IMPLEMENTASI TEKNIK *STEGANOGRAPHY* LSB (*LEAST SIGNIFICANT BIT*) SEBAGAI KEAMANAN KOMUNIKASI DATA

Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Mengikuti Ujian Akhir Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains Dan Teknologi Universitas Pembangunan Panca Budi Medan

SKRIPSI

OLEH

NAMA	**: MUHAMMAD RANDY PRATAMA**
N.P.M	**: 1314370417**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

IMPLEMENTASI TEKNIK *STEGANOGRAPHY* LSB (*LEAST SIGNIFICANT BIT*) SEBAGAI KEAMANAN KOMUNIKASI DATA

Disusun Oleh :

NAMA	**: MUHAMMAD RANDY PRATAMA**
N.P.M	**: 1314370417**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi
Pada tanggal 28 Agustus 2019 :

Dosen Pembimbing I	Dosen Pembimbing II
Herdianto, S.Kom., M.T	**Hermansyah, S.Kom., M.Kom**

Mengetahui,

Dekan Fakultas Sains Dan Teknologi	Ketua Program Studi Sistem Komputer
Sri Shadi Indra, S.T., M.Sc	**Dr. Muhammad Iqbal S.Kom., M.Kom**

Plagiarism Detector v. 1092 - Originality Report:

Analyzed document: 21-01-19 10:19:58 AM

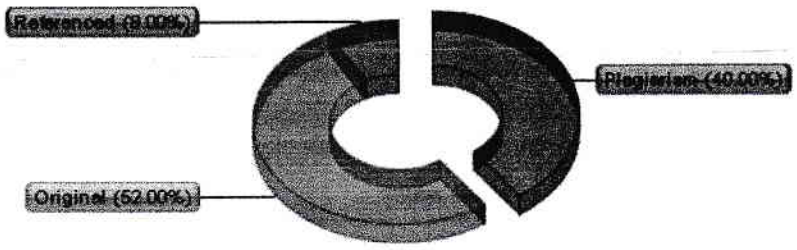
"MUHAMMAD RANDY PRATAMA_1314370417_SISTEM KOMPUTER.doc"

Licensed to: **Universitas Pembangunan Panca Budi_License2**

UNIVERSITAS PEMBANGUNAN PANCA BUDI
Beriman. Berilmu. Berkarya

LEMBAGA PENJAMIN MUTU UNIVERSITAS
UNPA-B
UNIVERSITAS PEMBANGUNAN PANCA BUDI

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 12	wrds: 1030	http://riotugasmetolit.blogspot.com/
% 11	wrds: 894	http://aab-boleh.blogspot.com/2014/09/kriptografi-itu-part-4-perbedaanya.html
% 11	wrds: 894	http://aab-boleh.blogspot.com/2014/09/

[Show other Sources:]

Processed resources details:

182 - Ok / 33 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama	:	MUHAMMAD RANDY PRATAMA
N.P.M.	:	1314370417
Tingkat/Semester	:	Akhir
Fakultas	:	SAINS & TEKNOLOGI
Jurusan/Prodi	:	Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 21 Juni 2019
Ka. Laboratorium

YAYASAN PROF. DR. H. KADIRUN YAHYA
MEDAN
Fachrid Wadly, S.Kom
INDONESIA

Telah Diperiksa oleh LPMU
dengan Plagiarisme...40...%
Medan 21 JUNI 2019
AN Ka. LPMU
UNPAB
HUSNI M. BITONGA, BA., MSc.
Calvo Premono, SE, MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 21 Juni 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan 21 JUN 2019
a.n. Ka. BPAA
TEGUH WAHYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	**: MUHAMMAD RANDY PRATAMA**
Tempat/Tgl. Lahir	**: STABAT / 18 MEI 1995**
Nama Orang Tua	**: Drs. Idran**
N. P. M	**: 1314370417**
Fakultas	**: SAINS & TEKNOLOGI**
Program Studi	**: Sistem Komputer**
No. HP	**: 082274456357**
Alamat	**: Lk IX Kel. Kuala Bingai Kec. Stabat. Kab. Langkat**

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **IMPLEMENTASI TEKNIK STEGANOGRAPHY LSB (Least Significant Bit) SEBAGAI KEAMANAN KOMUNIKASI DATA**, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	200.000 21/06/19
2.	[170] Administrasi Wisuda	: Rp.	1,500,000
3.	[202] Bebas Pustaka	: Rp.	100,000
4.	[221] Bebas LAB	: Rp.	5,000
Total Biaya		: Rp.	1,805,000
UK. T. 55%		Rp.	2.500.000
		Rp.	4.305.000

Ukuran Toga : XL

Mengetahui/Disetujui oleh :
Hormat saya

Shindi Indira, S.T.,M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

MUHAMMAD RANDY PRATAMA
1314370417

Catatan :

- 1.Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2.Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

