PERBANDINGAN METODE STEGANOGRAFI DCT DAN DWT PADA BERKAS VIDEO MP4

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau

OLEH:

MEILIA RIANTI
143510403

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2021

ABSTRAK

Kurangnya keamanan saluran tranmisi dalam jaringan pada saat pengiriman data dan menguji perbandingan proses enkripsi menggunakan Metode Steganografi DCT dan DWT Pada Berkas Video MP4. Tujuan dari penelitian ini untuk menguji kualitas stego-video setelah proses penyisipan gambar melalui pengukuran parameter Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE).Pada penelitian ini dilakukan analisis penyisipan file citra ke dalam file video menggunakan algoritma Discrete Cosine Transform (DCT) dan Discrete Wavelet Transform (DWT). File citra yang digunakan adalah berformat jpg dan gif dan format file video menggunakan AVI dan MP4.Setelah dilakukan pengujian kedua algoritma DCT dan DWT sebanyak 5 video dan juga 5 gambar, masing-masing stego-video mengalami perubahan nilai MSE dan PSNR. 2. Sistem yang dirancang berhasil mengetahui perbandingan hasil nilai MSE dan PSNR dari kedua algoritma tersebut dengan menunjukkan angka yang berbeda.Untuk menyempurnakan hasil dan menambahkan file image dan video lebih banyak untuk mengetahui nilai MSE dan PSNR yang lebih baik. 2. Untuk sistem yang dibangun selanjutnya agar lebih disempurnakan dengan menampilkan hasil nilai MSE dan PSNR setiap melakukan proses DCT dan DWT.

***Kata Kunci** : Steganografi, DCT, DWT, file citra, video*

ABSTRACT

Lack of security of transmission channels in the network at the time of data transmission and testing the comparison of encryption processes using the DCT and DWT Steganography Methods on MP4 Video Files. The goal of the study was to test the quality of stego-video after the image insertion process through measurements of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) parameters.The study analyzed the insertion of image files into video files using discrete cosine transform (DCT) and discrete wavelet transform (DWT) algorithms. The image files used are jpg and gif format and the video file format uses AVI and MP4. After testing both DCT and DWT algorithms as many as 5 videos and also 5 images, each stego-video experienced changes in MSE and PSNR values. 2. The designed system successfully knows the comparison of MSE and PSNR values from both algorithms by showing different numbers. To improve results and add more image and video files to better know mse and PSNR values. 2. For the system that is built next to be further refined by displaying the results of MSE and PSNR values each doing DCT and DWT processes.

keywords: Steganography, DCT, DWT, image file, video

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Assalamu'alaikum Wr.Wb.

Alhamdulillah, segala puji dan syukur penulis ucapkan kehadiran Allah SWT, karena atas rahmat dan hidayahnya penulis dapat menyelesaikan laporan penelitian skripsi dengan judul **"PERBANDINGAN METODE STEGANOGRAFI DCT DAN DWT PADA BERKAS VIDEO MP4"** dengan tujuan untuk memenuhi salah satu syarat menyelesaikan pendidikan Strata Satu (S1) Teknik informatika di Universitas Islam Riau Pekanbaru.

Dalam penulisan laporan penelitian skripsi ini, penulis banyak mendapat bantuan dan bimbingan dari berbagai pihak, baik secara langsung maupun tidak langsung. Pada kesempatan ini, penulis mengucapkan terima kasih

Akhirnya penulis berharap semoga skripsi ini dapat bermanfaat bagi kita semua, khususnya bagi mahasiswa Teknik Informatika Universitas Islam Riau. Penulis menyadari masih banyak kekurangan dalam penyusunan skripsi ini. Oleh karena itu penulis mengharapkan adanya masukan dari semua pihak demi menambah pengetahuan teknologi informasi di Indonesia

Pekanbaru, November 2021

Meilia Rianti

DAFTAR ISI

ABSTRAK i
ABSTRACT ii
KATA PENGANTAR iii
DAFTAR ISI iv
DAFTAR GAMBAR vi
DAFTAR TABEL vii
BAB I PENDAHULUAN
1.1 Latar Belakang 1
1.2 Identifkasi Masalah 2
1.3 Rumusan Masalah 3
1.4 Batasan Masalah 3
1.5 Tujuan Penelitian 3
1.6 Manfaat Penelitian 4
BAB II LANDASAN TEORI
2.1 Studi Kepustakaan 5
2.2 Dasar Teori 7
2.2.1 *Discrete Cosine Transform* (DCT) 7
2.2.2 *Discrete Wavelet Transform* (DWT) 7
2.2.3 Steganografi 8
2.2.4 *Embedding* Pesan Rahasia 11
2.2.5 *Ekstraksi* Pesan Rahasia 12
2.2.6 Java 13
2.2.7 Microsoft Visual Studio 14
BAB III METODOLOGI PENELITIAN
3.1 Definisi Masalah dan Analisis 15
3.2 Alat dan Bahan Penelitian yang Digunakan 16
3.2.1 Perangkat Keras (*Hardware*) 16
3.2.2 Perangkat Lunak (*Software*) 16

3.3 Data yang Digunakan 16
3.4 *Flowchart* Penyisipan DCT 18
3.5 *Flowchart* Ekstraksi DCT 19
3.6 *Flowchart* Penyisipan DWT 21
3.7 *Flowchart* Ekstraksi DWT 23
BAB IV HASIL DAN PEMBAHASAN
4.1 Hasil Pengujian 26
4.1.1 Hasil Analisis 26
4.1.2 Hasil Steganografi DCT 27
4.1.3 Hasil Steganografi DWT 29
BAB V KESIMPULAN DAN SARAN
5.1 Kesimpulan 31
5.2 Saran 31
DAFTAR PUSTAKA 32

