

BAB IV

IMPLEMENTASI DAN PEMBAHASAN

4.1 Tinjauan Perangkat Lunak

Berikut adalah spesifikasi yang digunakan dalam pembangunan dan penyelesaian aplikasi stegorijndael adalah sebagai berikut.

- a. Perangkat keras yang digunakan:
 - Processor : Intel core i5-2450M 2,5 GHz
 - RAM : 4000 MB
 - Hardisk : 640 GB
- b. Perangkat lunak yang digunakan:
 - Sistem operasi windows 7 64 bit
 - Netbeans IDE 8.1

4.2 Hasil Implementasi

Pada bab ini membahas tentang aplikasi hasil implementasi algoritma Rijndael dalam steganografi citra digital metode LSB (*Least Significant Bit*) yang telah dibangun. Hasil implementasi akan dijelaskan dalam beberapa bagian. Tujuan dari implementasi ini adalah untuk mengetahui apakah aplikasi yang telah dibangun sudah sesuai dengan pernacangan sebelumnya.

4.2.1. Menu Utama

Menu utama merupakan tampilan utama dari program stegorijndael atau yang muncul pertama kali saat program stegorijndael ini dijalankan. Terdapat beberapa menu yang ada pada bagian menu utama ini yaitu menu sisipkan pesan, menu ekstrak pesan, menu *about* dan menu keluar. Menu sisipkan pesan apabila dipilih akan menuju pada halaman untuk keperluan penyisipan pesan. Menu ekstrak pesan akan menuju pada bagian pengambilan pesan atau ekstraksi. Menu

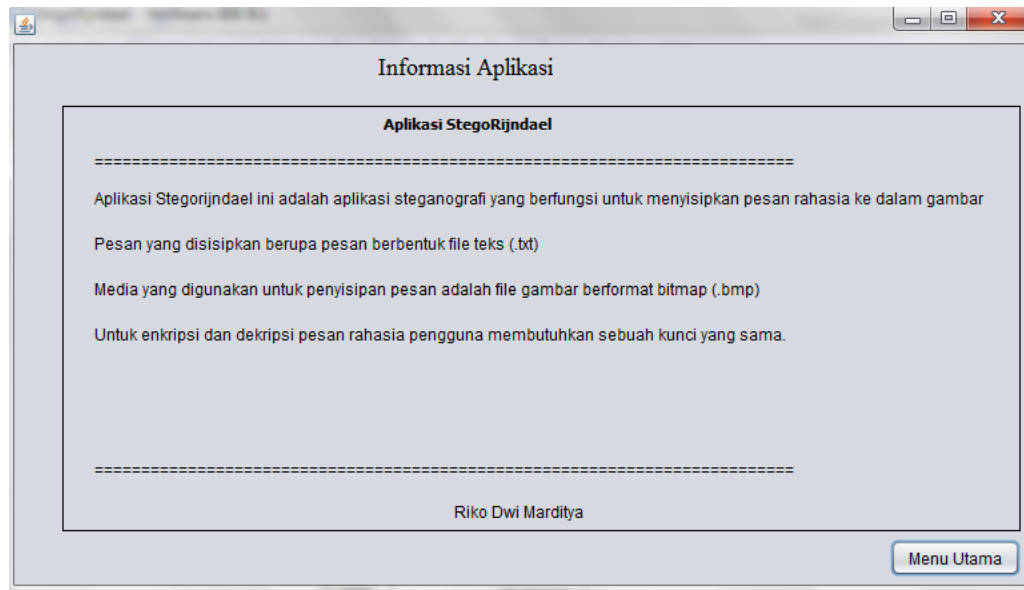
about sendiri berguna untuk memberikan informasi kepada pengguna tentang kegunaan dari program stegorijndael tersebut. Terakhir adalah menu keluar yang berfungsi untuk menutup program tersebut. Tampilan Menu Utama seperti pada gambar 4.1 berikut.



