PENGAMANAN DATA DENGAN METODE ADVANCED ENCRYPTION STANDARD DAN METODE LEAST SIGNIFICANT BIT

Adetya Krisna Prastyo

Jurusan Teknik Informatika-S1, Fakultas Ilmu Komputer,
Universitas Dian Nuswantoro Semarang
Jln. Nakula I no 5-17 Semarang 50131 INDONESIA
111201005272@mhs.dinus.ac.id

Penggunaan komputer dalam berbagai bidang membawa perkembangan yang pesat pada sebuah perangkat keras ataupun lunak, bahkan dalam bidang informasi perkembangan terus berlanjut dan ini memberikan pengruh besar terhadap kehidupan manusia. Contoh adalah jaringan internet yang memungkinkan pengguna untuk saling tukar file maupun data, bahkan dalam rasio besar antar perusahaan sering menggunakan fasilitas jaringan internet untuk melakukan transfer file ke perusahan lain. Dengan adanya kemajauan telekomunikasi dan komputer juga memungkinkan pengguna melakukan penyimpanan data secara digital. Dalam hal ini masalah keamanan dan kerahasian data adalah suatu hal yang sangat penting, maka harus ada perlindungan terhadap data yang dirahasiakan. Sebuah teknik dalam ilmu kriptografi merupakan salah satu cara yang dapat mengamankan data dari ganguan orang lain. Kriptografi merupakan seni dalam mengamankan pesan menjadi suatu pesan yang tidak dikenali. Rijndael atau dikenal juga Advance Encryption Standard (AES) merupakan salah algoritma enkripsi kriptografi yang digunakan. Namun dengan menggunakan satu metode masih dapat menimbulkan suatu kecurigaan, untuk melengakapi agar data tersembunyi dengan aman dan tidak menimbulkan kecurigaan. Penggunaan steganografi least significant bit (LSB) menjadi salah satu pilihin yang tepat. Least significant bit merupakan suatu metode untuk menyisipkan potongan sebuah informasi rahasia dalam suatu objek media lain seperti pada image atau jpg. Metode ini tidak menimbulkan perubahan yang besar terhadap gambar yang digunakan secara kasat mata.
Kata kunci : advance encryption standard, least significant bit.

The use of computers in various fields to bring rapid development to a hardware or software, even in the field of information and the continued development of this gives great pengruh to human life. Examples are internet network that allows users to exchange files and data, even in the large ratio between companies often use the internet facility to transfer files to other companies. With the kemajauan telecommunications and computer also allows users to store the data digitally. In this case the problem of security and confidentiality of data is a very important thing, then there must be protection for confidential data. A technique within the science of cryptography is one way that can secure data from disturbance of others. Cryptography is the art of securing the message into a message that is not recognized. Also known as Rijndael Advanced Encryption Standard (AES) is a cryptographic encryption algorithm used. However, by using the method can still give rise to a suspicion, for melengakapi to hidden data safely and not to arouse suspicion. The use of steganography the least significant bit (LSB) to be one pilihin right. Least significant bit is a method to insert a piece of confidential information in an object other media such as image or jpg. This method does not cause major changes to the images that are used by naked eye.
Keywords : advance encryption standard, least significant bit.

I. PENDAHULUAN

Penggunaan komputer dalam berbagai bidang membawa perkembangan yang pesat pada sebuah perangkat keras ataupun lunak, bahkan dalam bidang informasi perkembangan terus berlanjut dan ini memberikan pengruh besar terhadap kehidupan manusia. Contoh adalah jaringan internet yang memungkinkan pengguna untuk saling tukar file maupun data, bahkan dalam rasio besar antar perusahaan sering menggunakan fasilitas jaringan internet untuk melakukan transfer file ke perusahan lain. Dengan adanya kemajauan telekomunikasi dan komputer juga memungkinkan pengguna melakukan penyimpanan data secara digital.

