IMPLEMENTASI STEGANOGRAFI PADA MEDIA VIDEO DENGAN MENGGUNAKAN METODE FAST FOURIER TRANSFORM (FFT)

R. Firman Hidayatullah[1], Tjokorda Agung Budi Wirayuda[2], Rimba Widhiana Ciptasari[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Kemudahan dalam mengakses, menyalin, memanipulasi sekaligus mendistribusikan data digital (teks, gambar, suara, video dan lainnya) tidak saja dimanfaatkan untuk kepentingan yang positif, namun juga dalam hal yang negatif. Untuk itu diperlukan suatu cara pengamanan untuk melindungi informasi yang sifatnya rahasia, salah satunya dengan steganografi. Dengan steganografi kita hanya perlu menyembunyikan suatu data ke dalam media lain. Kebutuhan penyembunyian data dalam jumlah besar dan teknik penyembunyian yang tangguh membutuhkan media pembawa yang cukup besar dan teknik yang tangguh pula. Maka pemilihan video sebagai media steganografi merupakan langkah yang tepat.

Dalam tugas akhir ini diimplementasikan steganografi pada video jenis AVI uncompressed dengan menggunakan FFT sebagai metode transformasinya. FFT mengubah byte data dari domain spatial ke domain frekuensi yang selanjutnya dilakukan modifikasi dengan penambahan byte-byte data yang akan disisipkan. Hal ini dilakukan agar perubahan yang dilakukan tidak terlalu terlihat dengan memanfaatkan keterbatasan penglihatan manusia. Pengujian dilakukan untuk melihat kualitas video stego berdasar nilai MSE dan PSNR, sisi ketahanan, dan juga tingkat validitas data hasil ekstraksi.

Dari hasil pengujian diperoleh kualitas video stego memiliki kualitas yang baik. Selain itu tingkat validitas mencapai 100%, artinya data ekstraksi sama persis dengan data aslinya. Namun dari sisi ketahanan, video stego yang dihasilkan dikategorikan fragile, karena tidak tahan terhadap gangguan seperti pengubahan wadah penampung.

Kata Kunci : steganography, video, FFT

Abstract

The easy way for accessing, copying, manipulating, and distributing digital data (text, image, voice, video, etc) does not for a good purpose only, but also for the bad thing. For that reason, there is the way to protect a secret information, one of them is steganography. With steganography we just concealing data to another media. A needs to conceal large data in a good technique can be accomoted by video steganography which is video as a media carrier.

This final project implements steganography in AVI uncompressed by using FFT as transformation method. FFT will change byte of data from spatial domain to frequency domain, then modifiy with addition bytes of data hiding. FFT is used in order to alteration that happened not seen by take advantage limitation of human visual system. The examination purpose is to observe the quality of video stego based on MSE and PSNR, robustness, and the validity of extracted data.

From examination result obtained a good quality of video stego. Besides that, the validity reached 100%, it means extracted data same as original data. Nevertheless, in the robustness can be concluded that the result can be categorized as fragile because does not resist against converting file format.

Keywords : Steganography, video, FFT

BAB I
PENDAHULUAN

1.1 Latar belakang masalah

Perkembangan teknologi informasi dan Internet saat ini sangat pesat dan banyak memberikan kemudahan bagi kita untuk mengakses, menyalin, memanipulasi sekaligus mendistribusikan data digital (teks, gambar, suara, video dan lainnya). Namun tidak sedikit orang yang menyalahgunakan perkembangan tersebut seperti contohnya mencoba mengakses informasi yang bukan hak mereka. Oleh karena itu, diperlukan pula pengamanan sistem informasi yang tangguh, salah satunya dengan steganografi.

Steganografi adalah suatu cara untuk melindungi informasi dengan cara menyembunyikan data digital pada media digital lainnya sehingga keberadaan informasi rahasia tersebut tidak diketahui oleh indera manusia.

Ukuran data penyisipan sebanding dengan ukuran media pembawanya. Semakin besar ukuran media pembawanya, maka semakin besar pula ukuran data yang bisa disisipkan. Hal tersebut juga harus memperhatikan masalah keterlihatan (*imperceptibility/invisibility*), kapasitas (*capacity*), dan ketahanan (*robustness*) dimana ketiganya memiliki keterikatan satu sama lain.

Kebutuhan penyembunyian data dalam jumlah besar dan teknik penyembunyian yang tangguh membutuhkan media pembawa yang cukup besar dan teknik yang tangguh pula. Maka pemilihan video sebagai media steganografi merupakan langkah yang tepat untuk mengakomodasi kebutuhan tersebut. Video merupakan salah satu teknologi komunikasi informasi. Semakin beragamnya format dan aplikasi video dalam pengunaannya sehari-hari, memungkinkan adanya penyisipan informasi dalam video. Sehingga sangat disayangkan dengan kemampuan yang cukup, seseorang (*eavesdropper*) dapat mengetahui informasi tersebut.

