Perancangan Perangkat Lunak Steganografi Menggunakan Least Significant Bit Dengan Enkripsi Vigenere Cipher

Septa Festi Burna Jaya, Susanti M. Kuway, Gusti Syarifudin
[1,2]STMIK Pontianak; Jl Merdeka Barat No. 372, (0561) 735555
[3]Jurusan Teknik Informatika, STMIK Pontianak
e-mail: info@stmikpontianak.ac.id,fbj.septa@gmail.com, shanty_stmikptk@yahoo.com, gus_wet@yahoo.com

Abstrak

Teknologi informasi merupakan seperangkat alat dalam membantu pemprosesan atau penataan data yang mempunyai nilai pengetahuan bagi penggunanya. Dalam menjamin kerahasian dan keamanan suatu data diperlukan metode steganografi, yang merupakan metode untuk menjaga kerahasian pada informasi. Pada dasarnya pesan teks tersebut tanpa ada melakukan pengamanan terhadap isi pesan yang dikirim, sehingga ketika dilakukan penyadapan terhadap alur pengirimanya maka pesan teks yang disadap dapat langsung dibaca oleh penyadap. Untuk itu dibutuhkan perangkat lunak sebagai penunjang metode tertentu sehingga pesan terkirim tersebut menjadi lebih aman. Dalam penelitian ini penulis menggunakan bentuk penelitian studi literatur dan eksperimen. Sedangkan metode perancangan perangkat lunak menggunakan metode Prototype karena proses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat dan pemanfaatan fungsi yang pada sebelumnya. Adapun teknik pengumpulan data menggunakan studi dokumentasi dan observasi untuk memperoleh teori Least Significant Bit (LSB) dan Vigenere Cipher. Penggunaan metode Least Significant Bit (LSB) dan Vigenere Cipher termasuk cukup cepat dalam melakukan proses embedding dan extraction pada sebuah file teks. Perancangan perangkat lunak menggunakan bahasa pemrograman NetBeans IDE hasil perancangan ini menghasilkan sebuah perangkat lunak yang dapat memberi keamanan saat dalam bebagi informasi rahasia.

Kata kunci : *Steganografi, Embedding, Extraction, Least Significant Bit (LSB), Vigenere Cipher, NetBeans, Prototype.*

Abstract

Information technology is a set of tools in helping Setup or processing data that has a value of knowledge for its users. In ensuring the security and confidentiality of data required a method of steganography, which is a method for keeping the confidentiality of the information. Basically the text messages without doing a safeguard against the content of the messages sent, so that when it is done tapping against the groove sent then intercepted text messages can be directly read by the tappers. For that it needs the software as supporting certain methods so that the message sent is secure. In this study the authors using this form of research studies and experimental literature. While the method of design software using the Prototype method because the process of software development places emphasis on a short development cycle and utilization functions in advance. As for the technique of data collection using the study documentation and observation to gain the Least Significant Bit (LSB) of the theory and the Vigenere Cipher. The use of the method of Least Significant Bit (LSB) and the Vigenere Cipher including fast enough in doing the process of embedding and extraction in a text file. The design of the programming language software using NetBeans IDE results this design generates a software that can give security in share of confidential information.

Keyword : *Steganografi, Embedding, Extraction, Least Significant Bit (LSB), Vigenere Cipher, NetBeans, Prototype.*

1. PENDAHULUAN

Pengiriman informasi melalui jaringan elektronik saat ini memerlukan suatu proses yang menjamin keamanan dan keutuhan dari informasi yang dikirimkan tersebut. Informasi tersebut harus tetap terjaga kerahasiaannya selama pengiriman dan informasi harus tetap asli pada saat penerimaan di tujuan.

Oleh karna itu, diperlukan sebuah tool untuk mengamankan informasi yang nantinya akan dikirimkan kepada penerima. Salah satu cara yang digunakan untuk mengamankan data yaitu Steganografi dan Kriptografi. Steganografi dan Kriptografi merupakan cara yang paling aman dikarenakan informasi tersebut akan disembunyikan ke dalam media lain yang sekiranya tidak mudah dideteksi oleh hacker maupun cracker [1].

Steganografi merupakan "seni dan ilmu menulis atau menyembunyikan pesan tersembunyi dengan cara tertentu sehingga selain pengirim dan penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Istilah steganografi (*steganography*) berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *graphein* yang berarti tulisan. Jadi steganografi (*steganography*) bisa diartikan sebagai seni menyamarkan / menyembunyikan pesan tertulis ke dalam pesan lainnya"[2].

Kriptografi adalah "suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *cryptographer*, sedangkan *cryptanalysis* adalah suatu ilmu dan seni membuka (*breaking*) *ciphertext* dan orang yang melakukannya disebut *cryptanalyst*. Implementasi dari kriptografi adalah proses penyandian informasi yang disebut teknik enkripsi" [3].

Dalam penelitian ini, penulis menggunakan metode studi literatur dan perancangan eksperimen. Studi literatur merupakan studi yang bisa dijadikan sebagai bahan untuk mengumpulkan dan mengkaji data dengan membaca berbagai literatur seperti buku, jurnal, skripsi maupun bentuk tulisan lainnya yang isinya berkaitan erat dengan masalah yang akan diteliti sebagai bahan referensi tertulis. Eksperimen dilakukan dengan cara melakukan perancangan, implementasi sistem untuk membuat gambaran yang jelas dari masalah yang dihadapi.

