PENGAMANAN FILE MENGGUNAKAN *ADVANCED ENCRYPTION STANDARD* DAN *LEAST SIGNIFICANT BIT*

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau

OLEH:

FERI RAMA ANDIKA
NPM : 133510333

PROGRAM STUDI TEKNIK INFORMATIKA
FAKUTAS TEKNIK
UNIVERSITAS ISLAM RIAU
2020

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

HALAMAN PERSEMBAHAN

Alhamdulillahirobbil`alamin.

Sujud syukurku kupersembahkan kepadamu Allah Azzawajalla yang Maha Agung, Maha Tinggi dan Maha Adil serta Maha Penyayang, atas takdir dan kehendakmu, engkau jadikan diriku manusia yang senantiasa berpikir, berilmu, beriman dan bersabar dalam menjalani kehidupan ini. Semoga langkah kecil ini menjadi awal sebuah keberhasilan bagi diriku untuk meraih cita-cita besar yang telah digantungkan. Sholawat dan salam senantiasa dilimpahkan kepada beliau Shallallahu`alaihiwasallam, betapa hambamu ini mencitai dirinya, keluarganya, para sahabatnya dan segenap pengikutnya.

Dengan menadahkan tangan seraya berdoa dalam syukur yang terkira terima kasih untukmu, kupersembahkan sebuah karya kecil untuk ayahanda **Maksum** dan ibunda tercinta **Wagiyem** yang tidak pernah berhenti memberiku semangat, doa, dorongan nasehat dan kasih sayang serta pengorbanannya yang tidak akan pernah bisa tergantikan dengan apapun dan sampai kapanpun. Wahai ibunda terimalah bukti kecil ini sebagai kado keseriusanku untuk membalas semua yang telah diberikan kepadaku. Mohon maaf yang sebesar-besarnya sampai detik ini ananda masih saja menyusahkanmu.

Untuk jutaan impian yang harus dicapai, mengejar keping-kepingan hidup menjadi sebuah kebagagiaan agar hidup lebih bermakna teruslah belajar, berusaha dan berdoa untuk menggapainya. Bila gagal mencoba kembali, bila jatuh berdiri kembali jangan pernah sedikitpun terbesit untuk menyerah.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Untaian kata-kata kecil inilah yang saya persembahkan buat kalian. Terima kasih yang tidak terhingga saya ucapkan. Atas segala kekurangan dan kekhilafan kurendahkan hati dan dengan mengucapkan berjuta-juta maaf yang tercurah.

Pekanbaru, 21 September 2020

Feri Rama Andika

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Alhamdulillaahi Robbil'alamin, dengan mengucapkan puji syukur ke-hadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penulisan laporan skripsi yang berjudul "Pengamanan *File* Menggunakan *Advanced Encryption Standard* dan *Least Significant Bit*". *Allahumma sholli'ala Muhammad wa'ala ali sayyidina Muhammad,* yang selalu penulis ucapkan untuk baginda Nabi besar, Muhammad SAW.

Adapun penyusunan laporan skripsi ini dilakukan sebagai salah satu prasyarat untuk menyelesaikan Program Studi Strata 1 pada Jurusan Teknik Informatika di Fakultas Teknik, Universitas Islam Riau (UIR).

Penulis menyadari adanya banyak keterbatasan yang penulis miliki, sehingga ada banyak pihak yang telah membantu baik moril maupun materil dalam menyelesaikan penelitian ini. Maka dari itu dengan segenap kerendahan hati penulis mengucapkan terima kasih kepada :

1. Bapak Dr. Eng. Muslim, ST., MT selaku Dekan Fakultas Teknik dan selaku penasehat akademis yang telah iklas dan sabar memberikan bimbingan dan arahan di sela-sela kesibukan beliau.
2. Ibu Drs. Mursyidah, S.SI., M.Cs selaku Wakil Dekan I, Bapak Dr. Anas Puri, ST., MT selaku Wakil Dekan II, dan Bapak Akmar Efendi, S.Kom., M.Kom selaku Wakil Dekan III Fakultas Teknik Universitas Islam Riau.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. Bapak Dr. Arbi Haza Nasution, B.IT (Hons)., M.IT selaku Ketua Program Studi Teknik Informatika.
4. Bapak Yudhi Arta, ST., M. Kom selaku Dosen Pembimbing yang telah iklas dan sabar memberikan bimbingan dan arahan di sela-sela kesibukan beliau.
5. Bapak dan Ibu Dosen Teknik UIR yang telah banyak memberika ilmunya selama penulis menduduki bangku perkuliahan khususnya bagi Bapak dan Ibu Dosen Program Studi Teknik Informatika.
6. Kepada seluruh staff Tata Usaha Fakultas Teknik yang telah membantu dalam kelancaran pada penyelesaian skripsi ini.

Akhirnya, penulis menyadari dalam penulisan laporan skripsi ini masih terdapat kekeliruan dan kesalahan. Oleh karena itu, penulis mengharapkan kritik dan saran untuk kemajuan penulis secara pribadi serta berharap proposal skripsi ini dapat memberikan manfaat bagi khasanah pengetahuan Teknologi Informasi di Indonesia. Terima Kasih.

Pekanbaru, 21 September 2020

Penulis

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Pengamanan File Menggunakan *Advanced Encryption Standard* Dan *Least Significant Bit*

Feri Rama Andika
Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Riau
Email : ferira@student.uir.ac.id

ABSTRAK

Perkembangan teknologi komputer yang pesat tersebut memicu kejahatan-kejahatan yang memenfaatkan kelemahan pada system komputer. Salah satu bentuk kejahatannya adalah perbuatan hacker yang mengambil data dan informasi melaui celah keamanan komputer. Data tersebut digunakan untuk berbagai hal yang tidak semestinya. Informasi yang dikirim melalui media komunikasi dapat diambil dan disalah gunakan oleh pihak-pihak yang tidak bertanggung jawab. Sistem kemanan data elektronik sebenarnya sudah dikembangkan. Dengan munculnya berbagai metode pengamanan data seperti enkripsi dan steganografi. Enkripsi adalah salah satu cara pengamanan file data dengan cara mengacak suatu dokumen, sedangkan Steganografi adalah pengamanan data elektronik dengan cara menyembunyikan sebuah file kedalam file lainnya. Berdasarkan uji kelayakan sistem dengan kuesioner oleh 20 responden menunjukkan hasil 87% yang dimana hasil ini dikategorikan "sangat baik".
Kata kunci : *Enkripsi* , Kriptografi, Steganografi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

File Security Using Advanced Encryption Standard And Least Significant Bit

Feri Rama Andika
Informatics Engineering Program Faculty of Engineering,
Islamic University of Riau
Email : ferira@student.uir.ac.id

ABSTRACT

The rapid development of computer technology triggers crimes that take advantage of weaknesses in computer systems. One form of crime is the act of hackers who take data and information through computer security holes. This data is used for various things that are not supposed to. Information sent via communication media can taken and misused by parties who are not responsible. Electronic data security systems have actually been developed. With the emergence of various data security methods such as encryption and steganography. Encryption is one way of securing data files by means of a random documents, while Steganography is the protection of electronic data by hiding a file into another file. Based on the feasibility test of the system with a questionnaire by 20 respondents, it shows the results of 87% which are categorized as "very good".

Keywords: Encryption, Cryptography, Steganography.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR ISI

Halaman

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB II LANDASAN TEORI

BAB III METODOLOGI PENELITIAN

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR TABEL

Halaman

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR GAMBAR

Halaman

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR LAMPIRAN

Halaman

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi Informasi dan komunikasi saat ini sangat pesat. Hal ini ditandai dengan penggunaan teknologi komputer oleh semua kalangan masyarakat. Perkembangan teknologi komputer yang pesat tersebut memicu kejahatan-kejahatan yang memenfaatkan kelemahan pada sistem komputer. Salah satu bentuk kejahatannya adalah perbuatan *hacker* yang mengambil data dan informasi melaui celah keamanan komputer. Data tersebut digunakan untuk berbagai hal yang tidak semestinya. Informasi yang dikirim melalui media komunikasi dapat diambil dan disalah gunakan oleh pihak-pihak yang tidak bertanggung jawab.

Dengan adanya kasus tersebut, tentu saja penggunaan teknologi untuk pengiriman informasi menjadi hal yang rentan bagi beberapa pihak. Seperti pengiriman dokumen perusahaan, pengiriman dokumen pemerintahan bahkan pengiriman dokumen yang bersifat privasi pribadi pun akan merasa terganggu.

Sistem kemanan data elektronik sebenarnya sudah dikembangkan. Dengan munculnya berbagai metode pengamanan data seperti enkripsi dan steganografi. Enkripsi adalah salah satu cara pengamanan file data dengan cara mengacak suatu dokumen dan hanya bisa disusun kembali menggunkan kata kunci atau sandi yang ditelah di setting sebelumnya. Sedangkan Steganografi adalah pengamanan data elektronik dengan cara menyembunyikan sebuah file kedalam file lainnya.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Oleh karna itu, pada pada penelitian ini penulis tertarik membangun sistem yang dapat mengenkripsikan data sekaligus menyembunyikan data dan informasi didalam file vidio, agar data dan informasi yang dikirimkan melalui media elektronik dapat terjanmin keamanannya.

1.2 Identifikasi Masalah

Dari Latar belakang masalah pada sub bab sebelumnya dapat diidentifikasi masalah sebagai berikut :

1. Terdapat celah keamanan saat transaksi data menggunakan teknologi informasi standar.
2. Informasi yang bocor dapat merugikan pihak pemilik informasi yang melakukan transaksi data menggunakan teknologi informasi dan komunikasi

1.3 Batasan Masalah

Agar permasalahan yang ditinjau lebih terarah dan mencapai sasaran, maka dibuat batasan dari perumusan masalah, diantaranya sebagai berikut :

1. Sebelum proses steganografi, dilakukan pengenkripsian dengan menggunakan algoritma *Advanced Encryption Standard* (AES).
2. Algoritma *steganografi* yang digunakan adalah algoritma *Steganografi Least Significant Bit* (LSB).
3. Data yang dienkripsi merupakan file word (*.doc, *docx).

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4. Bahasa pemprograman yang digunakan untuk mengembangkan sistem adalah bahasa pemprograman *Python*.

1.4 Perumusan Masalah

Berdasarkan uraian pada latar belakang diatas, maka dapat dirumuskan masalah bagaimana cara membuat sebuah aplikasi yang dapat mengamankan file dengan Kriptografi dan steganografi.

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan Penelitian

Penelitian ini bertujuan untuk menerapkan suatu sistem keamanan data dan informasi dengan algoritma *Advanced Encryption Standard* (AES) dan algoritma *Steganografi Least Significant Bit* (LSB).

1.5.2 Manfaat Penelitian

Dengan adanya penelitian ini diharapkan dapat memberikan solusi untuk pengamanan data elektronik melalui teknologi informasi dan komunikasi sehingga tidak terjadi kebocoran data pada pihak yang tidak berwenang.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB II
LANDASAN TEORI

2.1 Studi Pustaka

Muhamad Fitra Syawal dalam Jurnal TICOM Vol.4 No.3 Mei 2016 meneliti tentang Implementasi Teknik Steganografi Menggunakan *Algoritma Vigenere Cipher* Dan Metode LSB. Penelitian ini dibuat menggunakan bahasa pemrograman web. Pada penelitian ini objek penelitian adalah dengan memasukan text kedalam gambar agar menghasilkan file yang tersembunyi dan tidak dapat diakses oleh pihak yang tidak berwenang.

