

APLIKASI STEGANOGRAFI UNTUK PENYEMBUNYIAN DATA KE DALAM CITRA DIGITAL DENGAN KOMBINASI METODE LEAST SIGNIFICANT BIT (LSB) DAN ALGORITMA VIGENERE CIPHER

Diding darisman¹, Petrus Sokibi², Marsani Asfi³

Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) CIC Cirebon
Jalan Kesambi No 202 Telp 220250

Email : DidingDarisman@gmail.com, petrus.sokibi@cic.ac.id, marsani.asfi@cic.ac.id

Abstrak

Steganografi adalah teknik yang digunakan untuk menyisipkan informasi di dalam media lainnya dengan tujuan menjaga keamanan informasi. Steganografi membutuhkan dua media yang berbeda, yaitu media penampung (cover parent) dan informasi yang akan disisipkan (child file). Media penampung dan data yang disisipkan dapat berupa gambar, suara, teks, dan video.

Dalam skripsi ini proses steganografi dibagi menjadi dua bagian yaitu proses steganografi untuk penyembunyian file bertipe teks dan steganografi untuk penyembunyian file bertipe image (jpg/jpeg, bmp, png dan gif), media penampung atau cover parent yang digunakan berupa file citra dengan format png/jpg untuk stegano tipe teks dan format bmp untuk stegano tipe image. Metode Steganografi yang digunakan dalam skripsi adalah metode steganografi least significant bit (LSB) yang dikombinasikan dengan algoritma vigenere cipher, metode LSB merupakan metode yang paling banyak digunakan karena kesederhanaan dalam prosesnya. Cara kerja metode ini adalah dengan memodifikasi bit LSB dari media penampung (cover parent) dengan bit-bit dari informasi yang akan disembunyikan.

Aplikasi Steganografi LSB ini tidak tahan terhadap manipulasi citra seperti crop, resize, rotate dan grayscale, oleh karena itu diperlukan pengembangan aplikasi lebih lanjut dengan metode lain yang lebih tahan terhadap manipulasi citra digital. Dalam pembuatan aplikasi steganografi ini, penulis menggunakan bahasa pemrograman Java.

Kata Kunci : steganografi, citra, teks, metode lsb, vigenere cipher.

Abstract

Steganography is a technique used to insert information in other media with the aim of ensuring information security. Steganography requires two different media, ie media container (parent cover) and information to be inserted (child files). Media reservoir and the data inserted may include images, sounds, text, and video.

In this thesis steganography is divided into two parts, namely steganography for hiding files of type text and steganography for hiding files of type image (jpg / jpeg, bmp, png and gif), media parent container or cover used in the form of image file formats png / jpg to stegano type text and bmp format to stegano type of image. Steganography methods used in the thesis is a steganography method of least significant bits (LSB) combined with vigenere cipher algorithm, the LSB method is the method most widely used because of the simplicity of the process. This method works is by modifying the LSB bits of the media container (parent cover) with bits of information to be hidden.

LSB Steganography Application is not resistant to image manipulation such as crop, resize, rotate and grayscale, therefore, requires the development of further applications with other methods that are more resistant to manipulation of digital images. In making this steganography applications, the authors use the Java programming language.

Keywords: steganography, image, text, method lsb, vigenere cipher.

1. PENDAHULUAN

Informasi saat ini sudah menjadi bagian yang tidak dapat dipisahkan dari kehidupan manusia. Hampir semua informasi telah disimpan dalam format file data ke dalam media digital seperti komputer, harddisk eksternal, *mobile phone*, dan lain-lain. Informasi yang disimpan dalam media digital memiliki beberapa keuntungan diantaranya mudah disimpan, mengurangi penggunaan kertas dan lebih tahan lama. namun disamping itu juga memiliki beberapa kelemahan diantaranya keasliannya mudah diubah dan mudah untuk diduplikasi. Beberapa informasi yang dinilai penting seperti dokumen negara atau perusahaan memerlukan pengamanan lebih untuk menjamin kerahasiaannya.

Banyak cara untuk mengamankan informasi yang disimpan dalam media digital, salah satu cara pengamanan informasi adalah dengan kriptografi. Kriptografi adalah seni dan ilmu untuk menjaga keamanan pesan (Sumber:Yusuf Kurniawan,*Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*,2004:1). Algoritma kriptografi terdiri dari dua bagian yaitu fungsi enkripsi dan dekripsi. Enkripsi adalah seni mengubah informasi biasa yang disebut plaintext menjadi format yang tidak terbaca yang disebut ciphertext. namun ciphertext yang dihasilkan dari enkripsi tersebut memiliki keunikan sehingga dapat mengundang kecurigaan, untuk menyembunyikan informasi yang telah dienkripsi dapat digunakan steganografi. Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) dengan sedemikian rupa sehingga keberadaan (*eksistensi*) pesan tidak terdeteksi oleh indera manusia.(sumber:Rinaldi Munir, *Steganografi dan Watermarking*,2004:1). Steganografi dapat menyamarkan pesan atau informasi ke dalam suatu media tanpa orang lain menyadari bahwa di dalam media tersebut telah disisipi suatu pesan. Hasil keluaran steganografi adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila diinterpretasikan menggunakan indera manusia, namun berbeda apabila diinterpretasikan dengan perangkat pengolah data digital seperti komputer.

1.1. Identifikasi Masalah

Identifikasi Masalah yang akan dikaji dan diselesaikan dalam skripsi ini adalah :

1. Bagaimana menyembunyikan atau menyisipkan data *child (hidden file)* ke dalam citra digital dengan menggunakan metode *least significant bit (LSB)*?
2. Bagaimana mengkombinasikan algoritma kriptografi *vigenere cipher* dengan metode *least significant bit (LSB)* pada steganografi untuk meningkatkan keamanan data?
3. Bagaimana mengembalikan data *child (hidden file)* yang disisipkan dalam file stego sehingga menjadi file yang utuh?

1.2. Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah :

1. Membuat aplikasi yang dapat menjaga keamanan data atau informasi yang bersifat pribadi atau rahasia dengan menyembunyikannya ke dalam citra digital agar keberadaan dari data atau informasi rahasia tersebut tidak diketahui.
2. Mengimplementasikan penyembunyian data atau informasi kedalam citra digital dengan kombinasi metode *least significant bit* dan algoritma kriptografi *vigenere cipher* untuk meningkatkan keamanan data.

