ANALISIS STEGANOGRAFI PADA CITRA DIGITAL MENGGUNAKAN DCT (DISCRETE COSINE TRANSFORM) DAN ENKRIPSI AES

Agustien Mulyantini[1], Bambang Hidayat[2], Rian Febrian Umbara[3]

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

Abstrak

Steganografi berasal dari bahasa Yunani yang berarti tulisan yang tertutup atau tulisan yang tersembunyi. Steganografi adalah seni atau ilmu menyembunyikan data rahasia kedalam suatu media lain yang tidak mencurigakan sehingga keberadaan dari data rahasia ini tidak diketahui oleh pihak lain. Media yang biasa digunakan dalam steganografi ini bisa beragam seperti citra digital, teks, audio maupun video.

Ada banyak metode steganografi yang digunakan salah satunya adalah Discrete Cosine Transform (DCT) dimana dalam proses penyembunyian berlangsung pada domain frekuensi yang mempunyai keuntungan lebih tahan daripada disembunyikan dalam domain ruang (spatial).

Pada tugas akhir ini digunakan citra sebagai objek dalam penelitian steganografi. Diperlukan 2 tipe citra yaitu citra cover yang digunakan sebagai media penyembunyian dan citra rahasia sebagai objek yang disembunyikan. Untuk memberikan keamanan yang lebih handal sistem steganografi ini akan dikombinasikan dengan kriptografi yaitu enkripsi Advance Encryption System (AES). Mulanya citra rahasia dienkripsi selanjutnya masuk ke proses utama yaitu penyisipan ke media penampungnya yaitu citra cover menggunakan metode DCT. Hasil akhir ini telah dianalisis performansinya menggunakan Mean Square Error (MSE), Peak signal to noise ratio (PSNR), Normalized Correlation (NC), dan Mean Opinion Score (MOS). Dimana parameter performansi tersebut dipengaruhi oleh nilai threshold yang digunakan. Nilai PSNR citra steganografi menunjukkan angka diatas 33 dB untuk semua nilai threshold. Dilakukan pula attacking berupa penskalaan, kompresi JPEG, crop, dan noise Gaussian.

Kata Kunci : Steganografi, Citra, DCT, AES

Abstract

Steganography is originated from Greek, which means closed or hidden writing. Steganography is the art or field to hide secret data to another unsuspicious media so teh data itself won't be recognised. The media can be used consists of digital image, text, audio, or video.

There's a lot of steganography method, one of them is Discrete Cosine Transform (DCT). In this method, hidden process happens in frequence domain, so that the result has better endurance than being hidden in spatial domain.

In this final project, image was used as steganography research's object. Two images were needed: cover image as covering media and secret image as the hidden object. For a better security, the steganography was combined with cryptography, specifically Advance Encyption System (AES). First, hidden image's encrypted, then inserted to the cover image using DCT. The final result's performance was analyzed using Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Normalized Correlation (NC), and Mean Opinion Score (MOS). The performance parameter were affectef by threshold used. Steganograpy image's PSNR result showed below 33 dB for all threshold value. Attacking using scaling, JPEG compression, crop, and Gaussian noise were also used.

Keywords : steganography, image, DCT, AES

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pertukaran informasi dan data merupakan suatu kebutuhan yang mendasar. Semakin maju teknologi akan beriringan juga dengan semakin mudahnya dalam pengaksesan informasi. Ditambah lagi dengan adanya Internet akan memberikan kebebasan bagi setiap orang untuk mendapatkan dan memberikan informasi. Kebebasan pertukaran informasi bisa disalahgunakan oleh oknum tertentu untuk kepentingannya sendiri sehingga kerahasiaan dan keamanan informasi menjadi suatu sorotan yang menarik.

Kini data ataupun informasi yang diakses bukan lagi dalam bentuk yang konvensional tapi sudah beralih ke data digital. Data digital (seperti teks, citra, audio, dan video) yang dipertukarkan tersebut sungguh sangat riskan mengalami penduplikasian, diproses sedemikian hingga disebarluaskan kembali. Untuk menghindari terjadinya hal tersebut maka diperlukan suatu sistem keamanan. Ada banyak cara yang digunakan untuk mengamankan suatu data digital misalnya dengan teknik kriptografi dan steganografi.

