Rancangan Perangkat Lunak Steganografi Pengamanan Pesan Teks Dalam File Gambar

Ramayana, Widyasari
[1,2]STMIK Pontianak; Jln. Merdeka Barat No. 372 Pontianak, (0561)73555/(0561)737777
[3]Jurusan Teknik Informatika, STMIK Pontianak
e-mail: **93ramayana@gmail.com, widyasari@stmikpontianak.ac.id**

Abstrak

Saat ini dapat terlihat jelas bahwa teknologi informasi sudah berkembang sedemikian pesat sehingga menjadi hal yang umum dan bahkan sudah menjadi keharusan bagi berbagai pihak untuk memenuhi kebutuhannya. Pihak-pihak yang saling berkomunikasi tersebut kemudian sampai pada kebutuhan lain yang juga penting, yaitu kebutuhan privasi akan informasi yang mereka komunikasikan. saat ini banyak sekali informasi–informasi yang sifatnya sangat sensitif tetapi dikirimkan melalui media yang terbuka sepenuhnya untuk umum, misalnya melalui internet yang dapat diakses oleh siapapun ,maka kemudian lahirlah suatu seni penyembunyian pesan data yang dikenal dengan steganografi. Tujuan dari penelitian ini adalah merancang dan membuat suatu aplikasi steganografi dengan algoritma Jsteg yang secara spesifik diterapkan pada format file bmp,jpeg, png yang sudah sangat umum digunakan sebagai format file image.

Kata kunci*—Steganografi,Android, Java, Image*

Abstract

When it was clear that information technology has been developing rapidly in such that it becomes a common thing and even has become a must for various parties to meet their needs. The parties communicate each other until later at another important requirements, namely the privacy requirements will be the information they communicate. currently an awful lot of information – information which is highly sensitive but delivered through media that are open to the public, for example via the internet which can be accessed by anyone, then later was an art concealing the message data is known as steganography. The purpose of this research is to design and make an application with steganography algorithms Jsteg specifically applied to the file formats bmp, jpeg, png, which is already very common is used as a file format image.

Keywords*— Steganography, Android, Java, Image*

1. PENDAHULUAN

Perkembangan teknologi yang begitu pesat saat ini mempermudah manusia dalam melakukan berbagai hal karena teknologi dapat mempersingkat jarak dan waktu. Dalam bidang teknologi komputer dan internet, banyak sekali orang yang menggunakan dan memanfaatkan teknologi tersebut. Salah satu contoh nyata adalah banyaknya pengiriman informasi melalui jaringan internet. Tentunya pengiriman informasi melalui internet sangatlah menguntungkan karena selain cepat, biayanya pun murah. Namun di sisi lain juga memiliki kelemahan yaitu informasi yang dikirim dapat dengan mudah dan tanpa diketahui pemilik informasi, dicuri oleh oknum yang tidak bertanggung jawab. Munculnya kebutuhan pengiriman sebuah informasi

yang bersifat rahasia atau privasi yang tidak diketahui oleh pihak lain, hanya antara pengirim dan penerima saja.

Sebagai contoh, pertukaran informasi penting sebuah perusahan, pertukaran informasi rahasia organisasi militer pemerintahan dan pihak lainnya. Hal ini membuat orang yang tidak memiliki hak atas informasi tersebut berusaha untuk mengetahaui isi dari informasinya. Ini membuat peroses pengiriman informasi rahasia yang aman, cepat dan akurat menjadi prioritas utama. Oleh karena itu dikembangkanlah aplikasi steganografi (*steganography*) yang merupakan teknik untuk menyisipkan pesan atau data rahasia ke dalam suatu media yang tidak terlihat menunjukan ciri-ciri perubahan dari kualitas dan struktur media semula, sehingga mengurangi kecurigaan sebab tidak ada pihak ketiga yang mengetahui keberadan pesan atau data rahasia tersebut. *Steganography* dapat diterapkan pada berbagai media digital, misalnya teks, citra(image), suara(audio), dan vidio.

Steganography pada image merupakan teknik penyisipan pesan pada gambar dengan menyisipkan text pada bit-bit yang memiliki nilai terendah dalam barisan biner, untuk *steganography* pada Mp3 yaitu menyembunyikan pesan ke dalam sinya yang membentuk echo kemudian pesan disembunyikan dengan memvariasikan tiga parameter dalam echo. Sedangkan pada *steganography* pada vidio yaitu pesan atau data disisipkan pada setiap frame vidio. Dalam berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna 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 pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.

