REKAYASA PERANCANGAN PENYEMBUNYIAN PESAN FILE DAN TEXT DENGAN METODE ENKRIPSI DES DAN ENKRIPSI RC4

Asih Rohmani[1], Sasono Wibowo[2]
[1,2]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11, Semarang, 50131, (024) 3517261
E-mail : aseharsoyo@dsn.dinus.ac.id[1], sasono_skd@yahoo.com[2]

Abstrak

Keamanan suatu informasi merupakan hal yang sangat penting disamping kecepatan, kemudahan dan efisiensi. Steganography adalah salah satu cara dalam memberikan keamanan yang maksimal dalam proses pengiriman informasi dengan cara menyembunyikan suatu pesan atau data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Teknik steganography umum digunakan bersamaan dengan menggunakan dua media yang berbeda, dimana salah satunya berfungsi sebagai media yang berisikan informasi cover file (carrier file) dan yang lain berfungsi sebagai media pembawa informasi tersebut (secret file). Pengamanan text rahasia yang akan disisip kedalam cover file (carier file) yaitu dengan 2 enkripsi yang berbeda yaitu dengan algoritma RC4 yang digunakan untuk mengacak plain text dan algoritma DES untuk mengacak bit file text.

Kata Kunci : *Steganografi, Enkripsi DES, Enkripsi RC4.*

Abstrak

An information security is a very important thing besides the speed, ease and efficiency. Steganography is one way to provide maximum security in the process of information delivery by way of hiding a secret message or data in the data or other message that appears does not contain anything, except for people who understand the key. Steganography techniques commonly used in conjunction with the use of two different media, where one of them serves as a media cover contains information files (the carrier file) and the other one serves as a carrier of information media (the secret files). Security text secrets that will inserted into the cover file (carier files) with 2 different encryption with RC4 algorithm used to randomize the plain text and the DES algorithm to randomize the bit text file.

Keywords: *Steganography Encryption, DES, RC4 Encryption.*

1. PENDAHULUAN

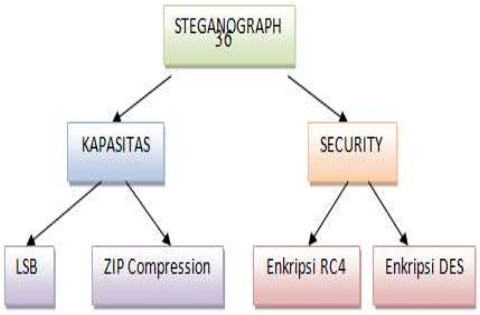
Keamanan suatu informasi pada jaman global ini makin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut tentang aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Dimana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya [1][2][3].

Steganografi merupakan cara untuk menyembunyikan suatu pesan atau data rahasia di dalam data atau pesan lain yang tampak tidak mengandung apa-apa, kecuali bagi orang yang mengerti kuncinya. Teknik steganografi umum digunakan bersamaan dengan menggunakan dua media yang berbeda, dimana salah satunya berfungsi sebagai media yang berisikan informasi cover file (*carrier file*) dan yang lain berfungsi sebagai

media pembawa informasi tersebut (*secret file*) [4].

Aplikasi Steganografi yang sekarang ini ada masih mengandalkan satu enkripsi saja sehingga hanya ada satu perlindungan password saja atau bahkan tampa password. Dan jarang yang menggunaka zip compression pada pesan yang akan disisipkan sehingga apabila pesan yang disisipkan itu banyak atau besar maka media pembawa informasi akan mengalami perbedaan yang besar pula dengan aslinya, sehingga ini akan membuat mudah diketahui oleh pihak yang tidak berkepentingan.

Steganografi yang digabung dengan algoritma *zip compression* diharapkan bisa membuat data teks lebih kecil sehingga mudah disisipkan ke media file pembawanya (*secret file*), sekaligus bias mengecoh orang lain kalau tidak ada file rahasia didalam media file tersebut. Dan untuk menambah keamanan data, maka data yang akan disisipkan sudah diacak dengan menggunakan algoritma enkripsi DES yang jarang digunakan untuk system keamanan karena dianggap kuno dan kurang aman. Karena jarang digunakan inilah yang menjadi kelebihan kriptografi ini. Untuk itulah algoritma enkripsi RC4 digunakan untuk menyempurnakan enkripsi pada *secret text* yang apabila enkripsi DES sudah terbuka maka text tersebut tidak bisa dibaca karena sebelumnya text sudah teracak dengan kunci tertentu sehingga pesan rahasia akan sangat aman karena mengalami 2 proses enkripsi yang berbeda.