DAFTAR GAMBAR

Gambar 2. 1 Diagram Blok Analisis Filter 8
Gambar 2. 2 Proses penyisipan pesan ke dalam media menggunakan DCT dan DWT 12
Gambar 2. 3 Alur Proses Ekstraksi Pesan dari Video 13
Gambar 3. 1 Frame Video. 17
Gambar 3. 2 Frame Citra 300 x 200 piksel 17
Gambar 3. 3 *Frame* Citra 3 x 3 piksel. ..... **Error! Bookmark not defined.**
Gambar 3. 4 *Flowchart* Penyisipan DCT 19
Gambar 3. 5 *Flowchart* Ekstraksi DCT 21
Gambar 3. 6 *Flowchart* Penyisipan DWT 23
Gambar 3. 7 *Flowchart* Ekstraksi DWT 25
Gambar 4. 1 Tampilan Halaman Utama 27
Gambar 4. 2 Tampilan Proses Steganografi Algoritma DCT 28
Gambar 4. 3 Tampilan Proses Steganografi Algoritma DWT 29

DAFTAR TABEL

Tabel 4. 1 Hasil Penyisipan Image Algoritma DCT 28
Tabel 4. 2 Hasil Penyisipan Image Algoritma DWT 30

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pesan digital dapat berbentuk teks, gambar, suara, atau video. Keamanan dari suatu pengiriman pesan digital terutama pesan digital rahasia sangatlah dibutuhkan. Hal ini ditujukan agar orang lain tidak dapat mengetahui pesan digital rahasia yang ingin disampaikan pengirim kepada penerima. Dengan terus berkembangnya bidang pengolahan dokumen digital, maka teknik keamanan bagi pesan digital pun dapat diselesaikan. Pesan rahasia digital dapat disisipkan ke dalam sebuah dokumen digital menggunakan sebuah teknik. Teknik penyisipan pesan rahasia digital ini dinamakan dengan steganografi. Steganografi merupakan sebuah ilmu, teknik atau seni menyembunyikan sebuah pesan rahasia dengan suatu cara sehingga pesan tersebut hanya akan diketahui oleh si pengirim dan si penerima pesan rahasia tersebut. Steganografi kebalikannya kriptografi yang menyamarkan arti dari sebuah pesan rahasia saja, tetapi tidak menyembunyikan bahwa ada sebuah pesan. Kelebihan Steganografi dibandingkan dengan Kriptografi adalah pesan-pesannya akan dibuat tidak menarik perhatian dan tidak menimbulkan kecurigaan, berbeda dengan Kriptografi yang pesannya tidak disembunyikan, walaupun pesannya sulit untuk di pecahkan akan tetapi itu akan menimbulkan kecurigaan pesan tersebut. Banyak metode yang dapat digunakan dalam teknik steganografi ini misalnya Least Significant Bit (LSB), Discrete Wavelet Transform (DWT), atau Discrete Cosine Transform (DCT). Least Significant Bit (LSB) merupakan metode yang digunakan dalam domain spasial

sedangkan Discrete Wavelet Transform (DWT) dan Discrete Cosine Transform (DCT) merupakan metode yang digunakan dalam domain transformasi. Fungsi DCT dan DWT yaitu mentransformasi data dari satu tempat (domain) ke tempat (domain) yang lain. Fungsi DCT yaitu mentransformasi data dari tempat spatial (spatial domain) ke tempat frekuensi (frequency domain).

Pada penelitian ini akan di analisis perbandingan metode-metode yang dapat digunakan dalam teknik steganografi, pada penelitian ini akan membandingkan metode sehingga mampu mengenkripsi dan deskripsi data tanpa mengubah integritas data tersebut. Berdasarkan latar belakang permasalahan di atas, maka penelitian ini akan menggunakan metode Discrete Wavelet Transform (DWT), atau Discrete Cosine Transform (DCT). Membandingkan dua metode tersebut pada berkas video. Sehingga penulis menarik sebuah judul yaitu "Perbandingan Metode Steganografi DCT dan DWT Pada Berkas Video MP4".

1.2 Identifkasi Masalah

Berdasarkan permasalahan yang telah diuraikan diatas, maka identifikasi masalah dalam pembuatan sistem ini adalah sebagai berikut:

1. Kurangnya keamanan saluran tranmisi dalam jaringan pada saat pengiriman data, sehingga membutuhkan proses menyembunyikan keberadaan (existence) pesan data untuk keamanan proses megirim data, tujuannya untuk menghindari kecurigaan (conspicuous) dari pihak ketiga (lawan).
2. Menguji perbandingan proses enkripsi menggunakan Metode Steganografi DCT dan DWT Pada Berkas Video MP4.

1.3 Rumusan Masalah

Pada penelitian ini, penulis merumuskan masalah sebagai berikut:

1. Bagaimana membandingan proses menyembunyikan pesan (information hiding) menggunakan Metode Steganografi DCT dan DWT pada berkas video MP4?
2. Bagaimana merancang aplikasi dengan membandingkan 2 metode steganografi DCT dan DWT penyembunyian pesan gambar ke dalam media video?

1.4 Batasan Masalah

Agar penelitian ini lebih terarah dan tidak menimbulkan perluasan pada pembahasannya nanti, maka diberi batasan ruang lingkup pembahasan yang dibahas. Batasan masalah yang dimaksud adalah:

1. Wadah yang digunakan untuk menyisipkan data adalah media dalam bentuk video dengan format MP4.
2. Hasil *file output* disimpan dengan format MP4stego.
3. Pada implementasi perangkat lunak dengan 2 metode steganografi DCT dan DWT data rahasia di enkripsi terlebih dahulu baru disisipkan pada file video MP4.

1.5 Tujuan Penelitian

Adapun tujuan dari penelitian ini untuk menguji kualitas stego-video setelah proses penyisipan gambar melalui pengukuran parameter Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE).

