PENYULITAN IMEJ MENGGUNAKAN ALGORITMA PIAWAI PENYULITAN LANJUTAN (AES)

NURUL IZZATI IFFAH BINTI NASIR
SALWANI ABDULLAH
KHAIRUL AKRAM ZAINOL ARIFFIN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Penyulitan dan Penyahsulitan Imej menggunakan algoritma Piawai Penyulitan Lanjutan (AES) sangat penting dalam melindungi data imej yang sulit daripada diakses oleh orang yang tidak dikenali. Dalam pada yang sama, peningkatan penggunaan imej dalam pelbagai bidang kini memerlukan perlindungan ini. Data imej berbeza dengan teks di mana ia tidak sesuai disulitkan secara terus dengan menggunakan sistem kripto tradisional seperti RSA dan Piawai Penyulitan Imej (DES). Hal ini kerana saiz imej lebih besar jika dibandingkan dengan teks. Hal ini menyebabkan sistem kripto tradisional memerlukan lebih masa untuk prosess penyulitan data imej. Selain itu, kandungan teks sebelum disulitkan dan selepas dinyahsulitkan perlu menghasilkan hasil yang sama. Walaubagaimanapun, keperluan ini tidak penting untuk data imej kerana disebabkan persepsi sifat manusia: imej yang telah disulitkan mengandungi sedikit perubahan, masih yang boleh diterima. Metod yang digunakan dalam aplikasi ini adalah Kitar Hayat Model Tokokan (*Incremental Development*). Model ini ialah metod di dalam pembangunan perisian di mana produk direka bentuk, diimplemen dan diuji secara berperingkat berdasarkan kepada pembentukan fasa-fasa.

1 PENGENALAN

Pada masa kini, isu keselamatan merupakan perkara yang penting semasa menggunakan Internet dan rangkaian yang lain. Pencerobohan keselamatan boleh menganggu privasi pengguna. Oleh itu, banyak langkah yang perlu diambil untuk mengatasi masalah pencerobohan keselamatan dalam rangkaian. Penyulitan adalah salah satu untuk mengatasi pencerobohan keselamatan dalam rangkaian. Kebanyakan teknik penyulitan mudah dilaksanakan dan digunakan secara meluas dalam bidang keselamatan maklumat. Penyulitan data adalah langkah yang dilakukan untuk melindunginya sebelum dihantar ke sebarang rangkaian. Penyulitan bermaksud mengubah data biasa kepada sifer (data yang dah disulitkan). Penyahsulitan pula proses menukar data yang telah disulitkan kepada yang asal supaya dapat dibaca oleh komputer (Devi et al., 2015).

Keperluan untuk melindungi maklumat di dalam Internet sangat penting kerana dengan jumlah pengguna Internet yang meningkat dari tahun ke tahun, pencerobohan keselamatan boleh membawa kemudaratan kepada organisasi yang bergantung kepada penggunaan rangkaian dalam menjalankan urusan harian. Kebanyakan proses dalam bidang komunikasi Internet, sistem multimedia, pengimejan perubatan, teleperubatan dan komunikasi

ketenteraan berkait rapat dengan data yang berbentuk imej. Data jenis ini berisiko tinggi jika diambil oleh orang yang tidak sepatutnya sekiranya mudah digodam dan terdedah kepada umum. Semakin banyak imej yang digunakan, semakin tinggi keselamatan yang diperlukan. Sebagai contoh, adalah penting untuk melindungi pangkalan data imej tentera, memastikan rakaman video pesalah sulit dan melindungi album fotografi individu dalam talian.

Selain itu, gambar juga merupakan alat yang penting untuk mentafsir maksud. Apabila membabitkan isu keselamatan, adalah lebih penting melindungi gambar daripada melindungi data teks. Penyulitan data banyak digunakan untuk memastikan keselamatan. Namun, kebanyakan algoritma penyulitan kini berdasarkan data teks. Saiz data yang besar dan kekangan masa nyata menyebabkan algoritma ini tidak sesuai dengan penyulitan jenis data imej.

