasi frekuensi sinyal. Contoh metode yang tergolong ke dalam teknik ranah frekuensi adalah *spread spectrum*. Sinyal dalam ranah spasial diubah ke dalam ranah frekuensi dengan menggunakan transformasi seperti: DCT (*Discrete Cosine Transform*), DFT (*Discrete Fourier Transform*), dan DWT (*Discrete Wavelet Transform*).

Kelebihan dari metode LSB adalah mudah diimplementasikan dan proses untuk melakukan *encoding* cepat.

Kelemahan dari metode LSB adalah tidak tahan terhadap perubahan pada *cover-object*. Pesan mudah dihapus karena lokasi penyisipan diketahui (bit LSB).

Kelebihan dari metode DCT adalah kokoh terhadap manipulasi pada *stego-object*.

Berikut adalah diagram transisi status untuk LSB *Flipping*:



4. 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. Permasalahan umum pada steganalisis adalah sedikitnya informasi yang tersedia untuk steganalis. Steganalisis dilakukan tanpa memerlukan pengetahuan mengenai kunci yang dipakai maupun algoritma steganografi untuk menyisipkan pesan. Hal penting yang menjadi bahasan utama dalam steganalisis adalah mengetahui ada atau tidaknya pesan yang disisipkan pada suatu objek.

Penyembunyian informasi dengan menggunakan media elektronik membutuhkan pengubahan pada sifat dari media itu sendiri. Hal ini menyebabkan beberapa bentuk degradasi atau karakteristik yang tidak biasa dari media yang disisipi informasi. Karakteristik seperti ini dapat menjadi tanda bahwa terdapat penyisipan pesan sehingga tujuan dari steganografi pun menjadi patah.

Serangan dan analisis terhadap informasi yang tersembunyi dapat dilakukan dalam beberapa bentuk, seperti menemukan, menyadap, dan melumpuhkan atau menghancurkan informasi tersembunyi tersebut. Bentuk-bentuk ini juga bervariasi tergantung pada metode yang digunakan untuk menyisipkan informasi ke dalam media penutup.

Tujuannya adalah bukan untuk menghilangkan atau melumpuhkan informasi yang tersembunyi seperti hak cipta, tetapi untuk menunjukkan pendekatan-pendekatan yang mudah diserang dan memanfaatkannya untuk menginvestigasi informasi tersembunyi yang haram.

Beberapa penyimpangan dan degradasi mungkin terjadi pada alat pembawa pesan tersembunyi, tapi indera manusia tidak dapat menemukan hal itu dengan mudah. Penyimpangan ini mungkin ganjil bagi alat pembawa yang normal. Kakas-kakas steganografi bervariasi dalam pendekatan yang mereka gunakan untuk menyembunyikan informasi. Tanpa mengetahui kakas mana yang digunakan dan kunci, jika ada, yang digunakan, menemukan informasi tersembunyi dapat akan menjadi cukup rumit. Bagaimanapun, beberapa pendekatan steganografi memiliki karakteristik yang dapat digunakan sebagai tanda mengenai metode dan kakas yang digunakan.

Steganalisis dapat dilakukan pada berbagai jenis pesan, seperti plainteks, media digital, seperti suara, gambar, atau video. Citra banyak digunakan untuk menyisipkan pesan. Kehandalan dari citra dibandingkan dengan suara adalah kualitas dari citra yang telah disisipi pesan rahasia tidak berbeda jauh dengan kualitas citra penutupnya. Pada media suara, kualitas objek penutup lebih mudah mengalami penurunan kualitas setelah penyisipan pesan rahasia.

Citra yang telah disisipi pesan rahasia disebut *stegoimage*. Berikut adalah contoh citra yang telah disisipi pesan :

Gambar 1 *Cover-image*

Stegoimage telah disisipkan pesan berupa citra lain dengan kata kunci logoitb. Dari kedua contoh gambar di atas (Gambar 1 dan 2) dapat dilihat bahwa melalui indera penglihatan manusia stegoimage yang dihasilkan tidak memiliki perbedaan dengan citra asli yang digunakan sebagai penutup.

Gambar 3 menunjukkan proses steganalisis secara umum.

Pendekatan steganalisis yang dasar adalah dengan memodelkan citra sebagai realisasi dari sebuah proses acak dan pengaruh teori penemuan untuk menentukan solusi yang optimal dan memperkirakan performansi.