Gambar 4.1 Menu Utama

4.2.2. Menu *About*

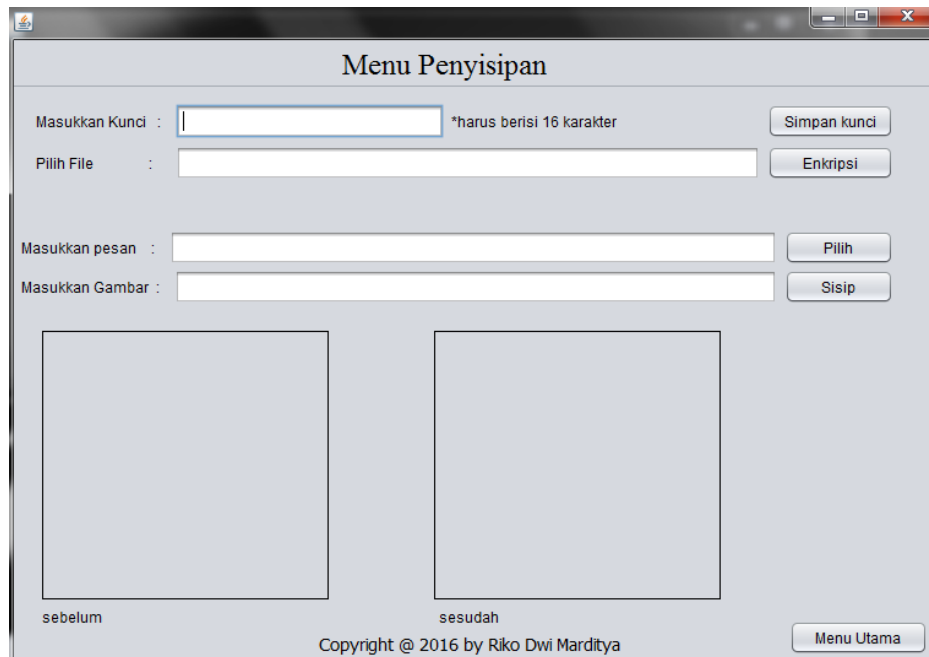
Menu ini adalah menu yang akan muncul apabila pengguna memilih tombol *about* pada menu utama. Menu ini akan menampilkan informasi tentang aplikasi ini agar pengguna paham tentang aplikasi ini.