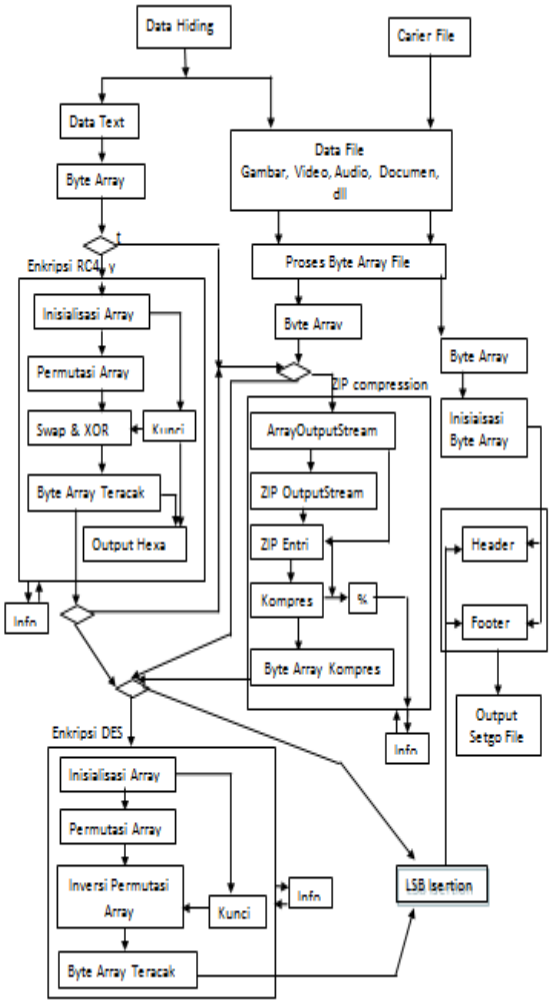


Gambar 1. Skema Komponen Program Steganograph

2. METODE PENELITIAN

2.1. Tahap Encoding Data

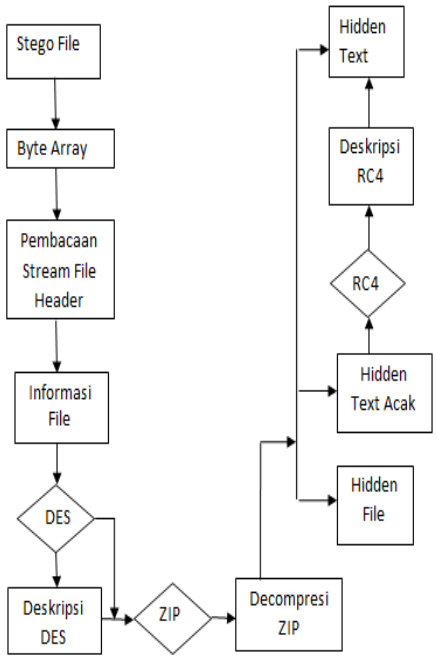
Berikut adalah bagan skema rancangan dari diagram alir Encode Data [5]:



Gambar 2. Diagram Alir Encode Data

2.2. Tahap Decoding Data

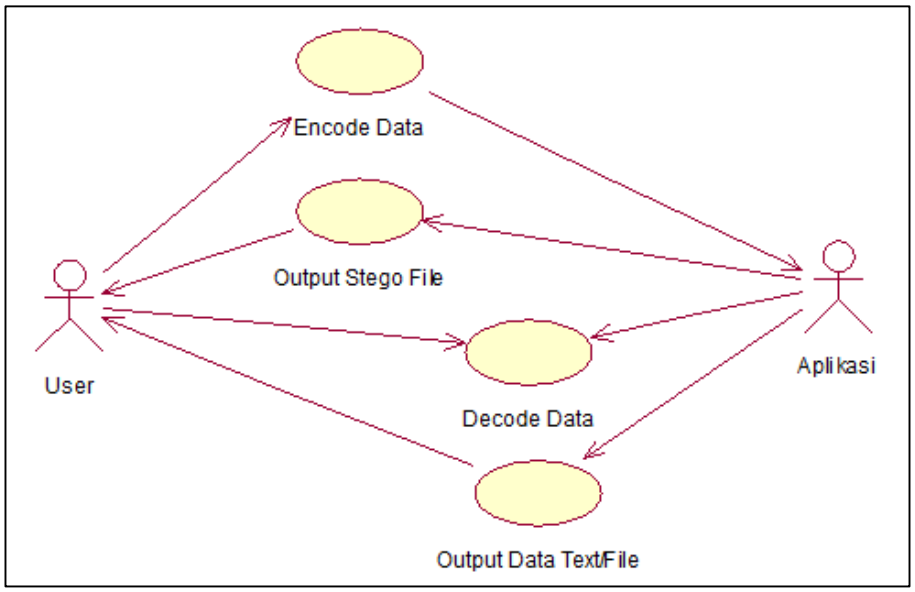
Tahap decoding data merupakan tahap pengungkapan atau decoding suatu data dari stego image yang bertujuan untuk mengambil kembali data yang telah disisipkan. Dengan telah dilakukannya beberapa modifikasi pada tahap encoding data menggunakan metode LSB, maka secara otomatis juga akan dilakukan penyesuaian Pada tahap decoding [6].



