SIMULASI DAN ANALISIS STEGANOGRAFI CITRA DIGITAL MENGGUNAKAN METODE ADVANCED ENCRYPTION STANDARD DAN BCH CODE

Ni Made Lidya Dewi Aristya[1], Bambang Hidayat[2], Rian Febrian Umbara[3]

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

Abstrak

Steganografi merupakan teknik menyembunyikan pesan ke dalam media lain sehingga keberadaan pesan tidak diketahui oleh orang lain. Pesan yang disisipkan ini dapat berupa tulisan, citra, suara, maupun video. Media yang disisipi (cover) pun dapat berupa tulisan, citra, suara, maupun video.

Dalam tugas akhir ini telah disimulasikan steganografi citra rahasia ke dalam media (cover) yang juga adalah citra digital. Pada penelitian yang telah dilakukan sebelumnya[8], teknik steganografi masih memiliki kekurangan, yaitu rusak/hilangnya pesan rahasia yang disisipkan akibat gangguan selama proses pengiriman/transmisi data. Oleh karena itu, pada tugas akhir ini dilakukan penggabungan metode enkripsi dan juga metode koreksi error untuk meningkatkan kualitas dan performansi steganografi. Metode enkripsi yang digunakan yaitu Advanced Encryption Standard (AES). Sedangkan untuk meminimalkan kesalahan dari data yang diterima, digunakan teknik deteksi dan koreksi error BCH Code.

Hasil yang telah diperoleh yaitu, citra rahasia yang dikirim oleh pengirim memiliki BER minimal hingga 0 dan nilai PSNR maksimum tak terhingga setelah diuji dengan noise Gaussian, noise Salt & Pepper, rescaling dan cropping. Sedangkan nilai PSNR citra steganografi yang didapat adalah di atas 287 dB dengan nilai MOS 4.6 - 4.7 yang merupakan rata-rata hasil survei kepada 30 orang pengamat.

Kata Kunci : steganografi, citra digital, Advanced Encryption Standard (AES), BCH Code

Abstract

Steganography is a technique to hide messages in other media so that the existence of the message is not known by others. Messages which are inserted can be a text, image, audio, and video. Cover media also can be a text, image, audio, and video.

In this final assignment, has been simulated steganography using digital image as a cover and a secret message. In the research that has been done before[8], steganography technique still has shortcomings, such as the damaged/loss of secret message because of disturbance during the process of sending / transmitting data. Therefore, in this final assignment, had been done research which merge the encryption method and error correction method to improve the quality and performance of steganography. The encryption method used is the Advanced Encryption Standard (AES). Meanwhile, to minimize the error of the received data, is used error detection and correction technique, BCH Code.

The results that have been obtained are the secret image sent by the sender has minimal BER to 0 and maximum PSNR to infinity after tested by Gaussian noise, Salt & Pepper noise, rescaling and cropping. While the PSNR value for steganography image is above 287 dB with MOS value 4.6 - 4.7 which is the average of the results from a survey to 30 observers.

Keywords : steganography, digital image, Advanced Encryption Standard (AES), BCH Code

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi internet yang sangat pesat membuat komunikasi dan pertukaran informasi antara pihak pengirim dan penerima menjadi lebih cepat dan mudah. Namun pengiriman data jarak jauh melalui gelombang radio maupun media lain, terutama media internet, yang digunakan masyarakat luas sangat memungkinkan pihak lain menyadap dan mengubah data yang dikirimkan. Perlu disadari bahwa banyak sekali ancaman terhadap keamanan dan kerahasiaan data yang mungkin akan mengganggu kita. Jumlah penyusup *(hacker)* dan perusak *(cracker)* yang banyak juga menjadi penyebab diperlukannya suatu cara untuk mengamankan data agar hanya pengirim dan penerima saja yang mengetahui isi data rahasia tersebut. Steganografi merupakan teknik menyembunyikan pesan ke dalam media lain sehingga keberadaan pesan tidak diketahui oleh orang lain[5]. Pesan yang disisipkan ini dapat berupa tulisan, citra, suara, maupun video. Media yang disisipi *(cover)* pun dapat berupa tulisan, citra, suara, maupun video.

