Pengamanan Dokumen Digital Perusahaan Menggunakan Metode Least Significant Bit (LSB) Dan Algoritma RC4 Stream Chipher

Handa Gustiawan[1)], Hesti Rian[2)*)]

[1)] Program Studi Sistem Informasi, Universitas Mohammad Husni Thamrin
[2)] Program Studi Manajemen Informatika, Politeknik LP3I Jakarta
Correspondence Author: hestiriangustiawan@gmail.com

DOI : https://doi.org/10.37012/jtik.v8i1.859

Abstrak

Pada era digital sekarang ini, dimana dokumen-dokumen perusahaan dibuat dalam bentuk digital maka Masalah keamanan dan kerahasiaan data atau dokumen merupakan salah satu aspek penting bagi perusahaan. Steganografi adalah suatu teknik untuk menyembunyikan pesan atau data rahasia di suatu tempat yang disebut carrier file. Sedangkan kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa gangguan pihak lain. Tujuan penelitian ini adalah memberikan pengamanan yang maksimal pada dokumen digital perusahaan, menggunakan metode steganografi Least Significant Bit (LSB) dan Algoritma kriptografi RC4 stream chipper. Hasil yang diharapkan dari penelitian ini adalah menghasilkan sebuah aplikasi yang dapat mengamankan dokumen digital perusahaan

Kata Kunci : steganografi, kriptografi, least significant bit, algoritma RC4

Abstract

In today's digital era, where company documents are made in digital form, the issue of security and confidentiality of data or documents is an important aspect for companies. Steganography is a technique to hide messages or secret data in a place called a carrier file. While cryptography is a science that studies how to keep data or messages safe when sent, from sender to recipient without interference from other parties. The purpose of this study is to provide maximum security for company digital documents, using the Least Significant Bit (LSB) steganography method and the RC4 stream cipher cryptographic algorithm. The expected result of this research is to produce an application that can secure the company's digital documents

Keywords : *Steganography, Cryptography, Least Significant Bit, RC4 Algorithm*

PENDAHULUAN

Teknologi informasi dan komunikasi telah berkembang pesat memberikan pengaruh yang besar bagi kehidupan manusia. Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Keamanan dan kerahasiaan merupakan aspek penting

yang dibutuhkan dalam proses pertukaran pesan atau informasi melalui jaringan/internet,karena turut berkembang pula kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan pesan atau informasi yang dikirimkan melalui jaringan/internet.

Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. RC4 merupakan salah satu jenis cipher aliran (*stream cipher*), didesain oleh Ron Rivest di Laboratorium RSA (RSA Data Security Inc.) pada tahun 1987. Cipher RC4 merupakan teknik enkripsi yang dapat dijalankan dengan panjang kunci yang variabel dan memproses data dalam ukuran byte.

Teknik lain yang dapat digunakan yaitu steganografi. Steganografi adalah seni dan ilmu untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Berbeda dengan kriptografi yang merahasiakan makna pesan namun keberadaan pesan tetap ada, steganografi merahasiakan dengan menutupi atau menyembunyikan pesan.

Steganografi menyisipkan atau menyembunyikan pesan di dalam sebuah gambar (covertext), agar pihak lain tidak menyadari keberadaan informasi yang ada di dalam gambar tersebut. Steganografi menjadikan gambar stego (stegotext) dalam bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut sebatas kemampuan indera manusia secara visual, artinya mata manusia tidak dapat mem-bedakan gambar stego dengan gambar asli yang tidak memiliki pesan di dalamnya.

Salah satu metode steganografi adalah *Least Significant Bit* (LSB), dengan teknik penyembunyian pesan pada lokasi bit terendah dalam Dokumen Digital. Pesan dikonversi ke dalam bentuk bit biner dan disembunyikan pada dokumen digital dengan metode LSB. Implementasi metode LSB tanpa dilengkapi dengan sistem keamanan berpeluang untuk dapat dibongkar dengan mudah melalui teknik pemecahan analisis frekuensi dengan membaca bit terendah.

Steganografi dapat dipandang sebagai kelanjutan kriptografi, terkait dengan fungsi stegokey sebagai kunci untuk proses enkripsi/dekripsi. Pesan rahasia dienkripsi dengan kunci lalu disembunyikan dalam citra, dan pesan rahasia dapat diekstraksi dan didekripsi

kembali persis sama seperti aslinya dengan menggunakan kunci yang sama. Kombinasi kriptografi dan steganografi dapat memberikan keamanan pada pesan rahasia. Pesan rahasia terlebih dahulu dienkripsi dengan algoritma RC4, kemudian cipherteks hasil kriptografi tersebut disembunyikan di dalam media gambar/citra dengan metode steganografi.

LANDASAN TEORI

Keamanan Data

Keamanan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan maupun individu (pribadi). Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Dalam hal ini sangat terkait betapa pentingnya informasi tersebut dikirim dan diterima oleh yang berkepentingan. Informasi akan tidak berguna lagi apabila ditengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak. Pada tema yang kita bahas kali ini adalah pengamanan dokumen dokumen perusahaan dengan menambahkan keterangan tersembunyi pada dokumen digital perusahaan.

