APLIKASI STEGANOGRAFI PADA VIDEO DENGAN METODE LEAST SIGNIFICANT BIT (LSB)

ASEP BUDIMAN
10103211

UNIVERSITAS KOMPUTER INDONESIA (UNIKOM)
Jl. Dipati ukur no.102-106 Tlp. 2503054 Fax. 2533754 Bandung 40132
Email : asbud01@gmail.com

Steganografi adalah suatu teknik untuk menyembunyikan suatu informasi yang rahasia atau sensitif tanpa terlihat agar tidak terlihat seperti semestinya. Data rahasia disembunyikan dengan cara disisipkan pada suatu media seperti image, audio, dan video sehingga tidak terlihat bahwa dalam media tersebut disembunyikan suatu pesan informasi.

Metode Least Significant Bit (LSB) yaitu suatu metode steganografi yang dapat menyisipkan suatu data ke dalam cover penyisipan seperti image, audio, dan video dengan cara mengubah bit-bit yang paling rendah dari suatu cover penyisipan sehingga file steganografi yang dihasilkan tidak akan kelihatan perubahannya meskipun telah disisipi suatu data.

Steganography pada video menggabungkan steganography pada image dan audio, pada dasarnya video merupakan gabungan image yang "bergerak" dan audio, yang lebih sulit dideteksi dan dapat menyimpan data rahasia lebih banyak jika dibanding pada image, karena video merupakan gabungan dari image-image.

Kata Kunci: *Steganografi video, video, least significant bit, LSB.*

BAB I
PENDAHULUAN
1.1 Latar Belakang Masalah

Perkembangan teknologi informasi (TI) saat ini memberikan kemudahan manusia untuk melakukan aktivitasnya. Termasuk kirim mengirim informasi dalam bentuk file menjadi hal yang biasa di era komputerisasi saat ini. Banyak diantara file tersebut bersifat rahasia dan sangat penting, dan tidak boleh diketahui oleh pihak lain. Dan seiring dengan perkembangan teknologi informasi tersebut, semakin berkembang pula teknik kejahatan yang berupa perusakan maupun pencurian data oleh pihak yang tidak memiliki wewenang atas data tersebut. Ada beberapa bentuk penyerangan terhadap data dan informasi, seperti hacker, cracker, trojan force attack, dan lain-lain. Oleh karena itu, pada saat ini telah dilakukan berbagai upaya untuk menjaga keamanan data dan mengatasi serangan-serangan tersebut.

Sebelumnya telah ada cara untuk menjaga keamanan data yang dikenal dengan nama kriptografi. Dengan kriptografi data rahasia terjaga keamanannya, namun bentuk chipertext yang diacak akan mudah terdeteksi dan menyadarkan pihak ketiga akan kerahasiaan file tersebut. Untuk itu diterapkan *steganography* yang dalam bahasa Yunani berarti "pesan tersembunyi" (covered writing) dalam usaha menjaga kerahasiaan data. *Steganography* 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. Dalam bidang keamanan komputer, *steganography* digunakan untuk menyembunyikan data rahasia pada saat proses enkripsi tidak dapat dilakukan atau bersamaan dengan proses enkripsi. Jadi, walaupun enkripsi berhasil dipecahkan (dechiper) pesan/data rahasia tetap tidak terlihat. Pada steganografi pesan disamarkan dalam bentuk yang relatif aman sehingga tidak terjadi kecurigaan tersebut. Steganografi dapat digunakan pada berbagai macam bentuk data, yaitu image, audio, dan video.

Steganography yang berkembang saat ini adalah *steganography* pada image dan audio, namun steganografi pada image dan audio masih banyak memiliki kelemahan seperti perubahan tampilan yang terlihat jelas pada image dan gangguan suara yang terjadi pada steganografi audio. Selain itu banyak software yang dapat mendeteksi data

dan informasi yang disisipkan pada image dan audio.

Berdasarkan pada berbagai kelemahan yang ada pada *steganography* pada image dan audio tersebut, dalam tugas akhir ini akan dibahas *steganography* pada video. *Steganography* pada video menggabungkan *steganography* pada image dan audio, pada dasarnya video merupakan gabungan dari image yang bergerak dengan audio, yang lebih sulit dideteksi. Hal ini dikarenakan video dapat menyembunyikan lebih banyak data dan video merupakan aliran dari image sehingga distorsi pada salah satu frame image tidak terlihat dengan mudah oleh mata manusia.

Dalam *steganography* video ini menggunakan metode *Least Significant Bit (LSB)*. Hal ini dikarenakan pada metode *Least Significant Bit (LSB)* ini dapat menyimpan file teks pada bit yang paling rendah dari frame-frame video sehingga hasil dari video steganografi tidak akan kelihatan terjadi perubahan.

1.2 Identifikasi Masalah

Berdasarkan latar belakang permasalahan di atas, maka masalah yang dirumuskan yaitu bagaimana membangun suatu aplikasi *steganography* untuk menyembunyikan pesan rahasia dan dapat melindungi keamanan datanya yang disisipkan pada video dengan menggunakan metode *Least Significant Bit* (LSB) sehingga kerahasiaan datanya tetap terjamin aman dan secara kasak mata tidak terjadi perubahan pada video tersebut meskipun telah disisipi data.

1.3 Maksud dan Tujuan

Maksud dari penulisan tugas akhir ini adalah untuk mengembangkan teknik *steganography* image dan audio yang sudah ada dikembangkan lagi menjadi teknik *steganography* video yang dapat menyembunyikan dan melindungi keamanan data yang disisipkan video avi dengan menggunakan metode *Least Significant Bit* (LSB).

Sedangkan tujuan yang akan dicapai dalam penelitian ini adalah :

1. Untuk membangun suatu perangkat lunak yang dapat menyembunyikan dan melindungi keamanan informasi rahasia yang disisipkan ke dalam video digital.
2. Untuk memberikan informasi bagaimana teknik *steganography* metode *Least Significant Bit* (LSB) dapat diterapkan dalam pengamanan video digital.
3. Untuk memanipulasi data video digital yang didalamnya terdapat informasi rahasia sehingga pesan rahasia tersebut tidak dapat diketahui keberadaannya dan secara kasak mata tidak terjadi perubahannya pada video digital hasil manipulasi.
4. Teknik *steganography* dengan menggunakan metode *Least Significant Bit* (LSB) supaya dapat menutupi kelemahan yang ada pada teknik *steganography* yang telah dibangun sebelumnya dengan menggunakan metode lain.

