Jurnal Teknik Informatika (JIKA) Universitas Muhammadiyah Tangerang *ISSN : 2519-0710*
Tangerang, Oktober 2017

Prototype "Pengamanan Ganda" pesan rahasia dengan menggunakan teknik Steganografi metode LSB dan Kriptografi metode *Vigenere Cipher*

Agung Wibowo
Universitas Muhammadiyah Tangerang / Fakultas Teknik,
Program Studi Informatika
Jl. Perintis Kemerdekaan 1/33 Cikokol Kota Tangerang TLP. 55793251, 55772949, 55793802, 55736926
e-mail: agungismyname @gmail.com

ABSTRAK

Saat ini teknologi informasi sudah sangat berkembang menjadi salah satu media yang paling populer didunia. dengan semakin berkembangnya teknologi informasi semakin berkembang pula tindak penyalahgunaan informasi yang bukan haknya. Maka dari itu perkembangan teknologi informasi harus juga dibarengi dengan perkembangan pengaman informasi seperti pesan rahasia. Salah satu cara pengamanan data pesan dapat dilakukan dengan kombinasi Teknik keamanan kriptografi dan steganografi. Tujuannya adalah untuk merahasiakan sebuah pesan. proses kombinasi kriptografi dan steganografi diyakini sebagai cara ampuh untuk melindungi pesan yang dikirim, serta sekaligus menghindari pesan tersebut dari kecurigaan.

Kata Kunci : Kriptografi, Steganografi, *Vigenere Cipher, Least Significan Bit (LSB),* Pesan rahasia.

ABSTRACT

Today information technology has growing into one of the world's most popular media. with the development of information technology is growing also acts misuse of information that is not right. then from development of information technology should also be coupled with the development of information security such as secret message. One way of securing data messages can be done with a combination of cryptography and steganography security techniques. The goal is to keep a message. the combination of cryptography and steganography believed to be a powerful way to protect messages sent and simultaneously avoid the message from suspicion.

Keyword : *cryptography*, *steganography*, *Vigenere Cipher, Least Significan Bit (LSB), Secret message*.

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi dan komunikasi yang begitu pesat memungkinkan manusia berkomunikasi dan saling bertukar informasi secara jarak jauh, khususnya melalui media internet bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan hal tersebut, tuntutan akan keamanan terhadap kerahasiaan informasi yang saling dikirimkan tersebut semakin meningkat. Penulis akan melakukan pengembangan terhadap pengamanan ganda pada pesan rahasia yang berupa text dengan menggunakan teknik Steganografi metode LSB (Least Significant Bit) dan teknik Kriptografi metode Vigenere Cipher. Pengamanan informasi dapat dilakukan dengan cara menyembunyikan informasi sebenarnya kedalam suatu media tertentu yang disebut dengan istilah Steganografi, atau mengacak informasi sebenarnya menjadi informasi yang tidak dapat dibaca dengan cara biasa yang disebut Kriptografi. Secara khusus kedua cara atau teknik tersebut adalah dua hal yang berbeda. Namun demikian kedua teknik tersebut

memiliki tujuan yang sama yakni untuk mengamankan informasi.

II. DASAR TEORI

A. STEGANOGRAFI

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [22]

Steganografi memanfaatkan media digital untuk menyisipkan pesan rahasia melalui kode biner pada media digital tersebut, seperti: gambar, audio, video, text atau file biner.

Dalam prakteknya, sebenarnya pesan yang disembunyikan akan membuat perubahan tipis terhadap data digital yang disisipinya. namun karena perubahan itu sulit dilihat dengan mata, maka data tersebut tidak akan menarik perhatian dari orang yang tidak berhak untuk membaca pesan tersebut.

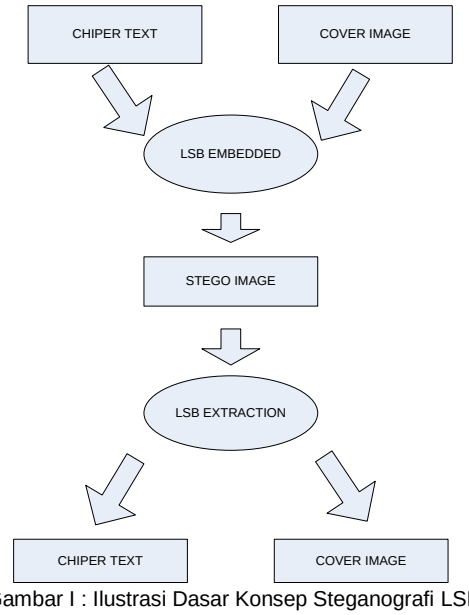
B. LSB (*LEAST SIGNIFICANT BIT*)

Metode steganografi sedemikian rupa dalam menyembunyikan isi suatu data di dalam suatu sampul media atau data digital lain yang tidak dapat diduga oleh orang biasa sehingga tidak menimbulkan kecurigaan kepada orang yang melihatnya.

Dalam membuat steganografi ada dua kriteria yang harus diperhatikan[12], yaitu:

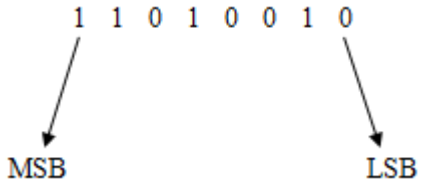
1. *Fidelity*. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. pihak ketiga tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
2. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (recovery). karena tujuan steganografi adalah penyembunyian pesan, maka sewaktu-waktu pesan rahasia didalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut

berikut adalah ilustrasi dasar dari konsep steganografi metode LSB (Least Significant Bit).



Gambar I : Ilustrasi Dasar Konsep Steganografi LSB

penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen gambar dengan bit-bit data rahasia. Metode yang paling sederhana adalah metode modifikasi LSB (Least Significant Bit Modification). Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling pertama (most significant bit atau MSB) dan bit yang paling terakir(least significant bit atau LSB).



Metode Least Significant Bit (LSB) adalah metode yang digunakan untuk menyembunyikan pesan dengan cara menyisipkannya pada *bit* rendah atau *bit* yang paling kanan (LSB) pada data piksel yang menyusun *file* tersebut. Pada citra *bitmap* 24 *bit*, setiap piksel (titik) pada citra tersebut terdiri dari tiga susunan warna, yaitu merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 *bit* (*byte*) dari 0 sampai 255 atau dengan format *biner* 00000000 sampai 11111111. Dengan demikian, pada setiap piksel citra *bitmap* 24 *bit* kita dapat menyisipkan 3 *bit* data.

C. KRIPTOGRAFI

Kriptografi adalah seni dan ilmu untuk menulis rahasia "*The Art of Secreet Writing*". Tujuannya agar pesan tidak dapat dibaca dengan mudah. Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) disebut dengan enkripsi (*encryption*).