Dalam tugas akhir ini, penulis mengkombinasikan teknik kriptografi dengan steganografi dimana motode yang digunakan adalah AES untuk kriptografi dan DCT untuk steganografi. Tugas akhir ini merupakan pengaplikasian metode dari tugas akhir sebelumnya[2] yang menggunakan DCT 2-D pada citra digital metode *scrambling*. AES digunakan untuk mengenkripsikan data rahasia sehingga sulit untuk dipahami secara langsung. Namun akan memancing kecurigaan dari pihak luar karena data setelah enkripsi terlihat acak maka dari itu akan dilakukan teknik steganografi dengan metode DCT yang akan disisipkan ke dalam media baru yang akan menyembunyikan data rahasia yang asli. Dengan menggunakan kombinasi dari kriptografi dan steganografi ini, data rahasia akan lebih aman dari serangan pihak yang tidak berwenang.

1.2 Tujuan

Tujuan dari tugas akhir ini diantaranya :

1. Merancang suatu sistem steganografi citra digital menggunakan metoda *Discrete Cosine Transform* (DCT) dan enkripsi AES.
2. Menganalisis performansi dari sistem steganografi tersebut.
3. Menganalisis kualitas *output* yang dihasilkan dengan parameter MSE *(Mean Square Error*), PSNR *(Peak Signal to Noise Ratio*), NC (*Normalized Correlation)*, dan MOS (*Mean Opinion Score*).

1.3 Batasan Masalah

1. Simulasi dilakukan dengan menggunakan *software* MATLAB (R2008a)
2. Data *cover* menggunakan citra digital RGB dengan *format* *.bmp dengan ukuran 512 x 512 piksel.
3. Pesan rahasia yang disisipkan berupa citra digital biner ber*format* *.bmp dengan ukuran 128 x 128 piksel.
4. Sistem yang dirancang hanya digunakan untuk menangani proses penyisipan citra ke dalam citra dan mengekstraksinya kembali.
5. Parameter performansi yang dianalisis meliputi MSE, PSNR, NC dan MOS.

1.4 Perumusan Masalah

1. Bagaimana merancang suatu sistem steganografi pada citra digital dengan menggunakan metode DCT dan enkripsi AES?
2. Bagaimana menyisipkan citra ke dalam citra menggunakan sistem DCT dan enkripsi AES sehingga mempunyai keamanan yang handal dan orang tidak menyadari bahwa didalam citra tersebut ada pesan rahasia?
3. Bagaimana performansi citra digital setelah dilakukan proses steganografi?

1.5 Metoda penelitian

1. Melakukan studi literatur dengan mempelajari berbagai bahan dan data yang berkaitan dengan steganografi citra digital dan enkripsi AES. Pemahaman terhadap materi didapatkan dari buku, jurnal ilmiah serta situs-situs internet.

2. Perancangan, implementasi serta pengujian sistem steganografi citra digital dilakukan pada Matlab.
3. Menganalisis data yang telah didapatkan sesuai dengan parameter yang telah ditentukan.
4. Melakukan penyusunan laporan hasil penelitian yang telah dilakukan kemudian menarik kesimpulan serta saran dari hasil penelitian tersebut.

1.6 Sistematika penulisan

Terdapat beberapa topik bahasan yang disusun secara sistematis pada tugas akhir ini yaitu

Bab I Pendahuluan

Bab ini membahas tentang latar belakang, tujuan, batasan masalah, rumusan masalah, metode penelitian dan sistematika penulisan.

Bab II Dasar Teori

Pada bab ini dibahas mengenai konsep dasar steganografi, sejarah steganografi, rumus dasar matematika yang diterapkan pada sistem, pembahasan tentang metode steganografi yang telah ada serta penjelasan mengenai enkripsi AES.

Bab III Perancangan dan Simulasi Sistem

Bab ini memaparkan algoritma proses pembuatan sistem steganografi serta realisasinya.

Bab IV Pengujian Sistem dan Analisis

Bab ini berisi tentang keluaran yang ingin didapat dari sistem steganografi yang direncanakan.