1.4 Batasan Masalah

Dalam pembuatan tugas akhir ini, untuk mengatasi permasalahan yang ada maka penyusun membatasi permasalahan sebagai berikut :

1. Video yang digunakan sebagai media penyisipan hanya video avi yang belum terkompres.
2. Berkas atau data rahasia yang disisipkan pada video berformat apa saja tapi ukurannya harus lebih kecil dari daya tampung dari video atau 1/8 dari frame video.
3. Bahasa pemograman yang digunakan adalah bahasa pascal.
4. Format file video yang dihasilkan dari program *steganografhy* ini adalah format *.avi.
5. Berkas atau data rahasia yang disisipkan atau disembunyikan pada video hanya satu file.

1.5 Metodologi Penelitian

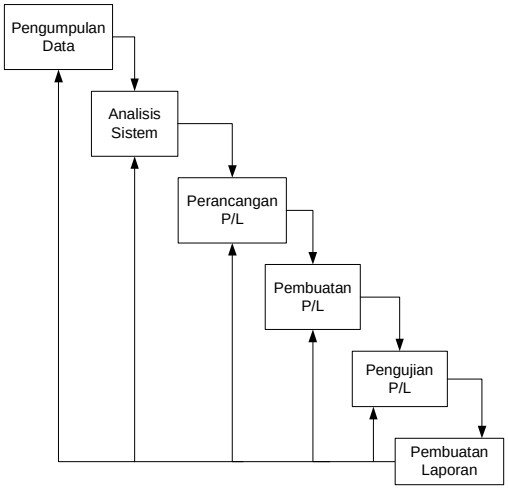
Metodologi yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

1. Tahap pengumpulan data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut :

a. Studi ke perpustakaan

Studi kepustakaan dilakukan untuk mencari informasi tentang *steganography* video dan prosesnya. Sumber kepustakaan diambil dari buku-buku yang berkaitan dengan *steganography* video dan informasi yang juga dapat diperoleh dari internet.



Gambar 1.1 Diagram metode *waterfall*

Penjelasan dari setiap tahap dari proses pada diagram *waterfall* diatas adalah sebagai berikut:

a. Pengumpulan data
   Pengumpulan data berupa literatur atau berupa karya-karya ilmiah yang berhubungan dengan penelitian yang dikerjakan
b. Analisis sistem
   Analisis sistem akan ditetapkan dengan memperhatikan kapasitas informasi dan proses pengolahan data yang diperlukan.
c. Perancangan Perangkat Lunak
   Perancangan Perangkat Lunak pengolahan data meliputi struktur data, menu dan prosedur pengoperasian.
d. Pembuatan Perangkat Lunak
   Pembuatan Perangkat Lunak pengolahan data akan dilakukan dengan penggunaan bahasa pemograman yang tepat, efektif dan efisien dengan memperhatikan teknologi komputerisasi.
e. Pengujian Perangkat Lunak
   Pengujian terhadap Perangkat Lunak pengolahan data akan dilakukan dengan sistematis yaitu secara parsial pada tahapan pembuatan dan pengujian akhir terintegrasi secara menyeluruh untuk memastikan bahwa pemograman yang dirancang telah memenuhi hasil yang diinginkan.
f. Pembuatan Laporan
   Hasil penelitian yang dilakukan akan didokumentasikan untuk kebutuhan lebih lanjut guna pengembangan selanjutnya apabila dibutuhkan.

2. Metode pengembangan perangkat lunak

Tahapan yang akan dilakukan dalam pembangunan sistem ini ialah dengan menggunakan metode *waterfall* seperti diperlihatkan pada gambar 1.1 yaitu :

1.6 Sistematika Penulisan

Sistematika penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN
Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan aplikasi yang dibangun, yang kemudian diikuti dengan pembatasan masalah, asumsi, serta sistematika penulisan.

BAB II. LANDASAN TEORI
Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya.

BAB III. ANALISIS DAN PERANCANGAN SISTEM
Bab ini menguraikan tentang analisis dan perancangan tentang teknik Steganography sebagai pengamanan video digital dengan menggunaka metode *Least Significant Bit* (LSB).

BAB IV. PERANCANGAN DAN IMPLEMENTASI
Bab ini membahas mengenai implementasi beserta tahapan yang dilakukan dalam penelitian, hasil pengujian analisa mengenai karakteristik program yang telah dibuat sampai penarikan kesimpulan.

BAB V. KESIMPULAN DAN SARAN

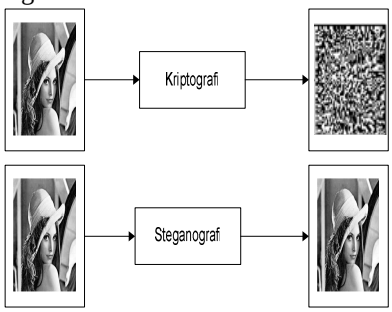
Berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir.

BAB II
LANDASAN TEORI
2.1 Steganography

Steganografi (*steganography*) berasal dari bahasa Yunani yaitu *Steganós* yang berarti menyembunyikan dan *Graptos* yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan. Secara umum steganografi merupakan salah satu cara untuk menyembunyikan suatu pesan rahasia (*hiding message*) di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia kecuali bagi orang yang mengerti kuncinya.

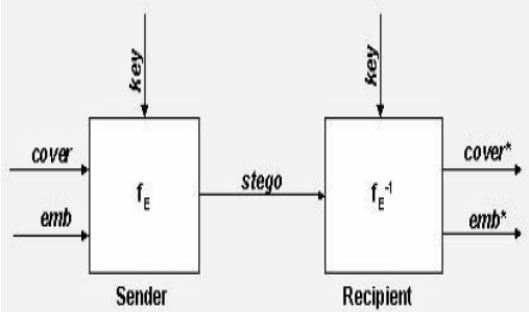
Steganografi membutuhkan dua properti: wadah penampung (*cover*) dan data rahasia yang akan disembunyikan. Steganografi *digital* menggunakan media *digital* sebagai *cover*, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Media yang telah disisipi data disebut *stegodata* atau *stegofile*. Proses penyembunyian data ke dalam media disebut penyisipan (*embedding*), sedangkan proses sebaliknya disebut ekstraksi (*extraction*).

Dalam bidang keamanan komputer, steganografi berbeda dengan kriptografi dimana steganografi digunakan untuk menyembunyikan data rahasia saat enkripsi tidak dapat dilakukan atau bersamaan dengan enkripsi. Jadi, walaupun enkripsi berhasil dipecahkan (decipher) pesan / data rahasia tetap tidak terlihat dan pesan "disamarkan" dalam bentuk yang relative "aman" sehingga tidak terjadi kecurigaan itu. Sedangkan pada kriptografi, dimana pihak ketiga dapat mendeteksi adanya data (*chipertext*) karena hasil dari kriptografi berupa data yang berbeda dari bentuk aslinya dan biasanya datanya seolah-olah berantakan tetapi dapat dikembalikan ke bentuk semula. Ilustrasi mengenai perbedaan kriptografi dan steganografi dapat dilihat pada Gambar 2.1.