Pada steganografi sendiri terdapat beberapa algoritma, salah satunya yaitu Least Significant Bit (LSB) dan untuk memperkuat keamanan data steganografi digabungkan dengan menggunakan kriptografi yaitu Vigenere Cipher. Dalam penelitian ini akan digunakan Least Significant Bit (LSB) dan Vigenere Cipher sebagai algoritma yang digunakan untuk mengamankan file data. Metode Least Significant Bit (LSB) merupakan teknik subsitusi pada stego, pada arsip 24-bit atau 8-bit digunakan untuk menyimpan citra digital. LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap *byte* warna pada sebuah piksel. Representasi warna dari piksel-piksel didapat dari warna-warna primer (RGB). Citra 24-bit menggunakan 3 *byte* untuk masing-masing piksel dan setiap warna primer direpresentasikan dengan ukuran 1 *byte* [4]. Metode Vigene Cipher merupakan bagian darikriptografi klasik. Nama *Vigenere* diambil dari seorang yang bernama *Blaise de Vigenere*. *Vigenere cipher* merupakan contoh *cipher* alfabet-majemuk "manual" yang dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenere pada abad 16, meskipun Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis di dalam bukunya *La Cifra del Sig,* tetapi algoritma ini baru dikenal luas 200 tahun kemudian yang oleh penemunya tersebut kemudian dinamakan *Vigenere cipher. Cipher* ini berhasil dipecahkan oleh Babage dan Kasiski pada pertengahan abad ke-19 [5].

Hasil dari perancangan yang dibuat dapat dimanfaatkan sebagai alat bantu dalam menjaga kerahasiaan sebuah data berlapis serta dapat mempelajari dan memahami cara kerja dari kedua metode steganografi dan kriptografi. Pada penelitian diatas sebagai suatu panduan penulis dalam menyelesaikan penelitian yang akan dilakukan oleh penulis, maka penulis berharap dapat merancang perangkat lunak yang baik dan terjaga keamanannnya tanpa harus merusak pesan serta dapat mengembalikan pesan yang terenkripsi *Least Significant Bit (LSB)* dan *Vigenere Cipher* yang sudah di *embedding* menjadi data asli kembali setelah di *extraction.*

2. METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan metode studi literatur dan perancangan eksperimen. Studi literatur merupakan studi yang bisa dijadikan sebagai bahan untuk mengumpulkan dan mengkaji data dengan membaca berbagai literatur seperti buku, skripsi, jurnal maupun bentuk tulisan lainnya yang isinya berkaitan erat dengan masalah yang akan diteliti sebagai bahan referensi tertulis. Eksperimen dilakukan dengan cara melakukan perancangan, implementasi sistem untuk membuat gambaran yang jelas dari masalah yang dihadapi.

Metode pengumpulan data merupakan bagian yang terpenting dari sebuah penelitian ini. Ketersediaan data akan sangat menentukan dalam proses pengolahan data dan analisa selanjutnya. Karena dengan adanya pengumpulan data yang tepat maka diharapkan jawaban dari perumusan masalah tidak biasa. Data yang dikumpulkan sesuai dengan tujuan dari penelitian. Sumber data dari penelitian ini merupakan data primer dan data sekunder.

Data primer yang berkaitan langsung dengan data yang diperoleh dari observasi yaitu dengan mempelajari hasil dari program-program deteksi tepi yang sudah jadi. Sedangkan data sekunder berkaitan dengan semua hasil pengumpulan data yang mendukung data yang diperoleh dari studi dokumentasi dimana data diperoleh dari buku dan *internet* mengenai artikel-artikel, jurnal, dan adanya hasil dari penelitian sebelumnya yang dapat digunakan sebagai bahan perbandingan dengan penelitian yang dilakukan.

Metode analisis dan perancangan yang digunakan penulis untuk mengembangkan sistem adalah metode *prototype*. Metode *prototype* ini melakukan pendekatan secara sistematis dan urut, mulai dari level identifikasi kebutuhan sistem, kemudian tahap mengembangkan *prototype*, menguji kelayakan *prototype*, memprogram sistem berdasarkan kebutuhan, pengujian sistem, menentukan kelayakan sistem, dan penggunaan sistem [6].