Kegiatan penyimpana data secara digital juga mempunyai banyak resiko , sama halnya dengan aktivitas di jaringan internet tentang keamanan komunikasi melalui internet. Hal ini jelas terlihat apabila dalam aktivitas tersebut terdapat informasi atau data yang peniting maupun bersifat rahasia dapat diakses oleh orang lain yang tidak berkepentingan, dikarenakan dalam kejahatan teknologi komunikasi dan informasi juga ikut berkembang, seperti halnya yang sering kita dengar adalah hacker dan cracker. Saat ini masalah keamanan pada komputer menjadi isu penting [1].

Dalam media penyimpanan leptop, hardisk eksternal, maupun sky drive. Tentang keamanan data pada leptop atau hardisk eksternal, yang sering dibawa memungkinkan hilang ataupun dicuri, bila hal ini terjadi hal yang dipikirkan awal adalah data-data yang terdapat pada memory penyimpanan walaupun data tersebut sudah memiliki back-up namun data dan file penting itu menjadi sebuah pemikiran utama, terlebih data yang tersimpan bersifat rahasia atau private.

Dalam hal ini perlindungan data dapat di lakukan dengan menggunakan sebuah algoritma keamanan data yang sering digunakan adalah kriptografi dan steganografi. Dua algoritma tersebut memiliki sebuah keuunggulan dalam hal pengamanan data.

Seiring dengan perkembangan jaman yang terus menerus terutama pada bidang teknologi informasi walaupun. Steganografi sering di kaitkan dengan kriptografi namun kedua metode ini sangatlah tidak sama dan berbeda [4].

Algoritma kriptografi adalah agoritma yang dapat melakukan sebuah pengamanan pada file yang akan di lindungi. Dalam algoritma ini data yang akan dilindungi akan disandikan , guna melindungi kerahasiaan dari data itu sendiri. Dalam algoritma ini file nantinya akan di enkripsi sehingga bentuk file nantinya tidak dapat dibuka seperti sebelum di enkripsi, penggunaan algoritma kriptografi saat ini sangatlah banyak salah satu contohnya adalah aes rijndael .

Dengan di kombinasikannya algoritma kriptografi dengan steganografi akan meningkatkan kualitas keamanan data. Penggunaan algoritma steganografi ini banyak menggunakan format digital yang dijadikan sebuah media penyembunyian. Pada dasranya steganografi adalah ilmu dan seni menyembunyikan pesan rahasia. Steganografi metode EoF(End of File) menggunakan cara dengan menyisipkan data, file hasil enkripsi dari steganografi ini tidak mengalami perubahan signifikan dari segi visual dalam kasat mata.[2]

Dari penjabaran diatas penulis bermaksud untuk mengimplementasikan kedua metode kriptografi dan steganografi pada file yang nantinya menjadi target keamanan.

II. METODE YANG DI USULKAN

2.1 Tinjauan Studi

Basuki Rakhmat dan Muhammad Fairuzabadi, M.kom, "*Steganografi menggunakan metode Least Significant Bit (LSB) dengan kombinasi Algoritma Kriptografi Vignere dan RC4*", mengintegrasikan kriptografi dan steganografi dalam sebuah sistem aplikasi.Pesan teks terlindungi dengan algoritma kriptografi dan tersembunyi dalam sebuah gambar.

Mahmuddin Yunus dan Agus Harjoko, "Penyembunyian Data pada File video menggunakan metode LSB dan DCT", mengkombinasikan metode Least Significant Bit (LSB) dan DCT untuk penyembunyian data pada file video.

Adira, "Analisis dan perancangan aplikasi Steganografi pada citra digital menggunakan metode LSB (Least Significant Bit).

Sugeng Murdowo, "Mengenal Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advance Encryption Standard(Aes) Rijdnael", eknik ekripsi dalam ilmu kriptografi merupakan salah satu cara yang dapat mengamankan data dari ganguan orang lain. Kriptografi merupakan seni dalam mengamankan pesan menjadi suatu pesan yang tidak dikenali.Rijndael atau dikenal juga Advance Encryption Standard (AES) merupakan salah algoritma kriptografi yang digunakan.

