Penyembunyian Data pada *File* Video Menggunakan Metode LSB dan DCT

Mahmuddin Yunus*[1] dan Agus Harjoko[2]
[1]Program Studi Ilmu Komputer, FMIPA UGM
[2]Jurusan Ilmu Komputer dan Elektronika, FMIPA UGM
Gedung SIC Lt.3 FMIPA UGM Sekip Utara Bulaksumur Yogyakarta
email: *[1]**didin_my@yahoo.co.id**, [2]aharjoko@ugm.ac.id

Abstrak

Penyembunyian data pada file video dikenal dengan istilah steganografi video. Metode steganografi yang dikenal diantaranya metode Least Significant Bit (LSB) dan Discrete Cosine Transform (DCT). Dalam penelitian ini dilakukan penyembunyian data pada file video dengan menggunakan metode LSB, metode DCT, dan gabungan metode LSB-DCT. Sedangkan kualitas file video yang dihasilkan setelah penyisipan dihitung dengan menggunakan Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). Uji eksperimen dilakukan berdasarkan ukuran file video, ukuran file berkas rahasia yang disisipkan, dan resolusi video.

Hasil pengujian menunjukkan tingkat keberhasilan steganografi video dengan menggunakan metode LSB adalah 38%, metode DCT adalah 90%, dan gabungan metode LSB-DCT adalah 64%. Sedangkan hasil perhitungan MSE, nilai MSE metode DCT paling rendah dibandingkan metode LSB dan gabungan metode LSB-DCT. Sedangkan metode LSB-DCT mempunyai nilai yang lebih kecil dibandingkan metode LSB. Pada pengujian PSNR diperoleh data bahwa nilai PSNR metode DCT lebih tinggi dibandingkan metode LSB dan gabungan metode LSB-DCT. Sedangkan nilai PSNR metode gabungan LSB-DCT lebih tinggi dibandingkan metode LSB.

Kata Kunci— *Steganografi, Video, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)*

Abstract

Hiding data in video files is known as video steganography. Some of the well known steganography methods are Least Significant Bit (LSB) and Discrete Cosine Transform (DCT) method. In this research, data will be hidden on the video file with LSB method, DCT method, and the combined method of LSB-DCT. While the quality result of video file after insertion is calculated using the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). The experiments were conducted based on the size of the video file, the file size of the inserted secret files, and video resolution.

The test results showed that the success rate of the video steganography using LSB method was 38%, DCT method was 90%, and the combined method of LSB-DCT was 64%. While the calculation of MSE, the MSE method DCT lower than the combined method of LSB and LSB-DCT method. While LSB-DCT method has a smaller value than the LSB method. The PNSR experiment showed that the DCT method PSNR value is higher than the combined method of LSB and LSB-DCT method. While PSNR combined method LSB-DCT higher compared LSB method.

Keywords— *Steganography, Video, Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)*

Received December 1st,2013; Revised January 1st, 2013; Accepted January 15th, 2014

1. PENDAHULUAN

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Steganografi *(Steganography)* merupakan salah satu cara untuk menyembunyikan suatu pesan atau data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Steganografi mempunyai sejarah yang hampir sama dengan kriptografi (*cryptograhpy*). Perbedaan steganografi dengan kriptografi terletak pada bagaimana proses penyembunyian data dan hasil akhir dari proses tersebut. Kriptografi melakukan proses pengacakan data aslinya sehingga menghasilkan data terenkripsi yang benar-benar acak dan berbeda dengan aslinya, sedangkan steganografi menyembunyikan dalam data lain yang akan ditumpanginya tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir sama [1].

Steganografi dapat digunakan pada berbagai macam bentuk data, yaitu *image*, *audio*, dan *video* [2]. Sudah banyak metode yang dilakukan untuk steganografi dan sudah banyak pula metode *steganalysis* yang digunakan untuk mendeteksinya. Diantara metode steganografi video adalah metode *Least Significant Bit* (LSB) dan metode *Discrete Cosine Transform* (DCT). Metode LSB menyembunyikan bit-bit pesan pada bit-bit segmen *frame* video. Sedangkan metode DCT menyembunyikan bit-bit pesan dengan melakukan perubahan pada koefisien DCT.

