

SIMULASI DAN ANALISIS PENGAMANAN PESAN TEKS PADA CITRA DIGITAL BERDASARKAN STEGANOGRAFI MENGGUNAKAN DWT (DISCRETE WAVELET TRANSFORM)

Vika Fatwa Onistyami¹, Bambang Hidayat², Dea³

¹Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Pertukaran informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Seiring dengan perkembangan tersebut kejahatan informasi juga turut berkembang, sehingga keamanan dan kerahasiaan informasi yang dikirimkan tidak terjaga. Steganografi berasal dari bahasa Yunani, yang berarti tulisan tersembunyi. Steganografi adalah seni atau ilmu menyembunyikan pesan rahasia kedalam media lain yang tidak mencurigakan sehingga pesan rahasia tersebut tidak diketahui oleh orang yang tidak berkepentingan. Banyak metode yang dapat digunakan pada steganografi, salah satunya metode DWT (Discrete Wavelet Transformation) yang membagi citra menjadi subband yang memiliki frekuensi tinggi dan frekuensi rendah.

Tugas akhir ini telah membuat sebuah teknik penyisipan data berupa teks dengan metode Discrete wavelet Transform (DWT). Tujuan utama dari tugas akhir ini adalah untuk menyembunyikan pesan rahasia yang disisipkan kedalam sebuah citra digital. Untuk meningkatkan sistem keamanan, pesan rahasia yang disisipkan dienkripsi terlebih dahulu menggunakan Advanced Encryption Standard (AES) yang merupakan enkripsi terbaik saat ini menurut NIST (National Institute Standards and Technology) dan dilakukan encoding menggunakan convolutional code. Pada sisi penerima, maka proses tersebut akan dibalikkan untuk mendapatkan secret message.

Dari hasil penelitian, sistem steganografi menggunakan DWT menghasilkan performansi imperceptibility antara citra cover dan citra stego sangatlah mirip. Kesimpulan ini ditunjukkan dengan hasil nilai PSNR sebesar 85,7921 dan nilai MSE sebesar 0,00017134 pada citra cover yang disisipi pesan sepanjang 33 karakter. Performansi robustness pada citra stego mempunyai nilai BER sebesar 0 (nol), artinya tidak ada bit eror dalam mengekstrak.

Kata Kunci : steganografi, keamanan dan kerahasiaan informasi , discrete wavelet transform

Abstract

Information exchange is growing quickly and provides a major influence for human life. Along with this development of crime information were also developed, so that the security and confidentiality of information transmitted is not safe. Steganography is originated from Greek, which means hidden writings. Steganography is the art or field to secret messages to another unsuspecting media so the message itself won't be recognized. There's a lot of steganography methods, one of them is DWT (Discrete Wavelet Transform) which divides the image into subbands which have high frequency and low frequency.

This final project made the data insertion technique of text message using Discrete Wavelet Transform (DWT). The main objective of this final project is to hide important information which it will be inserted to the digital image. For a better security, the secret messages are encrypted using the Advanced Encryption Standard (AES) which is the best encryption at this time according to NIST (National Institute Standards and Technology) and encoding using convolutional code. On the receiver side, then the process will be reversed to get the secret message.

The research says, steganography system using DWT gives the imperceptibility performance between cover image and stego image is very similar. The conclusion obtained from PSNR value of 85,7921 and MSE of 0,00017134 on the cover image insert with message 33 characters. Robustness performance for stego image the value of BER is 0 (zero), the meaning is there is no bit error in extraction.

Keywords : Steganography, Security and confidentiality information, discrete wavelet transform.

BAB I PENDAHULUAN

1.1 Latar Belakang

Kejahatan dalam pengiriman pesan baik itu berupa teks, gambar, suara ataupun video sangat sering terjadi. Setiap orang sudah tidak bisa merasakan kenyamanan dalam berkomunikasi karena pesan yang mereka kirimkan sewaktu-waktu bisa saja diketahui ataupun diduplikasi oleh pihak-pihak yang tidak berkepentingan. Jumlah penyusup (*hacker*) dan perusak (*cracker*) yang semakin banyak juga menjadi penyebab diperlukannya suatu cara untuk mengamankan pesan agar hanya pengirim dan penerima saja yang mengetahui isi pesan rahasia tersebut. Ada banyak cara yang digunakan untuk mengamankan pesan salah satunya adalah teknik steganografi.