Gambar 2 *Stegoimage*

5. Metode-metode Steganalisis

Meskipun *stegoimage* identik dengan citra penutup bila ditangkap dengan indera penglihatan, *stegoimage* seringkali menunjukkan statistik yang tidak biasa yang membedakan *stegoimage* dari citra penutupnya. Tujuan dari steganalisis statistik memperlihatkan ketidakbiasaan ini adalah untuk menunjukkan perbedaan yang kuat antara *stegoimage* dan citra penutupnya.

Algoritma steganalisis dapat dikelompokkan menjadi dua berdasarkan metode steganografi yang ditargetkan, yaitu algoritma universal dan algoritma berbasiskan model. Metode steganalisis universal mencoba untuk memeriksa sejumlah metode steganografi, bahkan metode yang belum diketahui sekalipun, dalam *framework* yang umum.

Meskipun algoritma ini disukai karena serbaguna, tapi performansinya sering lebih rendah daripada algoritma berbasiskan model yang khusus untuk sebuah metode steganografi. Dua algoritma berbasiskan model yang terkenal yang menargetkan steganalisisnya pada metode LSB adalah steganalisis PoV dan steganalisis RS

5.1 Steganalisis RS (*Regular dan Singular*)

Steganalisis RS dikenalkan oleh Fridrich. Fridrich dan kawan-kawannya mengelompokkan setiap *pixel* pada citra ke dalam kelompok *Regular*, *Singular*, dan *Unusable*. Pendeteksian dilakukan berdasarkan angka yang dihasilkan dari masing-masing kelompok tersebut.

Sebuah *pixel* dimasukkan ke dalam kelompok *Regular* apabila potensial kecocokannya lebih besar daripada stegoimage dengan metode LSB versi pembalikan bit (*flip bits*) dan sebuah *pixel* akan dimasukkan ke dalam kelompok *Singular* apabila potensialnya lebih kecil. Komputasi untuk menentukan potensial kecocokan ini memerlukan distribusi spasial dari *pixel* menjadi *account* dan menentukan batasan kehalusannya. Algoritma ini akhirnya hanya akan akurat pada citra-citra yang memenuhi asumsi kehalusan tertentu.

Algoritma ini sangat efektif, bahkan dapat mengetahui sekitar dua hingga empat persen adanya *flipped bits* yang acak sekalipun. Algoritma ini juga dapat mengatasi metode steganografi LSB dan variasinya.

Anggap C adalah citra yang akan diuji coba dan memiliki nilai *pixel* dari 0 hingga 255.

$$F_i(F_i(x)) = F_0(x) = x, \quad i \in \{-1,1\}$$
$$F_1 : 0 \leftrightarrow 1,\ 2 \leftrightarrow 3,\ \ldots, 254 \leftrightarrow 255$$
$$F_{-1} : -1 \leftrightarrow 0,\ 1 \leftrightarrow 2,\ \ldots, 253 \leftrightarrow 254,\ 255 \leftrightarrow 256$$
$$F \text{ has a 2-cycle.}$$
$$F_{-1}(x) = F_1(x+1) - 1 \quad \text{for all } x$$

Kelompok G ditetapkan dalam satu dari tiga jenis kelompok *pixel*.

$$\text{Regular Group} : G \in R \Leftrightarrow f(F_M(G)) > f(G)$$
$$\text{Singular Group} : G \in S \Leftrightarrow f(F_M(G)) < f(G)$$
$$\text{Unusable Group} : G \in U \Leftrightarrow f(F_M(G)) = f(G)$$

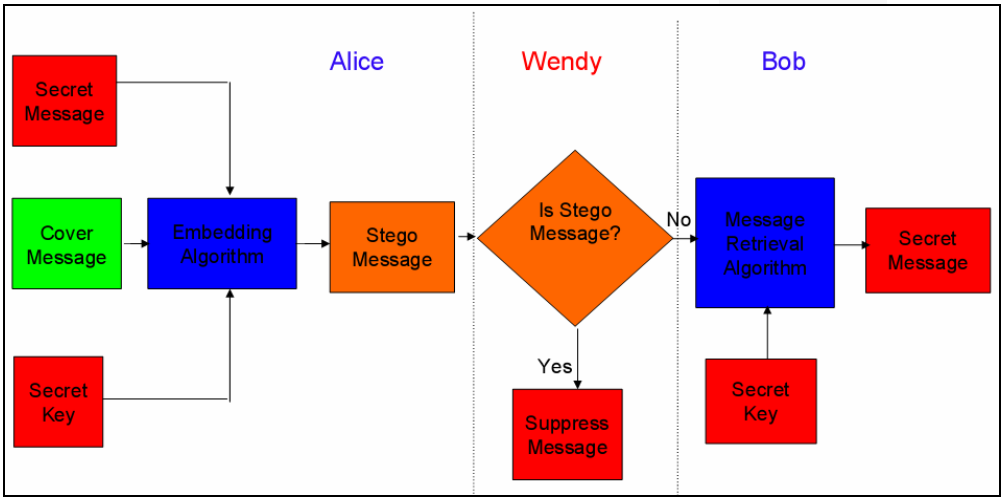
Sebagai contoh:

G = {1, 2, 3, 4}, M = [0, 1, 1, 0]

F_M (G) = {1, 2, 3, 4}

3 = f(G) < f(F_M(G)) = 5

$$G \in R$$



Gambar 3 Proses steganalisis secara umum

Kelompokkan C ke dalam n buah kelompok *pixel* yang berdekatan.

$$G = (x_1, \ldots, x_n) \in C.$$

Fungsi diskriminasi f didefinisikan sebagai berikut:

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n-1} \left| x_{i+1} - x_i \right|$$

Operasi F yang *invertible* pada x yang disebut *flipping* juga didefinisikan seperti di atas.

Ambil R_M (persentase dari seluruh kelompok) sebagai jumlah kelompok *regular* untuk penutup M dan S_M untuk kelompok *singular*.

Fridrich mengasumsikan hipotesis statistik dalam citra secara heuristik sebagai berikut :

$$R_M \cong R_{-M} \text{ and } S_M \cong S_{-M} \quad \cdots\cdots\cdots\cdots (1)$$
$$R_M(1/2) = S_M(1/2) \quad \cdots\cdots\cdots\cdots (2)$$

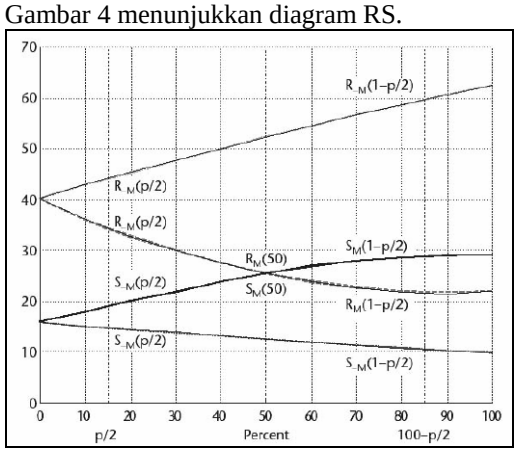
Jika sebuah pesan dengan panjang p% disisipkan pada *stegoimage*, tanpa *loss of generality*, maka (p/2)% dari *pixel stegoimage* akan dibalik (*flipped*) bersesuaian dengan nilai pixel yang dimilikinya. Lalu diperoleh 4 poin sebagai berikut:

$$R_M(p/2),\ S_M(p/2),\ R_{-M}(p/2),\ S_{-M}(p/2)$$

Dengan menerapkan *flipping* F_1 dan *shift fliping* F_{-1} pada semua *pixel*, 4 poin di atas menjadi:

$$R_M(1-p/2),\ S_M(1-p/2),\ R_{-M}(1-p/2),\ S_{-M}(1-p/2)$$

Gambar 4 menunjukkan diagram RS.



Gambar 4 Diagram RS

Asumsi (1) dan (2) memungkinkan untuk menurunkan suatu persamaan (3) untuk panjang pesan p.

$$2(d_1+d_0)x^2+(d_{-0}-d_{-1}-d_1-3d_0)x+d_0-d_{-0}=0 \quad \cdots\cdots (3)$$

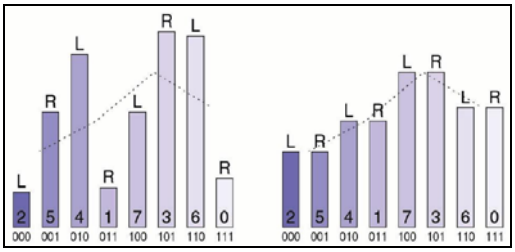
$$d_0 = R_M(p/2)-S_M(p/2)$$
$$d_1 = R_M(1-p/2)-S_M(1-p/2)$$
$$d_{-0} = R_{-M}(p/2)-S_{-M}(p/2)$$
$$d_{-1} = R_{-M}(1-p/2)-S_{-M}(1-p/2)$$
$$p = x/(x-1/2)$$

