STUDI ANALISIS PERBANDINGAN METODE STEGANALISIS TERHADAP *LSBIMAGE STEGANOGRAPHY*

Shauma Hayyu Syakura (13507025)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17025@students.if.itb.ac.id

***Abstrak*—Kebutuhan untuk menyembunyikan pesan dalam komunikasi agar pesan hanya bisa dibaca oleh penerima dan pengirim pesan tanpa menimbulkan kecurigaan menimbulkan munculnya steganografi. Steganografi adalah menyembunyikan pesan dalam objek lain sedemikian rupa sehingga tidak memunculkan kecurigaan. Salah satu metode steganografi adalah penyembunyian file di dalam file image dengan metode LSB (*Least Significant Bit*). Sebagai *counter-attack* dari LSB Steganography tersebut, muncul berbagai macam metode-metode serangan (*Steganography Attack* atau Steganalisis). Dalam makalah ini akan dibahas hasil studi mengenai beberapa perbandingan metode steganalisis terhadap LSB. Metode-metode yang dibandingkan adalah steganalisis naiv, metode *Center Mass of Histogram Characteristic Function,* dan *Autocorrelation Coefficient*. Studi ini dilakukan dengan tujuan untuk menentukan metode mana yang paling efektif.**

***Kata Kunci*—Steganografi, LSB, Steganalisis, Perbandingan Metode**

1. PENDAHULUAN

Dalam kebutuhan manusia agar dapat saling bertukar pesan secara rahasia salah satu caranya adalah dengan menggunakan kriptografi, yaitu menyembunyikan pesan dengan cara mengganti pesan tersebut menjadi kode yang tidak dapat dikenali orang lain. Namun tentunya hal tersebut akan langsung menimbulkan kecurigaan apabila ditemukan oleh orang lain, oleh karena itu muncul cara lain untuk bertukar pesan secara rahasia yaitu dengan steganografi. Steganografi adalah suatu cara menyampaikan pesan rahasia dengan menyembunyikan pesan di dalam suatu objek atau pesan yang tidak mencurigakan sehingga orang lain tidak mudah mengetahuinya.

Hal ini penting karena dapat menjamin keprivasian pesan dan menjaga pesan-pesan penting agar tidak diketahui orang lain, contohnya pada saat perang dimana informasi yang dimiliki suatu negara tidak bisa diketahui oleh negara lawan. Namun steganografi menjadi berbahaya apabila digunakan oleh *teroris* atau *kriminal*. Oleh karena itu, muncullah Steganalasis atau serangan terhadap Steganografi yang menjadi *counter attack* dari steganografi.

Sesuai dengan berkembangnya zaman, dan terutama karena ditemukannya komputer, muncul kebutuhan untuk melakukan steganografi pada media digital. Salah satu metode steganografi media digital yang paling terkenal adalah menyembunyikan pesan dalam media digital *image* atau gambar, dengan menggunakan metode LSB (*Least Significant Bit*).

Metode Steganografi dalam image dengan LSB menggunakan kelemahan mata manusia dalam mendeteksi perbedaan warna. Cara kerja metode ini adalah dengan menyisipkan bit-bit pesan pada bit-bit terakhir setiap byte pada image (contohnya image BMP), sehingga perubahan pada gambar tetap tidak terlihat dan sulit dibedakan.

Oleh karena itu sebagai penangkal dari metode LSB, muncul berbagai metode steganalisis untuk metode LSB. Tujuan dari steganalisis adalah untuk mendeteksi keberadaan pesan tersembunyi dalam sebuah image yang tersteganografi dan menghancurkan pesan yang tersembunyi tersebut. Memang belum ada metode yang benar-benar mangkus, namun metode-metode tersebut terus menghasilkan peningkatan dari tahun ke tahun, mulai dari metode

yang paling naif sampai menggunakan Intelegensia Buatan (*contohnya classifier*).

Dalam paper ini akan dilakukan studi analisis mengenai beberapa metode steganalisis terhadap LSB steganography yang sudah ada. Ada tiga metode yang akan dibandingkan, yaitu metode steganalisis naif (dengan hanya mencari selisih perbedaan bit antara file image stego (image hasil steganografi) dan file image asli), *Center of Mass of the Histogram Characteristic Function*, dan menggunakan *Auto-Correlating Coefficient*.