Jhoni Verlando Purba telah melakukan penelitian yang berjudul Implementasi Steganografi Pesan Text Ke Dalam File Sound (.Wav) Dengan Modifikasi Jarak Byte Pada Algoritma Least Significant Bit (Lsb) pada tahun 2017. Tujuan penelitian ini adalah untuk menyembunyikan file berekstensi .txt kedalah file berekstensi .Wav. Pada penelitian ini digunakan bahasa pemrograman web.

Tri Prasetyo Utomo telah melakukan penelitian dan menuangkan hasil penelitiannya dalam jurnal yang berjudul Steganografi Gambar Dengan Metode *Least Significant Bit* Untuk Proteksi Komunikasi Pada Media Online. Pada jurnal ini disisipkan sebuah pesan pada file gambar untuk dapat di ekstrak kembali menjadi pesan. Cara ini dilakukan untuk mengamankan pesan dan menghindari pihak yang tidak berkepentingan untuk memanfaatkan pesan tersebut.

Penelitian yang dilakukan Tri Prasetyo Utomo, Jhoni Verlando Purba, Muhamad Fitra dan penelitian yang penulis lakukan sama-sama mengamankan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

data dengan cara menyembunyikan data tersebut kedalam data lain. Perbedaannya terdapat pada objek yang diteliti, metode penelitian dan bahasa pemrograman yang digunakan dalam mengembangkan sistem tersebut.

2.2 Dasar Teori

2.2.1 Pengertian Sistem

Ada banyak pendapat tentang pengertian dan definisi sistem yang dijelaskan oleh beberapa ahli. Berikut pengertian dan definisi sistem menurut beberapa ahli:

1. Murdick, R.G (2015), Sistem adalah seperangkat elemen-elemen yang membentuk suatu kumpulan dari berbagai prosedur atau berbagai bagan pengolahan untuk mencari sebuah tujuan bersama dengan cara mengoperasikan data maupun barang untuk menghasilkan suatu informasi.
2. John Mc Manama (2014), Sistem adalah sebuah struktur konseptual yang tersusun dari fungsi-fungsi yang saling berhubungan yang bekerja sebagai suatu kesatuan organik untuk mencapai suatu hasil yang diinginkan secara efektif dan efisien.
3. Prajudi (2017), Sistem adalah suatu jaringan dari prosedur-prosedur yang berkaitan satu sama lain menurut skema atau pola yang bulat untuk menggerakkan suatu fungsi utama.
4. Andri Kristanto (2017), Sistem adalah jaringan kerja dari prosedur-prosedur yang saling berhubungan, berkumpul bersama-sama untuk melakukan suatu kegiatan atau menyelesaikan suatu sasaran tertentu.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

5. Bonnie Soeherman dan Marion Pinontoan (2016), Sistem adalah serangkaian komponen-komponen yang saling berinteraksi dan bekerja sama untuk mencapai tujuan tertentu.

2.2.2 Python

Python (bahasa pemrograman) merupakan bahasa pemrograman tingkat tinggi yang bisa melakukan eksekusi sejumlah instruksi multi guna secara langsung (*interpretatif*) dengan metode *Object Oriented Programming* dan juga menggunakan semantik dinamis untuk memberikan tingkat keterbacaan *syntax*. Sebagai bahasa pemrograman tinggi, python dapat dipelajari dengan mudah karena telah dilengkapi dengan manajemen memori otomatis.

Dalam penggunaannya, python bisa menentukan fungsi untuk menyediakan fungsionalitas yang dibutuhkan. Berikut ini merupakan aturan sederhana untuk mendefinisikan fungsi dengan Python :

1. Fungsi blok dimulai dengan def kata kunci diserta dengan nama fungsi dan tanda kurung (()).
2. Setiap parameter masukan atau argumen dan ditempatkan di dalam tanda kurung. Parameter juga dapat ditentukan di dalam tanda kurung ini.
3. Pernyataan pertama dari sebuah fungsi bisa berupa pernyataan opsional – string dokumentasi fungsi atau docstring.
4. Blok kode di dalam setiap fungsi dimulai dengan titik dua (:) dan indentasi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

5. Pernyataan kembali keluar dari sebuah fungsi, secara opsional menyampaikan kembali ekspresi ke pemanggil. Pernyataan pengembalian tanpa argumen sama dengan *return None*.

2.2.3 *Steganografi* dan Metode *Advanced Encryption Standard (AES)*

Teknik steganografi ini sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan *hieroglyphic* yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia. Tidak hanya bangsa Mesir saja, bangsa-bangsa lain juga telah mengggunakan teknik steganografi pada masa lalu, yaitu :

1. Teknik steganografi yang lain adalah tinta yang tidak tampak (invisible ink) yaitu dengan menggunakan air sari buah jeruk, urin atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas api. Tinta yang sebelumnya tidak terlihat, ketika terkena panas akan menjadi gelap sehingga dapat dibaca. Teknik ini digunakan oleh bangsa Romawi yang juga digunakan pada Perang Dunia II.
2. Bangsa Cina menggunakan cara yang berbeda pula, yaitu manusia sebagai media pembawa pesan. Orang itu akan dicukur rambutnya sampai botak dan pesan akan dituliskan di kepalanya. Kemudian pesan akan dikirimkan ketika rambutnya sudah tumbuh.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. Pada masyarakat Yunani kuno teknik yang digunakan adalah dengan menggunakan lilin sebagai media pembawa pesan. Lembaran pesan akan ditutup dengan lilin. Untuk melihat isi pesan, pihak penerima harus memanaskan lilin terlebih dahulu.
4. Pada Perang Dunia II, bangsa Jerman menggunakan *microdots* untuk berkomunikasi. Penggunaan teknik ini digunakan pada microfilm chip yang harus diperbesar sekitar 200 kali. Jerman menggunakan teknik ini untuk kebutuhan perang sehingga pesan rahasia strategi tidak diketahui pihak lawan. Karena pada saat itu teknik ini merupakan teknologi baru yang belum bisa digunakan lawan.

Akhir-akhir ini kata steganografi menjadi sering disebut di masyarakat bersama – sama dengan kata kriptografi setelah pemboman gedung WTC di AS, telah disebutkan oleh Pejabat Pemerintah dan Para Ahli dari Pemerintahan Amerika Serikat "yang tidak disebut namanya bahwa" bahwa Para Teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang chat sport, bulletin boards porno dan web site lainnya. Walaupun demikian sebenarnya belum ada bukti nyata dari pernyataan-pernyataan tersebut diatas. *Novel Da Vinci Code* pun turut mempopulerkan steganografi dan kriptografi.

Advanced Encryption Standard (AES) dipublikasikan oleh NIST (*National Institute of Standard and Technology*) pada tahun 2001. Menurut penelitian Tentang Perancangan Pengamanan Data Menggunakan Algoritma AES diperoleh pengertian AES merupakan algoritma cryptographic yang dapat digunakan untuk

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi dan dekripsi informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext, sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang dikenal sebagai *plaintext*.

Proses yang dilakukan pada setiap rondenya identik sama (dari ronde ke-1 sampai dengan ronde ke Nr-1) kecuali untuk ronde Nr. Proses yang identik tersebut terdiri atas SubBytes, ShiftRows, MixColumns dan AddRoundKey. Sedangkan pada ronde Nr, proses MixColumns tidak dilakukan. Tiap ronde memilki roundkey yang dihasilkan dari ekspansi dari kunci utama.

Proses enkripsi yang dilakukan menggunakan algoritma AES yaitu :

1. *AddRoundKey* : melakukan XOR antara state awal (*plainteks*) dengan *cipherkey*. Tahap ini disebut juga *initial round.*
2. Putaran sebanyak Nr – 1 kali. Proses yang dilakukan pada setiap putaran adalah:
   a. SubBytes: substitusi byte dengan menggunakan tabel substitusi (S-box).
   b. ShiftRows: pergeseran baris-baris array state secara wrapping.
   c. MixColumns: mengacak data di masing-masing kolom array state.
   d. AddRoundKey: melakukan XOR antara state sekarang round key.
3. *Final round* : proses untuk putaran terakhir :
   a. SubBytes
   b. ShiftRows

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

c. AddRoundKey

2.2.4 *Kriptografi* dan Metode *Least Significant Bit*

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu *cryptos* yang berarti *secret* (rahasia), sedangkan *graphien* artinya *writing* (tulisan). Jadi secara asal bahasa kriptografi berarti *secret writing* (tulisan rahasia). Kriptografi memiliki beberapa definisi. Salah satu definisi kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentifikasi data.

Perkembangan komunitasi telah mendorong manusia untuk menyembunyikan informasinya demi alasan keamanan dan privasi. Seseorang yang berusaha untuk mengembangkan dan membuat kode kriptografi disebut cryptographer. Sedangkan seseorang yang berusaha memecahkan kode tersebut disebut *cryptanalists*.

Jenis Kritografi berdasarkan perkembangannya :

1. Algoritma Kriptografi Klasik

Algoritma ini digunakan sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau tranposisi atau keduanya (Sadikin, 2012). Teknik substitusi adalah menggantikan karakter dalam plainteks menjadi karakter lain. Sedangkan transposisi adalah teknik mengubah plaintext menjadi ciphertext dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

yang melatabelakangi terbentuknya berbagai macam algoritma kriptografi modern.

2. Algoritma Kriptografi Modern

Algoritma ini memiliki tingkat kesulitan yang kompleks (Prayudi, 2005) dan kekuatan kriptografinya ada pada key atau kuncinya. Algoritma ini menggunakan pengolahan simbol biner karena berjalan mengikuti operasi komputer digital. Sehingga membutuhkan dasar berupa pengetahuan terhadap matematika untuk menguasainya.

Jenis Kriptografi Berdasarkan Kunci :

1. Algoritma Simetris

Algoritma ini disebut simetris karena memiliki key atau kunci yang sama dalam proses enkripsi dan dekripsi sehingga algoritma ini juga disebut algoritma kunci tunggal atau algoritma satu kunci. Key dalam algoritma ini bersifat rahasia atau private key sehingga algoritma ini juga disebut dengan algoritma kunci rahasia.

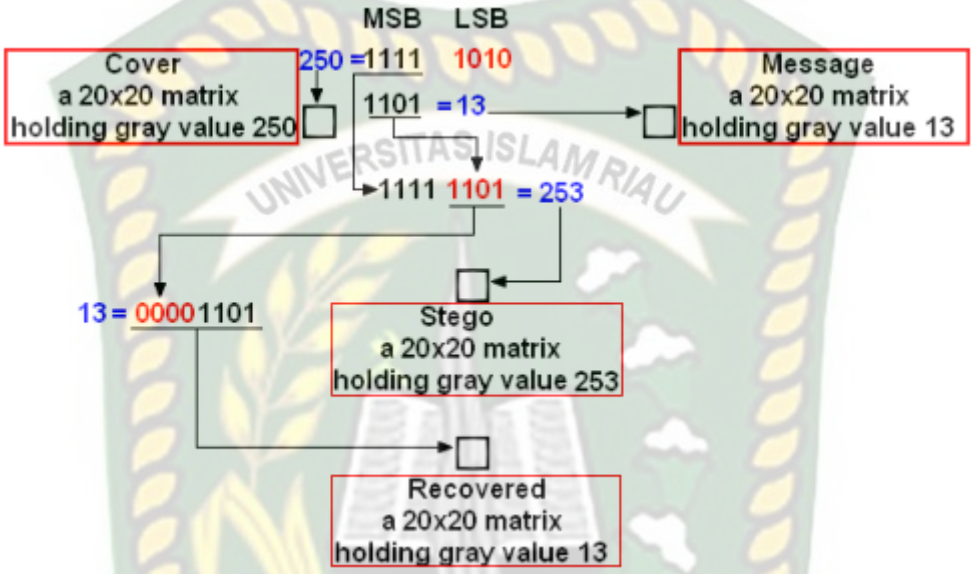
2. Algoritma Asimetris

Algoritma ini disebut asimetris karena kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Kunci yang digunakan untuk enkripsi adalah kunci publik atau public key sehingga algoritma ini juga disebut dengan algoritma kunci publik. Sedangkan kunci untuk dekripsi menggunakan kunci rahasia atau *private key*.

