

BAB IV

HASIL DAN PEMBAHASAN

IV.1. Tampilan Hasil

Tampilan hasil merupakan tahapan enkripsi gambar asli yang dienkripsi dengan tidak menyerupai hasil gambar setelah melakukan analisis dan perancangan sistem aplikasi enkripsi file gambar dengan algoritma triple DES pada siklus rekayasa perangkat lunak dimana aplikasi siap dioperasikan pada keadaan yang sebenarnya sehingga dari sini akan dapat diketahui apakah aplikasi atau sistem yang telah dibuat benar-benar dapat menghasilkan output atau keluaran atau keluaran yang sudah sesuai dengan tujuan yang diinginkan. dapat dilihat sebagai berikut :

1. Tampilan *Form* Selamat Datang

Tampilan *form* selamat datang untuk memulai sistem citraDES menggunakan algoritma triple DES terlihat pada gambar IV.1 berikut :



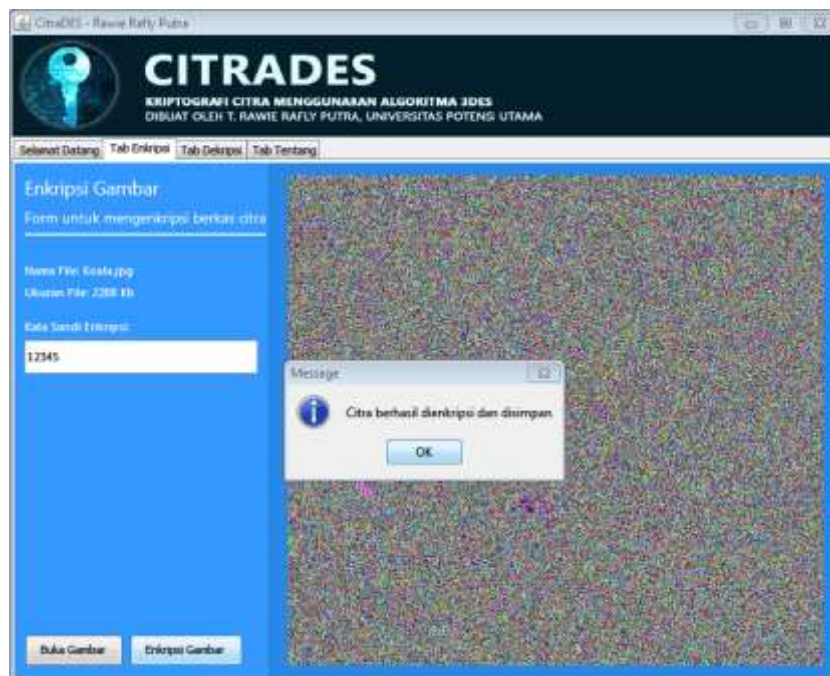
Gambar IV.1. Tampilan *Form* Selamat Datang

Keterangan :

Dari keterangan form selamat datang pada aplikasi meunjukkan fomr menu utama sistem yang dibuat sistem ini bertujuan untuk mengetahui aplikasi

2. Tampilan *Form* Tab Enkripsi

Tampilan form pada sistem untuk melakukan pengolahan Tab Enkripsi dapat terlihat seperti pada gambar IV.2 berikut :



Gambar IV.2. Tampilan *Form* Tab Enkripsi

Keterangan :

Form tab enkripsi ini bertujuan untuk melakukan enkripsi file gambar yang asli berubah menjadi hitam putih pada gambar yang asli, setelah file dibuka kemudian masukan kata sandi enkripsi. Bertujuan untuk keamanan setelah mau di enkripsi kemudian tekan bottom enkripsi gambar.

3. Tampilan *Form* Tab Dekripsi

Tampilan form pada sistem untuk melakukan pengolahan Tab Dekripsi dapat terlihat seperti pada gambar IV.3 berikut :



Gambar IV.3. Tampilan *Form* Tab Dekripsi

Keterangan :

form tab dekripsi bertujuan untuk mengembalikan file gambar menjadi semula. Cara melakukannya buka file gambar pada bottom buka gambar, kemudian pilih gambar yang terenkripsi, masukan katasandi yang sama dengan enkripsi lalu tekan bottom dekripsi pada aplikasi.

4. Tampilan *Form* Menu Tentang

Tampilan menu tentang yang dirancang untuk melakukan melihat aplikasi sistem terlihat seperti pada gambar IV.4 berikut :



Gambar.IV.4. Tampilan *Form* Menu Tentang

Keterangan :

Form tentang ini bertujuan mengetahui siapa yang buat aplikasi ini dan program ini. Dan menceritakan tentang triple DES

IV.2. Pembahasan

Sistem yang dibangun adalah perancangan aplikasi enkripsi file gambar dengan algoritma Triple DES. Sistem ini dibangun untuk menyelesaikan enkripsi file gambar menjadi buram dan DESkripsi gambar buram menjadi gambar semula, Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu yang digunakan untuk mengembangkan aplikasi yaitu *Java* enkripsi.

