SIMULASI DAN ANALISIS STEGANOGRAFI GANDA MENGGUNAKAN METODE DIAMOND ENCODING DAN DISCRETE WAVELET TRANSFORM (DWT)

To'at Waseso[1], Bambang Hidayat[2], Endang Budiasih Dra..[3]

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

---

Abstrak

Faktor keamanan data dalam proses pertukaran data antar perangkat informasi dalam suatu jaringan informasi menjadi sangat penting untuk diperhatikan seiring dengan kerahasiaan dari data yang dikirim. Salah satu teknik pengamanan data yaitu dengan teknik steganografi, namun penggunaan steganografi perlu dimodifikasi agar dapat meningkatkan keamanan pesan. Salah satu modifikasinya yaitu dengan menggandakan proses steganografi yang memungkinkan pengecohan terhadap pihak cracker.

Dalam tugas akhir ini, dilakukan dua kali penyembunyian pesan dengan teknik steganografi atau Steganografi ganda. Data rahasia yang disembunyikan merupakan text dengan format .txt yang disisipkan ke dalam data dengan format gambar bitmap (.bmp) dengan menggunakan metode Diamond Encoding yaitu citra cover dibagi menjadi blok sesuai parameter k dimana satu blok terdiri dari dua pixel yang bertetangga. Dengan metode ini akan dihasilkan diamond characteristic value (DCV) yang dihitung di dalam proses penyisipan dan ekstraksi. Setelah penyisipan pertama selesai, maka dilakukan penyisipan kembali terhadap file bitmap (stegoimage) yang berisi data rahasia ke dalam file dengan format audio (.wav) proses ini dilakukan dengan menggunakan penyisipan berdasarkan Discrete Wavelet Transform (DWT) yaitu menentukan representasi waktu dan skala dari sebuah sinyal menggunakan teknik pemfilteran digital dan operasi subsampling.

Dari hasil yang didapatkan, Sistem ini memiliki performansi yang cukup bagus dilihat dari nilai SNR stego audio yang bernilai 25.06 sampai dengan 40.15 dB. Sistem juga memiliki ketahanan yang tinggi terhadap serangan AWGN dilihat dari hasil ekstraksi pesan yang menghasilkan nilai CER=0%.

Kata Kunci : Steganografi Ganda, Diamond Encoding, Discrete Wavelet Transform (DWT)

Abstract

Security factor in the process of exchanging data between information devices in a network information is very important to be noted as the confidentiality of the data sent. One technique to support secure data is steganography technique, but the use of steganography need to be modified in order to improve the security of the message. One modification is to make double process of steganography that allows swindle against the cracker.

In this final project, done twice concealment message with steganography techniques or double steganography. Secret data .txt is inserted into image data with a bitmap format (. bmp) using the method of Diamond Encoding. The image cover is divided into blocks based on parameter k where one block consists of two neighboring pixels. This method will produce diamond characteristic value (DCV) that calculated in the process of insertion and extraction. After the completion of the first insertion, insertion is carried back to the bitmap file (stegoimage) that containing confidential data to the audio file format (.wav). The process is performed using insertion based on Discrete Wavelet Transform (DWT) that determines the timing and scale of a signal using digital filtering techniques and subsampling operations.

From the results obtained, this system has a good enough performance seen from the stego audio SNR value. The value is between 25.06-40.15 dB. The system also has a high resistance against AWGN attack seen from the extraction of messages that generate CERs value = 0%.

Keywords : Double Steganography, Diamond Encoding, Discrete Wavelet Transform (DWT)

BAB I

PENDAHULUAN

1.1 Latar Belakang

Faktor keamanan data dalam proses pertukaran data antar perangkat informasi sangat penting untuk diperhatikan seiring dengan maraknya penyalahgunaan data oleh pihak yang tidak diinginkan. Data penting yang seharusnya menjadi dokumen rahasia, malah menjadi obyek yang sering dicuri atau bocor kepada pihak-pihak yang tidak diinginkan karena kurangnya pengamanan data tersebut pada saat terjadi pertukaran data di media transmisi. Untuk meningkatkan keamanan data yang dipertukarkan antar perangkat informasi, perlu dilakukan suatu teknik pengamanan data, steganografi adalah salah satunya.

Teknik steganografi bertujuan untuk menyembunyikan informasi yang sebenarnya ke dalam sebuah data lain sehingga dapat mengelabuhi pihak penyerang bahwa pesan rahasia sesungguhnya berada di dalam sebuah data lain sehingga pesan tersebut tidak terlihat secara kasat mata. Akan tetapi penggunaan steganografi perlu dimodifikasi agar data rahasia memiliki tingkat keamanan yang tinggi. Teknik steganografi yang banyak diketahui saat ini hanya dilakukan sekali proses penyembunyian saja. Satu kali penyembunyian dengan metode steganografi terkadang tidak cukup mengingat semakin berkembangnya pengetahuan tentang metode steganografi yang memungkinkan terbongkarnya data rahasia oleh pihak yang tidak diinginkan. Untuk mengantisipasi hal tersebut, perlu dilakukan modifikasi yaitu salah satunya dengan menyembunyikan kembali pesan rahasia yang sebelumnya telah disembunyikan ke dalam sebuah data atau dengan melakukan penggandaan proses steganografi. Dengan demikian pihak penyerang tidak akan mengetahui pesan rahasia walaupun pihak-pihak tersebut mengetahui algoritma steganografi yang digunakan karena ekstraksi satu kali hanya akan membuka cover pesan rahasia.

