SISTEM KEAMANAN DATA MENGGUNAKAN SPREAD SPECTRUM IMAGE STEGANOGRAPHY (SSIS) DAN ALGORITMA KRIPTOGRAFI DES (DATA SECURITY SYSTEM USING SPREAD SPECTRUM IMAGE STEGANOGRAPHY (SSIS) AND DES CRYPTOGRPHY ALGORITHM)

Chaeriah Bin Ali Wael[1], -[2]

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

Abstrak

Steganography merupakan suatu teknik berkomunikasi dimana informasi disembunyikan pada media pembawa seperti citra, suara atau video tanpa memberikan perubahan yang berarti pada media tersebut. Berbeda dengan steganography yang menyembunyikan keberadaan informasi, kriptografi hanya menyembunyikan arti atau isi dari sebuah informasi. Kedua teknik ini dapat digabungkan sehingga menghasilkan informasi yang semakin sulit dilacak. Sistem yang akan dirancang ini meggunakan teknik image steganography dengan data digital yang disisipkan pada citra cover berupa teks (.txt) yang telah dienkripsi terlebih dahulu menggunakan algoritma kriptografi DES.

SSIS menggunakan metode spread spectrum, dimana informasi yang akan disisipkan ke citra cover disebar ke dalam noise yang memiliki band frekuensi yang lebar. Noise inilah yang ditambahkan ke dalam citra cover. Sebagai antisipasi terjadi error selama proses transmisi, digunakan teknik Error Control Coding (ECC) yang terdiri dari enkoder konvolusi di transmitter dan dekoder yang menggunakan algoritma viterbi di receiver.

Dari simulasi yang dilakukan, diketahui bahwa tingkat imperceptibility citra stego yang dihasilkan pada simulasi I (hanya untuk disimpan) tidak dipengaruhi oleh kriteria citra cover (low detail, medium detail, high detail) tapi dipengaruhi oleh jumlah bit yang disisipkan per tiap píksel citra cover. Kapasitas maksimum citra cover pada simulasi II, selain dibatasi oleh ukuran citra cover itu sendiri, juga dibatasi oleh jumlah code rate dari kode konvolusi yang digunakan dan level kuantisasi. Tingkat imperceptibility citra stego pada simulasi II dipengaruhi oleh kriteria citra cover (low detail, médium detail, high detail), ukuran file teks, dan jumlah bit yang disisipkan pada tiap piksel citra cover. Rata-rata penilai MOS dari sampel 30 orang didapatkan bahwa citra stego memiliki penilaian fine pada kanal dengan SNR diatas 22 dB.

Kata Kunci :

Abstract

Steganography is a technique in communication system, where information is concealed into a carrier media, such us image, voice and video, without make significant changes to the cover media. Different from steganography which hiding information in plain sight, cryptography applications are used to encrypt information so that only the sender and recipient can understand it. Both of this techniques can be combined so that the information can be more difficult to breaked. This system is designed using image steganography with text file (.txt) as hiding information that was encrypted before using DES algorithm.

SSIS is using spread spectrum method, where information that will be embedded into cover image is spreaded whitin noise that has wide band frequency. This noise is added then to the cover image. To anticipate an error along transmittion proccess, SSIS using Error Control Coding (ECC) with convolutional encoder in transmitter and decoder using viterbi algorithm in receiver.

From this simulation I (for storage), imperceptibility level of stego image is confined by the number of embedded bit in every pixel of cover image. The image criteria is not determining imperceptibility level. In simulation II, maximum capacity determined by the size of cover image it self, code rate of convolutional encoder and level of quantization. Image criteria (low detail, medium detail, high detail), the size of text file, and the number of embedded bit in every pixel of cover image are the parameter that determine imperceptibility level of stego image in simulation II. MOS subjective values with 30 samples show that received image has high quality (fine category) in multipath fading+AWGN channel with SNR upper than 22 dB.