Gambar 3. Diagram Alir Decode Data

3. HASIL DAN PEMBAHASAN

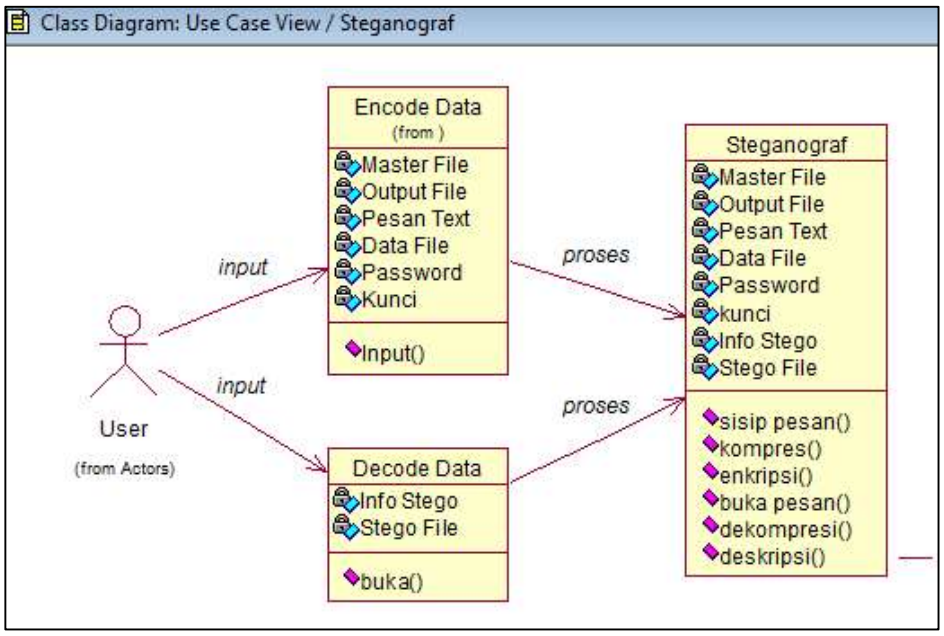
3.1. Use Case Diagram



Gambar 4. Use Case Diagram

Proses utama yang dilakukan ada dua yaitu proses encode data untuk penyembunyian dan keamanan pesan, proses output stego file untuk menerima hasil dari penyisipan pesan, proses decode data yaitu untuk membuka atau mengurai pesan, dan proses output data teks atau file untuk melihat hasil data yang disembunyikan.

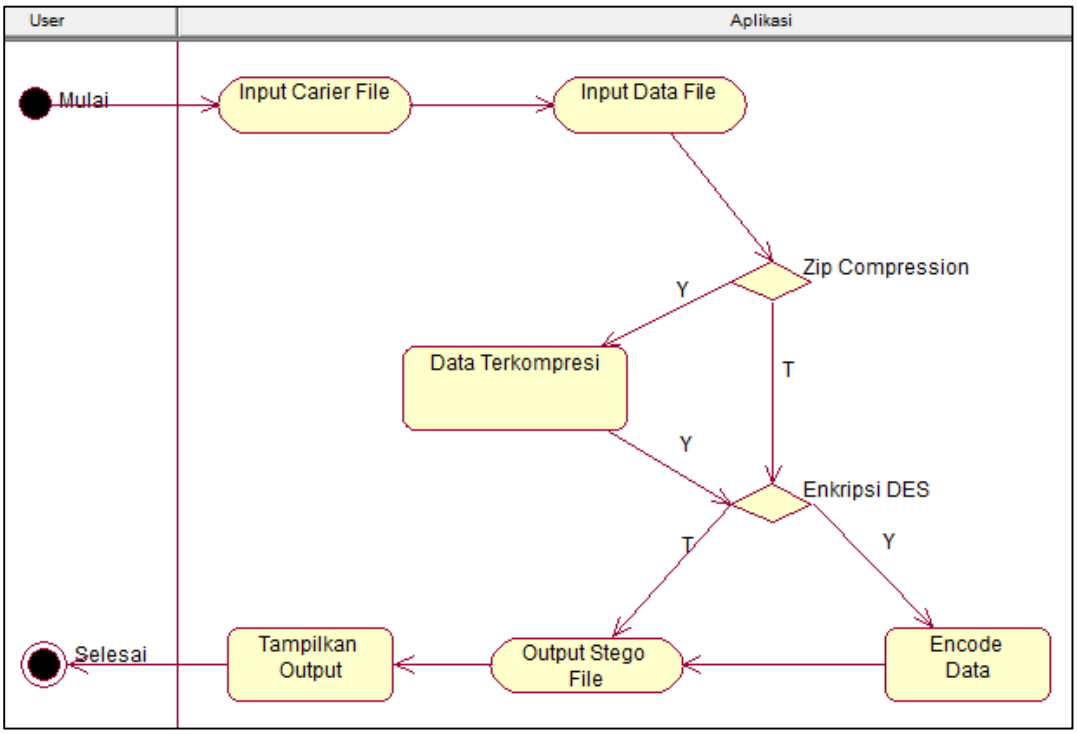
3.2 Class Diagram [7]