Secara umum keamanan computer mencakup beberapa aspek [4], yaitu :

1. Privacy / Convidentialyty

Keutamaan aspek ini digunakan untuk menjaga informasi dari orang yang tidak berhak untuk mengakses.*Privacy* lebih kearah data-data yang sifatnya privat, sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu

2. Integrity

Aspek ini menekan bahwa informasi tidak boleh diubah tanpa seizing pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat informasi yang dikirim, jika terdapat perbedaan antara informasi atau data yang dikirim dengan yang diterima maka aspek *integrity* tidak tercapai.

3. Authenticity

Aspek ini menggambarkan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah benar-benar yang dimaksud atau ditunjuk.

4. Availability

Hal ini berhubungan dengan ketersediaan data dan informasi artinya data dan informasi yang berbeda dalam suatu system computer tersedia dan dapat dimanfaatkan oleh orang yang berhak.

5. Access Control

Aspek ini berhubungan dengan cara pengaturan informasi, hal ini biasanya dihungkan dengan hal klarifikasi data. Akses control seringkali dilakukan dengan menggunakan kombinasi *user id / password* atau dengan menggunakan mekanisme lain. Dengan cara ini maka setiap *user* akan dibatasi sesuai dengan tingkat kebutuhannya.

Steganografi

Steganografi berasal dari bahasa Yunani, *"Stegos"* yang berarti *roof* (atap) atau *covered* (terlindungi) dan *"graphia"* yang bererti tulisan, jadi steganografi berarti "tulisan tersembunyi. Steganografi adalah ilmu dan seni menyembunyikan data atau pesan didalam media lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui [3], Secara garis besar, teknik steganografi adalah cara menyisipkan sepotong demi sepotong informasi pada sebuah media, sehingga informasi tersebut tampak kalah dominan dengan media pelindungnya.

Terdapat beberapa istilah berkaitan dengan steganografi :

a. *Hiddentext* atau *embed message* yaitu pesan yang disembunyikan.

b. *Convertext* atau *cover-objek* yaitu media yang digunakan untuk menyembunyikan *embed message.*

c. *Stegotext* atau *stego-objek* yaitu media yang sudah berisi *embed message*.

Kriteria Steganografi

Penyembunyian data rahasia ke dalam dokumen digital akan mengubah kualitas citra tersebut. Kreteria yang harus diperhatikan dalam penyembunyian data adalah [3]:

1. *Imperceptibility*. Keberadaan pesan rahasia tidak dapat dipersepsi oleh inderawi, misalnya jika *convertext* berupa citra, maka penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext* nya, jika *covertext* berupa audio (misal : MP3, wav, midi dan lain-lain) maka indera pendengaran (telinga) tidak dapat mendeteksi perubahan pada audio *stegotext*nya.

2. *Fidelity*. Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan tersebut tidak dapat dipersepsikan oleh inderawi.

3. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*reval*). Karena tujuan steganografi adalah data *hiding*, maka sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut.

Metode Least Significant Bit (LSB)

Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan dokumen digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Sebagai contoh byte

11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut. Misalkan segmen pixel-pixel citra/gambar sebelum penambahan bit-bit adalah:

00110011 10100010 11100010 10101011 00100110

10010110 11001001 11111001 10001000 10100011

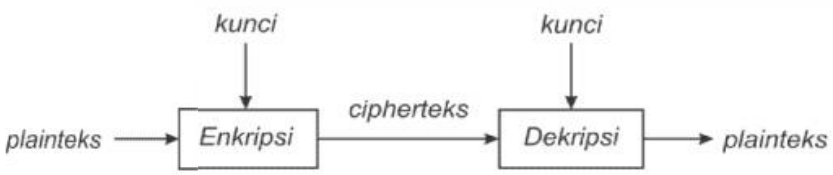
Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen pixel-pixel citra menjadi (digarisbawahi):

00110011 10100011 11100011 10101010 00100110

10010111 11001000 11111001 10001001 10100011

Kriptografi

Kriptografi (cryptography) berasal dari Bahasa Yunani: "cryptos" artinya "secret" (rahasia), sedangkan "graphein" artinya "writing" (tulisan), sehingga kriptografi berarti "secret writing" (tulisan rahasia). Kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi memiliki dua konsep utama, yaitu enkripsi (encryption) dan dekripsi (decryption). Enkripsi adalah proses penyandian plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi. Gambar 2.1 memperlihatkan skema enkripsi dan dekripsi dengan menggunakan kunci.



Gambar 1. Skema enkripsi dan dekripsi.

Kriptografi terbagi menjadi 2 (dua) yaitu:

1. Kriptografi klasik (mode karakter):

a. Cipher Substitusi

b. Cipher Transposisi

2. Kriptografi modern (mode bit/binary):

a. Cipher kunci simetri: cipher aliran (stream cipher), cipher blok (block cipher)

b. b. Cipher kunci publik (public key cryptography)

RC4 (*Rivest Code 4*)

RC4 atau *Rivest Code 4* dibuat oleh Ron Rivest di Laboraturium RSA pada tahun 1987[2]. RC4 adalah salah satu jenis *stream cipher* yang sinkron yaitu cipher yang

memiliki kunci simetris dan mengenkripsi atau mendekripsi plainteks secara digit per digit atau bit per bit dengan cara mengkombinasikan secara operasi biner (biasanya operasi XOR) dengan sebuah angka semiacak. RC4 dapat dijalankan dengan panjang kunci variabel dan beroperasi dengan orientasi byte.

