BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Perangkat Lunak

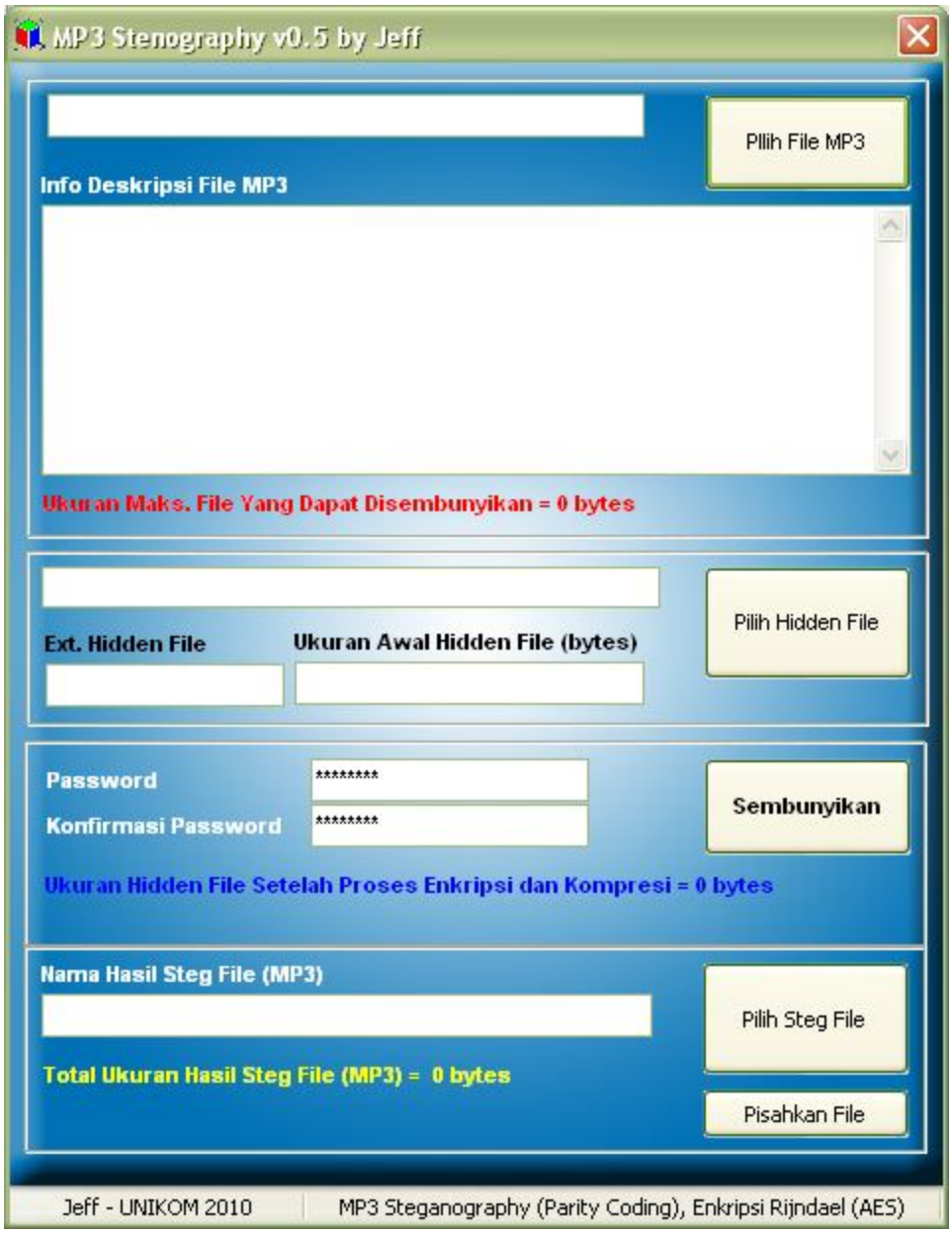
Berdasarkan hasil analisis dan perancangan sistem yang telah dilakukan, maka dilakukan implementasi/pengkodean ke dalam bentuk program komputer. Pengkodean merupakan tahap menerjemahkan hasil perancangan perangkat lunak secara rinci ke dalam bahasa pemrograman. Implementasi dilakukan dengan menggunakan bahasa pemrograman Borland Delphi 7, sehingga hanya dapat dijalankan pada komputer dengan sistem operasi Windows. Aplikasi peningkatan keamanan data pada audio steganografi ini disebut sebagai mp3STEG.

Pengujian dilakukan dengan menggunakan komputer dengan spesifikasi berikut:

- *Processor Intel Pentium M* @ 1,70 GHz
- *Memory* 512 MB DDR1
- *VGA Card Mobile Intel* 910GML *Express* 128 MB
- Sistem Operasi *Microsoft Windows XP Professional Edition*

4.1.1 Tampilan Program mp3STEG

Tampilan utama pada aplikasi Rijndael Steg ini dirancang sesederhana mungkin untuk dapat memudahkan pengguna dalam menggunakannya. Pada tampilan utama terdapat 5 buah tombol sebagaimana dapat dilihat dalam **Gambar 4.1** berikut.