Pada dasarnya komponen kriptografi terdiri dari beberapa kompenen, seperti:

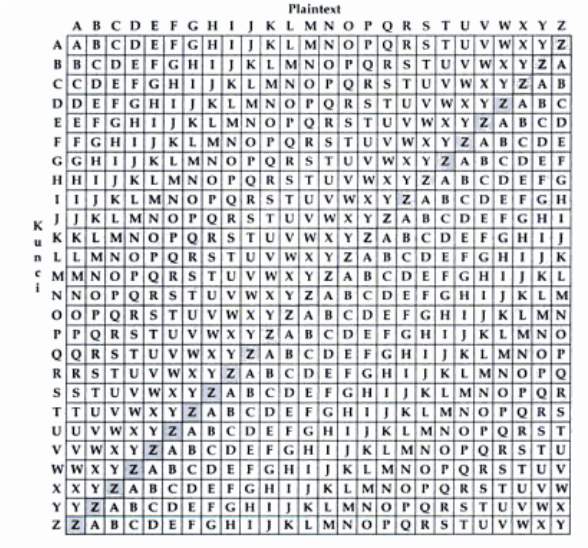
1. Enkripsi: merupakan hal yang sangat penting dalam kriptografi, merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. pesan asli disebut plaintext, yang diubah menjadi kode kode yang sulit dimengerti.
2. Deskripsi : merupakan kebalikan dari enkripsi. pesan yang telah di enkripsi dikembalikan ke bentuk asalnya.
3. Kunci: kunci yang dipakai untuk melakukan enkripsi dan denkripsi.
4. Chiphertext: merupakan suatu pesan yang telah melalui proses enkripsi. pesan yang ada pada text-kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidk mempunyai makna.
5. Plaintext: seding disebut dengan cleartext. text asli atau text biasa ini merupakan pesan yang ditulis atau diketik yang memiliki makna.

D. *VIGENERE CIPHER*

Ide dasarnya pengembangannya adalah menggunakan kode Caesar tetapi Jika pada *Caesar Cipher* setiap huruf digeser dengan besar geseran yang sama, maka pada *Vigènere Cipher* setiap huruf digeser dengan besar yang berbeda sesuai dengan kuncinya.

Kunci pada kriptografi *Vigènere Cipher* adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang *plaintext*, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada *plaintext*. Pergeseran setiap huruf pada *plaintext* akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada *plaintext*.

Vigènere Cipher menggunakan Bujursangkar Vigènere (*tabula recta*) untuk melakukan enkripsi dan dekripi. Seperti gambar dibawah ini:



Tabel I : Bujursangkar Vigènere (*tabula recta*)

Kolom paling kiri dari bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plaintext*. Setiap baris di dalam bujursangkar menyatakan huruf-huruf ciphertert yang diperoleh dengan *Caesar cipher*, yang mana jumlah pergeseran huruf *plaintext* ditentukan nilai numerik huruf kunci tersebut (yaitu, a=0, b=1, c=2, …, z=25). Sebagai contoh, huruf kunci c (=2) menyatakan huruf-huruf plaintext digeser sejauh 2 huruf ke kanan (dari susunan alfabetnya), sehingga huruf-huruf ciphertext pada baris c adalah:

Algoritma enkripsi vigenere cipher :

Ci = (Pi + Ki) mod 26

Algoritma dekripsi vigenere cipher :

Pi = (Ci – Ki) mod 26

Dimana :

Ci = nilai desimal karakter ciphertext ke-i

Pi = nilai desimal karakter plaintext ke-i

Ki = nilai desimal karakter kunci ke-i.

Sebagai contoh jika plaintext adalah THEBEAUTYANDTHEBEAST dan kunci adalah ABC maka proses enkripsi yang terjadi adalah sebagai berikut:

Plaintext : THEBEAUTYANDTHEBEAST
Kunci : ABCABCABCABCABCABCAB
Chipertext : TIGBFCUUAAOFTIGBFCSU

Pada contoh di atas kata kunci ABC diulang sedemikian rupa hingga panjang kunci sama dengan panjang plainteksnya. Kemudian setelah panjang kunci sama dengan panjang plainteks, proses enkripsi dilakukan dengan melakukan menggeser setiap huruf pada plainteks sesuai dengan huruf kunci yang bersesuaian dengan huruf plainteks tersebut. Pada contoh di atas plainteks huruf pertama adalah T akan dilakukan pergeseran huruf dengan kunci Ki=0 (kunci huruf pertama adalah A yang memiliki Ki=0) menjadi T. Huruf kedua pada plainteks adalah H akan dilakukan pergeseran huruf dengan kunci Ki=1 (kunci huruf kedua adalah B yang memiliki Ki=1) menjadi I. Begitu seterusnya dilakukan pergeseran sesuai dengan kunci pada tiap huruf hingga semua plainteks telah terenkripsi menjadi ciphertext.

E. TINJAUAN STUDI

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian tesis ini mengacu pada beberapa penelitian terkait yang telah dilakukan sebelumnya yaitu sebagai berikut.

Penulis	Judul Penelitian	Metode
[Sulidar 2009]	Implementasi algoritma Kriptografi DES dan Watermark dengan metode LSB pada data citra	Penelitian pengamanan ganda pada pesan rahasia yang berupa text dengan menggunakan teknik Steganografi metode LSB dengan Algoritma Kriptografi DES (Data Encryption Standard)
[B.Raja 2010]	Novel Skema Keamanan Informasi menggunakan Cryptic-Steganografi	Kriptografi yang digunakan MD-5 Algorithm untuk mengenkripsi pesan dan pada pesan tersembunyi Steganografi *Discrete Cosine Transform* (DCT)
[Esti 2010].	Kombinasi Kriptografi dengan *Hill Cipher* dan Steganografi dengan LSB untuk keamanan data teks	Penelitian pengamanan ganda pada pesan rahasia yang berupa text dengan menggunakan teknik Steganografi metode LSB dengan Algoritma Kriptografi *Hill Cipher*
[Shrikant 2010]	Implementasi Steganografi dengan Metode Bit-Plane Complexity Segmentation (BPCS) untuk Dokumen Citra Terkompresi	Pada penelitian ini dibahas mengenai steganografi dengan metode *Bit-Plane Complexity Segmentation* dengan media citra terkompresi. metode BPCS ini memanfaatkan perhitungan kompleksitas pada tiap bit-plane dalam menyelipkan informasi rahasia.
[Kamdar 2012]	Lapisan Dual Data Persembunyian Menggunakan Kriptografi Dan Steganografi	Hasil dari paket dari kriptografi gambar menggunakan kunci publik. Gambar yang dihasilkan dari Steganografi menggunakan discrete cosine transform (DCT)
[Shaik 2012]	Keamanan Data dan Otentikasi menggunakan Steganografi dan protokol STS	Pendekatan yang diusulkan dalam makalah ini menggunakan pendekatan steganografi yang menyediakan keamanan dan STS protokol yang menyediakan otentikasi. pengiriman berbagi kunci rahasia (stegokey)
[Shahana 2013]	Teknik Peningkatan Keamanan untuk Steganografi Menggunakan DCT dan RSA	Penelitian ini merupakan penggabungan algoritma Steganografi berbasis DCT, Untuk memberikan keamanan yang tinggi Steganografi dan Kriptografi digabungkan bersama-sama

Penelitian-penelitian di atas memiliki tujuan yang sama dengan penelitian tesis ini yaitu pengamanan ganda pada pesan rahasia yang berupa text dengan menggunakan teknik Steganografi metode LSB dengan Algoritma Kriptografi. Namun perbedaan yang mendasar adalah bahwa penelitian tesis ini menggunakan teknik Kriptografi metode Vigenere Cipher sebagai fokus utama dalam penelitiannya.