IV.2.1. Hasil Perhitungan

3DES (Triple Data Encryption Standard) merupakan suatu algoritma pengembangan dari algoritma DES (Data Encryption Standard). Pada dasarnya algoritma yang digunakan sama, hanya pada 3DES dikembangkan dengan melakukan enkripsi dengan implementasi algoritma DES sebanyak tiga kali.

3DES memiliki tiga buah kunci yang berukuran 64-bit

Input bits: 01001000 01000101 01001100 01001111 01001000 01000001
01001100 01001111

Key A bits: 00010010 00110100 01010110 01111000 00010010 00110100
01010110 01111000

Key B bits: 00010010 00110100 01010110 01111000 00010010 00110100
01010110 01111000

Enkripsi Tahap Pertama

CD[0]: 00000000 0110011 0010101 0101111 0101010 1011001 1010001
0001111

CD[1]: 00000000 1100110 0101010 1011110 1010101 0110011 0100010
0011110

KS[1]: 000100 000000 001011 101110 111101 000011 100001 010010

CD[2]: 00000001 1001100 1010101 0111100 0101010 1100110 1000100
0111101

KS[2]: 011100 001010 111011 010000 110110 111000 000111 000101

CD[3]: 0000110 0110010 1010101 1110000 0101011 0011010 0010001
1110101

KS[3]: 010101 001111 110000 000010 110000 101100 011110 001001

CD[4]: 0011001 1001010 1010111 1000000 0101100 1101000 1000111
1010101

KS[4]: 011000 101010 010101 010110 010110 100011 011100 001101

CD[5]: 1100110 0101010 1011110 0000000 0110011 0100010 0011110
1010101

KS[5]: 011011 001100 010000 000111 111110 100101 000110 101000

CD[6]: 0011001 0101010 1111000 0000011 1001101 0001000 1111010
1010101

KS[6]: 011000 111000 000100 111010 010000 000111 101100 101011

CD[7]: 1100101 0101011 1100000 0001100 0110100 0100011 1101010
1010110

KS[7]: 101011 001000 000010 110011 111101 100011 100000 111000

CD[8]: 0010101 0101111 0000000 0110011 1010001 0001111 0101010
1011001

KS[8]: 101101 110000 101000 011010 111000 010001 101101 111010
 CD[9]: 0101010 1011110 0000000 1100110 0100010 0011110 1010101
 0110011
 KS[9]: 001000 000101 101111 001011 110011 111100 011110 000000
 CD[10]: 0101010 1111000 0000011 0011001 0001000 1111010 1010101
 1001101
 KS[10]: 001100 010111 000101 000101 100110 000100 011101 001101
 CD[11]: 0101011 1100000 0001100 1100101 0100011 1101010 1010110
 0110100
 KS[11]: 000000 010100 110111 010001 110110 101101 001010 000100
 CD[12]: 0101111 0000000 0110011 0010101 0001111 0101010 1011001
 1010001
 KS[12]: 010101 010110 000110 110101 110100 000110 011110 101001
 CD[13]: 0111100 0000001 1001100 1010101 0111101 0101010 1100110
 1000100
 KS[13]: 100101 111000 010110 000001 101110 100011 101000 001001
 CD[14]: 1110000 0000110 0110010 1010101 1110101 0101011 0011010
 0010001
 KS[14]: 010110 110000 001010 100111 111100 100111 001100 110010
 CD[15]: 1000000 0011001 1001010 1010111 1010101 0101100 1101000
 1000111
 KS[15]: 101110 011001 000010 001100 001101 010010 101100 101010
 CD[16]: 0000000 0110011 0010101 0101111 0101010 1011001 1010001
 0001111
 KS[16]: 110000 010011 110010 001010 000001 100100 011111 010101

Ronde 12

E : 101001 011001 011010 101100 001101 010100 000110 101010
 KS : 010101 010110 000110 110101 110100 000110 011110 101001
 E xor KS: 111100 001111 011100 011001 111001 010010 011000 000011
 Sbox: 0101 1110 0010 0001 1010 1101 0101 1111
 P : 11011011 00011010 10101000 10111110
 L[i]: 01001100 11010110 01101010 00110101
 R[i]: 01111100 00011111 11111110 11010110

Ronde 13

E : 001111 111000 000011 111111 111111 111101 011010 101100
 KS : 100101 111000 010110 000001 101110 100011 101000 001001
 E xor KS: 101010 000000 010101 111110 010001 011110 110010 100101
 Sbox: 0110 1111 0101 0100 0101 1011 1111 1110
 P : 01111110 00111111 11110110 00110001
 L[i]: 01111100 00011111 11111110 11010110
 R[i]: 00110010 11101001 10011100 00000100

