ANALISIS PERBANDINGAN FIDELITY UNTUK STEGANOGRAPHY AUDIO & IMAGE DIGITAL

Rully Iman Fadillah[1], Iwan Iwut Tritoasmoro[2], Yudha Purwanto[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Pertukaran data merupakan suatu hal yang sering dijumpai pada internet. Format data yang dipertukarkan dapat berekstensi ".GIF" untuk image digital, ".WAV" untuk audio digital. Kedua jenis format tersebut terkadang dimanfaatkan untuk hal penting lainnya seperti perlindungan data.

Steganography merupakan teknik menyembunyikan pesan ke suatu carrier file (berkas pebawa) yang dapat memuat pesan tersebut dengan harapan agar pesan rahasia tidak terdeteksi keberadaannya selain pihak yang dituju. Spread spectrum (spektrum tersebar) adalah salah satu metoda yang digunakan untuk menghindari serangan terhadap pesan yang dipertukarkan dengan menyebar informasi menggunakan bantuan sinyal pseudo random (sinyal random palsu). Sinyal pseudo random dibangkitkan dari carrier file yang digunakan sehingga besar ukurannya sama dengan ukuran media.

Berdasarkan analisa, metoda spread spectrum lebih tepat digunakan pada carrier file audio digital dibandingkan dengan carrier file image digital. Pada pengujian carrier file dengan level sequence 8, 32, dan 128 pada file audio digital diperoleh nilai MOS sebesar 3,10. Sedangkan pada file image digital diperoleh nilai MOS sebesar 2,70. Kemudian berapapun ukuran file pesan yang disisipkan, tidak mempengaruhi kualitas fidelity.

Kata Kunci : Steganography, carrier file, spread spectrum, fidelity, stegfile

Abstract

Exchange of data is a common thing on the internet. Format of data that exchanged could be extended as ".GIF" for digital image files and ".WAV" for digital audio files. Both of them sometimes used for other important thing such as data protection.

Steganography is a technique to hide messages through a carrier file that can contain the message with expectation that the presence of secret message can not be detected by others except the intended party. Spread spectrum is a method that is used to avoid attacks on message that are exchanged by spreading information using the help of pseudo random signal (fake random signal). Pseudo random signal is generated from the carrier file so that it has similar size to the media.

Based on the analysis, the spread spectrum method is more appropriate to be used in digital audio files compared with digital image files. Considered by experiment of carrier files with level sequence 8, 32, and 128 on digital audio files obtained grade of MOS about 3,10. Nevertheles on digital image files obtained grade of MOS about 2,70. No matter how big the size of message files that embedded, it's not influence to quality of fidelity.

Keywords : Steganography, carrier media, spread spectrum, fidelity, stegfile

1. Pendahuluan

1.1 Latar Belakang

Keamanan informasi yang dipertukarkan merupakan hal yang penting untuk dijaga. Terutama bila informasi tersebut merupakan hal yang rahasia seperti keamanan negara, kebijakan bisnis, dsb. Keamanan informasi mulai dipermasalahkan bila informasi tersebut dipertukarkan melalui jalur yang dapat diakses oleh satu atau beberapa pihak yang bukan merupakan tujuan dari pengirim.

"*Steganography* merupakan teknik dan seni bagaimana menyembunyikan data digital di balik data digital lain yang berperan sebagai medium pembawa (*carrier*) sehingga keberadaannya tidak mengundang kecurigaan dari persepsi pengamatan manusia (Eddy Muntina Dharma, 2008)". Pengamatan manusia baik itu merupakan pengamatan *visual* (penglihatan) maupun *auditory* (pendengaran) memiliki batas nilai yang menyebabkan seolah-olah data yang sedang diamati adalah data kontinyu dan tidak peka terhadap perubahan data. Memanfaatkan keterbatasan pengamatan manusia, *steganography* digunakan untuk menutupi keberadaan pesan yang akan dipertukarkan dengan melakukan penyisipan pesan ke *carrier file*. Namun harga yang harus dibayar dari proses penyisipan itu adalah penurunan kualitas *carrier file* yang dikarenakan gangguan (*noise*) dari data yang disembunyikan agar dapat disisipkan pada *carrier file*. *File* penyisipan pesan dapat berupa *image digital* (citra digital), *audio digital* (suara), *video*, dan sebagainya.