2 PENYATAAN MASALAH

Sistem kripto ialah sistem untuk penyulitan. Terdapat pelbagai sistem penyulitan data untuk menyulit dan menyahsulit data yang sedia ada seperti Piawai Penyulitan Imej (DES), DES Ganda Tiga (3DES), *Blowfish*, Piawai Penyulitan Lanjutan (AES) dan lain-lain lagi. Kebanyakan sistem kripto tradisional atau moden direkabentuk untuk melindungi data teks. Teks biasa yang asal ditukar ke teks sifer (bentuk mesej yang tersembunyi) di mana ia disimpan atau dipindahkan ke rangkaian. Selepas itu, teks sifer boleh diubah kembali kepada teks biasa yang asal menggunakan algoritma penyahsulitan.

Masalah utama dalam proses penyulitan imej adalah masa yang diambil untuk pemprosesan imej dan tahap keselamatannya. Bagi penyulitan imej masa nyata, hanya data sifer yang digalakkan kerana tempoh masa yang diambil untuk pemprosesan imej lebih sedikit tetapi tiada ciri keselamatan. Skema penyulitan akan lambat diproses walaupun mempunyai ciri keselamatan yang tinggi.

Data imej berbeza dengan teks. Ia tidak sesuai digunakan walaupun sistem kripto tradisional seperti RSA dan Piawai Penyulitan Imej (DES) digunakan untuk menyulit imej secara terus. Hal ini kerana saiz imej selalunya lebih besar daripada teks. Oleh itu, sistem kripto tradisional memerlukan masa yang lebih untuk menyulit data imej. Selain itu, teks yang telah disulitkan mesti sama dengan teks yang asal. Keperluan ini tidak penting untuk data imej. Hal ini disebabkan persepsi sifat manusia: imej yang telah disulitkan mengandungi sedikit herotan yang boleh diterima.

Banyak cara penyulitan yang telah digunakan sebelum ini dan cara yang selalu digunakan untuk melindungi fail multimedia yang besar adalah dengan menggunakan teknik penyulitan yang biasa. Algoritma penyulitan kekunci persendirian seperti 3DES atau *Blowfish* tidak sesuai untuk penghantaran saiz data yang besar seperti imej. Oleh kerana struktur dalamannya yang rumit, algoritma ini tidak cepat dalam aspek kelajuan pemprosesan imej dan tidak boleh digunakan untuk imej dalam scenario masa nyata. Teknik tradisional kriptografi seperti DES tidak sesuai digunakan kepada imej kerana ciri-ciri imej seperti kapasiti data, pertindihan dan korelasi yang tinggi antara piksel.