Steganografi adalah seni atau ilmu menyembunyikan pesan rahasia kedalam media lain yang berupa teks, gambar, suara ataupun video, yang tidak mencurigakan sehingga pesan rahasia tersebut tidak diketahui oleh orang yang tidak berkepentingan. Pesan teks dan gambar merupakan suatu informasi yang sering dipertukarkan dalam kehidupan sehari-hari. Hal inilah yang mendasari untuk menggunakan pesan teks sebagai informasi yang akan disembunyikan (*secret message*) dan gambar sebagai media penyimpanannya (*citra cover*).

Pada tugas akhir sebelumnya menggunakan metode optimasi *harmony search* dan *S-Transform* dimana penyisipannya berdasarkan penempatan *window Gaussian* berskala yang menyediakan resolusi yang bergantung pada frekuensi. Pada tugas akhir ini metode yang digunakan adalah *Discreet Wavelet Transform* (DWT), yang membagi citra menjadi subband-subband yang memiliki frekuensi tinggi dan frekuensi rendah. Namun untuk lebih meningkatkan keamanan, akan dilakukan enkripsi dan *channel coding* terlebih dahulu.

1.2 Tujuan

Adapun tujuan dari tugas akhir ini adalah

- a. Merancang suatu sistem steganografi pada citra digital menggunakan metode DWT.
- b. Mengalisis performansi dari sistem steganografi tersebut.
- c. Menganalisis kualitas output yang dihasilkan menggunakan PSNR, MSE dan MOS

1.3 Batasan Masalah

Tugas akhir ini akan membatasi permasalahan pada poin-poin berikut ini.

- a. Simulasi dilakukan menggunakan *software* MATLAB R2009a.
- b. Pesan rahasia yang disisipkan berupa teks dengan panjang maksimal 1632 karakter.
- c. Kapasitas citra *cover* yang digunakan adalah 1024x1024 piksel.
- d. Citra *cover* berformat Bitmap.
- e. Sistem yang dirancang hanya digunakan untuk menangani proses penyisipan teks ke citra dan mengekstraksinya lagi.
- f. Digunakan metode AES untuk melakukan enkripsi pada pesan rahasia sebelum disisipkan.
- g. Melakukan *channel coding* hanya pada pesan rahasia yang telah di enkripsi.
- h. Parameter performansi yang dianalisis meliputi Waktu Komputasi, MSE, PSNR, MOS dan BER.
- i. Pengujian standar terhadap sistem steganografi adalah *noise* Gaussian, rotasi, dan *resize*.

1.4 Perumusan Masalah

Beberapa permasalahan pada tugas akhir dapat diformulasikan sebagai berikut.

- a. Bagaimana merancang suatu sistem steganografi pada citra digital menggunakan metode DWT?
- b. Bagaimana performansi citra digital setelah dilakukan proses steganografi?
- c. Bagaimana menyisipkan pesan teks ke dalam citra digital menggunakan DWT agar *output* yang dihasilkan sama seperti citra asli sebelum di sisipin pesan teks?

1.5 Metode Penelitian

Penelitian ini dilakukan dengan metode-metode sebagai berikut.

- a. Studi literatur yaitu mempelajari berbagai macam literatur yang berkaitan dengan tugas akhir penulis. Pemahaman materi didapat dari buku, jurnal ilmiah dan situs-situs di internet.
- b. Diskusi dengan pembimbing mengenai hasil analisis data-data yang diperoleh dari studi literatur.
- c. Perancangan, simulasi serta pengujian dilakukan dengan MATLAB.
- d. Penyusunan laporan Tugas Akhir.

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

Bab ini membahas mengenai teori dasar yang mendasari dan mendukung penelitian Tugas Akhir ini.

BAB III PERANCANGAN DAN IMPLEMENTASI

Bab ini membahas tentang proses desain dan simulasi program pengamanan pesan teks dengan metode *discrete wavelet transform*.

BAB IV PENGUJIAN SISTEM DAN ANALISIS HASIL

Bab ini membahas analisis hasil simulasi. Analisis dilakukan terhadap parameter kinerja sistem yang diamati setelah sistem diuji dengan *noise* dan teknik serangan geometris.