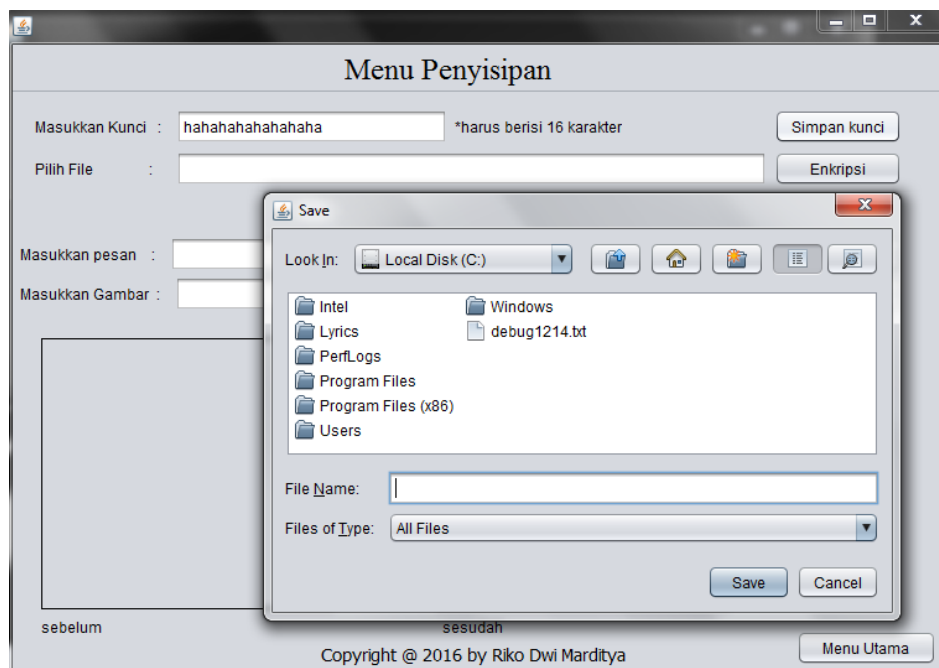
Gambar 4.2 Menu *about*

4.2.3. Penyisipan Pesan (*embedding*)

Pada menu penyisipan ini digunakan untuk menyisipkan sebuah pesan sebuah *file* teks (.txt) ke dalam media citra digital dengan format bitmap (.bmp). Pertama pengguna akan diminta untuk memasukan kode sebagai kunci enkripsi pesan, kemudian melalui tombol enkripsi pengguna memasukan pesan rahasia yang akan dienkripsi dan lakukan proses enkripsi pesan rahasia. Pengguna juga dapat menyimpan kode kunci enkripsi untuk keperluan dekripsi pesan rahasia dengan memilih tombol simpan kunci. Apabila berhasil melakukan proses enkripsi maka akan tersimpa *file* baru dengan ekstensi (.enc) sebagai tanda kalauproses enkripsi berhasil. Tampilan aplikasi pada gambar 4.2 dan gambar 4.3 berikut ini.



Gambar 4.3 Menu Penyisipan



Gambar 4.4 Penyimpanan Kunci

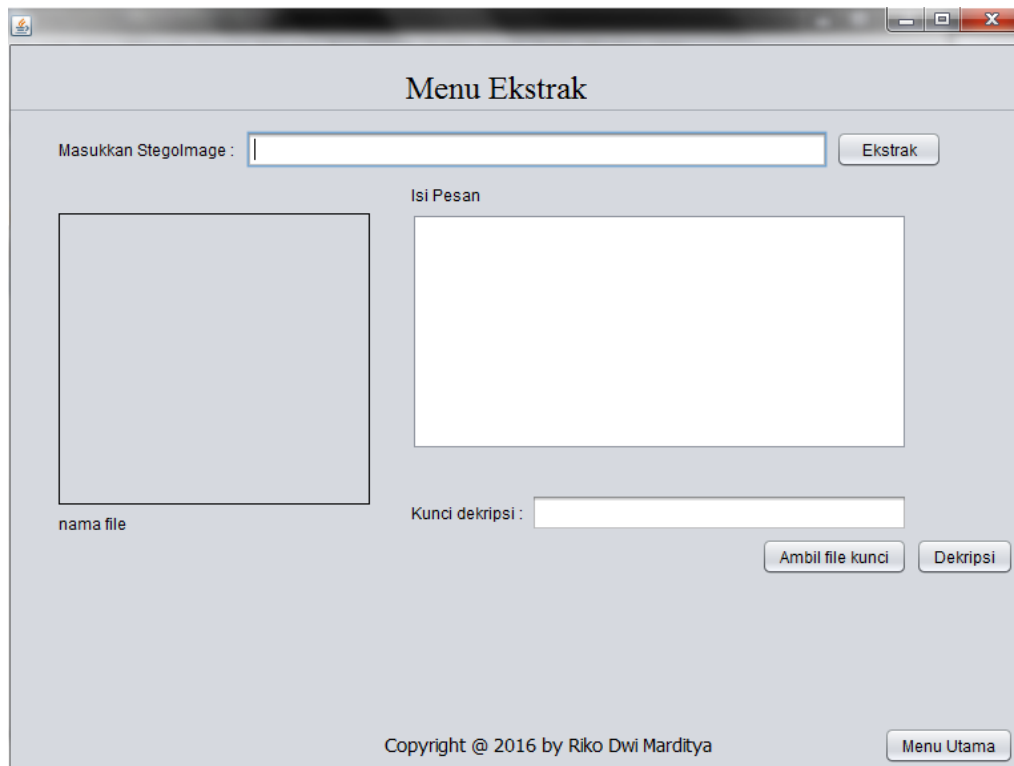
Kolom masukkan pesan yang ada pada menu penyisipan berfungsi untuk mengambil pesan yang sudah terenkripsi sebelumnya untuk siap disisipkan ke media gambar. Kolom masukkan gambar digunakan untuk memilih media penyisipan *file* gambar yang akan digunakan untuk disisipi pesan, *file* gambar tersebut berformat bitmap (.bmp) dan lakukan proses penyisipan. Apabila berhasil maka pengguna diminta memberi nama *file* baru untuk disimpan menjadi *stegoimage*. Di bagian bawah terdapat dua tampilan gambar, sebelah kiri merupakan tampilan gambar sebelum disisipi pesan dan pada sebelah kanan adalah tampilan gambar setelah disisipi pesan tersembunyi. Di pojok kanan bawah terdapat menu utama yang berfungsi untuk kembali ke menu utama program. Penyisipan berhasil apabila tampilan seperti gambar 4.4 berikut.