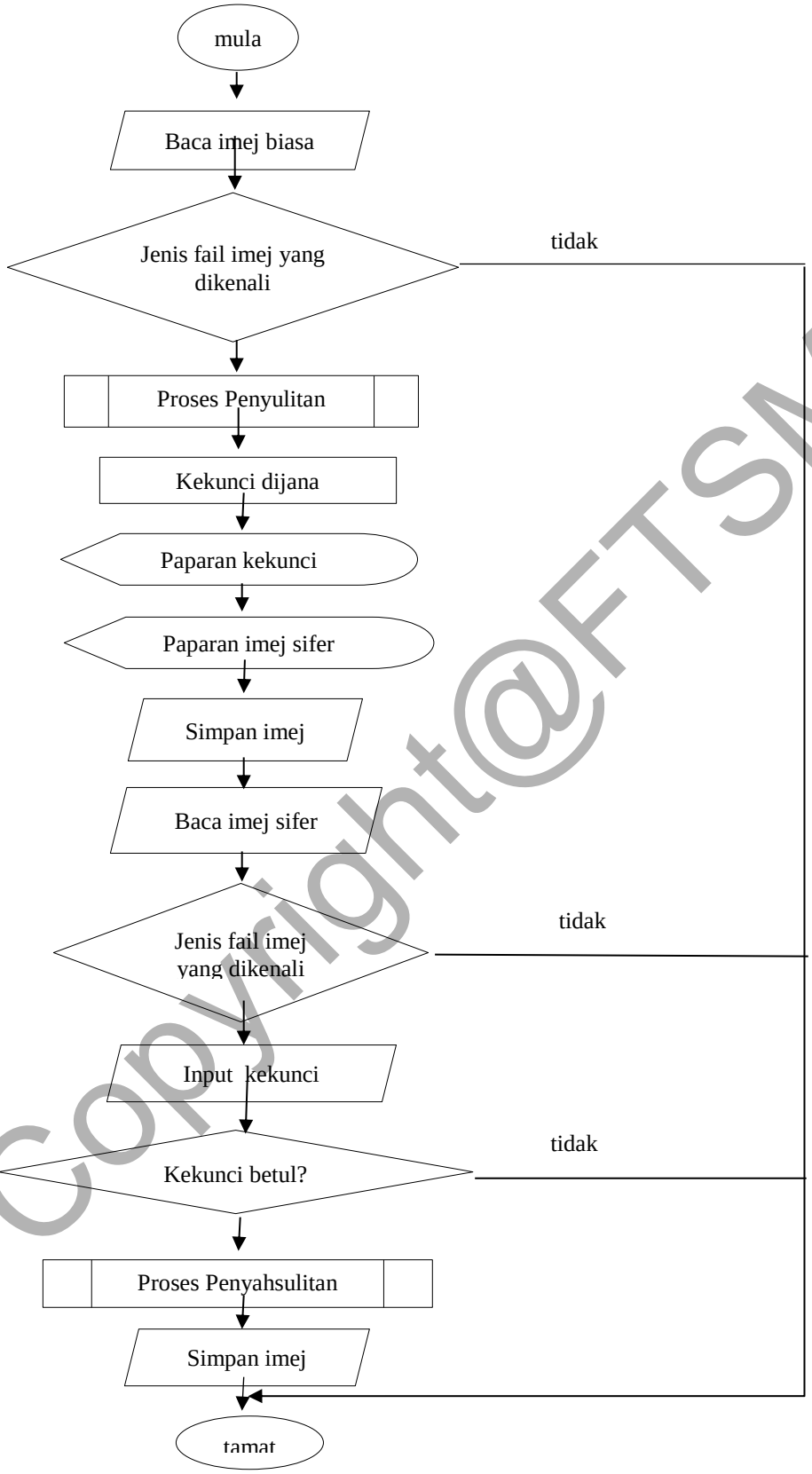
Aplikasi yang memproses imej lebih cepat adalah lebih baik. Aplikasi ini adalah terbaik dilaksanakan atas fail berdimensi kecil. Namun begitu, kelajuan pemprosesan imej adalah berbeza mengikut algoritma. Aspek kelajuan ini perlu diberi perhatian kerana imej-imej yang akan disulitkan atau dinyahsulitkan mempunyai nilai yang tinggi terutama dari aspek keselamatan. Jika aplikasi lambat berfungsi boleh menyebabkan data-data mudah diambil oleh pihak ketiga.

3 OBJEKTIF KAJIAN

Berdasarkan penyataan masalah yang dinyatakan sebelum ini, objektif yang telah dikenalpasti bagi membangunkan sistem ini adalah membangunkan Algoritma AES yang dapat menyulit dan menyahsulit gambar.

4 METOD KAJIAN

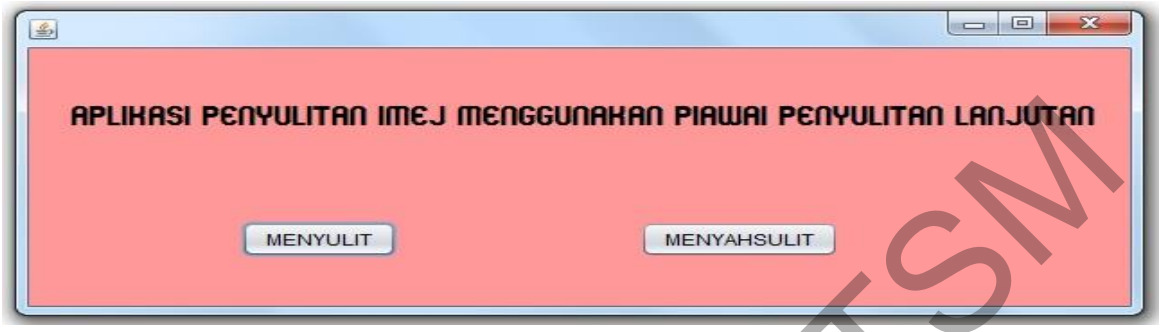
Aplikasi Penyulitan Imej menggunakan Piawai Penyulitan Lanjutan dibangun berdasarkan metodologi yang dikenali sebagai Kitar Hayat Model Tokokan (*Incremental Development*). Model ini ialah metod di dalam pembangunan perisian di mana produk direka bentuk, diimplemen dan diuji secara berperingkat berdasarkan kepada pembentukan fasa-fasa. Setiap fasa ini mempunyai perancangan kerja yang tertentu untuk membolehkan pembangunan projek ini dapat dijalankan dengan teratur dan terancang. Model ini boleh digunakan apabila keperluan untuk sistem yang lengkap telah sepenuhnya dikenalpasti. Semasa aplikasi ini dibangunkan, pembangun sistem boleh mengkaji semula sistem. Jika sistem mempunyai sebarang masalah, sistem perlu dibaiki dan diubahsuai mengikut keperluan. Jika tidak, pembangun boleh meneruskan pembangunan sistem sehingga selesai. Rajah 1 menunjukkan proses yang dilalui oleh fail imej untuk penyulitan dan penyahsulitan