2. LSB STEGANOGRAPHY

LSB (*Least Significant Bit*) Steganography pada image adalah metode steganografi dengan memanipulasi bit-bit terakhir pada *byte-byte* dalam suatu file gambar, seperti file-file bitmap dan JPEG. Gambar yang digunakan untuk menyembunyikan data disebut *cover image*, sementara image yang dihasilkan dari steganografi data tersebut disebut *stego image*[2].File-file gambar yang digunakan biasanya adalah file dengan tipe *lossless compression*, karena perbedaan bit pada *byte-byte*-nya tidak terlihat jelas. Terdapat dua jenis metode LSB yaitu *LSB Replacement* dan *LSB Matching*.

LSB Replacement berkerja dengan cara mengganti bit-bit terakhir pada *byte-byte* dalam file gambar, dengan bit-bit dari file yang ingin disembunyikan. Tetapi bit-bit tersebut tidak dimasukkan begitu saja secara berurutan, melainkan dimasukkan secara *pseudorandom* (secara acak namun tidak benar-benar acak). Bilangan acak tersebut dibangkitkan dengan kunci yang dimiliki oleh pengirim dan penerima pesan.

Pesan yang disembunyikan di dalam cover image terbatas dengan ukuran byte dari image tersebut. Dan semakin sedikit ukuran file yang disembunyikan, dan semakin tersebar posisi bit-bitnya, maka deteksi file pada stego image akan semakin sulit. Selain itu pemilihan gambar juga berpengaruh. Gambar dengan perbedaan warna yang banyak seperti fotografi merupakan pilihan terbaik sebagai cover image. Beberapa steganografer mengatakan bahwa gambar hitam putih merupakan gambar terbaik untuk digunakan sebagai cover image[2].

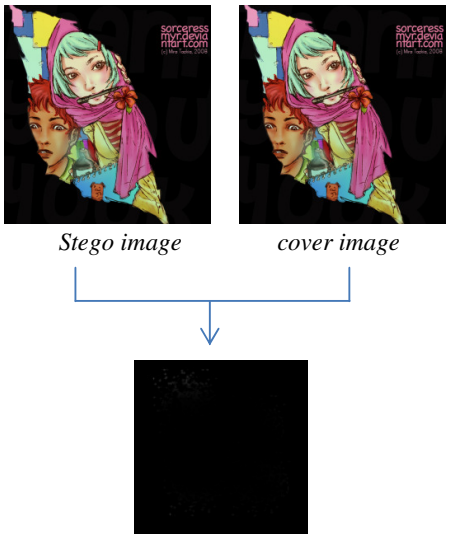
Pada *LSB Matching*, setiap bit-bit data yang disembunyikan dibandingkan dengan bit terakhir dari byte cover image yang berkoresponden. Jika cocok jangan lakukan apapun, jika tidak cocok, byte pada cover image ditambah satu atau dikurang satu secara acak (kecuali untuk byte yang ukurannya 0 tidak dapat dikurangi dan byte yang ukurannya 255 tidak dapat ditambah). Cara mengekstraksi pesan filenya sama dengan *LSB Replacement*, yaitu dengan menggunakan kunci untuk membangkitkan bilangan acak tersebut.

LSB Replacement umumnya lebih mudah dideteksi dibandingkan dengan LSB Matching[]. Hal ini disebabkan karena pada LSB Replacement, *byte-byte cover image* yang bernilai genap, pada *stego image* tetap bernilai sama atau bertambah satu. Perbedaan ini dapat digunakan untuk steganalisis. Sedangkan pada *LSB Matching* pada *stego image*-nya tidak terdapat *byte* yang bernilai genap sehingga metode steganalisis di atas tidak dapat digunakan.

3. STEGANALISIS NAIF

Berikut ini adalah metode yang dirancang oleh penulis sendiri. Steganalisis ini dikhususkan untuk mendeteksi file pada *stego image* yang menggunakan metode *LSB Replacement*. Steganalisis ini memanfaatkan perbedaan pada byte-byte cover image dan stego image, yaitu dimana pada *byte-byte* yang bernilai genap tetap bernilai sama atau ditambah 1.

Cara steganalisis metode ini adalah dengan mengurangi *byte-byte* pada stego image dengan cover image. Hasil pengurangannya kemudian dicetak lagi ke bitmap dengan matriks pixel yang sama.



