SIMULASI DAN IMPLEMENTASI STEGANOGRAFI VIDEO TERKOMPRESI BERFORMAT MPEG DENGAN MENGGUNAKAN METODE FAST FOURIER TRANSFORM

Andrisa Putra[1], Bmbang Hidayat[2], [3]

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

Abstrak

Kebutuhan untuk mengirimkan informasi dari suatu tempat ke tempat lain menjadi sangat mudah untuk dilakukan pada masa sekarang ini. Teknologi perangkat keras yang digunakan mengalami perkembangan yang pesat, begitu pula dengan kompleksitas algoritma dari perangkat lunak yang digunakan di dalamnya. Hal ini menyebabkan proses pengiriman informasi menjadi cepat. Jenis informasi yang bisa dikirimkan pun semakin beraneka ragam, dari yang hanya dapat mengirimkan tulisan yang berukuran kecil, hingga bentuk multimedia yang membutuhkan perhitungan rumit seperti video. Akan tetapi timbul masalah baru yaitu masalah keamanan dalam pengiriman informasi. Steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan / data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Steganografi dapat digunakan pada berbagai macam bentuk data, yaitu image, audio, dan video.dengan adanya steganografi maka pengirim pesan dapat merasa lebih aman. Dalam tugas akhir ini akan dilakukan simulasi dengan menggunakan matlab sebagai perangkat lunak pemograman. Dengan menggunakan video berformat MPEG sebagai media carrier dan pesan text sebagai informasi rahasia. Simulasi yang dilakukan antara lain proses penyisipan dan pengekstrakan serta proses penghitungan tingkat akurasi dari sistem ini. Hasil dari tugas akhir ini berupa sistem yang dapat memberikan keluaran berupa file video steganograf, file kunci dan nilai parameter SSIM yang menjadi tolak ukur kualitas perbandingan video. Serta keluaran berupa informasi rahasia disisi penerima. Dan juga dapat menghitung keakuratan sistem dalam persentase. Hasil dari sistem ini mendapatkan akurasi hasil pesan text 100%, nilai mos yang memiliki rata-rata 4,77 dan menghasilkan nilai SSIM mendekati 1

Kata Kunci : steganografi, fast fourier transform, mpeg, color space, SSIM

Abstract

The need to transmit information from one place to another becomes very easy to do at the present time. Technology hardware used to experience rapid growth, as well as the complexity of the software algorithms used in it. This causes a rapid process of information delivery. The type of information that can be sent even more diverse, from which only can post a small, up to multimedia forms that require complex calculations such as video.However, new problems that arise in the delivery of information security issues. Steganography is one way to hide a message / secret data in the data or other messages that seem not contain anything, except for those who understand the key. Steganography can be used in various forms of data, ie images, audio, and video.dengan the steganography the message sender can feel more secure. In the final project will be carried out simulations using the matlab software programming. By using MPEG video format as the carrier media and text messages as confidential. Simulations were carried out, among others, the process of insertion and extraction as well as the process of counting the accuracy of this system. Results of this final form of system that can provide output in the form of video files steganograf, key files and SSIM parameter values that become the benchmark of quality comparison video. As well as the output of the receiver side of the confidential information. And the accuracy of the system can also calculate in percentage. Results from this system to get accuracy results text message 100%, the value of the mos has an average yield of 4.77 and SSIM values close to 1.

Keywords : steganography, fast Fourier transform, mpeg, color space, SSIM

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini pengiriman informasi dari suatu tempat ke tempat lainnya menjadi kebutuhan setiap orang dari segala aspek kehidupan. Perkembangan teknologi perangkat keras pendukung semakin canggih, diiringi dengan perkembangan perangkat lunak yang digunakan didalam perangkat keras tersebut. Hal ini menyebabkan pengiriman data dapat dilakukan dengan cepat dan mudah. Jenis informasi yang dapat dikirimkan pun semakin beraneka ragam, mulai dari data, audio, dan video.

Era perkembangan teknologi semakin menuju kearah pemrosesan secara digital yang disebabkan oleh beberapa faktor :

1. Mudah dilakukan manipulasi data.
2. Mudah untuk melakukan pengiriman.
3. Mendukung pengiriman kebeberapa tempat secara bersamaan.
4. Mudah untuk didistribusikan terlebih lagi adanya internet yang semakin mendukung proses pengiriman informasi

Akan tetapi, dengan perkembangan teknologi yang semakin canggih tersebut juga diiringin dengan perkembangan kejahatan didalamnya. Hal ini menyebabkan aspek keamanan menjadi sangat penting terlebih untuk informasi yang bersifat rahasia. Salah satu teknologi yang dapat digunakan untuk menjaga keamanan informasi ialah dengan cara steganography. Dengan metoda ini, informasi yang dikirimkan disisipkan dalam suatu file lain yang memiliki format umum. sehingga jika ada seseorang yang ingin menyadap informasi yang dikirimkan kecurigaannya akan berkurang karena yang tampak hanyalah sebuah file media pada umumnya.