Rajah 1 Prosess penyulitan dan penyahsulitan untuk fail imej

5 HASIL KAJIAN

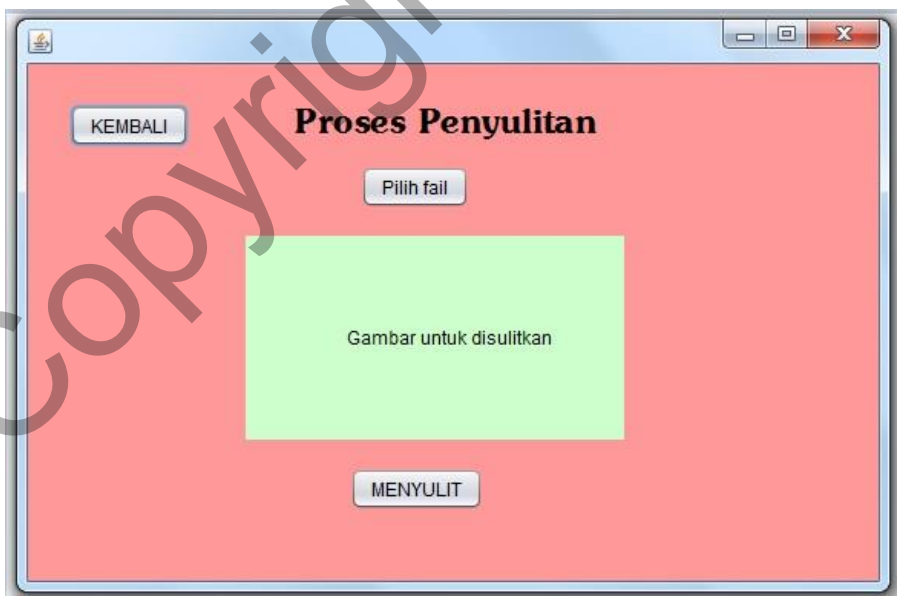
Aplikasi Penyulitan Imej menggunakan Piawai Penyulitan Lanjutan ini merupakan aplikasi untuk menyulit dan menyahsulit imej. Rajah 2 merupakan antara muka menu utama di mana terdapat dua pilihan fungsi iaitu menyulit dan menyahsulit.



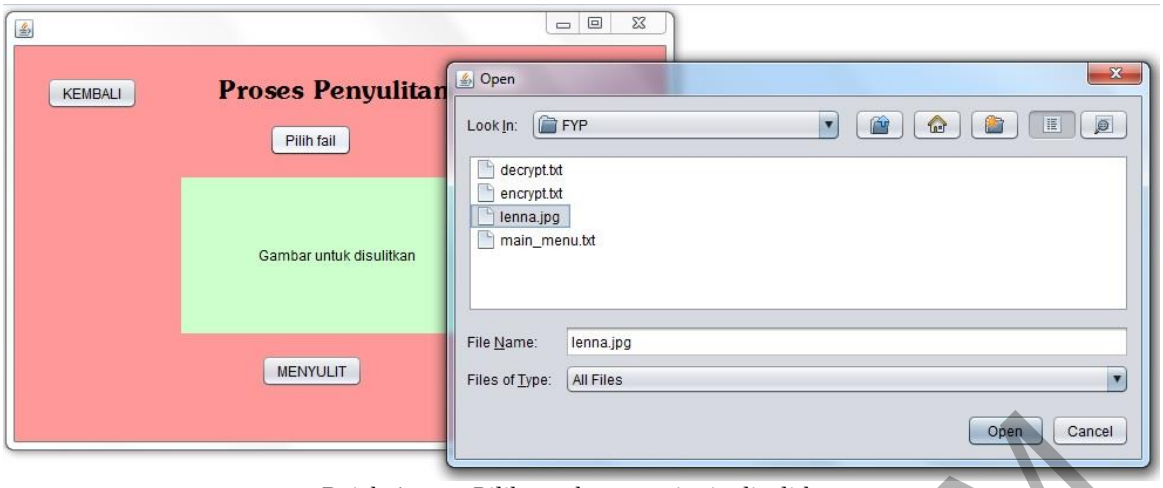
Rajah 2 Antara muka menu utama sistem

Rajah 3 adalah antara muka untuk butang menyulit. Berikut adalah langkah yang perlu diikuti bagi fungsi menyulit.