Steganografi video (*video steganography*) menggabungkan steganografi pada *image* dan *audio*. Pada dasarnya *video* merupakan gabungan *image* yang bergerak dan *audio*, yang lebih sulit dideteksi. Keuntungan dari steganografi video adalah banyaknya data yang dapat disembunyikan di dalamnya, serta fakta bahwa video merupakan "*streams*" dari beberapa *image* menyebabkan adanya distorsi pada salah satu *frame image* tidak akan dilihat dengan mudah dengan mata manusia [3]. Akan tetapi, semakin banyak data pesan yang disembunyikan, bukan hal yang mustahil jika perubahan pada video menjadi semakin mudah terlihat. Bahkan modifikasi kecil kepada media *stego* dapat menghancurkannya [4]. Dalam penelitian ini akan menggabungkan metode LSB dan metode DCT. Disamping itu, akan dilakukan uji coba antara metode LSB, metode DCT, dan gabungan metode LSB-DCT.

Untuk menyembunyikan pesan pada *cover* video, prinsipnya sama seperti pada steganografi citra. Pertama-tama dilakukan transformasi pada masing-masing *frame image cover* video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai *treshold* tertentu. Koefisien tersebut diganti dengan bit-bit data pesan yang akan disembunyikan. Setelah seluruh pesan di-*embed*, koefisien tadi ditransformasi balik untuk menghasilkan *stego* video.

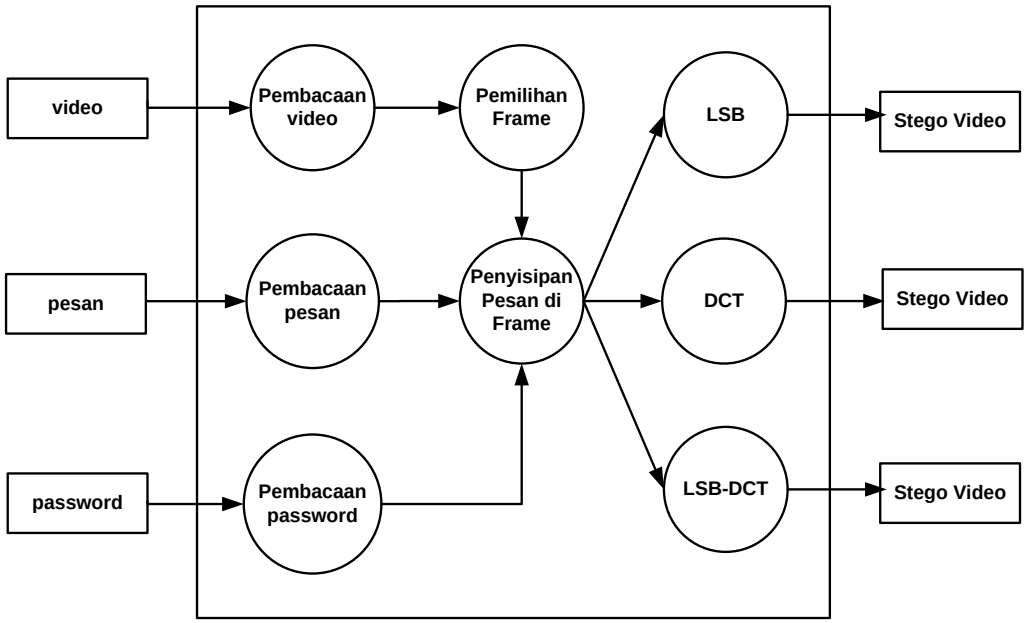
Untuk mengekstrak pesan dari *stego* video, prinsipnya juga sama seperti pada steganografi citra. Pertama-tama dilakukan transformasi pada masing-masing *frame image stego* video untuk memperoleh koefisien-koefisien yang akan dipilih berdasarkan nilai *treshold* tertentu. Koefisien tersebut akan merupakan bit-bit data pesan yang telah disembunyikan dan akan ditulis ke *file output* yang berisi pesan yang disembunyikan tersebut.

Pada implementasinya, biasanya terdapat masukan lain yang ditambahkan, yaitu sebuah kunci atau sandi rahasia untuk memperketat keamanan. Penggunaan kunci ini digunakan sebagai pengacak pada penyisipan. Contoh pada citra adalah blok-blok mana saja yang menjadi tempat disisipkannya pesan tersebut, atau bagaimana urutan *frame* yang akan digunakan sebagai tempat penyisipan pada media video. Hanya kunci yang benar yang dapat mengambil kembali pesan asli secara utuh. Apabila kunci yang dimasukkan salah, maka proses ekstraksi pesan akan gagal, atau menghasilkan pesan yang salah.