F. OBJEK PENELITIAN

Pada penelitian ini obyek penelitian yang akan menjadi fokus dalam mengembangkan aplikasi ini adalah sebagai berikut:

a. Laptop

Perangkat laptop yang akan digunakan untuk implementasi aplikasi khususnya untuk proses pemrograman memiliki spesifikasi sebagai berikut:

1) Prosesor: Intel *Core* i3 @ 2,53 Ghz
2) Memori: 4 GB
3) *Hard disk*: 283 GB
4) Microsoft Windows 7 Professional 64 bit

b. Komputer

Perangkat komputer yang akan digunakan untuk implementasi aplikasi khususnya untuk proses pemrograman memiliki spesifikasi sebagai berikut:

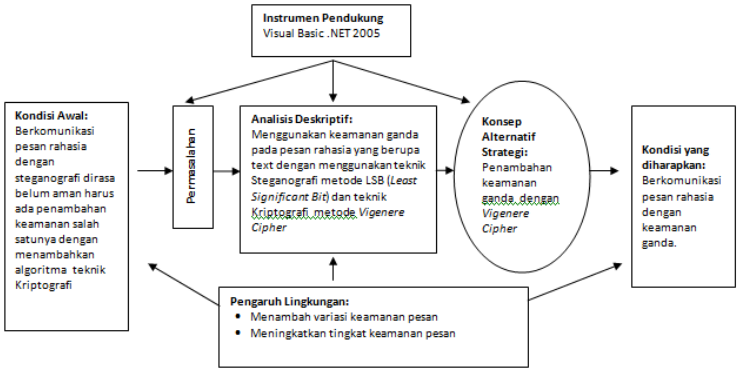
1) Prosesor: AMD A4-5300 CPU 3.4Ghz
2) Memori: 2 GB
3) *Hard disk*: 500 GB
4) Microsoft Windows XP SP2 32 *bit*.

c. Visual Basic .NET 2005

Dengan menggunakan alat ini, para programmer dapat membangun aplikasi Windows Forms,

G. POLA PIKIR

Dalam melakukan penelitian ini, pola pikir yang akan digunakan guna menyelesaikan rumusan masalah penelitian dapat dilihat pada Gambar berikut ini.

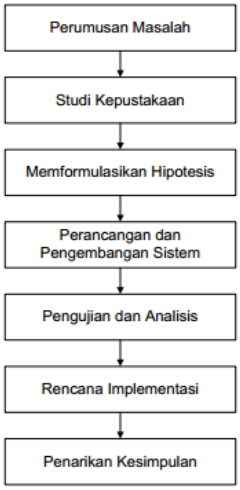


Gambar II : Ilustrasi Dasar Konsep Steganografi LSB

III. DESIGN PENELITIAN

A. LANGKAH LANGKAH PENELITIAN

Tahapan-tahapan yang dilakukan dalam rangka melakukan penelitian pengembangan aplikasi teknik pengamanan ganda pada pesan rahasia yang berupa text dengan menggunakan teknik Steganografi metode LSB (Least Significant Bit) dan teknik Kriptografi metode Vigenere Cipher adalah sebagai berikut:



Gambar III: Langkah-langkah penelitian

B. ALGORITMA SISTEM YANG DIKEMBANGKAN

Sistem yang dikembangkan memiliki algoritma *encode* dan *decode*. Algoritma *encode* sebagai berikut:

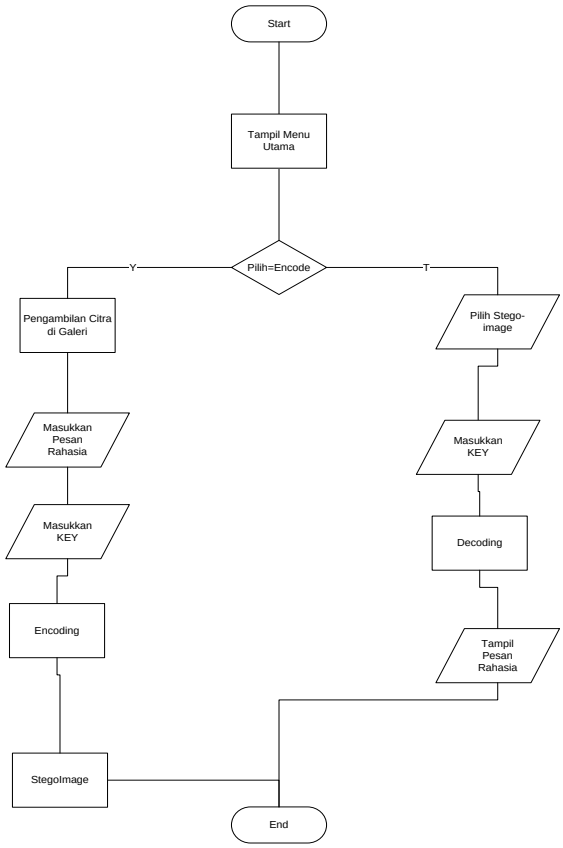
1. Tampil menu utama, dengan dua tombol pilihan, *encode* dan *decode*.
2. Pilihan *encode* akan menyisipkan pesan rahasia, akan tampil dua buah tombol untuk memilih *cover-image*, apakah dari kamera dengan memotret, atau dengan memilih citra yang sudah ada di galeri.
3. Setelah citra sudah ada, pesan rahasia diminta diketik untuk nantinya disisipkan ke dalam citra.
4. Memilih cara untuk mengirimkan *stego-image*.

Sedangkan algoritma *decode* adalah sebagai berikut:

1. Tampil menu utama, dengan dua tombol pilihan, *encode* dan *decode*.
2. Pilihan *decode* akan mengambil pesan rahasia dari *stego-image*.
3. Memilih *stego-image* dari media penyimpanan yang ada di dalam perangkat.
4. *Stego-image* di-*decode*, lalu tampil pesan rahasia.

C. FLOWCHART SISTEM YANG DIKEMBANGKAN

Alur diagram atau *flowchart* dari sistem yang dikembangkan adalah sebagai berikut:



Gambar IV : *Flowchart* Sistem

D. PENGUJIAN DAN ANALISIS

Proses pengujian dan analisis dilakukan untuk mengidentifikasi apakah sistem yang dikembangkan sesuai dengan analisis sistem yang telah dibuat. Pengujian sistem yang dilakukan dengan pengujian ISO 9126, black box serta PSNR dan MSE. Pegnujian ISO 9126 mengidentifikasi enam karakteristik kualitas perangkat lunak utama yaitu: Functionality, Reliability, Usability, Efficiency, Maintainability, Portability. Untuk syarat pengujian dapat digunakan minimal empat karakteristik sebagai acuan dasar. Pengujian black box dilakukan dengan menjalankan atau mengeksekusi unit atau modul, kemudian diamati apakah hasil dari unit tersebut sesuai dengan proses yang

diinginkan atau tidak. Pengujian Analisis Data PSNR dan MSE pada image cover-image dan stego-image untuk melihat perubahan kulitas gambar yang dihasilkan dan dinyatakan layak digunakan.