Berbagai peneltian yang dilakukan terdahulu, hasil yang menunjukan berbagai hasil yang didapat tentang penerapan metode MD5 dan Least Significant Bit (LSB).

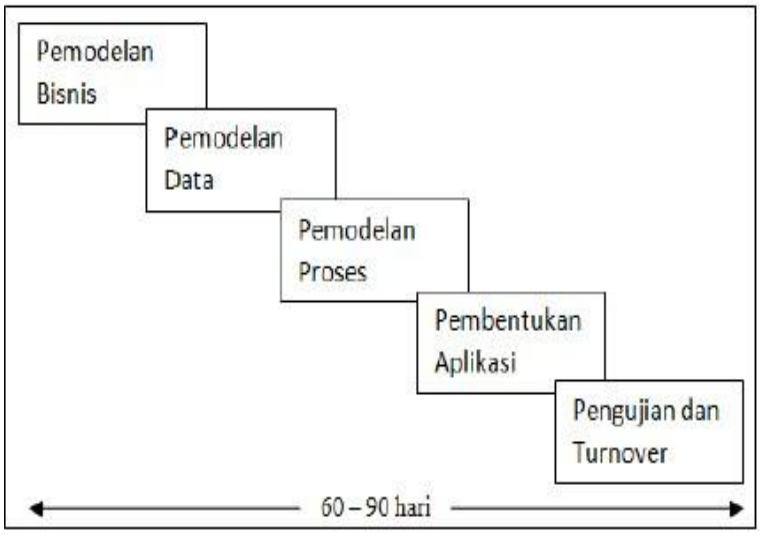
3.1 Metode Pengumpulan Data

Data yang didkumpulkan dalam penelitian ini merupakan data sekunder. Data yang diperoleh dari sumber-sumber literatur dan dokumen penelitian yang yang terkait seperti buku-buku, dan jurnal penelitian.

3.2 Metode Pengembangan Sistem

RAD adalah sebuah metode pengembangan sistem yang menekankan kecepatan pengembangan melalui keterlibatan pengguna ekstensif dalam konstruksi serangkaian prototype yang cepat, berulang, dan konstruksi inkremental yang pada akhirnya berkembang ke dalam sistem final. [Hariz Setyawan, Diana Puspitasari, Wiwik Budiawan,"Perancangan Sistem Informasi Peramalan Kebutuhan Dan Ketersediaan Bahan Baku Batik Dengan Metode Rapid Application Development (RAD)"]

3.3 Fase-fase Pengembangan Sistem



Gambar 3.1 : Fase-fase RAD

III. IMPLEMENTASI

4.1 Analisis Kebutuhan Aplikasi

Tujuan dari proses analisa kebutuhan aplikasi adalah untuk mengetahui sifat dari kebutuhan sistem sehingga mempermudah dalam perancangan. Tujuan lain dari analisa ini adalah untuk mendokumentasikan sifat program tersebut. Proses analisis meliputi analisis kebutuhan perangkat lunak dan perangkat keras, termasuk analisis terhadap kebutuhan sistem. Kebutuhan-kebutuhan tersebut adalah :

a. Spesifikasi kebutuhan perangkat lunak
    1. Software perangakat lunak Visual Basic 2008
       Bahasa pemprograman yang digunakan untuk perancangan system aplikasi adalah Microsoft Visual Basic 2008, dikarenakan bahasa ini merupakan bahasa mudah dipelajari dan memiliki beberapa implementasi bahas seperti seperti C#, C++, dan mudah dalam perhitungan aritmatika dan logika yang dibutuhkan dalam pembuatan aplikasi.
    2. Software Microsoft Word 2013
       Software ini digunakan dalam penelitian untuk mendukung aplikasi sebagai salah satu fasilitas dalam penyimpanan hasil enkripsi dan dekripsi data.
    3. OS windows 7
       Sistem operasi yang digunakan adalah windows 7, karena system opersi ini memeiliki kemudahan dalam pengoperasian dan juga banyak program yang konfert dengan OS ini.
    4. Balsamiq Mockups
       Kebutuhan akan pembuatan gambar rancangan model aplikasi.