2. LANDASAN TEORI

2.1. Pengertian Program Aplikasi

Program Aplikasi adalah Sederetan kode yang digunakan untuk mengatur komputer agar dapat melakukan pekerjaan sesuai dengan keinginan dari permasalahan pengguna.

(Hartono Jogiyanto, *Pengenalan Komputer*, 2000, P113)

aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher-(Diding darisman , Petrus Sokibi, Marsani Asfi)

2.2. Pengertian Keamanan Informasi

Keamanan informasi mempunyai beberapa aspek yang harus dipenuhi, agar informasi dapat terjamin keaslian dan keamanannya. Aspek-aspek umum tersebut meliputi *Authentication*, *Integrity*, *Non-Repudiation* dan *Authority*.

(Kurniawan Yusuf, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, 2004, P2)

2.3. Pengertian Citra

Citra merupakan suatu *representasi spatial* dari suatu obyek, dalam pandangan 2D atau 3D. Citra digital merupakan suatu fungsi dengan nilai-nilai yang berupa intensitas cahaya pada tiap-tiap titik (*dot*) pada bidang yang telah diquantisasikan (diambil sampelnya pada interval diskrit).

(Rachmat Antonius, Roswanto Alphone, *Multimedia*, 2006)

2.4. Pengertian Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (*hiding message*) dengan sedemikian rupa sehingga keberadaan (*eksistensi*) pesan tidak terdeteksi oleh indera manusia.

(Munir Rinaldi, *Steganografi dan Watermarking*, 2004, P1)

2.5. Pengertian Least Significant Bit (LSB)

Metode *Least Significant Bit* merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Dalam metode ini penyembunyian data dilakukan dengan mengganti bit-bit data yang ada di dalam segmen citra dengan bit-bit data pesan rahasia.

(Munir Rinaldi, *Steganografi dan Watermarking*, 2004, P5)

2.6. Pengertian Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana cara menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Terdiri dari tiga fungsi dasar yaitu enkripsi, dekripsi dan kunci.

(Kurniawan Yusuf, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, 2004)

2.7. Pengertian Algoritma Vigenere Cipher

Algoritma *vigenere cipher* ini adalah suatu algoritma yang dirancang untuk memperbaiki kelemahan dari algoritma substitusi tunggal, yaitu setiap karakter pada *plainteks* disubstitusikan dengan karakter yang sama.

2.8. Unified Modelling Language (UML)

2.8.1. Use Case Diagram

Use case diagram adalah suatu diagram fungsional yang menggambarkan fungsi dasar dari sebuah sistem yaitu, apa yang dapat dilakukan pengguna dan apa yang harus dilakukan sistem terhadap tindakan pengguna. *Use case* merupakan hal pokok untuk semua diagram dalam *UML*.

(Alan Denis., Barbara Haley W., Roberta M. Roth, 2005 , P171)

2.8.1. Activity Diagram

Activity diagram digunakan untuk menggambarkan perilaku dalam sebuah proses bisnis dari suatu objek.

(Alan Denis., Barbara Haley W., Roberta M. Roth, 2005 , P159)

2.8.2. Sequence Diagram

Sequence diagram adalah salah satu dari dua jenis diagram interaksi (*interaction diagrams*). Diagram ini menggambarkan objek-objek yang berperan dalam sebuah *use case*, dan pengiriman pesan antara objek dari waktu ke waktu untuk satu *use case*.

(Alan Denis., Barbara Haley W., Roberta M. Roth, 2005 , P238)

2.8.3. Class Diagram

Class diagram adalah model statis yang menunjukkan kelas beserta hubungannya dengan kelas-kelas lainnya yang tetap konstan dalam sistem dari waktu ke waktu. *Class diagram* menggambarkan kelas yang mencakup perilaku dan kondisi, serta hubungan antar kelasnya.

(Alan Denis., Barbara Haley W., Roberta M. Roth, 2005 : 216)

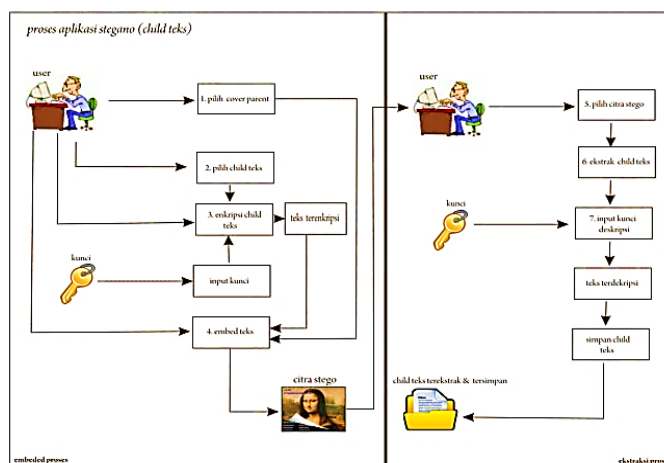
3. ANALISIS DAN PERANCANGAN

3.1. Analisis Sistem

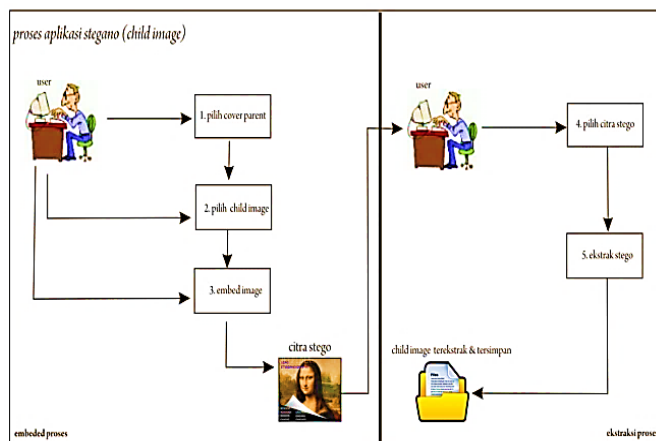
Analisis sistem merupakan suatu tahapan yang bertujuan untuk mengetahui dan mengamati apa saja yang terlibat dalam suatu sistem. Pembahasan yang ada pada analisis sistem ini meliputi analisis kerangka penelitian, analisis alat bantu penelitian, dan analisis tata laksana penelitian.