Keywords :

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi tidak hanya mendorong kecenderungan manusia untuk saling berkomunikasi semata. Tuntutan menjadi semakin kompleks sehingga masalah keamanan data menjadi hal yang sangat penting, apalagi data yang dikirimkan adalah data yang amat rahasia.

Berbagai usaha dilakukan untuk menjamin agar data rahasia yang dikirimkan tersebut tidak bisa diakses oleh pihak lain. Oleh karena itu, dalam dunia keamanan data muncul istilah kriptografi dan *steganography*. Kriptografi merupakan teknik yang digunakan untuk mengacak informasi sehingga informasi tersebut hanya dapat dimengerti oleh pihak yang saling berhubungan, sementara taknik *steganography* digunakan untuk menyembunyikan informasi pada suatu media tanpa memberikan perubahan yang berarti pada media tersebut.

Walaupun *steganography* dapat mempunyai hubungan yang erat dengan kriptografi, namun pada dasarnya kedua metode ini sangat berbeda. Kriptografi mengacak pesan sehingga tidak dimengerti, sedangkan *steganography* menyembunyikan pesan sehingga tidak terlihat. Pesan dalam *ciphertext* mungkin akan menimbulkan kecurigaan, sementara pesan yang menggunakan teknik *steganography* lebih terjamin. Kedua teknik ini dapat digabungkan untuk memperoleh hasil yang semakin sulit dilacak.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dikemukakan diatas, maka masalah yang akan diteliti adalah performansi sistem *steganography* dengan menerapkan metode *spread spectrum* terhadap pesan yang telah dienkripsi terlebih dahulu sebelum disisipkan. Performansi sistem yang dianalisa meliputi kapasitas *(payload)*, tingkat

keandalan *(robustness)* serta tingkat *imperceptibility* citra *stego* tanpa ditransmisikan *(storage)* dan yang ditransmisikan melalui kanal AWGN dan *multipath rayleigh*.

1.3 Batasan Masalah

Agar dalam pengerjaan Tugas Akhir ini diperoleh hasil yang optimal dan pembahasannya tidak meluas, maka masalah akan dibatasi sebagai berikut :

1. Citra asli merupakan citra berwarna 24 bit dalam format *bitmap* dengan ukuran 128x128 *pixels*.
2. Pesan yang disisipkan berupa teks (.txt)
3. *Error Control Code* yang digunakan adalah kode konvolusi dan algoritma viterbi pada dekoder.
4. Phasa acak *transmitter* dan *receiver* diasumsikan sama.
5. Ukuran kriteria performansi sistem adalah kriteria obyektif dan kriteria subyektif. Parameter kriteria obyektif yang digunakan adalah PSNR *(Paek Signal to Noise Ratio)*, MSE (Mean Square Error), dan BER *(Bit Error Rate)*, sementara kriteria subyektif menggunakan analisa MOS *(Mean Opinion Score)*.
6. Teknik *steganography* diimplementasikan menggunakan bahasa pemrograman MATLAB 7.0.1

1.4 Tujuan Penelitian

Secara umum tujuan penulisan yang ingin dicapai dalam Tugas Akhir ini adalah :

1. Merancang dan mensimulasikan sistem *Spread Spectrum Image Steganography* (SSIS) dengan data yang disisipkan berupa teks terenkripsi menggunakan algoritma kriptografi DES.
2. Menganalisa performansi sistem meliputi kapasitas *(payload)*, tingkat keandalan *(robustness)* serta tingkat *imperceptibility* citra *stego* tanpa

ditransmisikan *(storage)* dan yang ditransmisikan melalui kanal AWGN dan *multipath rayleigh*.