Bab V Kesimpulan dan Saran

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari pengujian yang telah dilakukan pada penelitian kali ini dapat disimpulakan bahwa :

1. Sistem yang dibangun mampu melakukan proses steganografi dengan metode *Discrete Cosine Transform* (DCT) dan enkripsi AES.
2. Sistem ini dapat bertahan terhadap serangan noise *Gaussian* pada level SNR ≥ 70 dB dengan batas *threshold* ≥ 30. *Threshold* berperan pada kualitas dan tingkat ketahanan citra stego. Semakin tinggi nilai *threshold* maka semakin buruk kualitas citra stego namun akan semakin dapat bertahan terhadap serangan *noise Gaussian*.
3. Sistem ini tidak tahan terhadap gangguan geometris penskalaan, *cropping*, dan kompresi JPEG. Serangan penskalaan dan *cropping* ini pada prosesnya akan ada piksel yang dihilangkan dan ditambahkan pada citra stego, sedangkan pada proses steganografi ini setiap piksel pada citra stego sangat berperan sehingga apabila dilakukan serangan tersebut akan berakibat rusaknya citra rahasia terekstraksi. Kompresi JPEG menghilangkan informasi citra pada *subband* H_H sedangkan pada proses steganografi ini citra rahasia ditanamkan pada *subband* H_H. Dengan alasan inilah citra stego ini tidak tahan terhadap serangan kompersi JPEG.

5.2. Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah :

1. Menggunakan bahasa pemrograman lain seperti Java dan C++ atau yang lainnya.
2. Memilih algoritma penanaman yang lain yang lebih tahan terhadap serangan geometris.
3. Citra pesan yang digunakan dapat diganti dengan citra grayscale maupun RGB.
4. Lakukan pengujian yang lebih banyak terhadap jenis gangguan agar didapatkan citra stego yang tahan terhadap segala usaha untuk menghilangkan pesan rahasia.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2006. "*Kriptografi".* Bandung: Informatika Bandung.

[2] Febriansyah, Agus. 2009. *Blind Watermarking pada Citra Digital Metode Scrambling menggunakan Discrete Cosine Transform 2-D (DCT 2-D).* Bandung: Institut Teknologi Bandung.

[3] Mearns, Brian. 2008. *Introduction to Steganography and Steganalysis With a Focus on Least Significant Bit Embedding Techniques.* Department of Electric and Computer Engineering University of Boston.

[4] M Blackledge, J. 2010. *Covert Cryptography and Steganography.* Warsaw University of Technology Development Programme.

[5] Putra, Darma. 2010. *"Pengolahan Citra Digital"*. Yogyakarta : ANDI.

[6] Oktavianty, Yukie. 2011. *Simulation and Analysis High Security Steganography System Based On DWT (Discrete Wavelet Transform) With Baker Map Encryption For Digital Image.* Bandung : Institut Teknologi Telkom.

[7] Prasad, K.Munivara dkk. 2010. "High Secure Image Steganography in BCBS Using DCT and Fractal Compression". *Journal of Computer Science and Network Security.* 10 (4), 162-170.

[8] Ariyana, Yoki. *Advanced Encryption Standard (AES).* [Online]. Tersedia: http://www.p4tkipa.org [Oktober 2011]

[9] Wahyudi, Kunjung dan Parasian DP. Silitonga. 2008. *Aplikasi Kriptografi Untuk Pertukaran Pesan Menggunakan Teknik Steganografi dan Algoritma AES.* Institut Teknologi Adhi Tama Surabaya.

[10] Iwata, Motoi dan Akira Shiozaki. 2001. "Watermarking Method for Embedding Index Data into Images Utilizing of Wavelet Transform". *IEICE TRANS. FUNDAMENTALS.* E84-A (7), 1772-1778.

[11] Yuniati, Voni dkk. 2009. "Enkripsi dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File". Jurnal Informatika. 5 (1), 22-31.

[12] Wu, Ja-Ling dan Chiou-Ting Hsu. 1999. "Hidden Digital Watermarks in Images". *IEEE Transactions on Image Processing*. 8 (1), 58-68.

[13] Buchholz, Jörg J. 2001. *MATLAB Implementation of The Advanced Encryption Standard.* [Online]. http://buchholz.hs-bremen.de [Oktober 2011]