TANDA BEBAS PUSTAKA
No. 2394/Perp/BP/2019
Dinyatakan tidak ada sangkut paut dengan UPT. Perpustakaan
Medan, 21 JUN 2019
Kepala UPT. Perpustakaan
UNPAB INDONESIA
UPT. PERPUSTAKAAN

Cetak Formulir Pengajuan Judul

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI TEKNIK ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROEKOTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

ng bertanda tangan di bawah ini :

engkap	: MUHAMMAD RANDY PRATAMA
Tgl. Lahir	: / 18 Mei 1995
Pokok Mahasiswa	: 1314370417
Studi	: Sistem Komputer
rasi	: Keamanan Jaringan Komputer
redit yang telah dicapai	: 141 SKS, IPK 2.91

mengajukan judul skripsi sesuai dengan bidang ilmu, dengan judul:

Judul Skripsi	Persetujuan
NCANG BANGUN APLIKASI PORTABLE PENYANDIAN PESAN PADA DOKUMEN DI KANTOR SEKOLAH SDIT ZAHRA KECAMATAN STABAT KABUPATEN LANGKAT MENGGUNAKAN VISUAL STUDIO 2010	☐
NCANGAN APLIKASI BINDING FILE SEBAGAI TEKNIK KOMUNIKASI AMAN DI BIDANG FORENSIK NGGUNAKAN VISUAL STUDIO 2010	☐
PLEMENTASI TEKNIK STEGANOGRAPHY SEBAGAI MEDIA PEMBELAJARAN KEAMANAN KOMUNIKASI DATA	☑

ng disetujui oleh Kepala Program Studi diberikan tanda ☑

Medan, 09 Februari 2018

Rektor,

(Ir. Bhakti Alamsyah, M.T., Ph.D.)

Pemohon,

(MUHAMMAD RANDY PRATAMA)

Nomor : .....
Tanggal : .....
Disahkan oleh
Dekan,

(Sri Shindi Indira, S.T.,M.Sc.)

Tanggal : 28-03-2018
Disetujui oleh :
Dosen Pembimbing I :

(Hery Sunato, S.Kom, MT)

Tanggal : 28 Maret 2018
Disetujui oleh:
Ka. Prodi Sistem Komputer

(MUHAMMAD IQBAL, S.Kom.,M.Kom.)

Tanggal : 23-03-2018
Disetujui oleh:
Dosen Pembimbing II:

(Ir. Nawawi Yah, S.Kom, M.Kom)

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : HERDIANTO, S.Kom, M.Kom
Dosen Pembimbing II : .....
Nama Mahasiswa : MUHAMMAD RANDY PRATAMA
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1314370417
Jenjang Pendidikan : S1
Judul Tugas Akhir/Skripsi : IMPLEMENTASI TEKNIK STEGANOGRAFI LSB (Least significant Bit) SEBAGAI KEAMANAN KOMUNIKASI DATA

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
9/10-2018	Penyerahan bab 1 - perbaikan latar belakang, rumusan masalah, tujuan penelitian		
23/10-2018	perbaikan rumusan masalah dan tujuan penelitian		
13/11-2018	penyerahan bab 2. tambahkan penjelasan mengenai metode LSB, Steganografi		
20/11-2018	tambahkan gambar pada bab 2 lebih rinci dan sebab penjelasan.		
27/12-2018	penyerahan bab 3 - Tambahkan contoh UML interface dan penjelasan proses Algoritma LSB dalam menyembunyikan pesan dalam gambar		
8/1-2019			
22/1-2018	penyerahan bab 4. tambahkan kutipan pembahasan		
28/1-2018	acc semua bab		
29/5-2018	acc bab		
29/8-2019	acc sidang		

Medan, 28 Mei 2018
Diketahui/Disetujui oleh :
Dekan,

UNIVERSITAS PEMBANGUNAN PANCA BUDI ★ UNPAB INDONESIA ★ FAKULTAS SAINS & TEKNOLOGI

Sri Shindi Indira, S.T.,M.Sc.

*) Coret yang tidak perlu

FM-BPAA-2012-038

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : .....
Dosen Pembimbing II : HERMANSYAH, S.Kom., M.Kom
Nama Mahasiswa : MUHAMMAD RANDY PRATAMA
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1314370417
Jenjang Pendidikan : S1
Judul Tugas Akhir/Skripsi : IMPLEMENTASI TEKNIK STEGANOGRAFI ~~SEBAGAI~~ LSB (Least Significant Bit) SEBAGAI KEAMANAN KOMUNIKASI DATA

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
29/5-18	Revisi Bab. I & Judul.		
20/7-18	Revisi Judul. Lnjt Bab II		
6/10-18	Tambah Referensi kutipan 2013		
1/11-18	Lnjt Bab III.		
14/11-18	Revisi Progam		
29/11-18	Revisi perbaiki. Lnjt Bab IV		
12/12-18	Lengkapi semua & Lnjt Bab V		
16/1-19	- Acc Sem		
25/5-4	- Acc Sid		
30/8-19	- Acc Jilid		

Medan, 28 Mei 2018
Diketahui/Disetujui oleh :
Dekan,

UNIVERSITAS PEMBANGUNAN PANCA BUDI
UNPAB INDONESIA
FAKULTAS SAINS & TEKNOLOGI

Sri Shindi Indira, S.T.,M.Sc.