Metode enkripsi RC4 memiliki kelemahan. Kelemahan yang paling dikenal adalah Bit-Flipping Attack atau BFA di mana penyerang dapat mengetahui sample atau keseluruhan plainteks dari cipherteks tanpa harus mengetahui kunci enkripsi. Walaupun punya banyak kelemahan, tetapi metode enkripsi RC4 saat ini masih menjadi metode enkripsi yang banyak digunakan. RC4 saat ini masih diaplikasikan pada pengenkripsian PDF, pengamanan WEP, dan SSL.

RC4 adalah salah satu bentuk stream cipher yang banyak digunakan pada protokol-protokol enkripsi, antara lain WEP, WPA, dan SSL/TSL.Dikemukakan oleh Ron Rivest (salah satu penggagas RSA) pada tahun 1987.Algoritma ini berjalan berdasarkan prinsip permutasi acak.

Teknik Penyimpanan Data

Teknik penyisipan data ke dalam *covertext* dapat dilakukan dalam dua macam ranah :

1. Ranah spasial (waktu) (*spatial/time domain*) Teknik ini memodifikasi langsung nilai *byte* dari *corverter* (nilai *byte* dapat mempresentasikan intensitas / warna pixel atau amplitude). Contoh metode yang tergolong ke dalam teknik ranah spasial adalah metode LSB

2. Ranah transform (transform domain) Teknik ini memodifikasi langsung hasil transformasi frekuensi sinyal. Contohnya metode yang tergolong ke dalam teknik ranah frekuensi adalah *spread spectrum.*

Pengenalan PHP

PHP (akronim dari PHP: Hypertext Preprocessor) adalah bahasa pemrograman yang berfungsi untuk membuat website dinamis maupun aplikasi web[4]. Berbeda dengan HTML yang hanya bisa menampilkan konten statis, PHP bisa berinteraksi dengan database, file dan folder, sehingga membuat PHP bisa menampilkan konten yang dinamis dari sebuah website. Blog, Toko Online, CMS, Forum, dan Website Social Networking adalah contoh

aplikasi web yang bisa dibuat oleh PHP. PHP adalah bahasa scripting, bukan bahasa tag-based seperti HTML. PHP termasuk bahasa yang cross-platform, ini artinya PHP bisa berjalan pada sistem operasi yang berbeda-beda (Windows, Linux, ataupun Mac). Program PHP ditulis dalam file plain text (teks biasa) dan mempunyai akhiran ".php".

PHP ditulis (diciptakan) oleh Rasmus Lerdorf, seorang software engineer asal Greenland sekitar tahun 1995. Pada awalnya PHP digunakan Rasmus hanya sebagai pencatat jumlah pengunjung pada website pribadi beliau. Karena itu bahasa tersebut dinamakan Personal Home Page (PHP) Tools. Tetapi karena perkembangan nya yang cukup disukai oleh komunitas nya, maka beliau pun merilis bahasa PHP tersebut ke publik dengan lisensi open-source. Saat ini, PHP adalah server-side scripting yang paling banyak digunakan di website-website di seluruh dunia, dengan versi sudah mencapai versi 5 dan statistiknya terus bertambah (www.php.net/usage.php).

METODE PENELITIAN

Metode Pengumpulan Data

1. Studi kasus

Dilakukan dengan cara membaca dan mempelajari buku – buku dan artikel yang berhubungan dengan keamanan data khusunya tentang steganografi, serta buku – buku yang mendukung dengan topic yang akan dibahas dalam penyusunan makalah ini.

2. Literature

Menggunakan beberapa jurnal dan makalah yang terkait dengan keamanan data khusunya steganografi dan teknik signatur digital sebagai refrensi bagi penulis.