Dari hasil pengujian tersebut selanjutnya akan dianalisis berdasarkan hipotesis yang telah diformulasikan untuk ditarik kesimpulan.

IV. PEMBAHASAN DAN HASIL PENELITIAN

A. ANALISIS SISTEM

Pada tahap analisis sistem aplikasi menggunakan teknik Steganografi metode LSB (Least Significant Bit) dan teknik Kriptografi metode Vigenere Cipher ini menggunakan pendekatan desain dan analisis berorientasi objek atau Object Oriented Analysis and Design (OOAD) dengan menggunakan notasi Unified Modeling Language (UML).

a) Actor

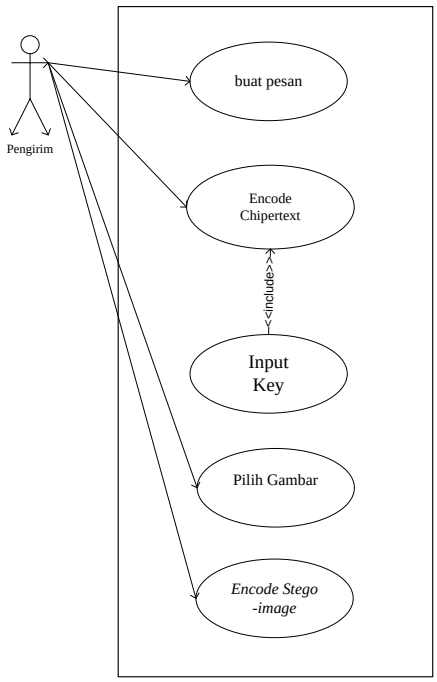
Actor pada aplikasi terbagi menjadi dua, yaitu pengirim dan penerima yang masing-masing memiliki tugas sebagai berikut.

Pengirim: Orang yang menggunakan aplikasi untuk mengirimkan pesan rahasia kepada penerima berupa StegoImage.
Penerima: Orang yang menggunakan aplikasi untuk membaca pesan rahasia didalam StegoImage yang dikirimkan oleh pengirim.

b) Use Case

Dalam rangka memberikan gambaran yang jelas terhadap use case aplikasi ini, maka use case diagram yang dibuat dibagi menjadi 2 yaitu Encode Stegano and kripto message use case diagram, dan decode Stegano and kripto message use case diagram. Secara detil setiap use case diagram aplikasi ini akan dijelaskan sebagai berikut.

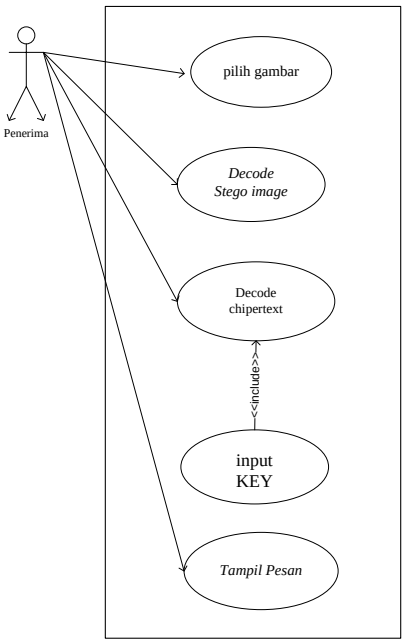
a. *Encode Stegano and kripto message use case diagram*



Gambar V : *Encode Stegano and kripto message*

Use case diagram di atas menggambarkan interaksi antara actor, yaitu pengirim pesan dengan sistem. Sedangkan use case terdiri dari enam yaitu: membuat pesan berupa *plaintext*, Memasukkan KEY, encode plaintext menajdi chipertext pada proses kriptografi, membuat *cover image*, encode chipertext menjadi *stego-image* pada proses steganografi, share *stego-image*.

b. *Decode Stegano and kripto message use case diagram*

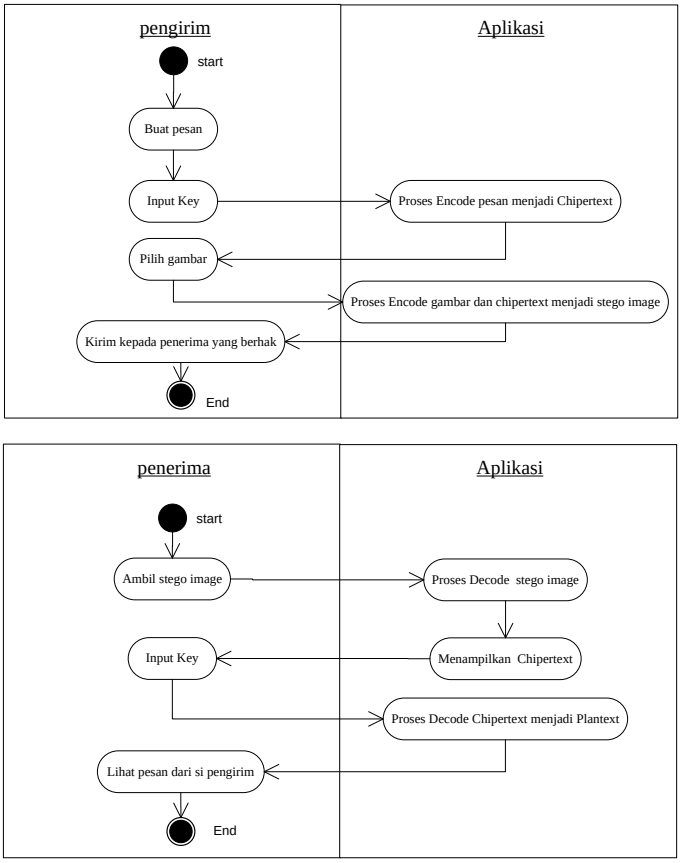


Gambar VI : *Decode Stegano and kripto message*

Use case diagram di atas menggambarkan interaksi antara actor, yaitu penerima pesan dengan sistem. Sedangkan use case di dalam aplikasi ini dibagi tiga yaitu: mengambil *stego-image*, decode stego image dan keluarkan *chipertext*, Masukkan KEY, decode chipertext menjadi *plaintext*, tampilkan pesan rahasia.

c) Activity Diagram

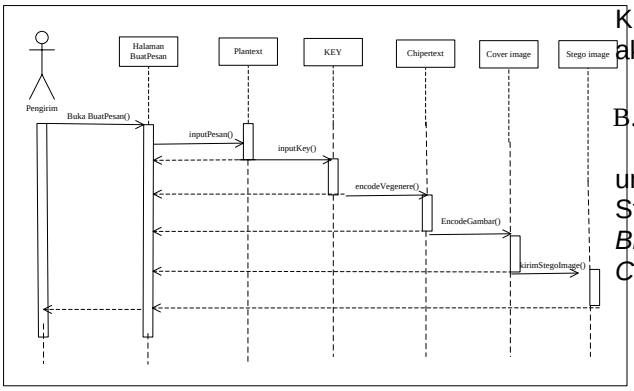
Activity diagram dibuat berdasarkan sebuah atau beberapa use case pada use case diagram. Activity diagram menggambarkan berbagai alur aktivitas dalam sebuah sistem yang sedang dirancang, bagaimana masing-masing alur memulai aktivitas, keputusan apa yang mungkin terjadi dan bagaimana aktivitas berakhir. Secara umum activity diagram untuk aplikasi pengamanan pesan rahasia menggunakan teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher* berbasis VB.NET dapat dilihat pada Gambar di bawah ini.