Karena memanfaatkan bit-bit LSB, metode ini tidak digunakan pada media yang mengalami kompresi terutama jenis lossy compression karena akan menghilangkan bit-bit LSB tersebut. Penggunaan metode LSB umumnya tidak mengubah ukuran file dan bekerja dengan baik pada file gambar atau audio yang memiliki resolusi atau bit rate tinggi. Sedangkan untuk algoritma yang digunakan yaitu algoritma JSEG, algoritma jseg menyisipkan data kedalam koefesien DCT JPEG secara sekuensial dengan cara mengganti LSB (*Least Significant Bit*) dengan LSB dari data yang akan disisipkan.

2. METODE PENELITIAN

Dalam melakukan penelitian, penulis menggunakan studi literatur dan "eksperimen murni menggunakan rancangan random. Penulis melakukan kajian atau pendekatan tentang bagaimana memecahkan masalah serta mendefinisikan, dengan melakukan eksperimen yang berkaitan erat dengan permasalhan yang ingin dipecahkan. Penulis juga mencari referensi dan informasi sebagai dasar dalam perancangan apliksi.

2.1 Metode Pengumpulan Data

Adapun jenis data yang digunakan penulis dalam penelitian ini yaitu, sebagai berikut:

a.Data primer

Merupakan sumber data yang diperoleh secara langsung dari sumber asli atau pihak pertama. Data primer secara khusus dikumpulkan oleh peneliti untuk menjawab pertanyaan riset atau penelitian. Data primer dapat berupa pendapat subjek riset (orang) baik secara individu maupun kelompok, hasil observasi terhadap suatu benda (fisik), kejadian, atau kegiatan, dan hasil pengujian. Menurut Sugiyono (2010:137) menyatakan bahwa, "sumber perimer adalah sumber data yang langsung memberikan data kepada pengumpul data.".

b.Data sekunder

Data sekunder adalah data yang tidak didapatkan secara langsung dari objek penelitian, melainkan sumber data yang diperoleh peneliti secara tidak langsung melalui media perantara. Data sekunder pada umumnya berupa bukti, catatan, atau laporan historis yang telah tersusun dalam arsip, baik yang dipublikasikan dan yang tidak dipublikasikan. Data

sekunder antaralain disajikan dalam bentuk tabel-tabel, diagram-diagram, atau mengenai topik penelitian.

2.2 Teknik Pengumpulan Data

Teknik pengumpulan data adalah cara-cara yang dilakukan untuk mencari, mengumpulkan dan memperoleh data untuk digunakan dalam melakukan penelitian, baik itu data yang diperoleh dengan servei langsung maupun dengan penggalian informasi. Menurut Sugiyono (2013:224) teknik pengumpulan data merupakan langkah yang paling strategis dalam penelitian, karena tujuan utama dari penelitian adalah mendapatkan data. Untuk memperoleh data dan informasi dalam penelitian ini, penulis menggunakan teknik pengambilan data sebagai berikut :

a.Studi Literatur

Teknik studi literatur mengenai steganogafi dan matenatika, bahwa pemograman java, encode dan decode dan lainnya, untuk menghasilkan aplikasi keamanan pesan text yaitu steganografi media image.

b.Studi Dokumentasi

Teknik dokumentasi berupa studi keputusan dan kajian dari buku-buku, jurnal-jurnal pendukung (hardcopy dan software), literatur dari internet dan sejumlah dokmen mengenai data variabel yang perlukan.

c.Observasi

Pada penelitian ini observasi yang dilakukan dengan pengamatan langsung mengumpulkan data mengenai dokumentasi yang mengacu pada instrumen pengamatan yang berisi definisi-definisi dari item-item data. Melakukan kajian letretur yang berkaitan dengan penelitian yang dilakukan, pengumpulan data yang diperoleh dari sumber tertulis seperti: literatur artikel, berbagai websait, dan tulisan ilmiah yang dianggap terkait dan relevan dengan topik penelitian