1.6 Manfaat Penelitian

Adapun manfaat dari penelitian yang dilakukan adalah :

1. Agar dapat mengamankan pesan maupun data rahasia sehingga aman.
2. Agar dapat digunakan sebagai salah satu program oprasional untuk penigkatan efisiensi kemanan penyimpanan maupun pengiriman data.
3. Agar dapat mengetahui perbandingan antara 2 metode steganografi berbeda kedalam aplikasi.

BAB II

LANDASAN TEORI

2.1 Studi Kepustakaan

Untuk menyusun proposal penelitian ini penulis juga melakukan studi kepustakaan yang merujuk kepada penelitian-penelitian sebelumnya yang berkaitan dengan penelitian yang penulis buat. Studi kepustakaan ini dilakukan sebagai bahan perbandingan dan referensi bagi penulis.

Studi keperpustakaan pertama adalah berdasarkan penelitian yang dilakukan oleh Indra Jaya Kusuma (2017), yang bertujuan untuk mengamankan pesan dengan cara menyembunyikan *file* ke dalam *file* lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu didalam *file* tersebut dengan menggunakan metode *parity coding* untuk memecahkan *file* audio menjadi beberapa *region* yang berbeda dan mengenkripsi setiap *bit* dari *file* rahasia yang ingin disisipkan pada sebuah sampel *region* yang berisi *parity bit*.

Studi keperpustakaan kedua adalah berdasarkan penelitian yang dilakukan oleh Akik Hidayat (2009), Keamanan dan kerahasiaan sangat dibutuhkan dalam dunia komunikasi khususnya dalam dunia komunikasi digital. Diperlukan metode khusus untuk menjamin keamanan informasi, supaya informasi hanya dapat dimengerti oleh pihak yang dituju. Teknik yang umum digunakan adalah dengan mengacak data atau Kriptografi. Tetapi informasi yang diacak sering menimbulkan kecurigaan, maka dibutuhkan teknik lain yaitu dengan menyembunyian data atau Steganografi. Teknik Steganografi dapat diterapkan sebagai kelanjutan dari Kriptografi, dan kombinasi dari keduanya akan

menghasilkan tingkat keamanan data yang sangat tinggi. Akan diperlihatkan menggabungkan teknik Kriptografi dan Steganografi untuk menjaga keamanan data teks sekaligus menyisipkan data teks tersebut dalam gambar digital tanpa mengubah gambar tersebut secara visual,sehingga menghasilkan sebuah metode Steganografi yang optimal untuk menyembunyikan suatu pesan teks di dalam sebuah gambar digital.

Studi keperpustakaan ketiga adalah berdasarkan penelitian yang dilakukan oleh Andreas Nicolas Tarigan (2014), Steganografi merupakan ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa pesan tersebut adalah sebuah pesan rahasia. Tujuan dari penelitian ini adalah untuk mengimplementasikan steganografi dengan metode *Least significant Bit Insertion* dalam penyembunyian *file* pada media video dengan format MP4 dan dapat dijadikan sebagai aplikasi *alternative* dalam penyembunyian *file* yang aman pada *file video*.

Orisinalitas pada penelitian ini dibandingkan dengan ketiga penelitian tersebut adalah pada metode yang digunakan, dimana pada penelitian tersebut menggunakan metode *parity coding*, metode kombinasi antara kriptografi dan steganografi, dan metode *Least significant Bit Insertion*, sedangkan pada penelitian ini mengangkat metode perbandingan antara DCT dan DWT. Persamaan dalam penelitian ini adalah sama-sama menggunakan metode steganografi.

2.2 Dasar Teori

Berikut ini adalah beberapa dasar teori yang berkenaan dalam penelitian tugas akhir ini:

2.2.1 *Discrete Cosine Transform* (DCT)

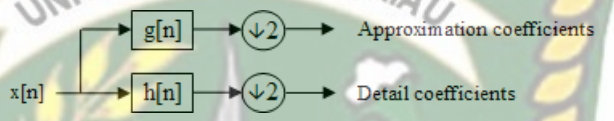
DCT adalah sebuah skema lossy compression dimana NxN blok ditransformasikan dari domain spasial ke domain DCT. Pada umumnya, DCT merupakan transformasi one-to-one mapping dari suatu array berisi nilai piksel menjadi komponen- komponen yang terbagi berdasarkan frekuensinya. Steganografi menggunakan DCT dilakukan dengan melakukan transformasi video kemudian dilakukan modifikasi terhadap koefisien DCT sesuai dengan bit pesan yang disisipkan. Setelah proses penyisipan selesai dilakukan, inverse DCT sebagai finalisasi untuk mengembalikan data citra ke domain spasial sehingga dapat kembali direpresentasikan.

2.2.2 *Discrete Wavelet Transform* (DWT)

DWT bekerja dengan membagi frekuensi gambar/frame kedalam beberapa sub-band frekuensi: rendah, menengah, dan tinggi. Dekomposisi 2D-DWT level 1 akan memecah frame menjadi beberapa frekuensi: Low-low frequency (LL), low-high frequency (LH), high-low frequency (HL), dan high- high frequency (HH). Dimana LL sub-band adalah aproksimasi frame, LH mendefinisikan frekuensi horizontal, HL mendefinisikan frekuensi vertikal, dan HH memberikan detail informasi frame, seperti nilai diagonal.

Dalam DWT, penggambaran sebuah skala waktu sinyal digital didapatkan dengan menggunakan teknik filterisasi digital [11]. Sinyal DWT (x) diuraikan

secara bersamaan menggunakan high pass (h) dan low pass (g) filter. Penguraian sinyal menggunakan high pass filter akan menghasilkan koefisien detail sedangkan penggunaan low pass filter akan menghasilkan koefisien aproksimasi. Kedua filter bekerja saling terkait satu sama lain atau disebut dengan filter cermin segi empat. Gambar 1 merupakan diagram keterkaitan antara filter high dan low pass.