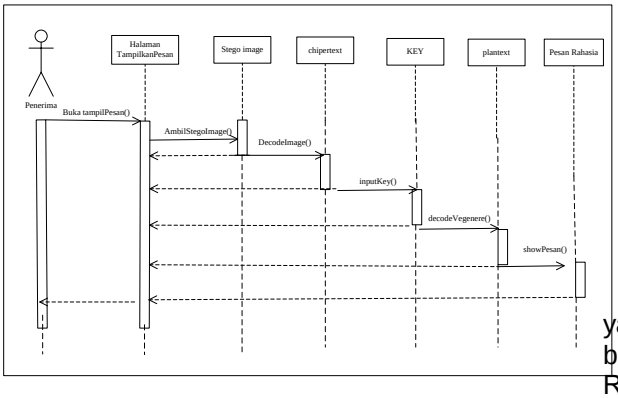
Gambar VII : *Activity diagram*

d) Sequence diagram

Sequence diagram tersebut menggambarkan interaksi antar obyek dan mengindikasikan komunikasi di antara obyek-obyek tersebut. Obyek-obyek tersebut kemudian diurutkan dari kiri ke kanan dimana *actor* yang menginisiasi interaksi diletakkan di paling kiri dari *sequence diagram*.



Gambar VIII: *Sequence diagram* pengirim aplikasi pesan rahasia

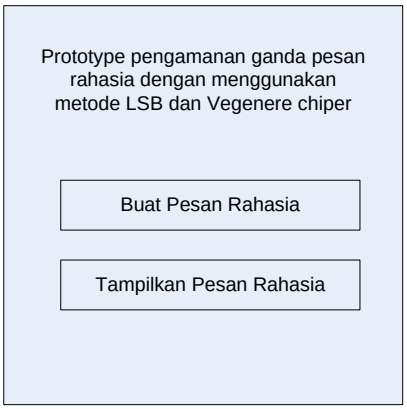


Gambar IX: *Sequence diagram* penerima aplikasi pesan rahasia

di atas merupakan *sequence diagram* dari aplikasi pengamanan pesan rahasia menggunakan teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher* yang akan dikembangkan.

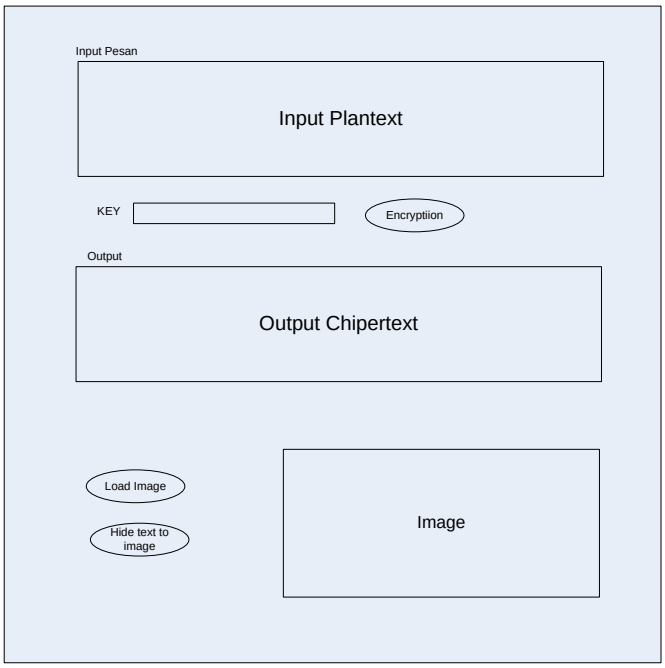
B. PERANCANGAN LAYAR APLIKASI

Berikut ini adalah GUI yang dirancang untuk aplikasi pesan rahasia teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher* berbasis VB.NET.



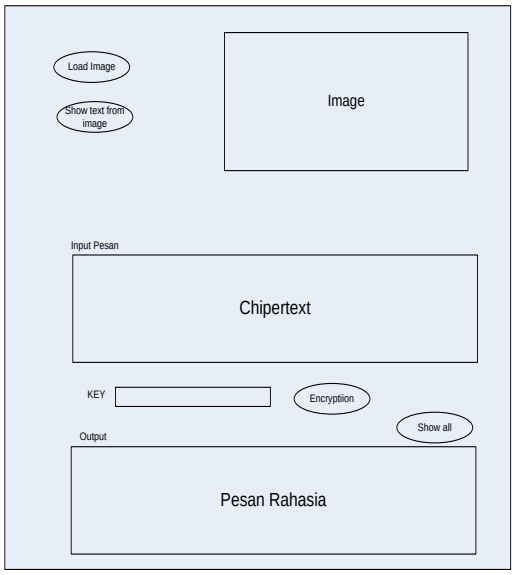
Gambar X: Rancangan layar halaman depan

Ketika aplikasi dijalankan, pertama kali yang muncul adalah halaman utama yang berisi menu pilihan. Ada pilihan “Buat pesan Rahasia” dan “Tampilkan Pesan Rahasia”. Bila pengirim ingin mengirimkan pesan rahasia, maka ia harus memilih “Buat pesan Rahasia” untuk memulainya.



Gambar XI: Rancangan layar "Buat pesan Rahasia"

Disini pengirim akan membuat pesan rahasia menjadi pesan yang bisa dimengerti (*plaintext*) menjadi pesan yang tidak bisa dimengerti (*chiperter*) menggunakan teknik *vigenere chiper* dan kemudian pengirim mengambil *cover-image* yang dia miliki Lalu secara otomatis sistem akan memasukkan *chipertext* yang telah ada kedalam *cover image* untuk diproses melalui teknik LSB menjadi sebuah *stego image*. *Stego image* yang dihasilkan bisa langsung disebarluaskan atau *share* melalui berbagai media seperti: *email*, *Social Media*, *sharing file*, dan lain-lain.