Gambar 1

Pada gambar hasil pengurangan (untuk byte-byte yang berbeda diberi nilai 255 agar berubah warna menjadi putih), tampak bercak-bercak putih tersebar

di pojok kiri atas yang menandakan adanya *byte-byte* yang berbeda dengan *byte* asli. Dapat disimpulkan bahwa terdapat pesan rahasia yang disimpan di dalam gambar tersebut.

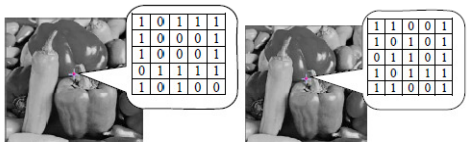
4. CENTER MASS OF HISTOGRAM CHARACTERISTIC FUNCTION

Metode ini memodelkan steganografi *LSB Matching* sebagai *noise* aditif yang tidak saling bergantung. Karena penambahan noise pada domain spatial gambar berhubungan dengan filter bawah pada histogram, histogram dari *stego image* memiliki nilai yang lebih rendah pada frekuensi tinggi di banding histogram dari *cover image*. Jadi, fungsi dari *center mass of the characteristic* H (fungsi H), yang didapatkan dari transformasi Fourier histogram h, akan menurun setelah image tersebut disisipkan dengan file menggunakan *LSB Matching*. Skema ini disebut dengan steganalisis *Histogram Characteristic Function* (HCF). Pusat massa dari HCF dihitung dengan rumus berikut:

$$C(H) = \frac{\sum_{i=0}^{127} i \times |H(i)|}{\sum_{i=0}^{127} |H(i)|} \quad (1)$$

5. AUTO-CORRELATING COEFICIENT

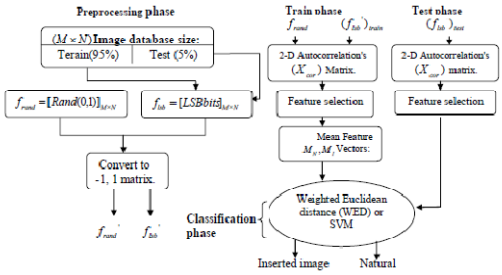
Dalam *file* gambar pada umumnya, ada suatu hubungan tingkat keabuan antar pixel yang bertetangga. Ini berarti, sebagian besar pixel-pixel yang bertetangga sebagian besar memiliki nilai yang sama. Namun jika suatu pesan dimasukkan ke dalam file gambar, maka hubungan tersebut akan rusak.



Cover image *Stego Image*

Gambar 2

Diagram dari metode ini diperlihatkan pada gambar sebagai berikut.



Gambar 3

Untuk mendeteksi gambar yang memiliki pesan tersembunyi, metode ini menggunakan *classifier.* F adalah gambar hitam putih yang memiliki M baris dan N kolom. Pada gambar tersebut dibuat matriks-matriks korelasi pada gambar tersebut. Kemudian beberapa matriks tersebut dipilih untuk dijadikan fitur yang kemudian akan digunakan untuk keperluan klasifikasi. Matriks yang dipilih adalah matriks yang memeiliki *matrix correlation* yang koefisiennya berbeda antara stego image dan cover image.

Setelah didapatkan fitur-fitur, digunakan 2 tipe *classifier*, SVM (*Support Vector Machine*) dan *Weighted Euclidian Distance*.

6. ANALISIS DAN PERBANDINGAN

Untuk metode naif, metode ini hanya dapat bekerja apabila *cover image* dimiliki oleh steganalisis. Dan sangat sulit digunakan apabila file yang disisipkan ukurannya sedikit.

Untuk performansi dengan menggunakan metode CMH, metode ini bagus digunakan untuk file-file gambar berwarna. Namun untuk file-file gambar hitam putih performansinya tidak bagus karena gambar hitam putih keberagaman pada histogramnya sedikit.

Sedangkan untuk eksperimen pada *auto-correlating coeficient,*hasil eksperimen mengunakan gambar dengan berbagai macam kualitas, baik gambar yang berwarna mau pun tidak berwarna dengan jumlah di atas 100 buah. Setelah basis data gambar disiapkan, 5 gambar digunakan sebagai data latih dan 120 gambar sebagai data uji untuk setiap kelas. Untuk membangun kelas-kelas *stego image*, setiap gambar pada kelas-kelas di atas dimasukkan dengan bit-bit acak dengan tingkatan yang berbeda-beda. Sehingga ada 2 banding 14 data yang tidak dimasukkan bit acak dan data yang dimasukkan.