LSB adalah teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode LSB yaitu mengubah bit redundan cover

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

image yang tidak berpengaruh signifikan dengan bit dari pesan rahasia. Gambar 2 berikut ini menunjukkan mekanisme metode LSB pada gambar 8 bit dengan memanfaatkan 4 bit LSB.



Gambar 2.1 Mekanisme LSB (Chedad et al, 2010)

Gambar 2 menunjukkan penerapan LSB menggunakan media gambar berbasis pixel dengan nilai 8 bit (gray value). Setiap pixel yang terdiri dari 8 bit dibagi menjadi 2 bagian yaitu, 4 bit MSB (most significant bit) dan 4 bit LSB (least significant bit). Bagian LSB lah yang diubah menjadi nilai dari pesan yang akan disisipkan. Setelah dibubuhi pesan rahasia, setiap pixel dibangun kembali menjadi gambar yang utuh menyerupai dengan media gambar semula.

2.2.5 Alat Bantu Dalam Analisa dan Perancangan Sistem

2.2.5.1 *Data Flow Diagram* (DFD)

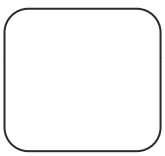
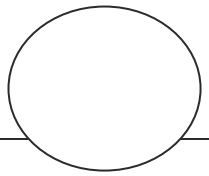
Data Flow Diagram (DFD) adalah diagram yang digunakan untuk menggambarkan aliran data dalam sistem. DFD sering digunakan untuk

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana *data* tersebut mengalir (misalnya lewat telpon, surat dan sebagainya) atau lingkungan fisik dimana *data* tersebut akan disimpan. DFD merupakan alat yang digunakan pada metodologi pengembangan sistem yang terstruktur (*structured Analysis and design*). DFD merupakan alat yang cukup popular sekarang ini, karena dapat menggambarkan arus *data* di dalam sistem dengan terstruktur dan jelas. Lebih lanjut DFD juga merupakan dokumentasi dari sistem yang baik. Bebarapa simbol yang digunakan di DFD untuk maksud mewakili:

1. *External entity* (kesatuan luar) atau *boundary* (batas sistem)
2. *Data flow* (arus *data*)
3. *Process* (proses)
4. *Data store* (Simpanan *data*). (Jogiyanto, 2004)

Tabel 2.1 Simbol *Data Flow Diagram*

Simbol	Nama	Fungsi
	Simbol entitas eksternal	Digunakan untuk menunjukkan tempat asal *data* atau sumber atau tempat tujuan *data* atau tujuan.
	Simbol proses	Digunakan untuk menunjukkan tugas atau proses yang dilakukan baik secara manual atau otomatis
	Simbol proses	Digunakan untuk menunjukkan tugas atau proses yang dilakukan baik

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

		secara manual atau otomatis
	Simbol penyimpanan *data*	Digunakan untuk menunjukkan gudang informasi atau *data*.
	Simbol arus *data*	Digunakan untuk menunjukkan arus dari proses.

2.2.5.2 *Activity Diagram*

Activity Diagram adalah diagram yang digunakan untuk menggambarkan aktifitas yang terjadi *didalam* sebuah sistem. Berikut ini adalah simbol-simbol yang digunakan dalam *Activity Diagram :*

Tabel 2.2 Simbol *Activity Diagram*

SIMBOL	KETERANGAN
	Titik Awal
	Titik Akhir
	Activity
	Pilihan Untuk mengambil Keputusan
	Fork; Digunakan untuk menunjukkan kegiatan yang dilakukan secara parallel atau untuk menggabungkan dua kegiatan peralel menjadi satu.
	Rake; Menunjukkan adanya dekomposisi

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

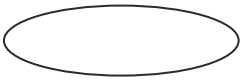
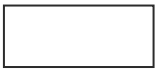
	Tanda Waktu
	Tanda pengiriman
	Tanda penerimaan
	Aliran akhir (Flow Final)

2.2.5.3 Program *Flowchart*

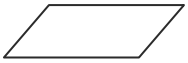
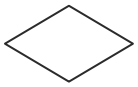
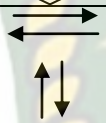
Ada dua *tool* yang sering digunakan untuk membantu menyusun dokumen pemrograman, yaitu *flowchart* dan *pseudocode* (kode semua). *Flowchart* adalah simbol-simbol pekerjaan yang menunjuk bagan aliran proses yang saling terhubung. Jadi, setiap simbol yang ditentukan oleh *American National Standard Institute Inc.*

Flowchart digunakan untuk mempermudah penyusunan program. Dengan menggunakan *flowchart*, logika pemrograman lebih mudah dipahami dan dianalisis, sehingga anda dapat menentukan kode-kode pemograman yang sesuai dengan pekerjaanya. *Flowchart* program dapat disamakan dengan *blue print* bangunan. Seperti diketahui arsitek akan membuat *blue print* bangunan sebelum memulai konstruksinya. Demikian pula seorang *programmer* disarankan untuk membuat *flowchart*. Sebelum menulis kode programnya. Berikut beberapa simbol standar *flowchart* yang sering digunakan dalam pemrograman komputer.

Tabel 2.3 Program *Flowchart*

Simbol	Arti
	Simbol ***Start*** atau ***End*** yang mendefenisikan awal atau akhir dari sebuah *flowchart*
	Simbol pemrosesan yang terjadi pada sebuah alur kerja

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

	Simbol ***Input/output*** mendefenisikan masukan dan keluaran proses
	Simbol untuk memtuskan proses lanjutan dari kondisi tertentu
	Simbol konektor untuk menyambung proses pada lembar kerja yang berbeda
	Simbol konektor untuk menyambung proses lembar kerja yang berbeda
	Simbol untuk menghubungkan antar proses atau antar symbol
	Simbol yang menyatakan bagian dari program (sub program)

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metodologi penilitian merupakan tahapan-tahapan yang dilalui oleh peneliti untuk memperoleh gambaran yang jelas.mengenai penelitian maka penyusunan metodologi penelitian sebagai berikut :

1. Data *Collecting*

   Yaitu proses pengumpulan data langsung dari sumber data. Data yang dikumpulkan tidak langsung dipakai, namun diseleksi terlebih dahulu. Jika masih terdapat *noise* maka data tersebut perlu disterilisasi..

2. Studi Literatur

   Studi literatur dilakukan dengan cara mengumpulkan dan mempelajari segala macam informasi yang berhubungan dengan sistem kriptografi dan steganografi serta segala hal yang berhubungan dengan model pemrogramannya.

3. Perancangan Sistem

   Pada tahap ini dilaksanakan perancangan sistem perangkat lunak yang akan dibuat berdasarkan hasil studi literatur yang ada. Perancangan perangkat lunak ini meliputi desain struktur data, desain aliran informasi, desain antar muka, desain algoritma dan pemrograman. Perancangan ini dengan membuat alur program, menentukan algoritma yang sesuai agar program dapat berjalan dengan baik dan efisien.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4. Implementasi Sistem

   Tahap implementasi sistem dilakukan secara bertahap dengan acuan studi literatur dan perancangan sistem yang telah dibuat. Perancangan sistem yang telah dibuat akan diimplementasikan pada bahasa pemrograman yang telah disepakati.

5. Pengujian dan Evaluasi

   Pada tahap ini dilakukan uji coba program untuk mencari masalah yang mungkintimbul, mengevaluasi jalannya program, dan mengadakan perbaikan jika ada kekurangan.

6. Penyusunan Laporan Penelitian

   Penyusunan laporan dilakukan pada tahap akhir sebagai dokumentasi. Dokumentasi ini dibuat untuk menjelaskan aplikasi agar memudahkan orang lain yang ingin mengembangkan aplikasi lebih lanjut.

3.2 Spesifikasi Kebutuhan *Hardware* dan *Software*

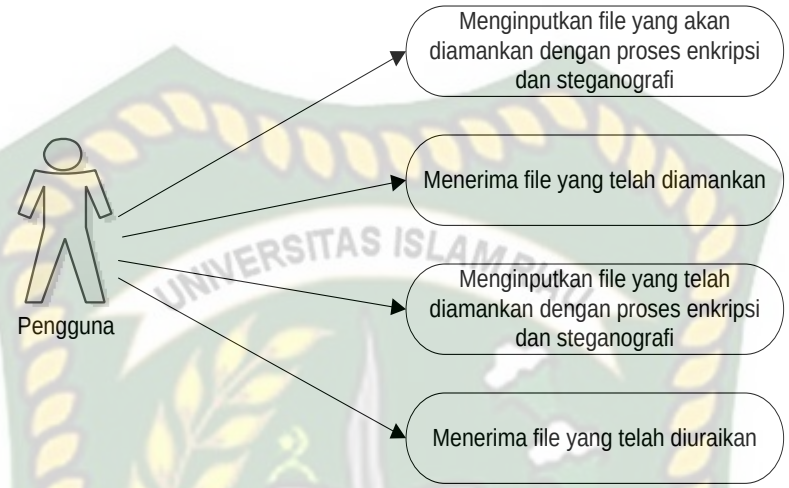
Pada penelitian ini dibangun dengan bahasa pemograman *Python* menggunakan spesifikasi perangkat lunak (*software*) dan perangkat keras sebagai berikut:

1. Sistem operasi menggunakan Windows 7 Ultimate 32-bit.
2. Processor Intel Core i7
3. 500 GB HDD
4. RAM 4 GB

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.3 Analisa *Use Case Diagram*

Adapun gambaran *use case diagram* sistem adalah sebagai berikut :



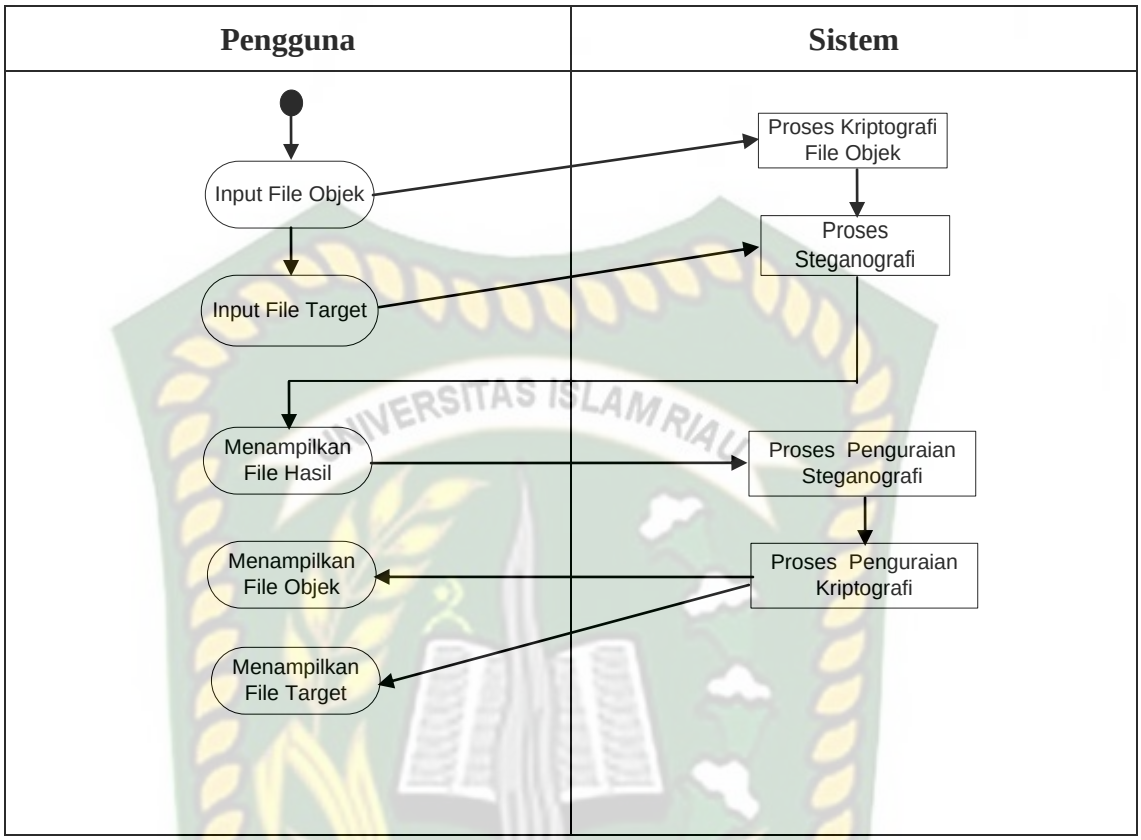
Gambar 3.1 *Use Case Diagaram*

Secara garis besar, pada sistem yang akan dikembangkan pengguna menginputkan file yang akan diamankan. Kemudian pengguna akan menerima file berupa file hasil yang sudah diamankan. Untuk menguraikannya kembali, pengguna cukup menginputkan file yang akan diuraikan, sistem akan otomatis memproses dan pengguna menerima file hasil penguraian.