b. Spesifikasi kebutuhan perangkat keras
    1. Prosesor minimal Duel core 1.80 GHz.
    2. Disk space 10GB.
    3. Ram 2GB.
    4. Layar 14’

4.2 Prosedur pembuatan aplikasi

Langkah - langkah pembuatan aplikasi dalam penelitian ini adalah sebagai berikut :

a. Mengumpulkan materi –materi yang dibutuhkan.
b. Melakukan pembatasan terhadap materi tersebut.
c. Mempersiapkan dan melakukan instalasi perangkat keras.
d. Mempersiapkan dan melakukan instalasi perangkat lunak sesuai
e. dengan spesifikasi kebutuhan.

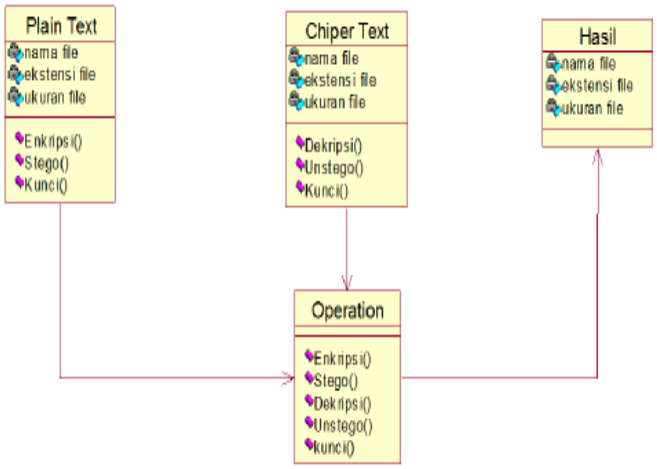
4.3 Pemodelan Bisnis

Dalam bahasa pemodelan ini, penulis menggunakan 2 (dua) buah aktor yaitu pengirim dan penerima sebagai urutannya meliputi :

a. Informasi yang mengendalikan
   Dalam tahap ini informasi di pegang penuh oleh peihak pengirim, yang nantinya akan di ubah kedalam bentuk format baru menggunakan aplikasi Advanced Encryption Standard dan dilanjutkan ke dalam proses penyisipan pesan dengan media gambar.
b. Informasi yang muncul
   Pihak penerima akan mendapatkan file berupa gambar, yang berekstensi “PNG”.
c. Pihak yang memunculkan
   Untuk tahap pemulihan file, dilakukan oleh pihak ke dua yaitu sipenerima yang akan melakukan Unstego dan deskripsi data.
d. Tujuan informasi
   Untuk melindungi data dari orang yang tidak memiliki hak untuk mengetahuinya. Meyakinkan bahwa data hanya dapat digunakan oleh sipenerima yang telah ditentukan
e. Pelaku pemroses
   Pihak pengirim dan penerima adalah 2 aktor yang menjadi pemroses data tersebut.

4.4 Unit Pemodelan Data

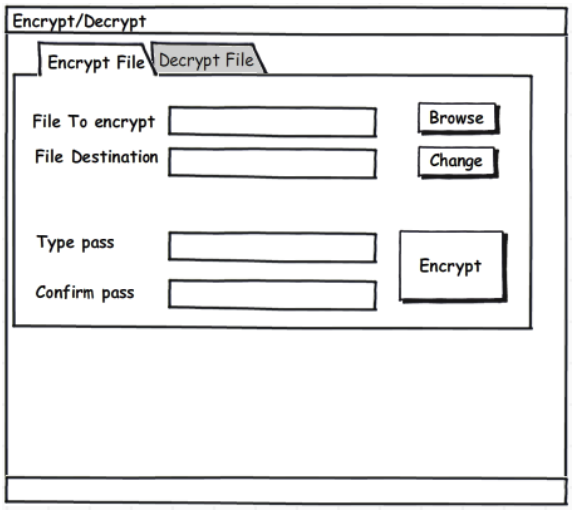
Pada Unit Pemodelan DATA penulis menggunakan class diagram, penulis menggunakan 4 macam kelas yaitu kelas plain text, chiper text, operation dan hasil. Kelas-kelas tersebut saling berhubungan dan mempunyai keterkaitan