BAB V PENUTUP

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

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari pengujian dan analisis sistem yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut :

1. Panjang *secret message* yang disisipkan pada citra *cover* mempengaruhi waktu penyisipan. Semakin panjang *secret message* yang disisipkan maka semakin lama waktu yang diperlukan untuk penyisipan.
2. Semakin panjang *secret message* maka waktu yang di butuhkan untuk proses ekstraksi akan semakin lama.
3. Panjang *secret message* yang disisipkan mempengaruhi kualitas citra stego. Semakin panjang *secret message* yang disisipkan maka semakin besar pula tingkat kesalahan/eror yang terjadi sehingga kualitas citra stego semakin turun.
4. Citra stego tahan terhadap serangan *resize* dengan cara memperbesar ukuran citra stego, namun tidak tahan terhadap serangan *resize* dengan cara memperkecil ukuran citra stego. Hal ini dibuktikan dengan nilai MSE hasil serangan memperbesar jauh lebih kecil dibanding dengan memperkecil.
5. Citra stego tahan terhadap serangan rotasi, hal ini terbukti pada nilai PSNR hasil serangan rotasi sebesar 90, 180 dan 270 derajat sama dengan nilai PSNR citra stego tanpa serangan.
6. Serangan *noise* Gaussian pada citra stego di pengaruhi oleh nilai *sigma*, semakin besar nilai *sigma* maka semakin besar pula nilai MSE sehingga tingkat kesalahan/eror semakin besar.

5.2 Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah :

1. Menggunakan algoritma kriptografi asimetrik seperti RSA yang di padukan dengan teknik steganografi agar pesan yang disisipkan lebih terjamin tingkat keamanannya.
2. Memilih metode penyisipan lain yang di kombinasi dengan Convolutional Code agar dapat bekerja secara maksimal sehingga pesan terekstraksi akan lebih baik pada serangan *noise* Gaussian ataupun serangan yang lainnya.
3. Menerapkan sistem steganografi dan kriptografi sehingga keamanan *secret message* lebih terjamin. Oleh karena itu untuk kedepannya sistem ini dapat diterapkan dan dikembangkan lagi agar kamanan pesan yang disisipkan lebih terjamin.

DAFTAR PUSTAKA

- [1] Buchholz, Jorg J. 2001. *"Matlab Implementation of the Advanced Encryption Standard"*.
- [2] Erika Kusumasari Rosita, Suwadi, Achmad Ansori. *"Implementasi Convolutional Code dan Viterbi pada DSK TMS320C6416T "*. Surabaya : Institut Teknologi Sepuluh Noverber.
- [3] Humaira, Ananstasia. 2012. *"Analisis Penggunaan Metode Optimasi Harmony Search Pada Steganografi Citra Digital Berbasis S-Transform"*. Bandung : Institut Teknologi Telkom.
- [4] Intel Corporation. 2008. *"Advance Encryption Standard (AES) Instructions Set".White Paper.*
- [5] Kuhn, Volken. 2009. *"Introduction into Error Correcting Code"*. Institute of Communications Engineering.
- [6] Liu, Er. 2004. *"Convolutional Coding & Viterbi Algorithm"*. Helsinki University of Technology.
- [7] Meylani, Linda. 2010. *"Diktat Kuliah Sistem Komunikasi IP"*. Bandung : Institut Teknologi Telkom Bandung.
- [8] Merry, R.J.E.2005. *"Wavelet Theory and Application"*. Department of Mechanical Engineering Eindhoven University of Technology . DCT 2005.53
- [9] Mulyantini, Agustien. 2012. *"Analisis Steganografi pada Citra Digital menggunakan DCT (Discrete Cosine Transform) dan Enkripsi AES"*. Bandung: Institut Teknologi Telkom.
- [10] Munir, Rinaldi. 2006. *"Kriptografi"*. Bandung : Informatika Bandung.
- [11] Putra, Darma.2010. *"Pengolahan Citra Digital"*. Yogyakarta : Andi.
- [12] Sirait, Hasanuddin. *"Teori Dasar Citra Digital"*. Slide. Di-download 30 September 2012.
- [13] Vidyasagar M. Potdar, Elizabeth Chang. 2004. *"Grey Level Modification Steganography for Secret Communication"*. Australia : School of Information System, Curtin University of Technology.
- [14] Voni Yuniati, Gani Indriyanta, Antonius Rachmat C. 2009. *"Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jenis File"*. Jurnal Informatika. 5 (1), 22-31