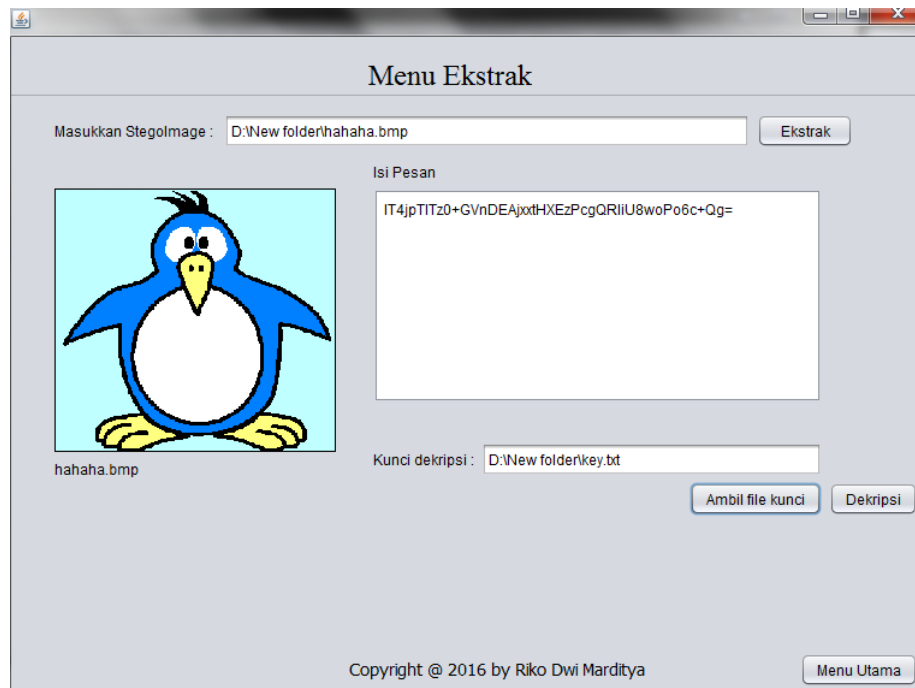
Gambar 4.5 Penyisipan Pesan Berhasil

4.2.4. Pengambilan Pesan (ekstraksi)

Menu ekstrak adalah menu yang akan ditampilkan bila tombol menu ekstrak pada menu utama dipilih. Bagian atas terdapat kolom masukkan *stegoimage* yang berfungsi untuk memilih *file stegoimage* yang ingin diekstrak. *Stegoimage* yaitu sebuah *file* yang dihasilkan pada proses penyisipan pesan sebelumnya. *Stegoimage* diambil untuk mengekstrak pesan yang terdapat di dalamnya. Pada kotak sebelah kiri menampilkan tampilan *stegoimage* yang diambil dan diekstrak. Pada bagian kanan terdapat sebuah kolom teks yang menampilkan isi pesan yang berhasil diekstrak dari dalam *stegoimage*. Di bawah kolom teks isi pesan terdapat tombol ambil *file* kunci yang telah disimpan saat proses penyisipan untuk digunakan dalam proses dekripsi *file* teks agar isi pesan dapat dibaca oleh pengguna. Di sebelah tombol ambil *file* kunci terdapat tombol dekripsi yang digunakan untuk melakukan proses dekripsi. Tampilan menu ekstrak seperti pada di gambar 4.5 dan gambar 4.6.