Gambar 4.1 Class diagram DATA

4.5 Proses Input Output

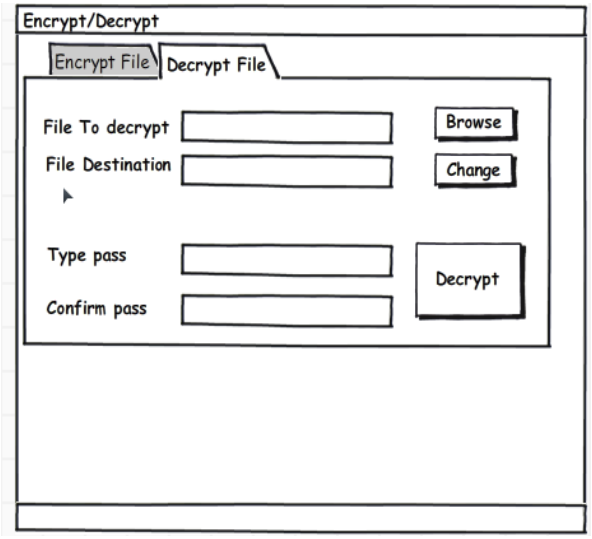
Dalam pembuatan pada aplikasi yang penulis buat menggunakan perangkat lunak berupa Visual Basic 6.0. Di bawah ini merupakan desain input output yang telah di buat adalah sebagai berikut :



Gambar 4.2 Mockups encrypt

Pada gambar Mocups di atas, terdapat gambaran dari rancangan aplikasi. Submenu – submenu dalam menu Encrypt di atas antara lain :

a. Sub menu Browse
   Dalam sub menu ini memberikan perintah untuk melakukan input file yang akan di encrypt.
b. Sub menu Change
   Sub menu ini berfungsi untuk mengganti file yang salah dalam penginputan file, atau ingin mengganti file yang akan di encrypt.
c. Encrypt
   Perintah eksekusi.



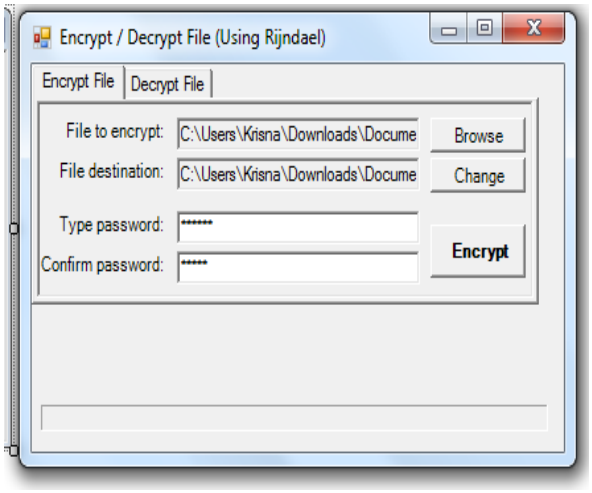
Gambar 4.3 Mockups decrypt

Pada gambar Mocups di atas, terdapat gambaran dari rancangan aplikasi. Submenu – submenu dalam menu Encrypt di atas antara lain :

a. Sub menu Browse
   Dalam sub menu ini memberikan perintah untuk melakukan input file yang akan di decrypt.
b. Sub menu Change
   Sub menu ini berfungsi untuk mengganti file yang salah dalam penginputan file, atau ingin mengganti file yang akan di decrypt.
c. Decrypt
   Perintah eksekusi.