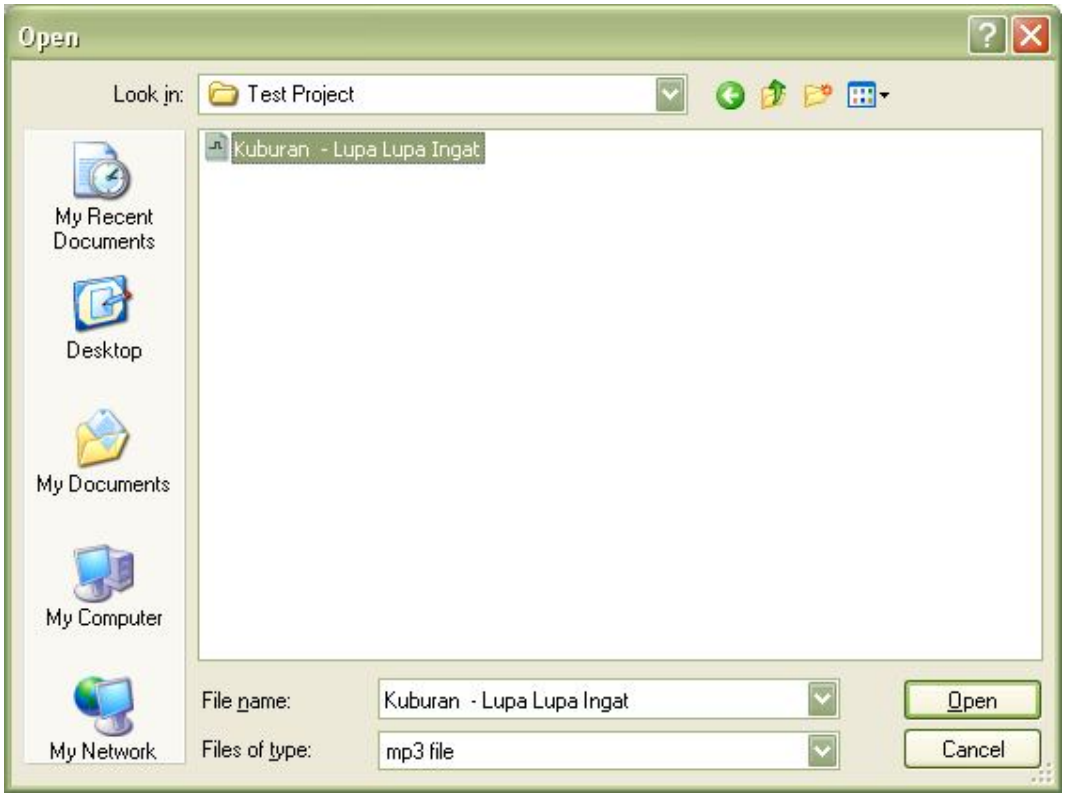


Gambar 4.1 Tampilan Program mp3STEG

4.1.2 Penyisipan Pesan Rahasia

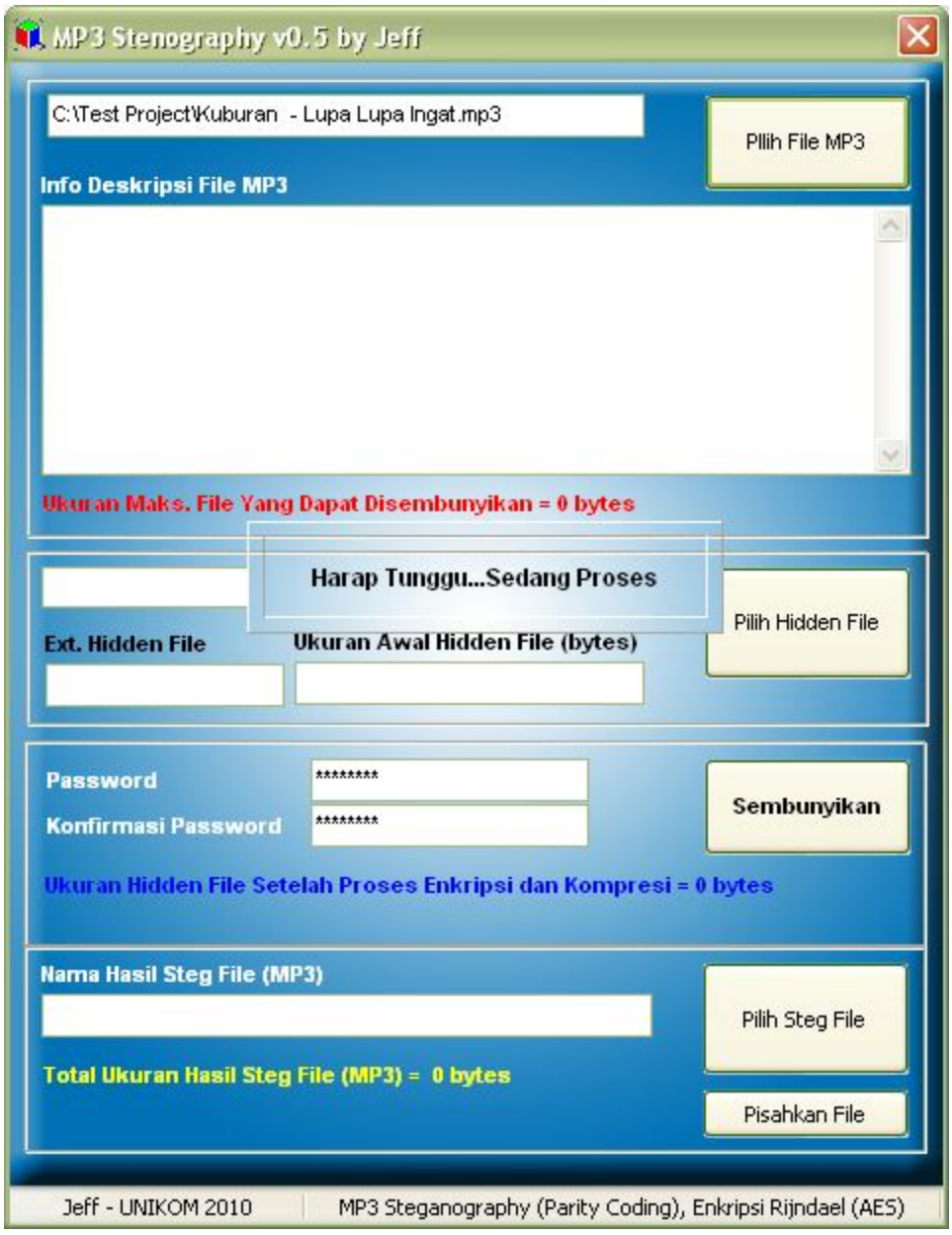
Untuk memulai proses penyisipan/penyembunyian pesan, pengguna harus memilih *file MP3 cover* sebagai media penampung pesan rahasia. Caranya

menekan tombol **“**Pilih File MP3”. Maka akan muncul kotak dialog sebagai berikut.



Gambar 4.2 Tampilan Kotak Dialog Pilih File MP3

Selanjutnya pengguna harus menunggu beberapa saat, karena proses pendeskripsian *MP3*, seperti terlihat pada gambar dibawah ini.



Gambar 4.3 Tampilan Tunggu Proses Info Deskripsi File MP3

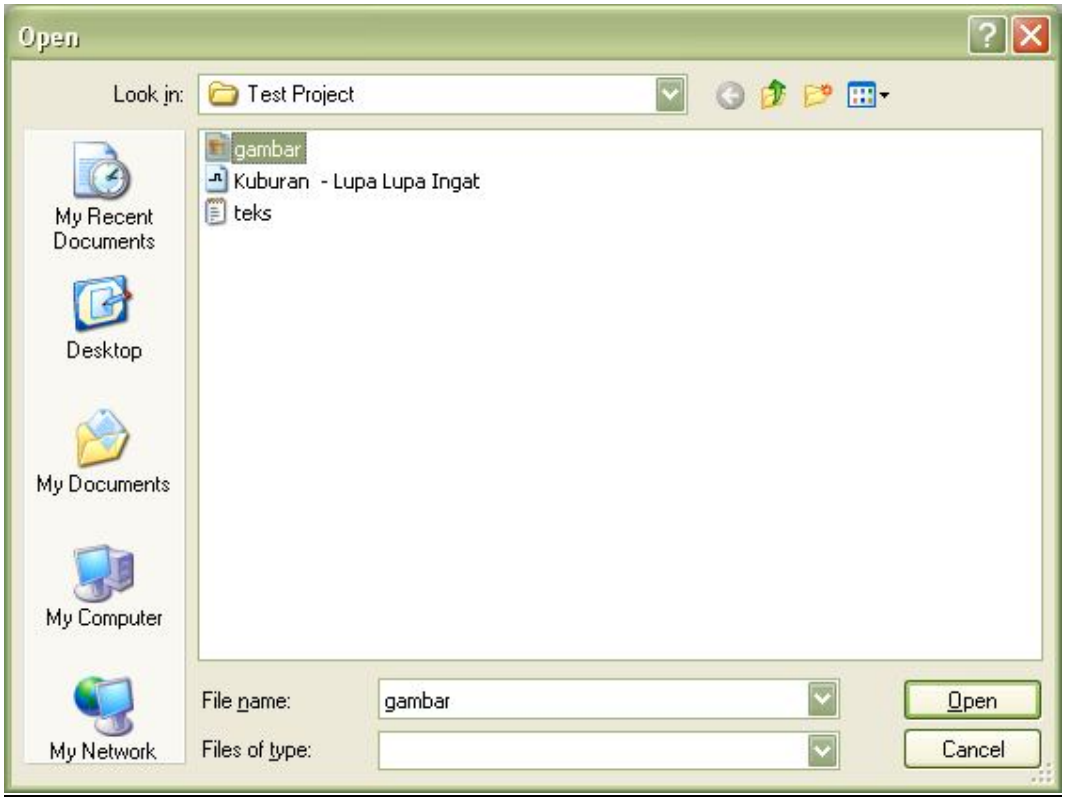
Selanjutnya akan ditampilkan info deskripsi dari *file MP3* yang ingin disisipi pesan rahasia.



Gambar 4.4 Tampilan Info Deskripsi File MP3

Secara otomatis program akan memberikan info ukuran maksimum pesan rahasia yang dapat disembunyikan, untuk menghindari kesalahan menyisipkan pesan yang lebih besar dari ukuran yang semestinya. Dalam pengujian ini ukuran maksimum pesan rahasia yang dapat disembunyikan adalah 42710 bytes. Hasil ini didapat dari konversi ke bytes pada *frame-frame* yang kosong pada *MP3* yang bisa diisi pesan rahasia.

Selanjutnya pengguna harus memilih *file* pesan rahasia yang akan disisipi (dalam pengujian ini akan dipilih tipe *file* gambar (.jpg)). Dengan cara menekan tombol “Pilih Hidden File”, lalu akan muncul kotak dialog sebagai berikut.



Gambar 4.5 Tampilan Pilih Hidden File

Setelah memilih *file* pesan rahasia yang ingin diinginkan, di program akan tampil info-info dari *file* pesan rahasia, seperti berikut.