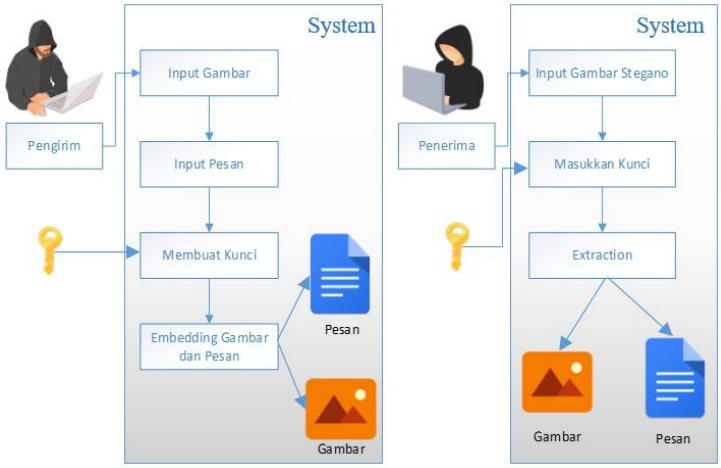
Pada penelitian ini penulis tidak menggunakan sesi wawancara kepada pengguna dikarenakan pada kasus ini perangkat lunak tidak bertujuan untuk kepuasan pengguna, melainkan bertujuan untuk menyisipkan suatu file ke dalam gambar, yang nantinya akan dikembangkan ke tahap selanjutnya.

3. HASIL DAN PEMBAHASAN

Pada tahap ini, penulis mendefinisikan fungsi-fungsi yang akan dipakai dalam pembuatan aplikasi. Penelitian bertujuan untuk merancang sebuah aplikasi yang dapat melakukan penyisipan suatu file pesan terhadap citra digital dengan menggunakan metode Least Significant Bit (LSB) dan Vigenere Cipher. Adapun langkah-langkah yang dilakukan dalam menyelesaikan masalah ini adalah sebagai berikut.

Mengumpulkan teori dan contoh-contoh kasus yang berhubungan dengan masalah steganografi, citra digital, metode Least Significant Bit (LSB) dan Vigenere Cipher. Teori-teori ini dikumpulkan dari beberapa sumber seperti buku-buku di perpustakaan, artikel-artikel di internet serta referensi dari paper yang berhubungan dengan masalah yang dihadapi. Selain mengumpulkan teori-teori, juga dikumpulkan contoh-contoh kasus dalam bentuk jurnal penelitian sebagai referensi dalam memecahkan masalah steganografi khususnya yang menggunakan metode Least Significant Bit (LSB) dan Vigenere Cipher.

Arsitektur perangkat lunak merupakan suatu pernyataan yang menggambarkan komponen perangkat lunak serta hubungan antara komponen tersebut. Agar perangkat lunak yang dibuat lebih mudah dipahami, berikut ini gambaran dari arsitektur perancangan perangkat lunak steganografi pada suatu citra pada gambar 1.



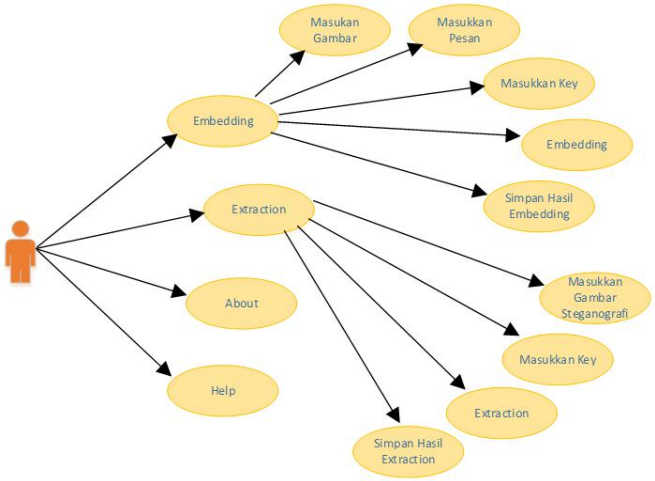
Gambar 1. Arsitektur Perangkat Lunak Steganografi

Dalam perancangan perangkat lunak steganografi ini, diambil tiga perancangan *Unified Modeling Language* (UML), yaitu *Use Case Diagram, Activity Diagram* dan *Sequence Diagram.*

Use case diagram berisi gambaran fungsionalitas yang diharapkan dari sebuah sistem dengan penekanan pada apa yang dilakukan oleh sistem. *Use case diagram* terdapat satu pihak yang berhubungan dengan *use case*. *Use case* adalah suatu *set scenario* yang dikumpulkan bersama-sama oleh hasil dari pengguna yang biasa terjadi. Diagram *use case* menggambarkan fungsi-fungsi dari sebuah sistem menggunakan aktor dan *use case. Use case* merupakan pelayan atau fungsi yang dimiliki oleh sistem untuk penggunanya. Tujuan dari pembuatan *use case* adalah:

a. Untuk memecah-mecah permintaan dari pengguna menjadi beberapa bagian yang memilki kesatuan arti.
b. Sebagai dasar dalam perencanaan konstruksi.
c. Sebagai basis untuk mencoba sistem.