Dari pengaruh gangguan tersebut menyebabkan kualitas *carrier file* menjadi berkurang sehingga dapat menyebabkan kecurigaan terhadap pihak yang melakukan penyerangan maupun *monitoring*. Oleh karena itu diperlukan pengetahuan tentang batasan besar *file* pesan yang optimal untuk disisipkan dan pengaruhnya terhadap *carrier file*.

1.2 Perumusan Masalah

Pada laporan penelitian ini diadakan perancangan dan analisa ketahanan *file* hasil dari aplikasi *steganography* pada dua jenis *carrier file*, yaitu *audio* dan *image digital* menggunakan metoda *spread spectrum*. Pada metoda *spread spectrum*, pesan rahasia disebar ke sinyal hasil dari *pseudo random generator* (pembangkit sinyal *pseudo random*) yang *dependent* (bergantung) pada *carrier file*. Setelah dilakukan penyebaran pesan, barulah proses *steganography* dilakukan.

Untuk dapat menerapkan metoda *spread spectrum*, beberapa hal yang perlu diperhatikan adalah:

1. Pada laporan penelitian ini digunakan *discrete cosinus transform* (transformasi kosinus diskrit) untuk membangkitkan sinyal *pseudo random* terhadap sinyal *carrier file*.
2. Kode penyebar atau di dalam laporan penelitian ini disebut *interleaving key* pada proses *interleaving* (penyebaran) menggunakan deret Lucas.
3. Pihak yang dituju telah memiliki *carrier file* yang digunakan oleh pengirim

4. hasil yang diharapakan adalah didapatkan pola optimasi interleaving key untuk setiap *carrier file* yang akan disisipkan *file* pesan sehingga dicapai *level sequence* yang optimal dan nilai *fidelity* tetap terjaga kehandalannya.

Analisa simulasi ini tetap memiliki batasan masalah, yaitu:

1. *carrier file* yang digunakan pada laporan penelitian ini adalah *audio* yang berformat “WAV” sinyal monoponik dan *image digital* berformat “.GIF” sinyal monokrom.
2. Tidak membahas *steganalysis* terhadap metode steganografi yang digunakan.
3. Tidak membahas pengaruh jaringan terhadap pertukaran data. Atau dapat dikatakan jaringan dianggap ideal.
4. Data rahasia yang akan disisipkan adalah data berformat teks.
5. Pada pembangkitan sinyal *pseudo random noise*, digunakan transformasi kosinus diskrit yang bergantung pada hasil pembacaan *carrier file.*
6. Penilaian kualitas *fidelity* (kesetiaan data) dilakukan dengan dua metoda analisa, yaitu analisa subjektif dan objektif.
   a. Data analisa subjektif diperoleh dari hasil kuisioner terhadap 20 orang *responder* berdasarkan penilaian indera penglihatan dan pendengaran sehingga didapatkan nilai *Mean Opinion Score* (MOS).
   b. Data analisa objektif diperoleh dari hasil analisa *file* hasil dari aplikasi *steganography* menggunakan metoda *spread spectrum* berdasarkan parameter

Bit Error Rate (BER), *Symbol Error Rate* (SER), dan *Peak Signal to Noise Ratio*(SNR).

1.3 Tujuan

Tujuan dari laporan penelitian ini adalah :

1. Merancang dan mengimplementasikan perangkat lunak steganografi *audio* dan *image digital* menggunakan metoda *spread spectrum*, yaitu :
   a. Menyisipkan data rahasia pada *audio* WAV atau *image digital* GIF yang bertindak sebagai *carrier file.*
   b. Melakukan proses pengacakan posisi urutan pesan pada *pseudo random noise*.
2. Menganalisa kelebihan dan kekurangan *steganography* yang diimplementasikan pada *audio* dan *image digital* . Analisa yang dilakukan adalah berdasarkan pengaruh panjang data yang akan disisipkan, besar koefisien *chunk* pada *audio* WAV dan nilai *pixel* warna *carrier file* terhadap pembangkitan *pseudo random noise*.