Gambar 4.6 Tampilan Info *File* Pesan Rahasia

Pada **Gambar 4.6**, ukuran awal *file* pesan rahasia yang akan disisipi adalah 27977 bytes, dengan tipe *file* .jpg.

Setelah *file MP3 cover*, dan *file* pesan rahasia sudah dipilih, sebelum memulai proses penyisipan/penyembunyian pesan rahasia ke *MP3*, pengguna harus mengisi kotak Password dan Konfirm Password (isi dengan password yang sama). Dalam pengujian ini Password yang diisi berupa angka "1234".



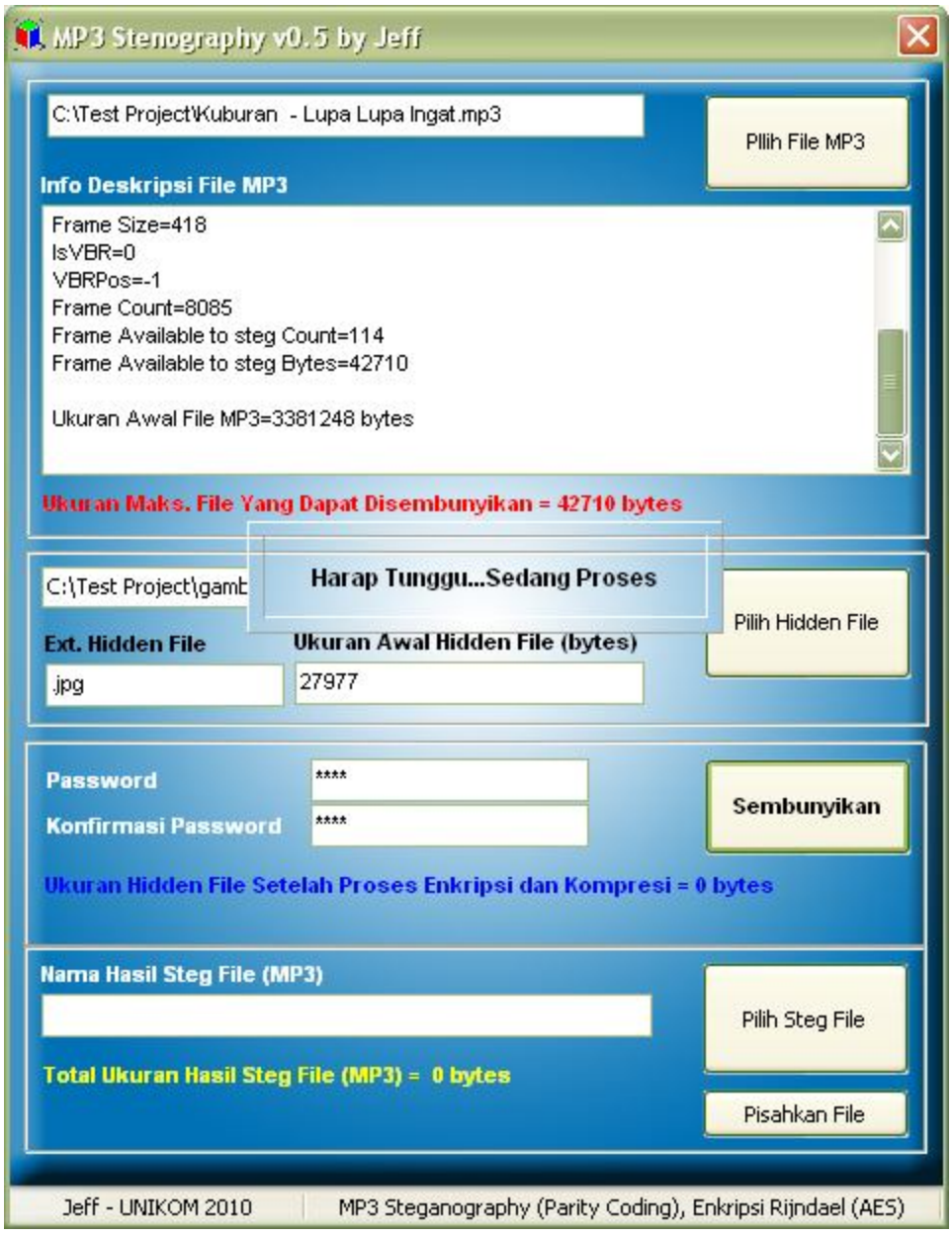
Gambar 4.7 Tampilan Pengisian Password dan Konfirm Password

Jika pengisian password tidak sama, maka akan muncul pesan error sebagai berikut.



Gambar 4.8 Tampilan Error Password

Kemudian untuk memulai proses penyisipan pesan rahasia, yaitu dengan cara menekan tombol "Sembunyikan", seperti terlihat pada **Gambar 4.7** diatas. Selanjutnya pengguna harus menunggu karena proses penyisipan pesan rahasia, seperti terlihat pada gambar di bawah ini.



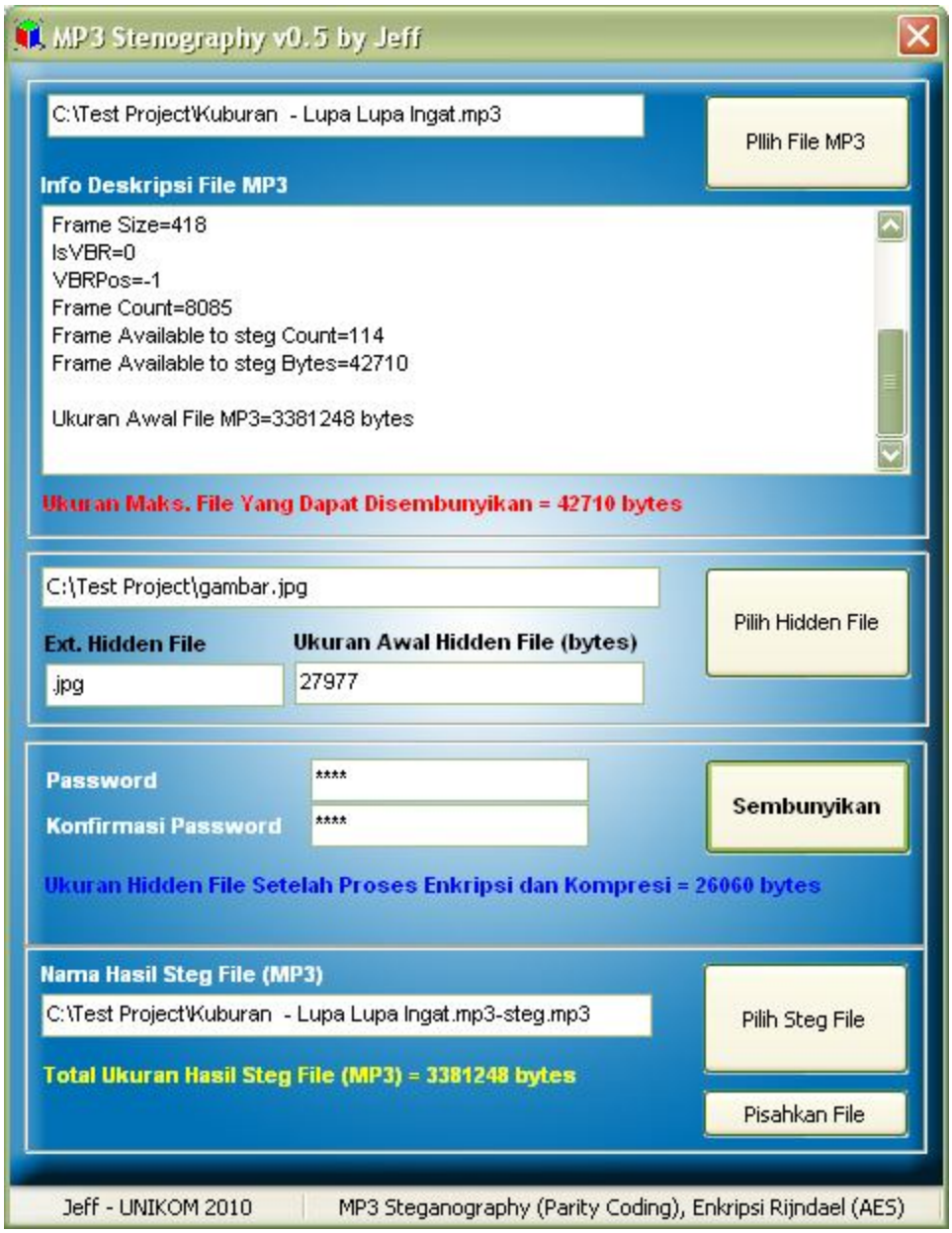
Gambar 4.9 Tampilan Tunggu Proses Penyisipan Pesan Rahasia

Setelah proses penyisipan pesan rahasia berhasil dilakukan, maka akan muncul kotak informasi, seperti terlihat pada gambar dibawah ini.