3.1.1 Analisis Kerangka Penelitian

Penelitian dilakukan dengan beberapa tahapan utama, antara lain tahap pemilihan *cover parent*, tahap pemilihan data child yang akan disembunyikan, proses enkripsi child teks, proses *embed* (penyisipan), tahap pemilihan *citra stego*, proses dekripsi child teks dan proses ekstrak (pengungkapan) *file stego*. Pada skripsi ini proses steganografi dibagi menjadi 2 bagian yaitu proses stego teks dan proses stego image. Tahapan-tahapan proses tersebut dapat dilihat pada gambar 1 (proses stego teks) dan 2 (proses stego image).



Gambar 1. Proses aplikasi stegano teks



Gambar 2. Proses aplikasi stegano teks

aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher-(Diding darisman , Petrus Sokibi, Marsani Asfi)

3.1.2 Analisis Alat Bantu Penelitian

Peralatan yang dibutuhkan untuk melaksanakan penelitian dibagi menjadi dua, yaitu perangkat keras dan perangkat lunak. Kebutuhan perangkat keras pada aplikasi ini dapat dilihat pada table 1 dan Kebutuhan perangkat lunak pada aplikasi dapat dilihat pada table 2.

Tabel 1. Kebutuhan Perangkat Keras

No	Perangkat Keras	Spesifikasi
1	Processor	Intel Core i3
2	Ram	2GB DDR3
3	Hardisk	320GB SATA 7200rpm
4	Layar Monitor	1366x768 (32 bit) (60Hz)
5	VGA Card	Intel HD Graphic 1270Mb

Tabel 2. Kebutuhan Perangkat Lunak

No	Perangkat Lunak	Keterangan
1	Sistem Operasi	Windows 7 32bit
2	Bahasa Pemrograman	Java
3	Perangkat Pendukung	Java Development Kit 7u40
4	Aplikasi Tools	Java Netbeans IDE 1.7.3
5	Picture Viewer	Picasa 3.9
6	Document Viewer	Notepad, Notepad++
7	Picture Editor	Adobe Photoshop CS3, Coreldraw x4

3.1.3 Analisis Tata Laksana Penelitian

Pada Proses ini dilakukan beberapa tahapan penelitian antara lain, tahap pemilihan cover parent, tahap pemilihan data child (child image dan teks), tahap enkripsi child teks, tahap embed (penyisipan data), tahap pemilihan citra stego yang akan di ekstrak, tahap dekripsi child teks, dan tahap ekstrak file stego.

3.2. Perancangan Sistem

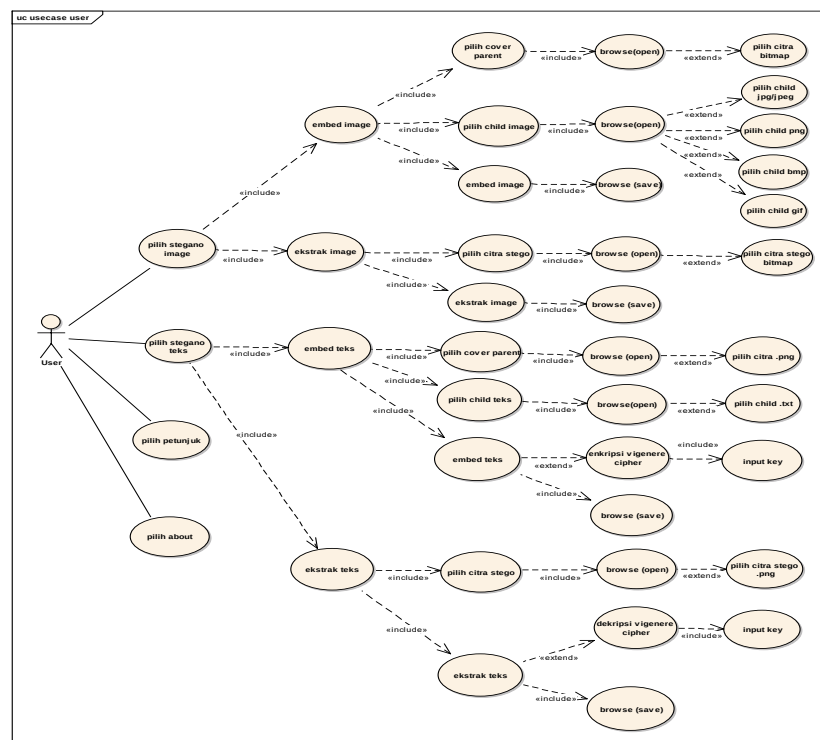
3.2.1. Use Case Diagram

Berikut adalah gambar dari *Use Case Diagram* pada aplikasi steganografi untuk menyembunyikan data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher.

Tabel 3. Diagram Use Case

No	Aktor	Nama Use Case	Dekripsi
1	User	- Pilih <i>embed image</i> - Pilih <i>cover parent</i> - Pilih <i>child file</i> <i>Embed file</i>	- Memilih menu <i>embed stegano image</i> - Memilih <i>citra yang akan dijadikan sebagai media parent</i> - Memilih image <i>child</i> (jpg, jpeg, gif, png dan bmp) - Menyisipkan image kedalam <i>cover parent</i>
2	User	- Pilih ekstrak - Pilih <i>Citra stego</i> - Ekstrak image	- Memilih menu ekstrak <i>stegano image</i> - Memilih <i>citra stego yang akan di ekstrak</i> - Mengekstrak child image yang ada didalam <i>citra stego</i>
3	User	- Pilih <i>embed teks</i> - Pilih <i>citra parent</i>	- Memilih Menu <i>Embed child teks</i> - Memilih citra yang akan dijadikan sebagai cover parent