...yang tidak perlu

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama	: Muhammad Randy Pratama
NPM	: 1314370417
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer (KJK)
Judul Skripsi	: Implementasi Teknik *Steganography* LSB (*Least Significant Bit*) Sebagai Keamanan Komunikasi Data.

Dengan ini menyatakan bahwa :

1. Tugas Akhir / Skripsi saya bukan hasil Plagiat.
2. Saya tidak akan menuntut perbaikan nilai Indeks Prestasi Kumulatif (IPK) setelah ujian Sidang Meja Hijau.
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut.

Demikian pernyataan ini saya perbuat dengan sebenar - benarnya, terima kasih.

Medan, 28 Agustus 2019

METERAI TEMPEL
DB6AHF080570106
6000 RIBU RUPIAH

Muhammad Randy Pratama
1314370417

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang diajukan untuk memperoleh kesarjanaan disuatu perguruan tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali yang secara tertulis diacu dalam skripsi ini dan disebutkan dalam daftar pustaka.

Medan, 28 Agustus 2019

Muhammad Randy Pratama

ABSTRAK

MUHAMMAD RANDY PRATAMA
Implementasi Teknik *Steganography* LSB *(Least Significant Bit)* Sebagai Keamanan Komunikasi Data
2019

Penelitian ini dilakukan atas dasar perlunya keamanan data pada media digital berupa metode pengolahan data yang dapat membangtu mengamankan data yang bersifat rahasia, sehingga data rahasia hanya dapat dibaca oleh orang yang diinginkan dan mengantisipasi agar data tidak terbaca oleh orang yang tidak berhak. Pada penelitian ini dibangun suatu sistem yang dapat digunakan dalam meningkatkan keamanan data-data penting. Adapun algoritma yang digunakan dalam mengubah data menjadi data biner ketika proses *embedding* adalah dengan modifikasi metode LSB (*Least Significant Bit*) untuk meningkatkan keamanan data. Penelitian ini bertujuan untuk dapat menyembunyikan text atau gambar menggunakan metode LSB (*Least Siginificant Bit*) dalam media cover gambar Bitmap dan untuk mengetahui pengaruh metode LSB (*Least Siginificant Bit*) terhadap *file* gambar dan besar ukuran *file* dalam penyembunyian *text* dan gambar. Metode yang digunakan pada penelitian ini adalah eksplorasi dan eksperimen (ujji coba). Dari hasil uji coba didapat bahwa perbedaan antara gambar asli dan gambar stego sangat sulit di bedakan, akibatnya dapat mengeploitasi pikiran manusia pada umumnya. Selain itu, ukuran *stage image* dari *steganography* metode LSB rata-rata mengalami pertambahan ukuran file namun tidak signifikan. Namun hasil keluaran dari *stage image* sendiri akan bertambah buruk dengan bertambahnya ukuran file yang disisipkan.

Kata Kunci *:* *Cover Image* Bitmap, Keamanan Data, LSB, *Steganography*, *Stego Image*.

DAFTAR ISI

BAB III METODE PENELITIAN

BAB IV HASIL DAN PEMBAHASAN

BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi mempermudah orang berkomunikasi, bentuk komunikasi yang sering digunakan adalah mengirim dan menerima pesan. Pertukaran pesan maupun data tidak hanya dilakukan antar teman (secara pribadi atau informal), tetapi juga antara rekan bisnis, atasan dengan bawahan, maupun sebaliknya (legal dan formal). Data atau pesan yang dikirim melalui internet dapat diretas (disadap) selama dalam proses pengiriman (Amal, *dkk*, 2015). Untuk mengatasi permasalahan penyadapan data yang dikirim melalui internet salah satu teknik yang dapat digunakan adalah *Steganografi*.

Penelitian yang menggunakan teknik *Steganografi* LSB (*Least Significant Bit*) telah dilakukan oleh peneliti sebelumnya. Sitorus, M.(2015) pada penelitian ini teknik steganografi hanya mampu menyembunyikan *file* jenis *text* ke dalam media gambar dengan format PNG. Pada pengujian menggunakan file PNG, aspek *impercebtibility* (keamanan) dan *recovery* (pengembalian) dapat terpenuhi dengan baik karena kualitas gambar dari file PNG yang telah disisipkan pesan memiliki kualitas yang baik. Sedangkan untuk aspek *fidelity* (mutu) tidak terpenuhi karena pada hasil uji coba, terjadi pembengkakan *size* pada gambar yang berisi pesan (Sari, *dkk*, 2012).

Oleh karena itu dibutuhkan evaluasi aplikasi yang dapat menyembunyikan jenis *file* digital seperti *text* dan gambar ke dalam sebuah media gambar. Pada penelitian ini akan menggunakan format file yang lain yaitu bitmap (BMP).