Gambar 4.10 Informasi Penyisipan Pesan Rahasia

Setelah meng-klik tombol OK pada kotak informasi pada **Gambar 4.10** diatas. Maka tampilan pada program adalah sebagai berikut.



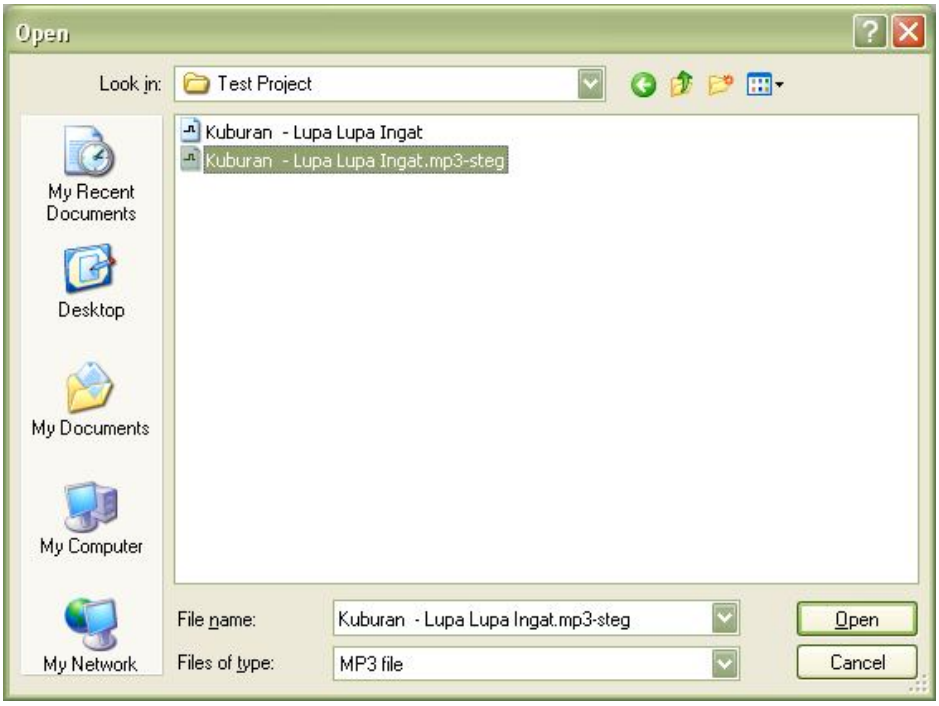
Gambar 4.11 Tampilan Program Setelah Proses Penyisipan Pesan Rahasia

Pada **Gambar 4.11** diatas, pengguna akan mendapatkan informasi ukuran *file* pesan rahasia setelah melalui proses penyisipan/penyembunyian. Dalam kasus ini terjadi penurunan Ukuran Hidden File Setelah Proses Enkripsi dan Kompresi yaitu = 26060 bytes, yang awalnya adalah 27977 bytes.

Nama hasil *file MP3 cover* yang telah disisipi pesan rahasia ditambahi ekstensi "steg", untuk menjaga kecurigaan pihak lain, diharapkan pengguna mengubah nama *file MP3 cover* yang telah disisipi. Namun, dalam pengujian ini nama *file MP3 steg* tidak akan diubah, agar dapat dibedakan mana *file MP3* yang sudah disisipi pesan dan mana *file MP3* yang belum disisipi pesan.

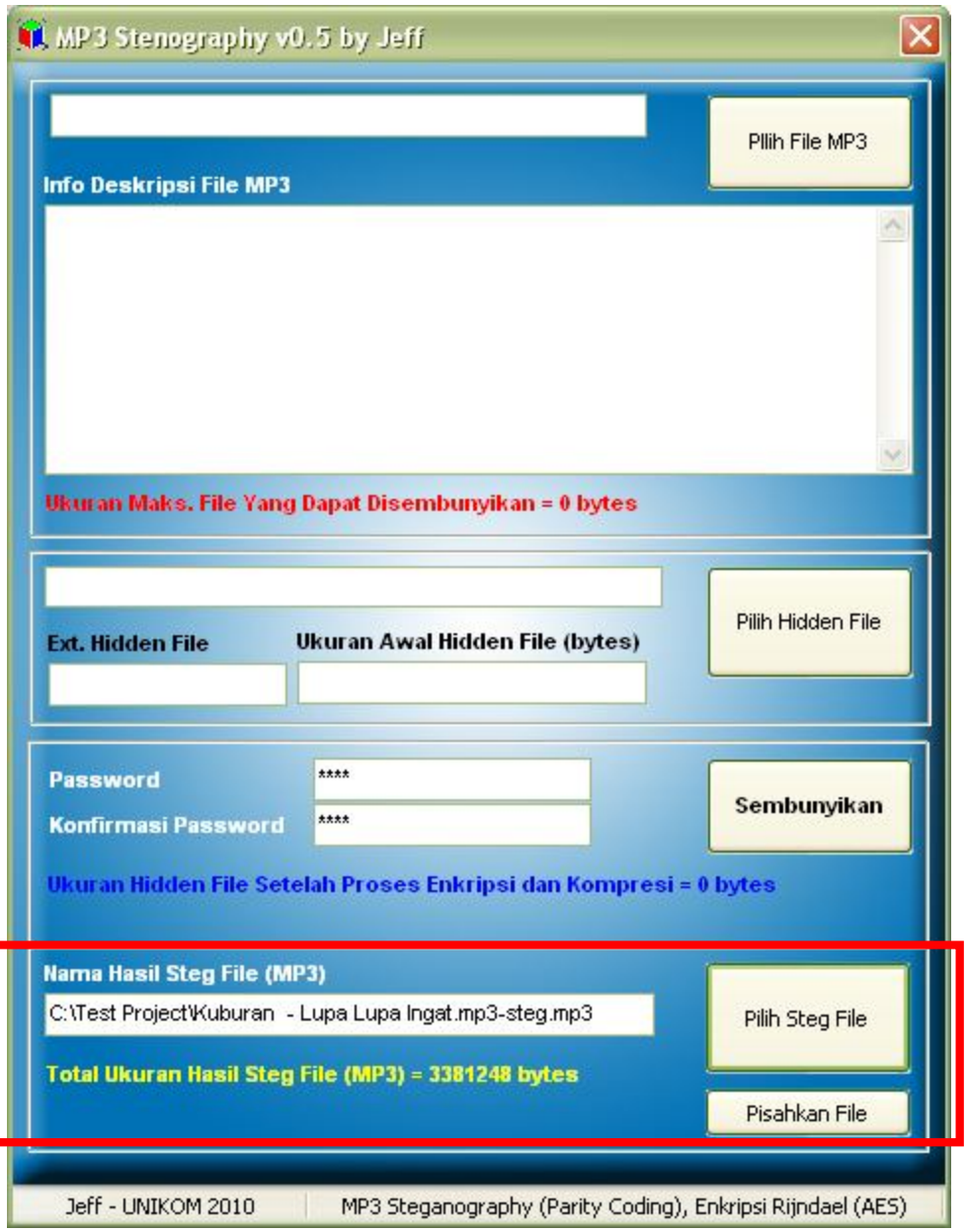
4.1.3 Pengungkapan Pesan Rahasia

Untuk memulai proses pengungkapan pesan, setelah membuka program mp3STEG, pengguna harus mengisi password dan konfirmasi password terlebih dahulu, dengan password yang sama ketika proses penyisipan/penyembunyian pesan rahasia. Kemudian pengguna dapat menekan tombol "Pilih Steg File", lalu akan muncul kotak dialog seperti terlihat pada gambar dibawah ini.