Penggunaan metode *Fast Fourier Transform* (FFT) sebagai metode transformasi telah banyak digunakan dalam perkembangan teknologi, salah satunya dipakai dalam *image processing*. Sebuah teknik steganografi yang ditempatkan dengan baik pada domain frekuensi citra tidak akan tampak oleh

mata. Dalam *image processing*, FFT digunakan untuk mengubah gambar ke dalam domain frekuensi yang selanjutnya dilakukan modifikasi dengan penambahan bit-bit data yang akan disisipkan. Hal ini bertujuan agar perubahan yang dilakukan tidak terlalu terlihat dengan memanfaatkan keterbatasan penglihatan manusia.

1.2 Perumusan Masalah

Bedasarakan latar belakang masalah di atas dapat dirumuskan menjadi beberapa masalah sebagai berikut :

3 Bagaimana data disembunyikan dan diekstrak dalam video dengan steganografi menggunakan metode *Fast Fourier Transform (FFT)* sebagai metode transformasinya.

4 Bagaimana hasil ekstraksi data yang disembunyikan dibandingkan dengan data aslinya.

5 Bagaimana kualitas *imperceptibilty* video dari penilaian objektif setelah dilakukan penyisipan berdasarkan nilai MSE dan PSNR.

6 Bagaimana kualitas *robustness* setelah dilakukan modifikasi terhadap *video stego*.

Adapun yang menjadi batasan masalah dari penyusunan tugas akhir ini adalah :

1. Penyimpanan informasi dalam video ini dilakukan pada kumpulan gambar yang bergerak saja, tidak melibatkan audio
2. *File* masukan dan keluaran untuk perangkat lunak berupa *file* video jenis AVI berdimensi 256x256
3. Ukuran data yang disisipkan lebih kecil dari ukuran media pembawa
4. Format data yang disisipkan berupa *file* dokumen (.txt, .doc, .pdf), gambar (.bmp, .jpeg, .gif), audio (.midi, .wav, .mp3), dan video (.mpeg, .avi)
5. Perangkat lunak tidak melakukan pemutaran video

1.3 Tujuan

1. Menganalisis tingkat validitas *file* yang disembunyikan dengan menghitung jumlah bit-bit yang berbeda antara *file* sebelum disembunyikan dengan *file* setelah disembunyikan.
2. Menganalisis kualitas video AVI dengan menghitung MSE dan PSNR dari perbandingan frame video yang belum disisipi dan frame video yang telah disisipi.
3. Menganalisis faktor *robustness* data hiding terhadap proses manipulasi wadah penampung. Proses manipulasi yang digunakan adalah mengubah format *file* avi menjadi format mpeg dan kemudian dikembalikan lagi menjadi format avi.

1.4 Metodologi penyelesaian masalah

Metode yang akan digunakan untuk menyelesaikan tugas akhir ini adalah :

1. Studi literatur

   Mencari beberapa referensi yang berkaitan dengan steganografi khususnya pada media citra digital sebagai objek *cover*. Kemudian mempelajari dasar teori dan literatur-literatur yang relevan dengan teknik-teknik steganografi, khususnya mengenai video AVI, *image processing, Fast Fourier Transform.*
2. Analisis dan Desain

   Melakukan analisis dan perancangan pengembangan perangkat lunak dengan menggambarkan modul-modul perangkat lunak yang terdapat pada sistem dengan metode terstruktur.
3. Implementasi Sistem

   Mengimplementasikan sistem berdasarkan analisis perancangan dan desain yang telah dibuat kedalam program.
4. Pengujian dan Analisis Hasil

   Menguji dan menganalisis hasil, yaitu validitas *file* yang disembunyikan dengan menghitung jumlah bit-bit yang berbeda sebelum dan sesudah disembunyikan, menghitung MSE dan PSNR dari perbandingan frame video sebelum dan sesudah disisipi, memutar video setelah dilakukan manipulasi wadah penampung video dari AVI menjadi MPEG.
5. Pengambilan kesimpulan dan penyusunan laporan tugas akhir.

