

SIMULASI STEGANOGRAFI CITRA DENGAN SISIPAN SINYAL SUARA DENGAN VERIFIKASI SUARA MENGGUNAKAN MEL FREQUENCY CEPSTRAL COEFFICIENT

Mariza Duma Putri¹, Ir Bambang Hidayat², Dea³

¹Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Di masa sekarang pertukaran informasi dengan menggunakan gelombang radio sangatlah berkembang dengan pesat, dengan memakai gelombang radio pertukaran informasi dapat berlangsung sangat cepat sampai ke penerima. Tetapi perkembangan yang pesat itu juga menghasilkan efek samping terutama pertukaran informasi melalui internet. Steganografi adalah suatu ilmu dan seni menyisipkan informasi bersifat rahasia ke dalam media cover tertentu dengan tujuan menyamarkan keberadaan informasi di dalamnya agar tidak diketahui oleh pihak lain yang tidak berhak atas informasi tersebut. Dalam menyisipkan informasi bisa berupa gambar, tulisan dan audio. Media yang disisipkan juga bisa berupa gambar, tulisan, audio dan video.

Suara adalah alat komunikasi yang terpenting karena dengan suara kita bisa mengetahui identitas seseorang dan mengenalinya. Pada tugas akhir ini akan dirancang suatu sistem yang akan melindungi pesan suara yang dikirim dan disisi penerima akan diverifikasi pemilik suara tersebut sehingga kita mengetahui identitas suara yang dilindungi. Untuk memverifikasi suara akan digunakan metode MFCC dan akan dilanjutkan Nearest Neighbor untuk pengelompokkan, Sedangkan audio yang akan disisipkan tidak diberi metode hanya dibagian cover image akan memakai metode DCT.

Hasil yang didapatkan adalah citra rahasia yang dikirimkan berhasil sampai disisi penerima dan verifikasi suara telah berhasil dilakukan dan didapatkan rata-rata akurasi verifikasi suara dari 6 percobaan menghasilkan nilai yang lebih tinggi apabila data uji hasil steganografi diujikan dengan data latih hasil steganografi yaitu 85 % dibandingkan data uji hasil steganografi diujikan dengan data latih suara asli yaitu 77.91 %

Kata Kunci : Steganografi, verifikasi suara, MFCC, Nearest Neighbor, DCT

Abstract

Nowadays information exchange using radio waves grows rapidly, with radio waves information can be delivered very fast to the receiver. But it also has its side effects, especially internet based information exchange. Steganography is a form of art and science to insert confidential information into a certain media in order to disguise the information existence so it is not possible for unwanted external party to access it. The information can come in many forms including text, image, and audio.

Voice is one of the most important aspects of communication; with it we can recognize one's identity. This thesis designed a system to disguise a voice message which the receiver can verify the voice to recognize an identity. MFCC method is used to verify and Nearest Neighbor method is used to classify the voice after. While no method are used for the inserted audio, DCT method is used for image cover

The results of this final project are the secret image is sent successfully to the receiver and voice verification has been successfully carried out and an average accuracy of 6 experimental verification of noise gets a higher value if the testing sample results steganography tested with training data results steganography is 85% compared to the data steganography test results tested with the original voice training data is 77.91%