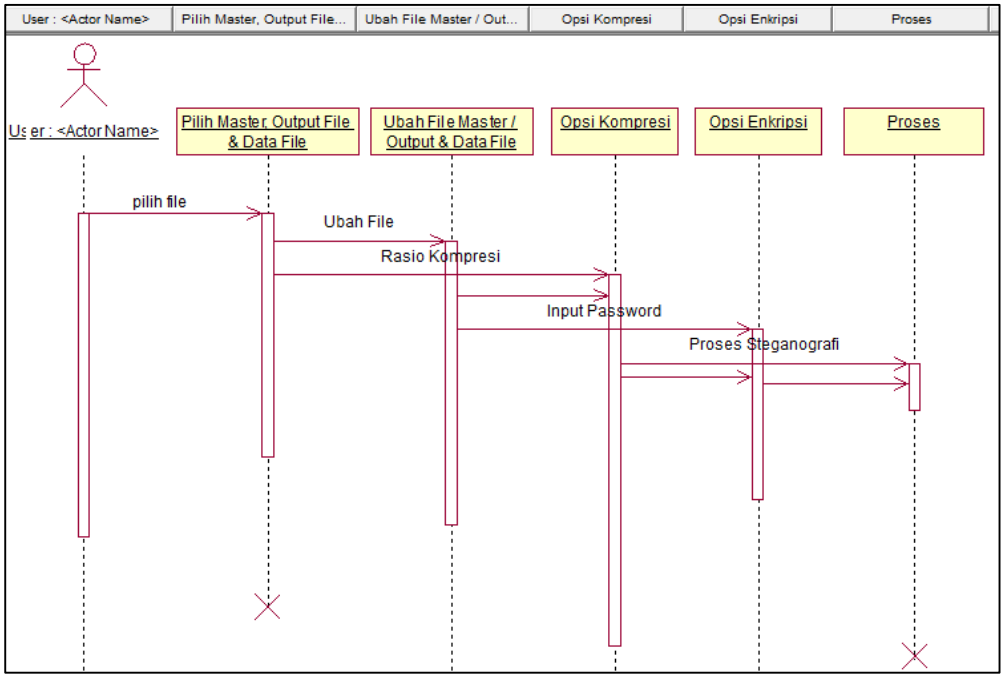
Gambar 5. Class Diagram

3.3. Proses Encode Data Text / File

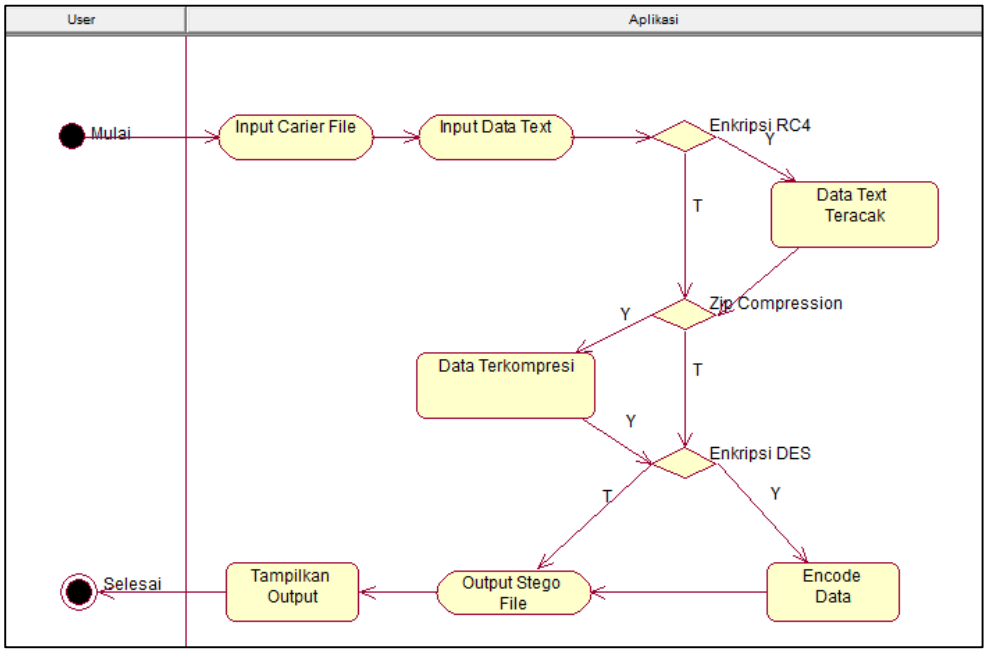
Proses ini berlangsung saat user ingin melakukan *encoding* (menyembunyikan) data text atau file ke dalam suatu media [8].