Gambar 2. 1 Diagram Blok Analisis Filter

2.2.3 Steganografi

Steganografi adalah ilmu dan seni untuk menyembunyikan suatu informasi "rahasia" didalam suatu informasi lainnya. Steganografi juga merupakan teknik menyembunyikan data dalam data lain yang akan ditumpanginya tanpa mengubah data tersebut sehingga pada data yang ditumpangi sebelum dan setelah proses penyembunyian hampir sama (Ariyus, 2006).

Dalam buku Histories of Herodatus Steganografi dengan media kepala budah (dikisahkan oleh Herodatus, penguasa Yunani di tahun 440 BC. Yaitu dengan cara kepala budak dibotaki, ditulisi pesan, rambut budak dibiarkan tumbuh, budak dikirim. Ditempat penerima kepala budak digunduli supaya pesan dapat terbaca. Pemakaian tinta tak-tampak (invisible ink), tinta dibuat dari campuraan sari buah, susu dan cuka. Tulisan diatas kertas bisa dibaca dengan memanaskan kertas tersebut.

Cara kerja atau prinsip dari steganografi adalah, untuk menyisipkan suatu pesan atau data yang ingin disembunyikan harus menggunakan dua unsur. Unsur pertama adalah media penampung seperti citra, suara, video, dan lain sebagainya yang tidak membuat curiga untuk menyiman pesan rahasia. Unsur kedua adalah pesan yang hendak disembunyikan yakni media penampung dalam bentuk citra yang disebut cover-object dan citra yang sudah disisipi pesan disebut stego-object.

Umumnya, ada dua proses dalam steganografi, yakni proses embedding untuk menyisipkan pesan kedalam cover-object dan proses decording untuk ekstrasi pesan dari stego-object. Kedua proses ini membutuhkan kunci rahasia yang disebut dengan stego-key supaya hanyak pihak yang memiliki hak saja yang bisa melakukan penyisipan dan ekstrasi pesan.

Menurut Cahyadi (2012), bahwa ada beberapa contoh media penyisipan pesan rahasia yang digunakan dalam teknik *steganography* antara lain:

1. Teks

Dalam algoritma *steganography* yang menggunakan teks sebagai media penyisipan biasanya digunakan teknik NLP (*Natural Language Processing*) sehingga teks yang telah disisipi pesan rahasia tidak akan mencurigakan untuk orang yang melihatnya.

2. Gambar

Format gambar paling sering digunakan, karena format ini merupakan salah satu format *file* yang sering dipertukarkan dalam dunia internet. Alasan lainnya adalah banyaknya tersedia algoritma *Steganography* untuk media penampung yang berupa citra.

3. Audio

Format ini pun sering dipilih karena biasanya berkas dengan format ini berukuran relatif besar, sehingga dapat menampung pesan rahasia dalam jumlah yang besar pula.

4. Video

Format ini memang merupakan format dengan ukuran *file* yang relatif sangat besar namun jarang digunakan karena ukurannya yang terlalu besar sehingga mengurangi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini.

Sebuah steganografi memiliki tiga aspek yang dapat menentukan berhasil tidaknya sebuah steganografi dalam melakukan pekerjaannya (Ermadi dkk, 2004):

1. Kapasitas (*capacity*)

Kapasitas merujuk pada jumlah informasi yang bisa disembunyikan dalam medium *cover*. Keamanan adalah ketidakmampuan pengamat untuk mendeteksi pesan tersembunyi dan ketahanan dalam jumlah modifikasi medium stego yang bisa bertahan sebelum musuh merusak pesan rahasia tersembunyi tersebut.

2. Keamanan (*security*)

Keamanan dari sistem steganografi klasik mewujudkan kerahasiaan sistem *encodingnya.*

3. Ketahanan (*robustness*)

Ketahanan mangacu pada data citra penampung seperti pengubah kontras, penajaman, rotasi, perbesar gambar, pemotongan dan lain-lainnya. Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.

2.2.4 *Embedding* Pesan Rahasia

Embedding adalah proses menyisipkan pesan rahasia kedalam objek stego. Embedding pada penelitian ini diawali dengan membaca frame dari video yang telah dipilih, kemudian dilakukan transformasi DWT dan DCT tiap frame yang berhasil dibaca. Menyisipkan bit-bit pesan ke dalam frame pada high frekuensi band hingga semua bit pesan masuk seluruhnya. Pada penelitian ini, sistem memiliki fungsi untuk dapat menghitung nilai PSNR dan MSE dari video yang telah melalui proses stego-video. Alur proses penyisipan pesan kedalam media menggunakan DCT dan DWT pada penelitian ini dapat dilihat pada Gambar 2.2.

Kualitas objek hasil stego-video dapat diukur dari tingkat perbedaan objek original dengan hasil proses stego-video. Kualitas stego-video dapat diuji secara eksperimental menggunakan metode kuantifikasi PSNR dalam decibel (dB) dapat dihitung menggunakan persamaan berikut :

$$PSNR = 10 \log_{10} \frac{Max_{or}2}{MSE}$$

Dengan

$$MSE = \frac{1}{r \; x \; c} \sum_{i=0}^{r-1} \sum_{j=0}^{c-1} (or_{i,j} - st_{i,j})$$