5.2 Steganalisis PoV (*Pair of Values*)

Pertama diusulkan oleh Pftizmann. Cara kerja dari metode ini adalah dengan menganalisis pasangan nilai yang muncul pada histogram. Keberadaan pesan yang disisipkan diketahui dengan menggunakan uji coba *Chi-square*, yaitu dengan mengevaluasi ketidaksamaan yang terdapat pada histogram yang berurutan.

Uji coba *Chi-square* ini diusulkan oleh Westfeld. Sifat acak dari pesan yang disisipkan membuat frekuensi dari nilai-nilai PoV pada *stegoimage* menjadi sama sementara nilai-nilai PoV pada citra penutup yang asli adalah tidak sama. Metode ini dapat menemukan citra-citra yang mencurigakan tanpa mengetahui citra aslinya (*Blind detection*). Gambar 4 menunjukkan histogram dari warna-warna yang terdapat pada citra sebelum dan setelah pesan disisipkan.

Metode ini sangat efektif untuk citra dengan *payload* yang besar, yaitu semua *pixel* atau hampir semua *pixel* digunakan untuk penyisipan dengan metode LSB. Metode ini dapat mendeteksi dengan tepat untuk ukuran pesan yang sebanding dengan ukuran bit latar.



Gambar 4 Histogram dari warna-warna yang terdapat pada citra sebelum dan setelah pesan disisipkan

Asumsikan terdapat k kategori dari PoV dari data yang mencurigakan, maka uji coba Chi-square sebagai berikut.

$$y_i^* = \frac{\left|n_{2i}+n_{2i+1}\right|}{2}, \quad 0 \le i \le k-1,$$

$$y_i = n_{2i},$$

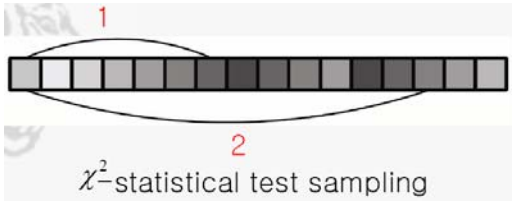
$$\chi^2_{k-1} = \sum_{i=1}^{k} \frac{(y_i - y_i^*)^2}{y_i^*}, \qquad y_i = n_{2i}$$

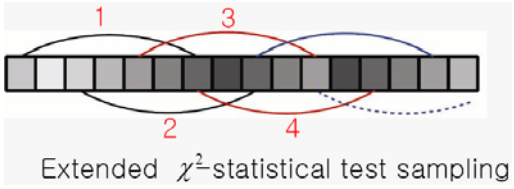
$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma(\frac{k-1}{2})}\int_0^{\chi^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1}\,dx$$

Γ : Euler Gamma function.

p: peluang penyisipan pesan dalam kondisi distribusi n dan n* adalah sama.

Provos juga memperluas analisis statistik *Chi-square* dengan melakukan *re-sampling* pada interval uji coba atau memperbaiki nilai *pixel*, dari pasangan *pixel* antara x dan x+1 menjadi x dan x-1. Gambar 5 menunjukkan percobaan *Chi-square* analisis biasa dan *Chi-square* yang diperluas oleh Provos.





5.3 *Palette Checking*

Definisi: Keanehan pada urutan palette adalah sebuah tanda adanya perubahan sistematis.
Metode steganografi yang ditargetkan: steganografi pada citra-citra palette.

5.4 Metode RQP

Definisi: Metode berbasiskan analisis terhadap kenaikan jumlah pasangan *close-color* dikarenakan proses penyisipan.
Metode steganografi yang ditargetkan: penyisipan LSB pada citra-citra *true color*.

5.5 Uji coba kompatibilitas JPEG

Definisi: Metode menemukan ketidakbiasaan dari JPEG *signature* yang melekat pada citra pada awal penyimpanan format JPEG.
Metode steganografi yang ditargetkan: Steganografi ranah spasial yang menggunakan citra-citra yang pada awalnya disimpan dalam format JPEG.