2. METODE PENELITIAN

2.1 Proses Penyisipan Pesan

Proses untuk penyisipan pesan pada video, membutuhkan masukan berupa video sebagai media penyisipan, pesan yang ingin disisipkan, serta *password* sebagai pengaman. Video yang digunakan sebagai media penyisipan pesan hanya video yang berformat AVI yang belum terkompresi. Sedangkan *file* berkas rahasia yang disisipkan adalah *file* teks. Secara garis besar proses penyisipan *file* berkas rahasia dapat dilihat pada Gambar 1.



Gambar 1 Diagram proses penyisipan berkas rahasia

Proses penyisipan dilakukan dengan cara pembacaan terhadap *file* video yang berformat AVI yang akan digunakan sebagai media penyisipan pesan. *File* video tersebut diubah menjadi kumpulan *frame*. Setiap *frame* dalam video diubah menjadi sebuah *file* BMP. Proses berikutnya adalah melakukan pembacaan terhadap *file* teks untuk mempersiapkan bit-bit *file* teks yang akan disisipkan pada video. Pesan yang disisipkan kedalam video berupa format teks yang ukurannya tidak melebihi daya tampung penyimpanan dari setiap *frame file* video tersebut. Langkah selanjutnya menyisipkan bit-bit *file* pesan dan *password* kedalam salah satu *frame* video dengan menggunakan metode LSB (*Least Significant Bit*), metode DCT (*Discrete Cosine Transform*), dan gabungan metode LSB-DCT.

Teknik *steganography* dengan metode *LSB* adalah teknik yang paling sering digunakan, informasi yang disembunyikan berupa data *ASCII*, dikonversikan dan diambil nilai binarinya kemudian disisipkan pada *LSB* sederetan *byte* pada *stego image*. Konsep dasar *LSB* adalah melekatkan data rahasia di paling kanan bit (bit dengan bobot terkecil) sehingga prosedur pemasukan data tidak mempengaruhi nilai piksel aslinya. Secara matematis untuk menyisipkan pesan dengan metode LSB dirumuskan:

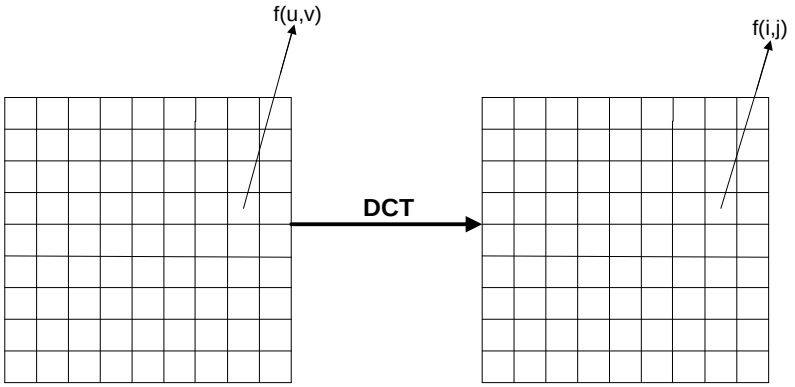
$$x_i' = x_i - x_i \, mod \, 2^k + m_i \quad (1)$$

Pada persamaan diatas x_i' mewakili nilai *i* dari *pixel stego image*, x_i mewakili dari gambar sebenarnya (*cover image)* dan m_i merupakan nilai desimal dari blok ke-*i* dalam data rahasia.

Jumlah *LSB* untuk diganti dinotasikan sebagai *k*. Ekstraksi proses untuk menyalin *k*-bit paling kanan langsung. Secara matematis untuk ekstraksi pesan dirumuskan:

$$m_i = x_i' \; mod \; 2^k \tag{2}$$

Metode DCT yaitu suatu teknik yang digunakan untuk melakukan konversi sinyal kedalam komponen frekuensi pembentuknya dengan memperhitungkan nilai real dari hasil transformasinya [5].



Gambar 2 Diagram transformasi DCT

Proses penyisipan pesan dengan metode DCT dilakukan dengan cara melakukan transformasi DCT dari citra digital [6]. Fungsi transformasi DCT adalah:

$$f(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} f(i,j) \cos\left(\frac{\pi.u}{2N}(2i+1)\right) \cos\left(\frac{\pi.v}{2M}(2j+1)\right) \tag{3}$$

Ukuran image adalah *M x N*. Sedangkan *f(u,v)* adalah nilai koefisien DCT pada matrik 8x8 kolom ke-*u* baris ke-*v*. Adapun *f(i,j)* merupakan nilai data yang hendak ditransformasikan pada matrik 8x8 kolom ke-*i* baris ke-*j*.