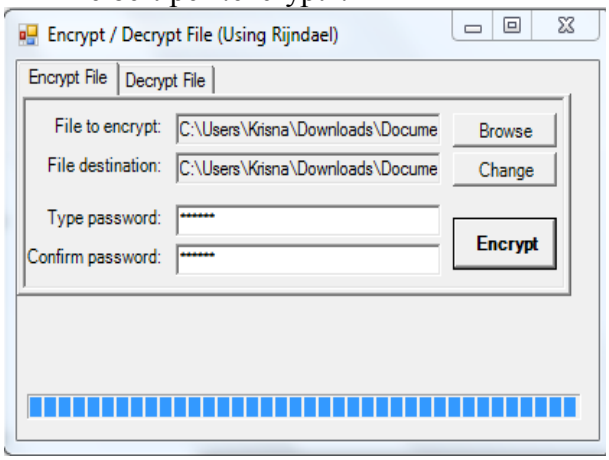
4.6 Implementasi

Penulis melakukan percobaan terhadap program advanced encryption standard (*AES*), salah satu diantara nya adalah :

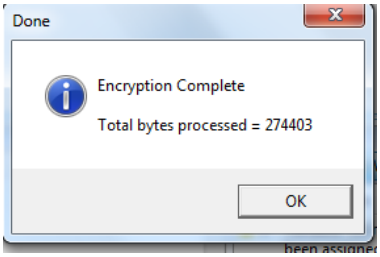


Gambar 4.9 file yang akan di encrypt

Pada gambar diatas penulis mencoba unuk mengencrypt file pada partisi "C" dan dalam tahap ini file akan menjadi sebuah *plaintext* dan pemberian password akan masuk dalam katagori *around key*. File yang telah di encrypt akan berubah menjadi file bertipe ".encrypt".



Gambar 4.10 proses encrypt



Gambar 4.11 pesan file telah di encrypt

Dua proses gambar diatas adalah hasil akhir dari tahap pengencryptsian file, yang di akhiri dengan tamilan pesan "*encryption complete*". Setelah terdapat tampilan pesan seperti pada gambar di atas lakukan klik ok untuk segera mengakhiri proses encryption. Untuk melakukan deskripsi agar file bisa dibuka akan dilakukan proses selanjutnya.

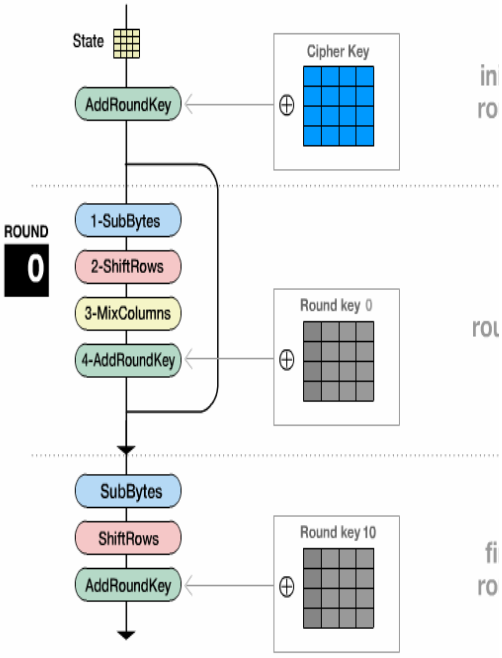
Setelah selesai dengan model enkripsi data selanjutnya proses melakukan penyembunyian file ke dalam sebuah image dengan menggunakan Least Significant Bit (LSB), salah satu diantaranya adalah :

Gambar 4.16 tampilan awal LSB

Pada gambar diatas terdapat 2 radio button dimana radio button pertama adalah intruksi untuk melakukan penyembunyian file atau enkripsi, sedangkan untuk radio button yang ke dua adalah intruksi untuk melakukan pengambilan data dari gambar atau deskripsi *image.*

IV. HASIL & PEMBAHASAN

4.9 Algoritma AES



Gambar 4.4 urutan enkripsi

A. AddRoundKey
Add Round Key pada dasarnya adalah mengkombinasikan chiper teks yang sudah ada dengan chiper key yang chiper key dengan hubungan XOR.