Media penampung yang sering digunakan dalam teknik steganography adalah data, audio dan video. Pemilihan media penampung dilakukan berdasarkan besar kecilnya informasi yang ingin dikirimkan. Media video merupakan media penampung terbesar saat ini karena memiliki ukuran file yang cukup besar sehingga tidak akan menimbulkan kecurigaan jika disisipkan informasi-informasi kecil didalamnnya.

Didalam seni steganography terdapat beberapa teknik yang umum digunakan antara lain *DCT (Discrete Cosine Transformation) Modification, wavelet, watermarking, dan*

Fast Fourier Tranform(FFT). Pada penelitian sebelumnya teknik steganografi yang dipakai ialah Analisis Pengamanan Pesan Teks Berdasarkan Model Steganografi Menggunakan Word Mapping Method (WMM)[9]. Teknik steganography yang digunakan dalam tugas akhir ini adalah Fast Fourier Transform dengan menggunakan video berformat MPEG sebagai media penampung dan file *text* sebagai informasi.

File MPEG dipilih karena masih banyak digunakan dalam teknik kompresi video misalnya untuk pembuatan VCD, video downloading, dan dreamscene sistem operasi windows.

1.2 Tujuan

Tujuan pelaksanaan tugas akhir ini adalah :

1. Melakukan simulasi steganografi dengan video sebagai media pembawa dan *file text* sebagai informasi rahasia dengan *Fast Fourier Transform*.
2. Mengetahui waktu komputasi dari sistem penyisipan dan ekstraksi.
3. Menganalisis hasil dari penyisipan dengan metode *Fast Fourier Transform* dengan menggunakan parameter SSIM dan MOS.
4. Mengetahui tingkat akurasi pesan yang dihasilkan.

1.3 Rumusan Masalah

Rumusan masalah didalam tugas akhir ini adalah :

1. Bagaimana cara menyisipkan informasi file *text* kedalam video tanpa membuat degradasi yang signifikan.
2. Bagaimana pengaruh besarnya file yang disisipkan terhadap waktu yang dibutuhkan untuk melakukan proses penyisipan dan ekstraksi.
3. Bagaimana hasil steganografi dengan melihat nilai SSIM dan MOS.
4. Bagaimana akurasi pesan teks yang dihasilkan.

1.4 Batasan Masalah

Untuk mempermudah dan membatasi cakupan pembahasan masalah pada Tugas Akhir ini, maka disimpulkan batasan-batasan sebagai berikut :

1. Tugas Akhir ini hanya membahas penyisipan informasi berupa *file text* ke dalam media carrier berupa video dengan format MPEG.
2. Teknik steganografi yang digunakan ialah Fast Fourier Transform

3. Tidak membahas masalah pengiriman data dan teknik-teknik manipulasi video yang dilakukan
4. Melakukan analisis video hasil steganografi dengan menggunakan parameter SSIM sebagai analisis objektif dan MOS sebagai analisis objektif.
5. Menggunakan perangkat lunak Matlab sebagai simulator

1.5 Metodologi

Dalam pelaksanaannya tugas akhir ini meliputi tahapan-tahapan antara lain:

1. study pustaka

   dilakukan studi dari berbagai literatur mengenai cara refresentasi file video dan teknik steganography dengan metode Fast Fourier Transform
2. Analisa

   Dilakukan analisis terhadap algoritma Fast Fourier Transform beserta teknik ekstraksinya dan analisis perangkat lunak yang akan dirancang untuk melakukan simulasi.
3. Perancangan perangkat lunak

   Dilakukan perancangan program dan antarmuka
4. Simulasi perangkat lunak

   Melakukan simulasi perangkat lunak yang telah dibuat dengan mengunakan matlab
5. Pengujian

   Melakukan pengujian terhadap perangkat lunak yang digunakan, yaitu keberhasilan penyembunyian data, dan perbandingan kualitas video sebelum dan setelah dilakukan proses penyisipan.

1.6 Sistematika Penulisan

Secara umum keseluruhan Tugas Akhir ini dibagi menjadi lima bab bahasan. Penjelasannya adalah sebagai berikut:

BAB I PENDAHULUAN

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

BAB II DASAR TEORI

Bab ini membahas teori mengenai steganografi, sistem warna, fast fourier transform, SSIM

BAB III METODOLOGI PENELITIAN

Bab ini membahas proses simulasi dan implementasi steganografi file video berformat MPEG dengan menggunakan kunci.