1.5 Metode Penelitian

Metodologi yang dilakukan dalam Tugas Akhir ini mencakup hal-hal sebagai berikut :

1. Mengumpulkan bahan-bahan referensi yang akan menunjang proses penelitian.
2. Studi literatur, merupakan tahap pendalaman materi, identifikasi permasalahan dan teori yang berkaitan dalam permasalahan dalam penelitian.
3. Menyusun algoritma program yang digunakan pada proses penyisipan dan deteksi kembali pesan yang disisipkan pada citra asli.
4. Merancang program berdasarkan algoritma yang telah dibuat dan mensimulasikan kedalam bahasa pemrograman Matlab 7.0.1.

1.6 Sistematika Penulisan Laporan

Tugas Akhir disusun secara sistematika pembahasan sebagai berikut :

BAB I Pendahuluan

Bab ini bersisi tentang latar belakang dilakukannya penelitian, perumusan masalah yang akan dianalisa, pembatasan masalah, tujuan yang ingin dicapai, metodologi pemecahan masalah dan sistematika penulisan.

BAB II Dasar Teori

Bab ini memuat penjelasan mengenai teori yang digunakan dalam perancangan dan implementasi sistem.

BAB III Perancangan dan Implementasi

Bab ini menjelaskan mengenai proses perancangan sistem *Spread Spectrum Image Steganography* dengan data berupa teks (.txt) yang terenkripsi *(ciphertext).*

BAB IV Analisa

Pada bab ini memuat tentang analisa terhadap kualitas citra *stego* secara objektif yang meliputi MSE, PSNR dan BER data, serta secara subjektif dengan menggunakan MOS dengan jumlah sampel 30 orang.

BAB V Penutup

Bagian ini menguraikan kesimpulan dari hasil penelitian Tugas Akhir ini serta saran-saran untuk pengembangan lebih lanjut.

BAB V
PENUTUP

5.1 Kesimpulan

Dari analisa terhadap pengukuran secara objektif maupun subjektif yang menunjukkan perfomansi sistem yang dirancang, maka dapat ditarik kesimpulan sebagai berikut :

1. Tingkat *imperceptibility* citra *stego* yang dihasilkan pada simulasi I (hanya untuk disimpan) tidak dipengaruhi oleh kriteria citra *cover (low detail, médium detail, high detail)* tapi dipengaruhi oleh jumlah bit yang disisipkan per tiap píksel citra *cover*.
2. Kapasitas maksimum citra *cover* pada simulasi II, selain dibatasi oleh ukuran *citra cover* itu sendiri, juga dibatasi oleh jumlah code rate dari kode konvolusi yang digunakan dan level kuantisasi.
3. Tingkat *imperceptibility* citra *stego* pada simulasi II dipengaruhi oleh kriteria citra *cover (low detail, médium detail, high detail)*, ukuran file teks, dan jumlah bit yang disisipkan pada tiap piksel citra *cover*.
4. Grafik BER informasi pada simulasi II lebih baik dari pada grafik BER kanal karena pada enkoder SSIS dilengkapi dengan blok *error control coding* dan interleaver untuk mengatasi *random error* dan *burst error* selama pentransmisian.
5. Rata–rata penilai MOS dari sampel 30 orang didapatkan bahwa citra *stego* memiliki penilaian *fine* pada kanal dengan SNR diatas 22 dB.
6. Penggabungan teknik kriptografi dan *steganography* dapat memberikan perlindungan ganda *(double protection)* terhadap pesan rahasia yang dikirimkan sehingga pesan tersebut akan semakin sulit dilacak.

5.2 Saran

Beberapa hal yang disarankan untuk dilakukan penelitian di masa mendatang, yaitu sebagai berikut :

1. Sistem ini untuk selanjutnya dapat ditujukan tidak hanya pada kanal multipath *flat fading* saja tapi juga bisa diimplementasikan pada kanal *selektif fading*.
2. Algoritma untuk penyisipan pesan dapat dikembangkan dengan menggunakan metode-metode lain yang lebih baik.
3. Dapat diimplementasikan pada studi kasus yang nyata seperti pada pesawat telepon dan email.