3.4 *Activity Diagram*

Adapun *activity diagram* pada sistem yang dikembangkan adalah sebagai berikut :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 3.2 ***Activity Diagram***

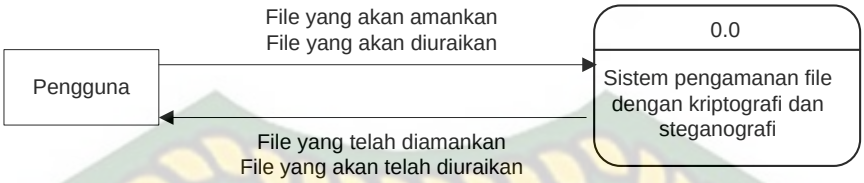
Terdapat satu jenis pengguna didalam sistem yang dikembangkan. Adapun fitur yang disediakan adalah fitur untuk mengamankan file menggunkan steganografi dan kriptografi dan penguraian file yang telah diamankan menjadi file asli.

3.5 Pengembangan dan Perancangan Sistem

Sistem yang akan dibuat dapat digambarkan melalui pengembangan sistem sebagai berikut :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

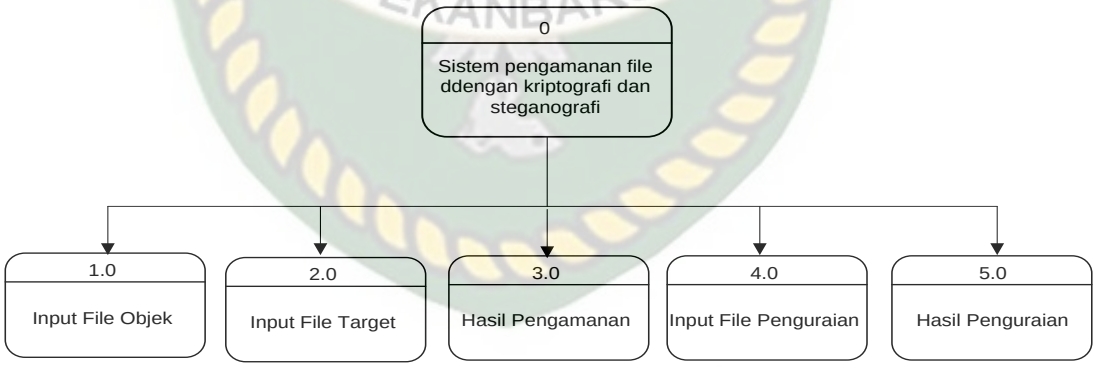
3.5.1 Konteks Diagram



Gambar 3.3 Konteks Diagram Sistem yang Sedang Dikembangkan

Gambar 3.3 Konteks Diagram mengambarkan garis besar aliran data yang berjalan didalam sistem. Dalam konteks diagram digambarkan bahwa terdapat satu jenist pengguna dalam sistem. Pengguna dapat mengakses fitur disistem berupa proses pengamanan file dangan kriptografi dan steganografi. Pengguna juga dapat mengakses menu untuk penguraian file hasil pengamanan kedalam bentuk semula.

3.5.2 *Hierarchy Chart*



Gambar 3.4 *Hierarchy Chart* Sistem yang Sedang Dikembangan

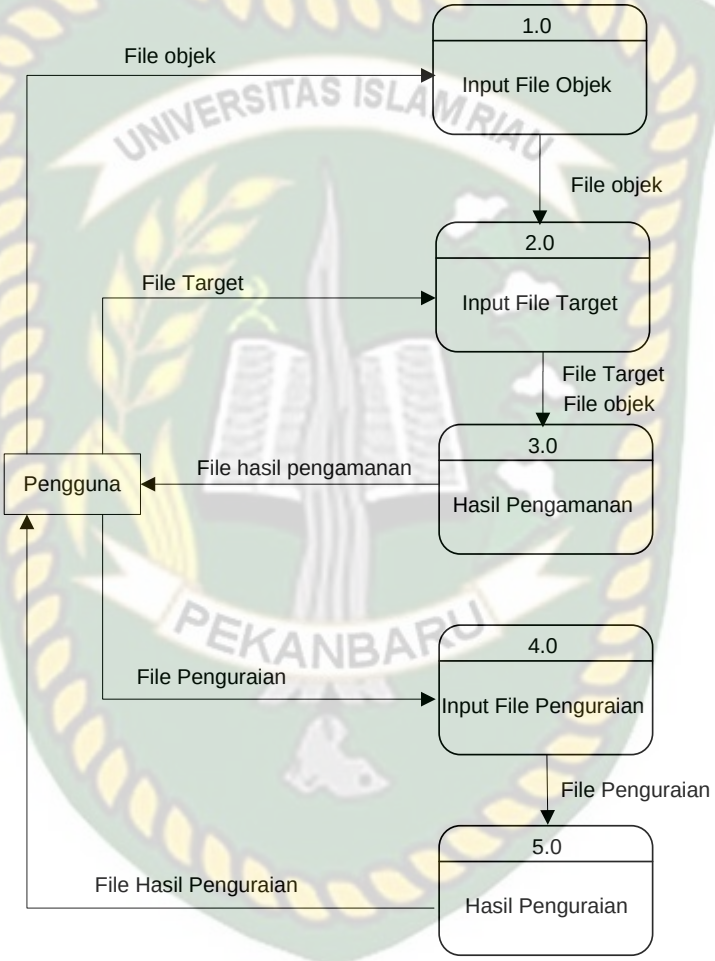
Dari gambar 3.4 *Hierarchy chart* dapat dilihat bahwa pada sistem yang akan dibangun terdapat 5 proses level 0. Adapun proses DFD level 0 terdiri dari input file onjek, input file target, hasil pengamanan, input file penguraian dan hasil penguraian.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.5.3 *Data Flow Diagram* (DFD)

Data Flow Diagram adalah sebuah gambar yang menjelaskan alur data dalam sistem. Berikut ini adalah DFD dari sistem yang akan dibangun :

3.5.3.1 *Data Flow Diagram* (DFD) *Level* 0



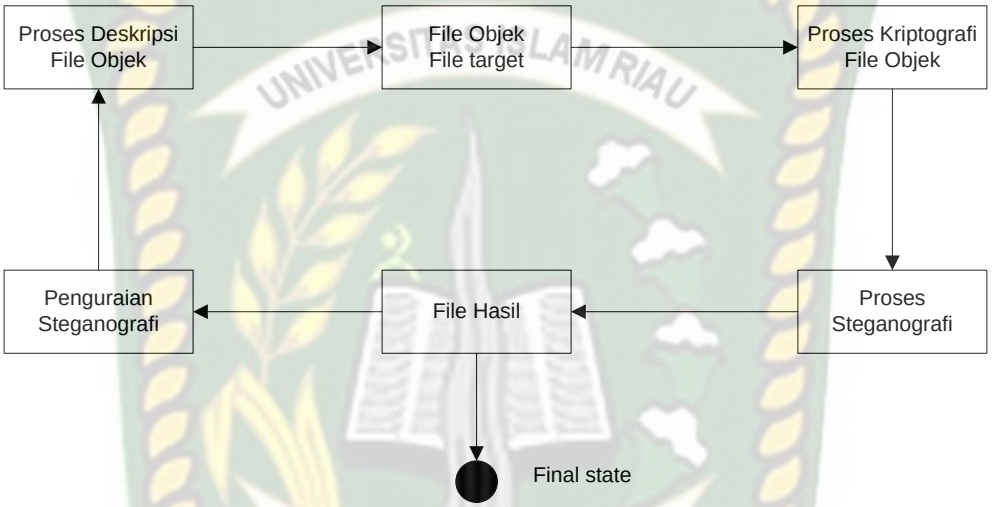
Gambar 3.5 Data *Flow Diagram Level* 0 Sistem yang Sedang Dikembangkan

Data Flow Diagram (DFD) di atas memperlihatkan data yang mengalir dalam sistem. Pada sistem ini terdapat 5 proses yang ada di DFD level 0 yaitu input data objek, input data target, hasil pengamanan, input data penguraian dan hasil penguraian.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.5.4 *State Machine Diagram*

State machine diagram adalah sebuah diagram yang digunakan untuk menggambarkan proses dinamis suatu sistem. Pada sistem yang sedang dikembangkan dapat digambarkan *State machine diagram* seperti pada gambar 3.6 berikut.

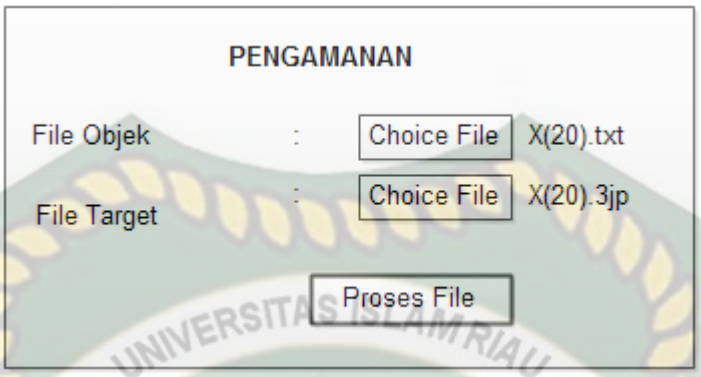


Gambar 3.6 *State Machine Diagram* Sistem yang Sedang Dikembangkan

Gambar 3.6 dapat mendeskripsikan alur dinamis program yang sedang dikembangkan. Dimana file awal terdiri dari file objek dan file target. Selanjutnya dilakukan proses kriptografi pada file objek. Setelah kriptografi selesai, maka dilanjutkan dengan proses steganografi sehingga mendapatkan file hasil yang merupakan tujuan dari sistem. File hasil kemudian dapat diuraikan kembali menjadi file semula dengan melewati proses penguraian steganografi dan deskripsi file objek.