Pada perkembangannya, teknik steganografi ini banyak dikombinasikan dengan berbagai metode enkripsi untuk lebih dapat meningkatkan kualitas dan performansi steganografi. Pengkombinasian ini biasanya disebut dengan *Hybrid Steganography*. Pada penelitian yang telah dilakukan sebelumnya[8], metode *Hybrid Steganography* juga masih memiliki kekurangan, yaitu rusak/hilangnya pesan rahasia yang disisipkan akibat gangguan selama proses pengiriman/transmisi data, baik gangguan yang terjadi pada kanal transmisi maupun serangan geometris pada citra yang dilakukan secara sengaja oleh manusia. Oleh karena itu, dalam tugas akhir ini dilakukan penelitian yang menggabungkan metode enkripsi dan juga metode *error correction* pada citra rahasia yang disisipkan. Metode enkripsi yang digunakan yaitu *Advanced Encryption Standard* (AES). Sedangkan untuk meminimalkan kesalahan dari data yang diterima, digunakan teknik deteksi dan koreksi *error* BCH *Code*. Sistem steganografi yang disimulasikan pada tugas akhir ini menggunakan citra digital sebagai *cover* dan juga pesan rahasianya.

1.2 Rumusan Masalah

Dari latar belakang yang telah disampaikan sebelumnya, maka dapat dijabarkan beberapa rumusan masalah yang dibahas pada Tugas Akhir ini, yaitu:

1. Bagaimana penerapan metode enkripsi dan dekripsi *Advanced Encryption Standard* (AES) pada citra rahasia yang disisipkan?
2. Bagaimana merancang dan mengimplementasikan sebuah sistem untuk melakukan steganografi dengan BCH *encoding* di sisi pengirim dan mengekstraksi kembali citra rahasia yang disisipkan serta melakukan BCH *decoding* di sisi penerima?
3. Bagaimanakah kualitas citra hasil steganografi dan citra hasil ekstraksi yang telah diuji dengan *noise* Gaussian, *noise* Salt & Pepper, *rescaling*, dan *cropping* ditinjau dari nilai BER, PSNR, dan MOS?

1.3 Tujuan

Tujuan tugas akhir ini adalah untuk menyisipkan citra rahasia ke dalam sebuah *cover* citra digital, lalu melakukan metode enkripsi untuk menjamin kemananan data dan mengkodekannya agar citra rahasia yang diterima oleh penerima dapat diminimalisir kesalahannya.

1.4 Batasan Masalah

Beberapa batasan masalah pada penelitian Tugas Akhir ini adalah:

1. Ukuran/kapasitas citra *cover* yang digunakan adalah 1024x1024 piksel.
2. Ukuran/kapasitas citra rahasia yang digunakan adalah 32x32 piksel.
3. Citra cover adalah citra *grayscale* berformat Bitmap, sedangkan citra rahasia adalah citra biner (BW *image*) yang juga berformat Bitmap.
4. Digunakan metode *joint* DWT-DCT dalam proses penyisipan.
5. Metode deteksi dan koreksi *error* yang digunakan adalah BCH *Code* (15,5) dengan kemampuan koreksi 3 bit dari 5 bit masukan.
6. Pengujian standar terhadap sistem steganografi adalah dengan *noise* Gaussian, *noise* Salt & Pepper, *rescaling*, dan *cropping*.
7. Parameter hasil yang digunakan adalah BER, PSNR, dan MOS.
8. Sistem disimulasikan menggunakan MATLAB R2011b.

1.5 Metodologi Penelitian

Dalam Tugas Akhir ini digunakan metode simulasi dengan *software* Matlab R2011b untuk merancang sebuah sistem yang dapat melakukan steganografi, proses enkripsi dan dekripsi AES, proses *encoding* dan *decoding* BCH, serta proses ekstraksi.

1.6 Sistematika Penulisan

Tugas akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis sebagai berikut :

Bab I PENDAHULUAN

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

Bab II DASAR TEORI

Bab ini membahas dasar teori steganografi, citra digital, analisis matematika, dan algoritma yang digunakan dalam metode AES dan BCH *Code*.