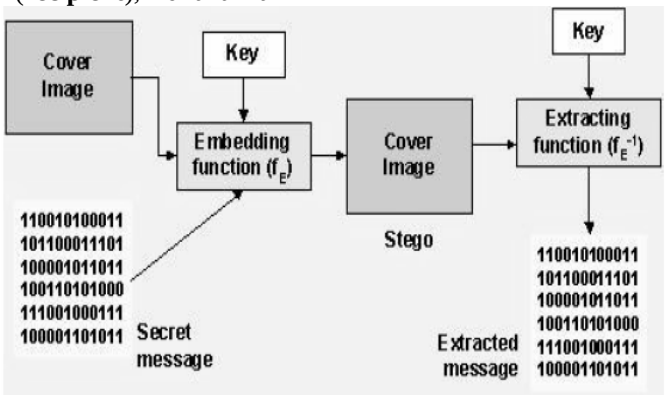
Gambar 2.1 Ilustrasi kriptografi dan steganografi

Steganografi juga membahas bagaimana sebuah pesan dapat disisipkan ke dalam sebuah berkas media sehingga pihak ketiga tidak menyadarinya. Steganografi memanfaatkan keterbatasan sistem indera manusia seperti mata dan telinga. Dengan adanya keterbatasan inilah metode steganografi ini dapat diterapkan pada berbagai media *digital*. Hasil keluaran dari steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi di sini sebatas oleh kemampuan indera manusia, tetapi tidak oleh komputer atau perangkat pengolah *digital* lainnya.



Gambar 2.2 Sistem steganography

Gambar 2.2 menunjukkan sebuah sistem *steganography* umum dimana dibagian pengirim pesan (**sender**), dilakukkan proses *embedding* (**fE**) pesan yang hendak dikirim secara rahasia (**emb**) ke dalam data cover sebagai tempat meyimpannya (**cover**), dengan menggunakan kunci tertentu (**key**), sehingga dihasilkan data dengan pesan tersembunyi di dalamnya (**stego**). Di bagian penerima pesan (**recipient**), dilakukkan proses *extracting* (**fE-1**) pada **stego** untuk memisahkan pesan rahasia (**emb**) dan data penyimpan (**cover**) tadi dengan menggunakan kunci yang sama seperti pada proses *embedding* tadi. Jadi hanya orang yang tahu kunci ini saja yang dapat mengekstrak pesan rahasia tadi. Proses tadi dapat direpresentasikan secara lebih jelas pada gambar 2.3 di bawah.



Gambar 2.3 Graphical Version of a Steganographic System

2.1.1 Sejarah Steganografi

Steganografi sudah digunakan sejak dahulu kala untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi sebagai alat. Beberapa contoh penggunaan steganografi:

1. Steganografi pada tubuh budak: Pada jaman Yunani Kuno, Herodotus (sejarawan Yunani) menyampaikan pesan dengan cara mencukur kepala budak dan mentato kepalanya dengan pesan tersebut. Kemudian saat rambutnya tumbuh kembali, budak dikirimkan pada tempat tujuan dan saat rambutnya kembali digunduli maka pesan akan terbaca.
2. Steganografi dalam lapisan lilin: Masih pada jaman Yunani Kuno, pesan rahasia di ukir pada kayu kemudian diberi lapisan lilin untuk menutupi pesan tersebut, dengan begitu pesan dapat disampaikan tanpa menimbulkan kecurigaan.
3. Steganografi pada kertas: Pada Perang Dunia II, pemerintah Amerika Serikat menulis pesan rahasia pada tentaranya yang di tawan oleh Jerman dengan menggunakan tinta tak terlihat di atas atau di bagian kosong pesan lainnya dan untuk mendeteksinya digunakan air.
4. Steganografi dengan *microdots*: Masih pada Perang Dunia II, agen mata-mata menggunakan *microdots* untuk mengirimkan informasi. Penggunaan teknik ini biasa digunakan pada *microfilm* chip yang harus diperbesar sekitar 200 kali.

5. Steganografi dunia *digital*: Pada suatu pengarahan yang dilakukan oleh FBI pada akhir September 2001, asisten direktur FBI, Ron Dick menyatakan kemungkinan para pembajak pesawat pada serangan 11 September ke gedung *World Trade Center* menggunakan teknologi internet seperti *website* perusahaan palsu atau *website* porno, *e-mail*, *chat rooms*, *bulletin boar*ds untuk mengkoordinasi serangan.

2.1.2 Steganalysis

Steganalysis merupakan suatu teknik atau yang digunakan untuk mengungkapkan keberadaan pesan tersembunyi atau tersamar dari steganografi. Steganalysis menjadi suatu misteri tersendiri untuk dapat diketahui bagaimana teknik untuk melakukan proses dekripsi atau pemecahan atau penemuan pesan tersebut. Terdapat beberapa *software* yang dapat melakukan analisa adanya penggunaan teknik steganografi. Dalam praktiknya cara pemecahan teknik apa yang digunakan dalam steganalysis sendiri secara empirik berkisar diantara :

1. Menganalisa dari perubahan yang dilakukan terhadap meta data *file* tersebut.
2. Menganalisa dari ciri-ciri *file* telah menggunakan *software* tertentu untuk steganografi.
3. Membandingkan *file* asli, lalu dicari perbedaannya dan pola yang digunakan sehingga dengan cara ini bukan saja dapat diketahui *file* telah mengalami proses steganografi dapat pula diketahui pesan yang disembunyikan.

Tetapi teknik steganalysis tidak dapat digunakan untuk mengetahui pesan yang disembunyikan bila ternyata pesan tersebut mengalami kriptografi atau pengkodean pesan lagi. Jadi cara yang baik untuk melakukan steganografi adalah dengan melakukan asumsi bahwa orang akan tahu bahwa ada pesan yang disembunyikan sehingga dilakukan pengamanan lagi dengan kriptografi. Pemilihan kriptografi juga jangan dilakukan dengan sembarangan dan gunakan yang sudah terbukti keampuhannya seperti 3DES dan SHA-1.

2.1.3 Manfaat Stenaganography

Steganography adalah sebuah pisau bermata dua, ia bisa digunakan untuk alasan-alasan yang baik, tetapi bisa juga digunakan sebagai sarana kejahatan. Steganography juga dapat digunakan sebagai salah satu metode watermarking pada image untuk proteksi hak cipta, seperti juga digital watermarking (fingerprinting). Steganography juga dapat digunakan sebagai pengganti hash.