2.3 Pengembangan Perangkat Lunak RAD

Penulis mengunakan metode perancangan RAD (*Rapid Application Developement*) karena peroses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat dan pemanfaatan fungsi yang telah ada sebelumnya. Adapun langka-langkah yang dilakukan penulis yaitu:

a. *Bunssing Modeling*. Pada tahap ini, penulis mendaftarkan dan mendefinisikan fungis-fungsi yang akan dipakai dalam pembuatan aplikasi.
b. *Data modeling*. Penulis mengunakan informasi yang didapat dalam tahap diatas untuk menentukan banyaknya modul dan form yang akan digunakan dalam program tersebut.
c. *Process Modeling*. Form dan modul yang sudah didefinisikan sebelumnya beserta komponennya disatukan untuk menentukan suatu program untuk. Hubungan antara modul dengan form juga didefinisikan oleh penulis
d. *Application Generation.* Penulis membangun aplikasi Steganografi pengaman pesan teks pada gambar dengan mengunakan metode LSB ((*Least Significant Bit*) ini mengunakan program *Eclipse* dengan instrumen penelitian berupa *algoritma JSEG, flowchart* dan *pseudocode.*
e. *Testing and turnover.* Setelah modul dirancang ke dalam program tersebut penulis melakukan testing pada form yang membuat modul tersbut.setelah setiap modul dan form terbentuk dan diuji, semua modul dan form tersebut kemudian disatukan dan dilakukan pengujian kembali akan integritasnya, termasuk didalamnya pengujian validasi input tiap form.

2.4 Alat Pengembangan Sistem Perangkat Lunak

2.4.1 Flowchart

Flowchart adalah adalah suatu bagan dengan simbol-simbol tertentu yang menggambarkan urutan proses secara mendetail dan hubungan antara suatu proses (instruksi) dengan proses lainnya dalam suatu program

2.4.2 Algoritma

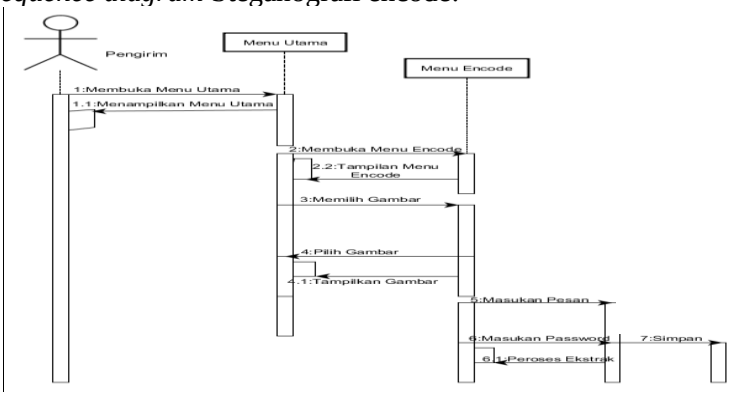
Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis". Kata logis merupakan kata kunci dalam algoritma. Langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar. Dalam beberapa konteks, algoritma adalah spesifikasi urutan langkah untuk melakukan pekerjaan tertentu. Pertimbangan dalam pemilihan algoritma adalah, pertama, algoritma haruslah benar. Artinya algoritma akan memberikan keluaran yang dikehendaki dari sejumlah masukan yang diberikan. Tidak peduli sebagus apapun algoritma, kalau memberikan keluaran yang salah, pastilah algoritma tersebut bukanlah algoritma yang baik.

2.4.3UML (Unified Modelling Language)

Unified Modeling Language (UML) adalah bahasa pemodelan secara grafis untuk menspesifikasikan, menvisualisasikan, membangun, dan mendokumentasikan seluruh rancangan sistem perangkat lunak. Penggunaan model ini bertujuan untuk mengidentifikasikan bagian-bagian yang termasuk dalam lingkup sistem yang dibahas dan bagaimana hubungan antara sistem dengan subsistem maupun sistem lain di luarnya. Selain itu UML menggunakan class dan operation dalam konsep dasarnya, maka ia lebih cocok untuk penulisan