Nantinya sistem ini akan dituangkan dalam bentuk skripsi dengan judul **"IMPLEMENTASI TEKNIK *STEGANOGRAPHY* LSB *(Least Significant Bit)* SEBAGAI KEAMANAN KOMUNIKASI DATA".**

1.2. Rumusan Masalah

Berdasarkan pada latar belakang masalah yang telah diuraikan, maka masalah yang muncul dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana menggunakan metode LSB dapat menyembunyikan pesan dalam *file* gambar?
2. Bagaimana pengaruh metode LSB terhadap *file* gambar dan besar ukuran *file* dalam penyembunyian *text* dan gambar?

1.3. Batasan Masalah

Untuk membatasi luasnya penelitian maka penulis perlu membatasi pada hal-hal sebagai berikut :

1. Program aplikasi yang digunakan adalah Visual Studio.
2. *File* gambar yang akan digunakan sebagai *cover* adalah jenis .Bmp.
3. Ukuran *file* gambar yang akan digunakan sebagai *cover* sebesar 300kb.
4. Ukuran *file* yang akan disisipkan tidak lebih dari *file cover*.
5. *File* yang akan disisipkan adalah jenis *text* dan gambar jenis .Jpg.

1.4. Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Dapat menyembunyikan text atau gambar menggunakan metode LSB (*Least Siginificant Bit*) dalam media cover gambar .Bmp.
2. Untuk mengetahui pengaruh metode LSB (*Least Siginificant Bit*) terhadap *file* gambar dan besar ukuran *file* dalam penyembunyian *text* dan gambar.

1.5. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penulisan penelitian ini adalah sebagai berikut :

1. Manfaat bagi Penulis.

Sebagai sarana belajar untuk mengintegrasikan pengetahuan dalam memahami dan mengetahui pentingnya keamanan data.

2. Manfaat bagi Lembaga atau Intitusi Pendidikan

Manfaat bagi lembaga atau intitusi pendidikan adalah sebagai bahan referensi dan pengembangan materi yang masih berhubungan bagi peneliti berikutnya untuk dikembangkan lebih lanjut dikemudian hari.

3. Manfaat bagi peneliti yang lain

Sebagai bahan perbandingan yang membahas dan meneliti permasalahan yang sama.

BAB II

LANDASAN TEORI

2.1. Data

2.1.1. Pengertian Data

Dikutip dari jurnal Hermansyah dan Nurhayati yang berjudul “Sistem informasi jumlah angkatan kerja menggunakan visual basic pada badan pusat statistik (bps) kabupaten langkat“ menyatakan bahwa data adalah sekumpulan baris fakta yang mewakili peristiwa yang terjadi pada organisasi atau pada lingkungan fisik sebelum diolah kedalam format yang bisa dimengerti dan digunakan orang. Data dapat berupa catatan-catatan kertas, buku atau sebagai file yang tersimpan dalam basis data.

2.2. Steganografi

2.2.1. Pengertian Steganografi

Steganografi merupakan seni komunikasi rahasia dengan menyembunyikan pesan pada objek yang tampaknya tidak berbahaya. Keberadaan pesan steganografi adalah rahasia. Istilah Yunani ini berasal dari kata Steganos, yang berarti tertutup dan Graphia, yang berarti menulis (Muhammad Syawal Fitra. 2016).

Steganografi adalah jenis komunikasi yang tersembunyi, yang secara harfiah berarti "tulisan tertutup." Pesannya terbuka, selalu terlihat, tetapi tidak terdeteksi bahwa adanya pesan rahasia. Deskripsi lain yang popular untuk steganografi adalah *Hidden in Plain Sight* yang artinya tersembunyi di depan

mata. Sebaliknya, kriptografi adalah tempat pesan acak, tak dapat dibaca dan keberadaan pesan sering dikenal.

Dikutip langsung dari jurnal Muhammad Fitra Syawal yang berjudul "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB", istilah steganografi berasal dari bahasa Yunani, yaitu "steganos yang berarti penyamaran atau penyembunyian dan graphein yang berarti tulisan. Jadi, steganografi bisa diartikan sebagai "seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama".

Sedangkan menurut H. B. Kekre, (2011). Steganografi merupakan seni dan ilmu berkomunikasi dengan cara menyembunyikan keberadaan komunikasi itu. Berbeda dengan Kriptografi, di mana musuh diperbolehkan untuk mendeteksi, menangkal dan memodifikasi pesan tanpa bisa melanggar keamanan tempat tertentu yang dijamin oleh suatu *cryptosystem*, tujuan dari steganografi adalah untuk menyembunyikan pesan dalam pesan berbahaya lainnya dengan cara yang tidak memungkinkan musuh apapun bahkan untuk mendeteksi bahwa ada pesan kedua. Secara umum, teknik steganografi yang baik harus memiliki visual / *imperceptibility* statistik yang baik dan *payload* yang cukup.