Tahap berikutnya adalah menghitung nilai koefisien DCT dan menggantikan bit pada citra tersebut dengan bit pesan yang akan dimasukkan agar tidak terlihat. Kemudian dilakukan transformasi invers DCT sebelum menyimpannya sebagai citra yang disisipi pesan. Fungsi invers DCT sebagai berikut:

$$f(i,j) = \sum_{i=0}^{N-1} \sum_{j=0}^{M} \left(\frac{2}{N}\right)^{\frac{1}{2}} \left(\frac{2}{M}\right)^{\frac{1}{2}} f(u,v) \cos\left(\frac{\pi(2i+1)u}{2N}\right) \cos\left(\frac{\pi(2j+1)v}{2M}\right) \tag{4}$$

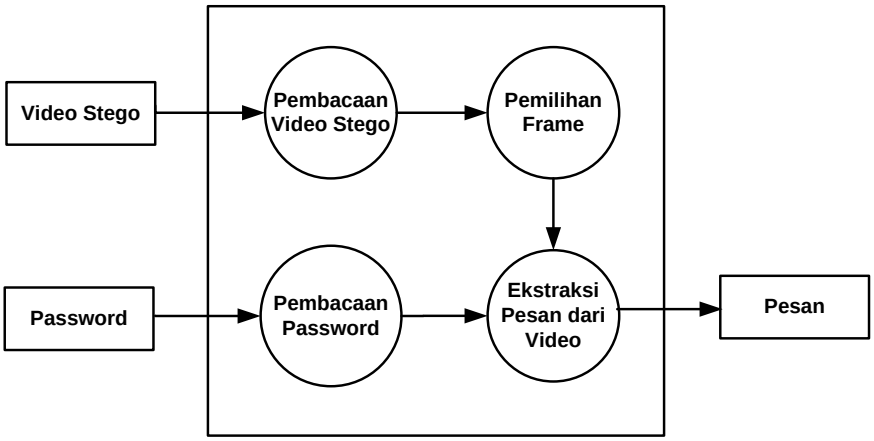
Metode berikutnya adalah gabungan metode LSB-DCT. Proses dilakukan dengan cara menggabungkan metode LSB dan metode DCT.

Tahap akhir proses penyisipan adalah menggabungkan kembali kumpulan *frame* tersebut yang telah disisipi pesan sehingga menjadi video yang mengandung pesan.

2.2 Proses Ekstraksi Pesan

Proses untuk mengekstraksi pesan pada video memerlukan dua buah masukan yaitu video yang mengandung pesan (video *stego*), serta *password* yang diinputkan sebagai pengamannya. Video ini memiliki format yang sama pada saat penyisipan yaitu video yang berformat AVI. Proses ekstraksi pesan dimulai dengan pemilihan *frame* pada video yang akan

dibaca. Kemudian pesan didalamnya dibaca. *Password* yang diinputkan akan menjadi penentu kebenaran pesan. Hanya *password* yang digunakan pada saat penyisipan yang dapat menghasilkan pesan asli kembali. Proses ekstraksi pesan dapat dilihat pada Gambar 3.



Gambar 3 Diagram proses ekstraksi berkas rahasia

Proses ekstraksi pesan dilakukan dengan pembacaan terhadap *file* video yang telah disisipi pesan yang dihasilkan pada proses penyisipan pesan. *File* video tersebut diubah menjadi kumpulan *frame*. Setiap *frame* dalam video tersebut diubah menjadi kumpulan *file* BMP. Kemudian memeriksa masukan *password* apakah sudah sama dengan *password* yang tersimpan di *file* BMP pertama. Jika sama maka dilanjutkan ke proses selanjutnya, jika tidak sama maka akan menampilkan pesan kesalahan.

Tahap berikutnya adalah mendeteksi bit data pada *frame* yang mengandung kode data pesan, sebelum menuliskan bit-bit data yang telah diekstraksi menjadi sebuah *file*. Pada metode LSB dilakukan dengan cara menghitung LSB dari setiap piksel gambar *stego*. Kemudian mengambil bit dan mengkonversi setiap 8 bit menjadi karakter.

Pada proses DCT pembacaan pesan dilakukan dengan cara menghitung transformasi DCT dari citra tersisipkan pesan, serta menghitung koefisien DCT. Kemudian dilakukan ekstraksi bit data dari koefisien terebut dan menggabungkan bit-bit tersebut menjadi sebuah pesan.