Dan yang terutama, seperti disebutkan sebelumnya, steganography dapat digunakan untuk menyembunyikan informasi rahasia, untuk melindunginya dari pencurian dan dari orang yang tidak berhak untuk mengetahuinya. Sayangnya, steganography juga dapat digunakan untuk mencuri data yang disembunyikan pada data lain sehingga dapat dikirim ke pihak lain, yang tidak berhak, tanpa ada yang curiga. Steganography juga dapat digunakan oleh para teroris untuk saling berkomunikasi satu dengan yang lain. Sehubungan dengan keamanan sistem informasi, steganography hanya merupakan salah satu dari banyak cara yang dapat dilakukan untuk menyembunyikan pesan rahasia. Steganography lebih cocok digunakan bersamaan dengan metode lain tersebut untuk menciptakan keamanan yang berlapis. Sebagai contoh steganography dapat digunakan bersama dengan enkripsi. Windows dan Unix juga menggunakan steganography dalam mengimplementasikan hidden directory.

2.1.4 Faktor Penting Dalam Steganografi

Penyembunyian data rahasia ke dalam media *digital* mengubah kualitas media tersebut. Faktor penting dalam penyembunyian data diantaranya adalah:

1. *Fidelity*. Mutu media penampung tidak jauh berubah. Setelah penambahan data rahasia pengamat tidak mengetahui kalau di dalam media tersebut terdapat data rahasia.
2. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). karena tujuan steganografi adalah menyembunyikan data, maka sewaktu-waktu data rahasia didalam media penampung harus dapat

diambil kembali untuk digunakan lebih lanjut.

2.1.5 Media Steganografi

Steganografi menggunakan sebuah *cover*, tujuannya sebagai kamuflase dari pesan yang sebenarnya. Banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Pada jaman modern seperti saat ini, steganografi biasanya dilakukan dengan melibatkan berkas-berkas seperti teks, citra, suara dan video.

2.1.6 Least Significant Bit (LSB)

Metode steganografi yang paling umum pada tipe berkas citra adalah *least significant bit* (LSB). Metode ini menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam *cover* dengan bit-bit data rahasia. Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), ada bit yang paling berarti *(most significant bit* (MSB) dan bit yang paling kurang berarti *least significant bit* (LSB).

1 0 1 0 0 1 0

MSB LSB

Bit yang cocok untuk diganti adalah bit *LSB*, sebab perubahan tersebut hanya mengubah nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan pada cover *citra*, *byte* tersebut menyatakan warna merah, maka perubahan satu

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam pixel di atas maka akan dihasilkan

00100111 11101001 11001000
00100111 11001000 11101000

bit LSB tidak mengubah warna merah tersebut secara berarti, apalagi mata manusia tidak dapat membedakan perubahan yang kecil. Sebagai contoh, misalnya terdapat data *raster original file* citra yang akan digunakan sebagai *cover* sebagai berikut:

11001000 00100111 11101001

Terlihat hanya tiga bit rendah yang berubah (cetak tebal), untuk penglihatan mata manusia sangatlah mustahil untuk dapat membedakan warna pada *file* citra yang sudah diisi pesan rahasia jika dibandingkan dengan *file* citra asli sebelum disisipi dengan pesan rahasia.

BAB III
ANALISIS DAN PERANCANGAN

Analisis dan perancangan sistem berfungsi untuk mempermudah dalam memahami dan menyusun tahapan selanjutnya yang akan dilakukannya penguraian dari suatu sistem yang utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasikan dan mengevaluasi permasalahan-permasalahan sehingga ditemukan kelemahan, kesempatan, dan hambatan yang terjadi serta kebutuhan-kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan-perbaikannya.

3.1 Analisis Masalah

Analisis ini mencakup semua permasalahan yang terjadi pada teknik *steganography* video ini seperti bagaimana proses penyisipan / *embed* pesan pada video, proses ekstraksi pesan, penggunaan password untuk menambah keamanan, serta proses pengukuran kualitas video untuk mengetahui bagaimana perbedaan video yang dihasilkan.

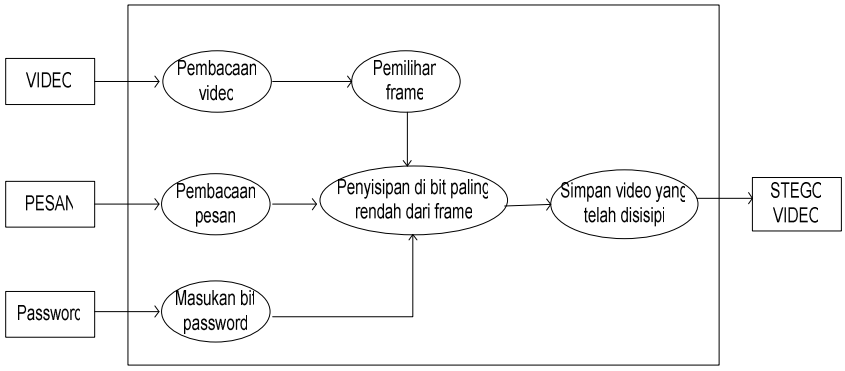
Pada steganografi video dengan menggunakan metode LSB menyembunyikan bit-bit dari berkas rahasia pada bit-bit segmen frame video. Penyembunyian ini pada dasarnya memberikan pengaruh terhadap berkas cover frame video, tetapi karena perubahan yang terjadi sangat kecil sehingga tidak tertangkap oleh indera manusia. Sebagai contoh, untuk citra bitmap 24-bit yang berukuran 256 x 256 piksel terdapat 65536 piksel dan setiap pikselnya berukuran 3 byte (R=1 byte, G=1 byte dan B=1 byte), berarti seluruhnya ada 65536 x 3 = 196608 byte.

Karena dalam setiap byte hanya bisa menyembunyikan 1 bit pada LSB-nya, maka ukuran berkas rahasia maksimum yang dapat disimpan pada citra tersebut adalah 196608/ 8 = 24576 byte atau 1/8 dari ukuran citra tersebut.

3.1.1 Penyisipan pesan pada video

Sistem 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. Aktifitas yang akan dilakukan pada proses penyisipan pesan ini adalah sebagai berikut :

1. Melakukan pembacaan terhadap file video yang berformat *.avi untuk mempersiapkan file video tersebut yang akan digunakan sebagai media penyisipan pesan. File video tersebut diubah menjadi kumpulan frame-frame. Setiap frame dalam video diubah menjadi sebuah file BMP.
2. Melakukan pembacaan terhadap file teks untuk mempersiapkan bit-bit file teks yang akan disisipkan pada video. Pesan yang disisipkan kedalam video bisa berformat apa saja tapi ukurannya tidak melebihi daya tampung penyimpanan dari video tersebut.
3. Menyisipkan bit-bit file pesan kedalam bit yang paling rendah dari salah satu frame video yang digunakan sebagai tempat penyisipan yang dihasilkan pada langkah pertama, password disisipkan pada frame pertama sedangkan untuk pesan rahasia akan disisipkan pada frame berikutnya.
4. Menggabungkan kembali kumpulan frame-frame tersebut yang telah disisipi pesan sehingga menjadi video yang mengandung pesan.