Semua metode steganografi berusaha untuk mendapatkan sesedikit mungkin jumlah penyimpangan dengan tujuan meminimalisasi kemungkinan dari pengenalan artifak pada permulaan analisis. Bagaimanapun, jika citra penutup pada awalnya disimpan dalam format JPEG, pesan yang disisipkan dalam ranah spasial akan merusak tapi tidak akan menghapus karakteristik struktur yang telah diciptakan oleh kompresi JPEG dan seseorang masih dapat dengan mudah menentukan apakah citra yang diberikan pernah disimpan dalam bentuk JPEG atau tidak.

Tentu saja, hal itu memungkinkan untuk memperoleh kembali tabel *quantization* JPEG dari *stegoimage* dengan menganalisis nilai-nilai koefisien DCT dalam blok 8x8. Setelah pesan disisipkan, bagaimanapun, citra penutup akan menjadi (dengan peluang yang tinggi) tidak kompatibel dengan format JPEG, dalam pengertian bahwa blok *pixel* 8x8 tidak akan dapat menghasilkan dekompresi JPEG untuk setiap blok dari koefisien yang *quantized*. Penemuan ini memberikan bukti yang kuat bahwa blok telah mengalami modifikasi. Tentu saja, hal ini menimbulkan kecurigaan yang tinggi untuk menemukan citra yang tersimpan dalam format yang *lossless* yang menghasilkan kompresi JPEG yang tidak kompatibel dengan citra JPEG terkompresi manapun. Hal ini dapat menjadi bukti adanya steganografi.

Dengan melakukan pemeriksaan terhadap kompatibiltas JPEG di setiap blok, kita mungkin dapat menemukan pesan sepanjang 1 bit. Dan metode steganalisis ini dapat digunakan untuk metode steganografi spasial atau metode watermarking manapun, dan bukan hanya penyisipan LSB.

Seseorang bahkan dapat memperkirakan panjang dari pesan dan posisinya pada citra dengan menentukan blok 8x8 mana yang tidak kompatibel dengan kompresi JPEG. Bahkan seseorang juga dapat menganalisis citra dan memperkirakan citra penutup dan bloknya. Dengan menggunakan metode ini, kita dapat mengidentifikasi *pixel-pixel* yang telah diubah.

Berikut adalah deskripsi algoritmanya:

1. Pisahkan citra ke dalam kotak blok berukuran 8x8, lewati beberapa baris dan kolom terakhir apabila dimensi citra bukan kelipatan dari 8.
2. Susun blok dalam sebuah *list* dan hapus semua blok yang *saturated* dari *list* (sebuah blok dikatakan *saturated* jika blok tersebut memiliki setidaknya satu *pixel* dengan nilai *gray* 0 atau 255). Simpan jumlah total blok sebagai T.
3. Ekstraksi matiks *quantization* Q dari semua T blok. Jika jumlah kandidat untuk Q adalah satu, maka citra bukan disimpan sebagai JPEG sebelumnya dan metode steganalisis tidak digunakan (keluar dari algoritma). Jika terdapat lebih dari satu kandidat elemen dari Q, maka langkah 4-6 perlu dilakukan untuk semua kandidat. Hasil yang memberikan angka tertinggi dari blok yang kompatibel dengan JPEG akan diambil sebagai hasil dari algoritma ini.
4. Untuk setiap blok B, hitung jumlah S dari persamaan berikut

$$16 \geq \left\| QD' - QD \right\|^2 \geq \sum_{i=1}^{64} \left| QD'(i) - Q(i) round\left(\frac{QD'(i)}{Q(i)} \right) \right| = S. \quad (7)$$

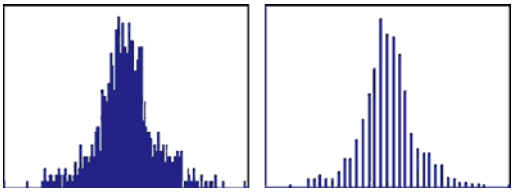
   a. Jika S > 16, maka blok B tidak kompatibel dengan kompresi JPEG dengan matriks *quantization* Q.
   b. Jika S <= 16, maka untuk setiap koefisien DCT QDi', hitung perkalian terdekat dari Q(i), terurut berdasarkan jaraknya dengan QDi', dan simpan mereka dalam qp(i), p = 1, dan seterusnya. Untuk kombinasinya, untuk setiap pertidaksamaan (8) dipenuhi, maka periksa apakah ekspresi (9) dipenuhi atau tidak. Jika untuk setiap set index {p(1), ..., p(64)}, ekspresi (9) dipenuhi, maka blok B kompatibel dengan kompresi JPEG, dan tidak berlaku sebaliknya.