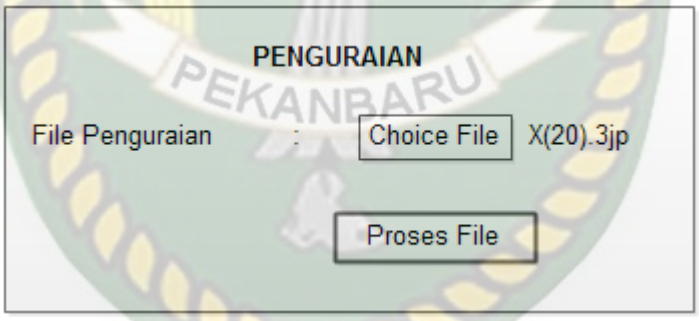
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.5.5 Desain *Input*



Gambar 3.7 Rancangan *Input* Pengamanan *File*

Gambar 3.7 diatas adalah rancangan tampilan Input data pengamanan file. Pada rancangan ini terdapat *field-field* yang diperlukan untuk melengkapi data. Jenis masukan yang disediakan sistem telah disesuaikan dengan kebutuhan data pada *field* tersebut.



Gambar 3.8 Rancangan *Input* Penguraian *File*

Gambar 3.8 diatas adalah rancangan tampilan input data penguraian file. Pada rancangan ini terdapat *field-field* yang diperlukan untuk melengkapi data. Jenis masukan yang disediakan sistem telah disesuaikan dengan kebutuhan data pada *field* tersebut.

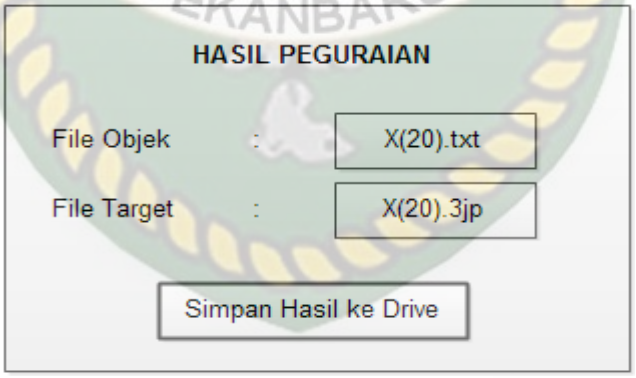
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.5.6 Desain *Output*

Rancangan desain *output* pada sistem yang akan dikembangkan dapat dilihat melalui gambar berikut ini.

Gambar 3.9 Rancangan *Output* Pengamanan *File*

Gambar 3.9 adalah rancangan tampilan hasil pengamanan file. File hasil pengamanan telah tersembunyi didalam file target. Selanjutnya pengguna dapat menyimpan file tersebut kedalam *drive*.



Gambar 3.10 Rancangan *Output* Penguraian *File*

Gambar 3.10 adalah rancangan tampilan hasil penguraian file. File yang disembunyikan didalam file target telah diuraikan kedalam bentuk semula. Selanjutnya pengguna dapat menyimpan file tersebut kedalam *drive*.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3.5.7 Desain Logika Program

Desain logika program yang akan dikembangkan adalah sebagai berikut :

3.5.7.1 *Pseudocode Program*

Berikut ini adalah *pseudocode* program yang sedang dikembangkan pada penelitian ini :

Initialization
Password, Key, time, salt : string
Time <- get_time
Input <- password
Key <- salt+time

Encryption
New_vid <-LSB(Video, Chipertext)
Chipertext <- AES encrypt (password, key)
Output(Chipertext)

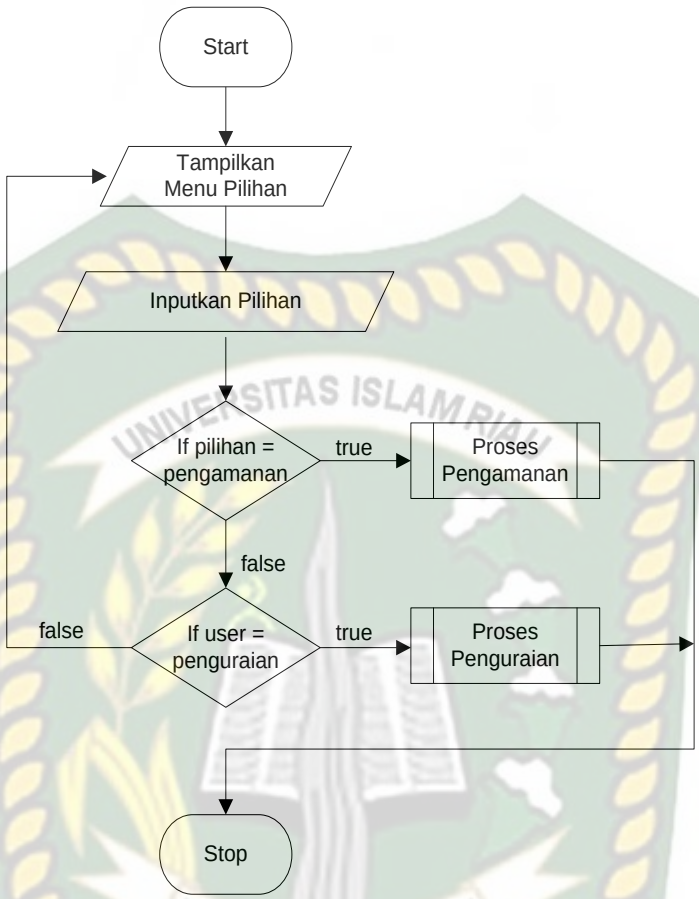
Decryption
(vid_orig, Chipertext)->LSB(new_vid)
Key <- salt- time
For much tolerance give time
    If key = get_time
        Key<-salt +time
        Palintext <-AES decrypt (Chipertext, key)
    End if
End for
Output(plaintext)

3.5.7.2 *Flowchart* Program

Adapun alur logika program digambarkan melalui *flowchart* berikut ini :

1. Flowchart Utama Program

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

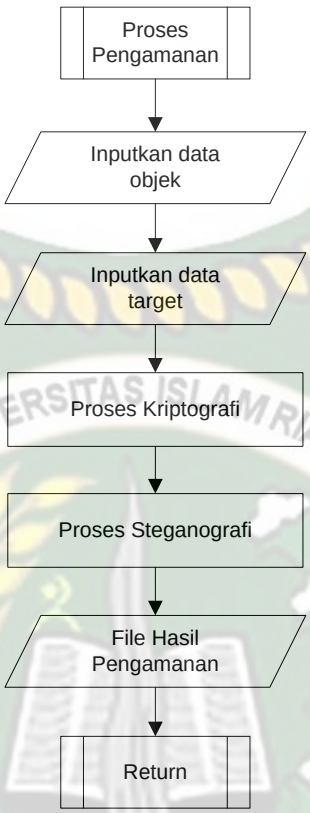


Gambar 3.11 Desain Logika Utama Program

Dari *flowchart* diatas dapat dilihat bahwa terdapat tampilan menu fitur, Pengguna dapat memilih fitur sesuai kebutuhan. Jika fitur yang dipilih adalah fitur pengamanan maka sistem akan melanjutkan k proses pengamanan file. Sedangkan jika fitur yang dipilih adalah fitur penguraian maka sistem dapat melanjutkan keproses penguraian file

2. Flowchart Pengamanan File

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

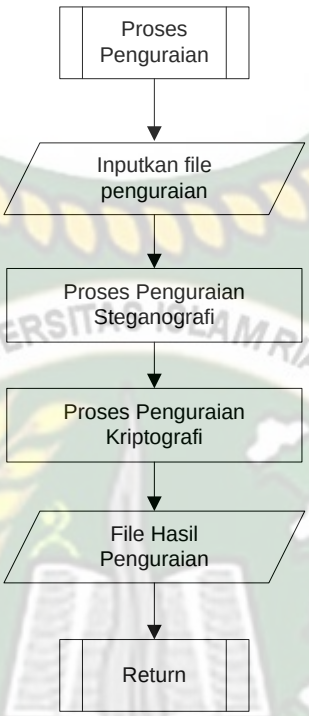


Gambar 3.12 *Flowchart* Pengamanan *File*

Gambar 3.12 adalah menu akses pengamanan file. Pada menu inipennguna menginputkan data target dan data objek. Selanjutnya sistem akan memproses file objek dengan proses kriptografi. Selanjutnya hasil kriptografi akan diproses kembali denganproses steganografi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

3. Flowchart Pengamanan File



Gambar 3.13 *Flowchart* Pengamanan *File*

Gambar 3.13 adalah menu akses untuk penguraia file yang diamankan sebelumnya. Pengguna akan meniputkan file yang akan diuraikan, kemudian sistem akan memproses file tersebut dengan proses penguraian steganografi terlebih dahulu. Setelah itu file objek akan diproses kembali dengan proses penguraian kriptografi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil Penelitian

Sebelum aplikasi yang dibangun dipublikasikan, ada beberapa tahapan yang harus dilakukan, hal ini dimaksudkan agar sewaktu aplikasi benar-benar sudah dipublikasikan tidak terjadi lagi kesalahan. Dalam pengujian sistem ini dilakukan dengan metode *black box*.

4.2 Pengujian *Black Box*

Pengujian *black box* (*black box testing*) adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada *input* dan *output* aplikasi.

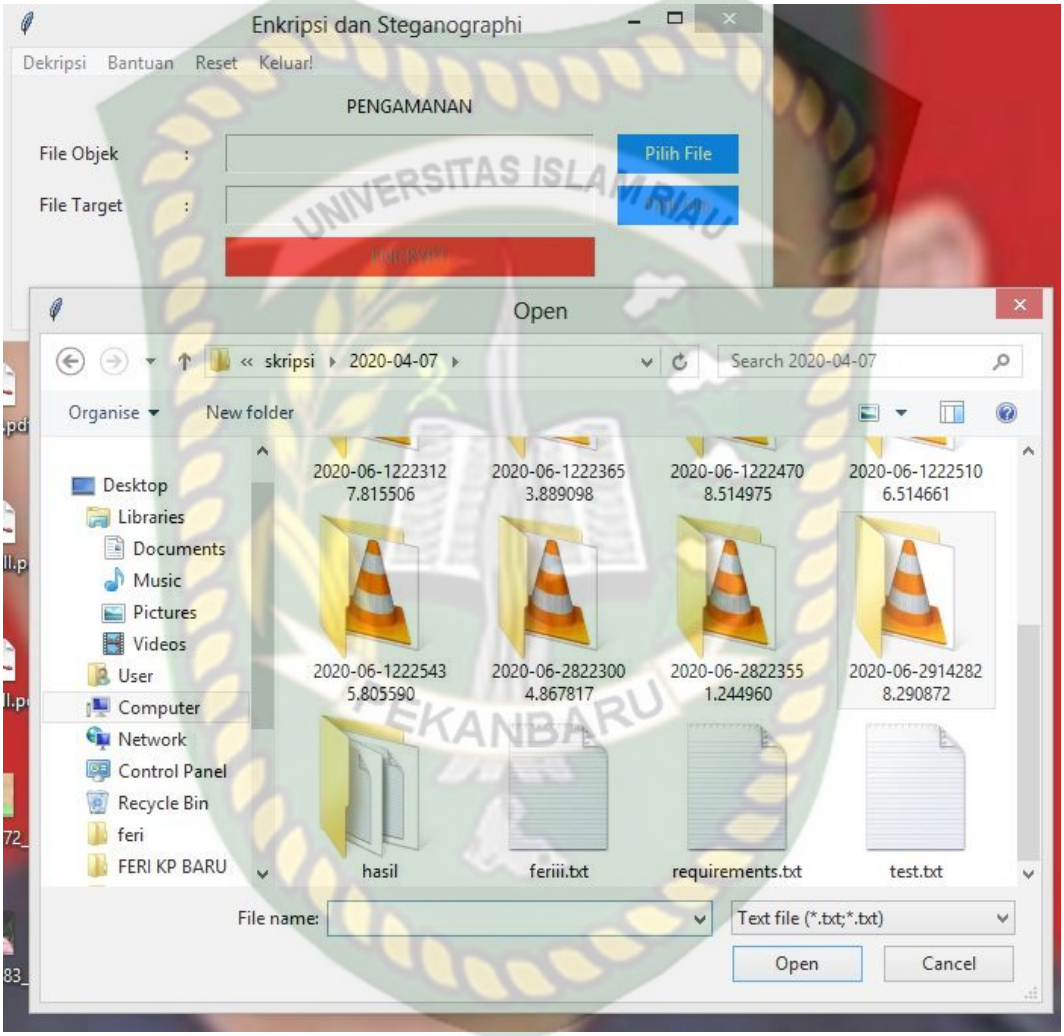
4.2.1 Pengujian *Black Box Form* Enkripsi