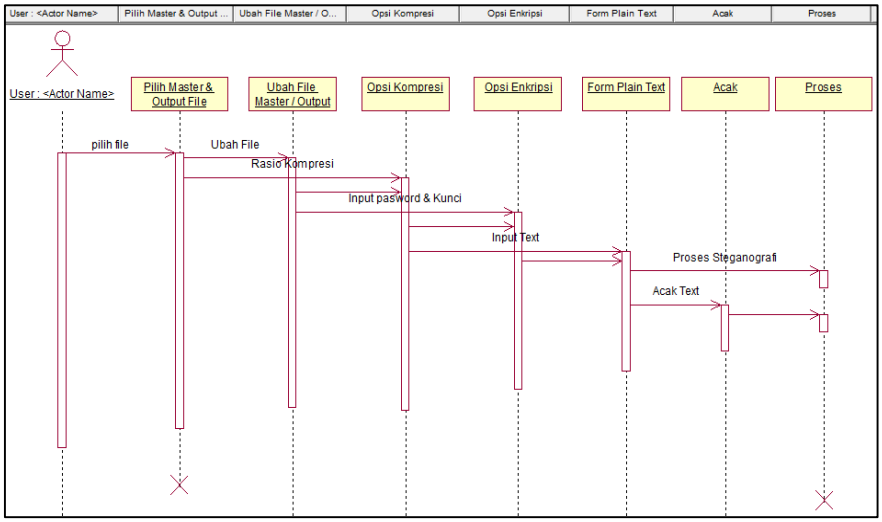
Gambar 6. Activity Diagram Encode Data File



Gambar 7. Sequence Diagram Encode Data File



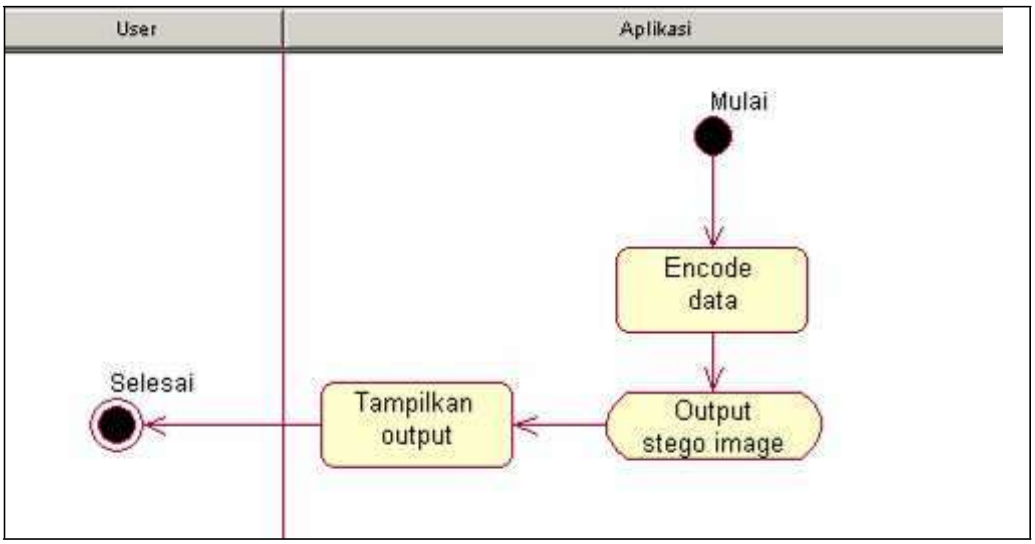
Gambar 8. Activity Diagram Encode Data Text