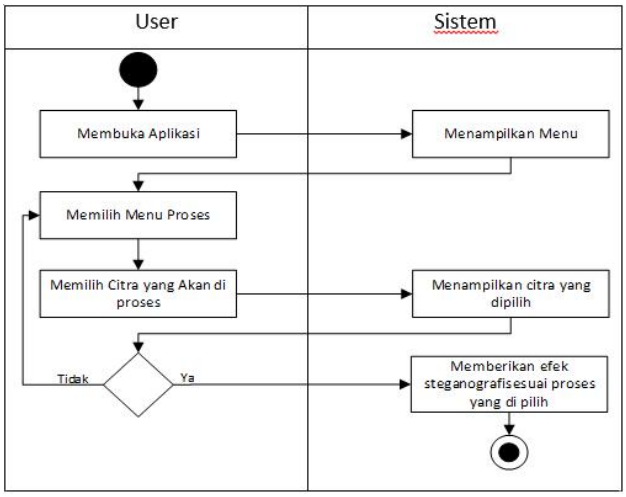
Penggunaan *use case diagram* disini untuk menjelaskan perancangan aplikasi manipulasi citra dengan metode konvolusi. Dalam model *use case*, aktor merupakan satu-satunya kesatuan eksternal yang berinteraksi dengan sistem. Adapun aktor yang berperan dapat dilihat pada gambar 2 berikut:



Gambar 2. *Use Case Diagram*

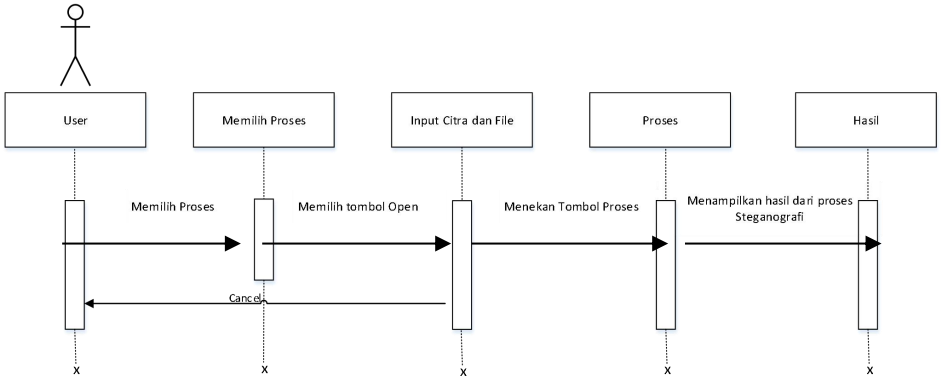
Activity Diagram adalah teknik untuk menggambarkan logika *procedural*, proses bisnis dan aliran kerja dalam banyak kasus dalam sistem yang sedang dirancang dan bagaimana

masing-masing berawal dan bagaimana sistem itu berakhir. *Activity Diagram* merupakan *state diagram* khusus dimana sebagaian besar *state* adalah *action* dan sebagaian transisi di *trigger* oleh selesainya *state* sebelumnya. Sebuah aktivitas dapat dijalankan oleh satu *use case* atau lebih. Aktivitas menggambarkan proses yang berjalan, sementara *use case* menggambarkan bagaimana aktor menggunakan sistem untuk melakukan aktivitas. Gambar 3 merupakan *activity diagram* pada perangkat lunak perbandingan steganografi ini sebagai berikut:



Gambar 3. *Activity Diagram*

Sequence Diagram digunakan untuk menggambarkan perilaku pada sebuah skenario. *Sequence Diagram* digunakan untuk memberikan gambaran detail dari setiap *use case diagram* yang dibuat sebelumnya. Setiap objek yang terlihat dalam sebuah *use case* digambarkan dengan garis pututs-putus vertikal, kemudian *message* yang dikirim oleh objek digambarkan dengan garis horizontal. Gambar 4 merupakan *Sequence Diagram* pada perangkat steganografi ini sebagai berikut:



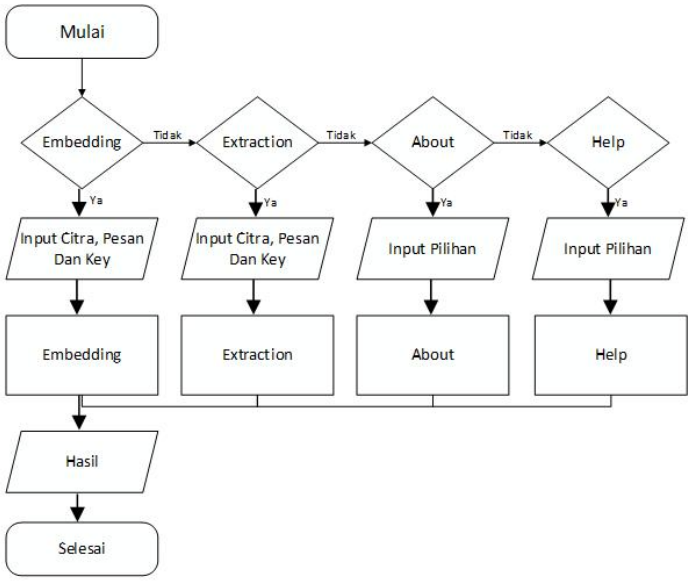
Gambar 4. *Sequence Diagram*

Kemudian langkah selanjutnya adalah merancang *flowchart*, *flowchart* ini merupakan langkah awal pembuatan program. Dengan adanya *flowchart* urutan poses kegiatan menjadi lebih jelas. Jika ada penambahan proses maka dapat dilakukan lebih mudah, setelah *flowchart* selesai disusun, selanjutnya pemrogram (*programmer*) menterjemahkannya ke bentuk program dengan bahasa pemrograman.