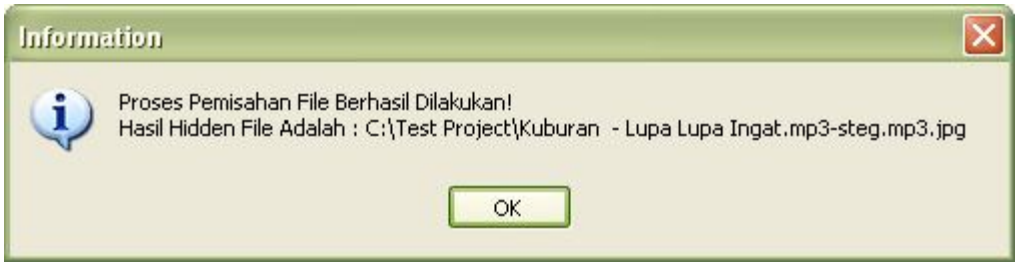
Gambar 4.12 Tampilan Kotak Dialog Pilih Steg File

Pada program, tampilannya adalah seperti gambar dibawah ini.



Gambar 4.13 Tampilan Program Pilih Steg File

Setelah memilih *file MP3* yang mengandung pesan rahasia, selanjutnya pengguna dapat menekan tombol “Pisahkan File”. Apabila proses pengungkapan pesan rahasia sudah selesai, maka akan muncul kotak informasi seperti dibawah ini.



Gambar 4.14 Informasi Pengungkapan/Pemisahan File

Selanjutnya pengguna dapat mengecek pesan rahasia yang sudah dipisah/diungkap. Nama *file* yang terungkap akan disamakan dengan nama *MP3 cover*, agar pengguna mudah mencari *file* yang sudah disisipi.

4.2 Pengujian Perangkat Lunak

Tahap pengujian bertujuan untuk memastikan bahwa perangkat aplikasi yang dibuat memenuhi tujuan yang diinginkan. Pada tahap ini perangkat lunak akan diuji berdasarkan parameter yang telah ditetapkan pada batasan masalah, yaitu aspek keamanan data berupa *fidelity, recovery, robustness* dan *security*.

4.2.1 Aspek *Fidelity*

Aspek *fidelity* yang dimaksud adalah bahwa mutu berkas MP3 hasil steganografi tidak jauh berubah jika dibandingkan dengan berkas MP3 asli. Setelah data rahasia disisipkan ke dalamnya, maka berkas MP3 hasil steganografi

tidak mengalami degradasi yang signifikan, sehingga perubahan tersebut tidak disadari oleh indera pendengaran manusia. Dengan kata lain berkas MP3 yang dihasilkan masih dapat didengarkan dengan baik oleh manusia.

Untuk menguji aspek *fidelity* pada aplikasi ini, akan digunakan dua cara. Yang pertama adalah pengujian secara subjektif dengan menggunakan *Mean Opinion Source (MOS)* dengan melibatkan beberapa orang responden untuk mendengarkan dan membandingkan MP3 asli dengan MP3 hasil steganografi. Cara kedua adalah secara objektif dengan cara melihat perubahan gelombang dan perubahan spectrum dengan menggunakan aplikasi *Cool Edit Pro 2.1* dan pengujian secara objektif, dengan menghitung nilai *Peak Signal to Noise Ratio* (PSNR) pada MP3.

4.2.1.1 Pengujian Subjektif (*Mean Opinion Score (MOS)*)

Mean Opinion Score (MOS) merupakan sebuah metode dalam mengukur kualitas suara berdasarkan deskripsi kualitatif dari apa yang kita dengar, misalnya "sangat bagus" atau "sangat buruk". MOS memberikan indikasi numerik tentang kualitas suara yang didapatkan setelah melalui jalur transmisi atau setelah mengalami pengkodean. Terminologi MOS merupakan hasil rekomendasi dari International Telecommunication Union (ITU-T P.800).

Nilai MOS yang diperoleh tidak harus bilangan bulat. Teknisnya beberapa orang diminta untuk mendengarkan sebuah media audio. Setiap orang diminta untuk menilai kualitas audio tersebut dengan rentang 1 sampai dengan 5. Nilai 1 menyatakan nilai yang terburuk dan 5 untuk menyatakan yang terbaik. Kemudian

dihitung rata-rata penilaian dari seluruh responden sehingga diperoleh nilai *Mean Opinion Score* dari media audio tersebut.

Tabel 4.1 Parameter Penilaian MOS

Nilai	Kualitas MP3	Keterangan
5	*Excellent*	Tidak terdapat derau sama sekali *(Imperceptible*)
4	*Good*	Derau terdengar, namun tidak mengganggu *(Perceptible but not annoying)*
3	*Fair*	Derau sedikit mengganggu *(Slightly annoying)*
2	*Poor*	Derau mengganggu (*Annoying*)
1	*Bad*	Derau sangat mengganggu (*Very annoying*)

Pada pengujian ini, jumlah pengamat sebanyak 6 orang yang dipilih secara acak, masing-masing responden diminta untuk mendengarkan dan membandingkan MP3 asli dengan MP3 hasil proses steganografi, kemudian memberikan nilai MOS berdasarkan kriteria sesuai **Tabel** di atas. Berikut ini adalah hasil uji coba yang dilakukan terhadap 3 berkas MP3 dan telah dinilai oleh masing-masing 6 orang responden.

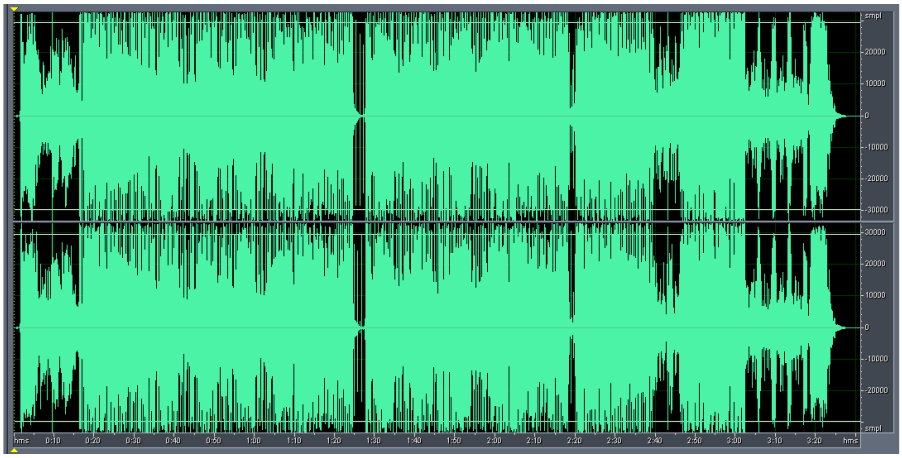
Tabel 4.2 Hasil Pengujian MOS

Pengujian ke-	Keterangan	Nilai MOS
1	Nama MP3: Ke$ha - Your Love Is My Drug.mp3 Ukuran MP3: 3051969 bytes Nama Pesan: pesona-alam-residence-depok.jpg Ukuran Pesan: 57227 bytes Ukuran MP3 Stegged: 3051969 bytes	4,65
2	Nama MP3: Kuburan - Lupa Lupa Ingat.mp3 Ukuran MP3: 3381248 bytes Nama Pesan: gambar.jpg Ukuran Pesan: 27977 bytes Ukuran MP3 Stegged: 3381248 bytes	4,6
3	Nama MP3: We Are The In Crowd - Never Be What You Want.mp3 Ukuran MP3: 4037627 bytes Nama Pesan: b-c-rich-platinum-beast-guitar-black.jpg Ukuran Pesan: 12839 bytes Ukuran MP3 Stegged: 4037627 bytes	4,75