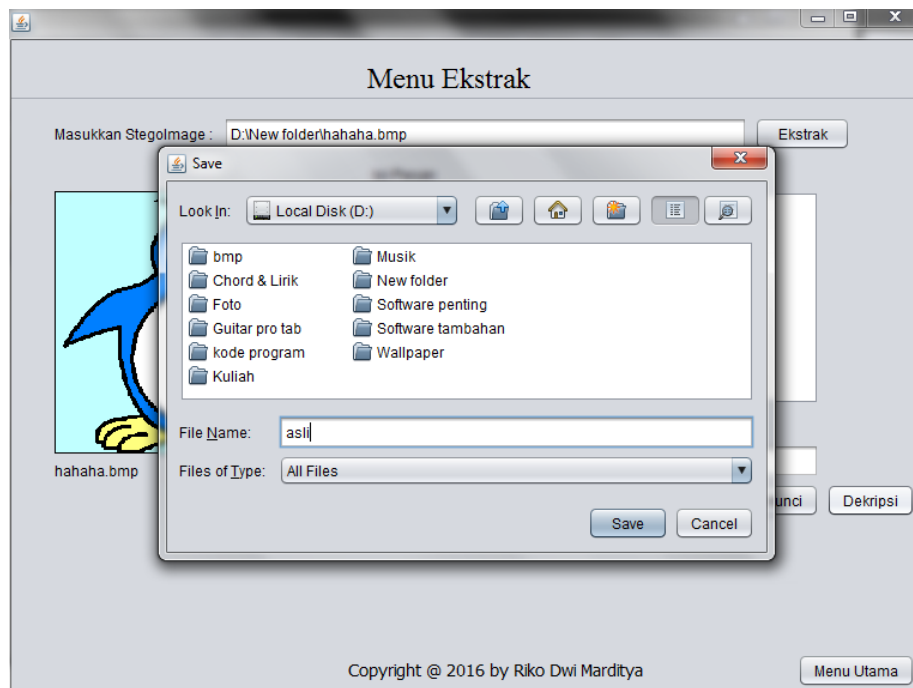
Gambar 4.6 Menu Ekstrak



Gambar 4.7 Ekstrak pesan

4.2.5. Proses Dekripsi

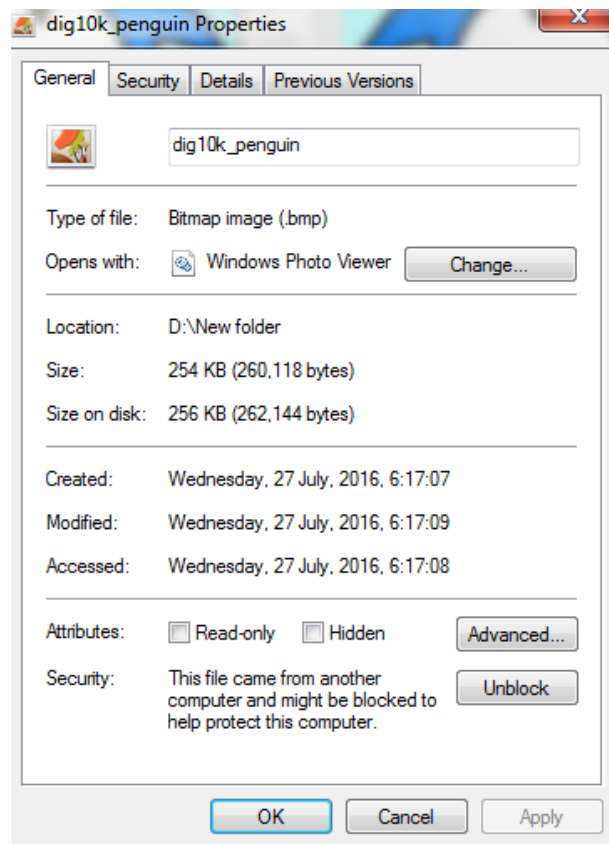
Setelah pengguna memilih *file* kunci dekripsi, kemudian akan melakukan dekripsi dengan menggunakan tombol dekripsi. Apabila pesan berhasil didekripsi, pesan rahasia akan disimpan dengan nama dan lokasi sesuai dengan yang pengguna tentukan. Tampilan proses dekripsi adalah sebagai berikut.