Gambar 4.1 Pengujian Menu Enkripsi

Pada gambar 4.1 dijelaskan bahwa ketika pengguna membuka menu enkripsi maka terdapat 2 field yang harus diisi. Field pertama adalah pilih file

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

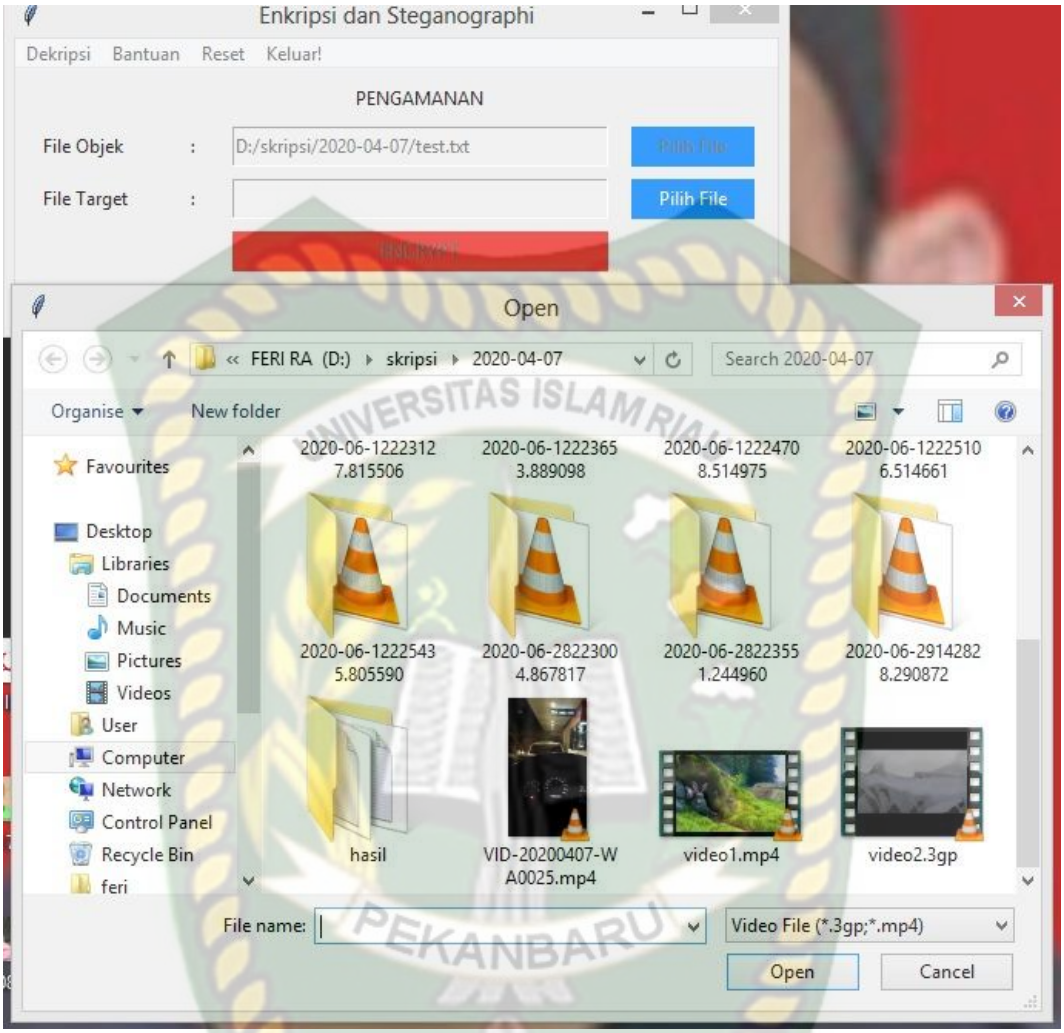
objek dan file yang kedua adalah pilih file target. File objek adalah file berektensi .txt yang akan disembunyikan. Sedangkan file target adalah file vidio tempat file objek akan disembunyikan.



Gambar 4.2 Pengujian Tombol Pilih *File* Objek

Pada gambar 4.2 dijelaskan bahwa ketika pengguna menekan tombol pilih file objek maka sistem akan membuka kotak dialog *mycomputer* dan menampilkan file berekstensi .txt untuk dapat dipilih sebagai file objek.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



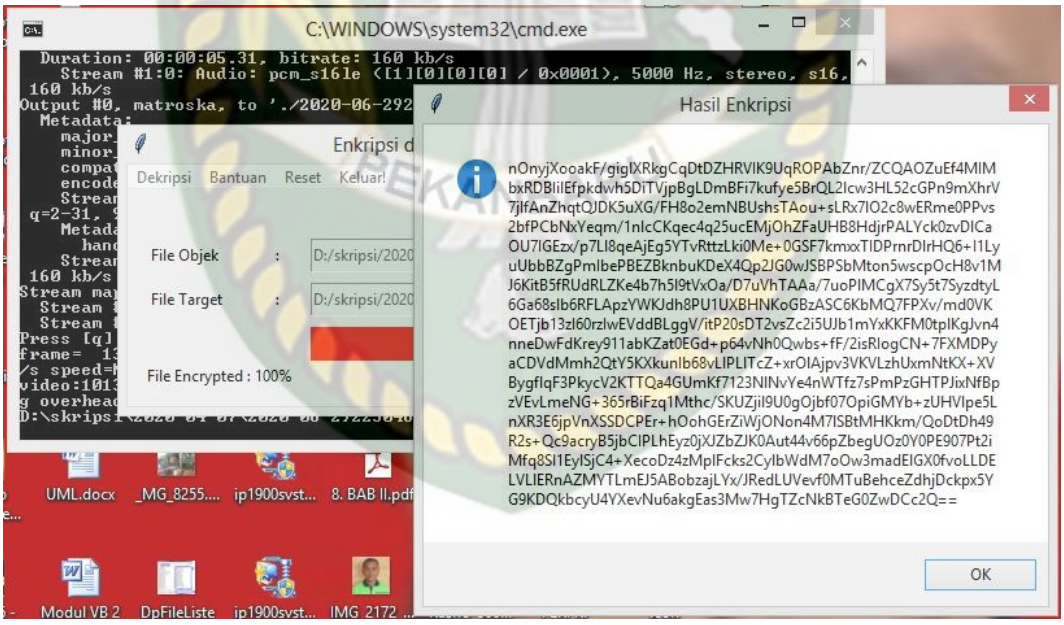
Gambar 4.3 Pengujian Tombol Pilih *File* Target

Pada gambar 4.3 dijelaskan bahwa ketika pengguna menekan tombol pilih file target maka sistem akan membuka kotak dialog *mycomputer* dan menampilkan file vidio untuk dapat dipilih sebagai file target.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

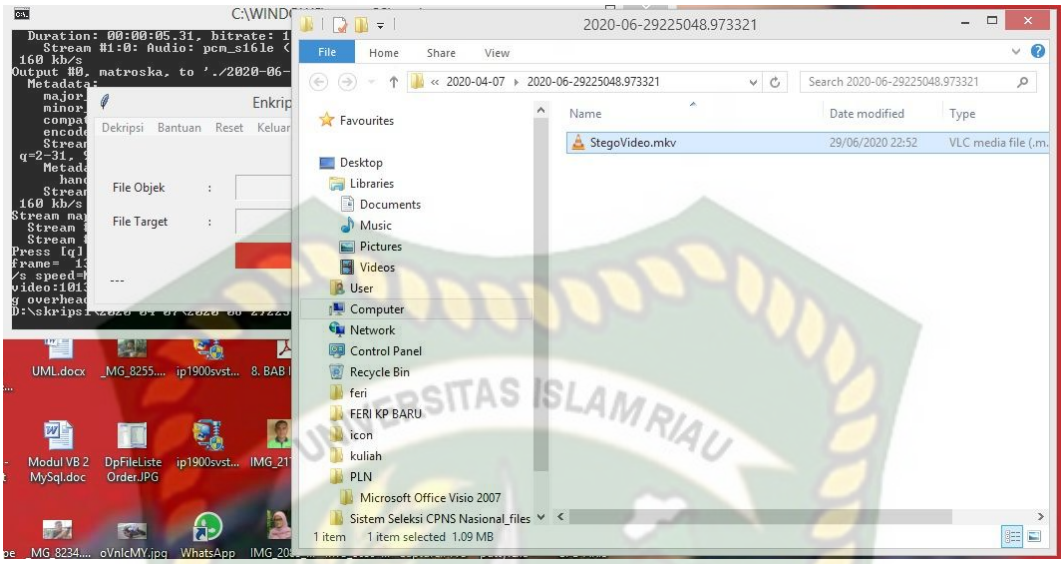
Gambar 4.4 Pengujian Tombol *Encrypt*

Pada gambar 4.4 dijelaskan bahwa ketika pengguna menekan tombol *Encrypt* maka sistem akan memunculkan kotak dialog agar pengguna dapat menginputka kata sandi.



Gambar 4.5 Pengujian Tombol *Encrypt(2)*

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.6 Pengujian Tombol *Encrypt(3)*

Setelah pengguna memasukan kata sandi, maka sistem akan memproses enkripsi file yang dapat dilihat digambar 4.5. Setelah itu sistem akan menyembunyikan file hasil enkripsi kedalam file vidio yang dapat dilihat pada gambar 4.6.

Tabel 4.1 Pengujian *Black Box Form* Enkripsi

No.	Komponen yang diuji	Skenario Penguji	Hasil yang diharapkan	Hasil
1.	Tombol Pilih File Objek	Menekan Tombol Pilih File Objek	Sistem akan menampilkan kotak dialog baru untuk memilih file yang diinginkan	[✓]Sesuai Harapan [ ] Tidak Sesuai Harapan
2.	Tombol Pilih File Target	Menekan tombol Pilih File Target	Sistem akan menampilkan kotak dialog baru untuk memilih file yang diinginkan	[✓]Sesuai Harapan [ ] Tidak Sesuai Harapan
3.	Tombol Enkripsi	Menekan Tombol Enkripsi	Sistem akan memunculkan kotak dialog untuk pengisian *keyword*	[✓]Sesuai Harapan [ ] Tidak Sesuai Harapan
4	Proses Enkripsi	Mengisi kata kunci	Sistem akan memproses enkripsi, lalu stegano. Memunculkan notifikasi	[✓]Sesuai Harapan [ ] Tidak Sesuai Harapan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

			hasil enkripsi dan memunculkan folder tempat stegano diletakan	

Berdasarkan pengujian yang telah dilakukan dapat ditarik kesimpulan bahwa dalam pengujian *black box* yang telah dilakukan terhadap sistem pada form enkripsi telah sesuai dengan harapan.