Bab III PERANCANGAN DAN IMPLEMENTASI

Bab ini menjelaskan proses desain, realisasi sistem, jenis-jenis *attack* yang digunakan, dan parameter pengujian.

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 yang telah dilakukan pada penelitian kali ini, dapat disimpulkan bahwa:

1. Sistem yang dibangun mampu melakukan proses steganografi dengan metode AES dan BCH *Code*.
2. Citra *cover* harus berukuran lebih besar minimal 2 kali lipat dari citra pesan, karena sifat BCH *Code* akan memperpanjang bit citra pesan, tergantung dari jumlah kemampuan koreksi yang diinginkan.
3. Citra rahasia hasil ekstraksi di sisi penerima memiliki BER minimal hingga 0 dan nilai PSNR maksimum tak terhingga setelah diuji dengan *noise* Gaussian, *noise* Salt & Pepper, *rescaling* dan *cropping*. Sedangkan nilai PSNR citra steganografi yang didapat adalah di atas 287 dB dengan nilai MOS 4.6 - 4.7 yang merupakan rata-rata hasil survei kepada 30 orang pengamat.
4. Sistem dengan BCH *Code* ini bekerja secara signifikan. Dapat bertahan dengan baik terhadap serangan *noise* maupun serangan geometris pada skala yang cukup kecil. Namun saat *error* yang terjadi melebihi kemampuan koreksi *error* yang digunakan, penggunaan BCH *Code* bahkan dapat lebih buruk daripada yang tidak.

5.2 Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah:

1. Mengaplikasikan steganografi pada *hardware*, misal FPGA, agar prosesnya dapat lebih cepat.
2. Memilih metode penyisipan lain yang jika dikombinasikan dengan BCH *Code*, dapat bekerja lebih maksimal sehingga hasil pesan terekstraksi akan lebih baik dan akurat pada serangan *noise* maupun serangan geometris dalam intensitas yang sangat besar.

DAFTAR PUSTAKA

[1] Amirgholipour, Saeed K dan Naghsh-Nilchi, Ahmad R. 2009. *Robust Digital Image Watermarking Based on Joint DWT-DCT*. International Journal of Digital Content Technology and its Applications, Volume 3, Number 2.

[2] Anandika, Hari. 2012. *Perancangan dan Analisis Multiple Watermarking pada Citra Digital berbasis Iterative Threshold dan Deteksi Tepi*. Bandung: Institut Teknologi Telkom.

[3] Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi.* Yogyakarta: Andi.

[4] Buchholz, Jorg J. 2001. *Matlab Implementation of the Advanced Encryption Standard.*

[5] Calvianty, Intan Yusantina. 2009. *Multiple Watermarking pada Citra Medis pada Domain Wavelett Menggunakan BCH Encoding.* Bandung: Institut Teknologi Telkom.

[6] Emy. 2007. http://elista.akprind.ac.id/upload/files/4596_Pertemuan_8.pdf. Diakses pada 31 Januari 2013, pukul 23.24 WIB.

[7] Komputer, Wahana. 2003. *Memahami Model Enkripsi dan Security Data.* Yogyakarta: Andi.

[8] Lin, Shu. 1970. *An Introduction to Error Correcting Codes*. New Jersey: Prentice-Hall, Inc. Englewood Cliffs.

[9] Lin, Shu / Daniel J. Costello, Jr. 1983. *Error Control Coding: Fundamentals and Applications.* New Jersey: Prentice-Hall, Inc. Englewood Cliffs.

[10] Mulyantini, Agustien. 2012. *Analisis Steganografi pada Citra Digital menggunakan DCT (Discrete Cosine Transform) dan Enkripsi AES.* Bandung: Institut Teknologi Telkom.

[11] Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit Informatika

[12] Paar, Christof and Jan Pelzi. 2009. *Understanding Cryptography Chapter 4: The Advanced Encryption Standard (AES)*. www.crypto-textbook.com

[13] Putra, Darma. 2010. *Pengolahan* Citra Digital. Yogyakarta: Andi.

[14] Putra, Hadi. 2009. *Macam Format Gambar Digital*. Diakses di http://hady-putra.blogspot.com/2009/10/macam-format-gambar-digital.html pada 7 Maret 2012 pukul 19.25