Berikut ini ditampilkan data-data hasil pengujian. Tabel 1 untuk gambar berwarna dan tambel 2 untuk gambar hitam putih. Nilai di kolom adalah persentasi hasil yang salah, terhadap embedding rate (tingkat bit yang dimasukkan ke dalam gambar).

Tabel 1

Embedding Rate(bpp)	0	0.01	0.02	0.04	0.05	0.06	0.07	0.08	0.09	0.1
False Alarm (%)(WEDM)	0.21	0	0	0	0	0	0	0	0	0
False Alarm (%) (SVM)	0.12	0	0	0	0	0	0	0	0	0

Embedding Rate(bpp)	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
False Alarm (%)(WEDM)	0	0	0	0	0	0	0	0	0
False Alarm (%) (SVM)	0	0	0	0	0	0	0	0	0

Tabel 2

Embedding Rate(bpp)	0	0.01	0.02	0.04	0.05	0.06	0.07	0.08	0.09	0.1
False Alarm (%)(WEDM)	0.22	0.01	0	0	0	0	0	0	0	0
False Alarm (%) (SVM)	0.24	0.07	0.05	0.02	0	0	0	0	0	0

Embedding Rate/bpp)	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
False Alarm (%)(WEDM)	0	0	0	0	0	0	0	0	0
False Alarm (%) (SVM)	0	0	0	0	0	0	0	0	0

Dapat kita lihat pada tabel 1 dan 2 terdapat perbedaan. Untuk gambar berwarna SVM memiliki performansi yang lebih bagus. Sedangkan untuk gambar hitam putih WEDM memiliki performansi yang lebih bagus.

Dari ketiga metode di atas, dapat dilihat bahwa metode *autocorellation coeffiecient* memiliki performansi yang paling baik. Hal ini dikarenakan program memiliki sistem *learning* dari basis data matriks-matriks yang dimilikinya. Dapat kita lihat metode ini dapat mendeteksi file tersembunyi yang ukurannya kecil sekalipun. Sedangkan kedua metode sebelumnya tidak selalu dapat mendeteksi file tersembunyi pada *stego image*.

7. KESIMPULAN

Karena metode steganografi menggunakan LSB sangat mudah untuk dieksekusi, karena itu metode LSB masih banyak digunakan hingga sekarang. Dan hal ini berbahaya bila digunakan oleh pihak yang salah. Oleh karena itu, steganalisis harus terus menyempurnakan metode-metode yang ada sebelumnya.

Selain itu, untuk metode steganalisis modern, selain melihat kelemahan dari karakteristik file gambar, sebaiknya diberikan sistem *learning* intelegensia buatan seperti yang digunakan metode *Autocorrelation Coeffition*. Dengan sistem *learning*, kemampuan dan performansi program steganalisis akan semakin meningkat. Bahkan file-file kecil dalam gambar pun dapat dideteksi oleh program steganalisis. Metode *learning* yang digunakan juga tidak terbatas pada klasifikasi saja, untuk pengembangan steganalisis selanjutnya perlu dipertimbangkan penggunaan metode *learning* lainnya seperti *Clustering* dan *Artificial Neural Network*.

Dengan menggunakan metode learning, metode ini dapat dikembangkan pula untuk mendeteksi berbagai file tersembunyi pada gambar yang menggunakan algoritma steganografi yang berbeda-beda.

REFERENSI

[1] Yadollahpour, Arezzo, and Naimi, Hossein Miar. “Attack on LSB Steganography in Color and Grayscale Images
Using Autocorrelation Coefficients”.ISSN 1450-216X Vol.31 No.2 (2009), pp.172-183

[2] Fridrich, Jessica, Goljan, Misrolaf, and Du, Rui. “Reliable Detection of LSB Steganography in Color and Grayscale Images”. SUNY Binghamton Departement of EE.

[3] Zhang, Jun, Hu, Yuping, and Yuan, Zhibin. ”Detection of LSB Matching Steganography using
the Envelope of Histogram”. Guangdong University of Business Studies.2009.

[4] Ker, Andrew D. “Improved Detection of LSB Steganography in
Grayscale Images”. Oxford University Computing Laboratory.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 29 April 2010