4.2.2 Pengujian *Black Box* Form Deskripsi

Gambar 4.7 Pengujian Menu Deskripsi

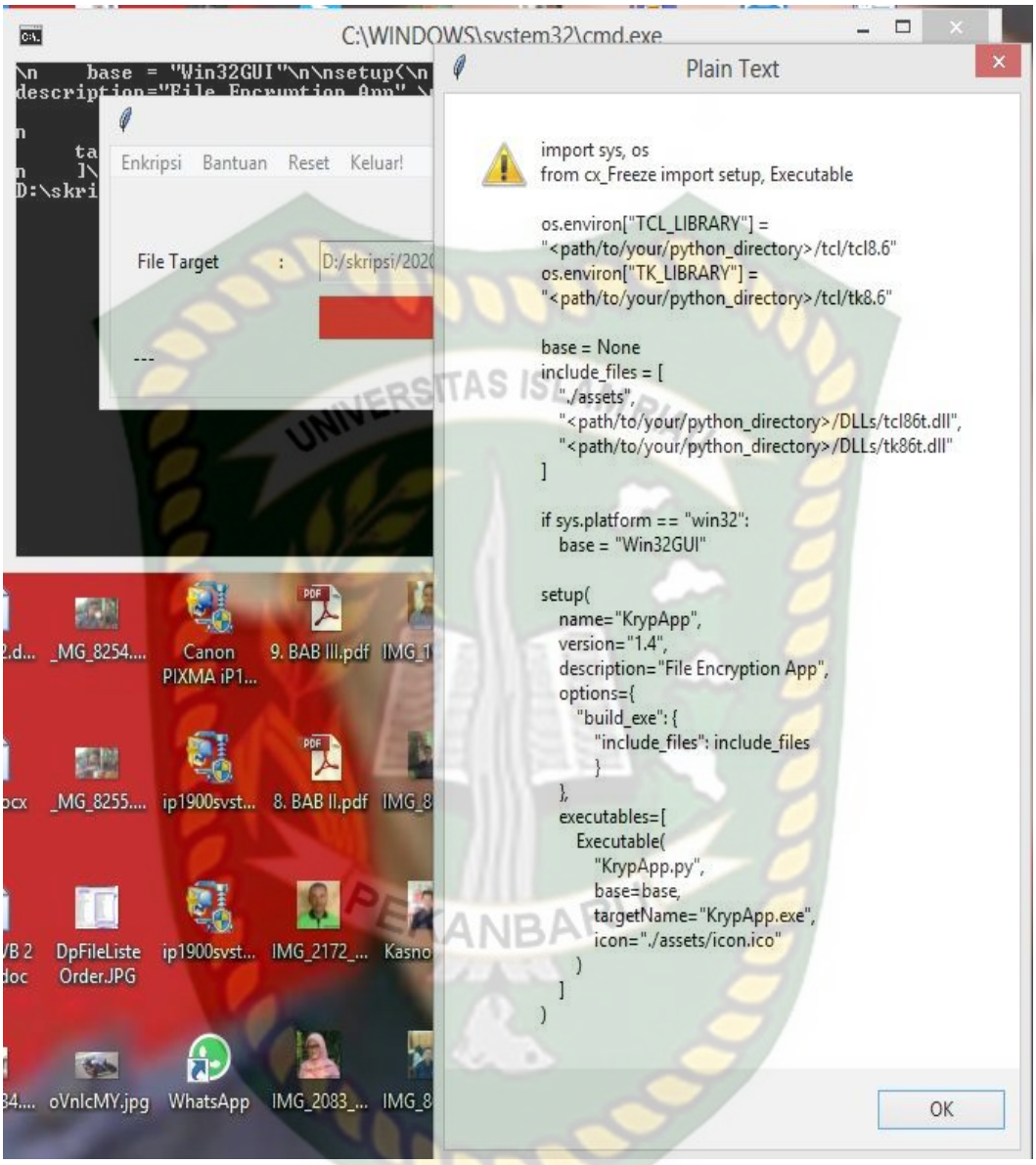
Pada gambar 4.7 dijelaskan bahwa ketika pengguna membuka menu deskripsi maka terdapat 1 *field* yang harus diisi yaitu pilih file. Ketika ditekan sistem akan memunculkan kotak dialog *mycomputer*. Penguna bisa memilih file yang akan diuraikan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Gambar 4.8 Pengujian Tombol Deskripsi

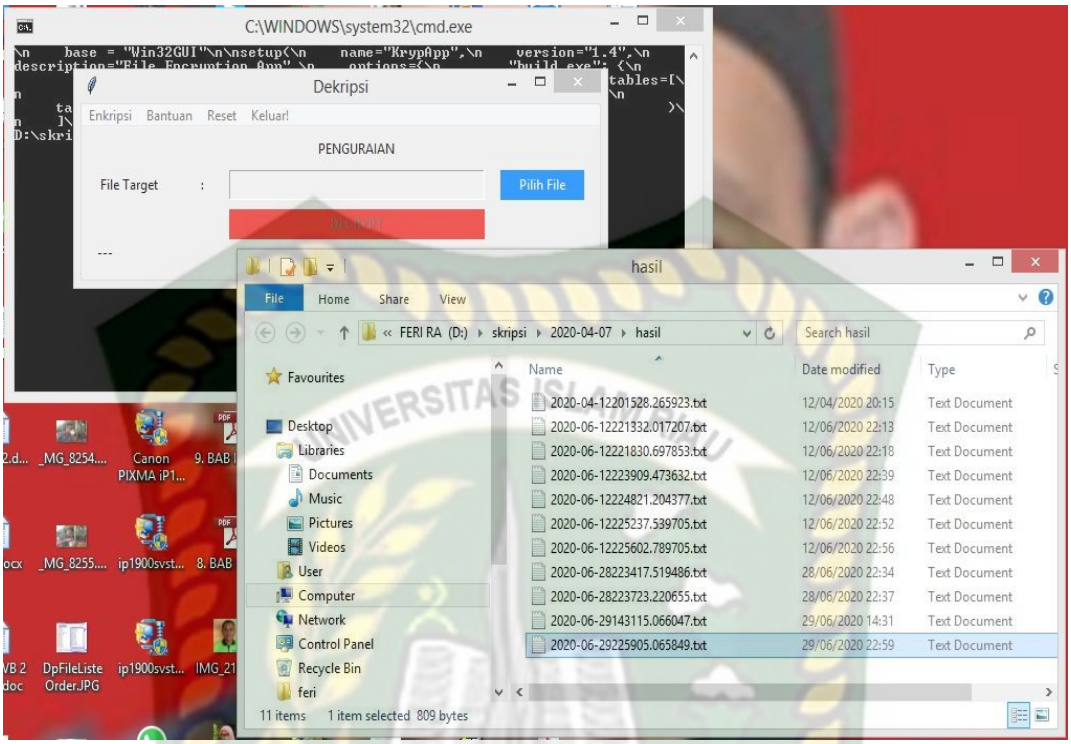
Pada gambar 4.8 dijelaskan bahwa ketika pengguna menekan tombol deskripsi sistem akan membuka kotak dialog dan meminta pengguna untuk mengisi keyword yang telah di set ketika melakukan enkripsi dan stegano file.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.9 Pengujian Proses Deskripsi

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.10 Hasil Penguraian

Pada gambar 4.10 dijelaskan bahwa setelah memasukan keyword yang tepat, sistem akan melakukan proses penguraian file stegano dan melakukan deskripsi. Kemudian akan muncul kotak dialog hasil penguraian. File hasil penguraian akan disimpan didalam folder yang telah ditentukan seperti gambar 4.10.

Tabel 4.2 Pengujian *Black Box Form* Deskripsi

No.	Komponen yang diuji	Skenario Penguji	Hasil yang diharapkan	Hasil
1.	Tombol Pilih File	Menekan Tombol Pilih File	Sistem akan menampilkan kotak dialog baru untuk memilih file yang diinginkan	[✓]Sesuai Harapan [ ] Tidak Sesuai Harapan
2.	Tombol Enkripsi	Menekan tombol Deskripsi	Sistem menampilkan kotak dialog dan meminta pengguna memasukan keyword	[✓]Sesuai Harapan [ ] Tidak Sesuai Harapan
3.	Keyword	Pengguna	Sistem melakukan	[✓]Sesuai Harapan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

		memasukan keyword yang sesuai	proses penguraian stegano dan deskripsi Kriptografi	[ ] Tidak Sesuai Harapan

Berdasarkan pengujian yang telah dilakukan dapat ditarik kesimpulan bahwa dalam pengujian *black box* yang telah dilakukan terhadap sistem pada form deskripsi telah sesuai dengan harapan.

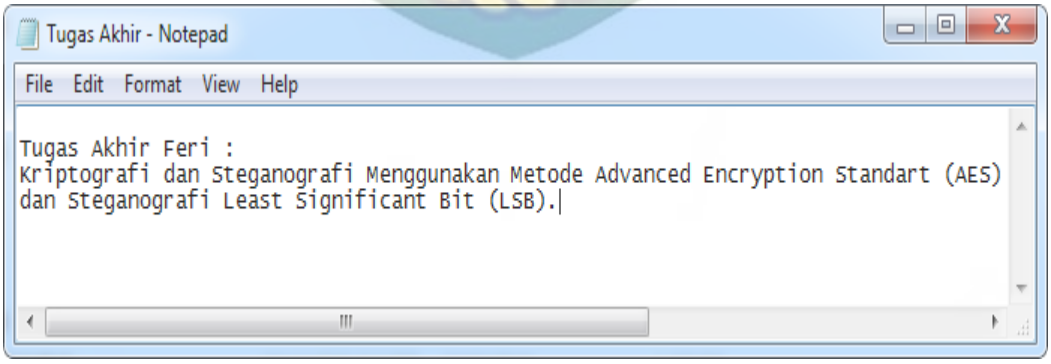
4.2.3 Kesimpulan Pengujian *Black Box*

Berdasarkan pengujian *black box* yang sudah di lakukan dapat di tarik kesimpulan bahwa setiap form dari Aplikasi Pengamanan *File* Menggunakan *Advanced Encryption Standard* dan *Least Significant Bit* sudah berjalan sesuai dengan yang di harapkan atau dapat di katakana 100% berjalan dengan sesuai fungsinya.