Keywords : Steganography, voice verification, MFCC, Nearest Neighbor, DCT

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Di masa sekarang pertukaran informasi dengan menggunakan gelombang radio sangatlah berkembang dengan pesat, dengan memakai gelombang radio pertukaran informasi dapat berlangsung sangat cepat sampai ke penerima. Tetapi perkembangan yang pesat itu juga menghasilkan efek samping terutama pertukaran informasi melalui internet. Media internet telah digunakan oleh masyarakat luas hal ini memungkinkan penyadapan dan pengubahan data yang dikirim sehingga informasi tersebut sudah diketahui oleh orang luar dan informasi yang diterima sudah berbeda dengan yang aslinya. Sebagai masyarakat yang pintar kita harus menyadari bahwa banyak ancaman yang mengganggu data kita. Jumlah hacker dan penyusup di dunia maya sangatlah banyak untuk itulah kita harus mempunyai dan mengerti metode bagaimana cara agar data yang kita kirim bisa sampai ke tangan penerima dengan baik. Dan tentu saja agar hanya pengirim dan penerima saja yang mengetahui isi data tersebut. Steganografi adalah suatu ilmu dan seni menyisipkan informasi bersifat rahasia ke dalam media cover tertentu dengan tujuan menyamarkan keberadaan informasi di dalamnya agar tidak diketahui oleh pihak lain yang tidak berhak atas informasi tersebut^[1]. Dalam menyisipkan informasi bisa berupa gambar, tulisan dan audio. Media yang disisipkan juga bisa berupa gambar, tulisan, audio dan video.

Suara merupakan hal terpenting dalam komunikasi dengan suara kita dapat berkomunikasi secara langsung dan tepat sasaran, tetapi pertukaran informasi suara melalui internet memiliki banyak kelemahan salah satunya adalah terkadang suara tersebut bisa disadap dan penerima terkadang tidak mengetahui pemilik suara tersebut. Ketidaktahuan pemilik suara bisa menyebabkan banyak masalah dalam pengambilan keputusan, apabila terjadi hal yang tidak diinginkan penanggung jawab tidak diketahui karena ketidaktahuan pemilik suara. Perkembangan teknologi

menciptakan bahwa suara dapat dipakai dalam sistem *security*, dalam pengenalan suara kita ingin mendapatkan identitas seseorang dengan menggunakan *sample*. Teknik ini memungkinkan untuk verifikasi identitas dan pengendalian perintah atau akses melalui suara.

Dalam tugas akhir ini akan disimulasikan steganografi audio yang akan disisipkan ke citra digital, yang keluarannya akan memverifikasi suara disisi penerima. Audio yang digunakan berformat wav yaitu format audio tidak terkompresi, steganografi dalam bentuk domain frekuensi memiliki ketahanan yang lebih baik daripada domain waktu. Didalam tugas akhir ini akan diimplementasikan suatu sistem steganografi dengan menggunakan *discrete cosine transform* untuk transformasi media cover dalam hal ini citra lalu menggunakan *invers discrete cosine transform* setelah penyisipan file audio ke dalam citra digital, setelah pengiriman file audio akan diverifikasi menggunakan *Mel Frequency Cepstral Coefficient*. dan *k-nearest neighbor*. Didalam MATLAB dapat disimulasikan pengiriman data dan verifikasi suara melalui sturuktur yang sudah ada.

1.2 Tujuan Penelitian

Tujuan tugas akhir ini dapat dirumuskan sebagai berikut.

1. Menyisipkan file audio berformat wav ke dalam citra digital dengan menggunakan *discrete cosine transform* lalu menginversnya kembali.
2. Menerapkan algoritma pengklasifikasian dalam sistem pengenalan jenis suara manusia.
3. Merancang dan merealisasikan suatu sistem steganografi dengan hasil verifikasi suara.
4. Melakukan analisa kerja sistem dalam steganografi penyisipan audio ke citra digital dan verifikasi suara manusia.

1.3 Perumusan Masalah

Beberapa permasalahan pada tugas akhir dapat diformulasikan sebagai berikut.

1. Bagaimana mengimplementasikan penyisipan pesan audio pada citra digital berformat jpg menggunakan metode DCT dan IDCT dalam MATLAB.
2. Bagaimana melakukan analisis *Mel Frequency Cepstrum Coefficient* untuk mendapatkan feature atau ciri dari suara manusia.
3. Bagaimana melakukan identifikasi dari *feature* atau ciri yang ada untuk verifikasi suara.
4. Bagaimana melakukan analisis metode DCT dan IDCT saat penyisipan data audio kedalam citra digital.