2.4.4 Sequence Diagram

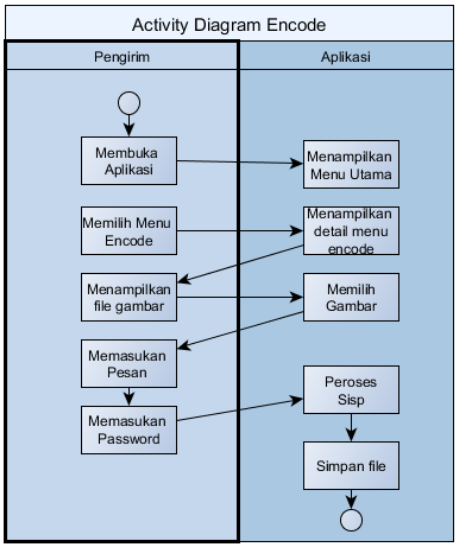
Sequence Diagram digunakan untuk menggambarkan scenario atau rangkaian langkah-langkah yang dilakukan sebagai suatu respon dari kejadian untuk menghasilkan output tertentu. Berikut adalah *Sequence diagram* Steganografi encode:



Gambar 2.2 Diagram Sequence Encode

2.4.5 Activity Diagram

Menggambarkan rangkaian aliran dari aktivitas, digunakan untuk mendeskripsikan aktifitas yang dibentuk dalam suatu operasi sehingga dapat juga digunakan untuk aktifitas lainnya seperti use case atau interaksi berikut merupakan gambaran dari activity steganografi



Gambar 2.4 Activity Diagram Encode

2.4.6 Use Case Diagram

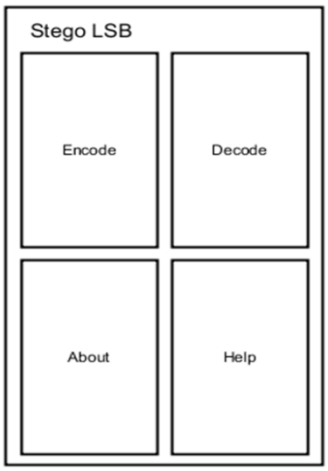
Gambar 2.6 Use case digram Steganografi

3. HASIL DAN PEMBAHASAN

3.1 Tampilan Menu Utama

Dari menu utama dari perangkat lunak steganografi ini ada terdapat empat tombol peroses yaitu:

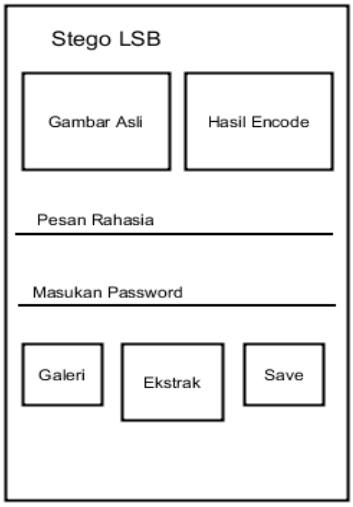
a. Tombol encode berfungsi untuk menampilkan tampilan dari menu encode.
b. Tombol decode berfungsi untuk menampilkan tampilan dari menu decode.
c. Tombol about berfungsi untuk menampilkan tampilan dari menu about.
d. Tombol help berfungsi untuk menampilkan tampilan dari menu help.



Gambar 3.1 Rancangan Menu Utama

3.2 Tampilan Menu Encode

Pada saat perangkat lunak steganografi ini dijalankan, maka pertama kali yang akan ditampilkan yaitu menu utama dimenu ini user bisa langsung memilih menu encode yang diinginkan. Tampilan encode berfungsi untuk melakukan peroses penyisipan pesan kedalam file penampungan yaitu berupa file image sebagai *cover-object*nya. Tampilan rancangan menu encode dapat dilihat pada gambar dibawah ini:



Gambar 3.2 Rancangan Menu Encode

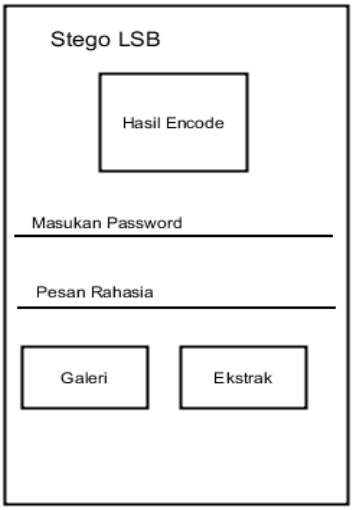
Pada gambar 3.2 merupakan desain tampilan menu encode, yang dirancang degan beberapa tombol dan *textbox* untuk melakukan peroses ekstraksi pesan rahasia yaitu:

a. Pada bagian tampilan gambar asli berfungsi untuk menempatkan cover yang akan disisipkan pesan rahasia.
b. Pada bagian tampilan hasil encode merupakan isi dari cover yang telah disisipkan pesan rahasia dan juga telah memiliki password.
c. Sedangkan pada bagian pesan rahasia berfungsi untuk memasukan pesan yang akan disispkan pada cover yang telah dipilih.

d. Sedangkan pada bagian memasukan password berfungsi untuk memasukan password yang akan menjadi kunci dari cover dan pesan rahasia yang akan diekstrak.
e. Tombol galleri digunakan untuk memilih gambar yang akan menjadi cover tempat penyisipan pesan rahasia
f. Tombol ekstrak digunakan untuk mengabungkan antara pesan rahasia, cover dan juga password untuk dijadikan satu file.
g. Tombol save digunakan untuk menyimpan *cover-object* yang telah berisikan pesan rahasia.

3.3. Tampilan Menu Decode

Tampilan menu decode berfungsi untuk melakukan proses pengekstrakan pesan dari file *cover-object* atau file image yang telah disisipkan pesan rahasia, dilakukan proses ekstrak untuk memisahkan pesan rahasi dan data penyimpanan dengan menggunakan kunci yang sama pada peroses encode, adapun tampilan decod dapat dilihat pada gambar dibawah ini:



Gambar 3.3 Rancangan Menu Decode

Didalam tampilan menu decode terdapat beberapa tombol untuk melakukan peroses ekstraksi yaitu:

a. Pada bagian tampilan hasil encode berfungsi untuk menempatkan cover yang telah berisi pesan rahasia akan diekstrak.
b. Sedangkan pada bagian memasukan password berfungsi untuk memasukan password yang sama pada saat peroses encode.
c. Sedangkan pada bagian pesan rahasia berfungsi untuk menampilkan isi dari pesan rahasia yang telah dipisahkan dari covernya.
d. Tombol galleri digunakan untuk memilih gambar yang telah berisikan pesan rahasia yang telah disisipkan pada saat peroses.
e. Tombol ekstrak pada decode digunakan untuk memisahkan antara pesan rahasia dengan covernya.

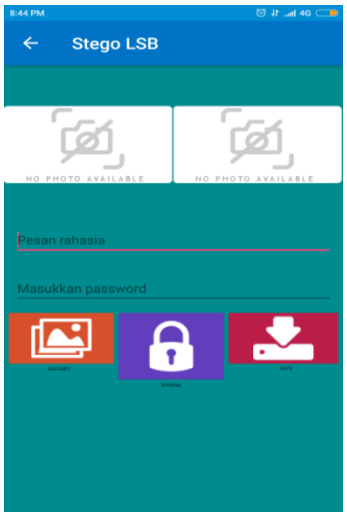
3.4. Cara Kerja Perangkat Lunak Steganografi

Perangkat lunak steganografi ini merupakan perangkat lunak untuk melakukan proses enkripsi dan dekripsi data pada file image. Pada saat program dieksukusi, terlebih dahulu akan muncul tampilan utama berikut adalah tampilan dan cara kerja dari tampilan utma ke tampilan encode.

a. Agar bisa melakukan peroses penyisipan pesan rahasia pada media file image, maka lakukan peroses berikut ini:
   1. Klik tombol “Encode” pada menu utama maka secara otomatis akan langsung menuju ke menu encode.