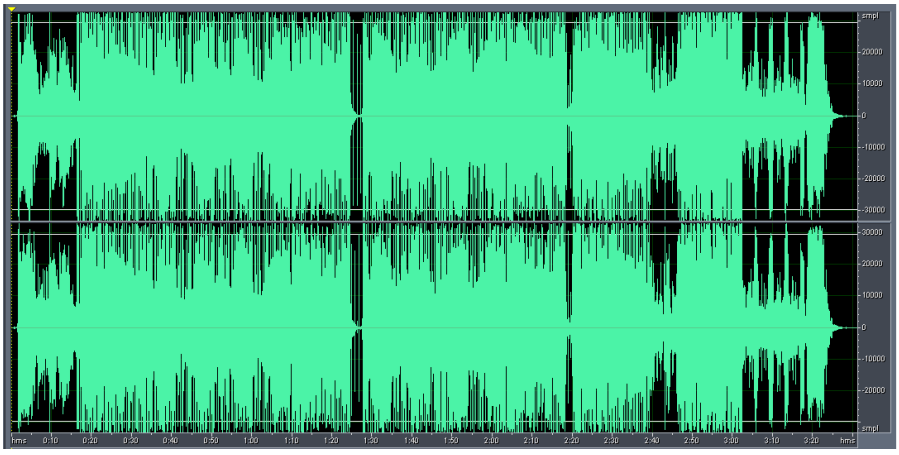
Dari data di atas, dapat dilihat bahwa ketiga pengujian MP3 mendapatkan nilai MOS dengan kualitas *Good,* yang artinya derau terdengar, namun tidak mengganggu *(perceptible but not annoying).* Melalui pengujian secara subjektif dapat disimpulkan, bahwa penyisipan pesan ke dalam MP3 tidak membuat perubahan yang signifikan terhadap kualitas MP3 dan masih dapat didengar dengan baik, sehingga dapat memenuhi aspek *fidelity.*

4.2.1.2 Pengujian Objektif (Perubahan Gelombang & Spectrum Pada MP3)

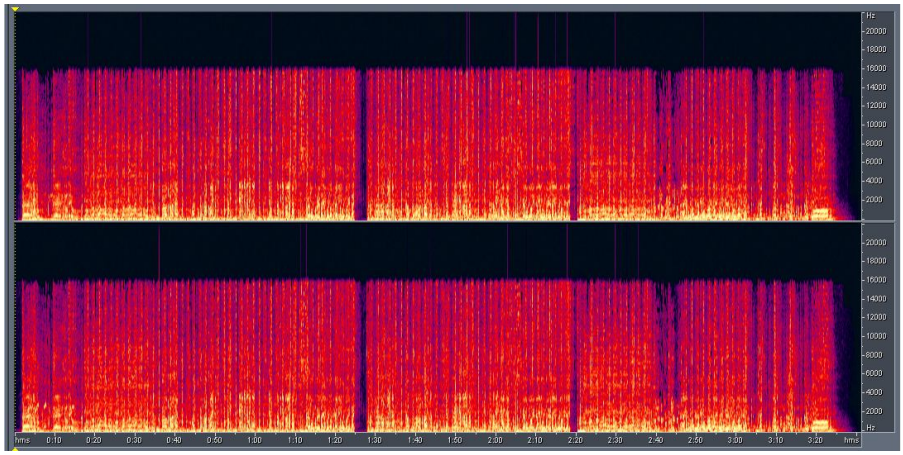
Pada pengujian ini, akan dicoba untuk melihat perubahan gelombang dan perubahan *spectrum* yang terjadi pada *file audio MP3* sebelum dan sesudah disisipi pesan rahasia. Berkas MP3 yang digunakan berjudul **Kuburan - Lupa Lupa Ingat.mp3**. Aplikasi pendukung yang digunakan adalah *Cool Edit Pro 2.1*.



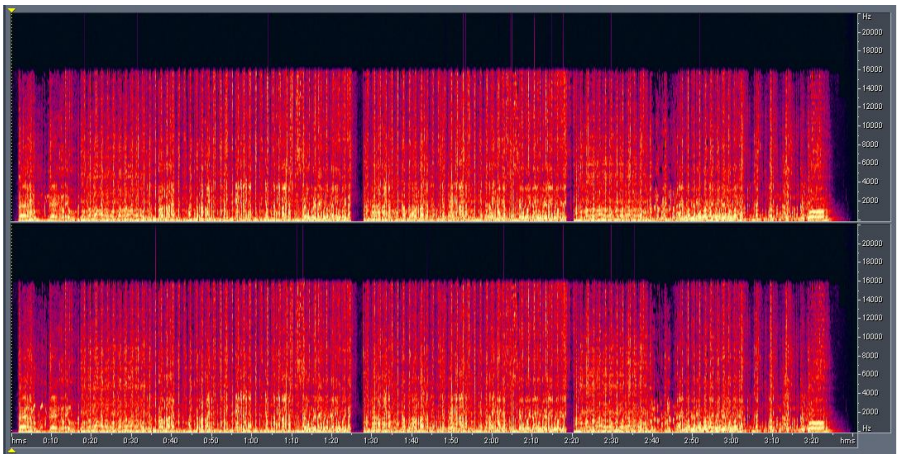
Gambar 4.15 Gelombang MP3 Asli



Gambar 4.16 Gambar Gelombang MP3 *Stegged*



Gambar 4.17 Gambar Spectrum MP3 Asli



Gambar 4.18 Gambar Spectrum MP3 *Stegged*

Dari hasil percobaan diatas, pada **Gambar 4.15** dan **Gambar 4.16**, dapat dilihat gelombang antara MP3 asli dan MP3 hasil *steganography* terlihat sama. Dan saat pemeriksaan *spectrum* menunjukkan hamper tidak terdapat perubahan

spectrum pada MP3 hasil *steganography*, seperti terlihat pada **Gambar 4.17** dan **Gambar 4.18**.

4.2.1.3 Pengujian PSNR (*Peak to Signal Noise Ratio*)

Penilaian kualitas berkas audio MP3 tersebut dilakukan secara subjektif dan objektif. Penilaian subjektif dengan cara mendengarkan suara hasil pemutaran berkas audio MP3. Penilaian objektif dengan cara menghitung nilai PSNR (*Peak Signal to Noise Ratio*). Nilai PSNR dalam satuan desibel (dB) dihitung dengan rumus :

$$PSNR = 10log_{10}\left(\frac{P_1^2}{P_1^2 + P_0^2 - 2P_1P_o}\right)$$

Dengan:

P_0: kekuatan sinyal awal MP3 (dB).

$P_{1:}$ kekuatan sinyal MP3 setelah disisipi data (dB).

P_0 dan P_1 diukur dalam satuan desibel (dB). Nilai PSNR yang wajar mempunyai angka minimal 30 dB. Apabila hasil yang didapat dibawah 30 dB, maka *noise* akan terdengar oleh pendengaran manusia normal.

Tabel 4.3 Hasil Pengujian nilai PSNR

MP3 Asli	Ukuran (byte)	Kapasitas Max Sisip (byte)	Pesan Rahasia	Ukuran (byte)	P_0 (dB)	P_1 (dB)	PSNR (dB)
Kuburan - Lupa Lupa Ingat.mp3	3381248	42710	gambar.jpg	27977	15.64	15.60	57,8
Taylor Swift - Fearless.mp3	7370246	41460	Germany_football_shirt_logo.png	20070	13.85	13.84	62,8
Ke$ha - Your Love Is My Drug.mp3	3051969	61986	pesona-alam-residence-depok.jpg	57227	15.23	15.20	57,8
Miley Cyrus - When I Look at You.mp3	3996975	26457	SEJARAH STEGANOGRAFI.docx	12126	14.53	14,51	57,2

Dari hasil pengujian diatas bisa disimpulkan, angka *decibel* (dB) yang didapat MP3 *cover* dan MP3 *stegged* tidak terjadi perubahan yang signifikan. Sehingga *noise* yang dihasilkan oleh MP3 *stegged* bisa dikatakan tidak terdengar, karena nilai PSNR yang dihasilkan diatas batas minimum yaitu 30 dB.