Ronde 14

E : 000110 100101 011101 010011 110011 111000 000000 001000
 KS : 010110 110000 001010 100111 111100 100111 001100 110010

E xor KS: 010000 010101 010111 110100 001111 011111 001100 111010
 Sbox: 0011 0001 1110 0011 0001 1000 1000 0011
 P : 10110000 01000011 01001011 00000111
 L[i]: 00110010 11101001 10011100 00000100
 R[i]: 11001100 01011100 10110101 11010001
 Ronde 15
 E : 111001 011000 001011 111001 010110 101011 111010 100011
 KS : 101110 011001 000010 001100 001101 010010 101100 101010
 E xor KS: 010111 000001 001001 110101 011011 111001 010110 001001
 Sbox: 1011 0011 0011 0101 1001 0110 0111 1010
 P : 11101111 10110010 01010110 00001110
 L[i]: 11001100 01011100 10110101 11010001
 R[i]: 11011101 01011011 11001010 00001010
 Ronde 16
 E : 011011 111010 101011 110111 111001 010100 000001 010101
 KS : 110000 010011 110010 001010 000001 100100 011111 010101
 E xor KS: 101011 101001 011001 111101 111000 110000 011110 000000
 Sbox: 1001 0011 1100 0010 0110 0111 0001 1101
 P : 01001010 11100101 01101001 10101010
 L[i]: 11011101 01011011 11001010 00001010
 R[i]: 10000110 10111001 11011100 01111011
 LR[16] 10000110 10111001 11011100 01111011 11011101 01011011 11001010
 00001010

 Output Bit Terenkripsi: 10110001 01101011 11000100 10111111 10110101
 00010001 10101101 11011100

IV.2.1. Uji Coba Program

Uji coba sistem dilakukan ketika pembuatan aplikasi telah selesai dan memastikan bahwa program dapat berjalan dengan baik sesuai dengan rancangan awal. Instrumen yang digunakan untuk melakukan pengujian ini yaitu dengan menggunakan:

1. Satu unit laptop atau PC dengan spesifikasi sebagai berikut:
 - a. Processor Intel Core I3
 - b. Memory 4 Gb
 - c. Hardisk 500 Gb

2. Perangkat Lunak dengan spesifikasi sebagai berikut:

- a. Java
- b. iReport

3. Pengujian Program

- a. Sistem keamanan

IV.2.2. Metode *Black Box*

Pengujian dengan menggunakan metode *Black Box* testing merupakan tahap pengujian yang memfokuskan kepada persyaratan fungsional perangkat lunak. *Test Case* ini bertujuan untuk menunjukkan fungsi perangkat lunak tentang cara beroprasinya. Hasil pengujian sistem ini merupakan suatu hasil yang menunjukkan keakuratan dari sebuah sistem.

IV.2.1. Skenario Pengujian

1. Pengujian Tab Enkripsi

Tabel IV.2. Pengujian Blackbox Tab Enkripsi

Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Buka Gambar	Memunculkan Folder file gambar yang mau dienkripsi	Gambar akan masuk ke box fie gambar	[√] diterima [] ditolak
Masukan Katasandi	Kata sandi ini untuk keamanan yang akan didekripsi	Katasandi ini harus sama dengan kata sandi enkripsi	[√] diterima [] ditolak
Enkripsi gambar	Gambar akan berubah menjadi tidak terlihat atau buram	Gambar yang berubah akan masuk pada folder gambar	

1. Pengujian Tab Enkripsi

Tabel IV.2. Pengujian Blackbox Tab Enkripsi

Data Masukan	Yang Diharapkan	Pengamatan	Kesimpulan
Buka Gambar	Memunculkan Folder file gambar yang mau didekripsi	Gambar akan masuk ke box fie gambar	[√] diterima [] ditolak
Masukan Katasandi	Kata sandi ini untuk keamanan yang akan didekripsi	Katasandi ini harus sama dengan kata sandi enkripsi	[√] diterima [] ditolak
Dekripsi gambar	Gambar akan berubah menjadi gambar semula	Gambar yang berubah akan masuk pada folder gambar	[√] diterima [] ditolak

IV.3. Kelebihan dan Kekurangan Sistem

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

IV.3.1. Kelebihan Sistem

1. Kelebihan.

- a. Membuat gambar mengecilkan size file gambar dan ukuran gambar
- b. Gambar yang dihasilkan tersimpan di dalam folde img pada program

2. Kekurangan.

- a. Gambar yang dienkrpsi dua kali lalu didekripsi menjadi original tidak bias lagi
- b. Aplikasi tidak menggunakan database untuk minyimpan gambar yang dienkrpsi.