Gambar 4.8 Proses Dekripsi

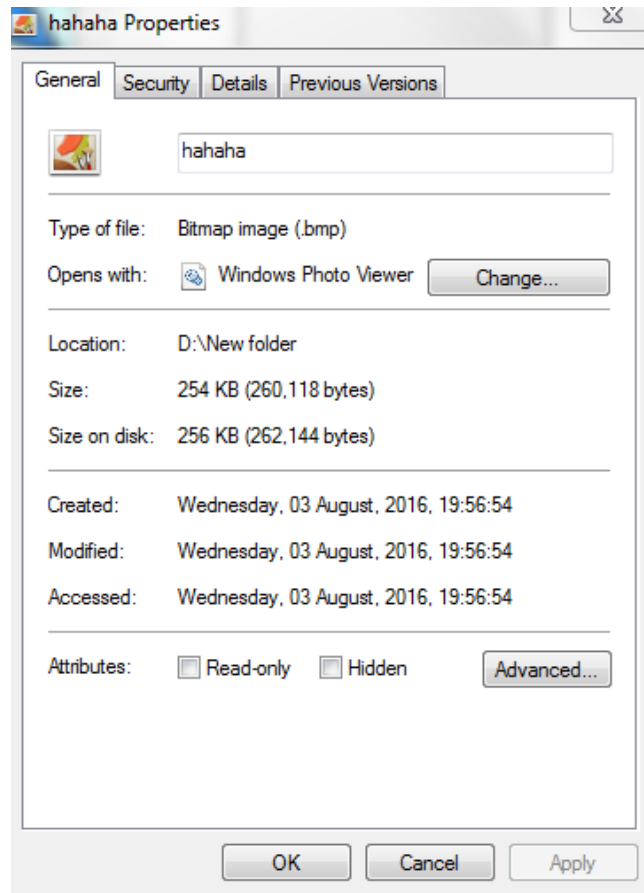
4.2.6. Pengujian *File* Gambar Sebelum dan Sesudah Penyisipan

Dalam pengujian ini akan dilakukan analisis perbandingan *file* gambar sebagai media penyisipan pesan rahasia sebelum dan sesudah dilakukan proses penyisipan. Gambar yang digunakan berformat bitmap (.bmp). Gambar yang digunakan sebelum penyisipan dengan dig10k_penguin.bmp. Rincian gambar sebelum dilakukan proses penyisipan adalah sebagai berikut.



Gambar 4.9 Gambar sebelum proses penyisipan

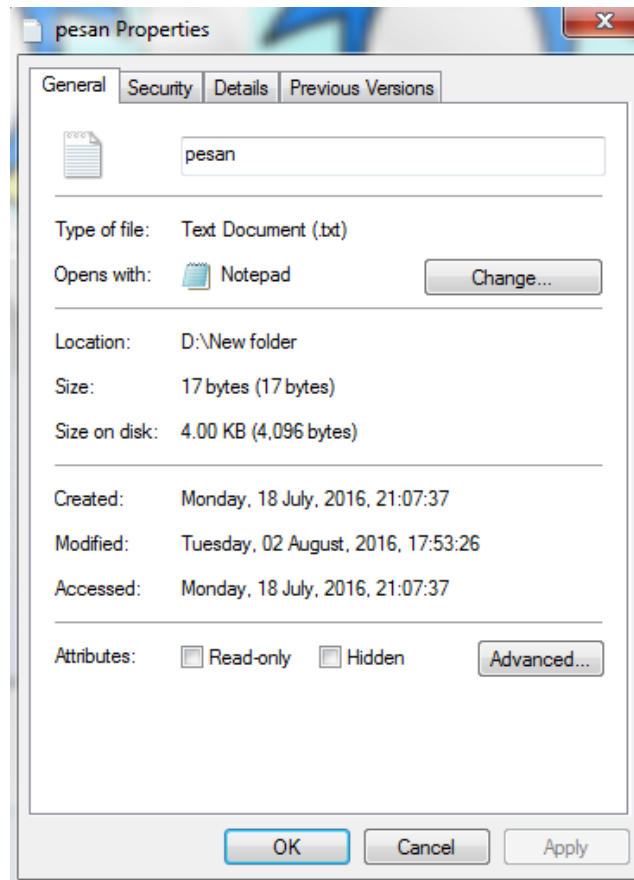
Setelah melakukan proses penyisipan pesan rahasia, maka hasil proses penyisipan adalah *file stegoimage* dengan format bitmap yang telah dinamai *hahaha.bmp*. Perubahan ukuran *file* gambar setelah proses penyisipan tidak begitu signifikan yaitu masih tetap. Detail dari ukuran gambar *hahaha.bmp* adalah sebagai berikut.