$$S = \sum_{i=1}^{64} \left| QD'(i) - q_{p(i)}(i) \right| \leq 16 \quad (8)$$

$$B = [DCT^{-1}(QD)], \text{ where } QD(i) = q_{p(i)}(i). \quad (9)$$

5.6 Analisis Histogram

Definisi: Metode mengungkapkan ciri-ciri atau sifat periodik dalam koefisien khusus dan pengubahan berkaitan dengan *quantization*.
Metode steganografi yang ditargetkan: QIM atau metode *quantization-related embedding* lainnya. Gambar 6 menunjukkan analisis histogram.



Gambar 6 Kiri: histogram dari koefisien dual-transform dari citra penutup Lena; Kanan: tanda penyisipan QIM.

5.7 *Universal Blind Detection*

Definisi: Statistik tingkat tinggi membangun statistik kuantitas, dan model penemuan dibangun dengan permulaan yang didapatkan dari proses pelatihan.
Metode steganografi yang ditargetkan: bermacam-macam teknik steganografi.

Dengan pengecualian steganalisis kompatibilitas JPEG, yang dapat diterapkan padaa semua metode steganografi spasial, metode-metode yang diusulkan sebelumnya disesuaikan untuk suatu algoritma penyisipan tertentu atau variasinya. *Universal blind detection* adalah suatu metode *meta-detection* yang dapat diatur, setelah pelatihan terhadap citra asli dan *stegoimage*, untuk menemukan metode steganografi tanpa memperhatikan ranah penyisipannya. Idenya adalah untuk menemukan set dari sejumlah statistik kuantitas yang sensitif dengan kemampuan untuk membedakan. Neural networks, algoritma clustering dan kakas lainnya dapat digunakan untuk menemukan permulaan yang tepat dan membangun model pendeteksian dari data eksperimen yang telah dikumpulkan.

Farid mengusulkan sebuah set dari statistik sensitif dengan urutan yang lebih tinggi yang diturunkan dari dekomposisi wavelet stegoimage.

Kemudian, dia menggunakan analisis *Fisher Linear Discrimination* untuk memisahkan *feature vectors* ke dalam dua buah *linear subspaces*. Satu vektor untuk *stegoimage* dan yang lainnya untuk citra aslinya. Penentuan permulaan dapat disesuaikan dengan *trade missed detections* untuk kesalahan positif.

Menyadari fakta bahwa pendekatan ini memiliki sejumlah pilihan yang berubah-ubah, pendekatan ini luar biasa dalam performansinya.

Pendekatan Farid diawali dari level ke-n dekomposisi *wavelet stegoimage* dengan Vi(x,y), Hi(x,y), dan Di(x,y) merepresentasikan vertikal, horizontal, and diagonal *subbands* pada skala i. Kemudian, ia mengkalkulasikan 4 momen pertama untuk tiga *subbands* untuk semua level i = 1 hingga n-1. Kalkulasi ini memberikan total dari 12 (n – 1) statistik kuantitas. Kemudian, dia menggunakan *optimal linear predictor* dan mengumpulkan statistik momen yang sama untuk prediksi kesalahan antara nilai aktual dari koefisien *wavelet* dan prediksi *optimal linear* dari spasial, orientasi dan skala tetangganya (total dari 7 tetangga).

Sebagai contoh koefisien vertikal wavelet diprediksikan menggunakan *linear predictor* berikut: $V_i(x,y) = w_1V_i(x – 1, y) + w_2V_i(x + 1, y) + w_3V_i(x, y – 1) + w_4V_i(x, y+1) + w_5V_{i+1}(x/2, y/2) + w_6D_i(x, y) + w_7D_{i+1}(x/2,y/2)$.

Berat-berat yang meminimalkan kesalahan dihitung dengan menggunakan standard pendekatan *least square*.

Interpretasikan *linear prediction* untuk $V_i(x,y)$ sebagai V_i (x,y), *log error* dari prediksi didefinisikan sebagai $Ev(i) = \log_2(Vi) – \log_2(Vi$). Farid mengkalkulasikan empat momen pertama dari Ev(i) sebagai bagian lain dari *feature vector*-nya. Keseluruhan proses diulang untuk semua skala n-1 untuk horizontal dan diagonal *subbands*.