1.4 Batasan Masalah

Tugas akhir ini akan membatasi permasalahan sebagai berikut.

1. File citra yang digunakan sebagai media cover adalah citra digital RGB yang berformat Bitmap.
2. Pesan yang disisipkan adalah file audio yang berformat .wav dan berukuran 8 bit.
3. Ukuran kapasitas cover harus lebih besar dari yang disisipkan.
4. Sebelum dilakukan penyisipan, media cover diubah dulu menjadi domain frekuensi.
5. Data suara yang akan dianalisa dan dideteksi diambil dari orang Indonesia dan dalam kondisi berbicara secara normal.
6. Tidak mengenal perbedaan usia dan pria wanita.
7. Kata-kata yang diucapkan sama oleh setiap orang dan hanya 1 kata yaitu kata *down*.

8. Simulasi dilakukan dengan program matlab R2009a.

1.5 Metode Penyelesaian Masalah

Penelitian ini dilakukan dengan metode-metode sebagai berikut.

a. *Study Literature*

Tahap pertama yang dilakukan adalah dengan mencari referensi-referensi dan data-data yang akan membantu penulis dalam memperkuat dasar teori dan mendapatkan metoda yang tepat agar tepat sasaran.

b. Analisis dan desain

Tahap kedua adalah analisis dan desain pada tahap ini penulis menganalisis desain dan analisa untuk penyisipan file audio ke citra serta di sisi penerima akan menghasilkan verifikasi suara. Desain dari perangkat lunak yang akan digunakan dibentuk dengan pendekatan struktural dimana desain perancangan dibentuk dalam data *flow* diagram.

c. Implementasi Sistem

Tahap ketiga adalah implementasi sistem, penulis memulai untuk membuat sistem yang telah dirancang dan didesain pada tahap sebelumnya, ditahapan ini perancangan direalisasikan di *software* Matlab.

d. Pengujian dan Analisis Hasil

Tahap keempat adalah pengujian dan analisis hasil. Pada tahap ini penulis dilakukan pengujian terhadap sistem dan analisis terhadap keluaran sistem.

e. Penyusunan Laporan

Tahap terakhir yang dilakukan adalah penyusunan laporan, penulis melakukan penulisa laporan dari hasil penelitian yang telah dilakukan dan membuat kesimpulannya

1.6 Sistematika Penulisan

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

Bab I : PENDAHULUAN

Berisi latar belakang, tujuan, perumusan dan batasan masalah, metode penelitian yang dilakukan dan sistematika penulisan

Bab II : DASAR TEORI

Berisi teori-teori dasar mengenai steganografi, citra digital, DCT, suara, dan MFCC

Bab III : PERANCANGAN SISTEM DAN IMPLEMENTASI

Berisi diagram alir penelitian, perancangan sistem serta cara kerja sistem

BAB IV : PENGUJIAN SISTEM DAN ANALISIS

Berisi data hasil pengolahan citra acuan dan data hasil pengolahan citra uji menganalisis keakuratan hasil citra acuan sistem dengan hasil citra uji sistem

BAB V : KESIMPULAN DAN SARAN

Berisi kesimpulan atas hasil kerja yang telah dilakukan beserta rekomendasi dan saran untuk pengembangan dan perbaikan selanjutnya

Telkom
University

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

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

- Sistem yang dibangun mampu melakukan proses steganografi dengan metode DCT *comparison-based correlation* dengan BCH Code sebagai *error correction*.
- Sistem ini tidak tahan terhadap serangan
- 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.
- Hidden speech yang diekstraksi dapat bertahan dengan BCH Code dengan serangan yang diminimalisir, serangan teringan diberikan oleh cropping sedangkan untuk Gaussian dan Salt & pepper harus diberikan dengan variance kecil agar BER kecil
- Speech dapat dikenali dan dapat diklasifikasikan sesuai dengan pemilik suara walaupun sudah diserang
- Verifikasi suara dengan menggunakan noise kecil menghasilkan nilai akurasi yang sama antara data uji steganografi dengan data latih hasil steganografi dan data uji steganografi dengan data latih suara asli untuk cropping 100 dan noise Gaussian variance 0.00000001 yaitu 80 %
- Rata-rata akurasi verifikasi suara dari 6 percobaan telah menghasilkan nilai yang lebih tinggi apabila data uji hasil steganografi diujikan dengan data latih hasil steganografi yaitu 85 % dibandingkan data uji hasil steganografi diujikan dengan data latih suara asli yaitu 77.91 %