3. Diskusi

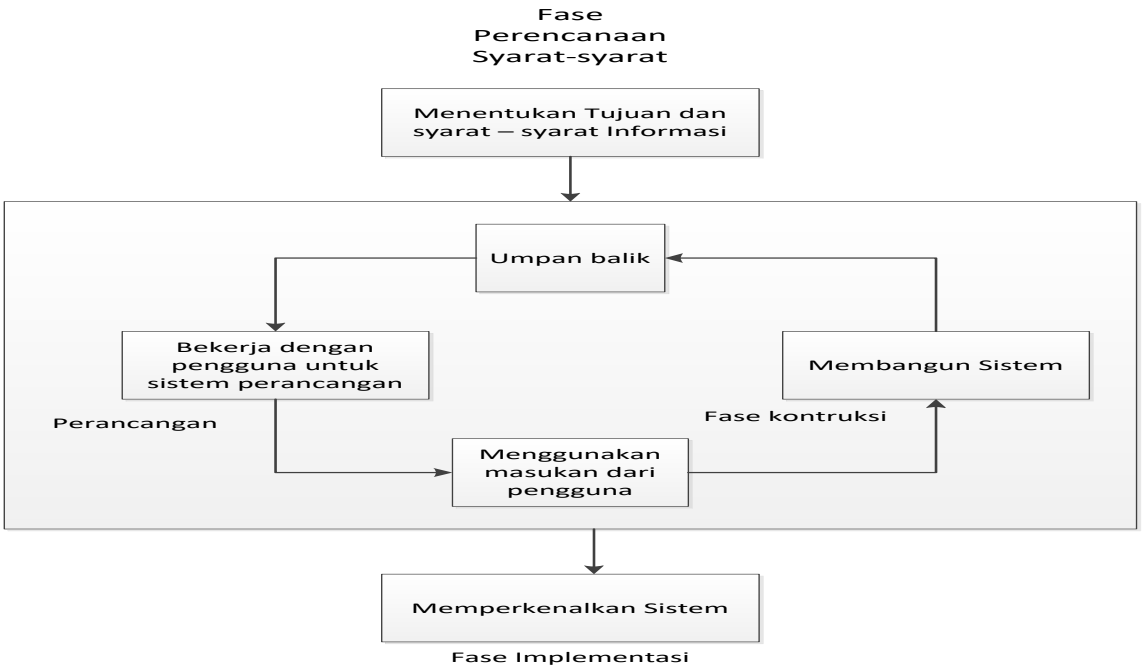
Melakukan diskusi dengan dosen dan teman – teman serta orang – orang yang mengerti terhadap materi bahasan agar mendapatkan bahan masukan untuk penyusunan makalah ini.

Metode Pengembangan Sistem

Pengembangan system dalam penelitian ini penulis lakukan menggunakan tiga tahap siklus pengembangan model RAD (Rapid Aplication Development), yaitu fase perencanaan

syarat, fase workshop desain (perancangan dan konstruksi) dan fase implementasi. Model RAD yaitu suatu pendekatan berorientasi objek terhadap pengembangan system yang mencakup suatu metode pengembangan perangkat-perangkat lunak. Tujuannya mempersingkat waktu pengerjaan aplikasi serta proses yang dihasilkan didapatkan secara cepat dan tepat

Kendall (2003:327) mengilustrasikan model RAD seperti gambar dibawah ini :

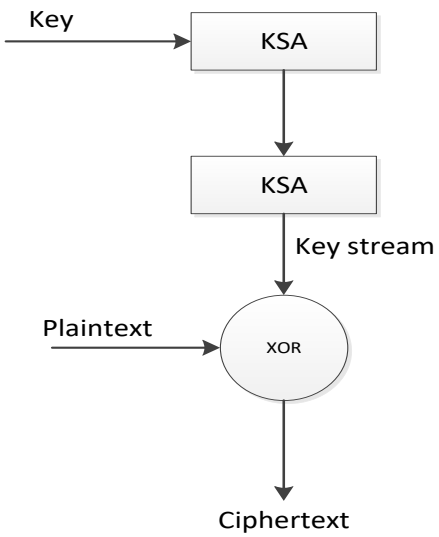


Gambar 2. Siklus pengembangan system model RAD

RC4 (Rivest Code 4)

RC4 (Rivest Code 4) merupakan suatu algoritma enkripsi *stream cipher* dan *symmentic key*, dimana algoritma ini melakukan proses enkripsi / deskripsi *one byte at a time* dan menggunakan kunci yang sama.

Algoritma RC4 terdiri dari 2 bagian yaitu *Key Scheduling Algoritm* (KSA) dan *Pseudo Random Generation Algorithm* (PRGA).



Gambar 3. Blok Diagram Algoritma RC4

Dari uraian diatas, maka metode penelitian yang dilakukan adalah merancang bangun perangkat lunak aplikasi enkripsi RC4 dengan menggunakan Visual Basic Ver.6 dan menganalisa proses dari KSA dan PRGA hingga mendapatkan hasil enkripsi (*ciphertext*) yang diinginkan.

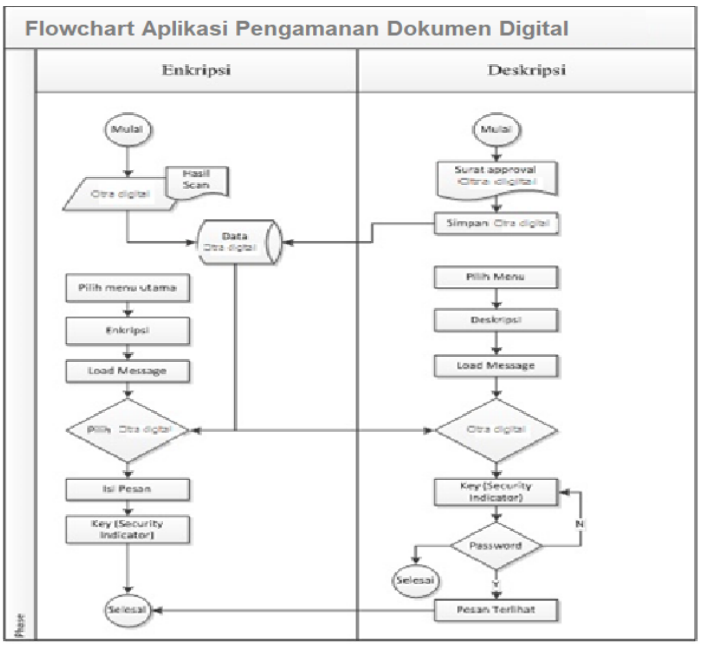
Perancangan Sistem

Sistem pengamanan dokumen digital yang dibahas akan di fokuskan kepada bagaimana cara membangun suatu sistem steganografi pada *dokumen digital* sebagai file otentik yang tidak dilakukan pemalsuan dalam surat yang sudah di *approval*.