Flowchart merupakan gambar atau bagan yang memperlihatkan urutan dan hubungan antar proses beserta instruksinya. Gambaran ini dinyatakan dengan simbol. Dengan demikian setiap simbol menggambarkan proses tertentu. Sedangkan hubungan antar proses digambarkan dengan garis penghubung. Form dan modul yang sudah didefinisikan sebelumnya beserta komponennya disatukan untuk membentuk suatu program utuh. Hubungan antar modul dengan

form juga didefinisikan. Pembuatan *flowchart* (bagan alir) ini untuk mempermudah dalam perancangan perangkat lunak steganografi pada citra digital.

Berikut gambar 5 ini *Flowchart* steganografi :

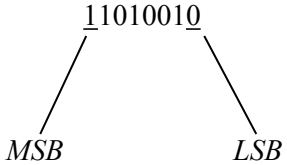


Gambar 5. *Flowchart* Steganografi

Berikut ini adalah algoritma dari *flowchart* proses steganografi:

a. Mulai
b. Pilih operator steganografi pada menu pilihan yang terdapat pada perangkat lunak
c. Memasukkan gambar yang akan di proses Steganografi
d. Jika Embedding yang dipilih pada menu pilihan, maka perangkat lunak akan menjalankan proses Embedding.
e. Jika Extraction yang dipilih pada menu pilihan, maka perangkat lunak akan menjalankan proses Extraction.
f. Jika About yang dipilih pada menu pilihan, maka perangkat lunak akan menjalankan proses About.
g. Jika Help yang dipilih pada menu pilihan, maka perangkat lunak akan menjalankan proses Help.
h. Setelah perhitungan operator yang dipilih selesai, maka perangkat lunak akan menampilkan hasil deteksi tepi sesuai dengan operator yang dipilih.

Least Significant Bit (LSB). Least Significant Bit (LSB) merupakan teknik penyembunyian data yang bekerja pada domain spasial atau waktu, yaitu teknik menyembunyikan informasi dengan menyisipkan bit data ke dalam byte covertext atau cover object. 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). Perhatikan contoh sebuah susunan bit pada sebuah byte :

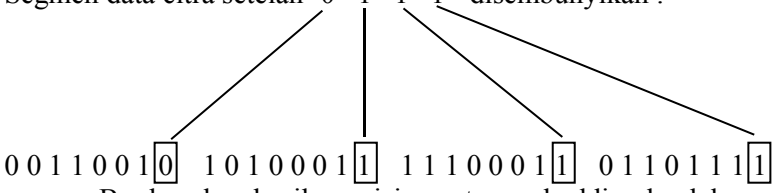


LSB = Least Significant Bit
MSB = Most Siginificant Bit

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

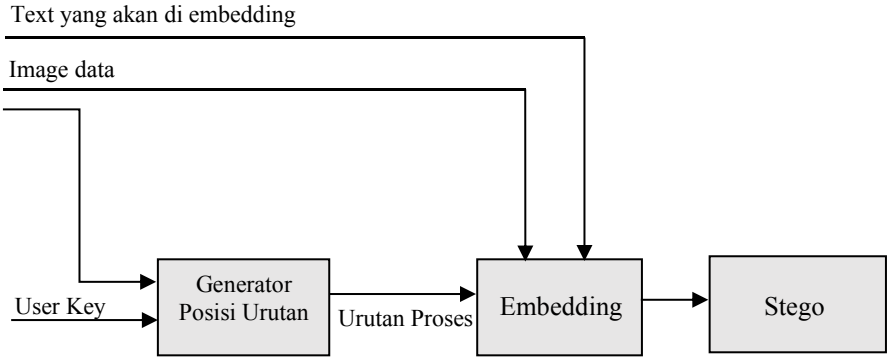
merah tersebut secara berarti. Lagi pula, mata manusia tidak dapat membedakan perubahan yang kecil. Misalkan segmen data citra sebelum perubahan :

0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 0 1 1 0 1 1 1 1
Segmen data citra setelah ‘0 1 1 1 ‘ disembunyikan :



Berdasarkan hasil penyisipan atau embedding ke dalam sekumpulan piksel citra tersebut akan diperoleh kembali sekumpulan piksel yang telah berubah pada posisi bit terendah atau LSB dari piksel tersebut, sehingga LSB menggantikan nilai bit-bit terendah dari setiap piksel untuk disisipkan dan digantikan oleh bit yang mengandung pesan.

Penggunaan kunci-stego menjadi penting karena keamanan atas suatu sistem proteksi tidak bisa didasarkan pada kerahasiaan dari algoritma itu sendiri, tetapi karena adanya suatu kunci rahasia.



Gambar 6. Proses Penggunaan Kunci

Perancangan form dan modul sudah didefinisikan sebelumnya sehingga membentuk aplikasi yang utuh. Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada plainteks dengan satu karakter pada kunci. Oleh karena itu, panjang kunci setidaknya harus sama dengan panjang plainteks. Enkripsi dapat dinyatakan sebagai penjumlahan modul 26 dari satu karakter plainteks dengan satu karakter kunci Vigenere:

$Ci = (pi + ki \bmod m) \bmod 26$

dimana Ci, Pi dan Ki merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Sedangkan proses dekripsi dapat menggunakan persamaan berikut :

$pi = (Ci - ki \bmod m) \bmod 26$

dengan Di adalah karakter hasil dekripsi, Ci adalah karakter *cipher text* atau sandi, Ki adalah karakter kunci.