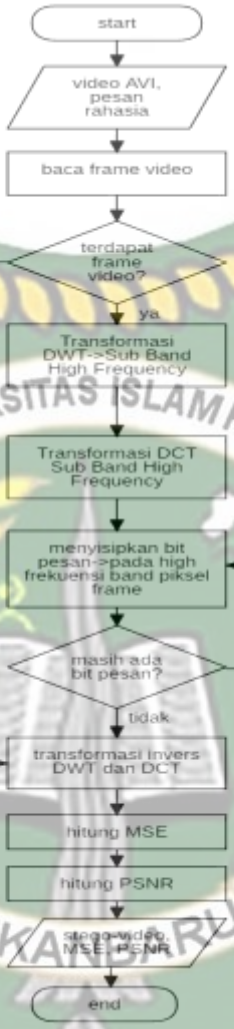
Dimana :

or = *original frame*

st = *stego frame*

r,c = *resolusi frame*

Max_{or} = nilai *pixel* maksimum dari *frame* asli



Gambar 2. 2 Proses penyisipan pesan ke dalam media menggunakan DCT dan DWT

2.2.5 *Ekstraksi* Pesan Rahasia

Proses ektraksi ditujukan untuk mendapatkan pesan rahasia yang berhasil disematkan di dalam sebuah media. Proses ini diperlukan agar sisi penerima dapat mengerti dan mendapatkan pesan yang dikirimkan oleh pengirim. Pesan yang diekstraksi haruslah sama dengan pesan yang dikirimkan tanpa adanya informasi yang hilang. Alur proses ekstraksi pesan menggunakan sistem ini dapat dilihat pada Gambar 2.3.

Gambar 2. 3 Alur Proses Ekstraksi Pesan dari Video

2.2.6 Java

Java adalah sebuah bahasa pemrograman *scripting* yang sering digunakan dalam pembuatan aplikasi berbasis *handphone* dan juga dapat digunakan untuk menyediakan akses objek yang disisipkan di aplikasi lain. Java berfungsi sebagai penambah tingkah laku agar *widget* dapat tampil lebih efektif (Garling dan Lestari *dalam* Achmad Fikri Sallaby 2015).

2.2.7 Microsoft Visual Studio

Microsoft Visual Studio merupakan sebuah perangkat lunak(suite) yang dapat digunakan untuk melakukan pengembangan aplikasi, baik itu aplikasi bisnis, aplikasi personal, ataupun komponen aplikasinya, dalam bentuk aplikasi console, aplikasi windows atau aplikasi web. Visual studio mencakup compiler, SDK, Integrated Development Environment(IDE), dan dokumentasi(umumnya berupa MSDN Library). Kompiler yang dimasukkan ke dalam paket Visual Studio antara lain Visual C++, Visual C#, Visual Basic, Visual Basic .NET, Visual InterDev, Visual J++, Visual J#, Visual Fox Pro, dan Visual SourceSafe.

Microsoft Visual Studio dapat digunakan untuk mengembangkan apliaksi dalam native code(dalam bentuk bahasa mesin yang berjalan di atas windows) ataupun managed code(dalam bentuk Microsoft Intermediate Language di atas .NET Framework). Selain itu Visual Studio juga dapat digunakan untuk mengembangkan apliaksi Silverlight, apliaksi Windows Mobile(yang berjalan di atas .NET Compact Framework).

BAB III

METODOLOGI PENELITIAN

Metodologi penelitian adalah langkah-langkah atau tahapan perencanaan dengan bantuan beberapa metode, teknik, alat (*tools*) dan dokumentasi dengan tujuan untuk membantu peneliti dalam meminimalkan resiko kegagalan dan menekankan pada proses atau sasaran penelitian (Zainal A. Hasibuan, 2007).

3.1 Definisi Masalah dan Analisis

Pada penelitian ini dilakukan analisis penyisipan file citra ke dalam file video menggunakan algoritma *Discrete Cosine Transform* (DCT) dan *Discrete Wavelet Transform* (DWT). File citra yang digunakan adalah berformat jpg dan gif dan format file video menggunakan AVI dan MP4. Pada fase penyisipan, file video bertindak sebagai media *cover* yang terdiri dari beberapa *frame* untuk tempat penyisipan. Setiap *frame* kemudian diubah menjadi model ruang warna Red Green Blue (RGB). Transformasi DWT dan DCT diterapkan pada RGB dimana pada *sub-band* frekuensi tinggi digunakan untuk penyisipan. Penyisip berupa file citra yang berformat JPG maupun Gif diubah menjadi bit stream biner. Setiap bit penyisip dimasukkan ke dalam koefisien DWT-DCT RGB dari frame video. Lalu dilakukan transformasi Invers DWT dan DCT diterapkan untuk mengembalikan *frame Stego* dalam domain spasialnya membentuk *Stego video*.

Pada fase ekstraksi, *stego video* dibaca untuk mendapatkancitra penyisip dari stego video. *Stego video* dibagi menjadi beberapa frame diambil untuk proses ekstraksi. Setiap frame kemudian diubah menjadi model ruang warna RGB. Transformasi DWT dan DCT diterapkan pada RGB. Frekuensi tinggi *sub-band*

digunakan untuk ekstraksi. Bit-bit diekstrak dari koefisien DWT-DCT sebesarnilai RGBnya dan kemudian bit biner tersebut diubah menjadi nilai desimal untuk membentuk matriks citra sebagai file *embed* citra hasil ekstraksi.

3.2 Alat dan Bahan Penelitian yang Digunakan

Adapun spesifikasi perangkat keras (*hardware*) yang digunakan untuk melakukan pengujian dan spesifikasi perangkat lunak (*software*) yang dibutuhkan untuk sistem yang akan dibangun adalah sebagai berikut:

3.2.1 Perangkat Keras (*Hardware*)

Spesifikasi perangkat keras (*hardware*) yang digunakan dalam penelitian ini adalah sebagai berikut:

1. *Processor* : *Intel Inside*
2. RAM : 4 GB
3. *Hardisk* : 1 TB
4. *System Type* : 64-bit *Operating System*

3.2.2 Perangkat Lunak (*Software*)

Perangkat lunak (*Software*) yang digunakan dalam pembuatan pengujian kinerja ini sebagai berikut:

1. Sistem Operasi : *Microsoft Windows* 10
2. Bahasa Pemrograman : *Microsoft Visual Studio, Phyton*

3.3 Data yang Digunakan

Data yang digunakan pada penelitian ini adalah file video dan citra yang diambil penulis sebagai file citra penyisip (*embedimage*) adalah berformat jpg dan gif serta file video yang disisipi berformat Avi dan mp4.