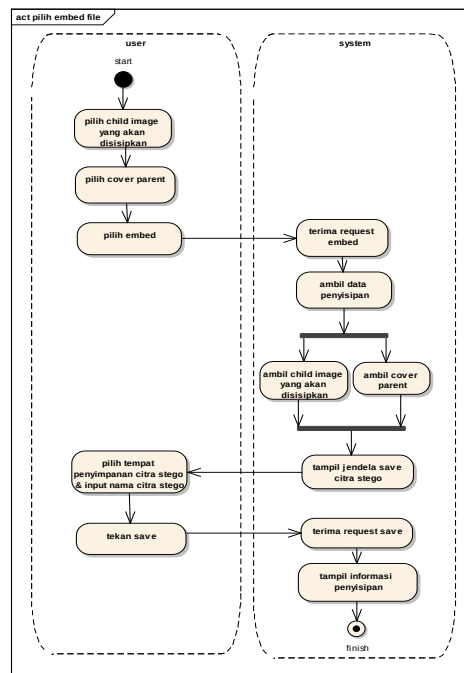
		- Pilih <i>child teks</i> - Enkripsi <i>child teks</i> <i>Embed teks</i>	- Memilih <i>child teks</i>) yang akan disembunyikan - Mengenkripsi isi <i>child teks</i> - Menyisipkan <i>child teks</i> kedalam <i>cover parent</i>
4	User	- Pilih ekstrak teks - Pilih <i>citra stego</i> - Ekstrak teks - Dekripsi <i>child teks</i>	- Memilih Menu Ekstrak stegano teks - Memilih <i>Citra stego</i> - Mengekstrak hidden <i>child</i> yang ada didalam <i>citra stego</i> ke komputer - Mendekripsi isi <i>child teks</i>
5	User	Lihat petunjuk	Melihat petunjuk bagaimana penggunaan aplikasi
6	User	Lihat About	Melihat informasi tentang aplikasi dan pembuat aplikasi



Gambar 3. Use Case Diagram

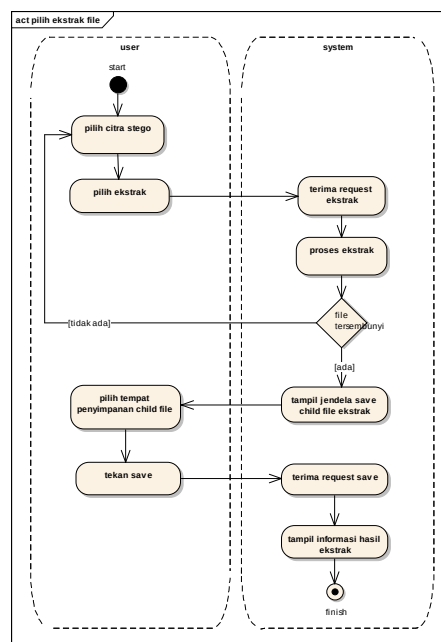
3.2.1. Activity Diagram

3.2.1.1 Activity Diagram Embed Image



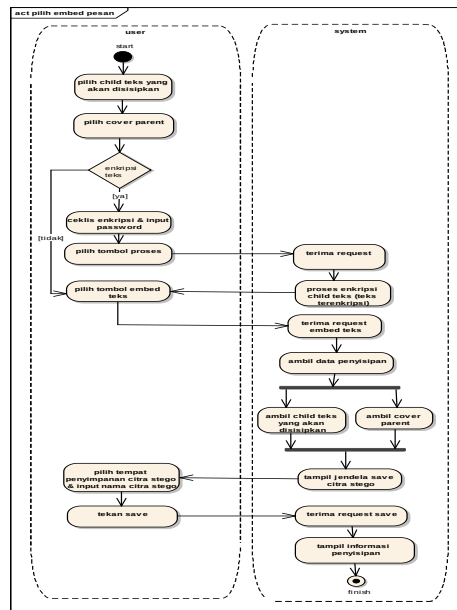
Gambar 4. Activity Diagram Embed Image

3.2.1.2 Activity Diagram Ekstrak Image



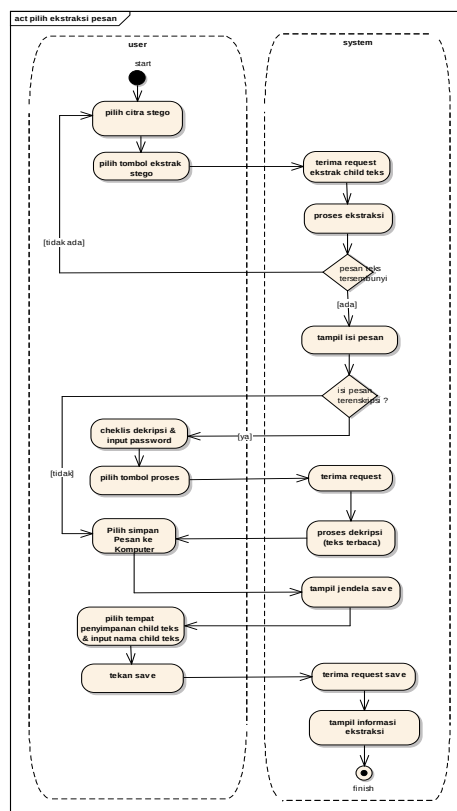
Gambar 5. Activity Diagram Ekstrak Image

3.2.1.3 Activity Diagram Embed Teks



Gambar 6. Activity Diagram Embed Teks

3.2.1.4 Activity Diagram Ekstrak Teks

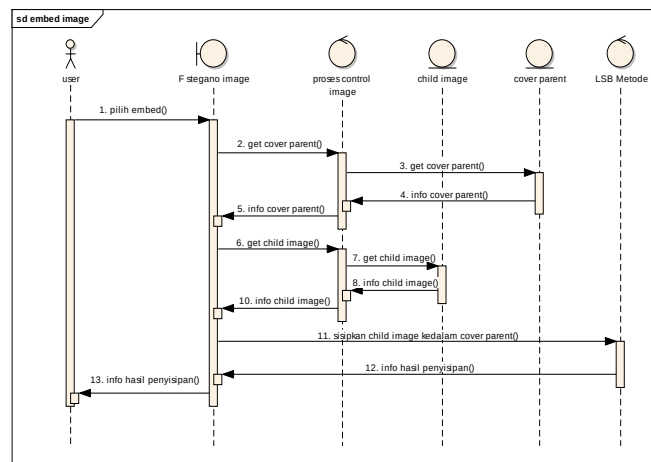


Gambar 7. Activity Diagram Ekstrak Teks

aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher-(Diding darisman , Petrus Sokibi, Marsani Asfi)