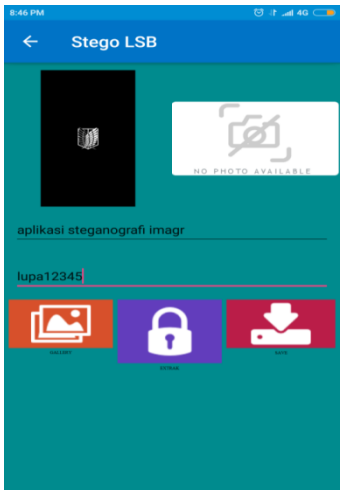
Gambar 3.4 Tampilan Menu Utama

   2. Muncul tampilan menu encode



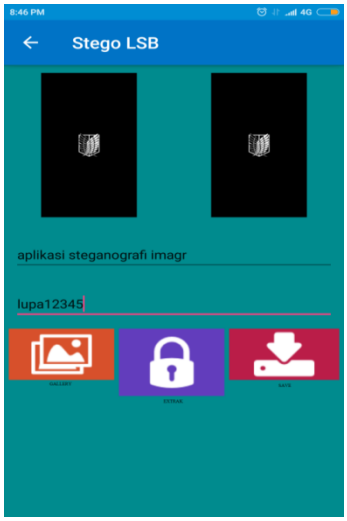
Gambar 3.5 Tampilan Menu Encode

   3. Klik tombol “Gallery” pada menu apa bila user tidak memilih gambar satu gambar pada gallery maka akan muncul pesan pemberitahuan pada menu encode, maka peroses akan diulang kembali pada menu encode lalu pilih gambar yang diinginkan, setelah itu akan muncul menu encode yang sudah terdapat gambar yang dipili.



Gambar 3.6 Tampilan Menu Encode Cover Asli

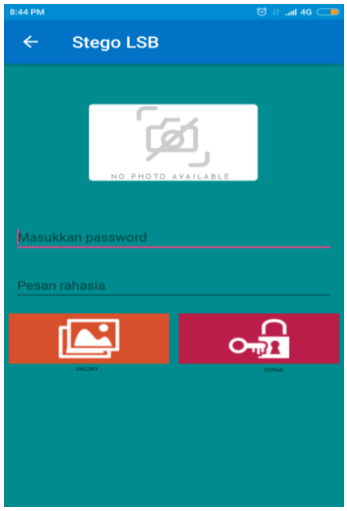
4. Kemudian masukan pesan rahasia yang akan disisipkan dan masukan *password* sesuai yang di inginkan, setelah itu klik tombol *ekstrak* tungu sampai peroses selesai



Gambar 3.7 Tampilan Menu Encode Hasil Ekstrak

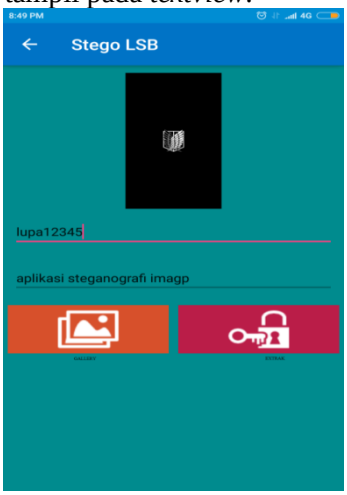
5. Kelik menu “Save” untuk menyimpan fill image yang sudah terdapat pesan rahasianya.

b. Untuk peroses pengekstrakan pesan rahasia pada media file image, maka lakukan proses berikut ini:
   1. Klik tombol “Decode” pada tampilan menu utama,
   2. Kemudian akan muncul tampilan decode lalu klik tombol “Gallery”.



Gambar 3.8 Tampilan Menu Decode

3. Masuk ke gallery pilih gambar yang sebelumnya sudah berisikan pesan rahasia pada saat peroses encode
4. Setelah user memasukan *Password* yang benar dan mengklik tombol "Ekstrak" maka peroses akan dilakukan, setelah itu pesan rahasia yang terdapat pada -*cover-object*nya akan tampil pada *textview*.



Gambar 3.11 Tampilan Hasil Ekstrak Menu Decode

3.5. Pengujian Image Menggunakan LSB

Pada tahap ini pengujian dilakukan dengan mengunakan image asli dengan format JPEG,BMP dan PNG dimana setiap image memiliki ukuran dan tingi serta lebar yang berbeda, berikut merupakan image yang menjadi *cover-objeck* pengujian dalam steganografi ini:

Tabel 3.1
Hasil Pengujian pada format PNG

	Image Asli

	Hasil Encode

Tabel 3.2
Hasil Pengujian Image pada LSB

Nama	Format	Ukuran (pixel)	Ukuran Sebelum (kb)	Ukuran Sesudah (kb)
Stego1 (Stego936)	JPEG (PNG)	720x1280	27,8	55,7
Stego 2 (Stego3577)	PNG (PNG)	275x183	117	60,2
Stego 3 (Stego4666)	BMP (PNG)	640x480	900	396