Gambar 3.1 Diagram proses penyisipan pesan

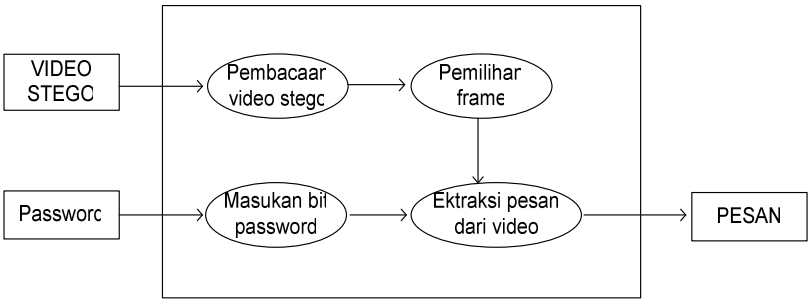
3.1.2 Ekstraksi pesan yang disisipkan pada video

Sistem untuk mengekstraksi pesan pada video memerlukan dua buah masukan yaitu video yang mengandung pesan, 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 dan koefesien pada video yang akan dibaca. Kemudian pesan didalamnya dibaca, menjadi pesan dalam bentuk acak, password yang diinputkan akan menjadi penentu kebenaran pesan, dimana deretan bilangan acak yang dibangkitkan oleh password akan mengatur bagaimana urutan pesan tersebut. Hanya password yang digunakan pada saat penyisipan yang dapat menghasilkan pesan asli kembali. Aktifitas yang dilakukan pada proses ini adalah sebagai berikut:

1. Melakukan pembacaan terhadap file video yang telah disisipi pesan yang dihasilkan pada proses penyisipan pesan. File video tersebut diubah menjadi kumpulan frame-frame. Setiap frame dalam video tersebut di ubah menjadi kumpulan file BMP.
2. 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.

3. Mendeteksi bit data pada frame kedua dan seterusnya yang mengandung kode data pesan.
4. Menuliskan bit-bit data yang telah diekstraksi menjadi sebuah file.



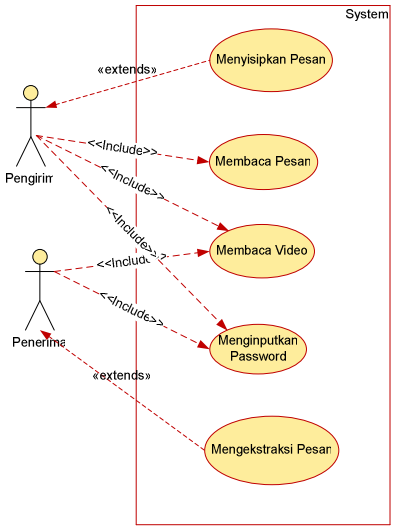
Gambar 3.2 Diagram proses ekstraksi pesan

3.2 Perancangan Sistem

Perancangan sistem adalah suatu proses yang menggambarkan bagaimana suatu sistem dibangun untuk memenuhi kebutuhan pada tahap analisis. Perancangan sistem bertujuan untuk memberikan gambaran sistem yang akan dibuat. Dengan kata lain perancangan sistem didefinisikan sebagai penggambaran atau pembuatan sketsa dari beberapa elemen yang terpisah kedalam satu kesatuan yang utuh dan berfungsi. Selain itu juga perancangan bertujuan untuk lebih mengarahkan sistem yang terinci, yaitu pembuatan perancangan yang jelas dan lengkap yang nantinya akan digunakan untuk pembuatan simulasi. Aplikasi *steganography* ini dibuat dengan sederhana, sehingga diharapkan *user* dapat dengan mudah menggunakan aplikasi *steganography* ini.

3.2.1 Use case Diagram

Diagram *use-case* (*use-case diagram)* merupakan salah satu diagram untuk memodelkan aspek perilaku sistem. Masing-masing diagram *use-case* menunjukan sekumpulan *use-case*, *actor* dan hubungannya. Diagram *use-case* sangat penting untuk memvisualisasikan, menspesifikasikan, dan mendokumentasikan kebutuhan perilaku sistem. Diagram *use-case* juga merupakan pusat pemodelan perilaku sistem, subsistem dan kelas. Use case juga dapat digunakan mendeskripsikan interaksi antara pengguna sistem dengan sistem itu sendiri, dengan memberikan sebuah narasi tentang bagaimana sistem tersebut digunakan.



Gambar 3.3 use case *steganography* video

Perangkat lunak *steganography* video ini memiliki 5 buah use case dan 2 buah aktor. Aktor pengirim merupakan pengguna yang melakukan penyisipan/embed pesan rahasia kedalam video, sedangkan aktor penerima merupakan pengguna yang melakukan ekstraksi pesan rahasia yang telah disisipkan ke dalam video.

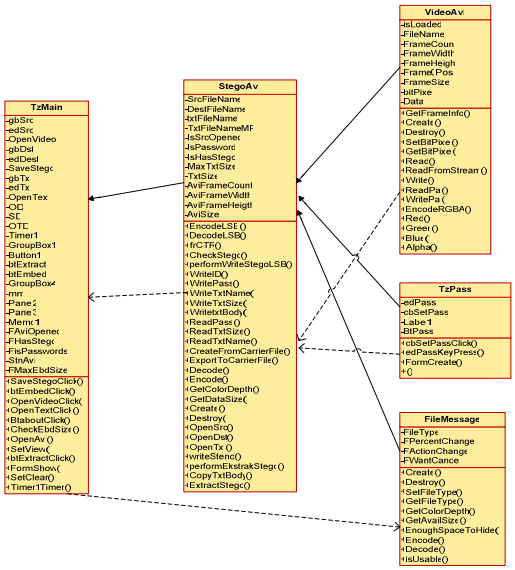
Use case menyisipkan pesan digunakan untuk melakukan menyisipkan data pesan kedalam video. Sedangkan use case membaca pesan digunakan untuk melakukan pembacaan pesan dan validasi ukuran pesan terhadap daya tampung video. Maka kedua use case ini hanya digunakan pada saat proses penyisipan.

Sedangkan untuk use case mengekstraksi pesan digunakan untuk mengekstraksi kembali pesan yang telah disisipkan kedalam video, maka use case ini hanya dapat digunakan pada proses ekstraksi.