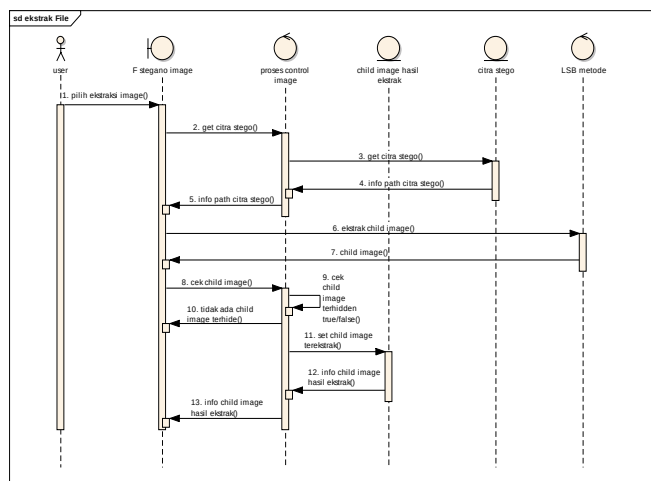
3.3. Sequence Diagram

3.3.1. Sequence Embed Image



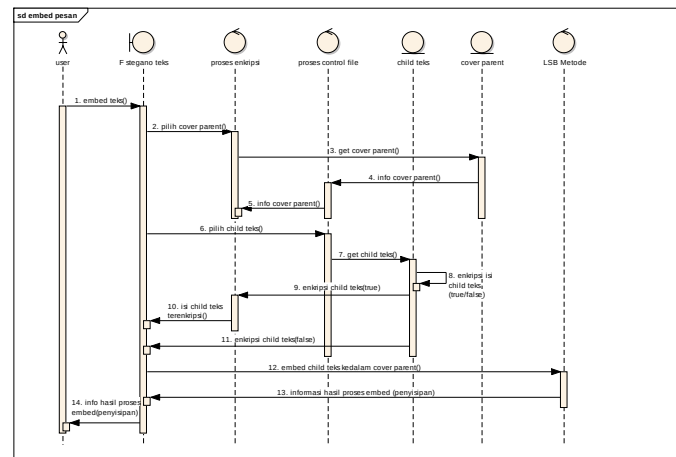
Gambar 8. Sequence Embed Image

3.3.2. Sequence Ekstrak Stego Image



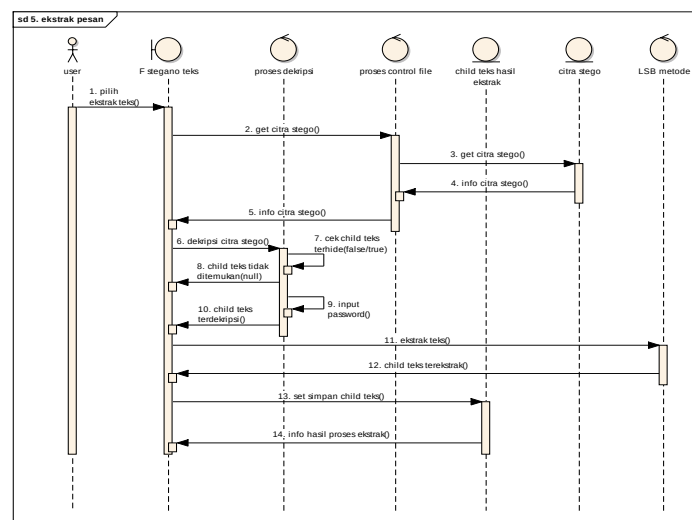
Gambar 9. Sequence Ekstrak Stego Image

3.3.3. Sequence Embed Teks



Gambar 10. Sequence Embed Teks

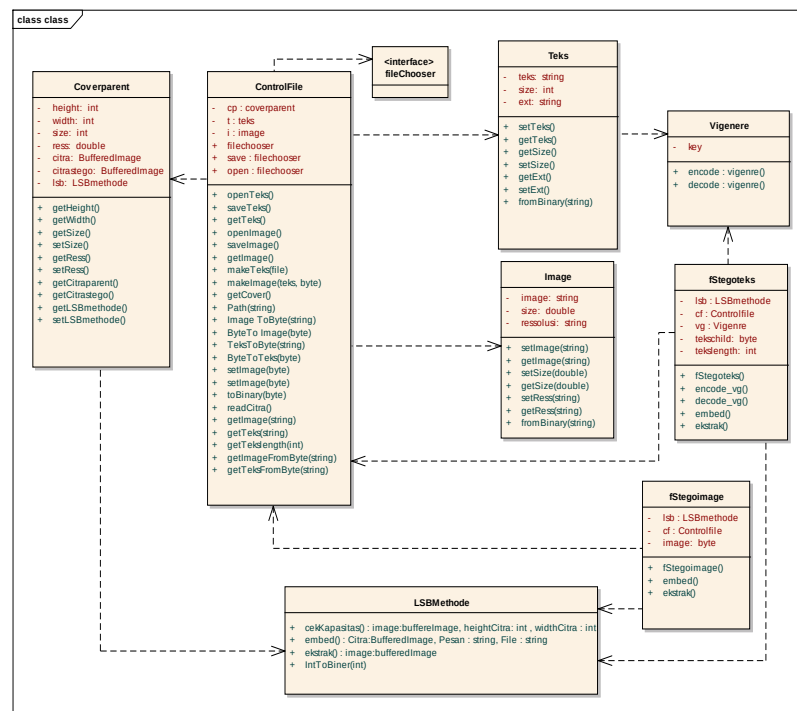
3.3.4 Sequence Ekstrak Stego Teks



Gambar 11. Sequence Ekstrak Stego Teks

3.4. Class Diagram

aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher-(Diding darisman , Petrus Sokibi, Marsani Asfi)



Gambar 12. Class Diagram

4. IMPLEMENTASI DAN PENGUJIAN SISTEM

Implementasi sistem merupakan tahap dimana sistem diimplementasikan dan siap untuk digunakan sesuai dengan perancangan yang telah dibuat .