Sedangkan metode lain untuk melakukan proses enkripsi dengan metode *vigenere cipher* yaitu menggunakan *tabula recta* (disebut juga bujursangkar *vigenere*).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 7**.** Contoh Tabula Recta Algoritma Kriptografi Vigenere Cipher

Tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar[5]. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

Enkripsi (penyandian) dengan sandi Vigenère juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$$Ci = (Pi + Ki) \bmod 26$$

atau C = P + K kalau jumlah dibawah 26 dan - 26 kalau hasil jumlah di atas 26 dan dekripsi,

$$Pi = (Ci - Ki) \bmod 26$$

atau P = C - K kalau hasilnya positif dan + 26 kalau hasil pengurangan minus

Keterangan: Ci adalah huruf ke-i pada teks tersandi, Pi adalah huruf ke-i pada teks terang, Ki adalah huruf ke-i pada kata kunci, dan mod adalah operasi modulus (sisa pembagian).

Rumus enkripsi vigenere cipher :

$$Pi = (Ci - Ki) \bmod 26$$

atau

Ci = (Pi + Ki) – 26 kalau hasil penjumlahan Pi dan Ki lebih dari 26

Rumus dekripsi vigenere cipher :

$$Pi = (Ci - Ki) \bmod 26$$

atau

Pi = (Ci – Ki) + 26 kalau hasil pengurangan Ci dengan Ki minus

Dimana:

Ci = nilai desimal karakter ciphertext ke-i

Pi = nilai desimal karakter plaintext ke-i

Ki = nilai desimal karakter kunci ke-i

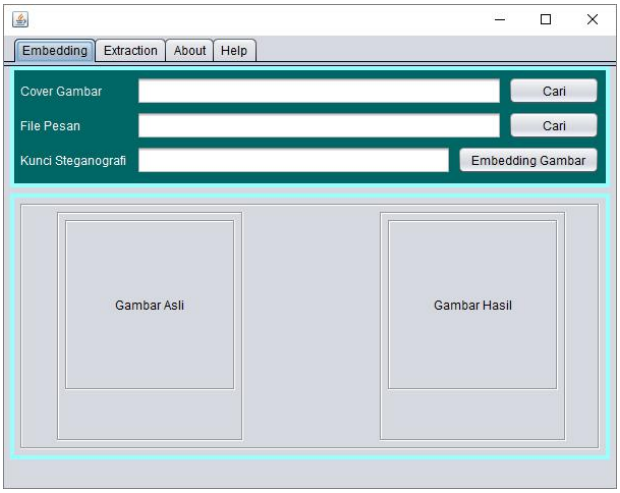
Nilai desimal karakter:

A=0 B=1 C=2 ... Z=25

Perangkat lunak Steganografi ini membutuhkan komponen pendukung seperti kebutuhan perangkat keras (*Hardware*), antara lain PC, Monitor VGA mempunyai resolusi minimal 800 x 1200 pixel, keyboard dan mouse untuk melakukan kegiatan user dan semua perangkat keras yang digunakan merupakan perangkat standar dalam sistem komputer

Penulis membangun perangkat lunak *steganografi* pada objek citra digital ini dengan menggunakan Visual Studio .NET 2010 sebagai compliler. Instrumen penelitian ini berupa form-form perangkat lunak dan *coding* dari perangkat lunak tersebut.

Berikut merupakan tampilan Form Steganografi pada gambar 8:



Gambar 8. Form Steganografi

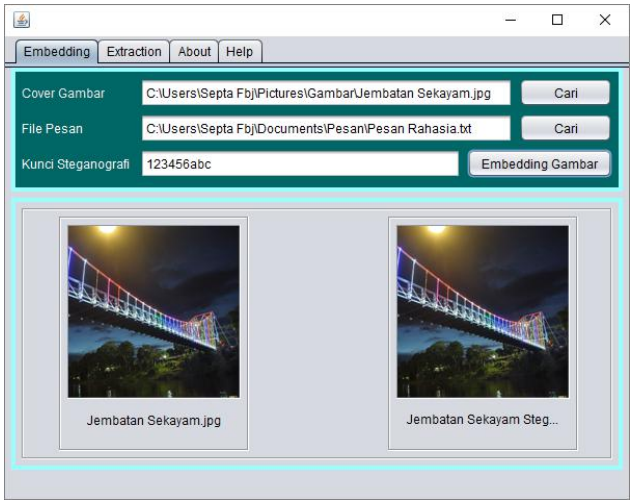
Fitur-fitur yang ada dalam halaman utama, yaitu Menu Embedding menampilkan tampilan halaman awal, form Embedding dipergunakan oleh user untuk melakukan penyisipkan file pesan ke dalam gambar. Rancangan Setelah modul dirancang ke dalam program tersebut, berikutnya melakukan *testing* pada form yang membuat modul tersebut. Setelah setiap modul dan form terbentuk dan diuji, semua modul dan form tersebut kemudian disatukan dan dilakukan pengujian kembali akan integritasnya, termasuk didalamnya pengujian validitas input tiap form.