Use case membaca video digunakan untuk melakukan pembacaan terhadap video dan validasi ukuran video serta apakah video tersebut sudah mengandung pesan atau belum. Dan use case menginputkan password digunakan pada saat proses penyisipan pesan sekaligus pada saat proses ekstraksi pesan, sehingga kedua use case ini terdapat pada kedua proses.

3.2.2 Class Diagram

Class diagram digunakan untuk mendeskripsikan jenis-jenis objek dalam sistem dan berbagai macam hubungan statis yang terdapat dalam sistem tersebut. *Class diagram* juga dapat menunjukan properti dan operasi sebuah *class* dan batasan-batasan yang terdapat dalam hubungan objek tersebut.



Gambar 3.4 class diagram aplikasi steganography video

Penjelasannya :

- Proses Penyisipan

Pada proses penyisipan membutuhkan 3 kelas masukan yaitu : kelas VideoAvi, kelas FileMessage, dan kelas TzPass.

Dimana kelas “VideoAvi” menangani segala proses terhadap video seperti validasi format video dan jumlah frame video yang dimasukan, mencari frame video yang tepat untuk dijadikan media penyisipan dan untuk menentukan kapasitas daya tampung dari video. Kelas “FileMessage” mengatur pembacaan file teks yang akan diembed dan untuk mengecek apakah ukuran file teks tersebut sesuai dengan daya tampung video. Kelas “TzPass” untuk menyimpan password sebagai pengaman dari proses embed yang dapat digunakan sebagai password pada saat mengekstraksinya kembali. Kelas “StegoAvi” merupakan kelas yang mengatur proses penyisipan pesan kedalam video, dan

juga digunakan untuk menyimpan hasil dari proses penyisipan.

- Proses Ekstraksi

Pada proses ekstraksi membutukan 2 kelas masukan yaitu kelas VideoAvi dan kelas TzPass.

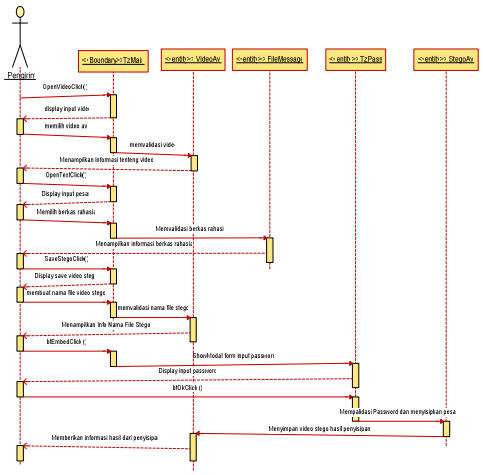
Dimana Kelas “VideoAvi” digunakan untuk melakukan pembacaan dan pengecekan terhadap video yang diinputkan apakah sudah mengandung pesan atau tidak. Kelas ”TzPass” digunakan melakukan pembacaan terhadap password yang diinputkan apakah sama dengan password yang inputkan pada saat proses penyisipan. Jika sama maka video tersebut dapat diekstrak, jika tidak sama maka video stego tersebut tidak dapat diekstrak. Kelas ”FileMessage” digunakan untuk menyimpan file teks hasil dari proses ekstrak video stego. Kelas ”StegoAvi” digunakan untuk proses ektraksi file teks dari video stego

3.2.3 *Sequence Diagram*

Dalam metodologi berorientasi objek untuk menunjukkan bagaimana suatu objek berkomunikasi dengan objek yang lain dengan memperhatikan urutan waktu yang dimodelkan didalam *sequence diagram*.

Sequence diagram terdiri dari objek-objek yang dipresentasikan dalam pembelajaran didalamnya memuat nama dari objek, pengenalan objek, baca objek yang direpresentasikan dengan garis panah dan *time* (waktu) yang direpresentasikan dengan *vertical progression*.

3.2.3.1 *Sequence Diagram* Proses Penyisipan / *Embed*



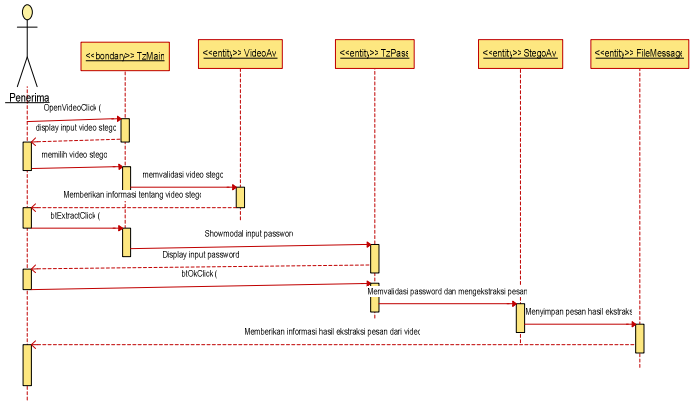
Gambar 3.5 Sequence Diagram Proses Penyisipan / *Embed*

Penjelasan dari gambar 3.5 sebagai berikut :

1. User pengirim mengklik button OpenVideo pada TzMain, kemudian sistem akan menampilkan layar browser input video untuk memilih video yang diinputkan.
2. User pengirim memilih video yang akan di inputkan dan mengklik button open pada layar browser input video, kemudian sistem akan memanggil kelas VideoAvi untuk memvalidasi video dan memberikan informasi dari video yang pilih tersebut kepada user pengirim.
3. User pengirim mengklik button OpenText pada TzMain, kemudian sistem akan menampilkan layar browser input file pesan untuk memilih pesan yang akan disisipkan kedalam video.
4. User pengirim memilih file pesan yang akan disisipkan pada video dan mengklik button open pada layar browser input file pesan, kemudian sistem akan memanggil kelas FileMessage untuk memvalidasi file pesan dan memberikan informasi dari file pesan yang dipilih tersebut.

5. User pengirim mengklik button SaveStego, kemudian sistem akan menampilkan layar browser save file stego, User pengirim membuat nama file dan alamat folder untuk menyimpan hasil penyisipan lalu mengklik button save, kemudian sistem akan memanggil lagi kelas VideoAvi untuk memvalidasi dari nama file stego dan memberikan informasi alamat dan nama file hasil penyisipan kepada user pengirim.
6. User pengirim mengklik button btEmbed, kemudian sistem menampilkan form input password yang digunakan sebagai pengamanan, lalu user pengirim mengisi password dan mengklik button OK, lalu sistem akan memanggil kelas TzPass untuk menginputkan dan memvalidasi password tersebut sebagai password penyisipan.
7. Kemudian sistem akan memanggil kelas StegoAvi untuk menyisipkan pesan kedalam video, kemudian menyimpan video stego dan menampilkan informasi hasil dari proses penyisipan tersebut.