Proses ekstraksi pesan pada metode gabungan LSB-DCT dilakukan dengan menggabungkan metode LSB dengan metode DCT.

2.3 Perhitungan MSE dan PSNR

Perhitungan kualitas video digital yang merupakan hasil modifikasi, terhadap video digital yang asli, dapat dilakukan dengan menghitung nilai *Mean Square Error* (MSE) dan juga nilai *Peak Signal-to-Noise Ratio* (PSNR). Video hasil steganografi dengan nilai MSE yang besar, menyatakan bahwa penyimpangan atau selisih antara video hasil steganografi dengan video aslinya cukup besar. Sedangkan semakin besar PSNR, maka kualitas video hasil steganografi akan semakin baik, sebab tidak banyak data yang mengalami perubahan, dibandingkan aslinya.

PSNR merupakan salah satu metode pengukuran yang banyak digunakan untuk sistem kompresi dan rekonstruksi citra. PSNR didefinisikan sebagai berikut:

$$\text{PSNR} = 20\log_{10}\frac{b}{\sqrt{MSE}} \tag{3}$$

Nilai b merupakan nilai maksimum dari piksel citra yang digunakan. Nilai b pada penelitian ini adalah 255. MSE merupakan suatu metode pengukuran kontrol dan kualitas yang sudah dapat

diterima luas. MSE dihitung dari sebuah contoh obyek yang kemudian dibandingkan dengan obyek aslinya sehingga dapat diketahui tingkat ketidaksesuaian antara obyek contoh dengan aslinya. Persamaan MSE terhadap deviasi dari target adalah sebagai berikut:

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I'(x,y)]^2 \quad (4)$$

dimana *M, N* adalah dimensi citra. *I(x,y)* merupakan nilai piksel di citra asli. Sedangkan *I'(x,y)* adalah nilai piksel pada citra hasil steganografi.

3. HASIL DAN PEMBAHASAN

3.1 Pengujian Terhadap Perbandingan Isi File Berkas Rahasia

Pengujian yang dilakukan dengan membandingkan isi dan ukuran dari berkas rahasia sebelum dan sesudah dilakukan proses steganografi. Pengujian ini dapat dikatakan berhasil apabila isi dan ukuran berkas sebelum dan sesudah dilakukan proses steganografi video harus sama persis baik isi maupun ukuran *file*nya.

