

SIMULASI DAN ANALISIS STEGANOGRAFI GANDA MENGGUNAKAN METODE DISCRETE COSINE TRANSFORM

Bandung Prihanto¹, Bambang Hidayat², Endang Budiasih Dra.³

¹Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Perkembangan media digital yang sangat pesat, menyebabkan keamanan pengiriman informasi yang bersifat rahasia dirasa sangatlah penting. Hal ini dapat diatasi dengan menggunakan teknik steganografi. Steganografi merupakan teknik menyembunyikan pesan atau informasi ke dalam suatu file yang berupa teks, image, audio maupun video tanpa harus menunjukkan perubahan yang signifikan dari kualitas atau bentuk file yang disisipi pesan tersebut. Akan tetapi teknik steganografi sudah cukup diketahui banyak hacker. Untuk itu data rahasia lebih baik disisipkan lebih dari sekali, hal ini bisa digunakan mengecoh hacker yang menganggap steganografi hanya berlaku pada satu algoritma saja.

Pada tugas akhir ini telah dirancang dua algoritma steganografi, yang pertama menyisipkan pesan gambar ke dalam cover gambar kemudian cover gambar tersisip disisipkan ke dalam cover suara. Metode yang digunakan penulis untuk algoritma steganografi pada proses penyisipan pesan gambar rahasia ke dalam cover gambar yaitu dalam domain spasial, sedangkan algoritma steganografi pada proses penyisipan cover gambar tersisip ke dalam cover audio menggunakan metode Discrete Cosine Transform (DCT).

Dari hasil pengujian performansi sistem, untuk cover gambar dengan dimensi 256x256 piksel berhasil disisipkan pesan gambar rahasia dengan dimensi 32x32 piksel dan 48x48 piksel dan untuk cover audio dengan panjang 30 detik dapat disisipkan cover gambar tersisip dengan dimensi 256x256 piksel. Audio stego yang dihasilkan memiliki kualitas yang baik yaitu SNR >90 dB dan MSE <1x10e-04 serta pesan rahasia hasil ekstraksi memiliki SNR >50 dB, MSE mendekati 0 dan cukup kuat terhadap serangan AWGN dengan SNR AWGN >55 dB.

Kata Kunci : Steganografi, Cover image, Cover audio, DCT

Abstract

Development of digital media very rapidly, it's causing that security of delivery confidential information deemed very important. This can be overcome by using steganography techniques. Steganography is a technique to hide messages or information into a file in the form of text, image, audio and video without having to show a significant change of the quality or shape files which inserted the message. But enough is known steganographic techniques many hackers. For it is better classified data inserted more than once, it can be used to outwit hackers who consider steganography algorithms only apply to one only.

In this final project have designed two steganography algorithms, first insert the secret messages into the cover image and then cover images inserted into audio cover. The method used by the author for the steganographic algorithm embedding secret message into the cover image is an image in the spatial domain, while the steganographic algorithm embedding in cover images inserted into a cover audio using the Discrete Cosine Transform (DCT).

From the results of performance testing system, the cover image with dimensions 256x256 pixels successfully inserted secret picture message with dimensions of 32x32 pixels and 48x48 pixels, and length 30 seconds of audio cover can be pasted cover image inserted with the dimensions of 256x256 pixels. Stego audio produced are of good quality with SNR > 90 dB and MSE <1x10e-04 as well as the extraction of the secret message has SNR > 50 dB, the MSE is close to 0 and strong enough to attack AWGN AWGN with SNR > 55 dB.

Keywords : Steganography, Cover image, audio Cover, DCT.

BAB I

PENDAHULUAN

1.1. Latar Belakang

Semakin meningkatnya kegiatan manusia akan pengiriman data yang serba digital melalui jaringan internet, menyebabkan keamanan akan pengiriman informasi yang bersifat rahasia atau pribadi dirasa sangatlah penting. Apalagi pengiriman data pada institusi-institusi pemerintah yang menangani keamanan dan pertahanan negara. Hal ini merupakan ancaman bagi pihak yang mempunyai pesan rahasia tersebut, karena apabila pesan rahasia sampai ke tangan pihak yang tidak berwenang akan membahayakan keamanan dan merugikan yang lain. Oleh karena itu dibutuhkanlah teknik yang bisa menyembunyikan pesan rahasia ke dalam suatu file yang dapat diakses oleh semua orang seperti file gambar maupun suara, dengan syarat file yang disisipi tersebut tidak kelihatan bahwa di dalamnya terdapat pesan rahasia.