3.2.3.2 *Sequence Diagram* Proses Ekstraksi



Gambar 3.6 Sequence Diagram Proses Ekstraksi

Penjelasan dari gambar 3.6 sebagai berikut :

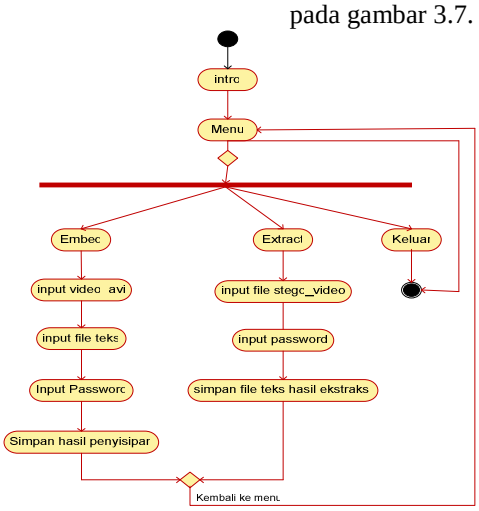
1. User penerima mengklik button OpenVideo pada TzMain, kemudian sistem akan menampilkan layar browser input video stego untuk memilih video stego.
2. User penerima memilih file video stego yang akan di inputkan dan mengklik button open pada layar browser input video stego, kemudian sistem akan memanggil kelas VideoAvi untuk memvalidasi apakah video tersebut telah memiliki pesan atau tidak dan memberikan informasi dari video stego yang pilih tersebut.
3. User penerima mengklik button btExtract pada TzMain, kemudian sistem menampilkan browser save file teks untuk membuat nama file dan memilih alamat folder untuk menyimpan file teks hasil dari ekstraksi tersebut, lalu user penerima mengklik button save, kemudian sistem akan memanggil kelas FileMessage untuk memvalidasi nama file pesan dan memberikan informasi alamat file pesan hasil dari ekstraksi tersebut. Kemudian sistem menampilkan form input password.
4. User penerima masukan password yang sama dengan password pada saat penyisipan, lalu mengklik button OK pada form input password, kemudian sistem akan memanggil kelas TzPass untuk memvalidasi password yang diinputkan apakah sama dengan password pada saat penyisipan.
5. Sistem akan memanggil kelas StegoAvi untuk mengekstraksi pesan

dari video. Lalu sistem memanggil kelas FileMessage untuk menyimpan pesan hasil dari proses ekstraksi dan memberikan informasi kepada user penerima.

3.4.2.4 *Activity Diagram*

Activity diagram didesain untuk memperlihatkan apa yang terjadi selama suatu proses dan operasi berlangsung. *Activity diagram* adalah suatu perluasan dari *state diagram*. *State diagram* menunjukan state-state suatu objek dan representasi aktivitas dinyatakan sebagai state yang dihubungkan dengan garis berarah.

Setiap aktivitas direpresentasikan dengan suatu *rounded rectangle*. Pemrosesan pada suatu aktivitas yang telah selesai akan dikirimkan ke aktivitas berikutnya secara otomatis untuk melakukan aktivitas berikutnya. Garis berarah menyatakan perpindahan aktivitas dari suatu aktivitas ke aktivitas berikutnya. Berikut ini merupakan *activity diagram* dari aplikasi *steganography* video, yang dapat dilihat pada gambar 3.7.



Gambar 3.7 Activity diagram dari aplikasi *steganography* video

BAB IV IMPLEMENTASI DAN PENGUJIAN

4.1 Implementasi

Tahapan ini dilakukan setelah perancangan selesai dilakukan dan selanjutnya akan diimplementasikan pada bahasa pemrograman yang akan digunakan. Tujuan implementasi adalah untuk menerapkan perancangan yang telah dilakukan terhadap aplikasi sehingga user dapat memberi masukan demi berkembangnya aplikasi steganography video yang telah dibangun.

4.1.1Perangkat Pendukung Yang Digunakan

Dalam proses pembuatan dan pengujiannya, aplikasi steganography video ini tentunya membutuhkan perangkat keras dan perangkat lunak. Berikut merupakan penjelasan dari perangkat keras dan perangkat lunak yang digunakan

4.1.1.1 Perangkat Keras (hardware)

Dalam proses pembuatan dan pengujiannya, aplikasi steganografi ini tentunya membutuhkan perangkat keras dan perangkat lunak. Berikut merupakan penjelasan dari perangkat keras dan perangkat lunak yang digunakan.

1. Processor AMD Athlon 64, 2.0Ghz.
2. RAM 1 Giga.
3. VGA 256 MB.
4. Hardisk 80 GB.
5. Mouse dan keyboard.

4.1.1.2 Perangkat Lunak (software)

Perangkat lunak yang digunakan dalam pembuatan dan pengujian aplikasi steganografi ini adalah sebagai berikut :

1. Borland Delphi 7.0
2. Windows media player
3. Virtual Dup
4. Win AVI Video Converter

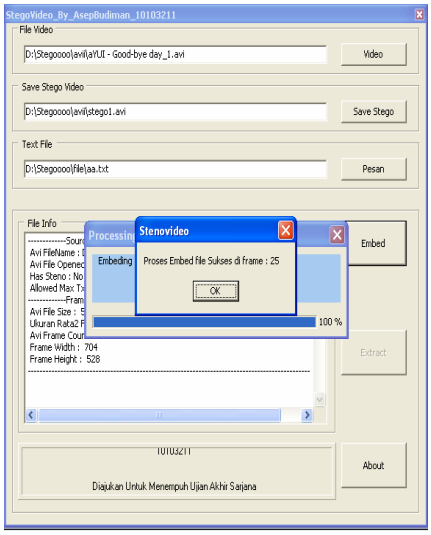
4.2 Pengujian Sistem

Pengujian sistem merupakan proses selanjutnya setelah implementasi perangkat lunak selesai dilakukan. Pengujian ini dilakukan untuk menguji berkas rahasia dan video avi yang digunakan.

4.2.1 Pengujian Terhadap Perbandingan Isi dan Ukuran File Berkas Rahasia

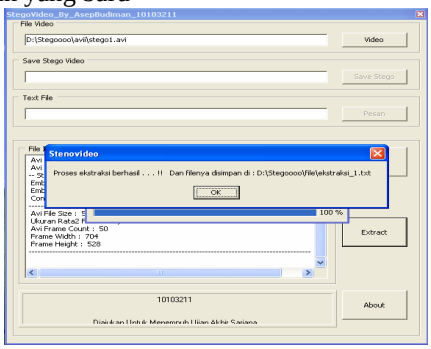
Pengujian yang dilakukan di sini yaitu dengan membandingkan isi dan ukuran dari berkas rahasia sebelum dan sesudah dilakukan proses steganografi. Pengujian ini dapat dikatakan berhasil apabila isi dan ukuran berkas sebelum dan sesudah dilakukan proses steganografi harus sama persis baik isi maupun ukuran filenya.