Gambar XII : Rancangan layar "Tampilkan Pesan Rahasia"

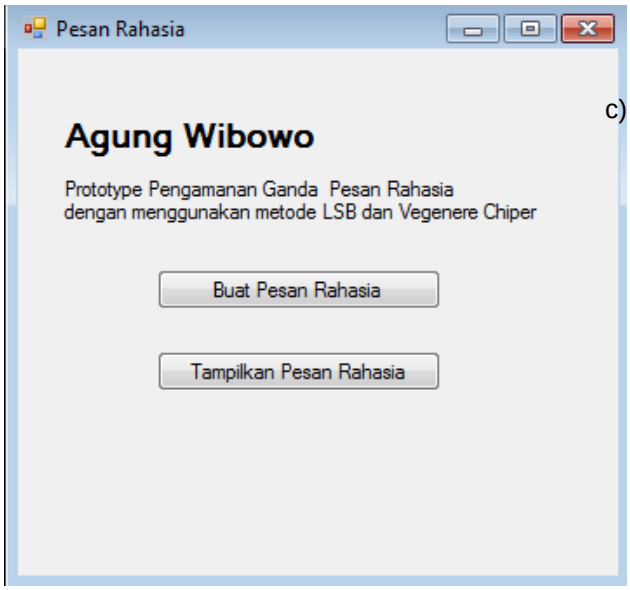
Penerima diminta untuk memasukkan *stego-image* yang telah ia terima. Setelah itu barulah tekan tombol *show text from image* seperti pada tampilan gambar diatas. Setelah itu akan muncul pesan rahasia yang masih bersifat *chipertext* sehingga belum bisa dipahami dengan jelas isi dari pesan yang ditampilkan. Untuk menampilkan pesan rahasia yang sesungguhnya pengguna atau

penerima harus mengetahu KEY yang dimasukkan sebelumnya oleh si pembuat pesan. Setelah itu barulah si penerima pesan dapat membaca pesan rahasia yang dimaksud.

C. IMPLEMENTASI PROGRAM

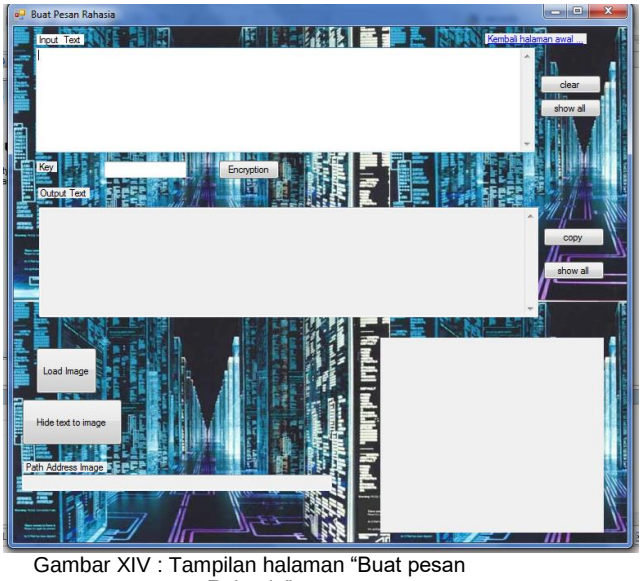
Pada tahap implementasi program akan dilakukan penerjemahan setiap use case yang terdapat pada analisis sistem dengan menggunakan bahasa pemrograman VB.NET menjadi bentuk method yang dimengerti oleh perangkat komputer untuk mengeksekusi suatu proses.

a) Halaman Utama
Ketika aplikasi steganografi ini dijalankan, maka yang akan muncul pertama kali adalah halaman utama. Pada halaman utama ini ada dua buah tombol yang berisi pilihan "Buat pesan Rahasia" dan "Tampilkan Pesan Rahasia".



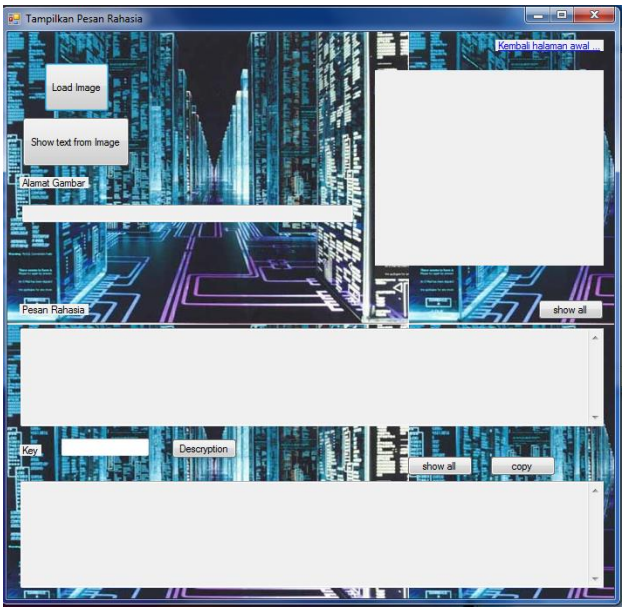
Gambar XIII : Tampilan halaman utama aplikasi

b) Halaman "Buat Pesan Rahasia"
Pada proses ini ada pembuatan pesan dari bentuk *plaintext* ke dalam bentuk *chipertext* dan dilanjutkan pengambilan citra yang akan digunakan untuk disisipi pesan, *cover-image* menjadi *stego-image* dengan menggunakan Proses penggabungan teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher*, dan setelah *stego-image* berhasil dibuat penggna dapat menyebarluaskan hasilnya melalui berbagai media.



Gambar XIV : Tampilan halaman "Buat pesan Rahasia"

c) Halaman "Tampilkan Pesan Rahasia"
Pada proses ini pengambilan *stego-image* media penyimpanan perangkat, lalu *stego-image* tersebut di-*decode* hingga ditampilkan isi pesan rahasianya.



Gambar XV : Tampilan halaman "Tampilkan Pesan Rahasia"

Selanjutnya jika pesan telah ditampilkan pengguna dapat memanfaatkan tampilan lebih lebar dengan menekan tombol fungsi "*show all*" yang menghasilkan tampilan lebih lebar dan nyaman untuk membaca isi pesan rahasia tersebut.

Gambar XVI : Tampilan *show all*

Ketika tombol fungsi *show all* di aktifkan maka seluruh pesan rahasia langsung dimunculkan di layar seperti gambar diatas.

D. PENGUJIAN SISTEM

Pengujian sistem yang dilakukan adalah pengujian *black box* dan pengujian PSNR (*peak signal to noise rasio*) dan MSE (*mean square error*) dan pengujian dengan pengujian ISO 9126.

a) Pengujian Black Box

Proses yang dijadikan objek pada pengujian *black box* ini terdiri proses *encode metode vigenere chiper*, encode *metode* LSB, *decode metode vigenere chiper* dan proses *decode metode* LSB.

a. Pengujian proses *encode metode vigenere chiper*.