BAB IV HASIL DAN ANALISIS

Bab ini berisi hasil dari penelitian dan menguraikan analisis dari hasil parameter video yang didapat

BAB V PENUTUP

Bab ini berisi kesimpulan dari hasil Tugas Akhir dan saran untuk pengembangan-pengembangan lebih lanjut.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil pengujian dan analisis yang telah dilakukan pada pengamanan pesan teks dengan menggunakan steganografi dengan metode *Fast Fourier Transform* dengan video MPG sebagai media pembawa dan file *text* sebagai *secret file* maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Ukuran *secret file* ditanam pada *video pembawa* mempengaruhi waktu proses sistem. Untuk *secret file* berukuran 39 Bytes maka waktu membutuhkan waktu 0.201604 s untuk proses penyisipan dan 0.0229746 s untuk ekstraksi. Semakin besar besar *secret file* yang akan ditanam maka semakin lama waktu yang diperlukan sistem untuk menghasilkan keluaran.
2. Ukuran *secret file* yang digunakan untuk proses berbanding terbalik dengan nilai dari SSIM. Untuk *secret file* berukuran 39 Bytes menghasilkan nilai SSIM 1 ini menunjukkan video hasil steganografi sangat mirip dengan video asli. Semakin besar ukuran *secret file* maka nilai SSIM akan semakin kecil. Hal ini akan menyebabkan degradasi pada video *carrier* semakin terlihat.
3. Semakin besar ukuran *secret file* maka semakin mungkin menimbulkan perbedaan antara *secret file* saat ekstraksi dan *secret file* saat sebelum penyisipan. Pada penggunaan data berukuran 39 Bytes sebagai informasi rahasia sistem menghasilkan akurasi 100% akan tetapi pada saat file berukuran 12 KBytes sistem hanya menghasilkan tingkat akurasi sebesar 99.7588%.
4. Sistem tidak tahan terhadap proses croping, converter, resize dan gangguan saat pengiriman. Semakin banyak manipulasi data maka semakin kecil tingkat akurasinya dengan demikian *secret file* yang diperoleh dari hasil ekstrasi akan semakin berbeda dengan *secret file* asli.
5. Nilai parameter MOS yang didapatkan adalah 4,73 yang artinya video tidak memiliki degradasi yang besar, dengan kata lain pesan yang disisipkan ke dalam video tersebut tidak terlihat jelas.

5.2 Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah :

1. Menggunakan format video yang lain dan format *secret file*
2. Menggunakan algoritma enkripsi pada *secret file* sehingga tingkat keamanan lebih tinggi
3. Dapat membuat sistem tahan terhadap proses manipulasi dan gangguan saat pengiriman video steganografi
4. Sebelum dilakukan proses penyisipan dilakukan kompresi terlebih dahulu seperti kompresi *hufmann* atau kompresi LZW.
5. Simulasi system dengan menggunakan bahasa pemrograman yang lain, misalnya C atau Java.
6. Memilih metode penyisipan yang lain

DAFTAR PUSTAKA

[1] Indradip Banerjee Souvik Bhattacharyya and Gautam Sanyal. Design and implementation of a secure text based steganography model. In *Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer Engineering, and Applied Computing(WorldComp 2010)*, LasVegas,USA, July 12-15,2010.

[2] MohammadShirali-Shahreza. *Text steganography by changing words spelling*. In *ICACT*, 2008.

[3] Souvik Bhattacharyya. and Gautam Sanyal. Study of secure steganograph model. *Proceedings of International Conference on AdvancedComputing and Communication Technologies (ICACCT-2008)*, Panipath,India, 2008.

[4] Alan C. Brooks and Thrasyvoulos N. Pappas. Structural similarity quality metrics in a coding context: exploring the space of realistic distortions, Proc. SPIE 6057, Human Vision and Electronic Imaging XI, 60570U February 09, 2006

[5] A. Nukada. FFTSS: A HIGH PERFORMANCE FAST FOURIER TRANSFORM LIBRARY, In Proceedings of the 2006 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2006), Vol. III, pp.980-983, IEEE, May 14-19, 2006

[6] Wang et.al., Zhou. Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE. 2004

[7] Multimedia Signal Processing Group Institute of Electrical Engineering.,2013., VQMT: Video Quality Measurement Tool http://mmspg.epfl.ch/vqmt. Diakses pada tanggal 21 Juni 2013

[8] Fondren Library - Rice University., 2011., Video Formats Guide., http://library.rice.edu/services/dmc/guides/video/VideoFormatsGuide.pdf., Diakses pada tanggal 21 Juni 2013

[9] Astia H Riris. Analisis Pengamanan Pesan Text Berdasarkan Model Steganografi dengan Menggunakan Word Mapping Method (WMM).,2012