Gambar 4.10 Gambar sesudah proses penyisipan

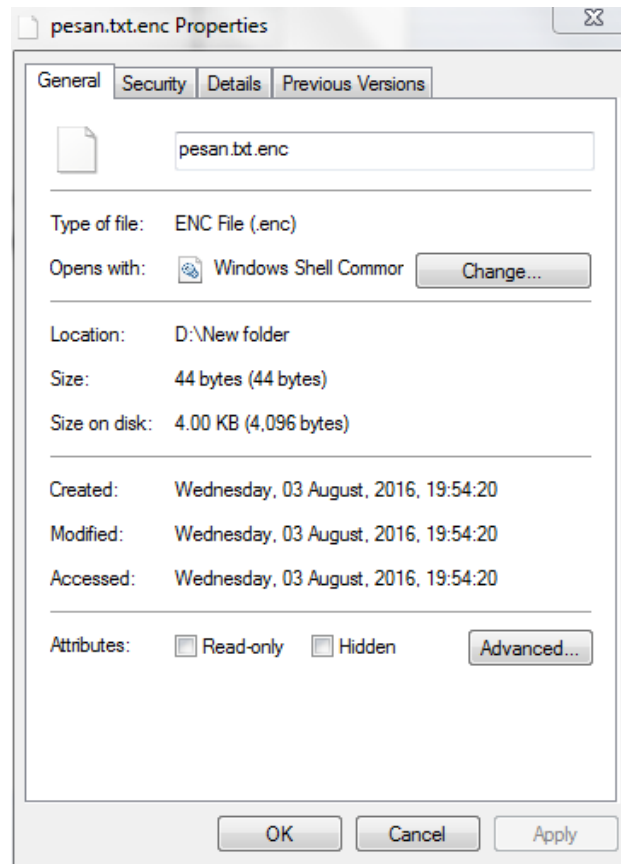
4.2.7. Pengujian *File* Pesan Sebelum dan Sesudah Proses Enkripsi

Pada bagian ini akan dilakukan perbandingan dari *file* pesan rahasia sebelum dilakukan proses enkripsi dan sesudah proses enkripsi. Sebelum dilakukan proses enkripsi, *file* teks pesan.txt yang berisi pesan rahasia yang telah dibuat manual berukuran 17 byte. Detail ukuran pesan.txt tersebut adalah sebagai berikut.



Gambar 4.11 Ukuran pesan.txt

Proses enkripsi dilakukan sesudah memasukkan kunci dan pesan berbentuk *file* teks. Hasil dari pesan rahasia setelah proses enkripsi adalah dengan nama pesan.txt.enc dengan tambahan .enc pada akhir nama *file* nya. Ukuran *file* sesudah dienkripsi berubah menjadi 44 byte karena isi pesan rahasia sudah berubah dari sebelum dienkripsi. Detail *file* pesan.txt.enc yaitu pada gambar 4.12 berikut.



Gambar 4.12 Ukuran pesan.txt.enc

4.3 Hasil Pengujian Kualitas Steganografi

Dalam hasil pengujian kualitas steganografi ini akan dibahas per kriteria steganografi:

a. Hasil Pengujian *Fidelity*

Hasil pengujian dari kriteria ini yaitu dengan menghitung nilai PSNR dan ukuran file tidak berubah dari sebelum penyisipan dan sesudah penyisipan. Nilai PSNR di atas 40 dB membuktikan kalau kualitas gambar stego image adalah termasuk baik dan apabila dibawah 30 dB maka kualitas stegoimage tergolong rendah. Pada hasil pengujian yang telah dilakukan dengan beberapa jenis gambar dalam penyisipan pesan, gambar stegoimage semuanya berada di atas 40 dB yang menunjukkan bahwa stegoimage yang dihasilkan berkualitas cukup baik. Kemudian untuk ukuran file gambar sebelum dan

sesudah disisipi yaitu terjadi penambahan ukuran file pada gambar berjenis grayscale. Tabel pengujian untuk kriteria *fidelity* adalah sebagai berikut :

Gambar asli	Ukuran	Jenis	Stegoimage	Ukuran	PSNR (dB)
Baboon.bmp	257 KB	Grayscale	a.bmp	768 KB	63.56
dig10k_penguin.bmp	254 KB	RGB	b.bmp	254 KB	61.74
frank.large.bmp	5.47 MB	RGB	c.bmp	5.47 MB	72.57
IvyTexture.bmp	179 KB	RGB	d.bmp	179 KB	59.46
Mountaintrain.bmp	957 KB	RGB	e.bmp	957 KB	66.68
Lena512.bmp	257 KB	Grayscale	f.bmp	768 KB	63.55

Tabel 4.1 Tabel Pengujian *Fidelity*

b. Hasil Pengujian *Robustness*

Untuk memenuhi kriteria *robustness* dilakukan dengan pengujian beberapa stegoimage, yaitu dengan melakukan manipulasi gambar pada gambar stegoimage yaitu dengan manipulasi crop, brightness, rotasi. Setelah dilakukan pengujian dari beberapa manipulasi semua gambar yang dimanipulasi tidak *robustness* karena tidak memenuhi kriteria yaitu stegoimage yang sudah dimanipulasi tidak dapat diekstrak. Tabel hasil pengujian *robustness* ditunjukkan pada tabel 4.3 berikut.