2.2.2. Sejarah Steganografi

Teknik steganografi ini sudah ada sejak 4000 tahun yang lalu di kota Menet Khufu, Mesir. Awalnya adalah penggunaan hieroglyphic yakni menulis menggunakan karakter-karakter dalam bentuk gambar. Ahli tulis menggunakan tulisan Mesir kuno ini untuk menceritakan kehidupan majikannya. Tulisan Mesir kuno tersebut menjadi ide untuk membuat pesan rahasia saat ini. Oleh karena itulah, tulisan Mesir kuno yang menggunakan gambar dianggap sebagai steganografi pertama di dunia (Muhammad Syawal Fitra. 2016).

Tidak hanya bangsa Mesir saja, bangsa-bangsa lain juga telah mengggunakan teknik steganografi pada masa lalu, yaitu :

1. Teknik steganografi yang lain adalah tinta yang tidak tampak (*invisible ink*) yaitu dengan menggunakan air sari buah jeruk, urin atau susu sebagai tinta untuk menulis pesan. Cara membacanya adalah dengan dipanaskan di atas api. Tinta yang sebelumnya tidak terlihat, ketika terkena panas akan menjadi gelap sehingga dapat dibaca. Teknik ini digunakan oleh bangsa Romawi yang juga digunakan pada Perang Dunia II.
2. Bangsa Cina menggunakan cara yang berbeda pula, yaitu manusia sebagai media pembawa pesan. Orang itu akan dicukur rambutnya sampai botak dan pesan akan dituliskan di kepalanya. Kemudian pesan akan dikirimkan ketika rambutnya sudah tumbuh.

3. Pada masyarakat Yunani kuno teknik yang digunakan adalah dengan menggunakan lilin sebagai media pembawa pesan. Lembaran pesan akan ditutup dengan lilin. Untuk melihat isi pesan, pihak penerima harus memanaskan lilin terlebih dahulu.

Pada Perang Dunia II, bangsa Jerman menggunakan microdots untuk berkomunikasi. Penggunaan teknik ini digunakan pada microfilm chip yang harus diperbesar sekitar 200 kali. Jerman menggunakan teknik ini untuk kebutuhan perang sehingga pesan rahasia strategi tidak diketahui pihak lawan. Karena pada saat itu teknik ini merupakan teknologi baru yang belum bisa digunakan lawan.

2.2.3. Teknik Steganografi

Menurut Ariyus (2012), ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu :

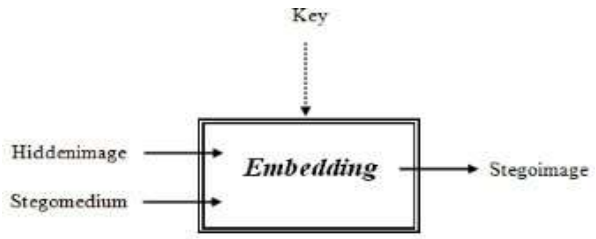
1. *Injection*, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut *embedding*.
2. *Substitusi*, data normal digantikan dengan data rahasia. Biasanya,hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada *file* media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.

3. *Transform Domain,* teknik ini sangat effektif. Pada dasarnya,transformasi domain menyembunyikan data pada *transform space*. Akan sangat lebih efektif teknik ini diterapkan pada *file* berekstensi JPG.
4. *Spread Spectrum*, sebuah teknik pengtransmisian menggunakan *pseudo-noise* code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.
5. *Statistical Method*, teknik ini disebut juga skema *steganographic* 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. *Distortion*, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
7. *Cover Generation*, metode ini lebih unik daripada metode lainnya karena *cover object* dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah *Spam Mimic.*

2.2.4. Proses Steganografi

Secara umum, terdapat dua proses didalam steganografi. Yaitu proses *embedding* untuk menyembunyikan pesan dan ekstraksi untuk mengekstraksi pesan yang disembunyikan.

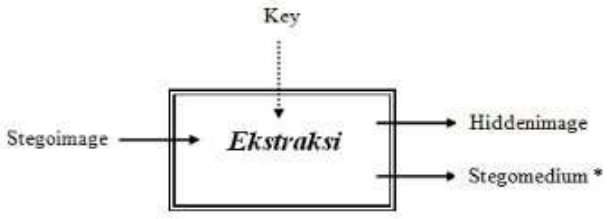
Gambar 2, menunjukkan proses penyembunyian pesan dimana di bagian pertama, dilakukan proses *embedding hidden image* yang hendak disembunyikan secara rahasia ke dalam *stegomedium* sebagai media penyimpanan, dengan memasukkan *file* lain kedalam wadah, sehingga dihasilkan media dengan data tersembunyi di dalamnya (*stegoimage*).



(Sumber : Raziq Ahmad, 2015)

Gambar 2.1. *Embedding Citra*

Pada Gambar 2, dilakukkan proses ekstraksi pada *stegoimage* dengan memilih lokasi penyimpanan yang ada sehingga didapatkan kembali *hiddenimage*.