File video yang akan diproses terdiri dari *frame-frameimage* (citra) yang berdimensi tertentu seperti pada Gambar 3.1.

Gambar 3. 1 *Frame* Video.

Citra frame-frame video tersebut diambil dari stream video yang kemudian dibaca nilai pikselnya dan sebagai contoh diberikan frame video berupa citra berdimensi 300 x 200 piksel seperti pada Gambar 3.2.

Gambar 3. 2 *Frame* Citra 300 x 200 *piksel*

Citra pada Gambar 3.2 di atas dilakukan penghitungan nilai komponen warna RGB-nya dengan membagi frame citra dalam piksel-piksel. Sebagai contoh diberikan cuplikan frame citra dengan ukuran 3 x 3 piksel seperti Gambar 3.3.

(0,0)	(0,1)	(0,2)
(1,0)	(1,1)	(1,2)
(2,0)	(2,1)	(2,2)

Gambar 3. 3 *Frame* Citra 3 x 3 piksel

3.4 *Flowchart* Penyisipan DCT

Adapun *flowchart* penyisipan video dengan citra menggunakan algoritma DCT dapat dilihat seperti pada Gambar 3.4.

Keterangan:

Pada *flowchart* dibawah, input data berupa file video berformat Avi dan Mp4 serta file penyisip citra berformat Jpg dan Gif. Setelah dilakukan penginputan, maka dilakukan proses pembacaan frame video. Apabila frame video ada, maka melakukan proses Transformasi DCT setiap frame menjadi Frekuensi Band, jika tidak ada maka akan langsung menuju ke Transformasi Invers DCT. Dan selanjutnya melakukan proses penyisipan bit-bit key dan embednya menjadi Pixel Frame pada Frekuensi Tengah. Didalam penyisipan embed ini jika dia benar maka akan mengulangi penyisipannya kembali, sedangkan jika salah maka dilakukan proses Transformasi Invers DCT. Setelah dilakukan penyisipan, maka dihitung nilai MSE dan PSNR dan menghasilkan output File Stego Video, MSE dan PSNR.

Gambar 3. 4 *Flowchart* Penyisipan DCT

3.5 *Flowchart Ekstraksi* DCT

Adapun *flowchart* ekstraksi file citra dari file *stego video* menggunakan algoritma DCT dapat dilihat seperti pada Gambar 3.5.

Keterangan:

Pada *flowchart* dibawah, input data berupa file stego video serta file penyisip citra berformat Jpg dan Gif. Setelah dilakukan penginputan, maka dilakukan proses pembacaan frame video. Apabila frame video ada, maka

melakukan proses Transformasi DCT setiap frame menjadi Frekuensi Band, jika tidak ada maka akan langsung menuju ke Transformasi Invers DCT. Dan selanjutnya melakukan proses penyisipan bit-bit key dan embednya menjadi Pixel Frame pada Frekuensi Tengah. Didalam penyisipan embed ini jika benar maka akan mengulangi penyisipannya kembali, sedangkan jika salah maka dilakukan proses Transformasi *Invers* DCT. Setelah dilakukan Transformasi Invers DCT selanjutnya dilakukan proses pengkonversian bit-bit embed ke desimal. Langkah selanjutnya simpan desimal menjadi matriks citra embed dan menghasilkan *output* citra *embed*.

Gambar 3. 5 *Flowchart* Ekstraksi DCT

3.6 *Flowchart* Penyisipan DWT

Adapun *flowchart* penyisipan video dengan citra menggunakan algoritma DWT dapat dilihat seperti pada Gambar 3.6.

Keterangan:

Pada *flowchart* dibawah, input data berupa file video berformat Avi dan Mp4 serta file penyisip citra berformat Jpg dan Gif. Setelah dilakukan penginputan, maka dilakukan proses pembacaan frame video. Apabila frame video ada, maka melakukan proses Transformasi DWT setiap frame menjadi High Frekuensi Band, jika tidak ada maka akan langsung menuju ke Transformasi Invers DWT. Dan selanjutnya melakukan proses penyisipan bit-bit key dan embednya menjadi pixel Frame pada High Frekuensi Band. Didalam penyisipan embed ini jika dia benar maka akan mengulangi penyisipannya kembali, sedangkan jika salah maka dilakukan proses Transformasi Invers DWT. Setelah dilakukan penyisipan, maka dihitung nilai MSE dan PSNR dan menghasilkan output File Stego Video, MSE dan PSNR.

Gambar 3. 6 *Flowchart* Penyisipan DWT

3.7 *Flowchart Ekstraksi* DWT

Adapun *flowchart* ekstraksi file citra dari file *stego video* menggunakan algoritma DCT dapat dilihat seperti pada Gambar 3.7.