Perubahan kualitas *file* sebelum dan sesudah dilakukan penyisipan :

a. Analisa rasio sinyal terhadap *noise* yang terjadi pada setiap *chunk* atau *pixel* setelah dilakukan penyisipan data rahasia ke dalam *carrier file* dengan cara menghitung PSNR (*Peak Signal-to-Noise Ratio*).
b. Analisa antara *carrier file* sebelum dan sesudah disisipi pesan rahasia dengan menghitung nilai *Symbol Error Rate* (SER) dan *Bit Error Rate* (BER).

c. Pengujian nilai MOS menggunakan indera pendengaran manusia terhadap *carrier file* sebelum dan sesudah proses *steganography*.

1.4 Metoda dan Penyelesaian Masalah

Pada proses pengerjaan laporan penelitian ini, langkah kerja yang ditempuh adalah:

1. Identifikasi permasalahan
2. Melakukan analisa latar belakang, rumusan masalah, dan tujuan akhir yang ingin dicapai.
3. Pengumpulan informasi dan Studi literatur
4. Mengumpulkan informasi dan mempelajari konsep *steganography* pada *audio* dan *image digital* menggunakan metoda *spread spectrum*, *carrier file audio* dengan *format* WAV dan *carrier file image* dengan *format* GIF, serta algoritma deret Fibonacci & Lucas.
5. Analisa perancangan aplikasi simulasi
6. Analisa kebutuhan aplikasi simulasi yang akan diterapkan dan melakukan perancangan aplikasi simulasi sesuai dengan judul laporan penelitian ini.
7. Pembangunan aplikasi simulasi
8. Merancang aplikasi simulasi berbentuk perangkat lunak yang bertindak sebagai aplikasi *steganography audio* dan *image digital* menggunakan metoda *spread spectrum*.

9. Melakukan simulasi proses *steganography audio* dan *image digital* lalu menganalisa respon yang terjadi akibat proses penyisipan pesan pada tiap jenis *carrier file*.
10. Menyusun laporan tertulis berdasarkan hasil penelitian yang dilakukan dan mengambil kesimpulan hasil dari penelitian, pemberian saran untuk pengembangan aplikasi simulasi analisa *fidelity* untuk *steganography audio* dan *image digital* yang dibangun ke depannya.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Dari hasil analisis perbandingan *fidelity* untuk *steganography* pola *audio* dan *image digital* dapat disimpulkan bahwa:

a. *Level sequence interleaving key* mempengaruhi besar ukuran pesan rahasia yang dapat disisipkan serta kualitas *stegfile*. Pada proses *steganography* menggunakan *level sequence* sebesar 32 dan 128, penyisipan tidak dapat terjadi. Hanya *file* pesan berukuran 3 Byte yang dapat disisipkan. *File* pesan yang memiliki ukuran lebih besar dari 3 Byte tidak dapat disisipkan karena tidak tersedia *slot* yang cukup untuk ditempati informasi dari *file* pesan.

b. Pada pengujian *carrier file* audio digital dengan *level sequence* sebesar 8, 32, dan 128 diperoleh nilai MOS tertinggi pada *sample rate* menengah dan *sample rate* tinggi yaitu sebesar 3,1 yang menyatakan bahwa *stegfile* hasil proses *steganography* dari *carrier file audio digital* tersebut memiliki tingkat distorsi *fair* (cukup). Atau dapat dikatakan noise pada *stegfile audio* terdeteksi dan sedikit mengganggu kualitas *stegfile*.

c. Pada pengujian *carrier file image digital* dengan level sequence sebesar 8, 32, dan 128 diperoleh nilai MOS tertinggi pada *file* “Malin.gif” dengan nilai 2,70 yang menyatakan bahwa *stegfile* hasil proses *steganography* dari *carrier file image digital* tersebut memiliki tingkat distorsi kurang dari standar penilaian untuk bisa dikatakan cukup baik.

d. Pada percobaan *steganography* untuk *carrier file audio digital*, besar *carrier file* yang disisipkan tidak berpengaruh pada kualitas *stegfile* berdasarkan nilai BER, dan SER yang didapat dari hasil percobaan bila *fidelity* dipandang sebagai suatu integritas data. Pada *carrier file audio digital* dengan nama *file* "bismillah.wav" nilai BER yang didapat sebesar 0,00038308 dan nilai SER sebesar 0,28343.