Table II : *encode metode vigenere chipper*

Skenario	Yang Diharapkan
Input pesan *plaintext* dan masukkan pula KEY sebagai syarat methode *vigenere chiper*	Pesan *plaintext* berhasil dirubah menjadi *chipertext vigenere chiper* sesuai dengan KEY yang dimasukkan
Tekan tombol *clear* yang ada pada input pesan	Form pengisian pesan yang sudah dimasukkan kembali kosong
Tekan tombol *show all* yang ada pada input pesan	Isi pesan dapat ditampikan secara lebih luas sehingga mudah untuk dibaca
Masukkan KEY yang berbeda lalu lakukan prose *encode vigenere chiper*	Pesan *chipertext* dapat berubah ubah tidak statis menyesuikan KEY yang dimasukkan sebelumnya, sehingga lebih sulit untuk ditebak.
Tekan tombol *copy* yang ada pada tampilan pesan rahasia yang sudah dirubah menjadi pesan *chipertext*	Isi pesan dapat di *copy* seluruhnya sehingga lebih memudahkan pengguna.

b. Pengujian proses *encode metode LSB*.

Table III : *encode metode LSB*

Skenario	Yang Diharapkan
Ambil gambar *cover-image* format JPG dan masukkan pesan *chipertext* kedalam gambar dengan LSB	Gambar *cover-image* disisipkan pesan *chipertext* dan menghasilkan *stego-image* berformat JPG
Ambil gambar *cover-*	Gambar *cover-image*

image format GIf dan masukkan pesan *chipertext* kedalam gambar dengan LSB	disisipkan pesan *chipertext* dan menghasilkan *stego-image* berformat Gif
Ambil gambar *cover-image* format BMP dan masukkan pesan *chipertext* kedalam gambar dengan LSB	Gambar *cover-image* disisipkan pesan *chipertext* dan menghasilkan *stego-image* berformat BMP

c. Pengujian proses *decode metode* LSB.

Table IV : *decode metode LSB*

Skenarion	Yang Diharapkan
Ambil gambar *stego-image* format JPG dan keluarkan isi pesan yang ada didalmnya dengan proses *decode* metode LSB	Pesan *chipertext* yang ada dalam *stego-image* dapat di keluarkan dan ditampilkan dengan proses *decode* metode LSB
Ambil gambar *stego-image* format Gif dan keluarkan isi pesan yang ada didalmnya dengan proses *decode* metode LSB	Pesan *chipertext* yang ada dalam *stego-image* dapat di keluarkan dan ditampilkan dengan proses *decode* metode LSB
Ambil gambar *stego-image* format BMP dan keluarkan isi pesan yang ada didalmnya dengan proses *decode* metode LSB	Pesan *chipertext* yang ada dalam *stego-image* dapat di keluarkan dan ditampilkan dengan proses *decode* metode LSB

d. Pengujian proses *decode metode vigenere chiper*.

Table V : *decode metode vigenere chiper*.

Skenario	Yang Diharapkan
Masukkan KEY yang benar dan Rubah *chipertext yang ada* untuk dikembalikan menjadi *plaintext*	Pesan *chipertext* bisa dirubah kembali menjadi plaintext sehingga bisa dibaca isi dari pesan rahasia didalamnya
Masukkan KEY yang salah dan Rubah *chipertext yang ada* untuk dikembalikan menjadi *plaintext*	Pesan *chipertext* bisa dirubah kembali menjadi plaintext tetapi tidak bisa dibaca isi dari pesan rahasia didalamnya
Tekan tombol *show all* yang ada pada tampilan pesan rahasia yang sudah kembali menjadi *plaintext*	Isi pesan dapat ditampikan secara lebih luas sehingga mudah untuk dibaca
Tekan tombol *copy* yang ada pada tampilan pesan rahasia yang sudah kembali menjadi *plaintext*	Isi pesan dapat di copy seluruhnya sehingga lebih memudahkan pengguna.

Berdasarkan hasil pengujian *black box* dapat disimpulkan bahwa sistem yang dikembangkan dapat mengetahui fungsi-fungsi yang salah atau hilang, kesalahan kinerja, inisialisasi dan secara fungsional mengeluarkan hasil yang sesuai dengan yang diharapkan.

b) Pengujian PSNR dan MSE

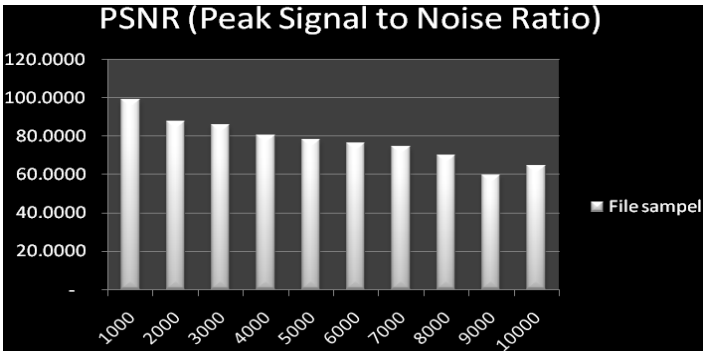
Proses yang dilakukan adalah dengan menggunakan 10 gambar *cover-image* berformat BMP dengan menyisipkan jumlah plaintext yang beragam. Data yang dihasilkan dimasukkan kedalam table. Aspek yang dicari adalah untuk menentukan perbandingan PSNR dan MSE dari masing-masing *cover-image* dan *stego-image.*

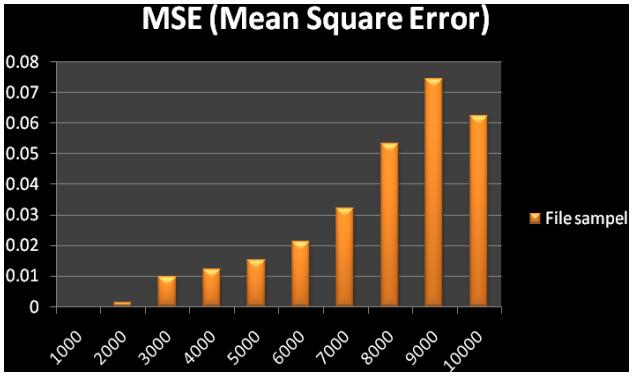
Table VI : Pengujian PSNR dan MSE

no	Cover image	Stego image	Total char	MSE	PSNR
1	sampel_1.bmp	sampel_1_stego.bmp	1000	0	99.0000
2	sampel_2.bmp	sampel_2_stego.bmp	2000	0.0013	87.6069
3	sampel_3.bmp	sampel_3_stego.bmp	3000	0.0097	85.7863

4	sampel_4.bmp	sampel_4_stego.bmp	4000	0.0121	80.3142
5	sampel_5.bmp	sampel_5_stego.bmp	5000	0.0153	78.1298
6	sampel_6.bmp	sampel_6_stego.bmp	6000	0.0212	76.1764
7	sampel_7.bmp	sampel_7_stego.bmp	7000	0.0321	74.6011
8	sampel_8.bmp	sampel_8_stego.bmp	8000	0.0532	70.2138
9	sampel_9.bmp	sampel_9_stego.bmp	9000	0.0746	59.4039
10	sampel_10.bmp	sampel_10_stego.bmp	10000	0.1624	64.6241

Perbandingan MSE dan SNR dapat kita kita melalui grafik berikut :