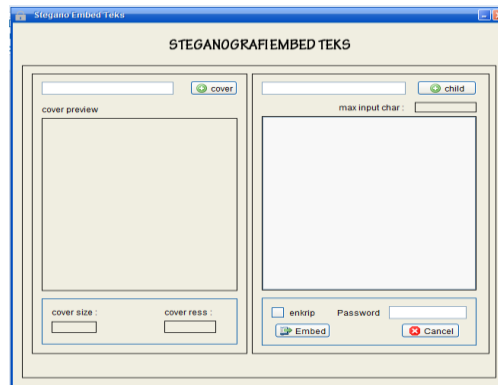
4.1 Implementasi Antarmuka

4.1.1 Form Menu Utama Aplikasi



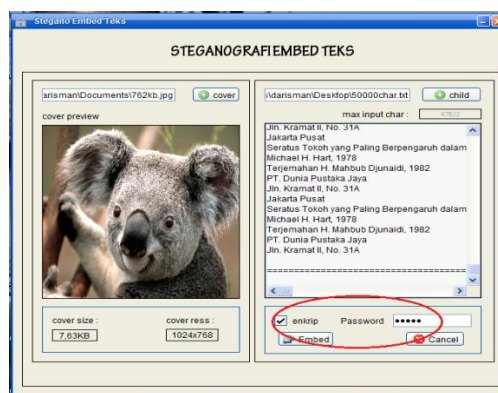
Gambar 13. Form Menu Utama Aplikasi

4.1.2 Form Menu Stego Embed Teks



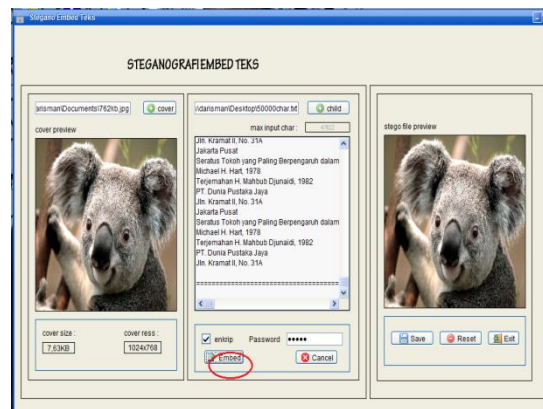
Gambar 14. Form Menu Stego Embed Teks

4.1.3 Form Menu Enkripsi Child Teks



Gambar 15. Form Menu Enkripsi Child Teks

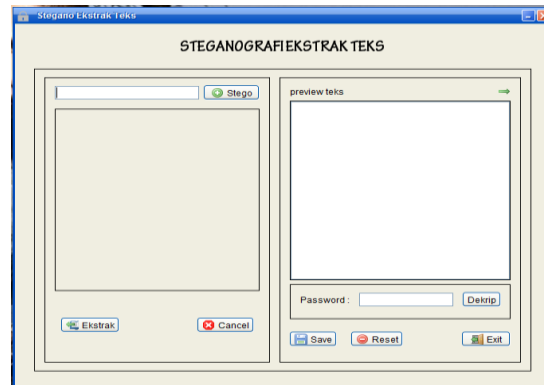
4.1.4 Form Menu Embed Teks



Gambar 16. Form Menu Embed Teks

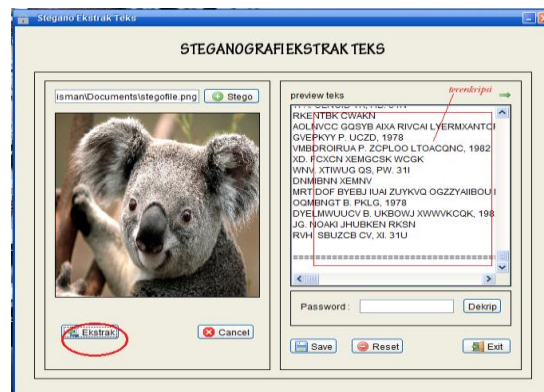
aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher- (Diding darisman, Petrus Sokibi, Marsani Asfi)