(Sumber : Raziq Ahmad, 2015)

Gambar 2.2. Ekstraksi Citra

2.3. Citra Digital

Semua citra digital yang ditampilkan di layar komputer adalah sederetan atau sekumpulan pixel (*picture element*). Citra tersebut dikatakan sebagai citra digital karena bentuk representasinya yang berupa bilangan. Oleh komputer akan dikenal dalam urutan ‘0’ dan ‘1’ (Syaiful Anwar, 2017).

Format file citra standar yang digunakan saat ini terdiri dari beberapa jenis. Format-format ini digunakan dalam menyimpan citra dalam sebuah file. Setiap format memiliki karakteristik masing-masing. Berikut adalah penjelasan beberapa format umum yang sering digunakan (Murni, 1992).

1. ***Tagged Image Format File* (.TIF, .TIFF)**

Format TIF merupakan format gambar terbaik dengan pengertian bahwa semua data dan informasi (data RGB, data CMYK, dan lainnya) yang berkaitan dengan koreksi atau manipulasi terhadap gambar tersebut tidak hilang. Format TIFF biasa digunakan untuk kebutuhan pencetakan dengan kualitas gambar yang sangat tinggi. Ukuran berkas untuk format ini biasanya sangat besar. Format file ini mampu menyimpan gambar dengan kualitas hingga 32 bit.

2. ***Joint Picture Expert Group* (.JPEG)**

Format JPEG adalah format yang sangat umum digunakan saat ini khususnya untuk transmisi citra.. Format JPEG memiliki ukuran yang lebih kecil dibandingkan dengan gambar berformat BMP. Gambar dengan format JPEG hanya mampu menghasilkan 16 bit kedalaman warna.

3. Graphics Interchange Format (.GIF)

Format gambar GIF merupakan gambar yang sudah mengalami kompresi tipe *lossy*. Kompresi tipe *lossy* adalah kompresi dimana terdapat data yang hilang selama proses kompresi. Akibatnya kualitas data yang dihasilkan jauh lebih rendah daripada kualitas data asli. Kualitas yang rendah menyebabkan format ini tidak terlalu populer dikalangan peneliti pengolahan citra digital. Gambar dengan format GIF hanya mampu menghasilkan 8 bit kedalaman warna, sehingga hanya digunakan untuk gambar-gambar kecil yang tidak memiliki banyak warna.

4. PNG

Portable Network Graphics biasa dibaca ‘ping’. Asal mulanya dikembangkan sebagai pengganti format GIF karena adanya penerapan lisensi GIF. Format ini mendukung pemampatan data tanpa menghilangkan informasi aslinya. Format ini cocok di gunakan dalam internet karena mendukung transparasi di dalam perambah (*browser*). Untuk keperluan pengolahan gambar meskipun format PNG bisa di jadikan alternatif selama proses pengolahan grafis namun format .jpg masih menjadi pilihan terbaik. Di samping itu format ini juga memiliki ukuran yang besar.

5. Bitmap (.BMP)

Bitmap adalah format gambar asli yang tidak mengalami proses kompresi. Ukuran citra dengan format ini sangat besar dan mampu menghasilkan 24 bit kedalaman warna. Karena gambar berformat BMP belum mengalami proses kompresi maka program aplikasi pengolahan citra yang dirancang ini menggunakan citra input berformat BMP.

Bitmap (BMP) adalah format gambar yang paling umum dan merupakan format standar windows. Kelebihan dari tipe *file* ini adalah dapat dibuka hampir di semua program pengolah gambar, selain itu gambar yang disimpan dengan tipe data BMP tidak akan mengalami penurunan kualitas, citra dalam format BMP umumnya tidak dimampatkan sehingga tidak ada informasi yang hilang. *File* ini merupakan format yang belum terkompresi dan menggunakan sistem warna RGB (*Red, Green, Blue*) yang masing-masing warna *pixel*nya terdiri dari 3 komponen yang dicampur menjadi satu (Murni, 1992).

Bitmap adalah representasi dari citra grafis yang terdiri dari susunan titik yang tersimpan di memori komputer. Dikembangkan oleh *Microsoft* dan nilai setiap titik diawali oleh satu bit data untuk gambar hitam putih, atau lebih bagi gambar berwarna. Kerapatan titik-titik tersebut dinamakan resolusi, yang menunjukkan seberapa tajam gambar ini ditampilkan, ditunjukkan dengan jumlah baris dan kolom. Citra dalam format BMP ada tiga macam, yakni citra biner, citra berwarna, dan citra hitam-putih (*grayscale*). Citra biner hanya mempunyai dua nilai keabuan, 0 dan 1. Oleh karena itu, 1 bit sudah cukup untuk merepresentasikan nilai piksel. Citra berwarna adalah citra yang lebih umum.

Warna yang terlihat pada citra bitmap merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau dan biru. Setiap piksel disusun oleh tiga komponen warna, yaitu R (*red*), G (*green*), dan B (*blue*). Kombinasi dari tiga warna RGB tersebut menghasilkan warna yang khas untuk *pixel* yang bersangkutan (Usman,2005).