4.3 Hasil Kriptografi

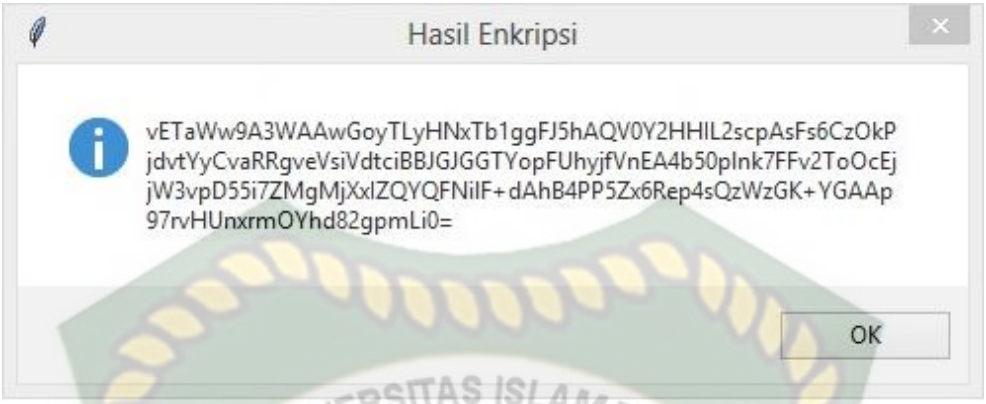
Berikut ini adalah hasil kriptografi/ ekripsi dari sistem yang sedang dibangun menggunakan metode *Advanced Encryption Standard* (AES):

Text Awal :



Gambar 4.11 *Text* Sebelum Enkipsi

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :



Gambar 4.12 *Text* Setelah di Enkripsi

Dari gambar 4.11 dan 4.12 diatas dapat dilihat tulisan pada file .txt sebelum dan sesudah dilakukan steganografi. JIka dilakukan deskripsi terhadap file yang telah di enkripsi maka akan menampilkan file asli sama seperti sebelum di enkripsi.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4.4 Waktu yang dibutuhkan Saat Implementasi Sistem

Berikut ini waktu yang dibutuhkan sistem dalam melakukan proses Kriptografi dan steganografi saat sistem dijalankan :

Tabel 4.3 Waktu yang dibutuhkan Untuk Proses Kripto dan Stagano

No	Nama File	Ukuran File	Nama Video	Ukuran Video	Durasi Video	Ukuran Video Setelah Stegano Dan Kripto	Waktu Eksekusi Program Saat Enkripsi (Detik)	Waktu Eksekusi Program Saat Dekripsi (Detik)	Ukuran Video Setelah Dekripsi	Ukuran File setelah Dekripsi
1	SourceCode.txt	13 KB	Video1	1.471 KB	0:00:52	1.622 KB	15.07 S	2 S	1.622 KB	13 KB
2	TextTest.txt	1 KB	Video1	1.471 KB	0:00:52	1.622 KB	12.21 S	1.9 S	1.622 KB	1 KB
3	TextTest.txt	1 KB	Video2	1.031 KB	0:00:05	1.119 KB	10.02 S	1.4 S	1.119 KB	1 KB
4	satu.txt	3.88 KB	andre	1.380 KB	0:01:00	1.707 KB	19.94 S	9.64 S	1.707 KB	4.KB
5	duaaa.txt	3.55 KB	andre	1.380 KB	0:01:00	1.707 KB	22.03 S	7.22 S	1.707 KB	4.KB
6	satu.txt	3.88 KB	Ikan	442 KB	0:00:30	727 KB	11.43 S	6.07 S	727 KB	4 KB
7	tigaa.txt	3.08 KB	Ikan	442 KB	0:00:30	727 KB	11.77 S	5.76 S	727 KB	4 KB
8	empaat.txt	9.27 KB	Asik	1.210 KB	0:00:57	1.594 KB	24.48 S	7.59 S	1.210 KB	10 KB
9	satu.txt	3.88 KB	Asik	1.210 KB	0:00:57	1.594 KB	16.37 S	5.89 S	1.210 KB	4 KB
10	TextTest.txt	1 KB	Tru	1.600 KB	0:00:30	2.205 KB	46.23 S	4.37 S	1.600 KB	1 KB
11	TextTest.txt	1 KB	Asik	1.210 KB	0:00:57	1.594 KB	15.87 S	4.82 S	1.210 KB	11 KB
12	satu.txt	3.88 KB	Video1	1.471 KB	0:00:52	1.622 KB	10.75 S	4.40 S	1.622 KB	4 KB

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

13	SourceCode.txt	13 KB	andre	1.380 KB	0:01:00	1.707 KB	12.40 S	5.45 S	1.707 KB	13 KB
14	duaaa.txt	3.55 KB	Asik	1.210 KB	0:00:57	1.594 KB	17.86 S	4.59 S	1.210 KB	4 KB
15	requiremen.txt	1 KB	sumatra	462 KB	0:00:31	735 KB	7.17 S	3.93 S	462 KB	1 KB

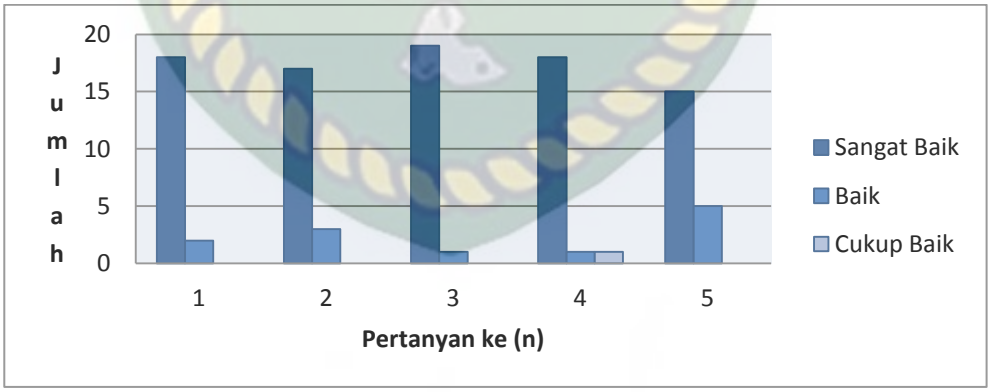
Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

4.5 Implementasi Sistem

Implementasi sistem yang dipakai adalah membuat kuisioner dengan 5 (lima) pertanyaan dan 20 koresponden yang mana ditujukan kepada personal yang dianggap intelektual. Kepada 20 koresponden diajukan pertanyaan yang terkait dengan kinerja dari aplikasi. Adapun kelima pertanyaan yang dimaksud adalah sebagai berikut :

1. Apakah informasi yang ditampilkan mudah dimengerti oleh user?
2. Bagaimana pendapat anda tentang tampilan aplikasi ini?
3. Apakah bahasa yang digunakan dalam aplikasi ini mudah dimengerti?
4. Apakah aplikasi cukup mudah untuk digunakan (dioperasikan)?
5. Menurut anda apakah aplikasi ini sudah layak dipublikasikan?

Dari pertanyaan-pertanyaan diatas, maka didapatkan hasil jawaban atau tanggapan dari koresponden terhadap kinerja dari sistem berdasarkan pertanyan yang diajukan disimpulkan dalam grafik yang terdapat pada gambar 4.12 :



Gambar 4.13 Grafik Hasil Kuisioner

4.6 Hasil Implementasi Sistem

Pada gambar 4.13 adalah grafik hasil kuesioner yang menunjukkan nilai untuk setiap pertanyaan-pertanyaan diatas adalah sebagai berikut :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

1. Apakah informasi yang ditampilkan mudah dimengerti oleh user memiliki nilai SANGAT BAIK : 18 koresponden, BAIK: 2 koresponden, CUKUP : 0 koresponden.
2. Bagaimana pendapat anda tentang tampilan aplikasi ini dimengerti memiliki nilai SANGAT BAIK : 17 koresponden, BAIK: 3 koresponden, CUKUP : 0 koresponden.
3. Apakah bahasa yang digunakan dalam aplikasi ini mudah dimengerti memiliki nilai SANGAT BAIK : 19 koresponden, BAIK : 1 koresponden, CUKUP : 0 koresponden.
4. Apakah aplikasi cukup mudah untuk digunakan (dioperasikan) memiliki nilai SANGAT BAIK : 18 koresponden, BAIK : 1 koresponden, CUKUP : 1 koresponden.
5. Menurut anda apakah aplikasi ini sudah layak dipublikasikan memiliki nilai SANGAT BAIK : 15 koresponden, BAIK : 5 koresponden, CUKUP : 0 koresponden.

4.7 Kesimpulan Pengujian Kuisioner

Berdasarkan hasil kuisioner tersebut maka dapat disimpulkan bahwa sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit* ini memiliki *persentase* sebagai berikut :

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

Tabel 4.4 Hasil Nilai Persentase Tiap Pertanyaan Kuisioner

No	Pertanyaan	Jumlah Persentase Koresponden		
		Sangat Baik	Baik	Cukup
1	Apakah informasi yang ditampilkan mudah dimengerti oleh user?	90%	10%	0%
2	Bagaimana pendapat anda tentang tampilan aplikasi ini?	85%	15%	0%
3	Apakah bahasa yang digunakan dalam aplikasi ini mudah dimengerti?	95%	5%	0%
4	Apakah aplikasi cukup mudah untuk digunakan (dioperasikan)?	90%	5%	5%
5	Menurut anda apakah aplikasi ini sudah layak dipublikasikan?	75%	25%	0%

Berdasarkan dari hasil persentase pada tabel 4.5 diatas, sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit* ini sudah sesuai dengan yang diharapkan, karena dari sistem yang dibangun memiliki *Performance* yang baik, *Performance* adalah kinerja atau nilai prestasi dari sistem yang di bangun, dengan nilai persentase kuisioner yang menyatakan Sangat Baik rata-rata sebesar 87%, sehingga aplikasi ini dapat diimplementasikan.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah melakukan penelitian, perancangan dan pengujian pada sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit,* maka dapat diambil kesimpulan sebagai berikut:

1. Telah berhasil membuat sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit*.
2. Berdasarkan hasil pengujian yang telah dilakukan dengan menggunakan *Black box,* sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit* ini sudah sesuai dengan yang di harapkan.
3. Berdasarkan hasil pengujian sistem yang dilakukan dengan metode kuisioner memiliki *performance* baik dengan nilai persentase rata-rata sebesar 87%.

5.2 Saran

Berdasarkan hasil penelitian, ada beberapa saran yang sebaiknya dilakukan guna pengembang sistem ini menjadi lebih baik, diantaranya sebagai berikut :

1. Dalam pengembangan sistem selanjutnya, sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit* dapat dikembangkan

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

menggunakan bahasa pemrograman *Android* agar bisa lebih mudah digunakan di perangkat *smartphone*.

2. Dalam pengembangan sistem selanjutnya, sistem pengamanan data menggunakan kriptorafi dan steganorafi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit* dapat diterapkan menggunakan algoritma selain AES dan LSB.
3. Dalam pengembangan sistem selanjutnya, sistem pengamanan data menggunakan kriptografi dan steganografi dengan metode *Advanced Encryption Standard* dan *Steganografi Least Significant Bit* dapat menggunakan file objek Ms. Office (Ms. Word, Ms. Power Point, Ms. Excel) yang disembunyikan kedalam file vidio.

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :

DAFTAR PUSTAKA

Andri Kristanto. 2017. *Perancangan Sistem Informasi dan Aplikasinya,* Gava Media, Yogyakarta.

A. Sadikin, Rifki., 2012, *Kriptografi untuk Keamanan Jaringan*. Yogyakarta.

Bonnie, Soeherman. 2016. *Designing Information System Concept & Cases with Visio,* PT Elex Media Komputindo, Jakarta.

Fitra, Muhammad, Syawal, dkk., 2016, *Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Chiper Dan Metode LSB,* Vol.4 No.3.

John Mc. Manama. 2014. *Design dan Perencanaan SistemInformasi,* Luxima, Jakarta.

Murdick, Robert, G, dan Joel, Ross, E., 2015, *Sistem Informasi untuk Manajemen Modern,* Erlangga, Jakarta.

Prayudi, Yudi dan Halik, Idham. 2005. *Studi dan Analisis Algoritma Rivest Code 6 Dalam Enkripsi/Dekripsi Data*. ISBN = 979-756-061-6.

Prasetyo , Tri, Utomo., 2012, *Steganografi Gambar dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online.*

Purba, Jhoni Verlando., Marihat, Situmorang, & Dedy, Arisandi. 2012. *Implementasi Steganografi Pesan Text ke Dalam File Sound (.Wav) dengan Modifikasi Jarak Byte pada Algoritma Least Significant Bit (LSB).*

Sutabri, Tata., 2012, *Konsep Dasar Informasi*. Andi, Yogyakarta,

Perpustakaan Universitas Islam Riau
Dokumen ini adalah Arsip Milik :