4.1.5 Form Menu Stego Ekstrak Teks



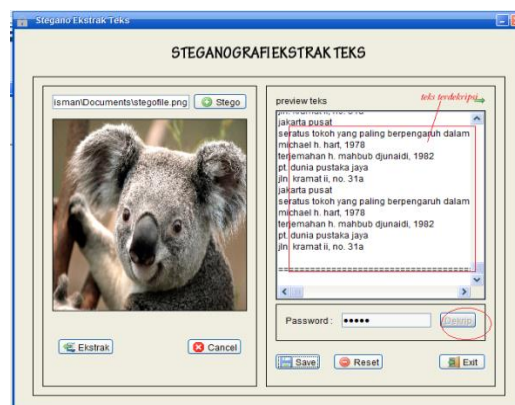
Gambar 17. Form Menu Stego Ekstrak Teks

4.1.6 Form Menu Ekstrak Teks



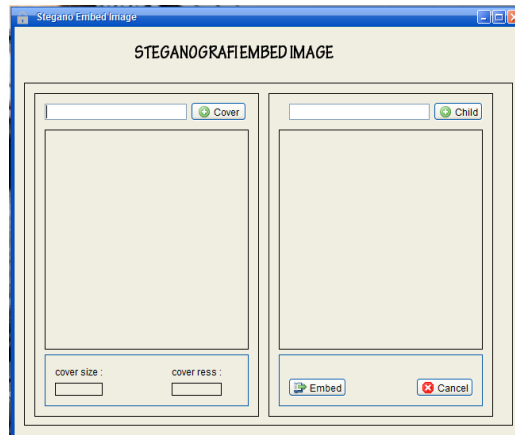
Gambar 18. Form Menu Ekstrak Teks

4.1.7 Form Menu Deskripsi Teks



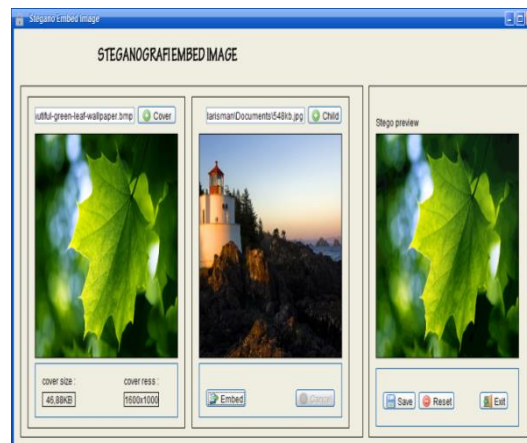
Gambar 19. Form Menu Deskripsi Teks

4.1.8 Form Menu Stego Embed Image



Gambar 20. Form Menu Stego Embed Image

4.1.9 Form Menu Embed Image



Gambar 21. Form Menu Embed Image

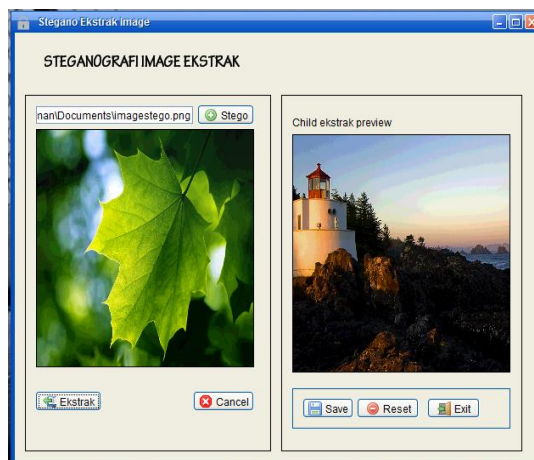
4.1.10 Form Menu Stego Ekstrak Image



Gambar 22. Form Menu Stego Ekstrak Image

aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher-(Diding darisman , Petrus Sokibi, Marsani Asfi)

4.1.11 Form Menu Ekstrak Image



Gambar 23. Form Menu Ekstrak Image

4.2 Pengujian Sistem

Tahap pengujian yang dilakukan pada aplikasi ini antara lain pengujian kapasitas citra parent, pengujian perbandingan ukuran file setelah proses embed atau ekstrak dan pengujian ketahanan citra stego.

4.2.1 Pengujian Kapasitas Citra Parent

Tabel 4. Pengujian Pengujian Kapasitas Citra Cover JPG

No	Nama Citra	Resolusi	Ukuran citra (byte)	Kapasitas (bytes)	Presentase Kapasitas
1	Tulip flower.jpg	320x240	51,915	6,485	12,49%
2	Tulip flower.jpg	400x300	75,342	9,414	12,48%
3	Tulip flower.jpg	640x480	235,987	29,494	12,49%
4	Tulip flower.jpg	800x600	206,788	25,845	12,49%
5	Tulip flower.jpg	1024x768	205,904	25,734	12,49%
6	Tulip flower.jpg	1600x1200	872,263	109,029	12,49%
Presentase Rata-rata					12,48%

Berdasarkan pada tabel diatas citra JPG mempunyai kapasitas yang lebih kecil dari ukuran citra aslinya. Rata-rata persentase kapasitas penyimpanan pesan pada citra JPG yaitu 12,48% dari ukuran citranya. Untuk perhitungan besar dari kapasitas citra parent sendiri dihitung berdasarkan ukuran/size dan kedalamn citra yang digunakan. yakni :

$$n = \frac{Px - Bw}{8}$$

Dimana n adalah jumlah kapasitas bit yang dapat disisipkan, Px adalah pixel atau ukuran citra parent, Bw adalah kedalaman bit warna dari citra parent dan 8 adalah nilai 8bit untuk warna penyusun citra.

4.2.2 Pengujian perbandingan ukuran file setelah proses embed dan ekstrak

A. Perbandingan ukuran file setelah proses embed dan ekstrak pada stegano teks

Tabel 5. Tabel persentasi rata-rata perubahan file

No	Size citra parent (bytes)	Ressolusi citra Parent	Rata2 perubahan size citra stego (png)	Rata2 perubahan size child teks ex-ekstrak (txt)	Rata2 perubahan size cover parent ex-ekstrak
1	51,915	320X240	397%	99%	40%
2	75,342	400X300	422%	99%	40%
3	235,987	640X480	347%	99%	28%
4	206,788	800X600	601%	99%	39%
5	205,904	1024X768	945%	99%	54%
6	872,263	1600X1200	532%	99%	28%
Rata-Rata total			540%	99%	38%

Tabel 5. adalah tabel persentasi rata-rata perubahan file sebelum dan setelah proses embed dan ekstrak. Pada proses penyisipan/embed citra stego yang dihasilkan mengalami peningkatan sebanyak 5x lipat lebih besar dari ukuran citra parent sebelum proses penyisipan. Pada citra cover ex-ekstrak file yang dihasilkan mengalami penurunan hingga 38% lebih kecil dari ukuran citra semula sebelum proses embedding/penyisipan. Dan pada child teks baik jumlah karakter atau pun ukuran dari child teks ex-ekstrak tidak mengalami perubahan.

B. Perbandingan ukuran file setelah proses embed dan ekstrak pada stegano image

Perbandingan Ukuran pada Stegano Image antara Cover Parent, Image Child, Citra Stego, dan Image Child Ex-Ekstrak.

Tabel 6. Perbandingan ukuran pada stegano image

INFO FILE PARENT BITMAP											
ID Parent		Nama File				Ukuran (Bytes)		Resolusi			
PRT-BMP		Bumblebee car				720,054		600x400			
HASIL PROSES											
INFO FILE CHILD				HASIL PROSES EMBED				HASIL PROSES EKSTRAK			
ID	Nama File Child	Size	Ressolusi								
				File Stego vs File Cover				Image Child Ekstrak vs Image Child ex-ekstrak			
				ID	Size stego	Ressolusi	presentase	ID	Size Child Ekstrak	Ressolusi	presentase
CH1-JPG	Flowers beauty	98,518	600x400	PNG	282,239	600x400	39%	PNG	160,311	600x400	162%
CH2-PNG	Switzerland	556,185	600x400	PNG	292,990	600x400	40%	PNG	167,410	600x400	30%
CH3-BMP	Green leaf	720,054	600x400	PNG	202,099	600x400	28%	PNG	92,486	600x400	13%
CH4 - GIF	Homer Simpson	100,147	320x320	PNG	59,864	320x320	14%	PNG	12,754	320x320	13%
Rata-rata presentase file stego							30%	Rata-rata presentase child ex-ekstrak			55%