i. Pilih fail gambar yang ingin disulitkan.
ii. Gambar tersebut akan dipaparkan pada ruang gambar untuk disulitkan
iii. Tekan butang menyulit



Rajah 3 Antara muka bagi fungsi menyulit



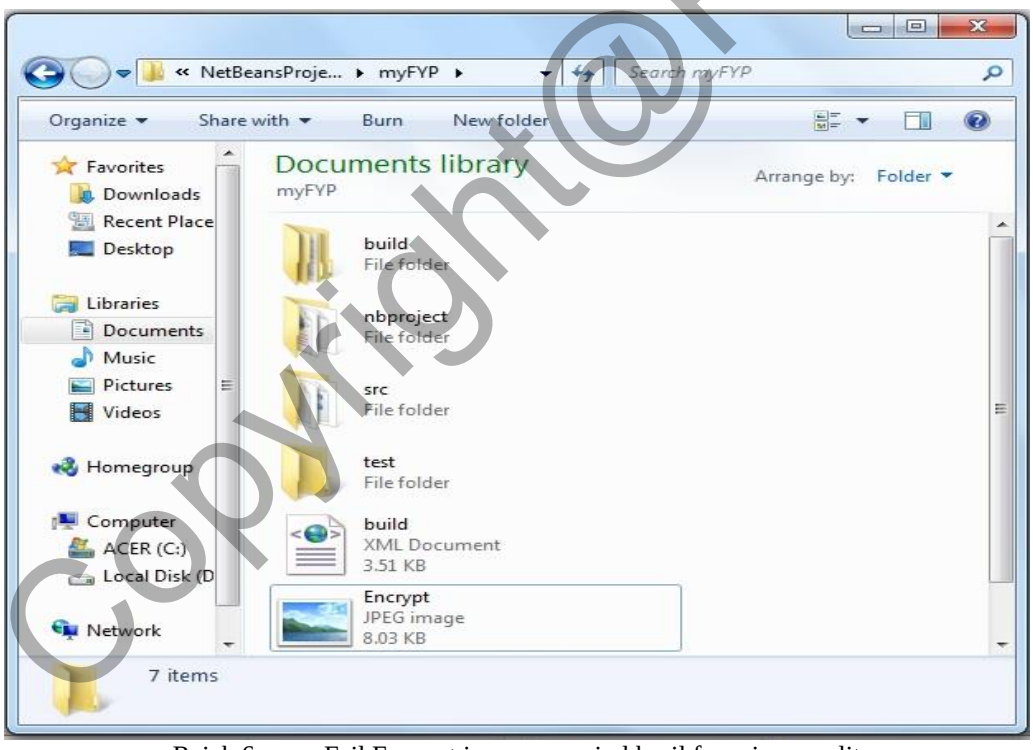
Rajah 4 Pilih gambar yang ingin disulitkan

Rajah 4 menunjukkan bagaimana sesebuah fail imej itu dipilih. Berdasarkan rajah tersebut, gambar yang dipilih adalan lenna.jpg di dalam fail FYP. Gambar tersebut akan dipaparkan di ruang gambar untuk disulitkan seperti dalam rajah 5.4.