4.2.2 Aspek *Recovery*

Aspek *recovery* yang dimaksud adalah data rahasia harus dapat disisipkan dan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut. Maka pada tahap ini akan dilakukan pengujian beberapa kali untuk memastikan bahwa data rahasia yang

disisipkan dalam MP3 dapat didapatkan kembali dalam keadaan utuh. Indikator keberhasilan pengujian ini adalah jika panjang teks pesan asli sama dengan panjang teks hasil ekstraksi.

Tabel 4.4 Hasil Pengujian terhadap Aspek *Recovery*

Nama MP3	Pesan Asli	Panjang Pesan Asli (byte)	Status Penyisipan Pesan	Pesan hasil Ekstraksi	Status Ekstraksi Pesan	Panjang pesan hasil ekstraksi (byte)
Kuburan - Lupa Lupa Ingat.mp3	gambar4.jpg	38383	Berhasil	Kuburan - Lupa Lupa Ingat.mp3-steg.mp3.jpg	Berhasil	38383
Justin Bieber feat Ludacris - Baby.mp3	teks0.txt	1938	Berhasil	Justin Bieber feat Ludacris - Baby.mp3-steg.mp3.txt	Berhasil	1938
Air Supply - All Out Of Love.MP3	JADWAL-World-Cup-2010.pdf	78386	Berhasil	Air Supply - All Out Of Love.MP3-steg.MP3.pdf	Berhasil	78386
500 Miles - Felicla's.mp3	57.gif	41235	Berhasil	500 Miles - Felicla's.mp3 -steg.mp3.gif	Berhasil	511
cek.mp3	gambar3.jpg	17600	Berhasil	cek.mp3-steg.mp3.jpg	Berhasil	17600

Setelah dilakukan pengujian, dilakukan penghitungan persentase dari keberhasilan proses *recovery* yang dibandingkan dengan jumlah percobaan yang dilakukan dengan perhitungan sebagai berikut.

$$\text{Presentase Keberhasilan} = \frac{(Jumlah\ percobaan\ yang\ dilakukan - jumlah\ percobaan\ gagal)}{Jumlah\ percobaan\ yang\ dilakukan} * 100\%$$

$$= \frac{(5-0)}{5} * 100\% = 100\%$$

Dari pengujian pada aspek *recovery* yang telah penulis lakukan, tingkat keberhasilannya adalah 100 %. Artinya, aplikasi mp3STEG ini mendukung aspek *recovery* pada keamanan data.

4.2.2.1 Analisis Presentase Terhadap MP3 *Cover*

Tabel di bawah ini adalah mengenai analisis presentase dari setiap pesan yang dapat dibawa oleh MP3 *cover*, menggunakan rumus:

$$\frac{Kapasitas\ Maks\ Sisip\ (byte)}{Ukuran\ MP3\ cover\ (byte)} \text{ x } 100\%$$

Tabel 4.5 Hasil Pengujian Presentase MP3 *Cover*

MP3 *Cover*	Ukuran (byte)	Kapasitas Maks Sisip (byte)	Presentase (%)
500 Miles - Felicla's.mp3	2210296	71434	3,23
eternal flame.mp3	3246793	87686	2,70
Barbra Streisand - Woman In Love.mp3	9397023	248210	2,64
Chris De Burgh - Lady In Red.mp3	10364598	263283	2,54
Breathe - How I Can Fall.mp3	11387553	278358	2,44
goodbye.mp3	3953144	94112	2,38

Dari hasil analisis yang didapat, bisa diambil kesimpulan bahwa ukuran (*size*) MP3 *cover* tidak berpengaruh signifikan terhadap kapasitas maksimum pesan yang dapat dibawa. Contoh: **Breathe - How I Can Fall.mp3** dengan ukuran **11387553 bytes (10,86 MB)**, hanya dapat membawa **2,44%** dari ukuran MP3 tersebut. Sedangkan **500 Miles - Felicla's.mp3** dengan ukuran **2210296**

bytes (2,11 MB), dapat membawa **3,23%** ukuran MP3. Jadi, kapasitas maksimum pesan yang dapat dibawa oleh *carrier* (MP3 *cover*) tergantung pada ketersediaan *frame-frame* pada MP3 *cover* yang bisa diisi pesan rahasia. Ini dikarenakan pada setiap MP3 mempunyai ketersediaan *frame* yang berbeda-beda.

4.2.3 Aspek *Robustness*

Robustness yang dimaksud adalah data rahasia yang disisipkan harus tahan terhadap pengolahan sinyal yang mungkin dilakukan. Untuk menguji aspek *Robustness,* dilakukan pengujian dengan mengubah *bitrate* dan frekuensi *sampling* sebuah MP3 hasil steganografi, Pengujian ini dilakukan pada berkas MP3 berjudul **Kuburan - Lupa Lupa Ingat.mp3**.

Berkas **Kuburan - Lupa Lupa Ingat.mp3** pada awalnya mempunyai *bitrate* sebesar 128 kbps dengan frekuensi *sampling* sebesar 44,1 kHz dan *channel* stereo. Kemudian *bitrate*nya diubah menjadi 112 kbps dengan frekuensi *sampling* sebesar 44,1 kHz dan *channel* mono. Setelah itu dilakukan proses pengungkapan pesan dengan mp3STEG dengan memberikan kunci enkripsi yang sesuai. Hasilnya pesan yang disisipkan tidak dapat diungkapkan kembali dan muncul pesan *error.*

Dari hasil pengujian diketahui bahwa metode pengamanan data dengan mp3STEG tidak mendukung aspek *robustness*. Hal ini disebabkan ketika dilakukan modifikasi pada sinyal MP3, akan turut merubah susunan byte yang ada pada MP3, sehingga akan mengganggu byte-byte pesan yang disisipkan di dalamnya.

4.2.3.1 Pengujian Pengolahan Sinyal Terhadap MP3

Pengujian berikut ini adalah menganalisis apakah terjadi perubahan kapasitas maksimum pesan rahasia yang akan disisipi apabila *bit rate* MP3 *cover* dimanipulasi (pengolahan sinyal) sebelum disisipi pesan rahasia. MP3 *cover* yang dianalisis mempunyai frekuensi 44,1 KHz dengan *bit rate* yang beragam. Pengolahan sinyal menggunakan program bantuan *DietMP3*.

Tabel 4.6 Hasil Pengujian Manipulasi MP3 *Cover*

MP3 *Cover*	*Bit Rate* Awal (kbps)	Kapasitas Maks Sisip Sebelum Manipulasi (byte)	*Bit Rate* Akhir (kbps)	Kapasitas Maks Sisip Setelah Manipulasi (byte)
500 Miles - Felicla's.mp3	128	71434	96	12850
eternal flame.mp3	128	87686	96	54146
Barbra Streisand - Woman In Love.mp3	320	248210	96	39377
Chris De Burgh - Lady In Red.mp3	320	263283	96	21330
Breathe - How I Can Fall.mp3	320	278358	96	42388
goodbye.mp3	128	94112	96	41568

Dari hasil analisis pengolahan sinyal terhadap MP3 *cover* sebelum disisipi pesan, terjadi perubahan / penurunan yang cukup signifikan terhadap kapasitas maksimum ukuran pesan yang dapat disisip. Ini dikarenakan, terjadi perubahan susunan *bit-bit* yang ada di *frame-frame* MP3 *cover* tersebut.