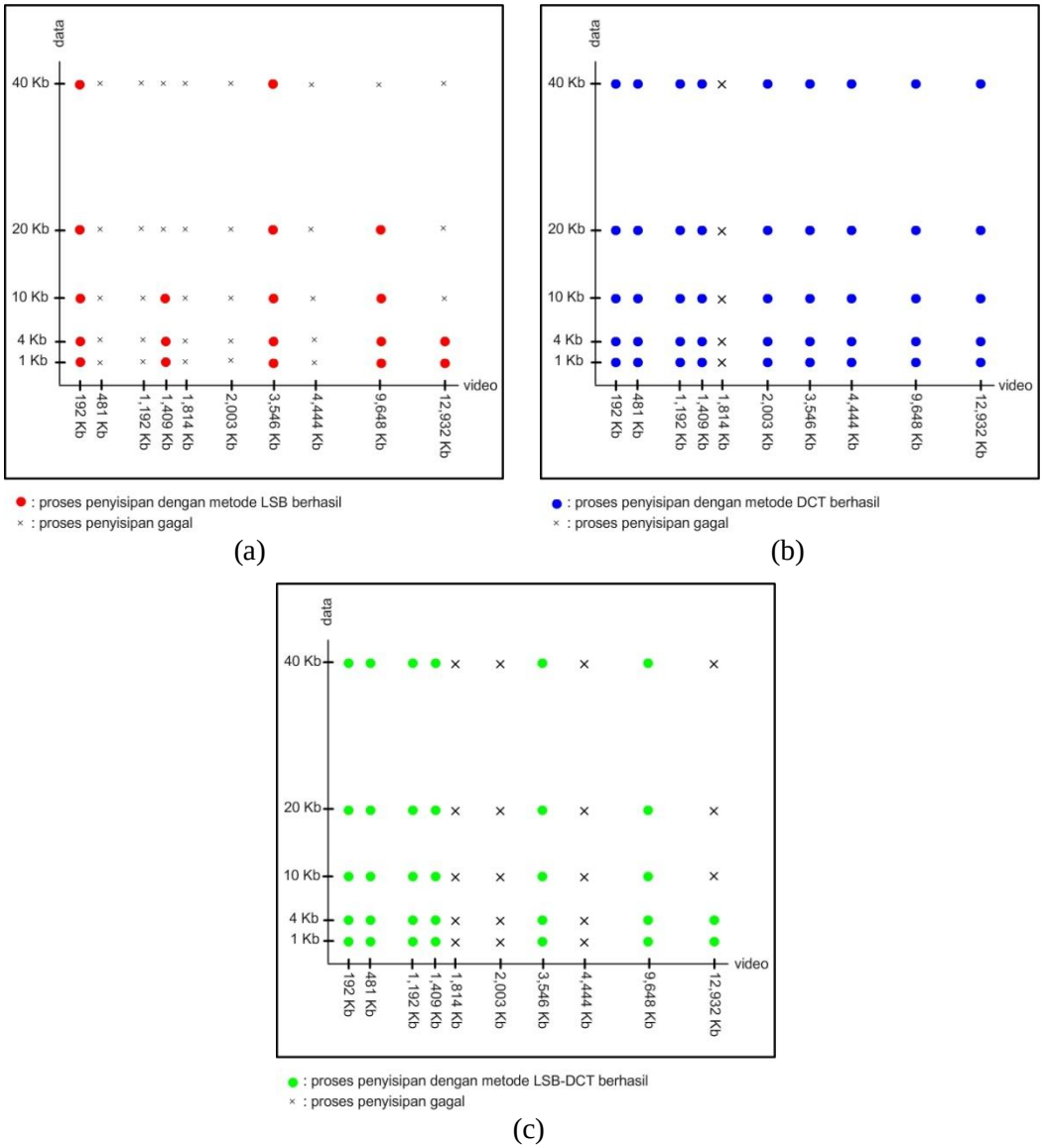
Hasil dari pengujian menunjukkan bahwa isi dan ukuran dari *file* berkas yang berhasil disisipkan sama dengan berkas rahasia aslinya, sehingga pengujian ini dapat dikatakan berhasil. Jika kunci yang dimasukkan pada saat proses ekstraksi tidak sama dengan kunci pada saat proses penyisipan, maka isi berkas rahasia tidak sama dengan berkas pada saat proses penyisipan.

3.2 Pengujian Steganografi Video Berdasarkan Ukuran File

Pengujian ini dilakukan untuk menyisipkan berkas rahasia pada video berdasarkan resolusi dari video yang digunakan sebagai media penyisipan. Pengujian dilakukan berdasarkan ukuran *file* video, ukuran *file* berkas rahasia yang disisipkan, dan resolusi video. *File* video yang akan disisipi adalah *file* AVI dengan resolusi berbeda-beda dan berukuran 192 Kb (resolusi 640x480 piksel), 481 Kb (resolusi 640x480 piksel), 1.192 Kb (resolusi 640x480 piksel), 1.409 Kb (resolusi 160x120 piksel), 1.814 Kb (resolusi 320x240 piksel), 2.003 Kb (resolusi 320x240 piksel), 3.546 Kb (resolusi 320x240 piksel), 4.444 Kb (resolusi 640x352 piksel), 9.648 Kb (resolusi 320x180 piksel), 12.932 Kb (resolusi 320x240 piksel). *File* berkas rahasia yang disisipkan adalah *file* teks (.txt) yang berukuran 1 Kb, 4 Kb, 10 Kb, 20 Kb, 40 Kb.

Sebelum proses penyisipan, *file* video akan dibagi menjadi beberapa *frame* yang terdiri dari *file* bitmap (.BMP). Kapasitas maksimal *file* berkas rahasia yang disisipkan tidak boleh melebihi kapasitas dari *frame*. Jumlah *frame* yang dihasilkan sebelum proses penyisipan dan ukuran masing-masing *frame* ditunjukkan pada program aplikasi. Sehingga *user* bisa menentukan ukuran *file* berkas rahasia yang disisipkan ke dalam *file* video tidak melebihi ukuran *frame*.

Berdasarkan hasil pengujian, tidak semua *file* berkas rahasia yang mempunyai ukuran *file* lebih kecil dari ukuran *frame* dapat disisipkan. Tingkat keberhasilan proses penyisipan *file* berkas rahasia pada *file* video dapat dilihat pada Gambar 4. Hasil pengujian menunjukkan tingkat keberhasilan steganografi video dengan menggunakan metode LSB adalah 38%, metode DCT adalah 90%, dan gabungan metode LSB-DCT adalah 64%. Hasil pengujian juga menunjukkan bahwa semakin besar *file* berkas rahasia yang disisipkan, semakin kecil tingkat keberhasilan proses penyisipan *file* berkas rahasia ke dalam *file* video.