Gambar 9. Sequence Diagram Data Text

3.4. Proses Output Stego File

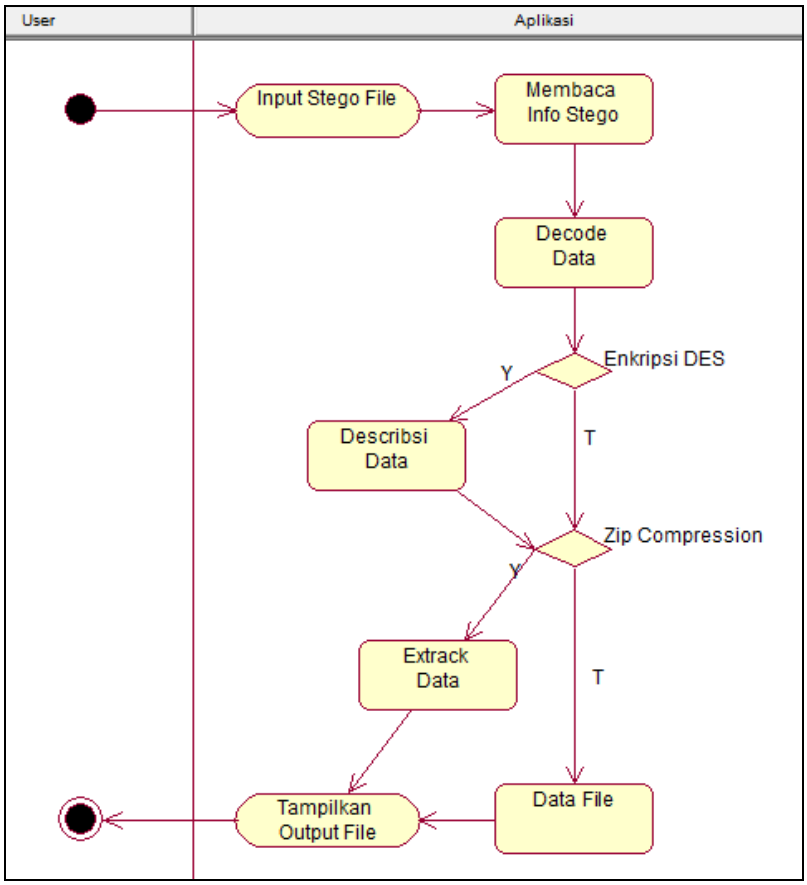
Dari proses *encoding* data, diperoleh hasil output file berupa stego *file*.



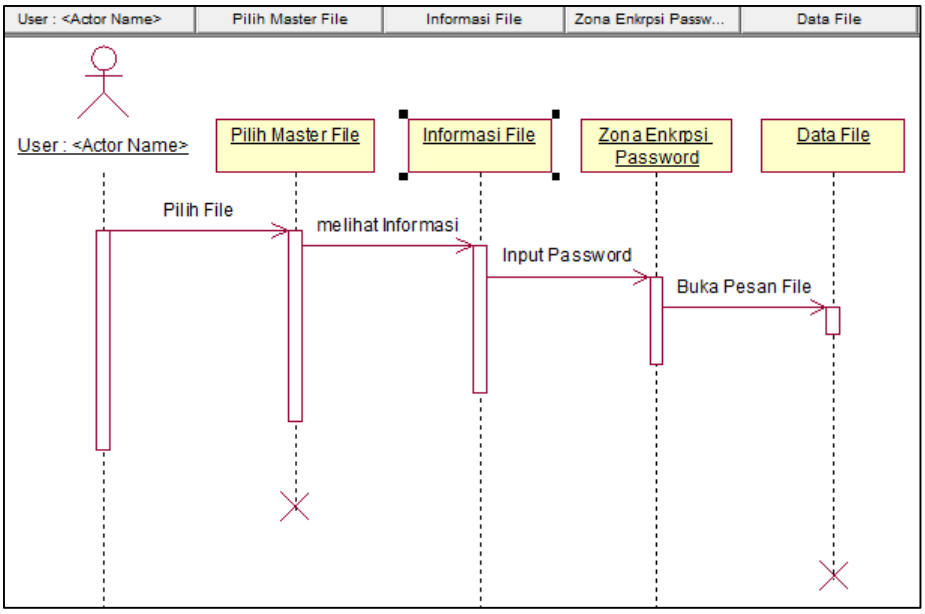
Gambar 10. Diagram Activity Output Stego file