Munculnya masalah seperti ini, maka dikembangkanlah teknik *steganography* yang merupakan teknik menyembunyikan pesan atau informasi ke dalam suatu file yang berupa teks, *image*, *audio* maupun video tanpa harus menunjukkan perubahan yang signifikan dari kualitas atau bentuk file yang disisipi pesan tersebut. Akan tetapi teknik steganografi ini sudah diketahui banyak *hacker*. Untuk itu data rahasia harus disisipkan lebih dari sekali, hal ini bisa digunakan mengecoh *hacker* yang menganggap steganografi hanya berlaku pada satu algoritma saja.

Dengan adanya teknik *steganography* ini, maka keamanan dalam pengiriman data digital baik untuk institusi maupun masyarakat umum bisa terjamin. Hal ini dapat kita coba dalam penggunaan media online seperti jejaring social. Kita dapat saling bertukar data baik gambar, suara, maupun video yang dengan secara bebas dapat dilihat atau didengar oleh orang lain tanpa mereka sadari bahwa di dalam data yang mereka dengar atau lihat tersebut terdapat pesan rahasia.

Untuk mewujudkan keinginan dari uraian latar belakang di atas, maka penulis akan merancang dua algoritma simulasi untuk teknik steganografi. Dua algoritma yang dirancang adalah menyisipkan pesan gambar ke dalam cover gambar kemudian cover gambar tersisip disisipkan ke dalam cover suara.

1.2. Rumusan Masalah

Permasalahan yang dibahas dalam tugas akhir ini adalah :

1. Bagaimana menyembunyikan file pesan gambar rahasia ke dalam cover gambar.
2. Bagaimana menyembunyikan file cover gambar tersisip ke dalam file cover audio
3. Bagaimana algoritma untuk mengekstrasi pesan yang tersembunyi dalam *cover-object* tersebut.
4. Bagaimana kualitas hasil steganografi dan pesan gambar hasil ekstraksi yang telah di uji dengan noise Gaussian ditinjau dari nilai BER, SNR, dan MOS.

1.3. Batasan Masalah

Agar pembahasan materi yang dipaparkan pada tugas akhir ini lebih terarah, maka penulis perlu membuat batasan-batasan masalah. Adapun batasan-batasan masalah tersebut antara lain :

1. Pesan gambar rahasia berformat .jpeg BW dengan ukuran 32x32 dan 48x48 piksel.
2. Sinyal audio yang digunakan sebagai *cover-object* memiliki format .wav panjang 30 detik dengan frekuensi sampling 44100Hz jenis pop dan keroncong.
3. Gambar yang digunakan sebagai *cover-object* memiliki format .bmp grayscale(4level) dengan ukuran 256x256 piksel.
4. Digunakan metode penyisipan dalam domain spasial pada proses penyisipan pesan gambar ke dalam cover gambar dan metode DCT pada proses penyisipan cover gambar tersisip ke dalam cover audio.
5. Sistem tidak dirancang untuk membentuk ulang data cover pada proses ekstraksinya.

6. Pengujian standar terhadap system steganografi adalah dengan noise Gaussian yang dilakukan hanya pada cover audio tersisip/ stego audio.
7. Parameter hasil yang digunakan adalah waktu komputasi, MSE, SNR, dan MOS.
8. Simulasi dengan menggunakan program Matlab 2011b.

1.4. Tujuan

Tujuan tugas akhir ini adalah sebagai berikut :

1. Menyisipkan pesan gambar rahasia ke dalam cover gambar
2. Menyisipkan cover gambar tersisip ke dalam cover suara
3. Berhasil mengekstraksi pesan gambar rahasia yang sudah disisipkan
4. Sistem yang dirancang mampu bertahan terhadap serangan noise.

1.5. Metodologi Penelitian

Metode yang digunakan dalam tugas akhir ini adalah sebagai berikut :

1. Studi Literatur
Metode ini merupakan metode pembelajaran dengan kajian berbagai sumber pustaka baik berupa buku, jurnal ilmiah, maupun media elektronik.
2. Konsultasi dengan Dosen Pembimbing
Konsultasi dengan dosen pembimbing diperlukan untuk mengkaji dan merumuskan metode yang tepat untuk diimplementasikan kedalam sistem. Selain itu konsultasi juga bertujuan untuk memecahkan masalah yang terjadi selama pengerjaan tugas akhir ini.
3. Simulasi dilakukan dalam bentuk perancangan algoritma dengan menggunakan software matlab 2011b.

1.6. Sistematika Penulisan

Untuk memberikan gambaran mengenai tugas akhir ini secara sistematis, maka sistematika penulisan dapat diuraikan 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 tentang prinsip dasar steganografi, citra gambar, file audio, dan algoritma yang digunakan untuk metode steganografi pada software matlab.

BAB III PERANCANGAN SISTEM

Bab ini menjelaskan proses desain dan realisasi sistem steganografi.