B. Subbytes
Proses SubBytes () memetakan setiap byte dari array State dengan menggunakan tabel substitusi S-Box. Tidak seperti Des S-box berbeda pada setiap putaran, AES hanya mempunyai satu buah S-Box.

C. SiftRows
Proses ShiftRows() ini adalah proses yang sangat sederhana. Pada ShiftRows() melakukan pergeseran wrapping (sikklik) pada 3 baris terakhir dari array state. Jumlah pergeseran bergantung nilai baris (r). Baris r = 1 digeser sejauh 1 byte, baris r = 2 digeser 2 byte, dan baris r = 3 digeser sejauh 3 byte. Baris r = 0 tidak digeser.

D. MixColums
Transformasi menggunakan MixColumns() adalah proses ketiga dalam satu Ronde enkripsi AES

Tabel 4.3 Bilangan Polynominal

02	01	01	03
03	02	01	01
01	03	02	01
01	01	02	03

Tahap berikutnya akan di lakukan perkalian mixcolumns terhadap hasil akhir dari proses shiftrows

4.10 Algoritma LSB

Bit atau binary digit adalah unit dasar penyimpanan data di dalam komputer, nilai bit suatu data adalah 0 atau 1. Semua data yang ada pada komputer disimpan ke dalam satuan bit ini, termasuk gambar, suara, ataupun video. Jenis-jenis format pewarnaan di dalam media gambar. Semakin besar wadah*(cover-image)* yang digunakan untuk penyembunyian pesan maka semakin besar atau banyak pula jumlah karakter yang dapat disembunyikan dan semakin besar teks yang disembunyikan di dalam citra, semakin besar pula kemungkinan teks tersebut rusak akibat manipulasi pada citra penampung.Rumus untuk menghitung jumlah maksimal karakter yang dapat disisipkan ke gambar :

$$\text{Max} = \frac{lebar\ gambat\ x\ panjang\ gambar}{8\ \text{bit karakter}} = \frac{200 \text{ x } 200}{8} =$$

5000 char

4.11 Analisa Percobaan

Penulis melakukan tahap pengujian pada aplikasi, dalam pengujian ini penulis menggunakan beberapa file bertipe pdf yang akan digunakan untuk pengujian.

Table 4.8 pengujian enkripsi *AES*

Nama berkas	Size In (KB)	Keterangan
13-37-1-PB.pdf	6.441	Berhasil
69-105-1-PB.pdf	1.415	berhasil
77-229-1-PB.pdf	190	Berhasil
lsb1.pdf	358	Berhasil
lsb4.pdf	3.122	Berhasil

Setelah pengujian terhadap aplikasi enkripsi Advanced Encryption Standard sebanyak 5 file semua berhasil di enkripsi.

Table 4.9 pengujin enkripsi *LSB*

Gambar	File	keterangan	File korup
IMG_2553	13-37-1-PB.pdf	Berhasil	TIDAK
IMG_2558	69-105-1-PB.pdf	berhasil	TIDAK
IMG_2559	77-229-1-PB.pdf	Berhasil	TIDAK
IMG_2575	lsb1.pdf	Berhasil	TIDAK
IMG_2576	lsb4.pdf	Berhasil	TIDAK

Setelah pengujian terhadap aplikasi enkripsi Least Significant Bit sebanyak 5 file gambar dan dokumen semua berhasil dan file tidak korup.