Misal file berkas dengan nama file (D:\Stegoooo\file\aa.txt) dengan ukuran 1kb disisipkan ke video dengan nama file (D:\Stegoooo\avii\aYUI - Good-bye day_1.avi) dengan ukuran 54499kb dan proses penyisipan berhasil di frame ke 25 dengan nama file stego(D:\Stegoooo\avii\stego1.avi) yang berukuran 54499kb.



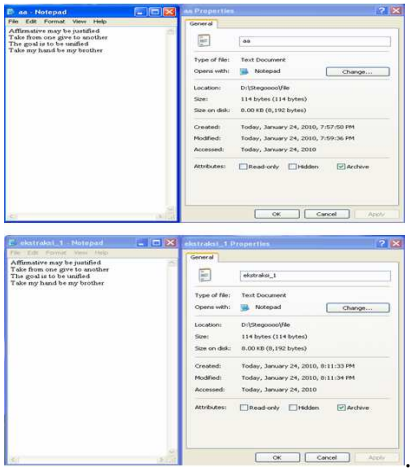
Gambar 4.1 Proses hasil penyisipan

Kemudian file stego (D:\Stegoooo\avii\stego1.avi) yang mengandung pesan tersebut diekstrak lagi sehingga menghasilkan file pesan yang baru dengan nama file (D:\Stegoooo\file\ekstraksi_1.txt) dengan ukuran 1kb.



Gambar 4.2 Proses hasil ekstraksi

Hasil dari pengujian ini menunjukan bahwa isi dan ukuran dari semua berkas yang berhasil di proses sama persis dengan berkas rahasia sebelumnya sehingga pengujian ini dapat dikatakan berhasil



Gambar 4.3 Isi dan Ukuran file berkas dan file hasil ekstraksi

4.2.2 Pengujian Terhadap Kondisi dan Ukuran video

Pada pengujian ini akan dibandingkan kondisi dan ukuran frame dari video sebelum dan sesudah dilakukan proses penyisipan. Perbandingan dilakukan dengan memberikan kuisioner kepada sepuluh orang yang tidak memiliki penyakit buta warna. Pengujian pada video ini dikatakan berhasil apabila kondisi video sesudah dilakukan proses penyisipan tidak mengalami perbedaan yang besar dibandingkan dengan video aslinya. Dengan kata lain, video dari berkas yang dihasilkan sulit untuk dibedakan dengan video dari berkas aslinya. Untuk pengujian ini digunakan file stego dari pengujian 4.2.2.



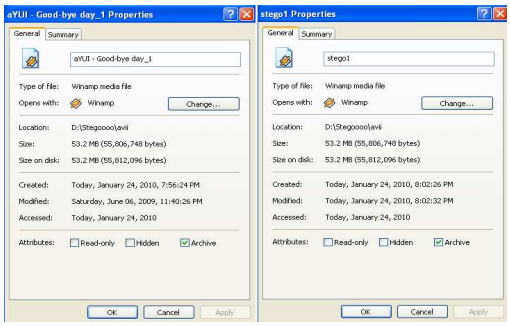
Gambar 4.4 Video (D:\Stegoooo\avii\aYUI-Good-bye day_1) frame 25



Gambar 4.5 Video (D:\Stegoooo\avii\stego1.avi) frame 25 yang sudah disisipi berkas rahasia

Dari hasil pengamatan yang dilakukan oleh sepuluh orang yang tidak memiliki penyakit buta warna tersebut seluruhnya menyimpulkan bahwa kedua gambar tersebut terlihat tidak ada perubahan meskipun telah mengalami proses steganografi dengan tersimpannya berkas teks.

Berhubung teknik steganografi yang digunakan dalam penelitian tugas akhir ini adalah dengan menggunakan teknik substitusi pada LSB, maka secara teori ukuran berkas stego tidak akan berbeda dengan berkas asli.



Gambar 4.5 Ukuran file video dengan file stego yang telah disisipi pesan

Pada gambar 4.5 terlihat ukuran (*size*) dari video asli dengan video stego tidak mengalami perubahan meskipun telah mengalami proses steganografi dengan tersimpannya berkas teks di dalamnya.

4.3 Kesimpulan Hasil Pengujian

Berdasarkan pengujian yang telah dilakukan, didapatkan bahwa aplikasi *steganography* video ini mampu menyimpan berkas-berkas teks dengan format apa saja tetapi ukuran berkas teks tersebut tidak melebihi daya tampung cover frame video dan dapat mengekstraksi kembali file berkas rahasia yang telah disisipkan kedalam video.

Pengujian yang dilakukan terhadap resolusi video yaitu untuk mengetahui daya tampung dari video tersebut. Jika video avi yang mempunyai resolusinya besar maka akan mempunyai daya tampung yang besar dan sebaliknya jika video avi yang resolusinya kecil maka akan mempunyai daya tampung yang kecil.

Pengujian yang dilakukan terhadap video menunjukan bahwa video stego yang dihasilkan dari proses penyisipan tidak berbeda dan ukurannya sama sekali tidak berubah meskipun telah mengalami proses

penyimpanan berkas teks di dalamnya. Dan file berkas yang dihasilkan dari hasil ekstraksi file stego tidak berubah baik isi maupun besar ukurannya sama seperti dengan file berkas asli yang disisipkan kedalam video. Dengan tidak berubahnya kualitas dan ukuran video stego yang signifikan dari video aslinya, kemungkinan besar orang lain tidak akan mengetahui bahwa ada suatu informasi di dalam video tersebut.

BAB V
KESIMPILAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan analisis dan implementasi sistem yang dilanjutkan dengan pengujian sistem, maka dari hasil implementasi dan pengujian tersebut maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Implementasi teknik *steganography* pada video dengan metode *Least Significant Bit* (LSB) avi berhasil dilakukan.
2. Dengan menggunakan password pada proses penyisipan dan ekstraksi maka keamanan data berkas rahasia yang disisipkan pada video dapat terjaga dengan aman.
3. Dengan teknik *steganography*, meskipun video yang sudah disisipi berkas rahasia tetap bisa di buka dengan berbagai sorfware pemutar video.
4. Semakin besar ukuran berkas rahasia yang disisipkan maka semakin kelihatan perubahan yang terjadi pada cover frame video.

5.2 Saran

Aplikasi *steganography* video yang dibangun ini masih belum sempurna. Aplikasi ini masih perlu dikembangkan lagi supaya dapat menyisipkan pada berbagai format video yang sudah terkompres dan dapat menyisipkan berkas rahasia dalam ukuran yang besar.