Sistem penyisipan informasi atau pesan berfungsi untuk melakukan proses penyembunyian pesan ke file dokumen digital gambar. Komponen dari sistem penyisipan ini yaitu terdapat komponen untuk menuliskan pesan yang dipakai untuk menempatkan penulisan pesan rahasia.

Flowchart

Berikut adalah bagan alir / flowchart Aplikasi steganografi pengamanan dokumen digital dengan metode RC4 (Rivest Code 4):

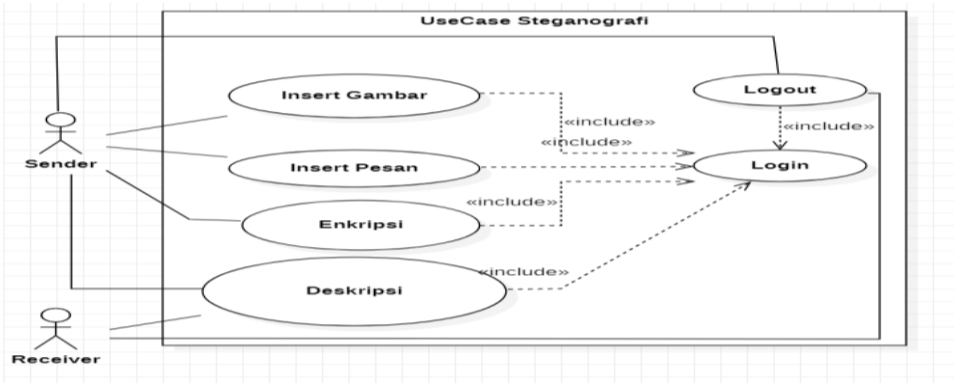


Gambar 4. Flowchart Steganografi Dokumen digital Gambar

Dari flowchart diatas terlihat proses pembuatan pesan steganografi dengan menyisipkan pesan kedalam *Dokumen Digital*, dan mengestrak *dokumen digital* berpesan dengan sebuah aplikasi steganografi.

Use Case Diagram

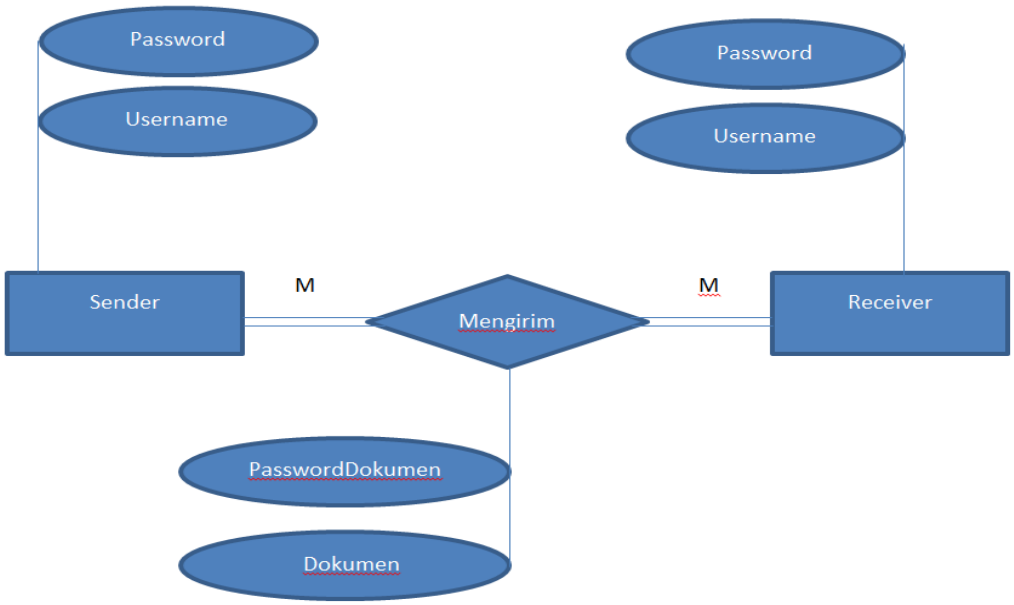
Berikut adalah Use Case Diagram sistem steganografi :



Gambar 5. Use Case Diagram Aplikasi Steganografi

Entity Relational Diagram (ERD)