5.2 Saran

Adapun saran untuk pengembangan tugas akhir selanjutnya adalah:

- Mengaplikasikan steganografi dengan sistem penyisipan lain agar lebih tahan serangan
- Speech yang digunakan lebih banyak kata-katanya tidak hanya satu
- Memakai metode lain seperti DWT
- Memakai metode pengklasifikasian yang lain seperti JST



DAFTAR PUSTAKA

- [1] Admin. 2008. diakses di <http://thesis.binus.ac.id/Asli/Bab2/2008-1-00283-MTIF%20Bab%202.pdf> pada tanggal 11 Oktober 2012 Pukul 20.00.
- [2] Admin. 2011. *definisi citra digital*, diakses di http://digilib.ittelkom.ac.id/index.php?option=com_content&view=article&id=840:definisi-citra-digital&catid=18:multimedia&Itemid=14 pada tanggal 12 Oktober 2012 pukul 16.00.
- [3] Aristya, Ni Made Lidya Dewi. 2013. *Simulasi dan Analisis Steganografi Citra Digital Menggunakan Metode Advanced Encryption Standard dan BCH Code*. Bandung : Institut Teknologi Telkom.
- [4] Ariyani, Nourma Dyah. 2012. *Analisis Teknik Autentikasi Watermark pada Citra Digital Dua Dimensi dengan Metode Weber's Descriptor*. Bandung: Institut Teknologi Telkom.
- [5] Budiyanto, Eko. Citra digital. Diakses di <http://geo.fis.unesa.ac.id/web/index.php/en/penginderaan-jauh/126-citra-digital> pada tanggal 12 Oktober 2012 pukul 16.00.
- [6] Evan. 2010. Diakses di <http://kuliahinformatika.wordpress.com/2010/02/13/buku-ta-k-nearest-neighbor-knn/> pada 12 Oktober 2012 pada pukul 22.00.
- [7] Fadhilah, Nurullaili. (2013). *Otomasi Music Player Speech Recognition Pada Platform Android*. Bandung: Institut Teknologi Telkom
- [8] Hasan, Rashidul Md., Mustafa Jamil, Md. Golam Rabbani, dan Md. Saifur Rahman. 2004. *Speaker Identification Using Mel Frequency Cepstral Coefficients*. Bangladesh University of Engineering and Technology, Dhaka.
- [9] Manunggal, H. S. (2005). *Perancangan dan Pembuatan Perangkat Lunak Pengenalan Suara Pembicara dengan Menggunakan Analisa MFCC*. Surabaya: Universitas Kristen Petra.

- [10] Munir,Rinaldi. 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Bandung: Informatika.
- [11] Mustofa, Ali. 2007. *Sistem Pengenalan Penutur dengan Metode Mel-frequency Wrapping*. Jurnal Teknik Elektro. Vol. 7. No. 2: 88 – 96.
- [12] S. C, "Hiden Bits: A Survey of Technique for Digital Watermarking," 2002.
- [13] Ulinnuha, Zulfa. (2011). Diakses di <http://paninalone.wordpress.com/2011/09/29/algoritma-nearest-neighbor/> pada 27 Juni 2013 pada pukul 16.29
- [14] X. J and W. Y, "Toward A Better Understanding of DCT Coefficient Watermarking," *IEEE*, p. 207, 2008.