Pada tugas akhir ini dilakukan dua kali proses steganografi dengan menggunakan dua metode yang berbeda di setiap *level* tahap steganografi. Pada

steganografi *level* pertama digunakan metode *diamond encoding*. Pemilihan metode ini berdasarkan pada penelitian sebelumnya yang memberikan hasil performansi steganografi yang tahan terhadap serangan sehingga pesan dapat diekstraksi sempurna dan tidak terdapat *error* [3]. Akan tetapi adanya kemungkinan pesan rahasia bocor jika hanya dilakukan satu kali proses steganografi, maka proses steganografi digandakan untuk mendapatkan tingkat keamanan pesan rahasia yang lebih tinggi. Oleh karena itu dilakukan penyisipan berlanjut dengan metode *discrete wavelet transform*. Kedua metode ini digabungkan untuk mengetahui performansi steganografi jika dilakukan modifikasi yaitu dengan cara menggandakan proses penyisipan dan ekstraksi sehingga didapatkan sistem yang lebih aman dan tahan terhadap serangan.

1.2 Tujuan

Tujuan dari Tugas Akhir ini adalah:

1. Dapat menyembunyikan pesan rahasia berupa teks dengan teknik steganografi ganda dengan metode *diamond encoding* dan *Discrete Wavelet Transform*.
2. Mengekstraksi kembali pesan rahasia awal berupa teks dengan error sekecil mungkin.
3. Menganalisis ketahanan sistem terhadap serangan AWGN (*Additive White Gaussian Noise*)
4. Mengukur performansi steganografi ganda yaitu pada *audio cover* yang telah dilakukan dua kali penyisipan dengan parameter SNR (*Signal to Noise Ratio*), waktu komputasi penyisipan, serta CER (*Character Error Ratio*) dari pesan yang diekstraksi. secara subjektif dilakukan analisis dengan MOS (*Mean Opinion Score*)

1.3 Perumusan Masalah

Dalam tugas akhir ini, hal-hal yang dibahas dapat dirumuskan sebagai berikut:

1. Bagaimana melakukan penyisipan pesan rahasia dengan penggandaan proses steganografi dengan metode *diamond encoding* dan *discrete wavelet transform* (DWT)?

2. Bagaimana cara mengekstraksi pesan asli sehingga diperoleh pesan rahasia?
3. Bagaimana performansi sistem dilihat dari SNR *stego audio*, waktu komputasi, dan CER?
4. Bagaimana pengaruh sistem jika diserang dengan AWGN pada level SNR AWGN yang berbeda beda?

1.4 Batasan Masalah

Untuk mempersempit cakupan masalah pada tugas akhir ini, maka ditentukan batasan masalah sebagai berikut:

1. Sistem yang dirancang hanya mengenai proses simulasi penyisipan pesan dan ekstraksi pesan tanpa melalui media transmisi
2. Cover terluar berupa audio dengan format.wav sedangkan cover gambar dalam berupa citra bitmap *grayscale* yang dilevelkan ke dalam 16-level *grayscale*
3. *File audio* berdurasi 30detik
4. Pesan rahasia berupa *text*
5. Stego audio hanya diperdengarkan untuk telinga manusia normal
6. Proses ekstraksi pesan membutuhkan *audio cover* asli (*Unblind* steganografi)
7. Parameter performansi yang diteliti dan dianalisis meliputi SNR, MOS, dan CER
8. Keseluruhan sistem diolah menggunakan MATLAB R2011b
9. Serangan berupa AWGN dengan SNR AWGN 20 dB, 30dB, 40dB, 50dB, dan 70 dB

1.5 Metodologi Penelitian

Metode penelitian yang digunakan dalam tugas akhir ini meliputi:

1. Melakukan *study literature* untuk mengumpulkan data-data dan mendapatkan informasi yang jelas yang dapat mendukung pembuatan dasar teori yang kuat dan metode yang digunakan
2. Merancang diagram alir sistem yang dijalankan di Matlab dan menganalisisnya
3. Menganalisis performansi sistem

4. Membuat kesimpulan berdasarkan hasil pengujian dari sistem yang dibuat
5. Menyusun laporan tugas akhir

1.6 Sistematika Penulisan

Tugas akhir ini disusun berdasarkan topik bahasan yang disusun secara sistematis sebagai berikut:

Bab I Pendahuluan

Bab ini membahas latar belakang, tujuan, perumusan dan batasan masalah, metodologi penelitian serta sistematika penulisan.

Bab II Dasar Teori

Bab ini membahas dasar-dasar teori yang mendukung penelitian tugas akhir ini.