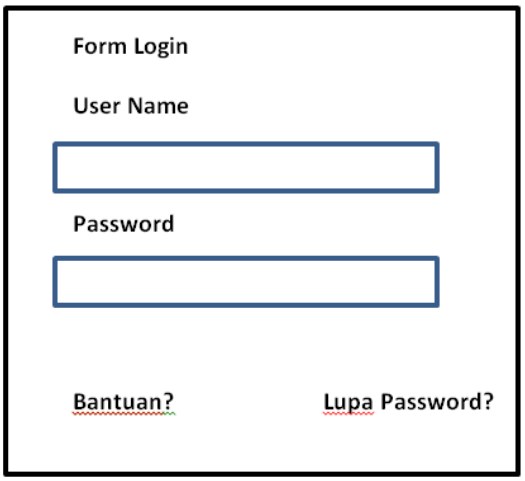
Berikut adalah ERD aplikasi steganografi :



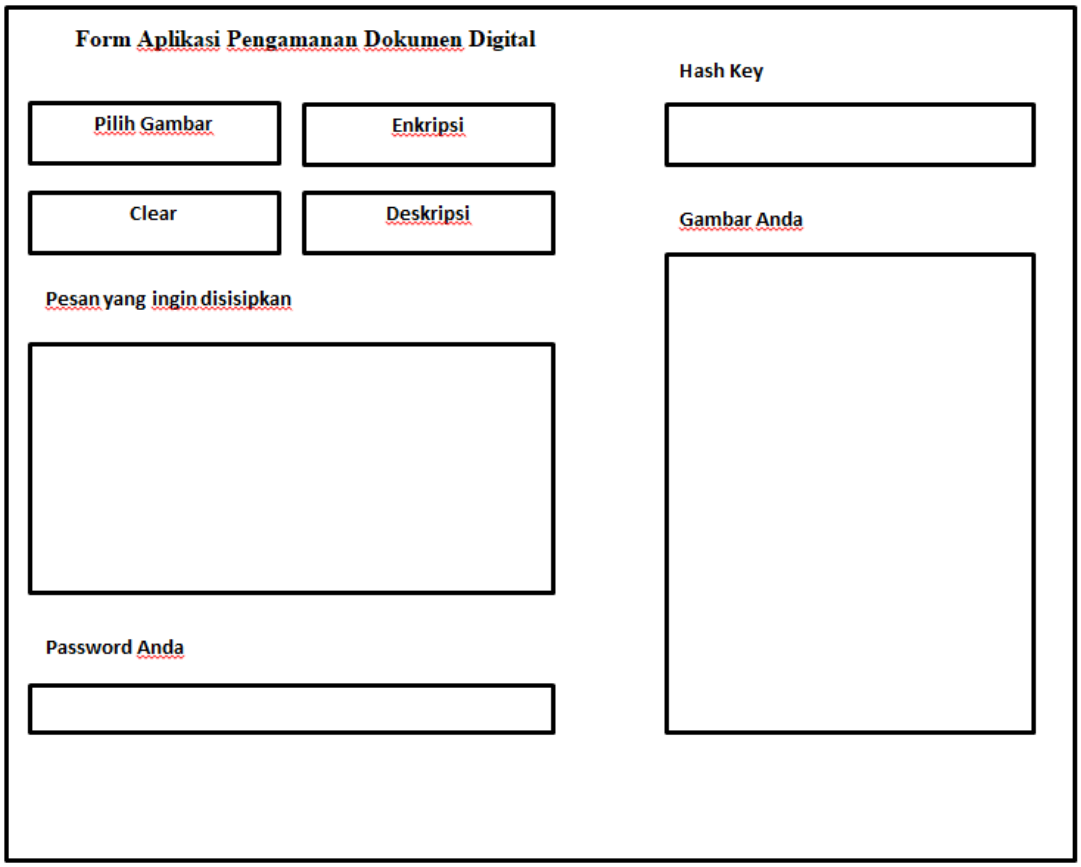
Gambar 6. Entity Relational Diagram Aplikasi Steganografi

User Interface

Berikut Perancangan User Interface aplikasi steganografi :



Gambar 7. Perancangan User Interface Form Login Aplikasi Steganografi



Gambar 8. Perancangan User Interface Form Aplikasi Aplikasi Steganografi

Implementasi Dan Pengujian Sistem

Implementasi Sistem

Untuk mengimplementasikan jurnal yang dibuat maka diperlukan beberapa komponen yang digunakan sebagai pendukung penelitian, diantaranya :

Rancangan Perangkat Sistem

Perangkat Keras (Hardware)

Spesifikasi minimal hardware/ komputer yang diusulkan untuk mengoperasikan Aplikasi ini adalah sebagai berikut :