4.2.4 Aspek *Security*

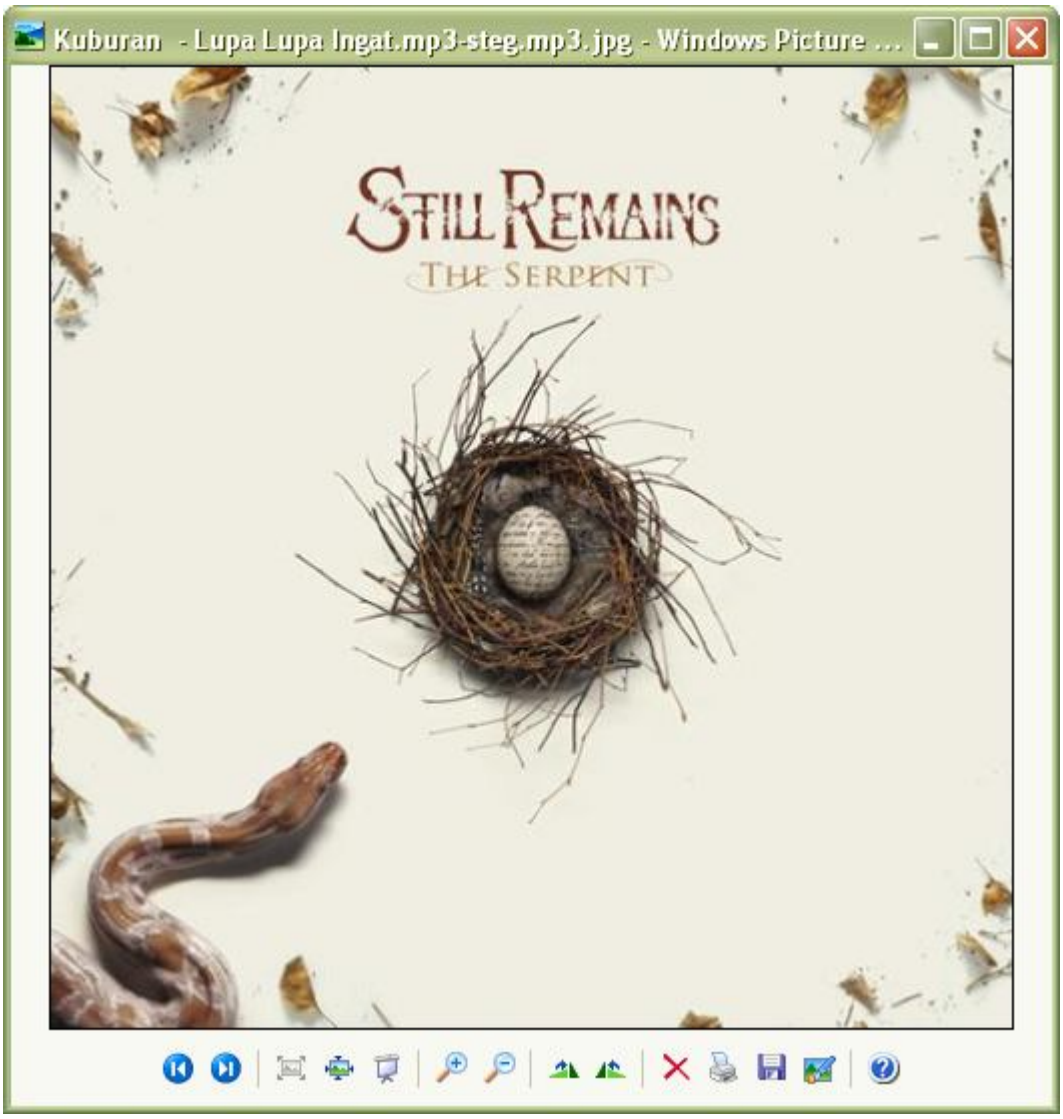
Aspek keamanan pada aplikasi ini diperoleh melalui kunci enkripsi. Untuk mendapatkan pesan rahasia yang telah disisipkan hanya dapat dilakukan dengan memberikan kata kunci yang tepat. Jika kata kunci yang dimasukkan tidak sesuai, maka aplikasi akan menampilkan pesan *error*.

Untuk mengetahui aspek *security* pada perangkat lunak, dilakukan pengujian dengan melakukan penyisipan dan pengungkapan pesan pada MP3. Dalam hal ini disediakan dua buah kasus. Kasus yang pertama apabila kunci enkripsi yang diberikan sesuai. Kasus kedua adalah apabila kunci dekripsi yang diberikan salah. Kasus pertama menghasilkan pesan yang sesuai dengan pesan asli. Sedangkan pada kasus kedua didapatkan bahwa aplikasi menampilkan pesan *error*. Berkas yang digunakan sebagai media penyisipan berjudul **Kuburan - Lupa Lupa Ingat.mp3** yang berukuran 3.381.248 bytes. Berkas gambar yang disisipkan berjudul **gambar.jpg** yang berukuran 27.977 bytes.



Gambar 4.19 Tampilan Pesan Asli (gambar.jpg)

Hasil dari proses penyisipan,pesan adalah **01 Kuburan - Lupa Lupa Ingat.mp3** dengan kunci enkripsi yang digunakan adalah **"1234".** Setelah itu dilakukan pengungkapan pesan dengan memberikan kunci yang sesuai yaitu **"1234"**, maka diperoleh pesan hasil ekstraksi dengan nama **Kuburan - Lupa Lupa Ingat.mp3-steg.mp3.jpg.**



Gambar 4.20 Tampilan Pesan Hasil Ekstraksi

4.2.5 Hasil Pengujian

Dari beberapa pengujian terhadap aspek-aspek keamanan data di atas, diperoleh hasil pengujian sebagai berikut.

Tabel 4.7 Hasil Pengujian terhadap Aspek Keamanan Data

No	Pengujian	Keterangan
1	*Fidelity*	Pada pengujian subjektif, nilai MOS yang didapatkan untuk tiga sampel MP3 yang diujikan bernilai > 4, menunjukkan bahwa kualitas MP3 hasil steganografi masih dapat didengarkan dengan baik. Pada pengujian objektif, Berkas yang diuji mempunyai nilai PSNR > 30 dB artinya mengalami derau yang rendah. Ukuran berkas MP3 hasil steganografi adalah sama dengan ukuran MP3 aslinya. Artinya penyisipan pesan rahasia ke dalam MP3 tidak mempengaruhi besar berkas MP3. Dari hasil pengujian di atas dapat dilihat bahwa perangkat lunak ini mendukung aspek *fidelity*, artinya MP3 hasil steganografi tidak mengalami degradasi yang signifikan dan masih dapat didengarkan dengan baik.
2	*Recovery*	Dari hasil pengujian, pesan yang disisipkan ke dalam MP3 dapat diungkapkan kembali dengan ukuran pesan sama dengan ukuran pesan aslinya, maka dapat dilketahui bahwa perangkat lunak ini dapat memenuhi aspek

		recovery.
3	*Robustness*	Pada pengujian untuk aspek robustness, setelah dilakukan modifikasi pada MP3 hasil steganografi dengan mengubah nilai bitrate dan frekuensi samplingnya, maka pesan yang ada di dalam MP3 hasil steganografi tidak dapat diungkapkan kembali. Dari pengujian di atas diketahui bahwa perangkat lunak tidak memenuhi aspek robustness. Apabila pengolahan sinyal dilakukan terhadap MP3 *cover* sebelum disisipi, maka terjadi penurunan terhadap ukuran kapasitas maksimum pesan yang dapat disisipi. Namun MP3 *cover* masih dapat membawa pesan rahasia dengan baik.
4	*Security*	Pada pengujian terhadap aspek security, hasilnya adalah pesan hanya dapat diungkap dari MP3 jika kunci dekripsi yang diberikan sesuai. Jika tidak, maka pesan tidak akan dapat diungkap. Dari pengujian ini diketahui bahwa perangkat lunak mendukung aspek security

Dari pengujian yang telah dilakukan, diketahui bahwa perangkat lunak memenuhi tiga dari aspek keamanan yang diujikan selain *robustness.* Seperti

halnya metode LSB, metode penyisipan pesan dengan penggantian bit kurang kokoh (*robust*) dan memiliki ketahanan yang rendah pada modifikasi sinyal (Cvejic, 2004). Karena perubahan tersebut akan merusak susunan bit pada MP3 sehingga mengganggu bit-bit pesan yang ada di dalamnya.

Berdasarkan hasil pengujian, dapat dilihat bahwa dengan menggunakan perangkat lunak ini, keamanan pesan yang disisipkan ke dalam MP3 akan semakin meningkat. Karena pesan yang disisipkan dalam keadaan terenkripsi, serta MP3 yang dijadikan sebagai penampung pesan tidak mengundang kecurigaan karena tidak mengalami perubahan berarti yang dapat dipersepsi manusia.