Pengujian terhadap suatu perangkat lunak bertujuan untuk melihat apakah perangkat lunak tersebut berfungsi sebagai aplikasi pengolahan citra yang dapat mengenal suatu citra dengan metode yang diinginkan. Pada pengujian perangkat lunak pengolahan citra ini, digunakan metode pengujian *blackbox*. Tipe *file* yang akan diuji adalah jpg (jpeg).

Dalam tahap ini, akan disisiplan sebuah citra. Adapun tampilan dari citra pada gambar 9 yang akan dijadikan pengujian perangkat lunak sebagai berikut:

Gambar 9. Objek yang akan diuji

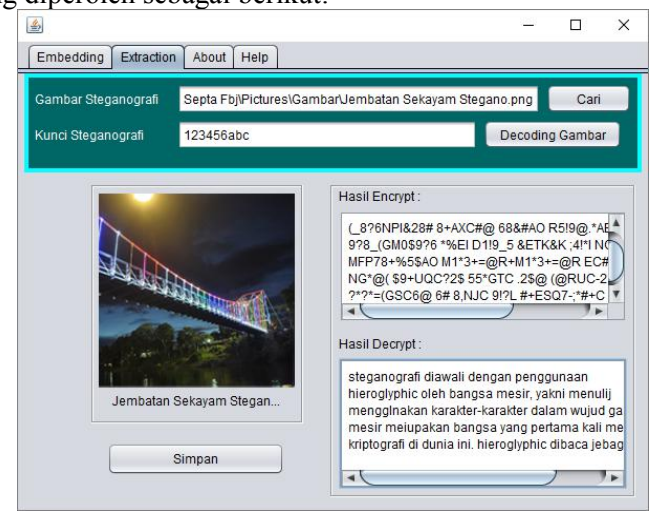
Selanjutnya dilakukan pengujian terhadap kemampuan sistem dalam melakukan penyisipan pesan ke dalam gambar. Pada tahap ini, akan diuji parameter kestabilan sistem, serta kestabilan hasil yang diharapkan. Adapun hasil pengujian pada gambar 10 yang diperoleh sebagai berikut:



Gambar 10. Hasil Pengujian Penyisipan Pesan

Pada pengujian ini, terlihat sistem telah dapat melakukan penyisipan citra digital. Berdasarkan hasil tampilan tersebut penyisipan citra telah dapat dilakukan dengan sempurna, sehingga diambil kesimpulan bahwa perangkat lunak ini tidak memiliki masalah dalam melakukan penyisipan pesan ke dalam citra digital.

Selanjutnya dilakukan pengujian terhadap kemampuan sistem dalam melakukan pengekstrakan citra digital file pesan yang sudah disiapkan. Pada tahap ini, akan diuji pengekstrakan kestabilan sistem, serta kestabilan hasil yang diharapkan. Adapun hasil pengujian pada gambar 11 yang diperoleh sebagai berikut:



Gambar 11. Hasil Pengujian Pengekstarkan Pesan

Rancangan pada form extraction digunakan user untuk melakukan pengekstrakan file pesan yang sudah disisipkan ke dalam gambar.

Dari hasil pengujian tersebut terlihat sistem telah dapan melakukan penyisipan pesan terhadap citra digital. Berdasarkan hasil tampilan tersebut penyisipan terhadap citra telah dapat dilakukan dengan sempurna, sehingga dapat diambil kesimpulan bahwa proses penyisipan tidak memiliki masalah dalam melakukan penyisipan citra digital.

Pada table 1 dibawah ini dapat dilihat hasil dari pengujian dilakukan dengan mengunakan gambar asli dengan format PNG dan JPG dimana setiap gambar memiliki ukuran dan tinggi serta lebar yang berbeda, berikut hasil pengujian proses embedding dan extraction dari perangkat lunak steganografi ini dengan menggunakan media:

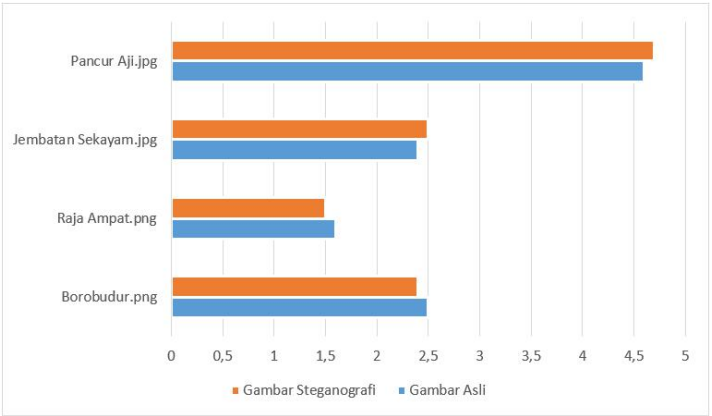
Tabel 1. Hasil Embedding dan Extraction

No	Nama	Gambar Asli	Resolusi	Gambar Stegano
1	Borobudur.png		358 X 358	
2	Raja Ampat.png		564 X 564	
3	Jembatan Sekayam .jpg		678 X 678	
4	Pancur Aji.jpg		856 X 856	

Bisa dilihat pada pengujian diatas merupakan hasil dari pengujian yang dilakukan dengan perangkat lunak steganografi, dimana pada setiap resolusi tidak mengalami perubahan sebaliknya pada *size*nya mengalami perubah pada gambar aslinya. Pada setiap format yang telah di *embedding* akan diubah menjadi format yang sesuai pada gambar yang diinputkan pada table 2.