3.5. Proses Decode Data

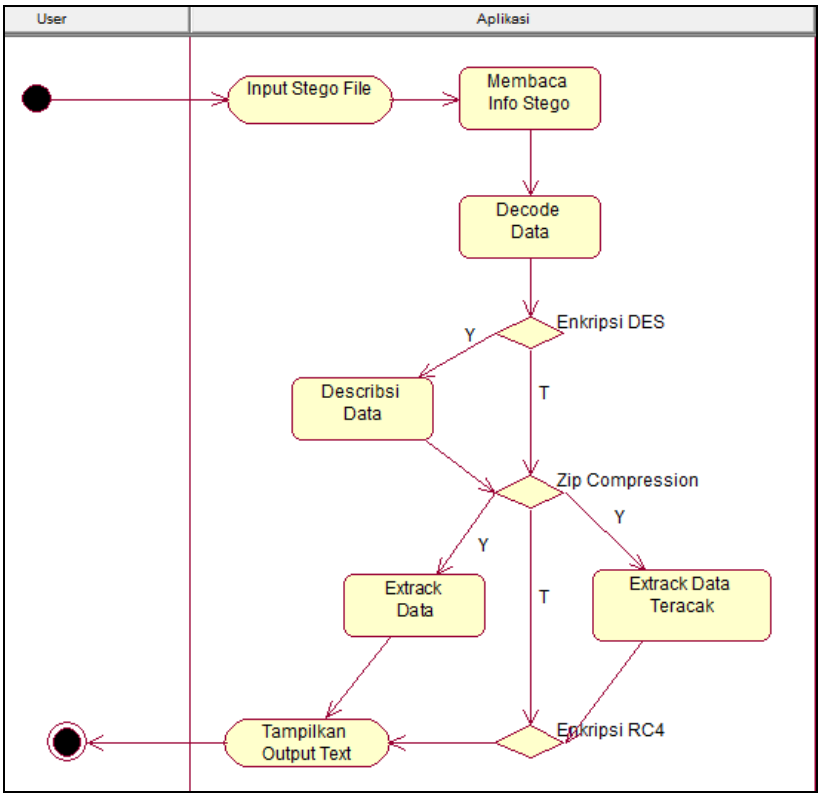
Proses ini berlangsung saat user ingin melakukan *decoding* (pengekstrakan) data dari berkas stego file



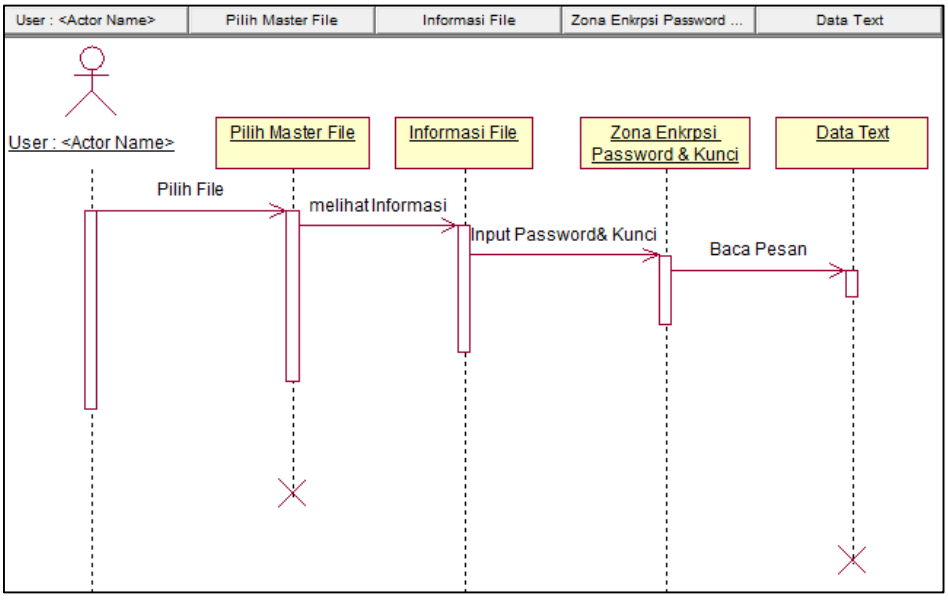
Gambar 11. Activity Diagram Decode Data File