e. *Carrier file* yang cocok diterapkan pada *steganography* metoda *spread spectrum* adalah pola *audio* dengan nama *file* "bismillah.wav" menggunakan level *interleaving key* sebesar 8 dan frekuensi *sampling* 64 kHz. Meskipun pada pengukuran nilai PSNR didapatkan kualitas lebih baik pada *carrier file* pola *image* dengan nama file "Malin.GIF" menggunakan level *interleaving key* yang sama sebesar 34,2571 dB bila dibandingkan nilai PSNR dari *file* "bismillah.wav" sebesar 31,8468 dB, namun bila dilihat dari parameter BER dan SER yang menyatakan seberapa sering terjadinya *error carrier file* "bismillah.wav" masih lebih unggul tingkat *fidelity*-nya dibandingkan "Malin.GIF".

5.2. Saran

Steganography dengan metoda spread spectrum pada laporan penelitian ini masih dapat dikembangkan terutama pada jenis *interleaving key* yang digunakan untuk mengacak urutan pesan rahasia, dan metoda pembangkitan sinyal *pseudo random noise*.

Interleaving key dalam laporan penelitian ini menggunakan deret Lucas sehingga banyak menyia-nyiakan *slot* LSB yang dapat dilakukan proses penyisipan. Permasalahan yang masih dapat dievaluasi adalah gangguan nilai koefisien *pixel* atau *chunk* dari sinyal *pseudo random noise* melalui proses transformasi kosinus diskrit. Apabila digunakan teknik pembangkitan sinyal *pseudo random noise* yang lebih baik sehingga tidak mengurangi nilai *fidelity*, maka dapat dihasilkan kualitas *stegfile* yang lebih baik.

Pada laporan penelitian ini tidak menganalisa nilai recovery dengan kondisi pihak yang dituju tidak memiliki carrier file yang digunakan untuk *steganalys* sehingga memungkinkan sidapatkan recovery yang buruk. Maka dari itu cukup menarik bila ditambahkan aplikasi untuk melakukan toleransi kesalahan bit.

Daftar Pustaka

1. Anonim, ___, ___, [pdf], http://digilib.petra.ac.id/viewer.php?page=1&submit.x=0&submit.y=0&qual=high&fname=/jiunkpe/s1/info/2008/jiunkpe-ns-s1-2008-26404112-11149-algoritma_des-chapter2.pdf. diakses pada tanggal 22 November 2009.
2. Anonim, ___, *Discrete Cosine Transform*, [online], http://en.wikipedia.org/wiki/Discrete_cosine_transform. diakses pada tanggal 22 November 2009.
3. Anonim, ___, *Least Significant Bit*, [online], http://en.wikipedia.org/wiki/Least_significant_bit. diakses pada tanggal 21 Agustus 2009.
4. Anonim, ___, *Mean Opinion Score*, [online], http://en.wikipedia.org/wiki/Mean_Opinion_Score. diakses pada tanggal 3 Januari 2010.
5. Anonim, ___, *Sekali Lagi Tentang Format Image: GIF, JPEG, dan PNG*, [online], http://www.web4profit.com/artikel/desain_website/format-gif-jpeg-png.html. diakses pada tanggal 2 Januari 2010.
6. Anonim, ___, *Steganography*, [online], http://en.wikipedia.org/wiki/Steganography. diakses pada tanggal 21 Agustus 2009.
7. Dharma, Edi Muntina, 2008, *Teknik Steganography Pada Citra Digital Dengan Transformasi Wavelet*, [online], http://digilib.itb.ac.id/gdl.php?mod=browse&op=read&id=jbptitbpp-gdl-eddymuntin-29394, diakses pada tanggal 21 Agustus 2009.
8. Irianto, 2009, *irianto-report*, [pdf], ___, diakses pada tanggal 22 November 2009.
9. Krisnawati. 2007. "*Kompresi Citra RGB dengan Metode Kuantisasi*". Yogyakarta.
10. Marvel, M., Lisa, Retter, T., Charles, and Boncelet, Jr., Carles G. 1998.

"*Hiding information in images*". United State.

11. Munir, Rinaldi. 2004. *Steganografi dan Watermarking*. Institut Teknologi Bandung :Bandung.