BAB V
Penutup

5.1 Kesimpulan

Dari hasil penelitian dan analisa yang dikerjakan dalam tugas akhir ini dapat diperoleh kesimpulan sebagai berikut :

1. Tingkat validitas *file* data ekstraksi dengan menggunakan metode FFT mencapai 100% apabila video *stego* tidak mengalami gangguan.
2. Jenis *file* dan besar *file* yang disisipkan tidak mempengaruhi tingkat validitas data, namun hanya akan mempengaruhi kualitas video *stego* yang dihasilkan.
3. Nilai *scaling factor* dan ukuran data berbanding terbalik dengan kualitas video yang dihasilkan. Namun secara umum video *stego* yang dihasilkan memiliki kualitas yang baik.
4. Video *stego* yang telah mengalami gangguan seperti perubahan wadah penampung akan mengalami kegagalan ketika proses ekstraksinya. Kegagalan dalam hal ini berarti bahwa data berhasil diekstraksi, namun data tersebut sama sekali tidak terbaca oleh aplikasi apapun. Oleh karena itu video steganografi yang dibangun dapat dikategorikan tidak *robust* atau dengan kata lain dikategorikan *fragile*.
5. Metode steganografi yang digunakan pada tugas akhir ini adalah *non-blind*, artinya dalam proses ekstraksinya memerlukan video asli.

5.2 Saran

Berdasarkan hasil pengujian dan analisa hasil pengujian, dapat diberikan saran sebagai berikut :

1. Video steganografi yang dibangun bisa dimanfaatkan untuk penghematan *hard disk*. Namun alangkah lebih baik jika steganografi yang dibangun bersifat *blind*.
2. Penyisipan pada video bisa dikembangkan dengan menggunakan metode lainnya lalu dibandingkan dari sisi kualitas, validitas data dan ketahanannya.

Daftar Pustaka

[1] Bender, W and Gruhl, D and Morimoto, N and Lu, A. IBM system journal, vol 35, NOS 3&4, 1996. *Techniques for Data Hiding*.
URL : http://www.almaden.ibm.com/cs/people/dgruhl/313.pdf diakses pada 20 Juni 2007

[2] Cacciaguerra, S and Ferretti, F, *Data Hiding: Steganography and Copyright Marking*.
URL : http://www.cs.unibo.it/~scacciag/home_files/teach/datahiding.pdf diakses pada 1 Agustus 2007

[3] Darma Eddy Muntina, 2006, "Materi Kuliah Grafika dan Citra : Kompresi Citra", Departemen teknik Informatika IT Telkom Bandung.

[4] http://en.wikipedia.org/wiki/Audio_Video_Interleave, *Audio Video Interleave*. Diakses pada 26 Juni 2008

[5] http://en.wikipedia.org/wiki/Discrete_Fourier_Transform, Discrete Fourier Transform. Diakses pada 4 September 2007.

[6] http://en.wikipedia.org/wiki/Fast_Fourier_Transform, Fast Fourier Transform. Diakses pada 4 September 2007.

[7] http://en.wikipedia.org/wiki/Mean_Squared_error , Mean Squared Error. Diakses pada 19 Agustus 2008

[8] http://en.wikipedia.org/wiki/Peak_Signal_to_Noise_Ratio, *Peak Signal to Noise Ratio*. Diakses pada 19 Agustus 2008

[9] Ingemar J. Cox and Kilian, J and Leighton F.T and Shamoon, T, *Secire Spread Spectrum Watermarking for Multimedia*. URL: http://ieeexplore.ieee.org/iel4/83/14163/00650120.pdf diakses pada 7 Juli 2007

[10] J.C. Judge, 2001, *Steganography : Past, Present, Future*. URL : http://www.llnl.gov/tid/lof/documents/pdf/245799.pdf Diakses pada 25 Juni 2007

[11] J.J. Chae and B. S. Manjunath., *Data Hiding in Video*. URL: http://www-iplab.ece.ucsb.edu/publications/99ICIP.pdf diakses pada 2 Agustus 2008

[12] Kessler, G.C., *An Overview of Steganography for The Computer Forensics Examiner*. URL : http://www.wetstonetech.com/f/stego-kessler.pdf diakses pada 25 Juni 2007

[13] Matlab, 2001, "Image Processing Toolbox", The Mathwork Inc.

[14] Rahmanda, F., 2006. *Steganography Pada Video Jenis MPEG dengan Transformasi Cosinus Dikrit.* Bandung : Jurusan Teknik Informatika STT Telkom.

[15] Smith, Steven W., 2007, *The Scientist and Engineer's Guide to Digital Signal Processing,* Chapter 12. URL : http://www.dspguide.com/CH12.PDF diakses pada 9 September 2007

[16] Smith, Steven W., 2007, *The Scientist and Engineer's Guide to Digital Signal Processing,* Chapter 8. URL : http://www.dspguide.com/CH8.PDF diakses pada 6 September 2007