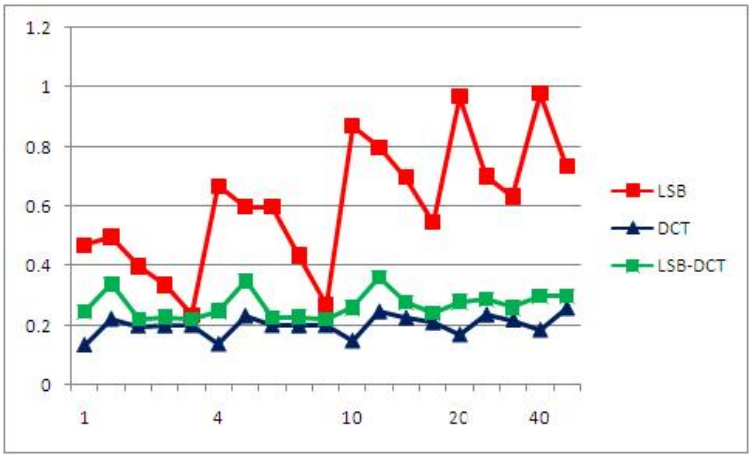


Gambar 4 Tingkat keberhasilan proses penyisipan (a) metode LSB (b) metode DCT (c) metode LSB-DCT

3.3 Pengujian Kualitas Video

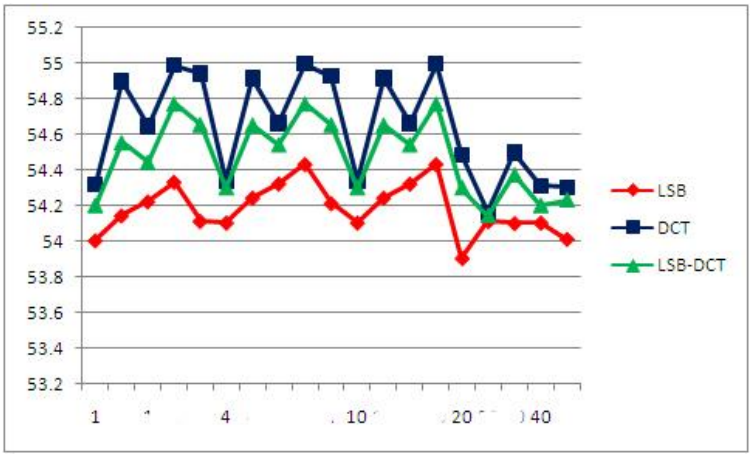
Berdasarkan proses steganografi yang sudah berhasil sebelumnya, dilakukan perhitungan untuk mengetahui kualitas video, dengan menggunakan perhitungan PSNR dan perhitungan MSE. Semakin besar nilai PSNR maka video hasil steganografi semakin mendekati video aslinya, dengan kata lain semakin bagus kualitas video hasil steganografi tersebut. Sebaliknya, semakin kecil nilai PSNR semakin jelek kualitas video hasil steganografi. Sedangkan semakin besar nilai MSE, maka semakin besar perbedaan antara 2 buah video yang dibandingkan.

Hasil pengujian pada Gambar 5 menunjukkan bahwa berdasarkan perhitungan MSE, nilai MSE metode DCT paling rendah dibandingkan metode LSB dan gabungan metode LSB-DCT. Sedangkan metode LSB-DCT mempunyai nilai yang lebih kecil dibandingkan metode LSB. Ini menunjukkan bahwa metode DCT mempunyai perbedaan yang kecil antara video asli dan video hasil steganografi.



Gambar 5 Grafik perbandingan hasil perhitungan MSE

Sedangkan pada pengujian PSNR pada Gambar 5 diperoleh data, bahwa nilai PSNR metode DCT, lebih tinggi dibandingkan metode LSB dan gabungan metode LSB-DCT. Sedangkan nilai PSNR metode gabungan LSB-DCT lebih tinggi dibandingan metode LSB. Hal ini menunujukkan bahwa kualitas video hasil *stego* yang paling baik adalah metode DCT.