Gambar 12. Sequence Diagram Decode Data File



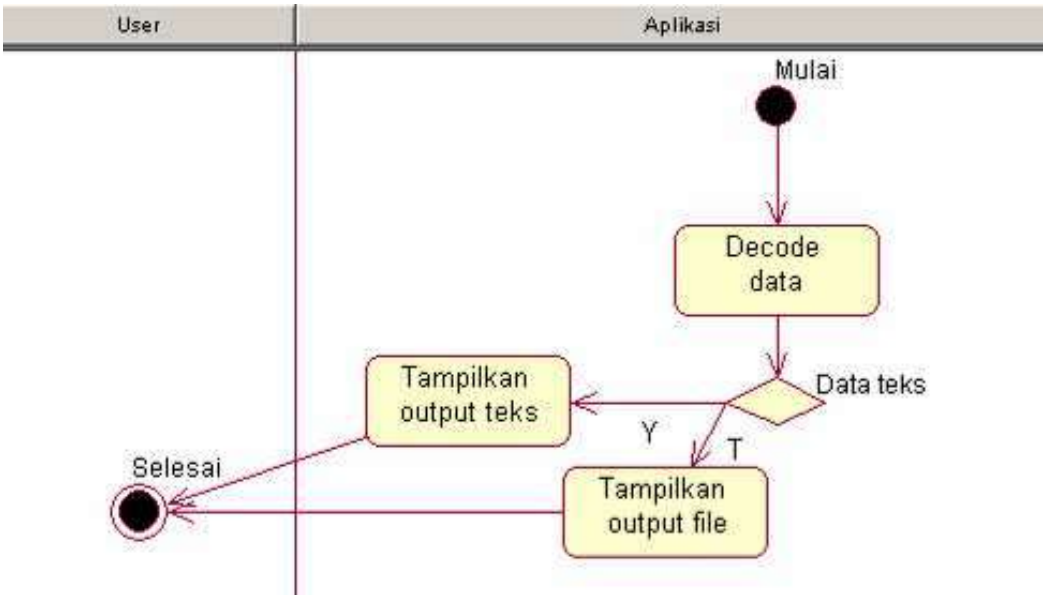
Gambar 13. Activity Diagram Decode Data Text



Gambar 14. Sequence Diagram Decode Data Text

3.6. Proses Output Data Teks atau File

Dari hasil proses *decoding* data, diperoleh hasil output berupa data teks atau data file.



Gambar 15. Diagram Activity Output Data Teks atau File

4. KESIMPULAN

Kesimpulan yang bisa diambil dari perancangan penyembunyaian pesan file dan text dengan metode Enkripsi DES dan Enkripsi RC4 adalah rancangan ini bisa digunakan sebagai panduan untuk pembangunan sebuah system yang digunakan untuk pengamanan informasi dengan cara penyembunyian file atau text sehingga informasi atau pesan yang disampaikan relative lebih aman.

5. SARAN

Pengembangan system khususnya untuk keamanan data maupun informasi tentunya sangat diperlukan rancangan ini adalah salah satu yang bisa digunakan, yang tentunya masih banyak yang bisa dikembangkan lagi dan melengkapinya.

DAFTAR PUSTAKA

[1] Agus Prihanto, Supeno Djanali, Muchammad Husni (2010). *Peningkatan Kapasitas Informasi Tersembunyi Pada Image Steganografi Dengan Menggunakan Teknik Hybrid,* Teknik Informatika, ITS http://digilib.its.ac.id/public/ITS-Master-14317-paperpdf.pdf Tanggal akses 16 September 2016

[2] Al-Mualla, Dr. Muhammed, Al–Ahmad, Prof. Husein (2003). *Information Hiding : Steganography and Watermarking*, Etisalat College of Engineering, UAE.

[3] A Hakim, Muhammad (2007), *Makalah Studi dan Implementasi Steganography Metode LSB dengan Preprocessing Kompresi data dan Ekspansi Wadah*, Teknik Informatika, ITB.

[4] Erdiansyah Fajar Nugraha (2010). *Meningkatkan Kapasistas Pesan yang disisipkan dengan Metode Redundant Pattern Encoding* . Skripsi Teknik Informatika . ITB. http://www.informatika.org/~rinaldi/Kriptografi/2010-2011/Makalah1/Makalah1-IF3058-

Sem1-2010-2011-043.pdf
Diakses tanggal 8 Oktober 2016

[5] Eriksson H-E and Penker M. (1998), UML Toolkit, John Wiley & Son Inc.

[6] Munir, Rinaldi (2005), Diktat Kuliah IF5054 Kriptografi, Teknik Informatika ITB, Bandung.

[7] Nurokhim, "*Case Tool Pengembangan Perangkat Lunak Berorientasi-objek menggunakan Unified Modeling Language (UML)*", Puspiptek Serpong, Tangerang, 2002
http://eprints.ums.ac.id/778/1/Emitor_RNR_CaseTool.pdf
Tanggal Akses : 23 Mei 2011

[8] Passa, Fitriani, "*Studi dan Analisis Implementasi Algoritma RC4 dengan Modifikasi Kunci Menggunakan Fungsi SHA-1*", Teknik Informatika ITB, Bandung, 2010
http://www.scribd.com/document_downloads/direct/56116097?extension=pdf&ft=1309408804&lt=1309412414&uahk=+DOklU+vR9sdflgDh9fFF1ZfNVQ
Tanggal Akses : 10 Agustus 2016