Rajah 5 Antara muka selepas imej dipilih

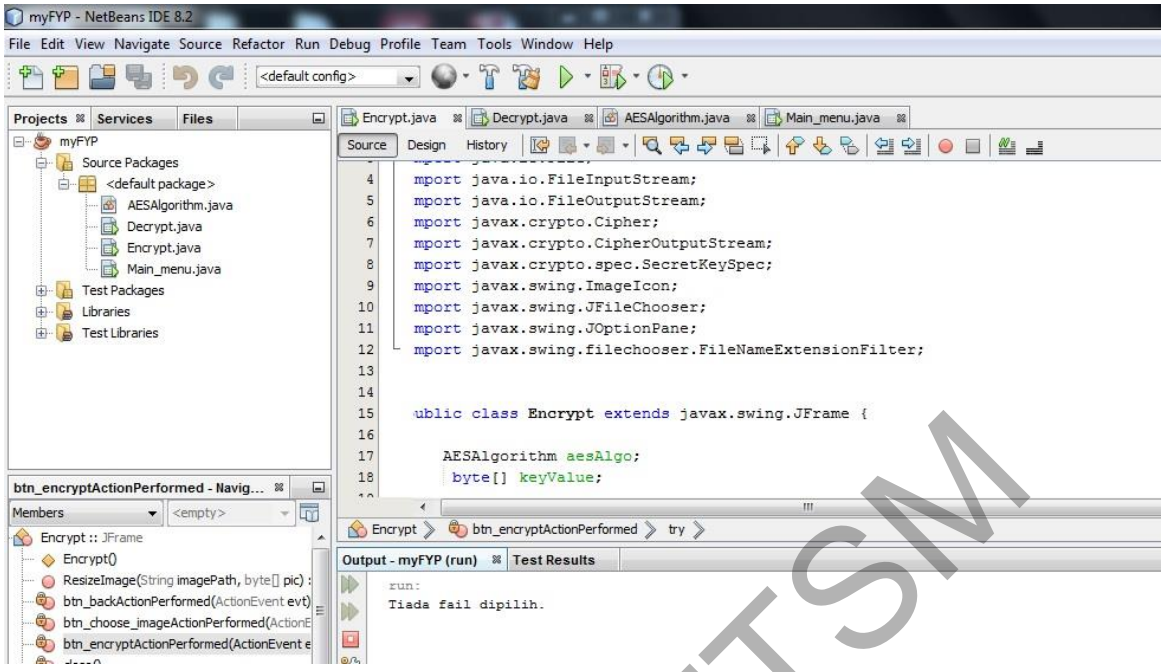
Rajah 5 Mesej yang akan muncul selepas menekan butang menyulit

Apabila butang menyulit ditekan, mesej akan muncul untuk sebagai pemberitahuan bahawa penyulitan telah berjaya. Gambaran sebenar adalah seperti dalam rajah 5.

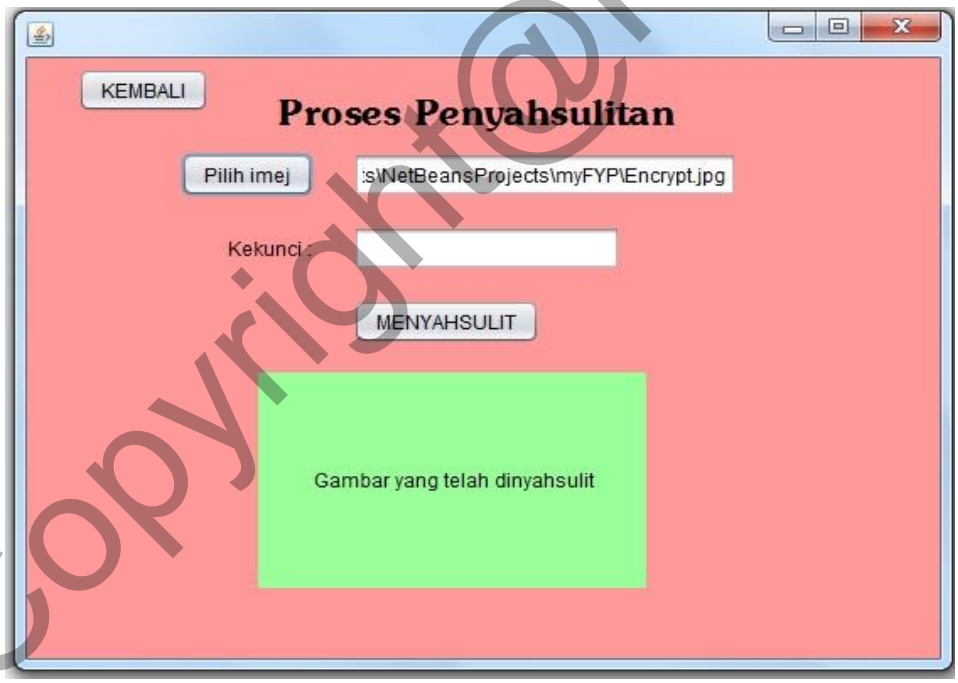


Rajah 6 Fail Encrypt.jpg yang wujud hasil fungsi menyulit

Fungsi butang menyulit adalah untuk menyulitkan gambar yang dipilih. Gambar tersebut akan muncul dalam fail Netbeans Project. Seperti dalam rajah 6, gambar yang telah dihasilkan selepas proses menyulit ialah gambar kosong. Rajah 7 menunjukkan keadaan sistem apabila tiada fail imej yang dipilih dalam proses menyulit.