Gambar XVII: Tampilan *chart diagram PSNR dan MSE*

Dari grafik tersebut terlihat bahwa hasil penyisipan mengeluarkan stego-image yang memiliki kualitas baik pada nilai *PSNR* tinggi dengan nilai rata-rata 80 hingga jika kapasitas jumlah karakter semakin besar akan menurun dan nilai MSE rendah dengan nilai rata rata 0.03 hingga jika kapasitas jumlah karakter semakin besar akan naik.

c) Pengujian ISO 9126

Pengujian dilakukan dengan kuesioner dengan menggunakan 4 kriteria yaitu:

Table VII : Pengujian ISO 9126

Aspek	Skor	Skor	%skor	kriteria
	Aktual	**Ideal**	**aktual**	
Functionality	153	180	85%	Sangat baik
Reliability	137	150	91%	Sangat baik
Usability	168	180	93%	Sangat baik
Efficiency	53	60	88%	Sangat baik
Total	**511**	**570**	**89.65%**	**Sangat baik**

$$\%\text{Skor aktual} = \frac{\text{Skor Aktual}}{\text{Skor Ideal}} \times 100\%$$

$$= \frac{511}{570} \times 100\% = 89.65\% \text{ (kriteria sangat baik)}$$

Berdasarkan keseluruhan tabel diatas dapat disimpulkan bahwa tingkat kualitas prototype aplikasi secara keseluruhan dalam kriteria sangat baik dengan persentase 89.65% kriteria sangat baik.

V. PENUTUP

A. KESIMPULAN

Penelitian penggunaan aplikasi pengamanan ganda pesan rahasia menggunakan teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher* berbasis VB.NET. Setelah dilakukannya pengujian fungsi-fungsi aplikasi secara *Black Box* dan pengujian kualitas gambar yang dihasilkan baik secara PSNR dan MSE aplikasi prototype pesan rahasia menggunakan teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher.* dan pengujian dengan pengujian ISO 9126. Secara umum bisa dinyatakan layak untuk diimplementasikan dan untuk digunakan oleh masyarakat umum.

B. SARAN

Dari penelitian ini masih memiliki kekurangan dan memerlukan penelitian lanjutan guna menyempurnakannya. Beberapa hal yang perlu penelitian lanjutan yaitu sebagai berikut:

a) Penelitian dapat dilanjutkan dengan meningkatkan keamanan dengan menerapkan metode pengamanan ganda yang lebih kompleks dari penggabungan teknik Steganografi metode LSB (*Least Significant Bit*) dan teknik Kriptografi metode *Vigenere Cipher*.
b) Penelitian dapat dilanjutkan dengan meningkatkan keamanan melalui penambahan *login* untuk menjalankan aplikasi ini.
c) Penelitian dapat dilanjutkan dengan menambahkan kemampuan aplikasi untuk dapat menyisipkan pesan rahasia pada media lain seperti suara, video dan *file* berformat lainnya.
d) Aplikasi dapat diimplementasikan juga pada aplikasi mobile seperti iOS, Android ataupun Windows Phone. diharapkan dapat lebih memudahkan pengguna.
e) Semakin banyak penelitian yang dilakukan, terutama yang berhubungan dengan keamanan pesan rahasia yang di lakukan secara berlapis, diharapkan dapat terus meningkatkan variasi-variasi teknik kemanan yang ada sekarang ini dan memberikan rasa aman yang lebih baik kedepannya

C. REFERENSI

[1] A. J Menezes, P. van Oorschot and S. Vanstone - *Handbook of Applied Cryptography* UK: CRC Press.

[2] Ariyus, Dony, Kriptografi – Keamanan Data Dan Komunikasi, Graha Ilmu, Yogyakarta, 2006.

[3] Ariyus, Dony, Pengantar Ilmu *Kriptografi*: Teori, *Analisis*, dan *Implementasi*. Penerbit Andi, Yogyakarta, 2008.

[4] Alatas, Putri, Implementasi Teknik Steganografi dengan Metode LSB pada Citra Digital, Universitas Gunadarma, Jakarta, 2009.

[5] B.Tjaru, Setia Negara, Modifikasi Full *Vigenere Chipher* dengan Pengacakan Susunan Huruf pada Bujur Sangkar Berdasarkan Kunci, ITB Bandung, 2012.

[7] G. Kamdar, Dolly Patira, Dr. C. H. Vithalani, *Dual Layer Data Hiding Using Cryptography And Steganography*, *International Journal of Scientific Engineering and Technology* (ISSN : 2277-1581) www.ijset.com, Volume No.1, Issue No.4, pg :134-138, Oktober 2012

[8] Leonardo, Kevin Handoyo, Modifikasi *Vigenere Cipher* dengan Metode Penyisipan Kunci pada Plaintext, ITB, Bandung, 2012.

[9] A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, *Information Hiding -A Survey*,

Proceeding of the IEEE, vol. 87, Issue 7, pp. 1062-1078, Juli 1999.

[10] Prasetyo, Bambang dan Jannah, L.M., *Metode Penelitian Kuantitatif*, Jakarta: PT. Rajagrafindo Persada, 2005.

[11] Ramadhani, Budi, Steganografi pada Citra GIF mengggunakan bahasa pemrograman Delphi, UII, Yogyakarta, 2006.

[12] Rosziati Ibrahim and Law Chia Kee, *MoBiSiS: An-Android based Application for Sending Stego Image through MMS*, ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology, 2012.

[13] Esti Suryani,Titin sri Martini, Kombinasi Kriptografi dengan Hillchipher dan staganografi dengan LSB untuk keamanan data text, Universitas Muhammadiyah, Magelang.

[14] Sulidar Fitri, Implementasi Algoritma Kriptografi DES dan Watermark dengan Metode LSB pada data Citra, Universitas AMIKOM, Yogyakarta, 2010.

[15] Suranta, Ricardo Pramana, Perbandingan Ketahanan Algoritma LSB dan F5 dalam Steganografi Citra, ITB, Bandung, 2012

[16] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D*, Bandung: Alfabeta, 2012.

[18] Shrikant S. Khaire and Dr. Sanjay L. Nalbalwar, *Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique*, International Journal of Engineering Science and Technology, Vol. 2(9), 4860-4868, 2010.

[19] Shahana T, *An Enhanced Security Technique for Steganography Using DCT and RSA, International Journal of Advanced Research in Computer Science and Software Engineering*, Vol 3, Issue 7, July 2013.

[20] Shaik Riyaz, J. Rajakala and M RamaKrishna, *Data Security and Authentication using Steganography and STS protocol, International Journal of Advanced Research in Computer Science and Electronics Engineering*, Volume 1, Issue 5, July 2012

[22] Namita Tiwari and Dr. Madhu Shandilya, *Evaluation of Various LSB based Methods of Image Steganography on GIF File Format*, International Journal of Computer Applications, vol. 6, September 2010.

[25] Triputra Safei, Timotius, Pengukuran dan Pengujian Kekuatan Algoritma Auto-key Vigenere Cipher, ITB, Bandung, 2012