Gambar 6 Grafik perbandingan hasil perhitungan PSNR

3.4 Pengujian Subyektif

Pengujian subyektif ditentukan berdasarkan hasil pengamatan mata manusia. Penilaian didasarkan atas karakteristik pengamatan manusia (*Human Visual System*). Pada pengujian subyektif terdapat kategori pada responden sebagai berikut:

1. Responden yang dipilih tidak buta.
2. Responden yang dipilih tidak buta warna.
3. Responden yang dipilih memiliki penglihatan yang bagus dalam antara 30-40 cm memakai kacamata ataupun tidak memakai kacamata.

Kuesioner dilakukan kepada sepuluh responden yang dipilih secara acak. Kuesioner yang diujikan memiliki bobot nilai pada atribut penilaian masing-masing dan perhitungan tes uji total. Hasil pengujian secara subyektif menunjukkan bahwa hasilnya bernilai lulus tes kualitas.

4. KESIMPULAN

Dari beberapa pengujian yang dilakukan dalam penelitian ini, dapat ditarik kesimpulan sebagai berikut:

1. Berdasarkan pengujian yang telah dilakukan, didapatkan bahwa aplikasi steganografi video ini mampu menyimpan berkas-berkas teks tetapi ukuran berkas teks tersebut tidak melebihi daya tampung *cover frame* video dan dapat mengekstraksi kembali *file* berkas rahasia yang telah disisipkan kedalam video. Berkas yang dihasilkan dari hasil ekstraksi video *stego* tidak berubah baik isi maupun besar ukurannya sama seperti dengan *file* berkas asli yang disisipkan kedalam video.
2. Hasil pengujian menunjukkan tingkat keberhasilan steganografi video dengan menggunakan metode LSB adalah 38%, metode DCT adalah 90%, dan gabungan metode LSB-DCT adalah 64%.
3. Berdasarkan perhitungan MSE, nilai MSE metode DCT paling rendah dibandingkan metode LSB dan gabungan metode LSB-DCT. Sedangkan metode LSB-DCT mempunyai nilai yang lebih kecil, dibandingkan metode LSB. Ini menunjukkan bahwa metode DCT mempunyai perbedaan yang kecil antara video asli dan video hasil steganografi.
4. Sedangkan pada pengujian PSNR diperoleh data, bahwa nilai PSNR metode DCT, lebih tinggi dibandingkan metode LSB dan gabungan metode LSB-DCT. Sedangkan nilai PSNR metode gabungan LSB-DCT lebih tinggi dibandingan metode LSB. Hal ini menunujukkan bahwa kualitas video hasil *stego* yang paling baik adalah metode DCT.
5. Hasil pengujian subyektif dengan pengamatan pandangan mata, diperoleh hasil bahwa video asli dan video hasil proses steganografi tidak jauh berbeda.

5. SARAN

Sedangkan saran untuk sistem ini antara lain adalah sebagai berikut

1. Aplikasi ini masih perlu dikembangkan lagi supaya dapat menyisipkan pada berbagai format video dan dapat menyisipkan berkas rahasia dalam ukuran yang besar.
2. Aplikasi belum mendukung sepenuhnya penyisipan sebuah pesan pada banyak video, sehingga semua pesan tersebut dipastikan dapat tertampung seluruhnya, dan disimpan per bagian pada tiap video

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada seluruh civitas akademika Program Pascasarjana Ilmu Komputer Universitas Gadjah Mada yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Johnson, Neil F., Duric, Zoran, Jajodia, Shushil, 2001, Information Hiding Steganography and Watermarking – Attacks and Countermeasures, *Advanced in Information Security*, Kluwer Academic Publisher, United State.

[2] Zhou, X., 2005., *Steganography File Sistem*, Department of Computer Science School of Computing, National University of Singapore.

[3] Agrawal, V.K., 2007, Perceptual Watermarking of Digital Video using The Variable Temporal Length 3D-DCT, *Thesis*, Department of Electrical Engineering, Indian Institute of Technology, Kanpur.

[4] Provos, N. dan Honeyman, P., 2003, *Hide and Seek: An Introduction to Steganography*, IEEE Computer Society.

[5] Patel, H. dan Dave, P., 2012, Steganography Technique Based on DCT Coefficients, *International Journal of Engineering Research and Applications (IJERA)*, ISSN: 2248-9622 Vol. 2, Issue 1, Jan-Feb 2012.

[6] Bodhak, P.V. dan Gunjal, B.L, 2012, Improved Protection In Video Steganography Using DCT & LSB, *International Journal of Engineering and Innovative Technology (IJEIT)*, Volume 1, Issue 4, April 2012.