1. Prosesor Core i7
2. Harddisk 1 TB (Secukupnya)
3. Memory RAM 8 GB

4. Perangkat pendukung keluaran (monitor)

5. Perangkat masukan (keyboard, mouse)

6. Scanner

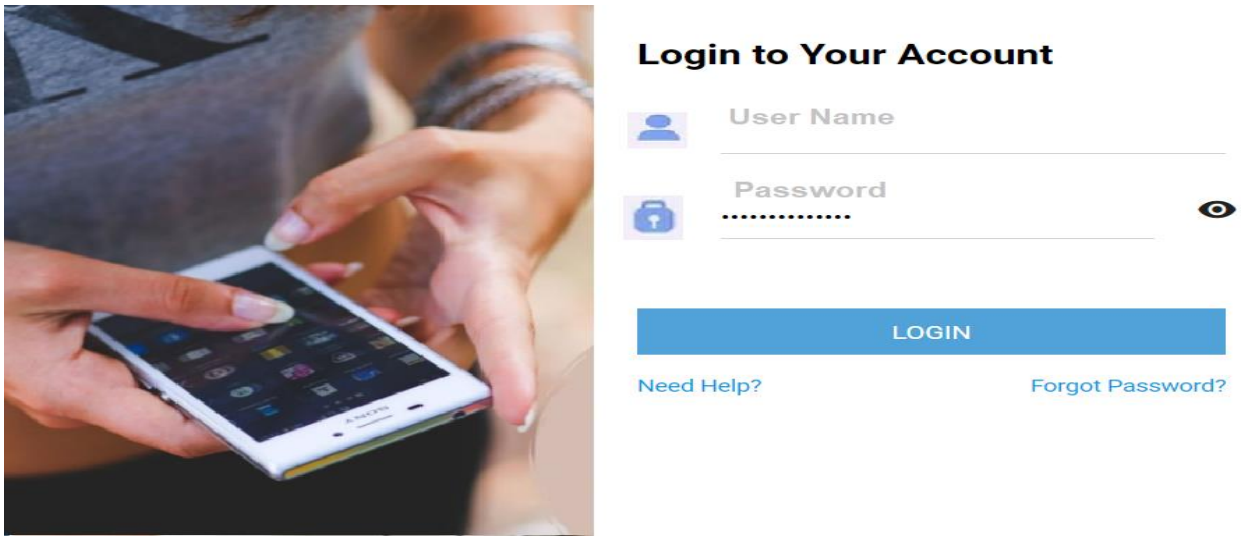
Perangkat Lunak (Software)

1. Windows 10

2. Bahasa pemrograman yang digunakan pada aplikasi steganografi ini adalah dibuat menggunakan bahasa pemrograman PHP

3. Adobe Acrobat Pro (Software untuk membuka File Pdf)

Rancangan Interface Aplikasi



Gambar 9. Form Login Aplikasi Pengamanan Dokumen Digital

Gambar 10. Form Aplikasi Pengamanan Dokumen Digital

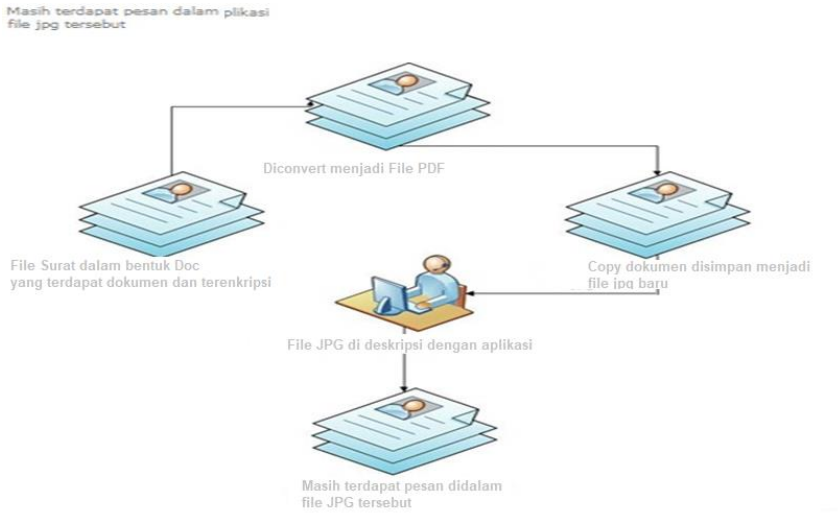
Menu aplikasi terdiri dari :

1. Gambar menu ini digunakan untuk memilih dokumen digital perusahaan yang tersedia untuk dienkripsi atau untuk dideskripsi.
2. Enkripsi menu ini digunakan untuk memasukan pesan pada Dokumen Digital.
3. Deskripsi menu ini digunakan untuk mengextract pesan yang telah dimasukan ke dalam Dokumen Digital.
4. Clear menu ini digunakan untuk membersihkan layar.

Pengujian Sistem

Pengujian Keaslian Dokumen

Cara yang dilakukan untuk pengujian keaslian file Dokumen Digital, penulis membuat file surat dalam bentuk file document(.doc) yang disisipkan file dokumen digital yang telah di enkripsi, kemudian file tersebut di rubah menjadi file pdf. Dari file pdf tersebut dokumen digital di copy dan disimpan dengan nama file jpg, kemudian di Deskripsi apakah pesan yang dibuat masih ada atau tidak. Gambaran pengujian sistem digambarkan dalam gambar berikut.