Lalu, panjang terakhir dari *feature vector* adalah 12(n-1) + 4x3(n-1) = 24(n-1). *Feature vector* dikalkulasikan untuk sebuah basis data yang besar dari citra yang asli dan *stegoimage* yang disisipkan dengan ukuran pesan yang tetap.
Farid menggunakan analisis *Fisher Linear Discriminant* (FLD) untuk mengklasifikasikan *feature vector* ke dalam dua *cluster* yang dipisahkan dengan sebuah permulaan. Keuntungan dari pendekatan ini adalah bahwa analisis FLD memungkinkan *scalar thresholding* yang cepat dan sederhana dalam satu dimensi.

Hasil yang diberikan oleh Farid menunjukkan bahwa pendekatannya adalah sebuah metode yang memberikan hasil yang mengesankan. Farid menggunakan basis data dari citra kualitas tinggi berukuran 1400x1000 yang di dalamnya ia sisipkan citra *grayscale* berukuran 256x256 pixel menggunakan J-Steg, EZ Stego dan dua versi dari OutGuess. Hasil terbaik yang didapatkan adalah sebagai berikut.

a. J-Steg ditemukan dengan kepercayaan 97,8% dengan 1,8% kesalahan positif.

b. EZ Stego ditemukan dengan kepercayaan 86.6% dengan 13.2% kesalahan positif.
c. OutGuess ditemukan dengan kepercayaan 80,4 % dan 19,4% kesalahan positif (untuk versi 0.1)
d. OutGuess ditemukan dengan kepercayaan 77,7 % dan 23,8% kesalahan positif (untuk versi 0.2)

Sebagai tambahan, metode steganalisis yang dikhususkan untuk suatu metode steganografi tertentu, seperti steganalisis RS, akan memberikan hasil yang lebih akurat dan terpercaya dibandingkan dengan metode steganalisis *universal blind* manapun. Meskipun demikian, pendekatan *universal blind* ini sangat penting karena fleksibilitas dan kemampuannya untuk menyesuaikan diri secara cepat untuk metode steganalisis yang baru maupun steganalisis yang tidak diketahui sama sekali.

6. Kesimpulan

Metode steganalisis yang khusus tertentu akan memberikan hasil steganalisis yang lebih akurat dan lebih terpercaya apabila dibandingkan dengan metode steganalisis *universal blind*. Namun metode steganalisis *universal blind* memiliki kelebihan dalam kemampuannya untuk mendeteksi adanya steganografi pada citra meskipun metode steganalisisnya belum diketahui sama sekali.

Steganalisis RS dan PoV baik digunakan untuk menemukan adanya steganografi pada citra dengan metode penyisipan LSB.

Kesimpulan lainnya yang dapat ditarik dari makalah ini adalah masih terdapat metode steganalisis yang dapat dikembangkan untuk memecahkan metode steganografi tertentu, seperti F5, EzStego, OutGuess, IQM, Bit-O-Steg, Zero Hiding, dll. Saat ini, metode-metode ini baru diselesaikan dengan menggunakan steganalisis *universal blind*.

DAFTAR PUSTAKA

[1] Celik, Mehmet U., Gaurav Sharma, Murat Tekalp. (2004). *Universal Image Steganalysis Using Rate-Distortion Curves*.

[2] Fridrich Jessica, Miroslav Goljan. (2001). *Practical Steganalysis of Digital Images – State of the Art*.

[3]http://acmqueue.com/modules.php?name=Content&pa=showpage&pid=241&page=1

[4] Image Steganography and Steganalysis. *http://www.ims.nus.edu.sg/Programs/imgsci/files/memon/sing_stego.pdf#search=%22History%20of%20Steganalysis%22* Tanggal akses: 10 Oktober 2006 pukul 12:30.

[5] Munir, Rinaldi. (2006). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[6] N.F. Johnson, S. Jajodia, “Exploring Steganography: Seeing the Unseen”, IEEE Computer, Februari1998, vol. 31, no. 2, pp.26-34

[7] N.F. Johnson, S. Jajodia, “Steganalysis: The Investigation of Hidden Information”, IEEE Computer, September 1998, George Mason University, MS:4A4, Fairfax, Virginia.