2.4. Metode LSB (*Least Significant Bit*)

Metode LSB (*Least Significant Bit)* adalah salah satu metode steganografi yang paling sederhana dengan teknik penyembunyian pesan pada lokasi bit terakhir pada citra digital. LSB mempunyai kelebihan yakni ukuran gambar tidak akan berubah. Sedangkan kekuranganya adalah pesan/atau data yang akan disisipkan terbatas, sesuai dengan ukuran citra (Teguh Budi Harjo, 2016).

Sebagai contoh, urutan bit berikut ini menggambarkan 3 piksel pada cover image 24-bit.Jika digunakan *image* 24 bit color sebagai cover, sebuah bit dari masing-masing komponen (RGB) *Red, Green,* dan *Blue*, yang masing masing disusun oleh bilangan 8 bit dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap *pixel (picture element)* berkas *bitmap* 24 bit kita dapat menyisipkan 3 bit data disimpan pada setiap *pixel*.

Perubahan pada LSB ini akan terlalu kecil untuk terdeteksi oleh mata manusia sehingga pesan dapat disembunyikan secara efektif. Sebuah *image* 800 x 600 *pixel* dapat digunakan untuk menyembunyikan 1.440.000 bit (180.000 bytes) data rahasia.

Misalnya di bawah ini terdapat 3 *pixel* dari *image* 24 *bit color* :

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

Jika diinginkan untuk menyembunyikan sebuah karakter A (01000001) dihasilkan:

(00100110 11101001 11001000)

(00100110 11001000 11101000)

(11001000 00100111 11101001)

Dapat dilihat bahwa hanya hanya 3 *pixel* saja yang perlu diubah untuk menyembunyikan karakter A ini. Perubahan yang sangat kecil untuk terdeteksi membuat penyembunyian pesan lebih efektif. Jika digunakan *image* 8 bit color sebagai cover, hanya 1 bit saja dari setiap *pixel* warna yang dapat dimodifikasi sehingga pemilihan *image* harus dilakukan dengan sangat hati-hati, karena perubahan LSB dapat menyebabkan terjadinya perubahan warna yang ditampilkan pada citra, dan akan lebih baik jika *image* berupa *image grayscale* karena perubahan warnanya akan lebih sulit dideteksi oleh mata manusia. Proses ektraksi pesan dapat dengan mudah dilakukan dengan mengektraks LSB dari masing masing *pixel* pada *steganography* secara berurutan dan menuliskan ke *output file* yang akan berisi pesan tersebut.

2.5. Keamanan Data

Keamanan data adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan data terhadap penggunaan tidak sah (Syaiful Anwar, 2017)

Keamanan merupakan komponen yang vital dalam komunikasi data elektronis. Masih banyak orang yang tidak sadar bahwa dengan berkembangnya teknologi informasi maka berkembang pula kejahatan sistem informasi. Misalnya pencurian, pengerusakan atau penyalahgunaan data yang terkirim melalui jaringan komputer oleh pihak yang tidak bertanggung jawab.

Ada beberapa teknik yang dapat digunakan untuk mengamankan pengiriman data-data elektronis. Antara lain kriptografi yaitu teknik untuk menyandikan sebuah data dengan kunci dan algoritma tertentu. Teknik lain untuk mengamankan data adalah dengan menyembunyikan / menyisipkan data tersebut pada suatu media tertentu yang disebut juga dengan teknik Steganografi, sehingga tidak terlihat oleh orang yang tidak berkepentingan.

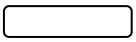
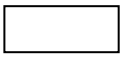
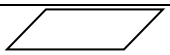
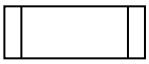
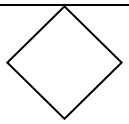
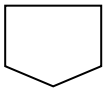
2.6. Permodelan Data Terstruktur

Alat-alat permodelan sistem informasi sangat dibutuhkan dalam proses analisis dan perancangan sistem. Alat-alat permodelan yang digunakan dalam penelitian ini adalah :

2.6.1. Flowchart

Flowchart adalah bagan alur yang menggambarkan langkah-langkah penyelesaian suatu masalah. Adapun simbol dari *flowchart yaitu :*

Tabel 2.1. Simbol-simbol *flowchart*

Simbol	Nama	Fungsi
	Terminator	Permulaan atau akhir program
	Garis Alir/ Flow Line	Arah aliran program
	Proses	Proses perhitungan atau pengolahan data
	Input / Output Data	Proses input atau output data, informasi, parameter
	Predefined Proses	Permulaan sub program atau proses menjalankan sub program
	Decision	Perbandingan pernyataan,penyeleksian data yangmemberikan pilihan untuk angkah selanjutnya
	One page Connector	Penghubung bagian-bagian flowchart yang ada dalam satu halaman
	Off Page Connector	Penghubung bagian-bagian flowchart yang berada pada halaman berbeda

2.6.2. *Unified Modelling Language (UML)*

Unified Modelling Language (UML) adalah standar bahasa yang banyak digunakan dalam industri untuk mendefinisikan *requirement*, desain, membuat analisis, serta menggambarkan arsitektur dalam pemrograman berorientasi objek.(Rosa A.S. dan M.Shalahuddin.2016)

1. *Use Case*

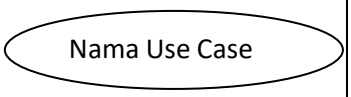
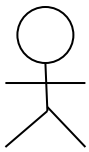
Diagram *use case* merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use case* ini mendeskripsikan sebuah interaksi antara atau lebih aktor dengan sistem informasi yang akan dibangun. *Use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut.