Keterangan:

Pada *flowchart* diatas, input data berupa file stego video serta file penyisip

citra berformat Jpg dan Gif. Setelah dilakukan penginputan, maka dilakukan proses pembacaan frame video. Apabila frame video ada, maka melakukan proses Transformasi DWT setiap frame menjadi High Frekuensi, jika tidak ada maka akan langsung menuju ke Transformasi Invers DWT. Dan selanjutnya melakukan proses pembacaan bit-bit embednya menjadi Pixel Frame pada High Frekuensi Band. Didalam penyisipan embed ini jika benar maka akan mengulangi penyisipannya kembali, sedangkan jika salah maka dilakukan proses Transformasi Invers DWT. Setelah dilakukan Transformasi Invers DWT selanjutnya dilakukan proses pengkonversian bit-bit embed ke desimal. Langkah selanjutnya simpan desimal menjadi matriks citra embed dan menghasilkan output citra embed

Gambar 3. 7 *Flowchart* Ekstraksi DWT

BAB IV

HASIL DAN PEMBAHASAN

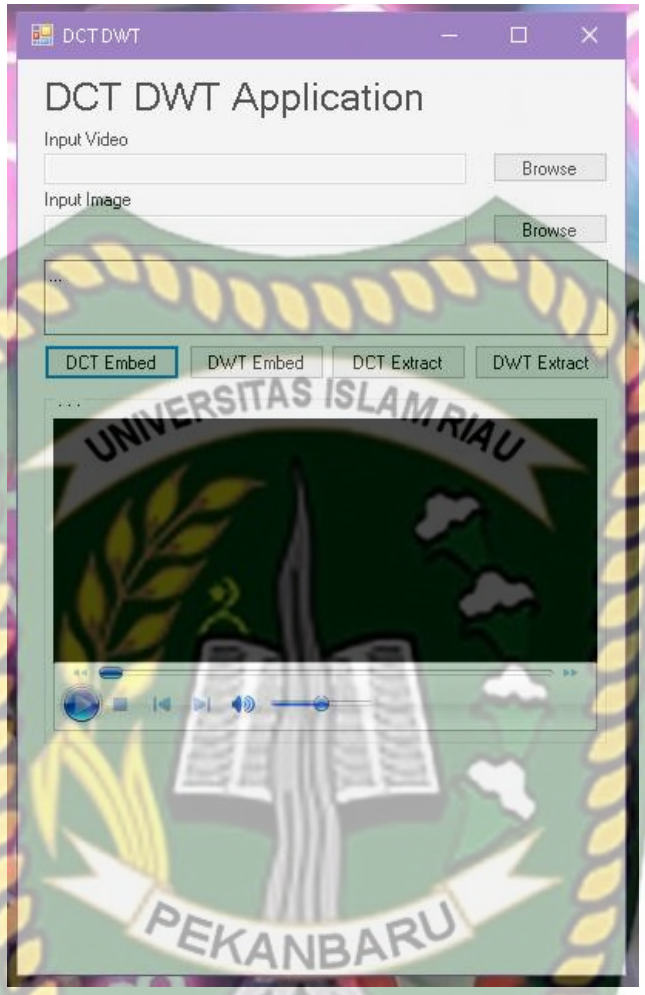
4.1 Hasil Pengujian

Pengujian yang dilakukan penulis untuk mendapatkan nilai ukuran video dari kedua algoritma yaitu algoritma *Discrete Cosine Transform* (DCT) dan *Discrete Wavelet Transform* (DWT). File citra yang digunakan adalah berformat JPG dan GIF dan format file video menggunakan AVI dan MP4. Pada fase penyisipan, file video bertindak sebagai media *cover* yang terdiri dari beberapa *frame* untuk tempat penyisipan. Selanjutnya untuk mengukur kehandalan algoritma dilakukan perhitungan nilai *Mean Squared Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) rata-rata sebagai *output* proses penyisipan.

Pada fase ekstraksi, *stego video* dibaca untuk mendapatkan citra penyisip dari *stego video*. *Stego video* dibagi menjadi beberapa *frame* diambil untuk proses ekstraksi. Setiap frame kemudian diubah menjadi model ruang warna RGB. Transformasi DWT dan DCT diterapkan pada RGB. Frekuensi tinggi *sub-band* digunakan untuk ekstraksi. Bit-bit diekstrak dari koefisien DWT-DCT sebesar nilai RGBnya dan kemudian bit biner tersebut diubah menjadi nilai desimal untuk membentuk matriks citra sebagai file *embed* citra hasil ekstraksi.

4.1.1 Hasil Analisis

Program yang sudah siap dirancang selanjutnya dilakukan implementasi untuk melakukan proses penyisipan dengan ketiga algoritma yang telah dirancang



Gambar 4. 1 Tampilan Halaman Utama

Pada gambar 4.1 terlihat menu input video dan input image serta tampilan output video dan image.

4.1.2 Hasil Steganografi DCT

Tampilan hasil steganografi DCT adalah program untuk melakukan penyisipan file image dengan algoritma DCT. Dapat dilihat pada gambar 4.2.

Gambar 4. 2 Tampilan Proses Steganografi Algoritma DCT

Pada gambar 4.2 hasil penyisipan file image berformat jpg dengan file video berformat mp4. untuk hasil perhitungannya dapat dilihat pada tabel berikut :

Tabel 4. 1 Hasil Penyisipan Image Algoritma DCT

No.	Video	Resolusi Video	Image	Resolusi Image	MSE	PSNR
1	1.mp4	640x360	1.jpg	640x480	14,5900	0,582

2	2.mp4	640x352	2.jpg	640x360	16,4773	1,798
3	3.mp4	640x360	3.jpg	234x159	8,3735	1,913
4	4.mp4	640x360	4.jpg	344x363	8,7945	1,928
5	5.mp4	640x360	5.jpg	580x842	7,6503	1,965
Rata-rata					**11,177114**	**1,637138**

Dari tabel hasil penyisipan file image dengan algoritma DCT dapat diperoleh nilai rata-rata MSE = **11,177114** dan PSNR = **1,637138**

4.1.3 Hasil Steganografi DWT

Tampilan hasil steganografi DWT adalah program untuk melakukan penyisipan file image dengan algoritma DWT. Dapat dilihat pada gambar 4.3.