Stegoimage	Ukuran	Jenis Manipulasi	Ukuran sesudahnya	Recovery
a.bmp	768 KB	Crop kanan	575 KB	Tidak
b.bmp	254 KB	Crop atas	190 KB	Tidak
c.bmp	5.47 MB	Crop bawah	4.63 MB	Tidak
d.bmp	179 KB	Brightness + 25%	238 KB	Tidak
e.bmp	957 KB	Rotasi ke kiri	1.24 MB	Tidak

Tabel 4.2 Tabel Pengujian *Robustness*

c. Hasil Pengujian *Recovery*

Untuk memenuhi kriteria *recovery* maka pesan rahasia yang disisipkan harus bisa diekstrak kembali tanpa ada kendala. Dalam pengujian ini masing – masing gambar stegoimage diekstrak dan diambil pesan rahasianya. Menurut hasil pengujian seluruh pesan disisipkan gambar dapat diekstrak kembali sehingga memenuhi kriteria *recovery*. Tabel hasil pengujian *recovery* ada pada tabel berikut.

Stegoimage	Ukuran	Pesan yang diekstrak	Ukuran Pesan	Dapat diekstrak/tidak
a.bmp	768 KB	pesan.txt	17 bytes	Dapat
b.bmp	254 KB	pesan 2.txt	628 bytes	Dapat
c.bmp	5.47 MB	pesan 3.txt	6,21 KB	Dapat
d.bmp	179 KB	pesan.txt	17 bytes	Dapat
e.bmp	957 KB	pesan 2.txt	628 bytes	Dapat
f.bmp	768 KB	pesan 3.txt	6,21 KB	Dapat

Tabel 4.3 Tabel Pengujian *Recovery*

d. Hasil Pengujian *Security*

Dari hasil pengujian untuk kriteria *security* maka dilakukan pengujian terhadap pesan yang disisipkan. Pada aplikasi stegorijndael ini pesan dienkripsi oleh algoritma rijndael 128 bit. Hasil pengujian ini menunjukkan bahwa semua pesan yang disisipkan berhasil dienkripsi dengan baik sehingga memenuhi aspek *security* yaitu pesan yang disisipkan dapat dijaga isi kerahasiaannya.

File sebelum enkripsi	Ukuran	File sesudah enkripsi	Ukuran
pesan.txt	17 bytes	pesan.txt.enc	44 bytes
pesan 2.txt	628 bytes	pesan 2.txt.enc	832 bytes
pesan 3.txt	6,21 KB	pesan 3.txt.enc	8,00 KB

Tabel 4.4 Tabel Pengujian *Security*

4.4 Kelebihan dan Kekurangan Aplikasi

Sebuah aplikasi yang telah dibuat tentu memiliki kelebihan dan kekurangannya masing – masing. Kekurangan pada suatu aplikasi dijadikan sebagai acuan untuk perbaikan dan perkembangan di masa yang akan datang. Kelebihan dari aplikasi stegorijndael ini adalah sebagai berikut :

1. Dapat menyimpan kunci ke dalam format *file* teks.
2. *File* stegoimage dan *file* chiperteks dapat disimpan.
3. Dapat menampilkan isi pesan yang disisipkan.
4. Dapat menyimpan hasil dekripsi ke dalam format *file* teks.
5. Dapat menampilkan gambar sebelum dan sesudah dilakukan penyisipan pesan.

Kekurangan dari aplikasi stegorijndael ini adalah sebagai berikut :

1. Aplikasi ini belum bisa menghitung nilai PSNR dari stegoimage.
2. Aplikasi ini belum bisa menghitung kecepatan dari proses enkripsi.
3. Aplikasi ini hanya menyediakan algoritma rijndael dengan kunci 128 bit saja.