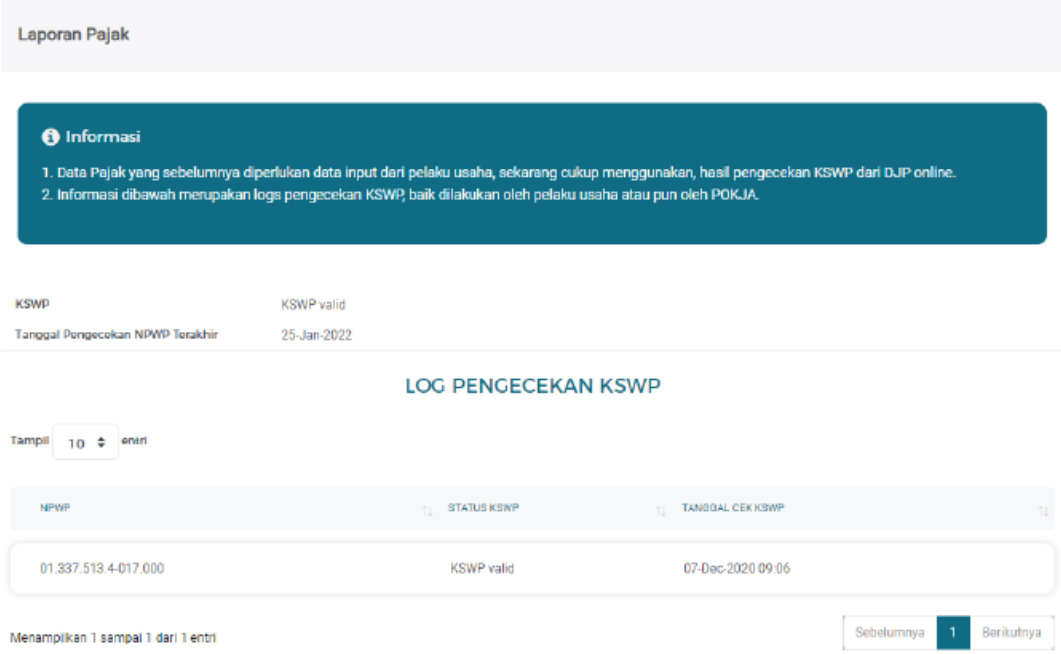
Gambar 11. Pengujian Aplikasi

Pengujian File yang telah dienkripsi

Pengujian yang dilakukan adalah memasukan beberapa file jpg dengan ukuran file yang berbeda kemudian dilakukan perbandingan antara file yang telah di enkrip dan yang belum di enkrip.

Tabel 1. Hasil Pengujian Ukuran File

Nama File	Ukuran awal	Ukuran Akhir	Status
Dokumen 1	105 Kb	105 Kb	OK
Dokumen 2	103 Kb	103 Kb	OK



Gambar 12. Gambar Pengujian file

Dari Data diatas diketahui bahwa enkripsi dengan menggunakan algoritma RC4 tidak ada perubahan dalam ukuran file.

Hasil Pembahasan

Algoritma RC4

a. *Key scheduling* Algoritma

Proses KSA melakukan pemberian nilai inisialisasi pada frame password & Security indicator dan selanjutnya melakukan proses permutasi sebanyak 256 iterasi.

b. *Pseudo Random Generation Algorithm* (PRGA)

Tabel Frame Password & Security Indicator hasil dari proses KSA digunakan lagi dalam proses PRGA ini untuk menghasilkan key stream yang akan di XOR kan dengan image untuk menghasilkan ciphertext.

Proses untuk menghasilkan key stream dilakukan proses permutasi pada Frame Password & Security Indicator berdasarkan nilai iterasi yang diambil secara random

```
i = 0
j = 0
For x= 1 To Len(inp)
i = (i + 1) Mod 256
j = (j + S(i)) Mod 256
temp = S(i)
S(i) = S(j)
S(j) = temp
t = (S(i) + (S(j) Mod 256)) Mod 256
Y = S(t)
Outp = Outp & Chr(Asc(Mid(inp,x,1))Xor Y)
Next
cRC4 = Outp
```

KESIMPULAN DAN REKOMENDASI

Berdasarkan metode yang digunakan dalam pembuatan aplikasi steganografi pengamanan dokumen digital dengan metode RC4 (Rivest Code 4) menggunakan bahasa pemrograman PHP dapat digunakan untuk membuat atau menyisipkan informasi atau pesan rahasia didalam file Dokumen digital dengan format JPG, dan dengan aplikasi ini dapat juga untuk mengekstrak pesan yang terdapat dalam objek Dokumen digital tersebut dengan kata kunci yang sesuai.

REFERENSI

Frank Cornelis, *Digital Signature* Service Protocol Specifications Version 0.5.0 (Th.2013)

WIRED EQUIVALENT PROTOCOL, Informatics Engineering Bilingual 2006-Computer System Faculty Sriwijaya University

Munir, Rinaldi, "Diktat Kuliah IF2151 Matematika Diskrit Edisi Ketujuh", Departemen Teknik Informatika Institut Teknologi Bandung, 2006.

Didik Setiawan, 'Buku Sakti Pemrograman Web: HTML, CSS, PHP, MySQL & Javascript', Start Up : Yogyakarta., 2017.

Jogiyanto Hartono , Analisis dan Desain Sistem Informasi, Andi Offset, Yogyakarta, 2007.