Tabel 2. Hasil Pengujian Embedding dan Extraction

Nama File	Ukuran File		Status	
	Source	Hasil	Dapat disisipkan	Dapat diekstrak
Borobudur.png	257 KB	250 KB	Ya	Ya
Raja Ampat.png	164 KB	158 KB	Ya	Ya
Jembatan Sekayam.jpg	244 KB	251 KB	Ya	Ya
Pancur Aji.jpg	466 KB	479 KB	Ya	Ya



Gambar 12. Hasil Embedding dan Extraction

Dapat dilihat dari grafik dan tabel diatas menjelaskan hasil dari sebuah proses perangkat lunak steganografi yang menjelaskan hasil sebelum dan sudah proses embedding dengan format yang sudah ditentukan.

4. KESIMPULAN

Dalam penelitian ini memberikan kesimpulan yang mengindikasikan diperlukannya pengamanan data dengan menggunakan teknik steganografi. Dari hasil analisis dan perancangan perangkat lunak steganografi pada suatu gambar atau citra digital yang telah di lakukan dapat di ambil kesimpulan sebagai berikut:

a. Besarnya resolusi gambar ataupun pesan dapat mempengaruhi hasil dari penyisipan pesan kedalam gambar dikarenakan proses penyisipan yaitu menggabungkan kedua file gambar dan pesan menjadi satu.
b. Penyisipan gambar dan metode least significant bit (LSB) dapat diimplemetasikan untuk menyisipkan pesan rahasia pada bit pixel gambar yang terenendah.
c. Perangkat lunak telah dilakukan pengujian dan cukup baik dalam penyisipan dan mengekstrasi pesan rahasia dengan baik, karena pesan yang diekstrasi mirip dengan pesan yang disisipkan.
d. Efisiensi waktu yang ditempuh dalam proses embeeding relatif cepat.
e. Program aplikasi yang dirancang dapat membantu seseorang yang ingin mengirim pesan rahasia yang tidak ingin dipublikasi atau diketahui siapapun selain penerima.

5. SARAN

Perangkat lunak ini selanjutnya dapat di kembangkan dan modifikasi metode least significant bit (LSB) dan Vigenere Cipher guna untuk mereduksi jumlah noise. Perangkat lunak ini dapat dikembangkann dengan menambah format citra digital yang dapat disisipkan seperti gambar bergerak (GIF). Perangkat lunak ini dapat dikembangkan sehingga pengguna dapat melakukan lebih dari satu kali proses penyisipan pada gambar dan pesan rahasia secara bersamaan serta dapat melakukan embedding dan extraction folder. Disarankan untuk merancang tampilan (interface) kembali agar aplikasi lebih menarik.

Penulis menyadari bahwa perangkat lunak steganografi yang dibuat ini belum sepenuhnya sempurna. Penulis berharap agar pembaca dan programmer yang lebih handal dapat mengembangkan dan menyenmpurnakan kekurangan dari perangkat lunak ini. Berikut ini adalah beberapa saran yang dapat diberikan untuk penelitian lebih lanjut :

a. Penelitian selanjutnya dapat mengembangkan dan memodifikasi metode least significant bit (LSB) dan Vigenere Cipher guna untuk mereduksi jumlah noise.
b. Perangkat lunak ini dapat dikembangkann dengan menambah format citra digital yang dapat disisipkan seperti gambar bergerak (GIF).
c. Perangkat lunak ini dapat dikembangkan sehingga pengguna dapat melakukan lebih dari satu kali proses penyisipan pada gambar dan pesan rahasia secara bersamaan serta dapat melakukan embedding dan extraction folder.
d. Disarankan untuk merancang tampilan (interface) kembali agar aplikasi lebih menarik.

DAFTAR PUSTAKA

[1] Johnson Neil F, 2006. *Steganography.* Center for Secure Information Systems, George Mason University.
[2] Munir, Rinaldi., 2006. *Kriptografi.* Informatika, Bandung.
[3] Ariyus, Dony, 2008. *Pengantar Ilmu Kriptografi Teori Analisis. dan Implementasi,* Andi, Yogyakarta.
[4] Ariyus, Dony, 2009. *Keamanan Multimedia*, Andi. Yogyakarta.
[5] Piper, Fred dan Sean Murphy, 2002. *Cryptography A Very Short Introduction*. Oxford.
[6] Pressman, Roger S, 2002. *Rekayasa Perangkat Lunak Pendekatan Praktisi*. CN Harnaningrum, Andi Offset, Yogyakarta.