Tabel 4.12 Pengujian editing gambar

Gambar Stego	Jenis editan	File korup
Gambar 1	Crop	Korup
Gambar 2	Menambah kontras	Korup
Gambar 3	Mengurangi kontras	Korup
Gambar 4	Sisip 1 objek baru	Tidak Korup
Gambar 5	Sisip 2 objek baru	Tidak Korup

Penulis melakukan pengujian 5 kali jenis editing gambar, membuktikan bahwa metode least significant bit tidak tahan terhadap editing gambar namun pada least significant bit hanya tahan terhadap penyisipan objek baru.

V. PENUTUP

5.1 KESIMPULAN

Dari hasil perancangan dan pembuatan program aplikasi kriptografi dengan Algoritma Advanced Encryption Standard (AES) dan Steganografi dengan metode Least Sifnificant Bit (LSB) ini, dapat diambil kesimpulan sebagai berikut :

1. Dari hasil yang telah dilakukan membuktikan bahwa aplikasi dapat melindungi file dengan membuatnya tidak dapat dibuka secara normal walaupun membuka dengan open with.
2. Hasil percobaan selanjutnya dengan menyisipkan file kedalam gambar tidak merusak kualitas gambar secara signifikan.
3. File dapat terlindungi dengan aman dan tidak rusak, dengan catatan tidak dilakukan cropping, penambahan kontras, dan pengurangan kontras.

5.2 SARAN

Saran-saran yang berguna pengembangan sistem dan aplikasi ini adalah sebagai berikut :

1. Dalam penyisipan pesan disesuaikan dengan kapasitas file gambar yang digunakan.
2. Aplikasi pengamanan data data ini dapat diimplementasikan di

instansi yang memeiliki beberapa dokumen yang harus dijaga.

3. Aplikasi ini masih terpisah akan lebih praktis apabila menjadi 1.
4. Aplikasi kriptografi dan stegonografi ini masih banyak dalam bentuk aplikasi berbasis desktop, akan lebih baik apabila berbasis mobile.

REFERENSI

[1] Nathasia,N. D. , & Wicaksono, A. E. (2011). Penggunaan teknik kriptografi Stream Cipher untuk pengaman basis data. *Jurnal basis data, ICT Research Center UNAS, 6(1), 1-22*

[2]Cahyono,Ari.Dwi."IMPLEMENTASI STEGANOGRAFI MENGGUNAKAN METODE END OF FILE (EOF) DALAM PENGAMANAN DATA (Studi kasus pada file AVI, MP3, dan JPEG)".

http://karya-ilmiah.um.ac.id/index.php/matematika/article/view/30525

[3] D. Ariyus, Keamanan Multimedia , Yogyakarta: ANDI, 2009

[4] Prastyo. Fahri Perdana. (2010). Steganografi menggunakan metode LSB dengan software Matlab, Jakarta , *UIN.*

[5] Z. Hendrikus. , Wirawan, Setia. (2012). Implementasi Steganografi pada Berkas Audio WAV untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding. *E-journal teknologi industry*, Gunadarma.

[6] Nurhayati, Dwi, Oky, ST, MT (2010). Keamanan Multimedia. Universitas Diponegoro.

[7] Aditya, y. , Pratama, A. , & Nurlifa, A. (2010). Studi Pustaka Untuk Steganografi dengan beberapa metode. *Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010),2010, 32-15*

[8] Basuki, Kurni, Dwi., S.Si., M.kom. , & Maulana, M. , Ahmad. , & N. , Uzzin, Isbat. , S.kom.(2009) *Data Hiding Steganograph Pada File Image Menggunakan Metode Least Significant Bit.* Industrial Electronic Seminar. , ITS Surabaya.

[9] Adira. (2010). Analisis dan Perancangan Aplikasi Steganografi pada Citra Digital Menggunakan Metode *Least Significant Bit (LSB).* UIN.

[10] Murdowo. , Sugeng. (2010). Mengenal proses perhitungan Enkripsi menggunakan algoritma Kriptografi Advance Encryption Standard (AES). AMIK JTC Semarang