Bab III Perancangan dan Simulasi Sistem

Bab ini menjelaskan proses desain dan realisasi sistem steganografi ganda menggunakan *diamond encoding* dan *discrete wavelet transform*.

Bab IV Pengujian Sistem dan Analisis

Bab ini membahas analisis dari hasil pengujian secara kualitatif dan kuantitatif. Analisis dilakukan terhadap parameter kinerja sistem yang damati berdasarkan keluaran yang dihasilkan oleh sistem.

Bab V Kesimpulan dan Saran

Bab ini membahas kesimpulan yang didapat dari hasil analisis terhadap sistem serta saran untuk memperbaiki sistem.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari analisis pada pengujian didapatkan kesimpulan sebagai berikut:

1. Nilai kualitas *audio stego* bergantung pada ukuran *cover* pertama yang digunakan yaitu *cover* gambar, bukan dari panjang karakter pesan yang digunakan. Semakin besar ukuran gambar, maka nilai SNR akan semakin kecil. Dari hasil pengujian didapatkan SNR *audio stego* yaitu 25.06 dB sampai dengan 40.15 dB, ini berarti *stego audio* dalam kualitas yang bagus.
2. Sistem Steganografi ganda pada tugas akhir ini tahan terhadap serangan AWGN, terbukti dari nilai CER yang menunjukkan angka 0% untuk serangan AWGN dengan SNR AWGN 20dB, 30dB, 40dB, 50dB, dan 70dB.
3. Waktu komputasi proses penyisipan dipengaruhi oleh media yang disisipkan. Semakin banyak jumlah yang disisipkan, semakin lama waktu komputasinya. Pada proses penyisipan pertama waktu komputasi dipengaruhi oleh panjang pesan rahasia, sedangkan pada penyisipan kedua, waktu komputasi dipengaruhi oleh ukuran *stego image* dari hasil proses penyisipan pertama. Dari total waktu penyisipan, penyisipan ke dua memberikan kontribusi sebesar 94.74%.
4. Hasil penilaian MOS terhadap *stego audio* menunjukkan kualitas *audio* hasil steganografi cukup hingga baik dengan nilai indeks diatas 3.84.

5.2 Saran

Setelah dilakukan Analisis terhadap metode yang digunakan dalam tugas akhir ini, maka dapat diperoleh beberapa saran:

1. Dilakukan perbaikan terhadap algoritma penyisipan *level* kedua sehingga dapat tahan terhadap serangan.

2. Proses steganografi dilakukan pada pesan yang berbeda seperti *video* dan atau *audio*.
3. Sistem dapat diimplementasiakan ke dalam bahasa pemrograman lain atau hardware sehingga dapat digunakan secara nyata.
4. Perlu dikaji lagi ketahanan sistem dengan serangan lain seperti *cropping*, dan atau *scaling*.
5. Untuk mendapatkan nilai MOS yang baik, sebaiknya kuisioner diisi oleh responden yang mengerti tentang sinyal *audio*.

DAFTAR PUSTAKA

[1] Berg G, Davidson, Ming-Yuan Dual, Paul G. 2003. *Searching For Hidden Messages: Automatic Detection of Steganography*. Washington: Computer Science Department, University at Albany

[2] Chao, Ruey-Ming**,** Wu**,** Hsien-Chu**,** Lee**,** Chih-Chiang and Chu Yen-Ping.2009. *A Novel Image Data Hiding Scheme with Diamond Encoding*. Taichung, Taiwan.

[3] Ginting, Bernard T.C.*"Steganografi Citra Digital dengan Diamond Encoding*". Tugas Akhir, Institut Teknologi Telkom Bandung, 2010.

[4] Goel, Dr. Anita. *Binary Arithmetic and Binary Coding Schemes*. Dyal Singh College, University of Delhi, India.

[5] K. K. Shukla, A. K. Tiwari.2013.*Efficient Algorithms for Discrete Wavelet Transform*. SpringerBriefs in Computer Science.

[6] Kurniawan, Erick, S.Kom, M.Kom.Slide:*"Suara dan Audio*".Yogyakarta:Universitas Kristen Duta Wacana (UKDW)

[7] Munir, Rinaldi Ir., MT.2004. *"Steganografi dan Watermarking"*. Bandung, Indonesia: Departemen Teknik Informatika ITB

[8] Nurjamillah, Siti.*"Simulasi dan Analisis Steganografi Audio dengan Convolutional Code dan Pemodelan Psychoaccoustic"*.Tugas Akhir, Institut Teknologi Telkom Bandung, 2013.

[9] Piarsa, I Nyoman.2011.*Steganografi Pada Citra JPEG Dengan Metode Sequential Dan Spreading*.Fakultas Teknik Universitas Udayana, Denpasar, Bali, Indonesia.

[10] Retnawati, Wirawan, Endang Widjiati.2009. *Kompresi Audio Secara Terdistribusi*
Pada Microphone Array. Surabaya, Indonesia.

[11] Sutoyo, T, dkk.2009.*Teori Pengolahan Citra Digital*.Yogyakarta:Andi.