Gambar 4. 3 Tampilan Proses Steganografi Algoritma DWT

Pada gambar 4.3 hasil penyisipan file image berformat jpg dengan file video berformat mp4. untuk hasil perhitungannya dapat dilihat pada tabel berikut :

Tabel 4. 2 Hasil Penyisipan Image Algoritma DWT

No.	Video	Resolusi Video	Image	Resolusi Image	MSE	PSNR
1	1.mp4	640x360	1.jpg	640x480	27310,6	2,218
2	2.mp4	640x352	2.jpg	640x360	20538,0	0,250
3	3.mp4	640x360	3.jpg	234x159	727,4	0,944
4	4.mp4	640x360	4.jpg	344x363	5673,1	0,523
5	5.mp4	640x360	5.jpg	580x842	545,3	1,038
Rata-rata					**10958,88**	**0,995**

Dari tabel hasil penyisipan file image dengan algoritma DWT dapat diperoleh nilai rata-rata MSE = **10958,88** dan PSNR = **0,995**.

Dari hasil penyisipan gambar pada kedua algoritma diatas dapat dilihat bahwa algoritma terbaik adalah algoritma DCT dengan nilai MSE sebesar 11,17711358.

Tabel 4. 3 Hasil Analisa Perbandingan Metode DCT & DWT

Metode DCT	**Metode DWT**
1. Ukuran *file* mengalami perubahan 2. Algoritma lebih unggul adalah algoritma DCT dengan nilai MSE sebesar 11,17711358.dari algoritma DWT 3. Dari 5 pengujian pada tabel 4.1 nilai Rata – rata PSNR yang dihasilkan PSNR = 1,637138008	1. Ukuran *file* mengalami perubahan 2. Algoritma DWT dapat diperoleh nilai rata-rata MSE = 10958,88184 3. Dari 5 pengujian pada tabel 4.2 nilai Rata- rata PSNR yang dihasilkan PSNR = 0,994655251.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dari penelitian diatas dapat disimpulkan beberapa hal seperti berikut :

1. Setelah dilakukan pengujian kedua algoritma DCT dan DWT sebanyak 5 video dan juga 5 gambar, masing-masing stego-video mengalami perubahan nilai MSE dan PSNR yang dapat dilihat pada tabel 4.1 dan 4.2.
2. Sistem yang dirancang berhasil mengetahui perbandingan hasil nilai MSE dan PSNR dari kedua algoritma tersebut dengan menunjukkan angka yang berbeda.

5.2 Saran

Dari hasi penelitian ini, adapun beberapa saran yang dibutuhkan adalah :

1. Untuk menyempurnakan hasil dan menambahkan file image dan video lebih banyak untuk mengetahui nilai MSE dan PSNR yang lebih baik.
2. Untuk sistem yang dibangun selanjutnya agar lebih disempurnakan dengan menampilkan hasil nilai MSE dan PSNR setiap melakukan proses DCT dan DWT.

DAFTAR PUSTAKA

Ariyus. Dony, 2006. "Kriptografi Keamanan Data dan Komunikasi". Graha Ilmu, Yogyakarta.

Cahyadi, Tri. 2012. "Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG."

Faruq, Umar Al. 2015. "Rancang Bangun Aplikasi Rekam Medis Poliklinik Universitas Trilogi." *Jurnal Informatika*.

Fatima, Siti. 2015. "Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan)." *Jurnal Ilmu Komputer dan Informatika*.

Galing, Hartanto Arum, 2010. Pembuatan Aplikasi Widget Untuk Monitoring Saham. STMIK AMIKOM. Yogyakarta.

Gata, Windu dan Gata, Grace. (2013). Sukses Membangun Aplikasi Penjualan dengan Java. Jakarta : Elex Media Komputindo.

Haviluddin. 2011. "Memahami Penggunaan UML (Unified Modelling Language)." *Memahami Penggunaan UML (Unified Modelling Language)* 6(1): 1–15. https://informatikamulawarman.files.wordpress.com/2011/10/01-jurnal-informatika-mulawarman-feb-2011.pdf.

Hidayat, Akik. 2009. Kriptografi dan Stenografi Menggunakan Algoritma Vignere dan Tiny Enkripsion Algorithm. Repositoy UNPAD, Indonesia

Informatika, Pelita, and Budi Darma. 2014. "Pembuatan Aplikasi Penyisipan Pesan Pada File Mp3 Menggunakan Metode Parity Coding Dan Enkripsi Caesar Cipher." : 50–56.

Kusuma, Indra Jaya. 2017. "Analisis Teknik Steganografi Pada Audio MP3 Menggunakan Metode Parity Coding Dan Enkripsi Cipher Transposition."

Jurnal Elektronik Sistem Informasi dan Komputer p. ISSN: 2477-5290 e. ISSN: 2502-2148 3(2). http://www.jesik.web.id/index.php/jesik/article/download/65/44%0A.

Nurdam, Nofriyadi. 2014. "Sequence Diagram Sebagai Perkakas Perancangan Antarmuka Pemakai." *Jurnal ULTIMATICS* 6(1): 21–25.

Sallaby, Achmad Fikri, Feri Hari Utami, and Yode Arliando. 2015. "Aplikasi Widget Berbasis Java." *Jurnal Media Infotama*.

Shalahuddin, M., A.S Rosa.(2008).Pemrograman J2ME Belajar Cepat Pemrograman Perangkat Telekomunikasi Mobile, Bandung: Penerbit Informatika

Suendri. 2018. "Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem (Studi Kasus : UIN Sumatera Utara Medan)." *Jurnal Ilmu Komputer dan Informatika*.

Witten, Jeffery L, et all.2004.Metode Disain & Analysis Sistem (Terjemahan). Yogyakarta: Andi Offset