Dari Percobaan sistem yang dilakukkan membuktikan bahwa semua tipe karakter baik huruf besar maupun huruf kecil, angka dan semua jenis simbol akan diperoleh jumlah byte yang sudah dikompresi atau jumlah bytenya berkurang. Dan terbukti akan dapat dikompresi tanpa ada yang terlewatkan. Apabila dilakukan dekompres maka akan menghasilkan outputan yang sama5dengan inputannya tadi atau dengan kata lain data sudah benar-benar valid.

4. KESIMPULAN

Setelah melalui proses penyelesaian skripsi yang berjudul “Perancangan dan Pengujian Perangkat Lunak Steganografi Pengaman Pesan Text Dalam File Gambar Berbasis Android”, penulis menarik kesimpulan sebagai berikut :

a. Pada proses penyembunyian penyisipan atau encode menggunakan algoritma Jseg, dilakukan terlebih dahulu untuk menentukan pixel-pixel yang akan disisipi dari kata kunci yang diinput. Kemudian pixel-pixel yang terpilih akan disisipi oleh bit panjang pesan dan bit-bit karakter pesan yang akan disisipi.
b. Pada proses penyembunyian penyisipan membutuhkan dua buah masukan yaitu media cover sebagai tempat penyisipan pesan dan pesan rahasia. Media cover yang digunakan adalah file image dan pesan rahasia yang dapat disisipkan berupa teks, file teks. File image yang digunakan adalah file image dengan format bmp, Sedangkan pada proses penguraian hanya dibutuhkan satu buah masukan. Masukan tersebut adalah text.

5. SARAN

Penulis ingin memberikan beberapa saran yang mungkin berguna untuk perkembangan lebih lanjut pada perancangan perangkat lunak steganografi menggunakan Algoritma Jseg, yaitu:

a. Algoritma Jseg bukan satu-satunya algoritma yang dipakai dalam system steganografi, akan tetapi banyak algoritma-algoritma yang dipakai dalam sistem steganografi.
b. Dalam perangkat lunak ini, tidak dipakai enkripsi dalam implementasinya, jadi agar dapat dikembangkan dengan enkripsi pada penyembunyian pesannya.
c. Perangkat lunak ini dapat dikembangkan dengan algoritma lainnya, sehingga mempermudah menyelesaikan masalah dalam bidang steganografi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada Tuhan YME, Ketua STMIK Pontianak, Ketua Jurusan Teknik Informatika STMIK Pontianak, Pembimbing Skripsi dan Jurnal, orangtua tercinta, teman dekat dan kerabat yang telah memberi dukungan financial terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Angga Syamditia Rahman (2015), Perancangan Perangkat Lunak Steganografi Mengunakan Algoritma Jseg : STMIK Budidarma medan
[2] Adi Nugroho. (2010). Rational Rose untuk Pemodelan Berorientasi Objek Informasi : Bandung.
[3] Adi Nugrpho. (2010). Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP . Yogyakarta: CV.Andi Offset.
[4] Ariyus, Dony. (2009) Keamanan Multimedia, Andi.Yogyakarta.
[5] Alston Evan Wijaya (2012), Implementasi Steganografi untuk Penyembunyian Pesan pada Video dengan Metode LSB : Teknik Informatika Politeknik Caltex Riau,
[6] Bruegge, Bernd dan Dutoit, Allen H (2010). Object-Oriented Software Engineering Using UML, Patterns, Java, Third Edition. Pearson Education, Inc., USA.
[7] Basuki Rakhmat dan Muhammad Fairuzabadi, M.Kom (2010), Steganografi Menggunakan Metode Least Significant Bit Dengan Kobinasi Algoritma Kriptografi Vigenere Dan RC4
[8] Citra Dewi Astuti Br Tarigan (2014) Steganografi Pada File Audio Mp3 Untuk Pengamana Data Mengunakan Metode Least Significat Bit : STMIK Budi darma Medan.
[9] Desi Lilyani (2014), Implementasi Steganografi Pada Citra Digital Dengan Menggunakan Metode Dynamic Cell Spreading : STMIK Budi darma Medan.