Pada Tabel 6. menunjukan bahwa perubahan ukuran file stego yang dihasilkan yang paling besar adalah file cover yang di embed dengan image child berformat PNG, terjadi perubahan sekitar 40% lebih kecil dari ukuran semula cover parent, dan ukuran dari file stego yang paling kecil adalah file cover yang diembed dengan image child berformat GIF, terjadi perubahan sebanyak 14% lebih kecil dari ukuran semula cover parent yang digunakan. Dapat dilihat pada table tersebut perubahan rata-rata file stego yang dihasilkan adalah 30%. Sedangkan pada image yang dihasilkan setelah proses ekstraksi format file child JPG menghasilkan ukuran child ex-ekstrak menjadi lebih besar dari ukuran file child sebelum proses

aplikasi steganografi untuk penyembunyian data ke dalam citra digital dengan kombinasi metode least significant bit (lsb) dan algoritma vigenere cipher-(Diding darisman , Petrus Sokibi, Marsani Asfi)

embed yakni sekitar 1,62%, ukuran file child ekstrak dengan image child berformat BMP menghasilkan file child ex-ekstrak menjadi 13 % dari ukuran file child sebelum embed

4.2.3 Pengujian ketahanan citra stego

A. Pengujian Ketahanan File Stego Teks

Hasil pengujian ketahanan pada citra stego teks terhadap manipulasi dapat dilihat pada tabel 7.

Tabel 7. Pengujian Ketahanan Citra Stego Teks

Citra Stego	Rotate left	Rotate right	Rotate 180°	Resize - 10%	Resize +10%	Grayscale	Crop
ST1	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
ST2	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
ST3	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
ST4	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
ST5	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal

B. Pengujian Ketahanan File Stego Image

Hasil pengujian ketahanan pada citra stego image terhadap manipulasi dapat dilihat pada tabel

4.8.

5. Tabel 8. Pengujian Ketahanan Citra Stego Image

Citra Stego	Rotate left	Rotate right	Rotate 180°	Resize - 10%	Resize +10%	Grayscale	Crop
SI1	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
SI2	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
SI3	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
SI4	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal
SI5	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal	Gagal

Pengujian ketahanan terhadap manipulasi yang dilakukan dengan hasil seperti pada tabel 7 dan tabel 8, menunjukkan bahwa citra stego yang dihasilkan tidak tahan terhadap manipulasi.

5. Kesimpulan dan Saran

5.1. Kesimpulan

Berdasarkan hasil pengamatan pada tahap analisa, implementasi dan pengujian dapat disimpulkan bahwa hasil penelitian Skripsi Aplikasi Steganografi Pada Citra Digital Dengan Kombinasi Metode Least Significan Bit (LSB) Dan Algoritma Vigenere Cipher adalah sebagai berikut :

1. Aplikasi Steganografi berhasil diImplementasikan menggunakan Metode *Least Significan Bit* (LSB) dan Algoritma *Vigenere Cipher*.
2. Kapasitas penyimpanan child teks menggunakan metode *least significan bit* (LSB) cukup besar dan bergantung pada ukuran dari cover parent yang digunakan.
3. Perubahan Ukuran pada file stego menjadi lebih besar dari ukuran cover parent sebelum di proses embed dan ekstra, hal ini dikarenakan ukuran dari file yang disisipkan beserta informasinya, semakin banyak ditambah informasi data yang disembunyikan maka akan semakin besar pula ukuran yang dihasilkan.
4. Metode *Least Significan Bit* (LSB) tidak tahan terhadap manipulasi citra.

5.2. Saran

Aplikasi steganografi ini masih mempunyai banyak kekurangan, sehingga perlu dikembangkan lagi agar aplikasi ini dapat lebih sempurna. Untuk meningkatkan kualitas dan fungsionalitas dari aplikasi steganografi ini, maka penulis menyampaikan saran-saran sebagai berikut :

1. Media penampung pesannya (*cover parent*) tidak hanya menggunakan citra digital saja, tetapi juga dapat menggunakan file audio atau video.

2. Jumlah file *child* yang disisipkan kedalam citra tidak hanya satu saja, tetapi dapat disesuaikan jumlahnya oleh pengguna.
3. File *child* yang disembunyikan lebih beragam jenisnya tidak sekedar hanya teks dan gambar saja melainkan audio file, video, doc, pdf, dan file kompresi seperti rar atau zip.
4. Dibutuhkan metode steganografi lain yang lebih tahan terhadap manipulasi citra digital.

Daftar Pustaka

- [1] Kurniawan Yusuf, “*Kriptografi keamanan internet dan jaringan komunikasi*,” Penerbit Informatika Bandung, Bandung, 2004.
- [2] Munir Rinaldi, “*Steganografi dan Watermarking*”, Departemen TI ITB, Bandung, 2004.
- [3] Denis Alan., W Haley Barbara., Roth M Roberto., “*System Analysis Design*” John Wiley & Sons, Inc , United states, 2009.
- [4] Rachmat Antonius, Roswanto Alphone, “*Multimedia*”, Fakultas Teknik Informatika Universitas Kristen duta wacana, 2005.
- [5] Jogiyanto, HM, “*Analisis dan Desain Sistem Informasi : Pendekatan Terstruktur Teori dan Praktik Aplikasi Bisnis*”, Penerbit Andi, Yogyakarta, 2005.
- [6] Maradilla Temmy, 2009, “*Aplikasi Steganografi untuk Penyisipan Data Teks kedalam Citra Digital*”. Universitas Gunadarma.
- [7] Purba Verlando Jhoni, Situmoraang Marihat, Arisandi Dedi, 2012, “*Implementasi Steganografi Pesan Teks ke dalam File Sound (.wav) dengan Modifikasi Jarak Byte pada Algoritma Least Significant Bit (LSB)*”. Universitas Sumatera Utara.
- [8] Widjanarka , Wijaya, “*Teknik Digital*”, Penerbit Erlangga :2006.
- [9] Morkel, T., Eloff, J.H.P., Oliver, M.S., (2005), *An Overview of Image Steganography*, ISSA2005) URL - [Http://mo.co.za/open/stegoverview.pdf](http://mo.co.za/open/stegoverview.pdf).