BAB IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Bab ini membahas analisis hasil simulasi. Analisis dilakukan terhadap parameter kinerja system yang diamati setelah system diuji dengan noise AWGN pada stego audio.

BAB V PENUTUP

Berisi kesimpulan dari Tugas Akhir ini dan saran yang dapat digunakan untuk penelitian dan pengembangan lebih lanjut atau sebagai bahan referensi.



Telkom
University

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan yang dapat diambil dari tahapan perancangan hingga pengujian yang dilakukan pada sistem steganografi ganda ini adalah sebagai berikut :

1. Rancangan sistem steganografi ganda berhasil menyisipkan pesan gambar rahasia berukuran 32x32 piksel dan 48x48 piksel ke dalam cover gambar berukuran 256x256 piksel.
2. Rancangan sistem steganografi berhasil menyisipkan stego gambar ke dalam cover audio.
3. Proses ekstraksi pesan pada sistem steganografi ini tidak membutuhkan *cover* asli (*blind steganography*).
4. Keberhasilan sistem dalam menghasilkan audio stego yang memiliki nilai SNR yang baik dipengaruhi oleh jenis, ukuran pesan, ukuran cover gambar dan serangan berupa noise AWGN dengan SNR AWGN > 55 dB. Sistem ini berhasil mendapatkan nilai SNR audio stego sebesar > 90 dB dengan nilai MSE < 1x10E-04 dan kualitas perceptual audio stego dengan nilai MOS sebesar 4.06.
5. Sistem steganografi ganda yang dirancang berhasil mengekstraksi pesan gambar rahasia dengan baik, akan tetapi untuk serangan noise AWGN dengan SNR AWGN kurang dari 55 dB pesan gambar rahasia hasil ekstraksi sudah tidak bisa dikenali, yaitu dengan nilai SNR < 50 dB dan skala nilai MOS 1.

5.2. Saran

Penelitian lebih lanjut diharapkan dapat memperbaiki kekurangan yang ada dan diharapkan dapat mengembangkan yang apa yang telah dilakukan pada penelitian ini. Untuk itu disarankan hal-hal berikut :

1. Sistem bisa disimulasikan dan dianalisis dengan bahasa pemrograman yang lain seperti bahasa java, C.
2. Menambahkan sistem dengan *error correction*, misalnya BCH code sehingga *error* hasil pesan rahasia bisa diminimalisir.
3. Menambahkan sistem dengan enkripsi, misalnya AES jadi selain steganografi ganda maka steganografi juga di enkripsi sehingga sistem bisa lebih aman.



DAFTAR PUSTAKA

- [1] Alfatwa, Dean Fathoni.2007.”*Watermarking Pada Citra Digital Menggunakan Discrete Wavelet Transform*”.Bandung:Institut teknologi Bandung.
- [2] Anandika, Hari. 2012. *Perancangan dan Analisis Multiple Watermarking pada Citra Digital berbasis Iterative Threshold dan Deteksi Tepi*. Bandung: Institut Teknologi Telkom.
- [3] Burrus, C Sidney, Gopinath, Ramesh A., Guo, Haitao.1998.”*Introduction to Wavelet and Wavelet Transform*”.Prentice-Hall,Inc.
- [4] Dave, Preeti, Patel, Hardik.2012.”*Steganography Technique Based on DCT Coefficients*”. India: Shantilal Shah College.
- [5] Komputer, Wahana. 2003. *Memahami Model Enkripsi dan Security Data*. Yogyakarta: Andi.
- [6] Laboratory, DSP. 2011. *Audio Processing DCT-Based Audio Steganography*. Bandung: Institut Teknologi Telkom.
- [7] Mulyantini, Agustien. 2012. *Analisis Steganografi pada Citra Digital menggunakan DCT (Discrete Cosine Transform) dan Enkripsi AES*. Bandung: Institut Teknologi Telkom.
- [8] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit Informatika
- [9] Peranginangin, Kasiman. 2006. *Pengenalan Matlab*. Yogyakarta : Penerbit Andi.
- [10]Purnomo, Mauridhi Hery, Muntasa, Arif.2010.”*Konsep Pengolahan Citra Digital dan Ekstraksi Fitur*”.Edisi Pertama.Yogyakarta:Graha Ilmu
- [11]Putra, Darma. 2010. *Pengolahan Citra Digital*. Yogyakarta: Andi.
- [12]Putra, Hadi. 2009. *Macam Format Gambar Digital*. Diakses di <http://hady-putra.blogspot.com/2009/10/macam-format-gambar-digital.html>
- [13]Saputra, Erwan. 2011. *Analysis of Multipurpose Audio Watermarking with Vector Quantization (VQ) in Discreate Cosine Transform (DCT) Domain*. Bandung : Institut Teknologi Telkom