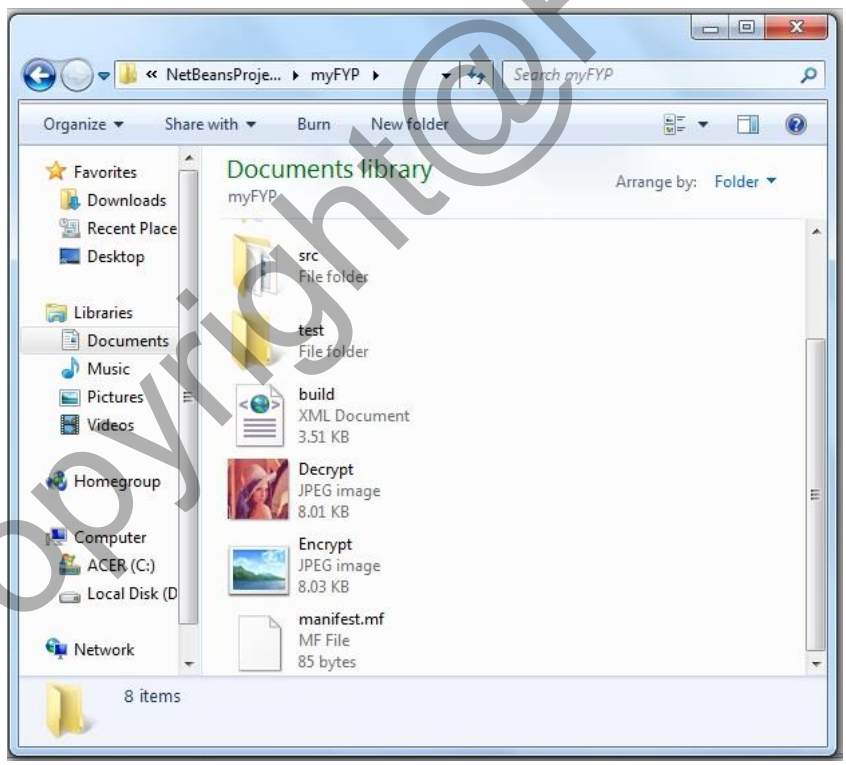
Rajah 7 Keadaan apabila tiada fail gambar yang dipilih untuk proses menyulit



Rajah 8 Antara muka bagi fungsi penyahsulitan

Rajah 8 adalah antara muka bagi proses penyahsulitan. Fail imej Encrypt.jpg yang telah dihasilkan sewaktu menyulit akan dipilih. Apabila butang menyahsulit ditekan, gambar yang telah dinyahsulit akan dipaparkan pada ruangan yang dilabelkan seperti dalam rajah 9.

Rajah 9 Antara muka apabila proses penyahsulitan berjaya



Rajah 10 Fail Decrypt.jpg yang wujud hasil fungsi menyahsulit

Rajah 10 adalah gambar tetingkap yang menunjukkan proses penyahsulitan berjaya di mana fail Decrypt.jpg dapat dihasilkan. Proses ini menunjukkan fungsi menyahsulit imej akan memberikan imej yang sama seperti imej asal.

6 KESIMPULAN

Melindungi data terutamanya data imej masih lagi sesuatu yang kurang diberi perhatian. Selaras dengan teknologi yang semakin berkembang kini, akan terdapat banyak aplikasi melanggar privasi pengguna. Oleh itu, penyulitan dan penyahsulitan imej perlu dilengkapi dengan aplikasi terkini selaras dengan keperluan semasa. Melalui aplikasi yang telah dibangunkan dapat memberi manfaat kepada orang yang mementingkan keselamatan dalam penghantaran imej. Diharapkan ia dapat memberi kepuasan dari aspek keselamatan seterusnya gambar yang penting dapat dipindahkan dengan selamat.

7 RUJUKAN

Devi, Aarti., Sharma, Ankush., Rangra, Anamika., 2015. A Review on DES, AES and Blowfish for Image Encryption & Decryption. *International Journal of Computer Science and Information Technologies* 6(3): 3034.