Syarat penamaan pada *Use case* adalah nama dapat diipahami dan dimengerti. Ada dua hal utama pada *use case* yaitu aktor dan *use case*.

a. Aktor merupakan orang, sistem lain, atau proses yang berinteraksi dengan sistem informasi yang akan dirancang diluar dari sistem informasi yang akan dirancang tersebut, walaupun simbol aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.
b. *Use Case* merupakan fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antara unit atau aktor.

Berikut adalah simbol-simbol yang ada pada diagram *use case* :

Tabel 2.2. Simbol-Simbol *Use case*

Simbol	Deskripsi
Use Case 	Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor, biasanya dinyatakan dengan menggunakan kata kerja diawal frase nama use case.
Aktor/Actor  Nama Aktor	Orang, proses atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat diluar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, biasanya dinyatakan menggunakan kata benda diawal frase nama aktor.
Asosiasi / Association 	Komunikasi antara aktor dan use case yang berpartisipasi pada use case atau use case memiliki interaksi dengan aktor
Ekstensi / Extend << extend >> 	Relasi use case tambahan ke sebuah use case dimana use case yang ditambahkan dapat berdiri sendiri walau tanpa use case tambahan itu, mirip dengan prinsip *inheritance* pada pemrograman berorientasi objek, biasanya use case tambahan memiliki nama depan yang sama dengan use case yang ditambahkan.

Generalisasi / Generalization 	Hubungan generalisasi dan spesialisasi (umum-khusus) antara dua buah use case dimana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.
Menggunakan / include / uses <<include>>  << uses >> 	Relasi use case tambahan ke sebuah use case dimana use case yang ditambahkan memerlukan use case ini untuk menjalankan fungsinya atau sebagai syarat dijalankannya use case ini.

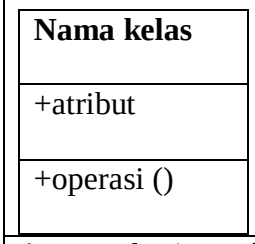
(Sumber : Rosa A.S dan M. Shalahudin, 2014:156)

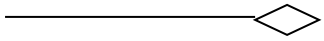
2. *Class Diagram*

Class diagram atau diagram kelas merupakan gambaran struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun atau merancang sebuah sistem. Kelas memiliki apa yang disebut atribut dan metode atau operasi sedangkan atribut adalah variabel-variabel yang dimilliki oleh suatu kelas dan operasi atau metode adalah fungsi-fungsi yang dimiliki oleh suatu kelas.

Diagram kelas dibuat agar programer membuat kelas-kelas sesuai dengan rancangan yang ada di diagram kelas agar antara dokumentasi perancangan dan *software* sinkron. Simbol-simbol diagram kelas:

Tabel 2.3. Simbol-simbol *class diagram*

Simbol	Deskripsi
Kelas  	Kelas pada struktur sistem.
Antarmuka / Interface  Nama interface	Samadengan konsep interface dalam pemrograman berorientasi objek.
Asosiasi / Association 	Relasi antar kelas dengan makna umum, asosiasi biasanya juga disertai dengan multiplicity
Asosiasi berarah /directed association 	Relasi antar kelas dengan makna kelas yang satu digunakan oleh kelas yang lain, asosiasi biasanya juga disertai dengan multiplicity.
Generalisasi 	Relasi antar kelas dengan makna generalisasi spesialisasi (umum-khusus)
Kebergantungan / Dependency 	Relasi antar kelas dengan makna kebergantungan antar kelas.

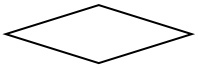
Agregasi / Aggregation 	Relasi antar kelas dengan makna semua bagian (whole-part)

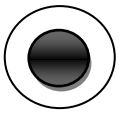
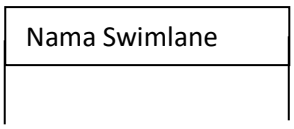
(Sumber : Rosa A.S dan M. Shalahudin, 2014:146)

3. *Activity Diagram*

Diagram aktivitas atau *activity diagram* merupakan gambaran *workflow* dari proses menu yang terdapat pada *software*. Yang perlu diperhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem. Berikut adalah simbol-simbol diagram aktivitas.

Tabel 2.4. Simbol-simbol *activity diagram*

Simbol	Deskripsi
Status awal 	Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal.
Aktivitas 	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.
Percabangan / decision 	Asosiasi percabangan dimana jika ada aktivitas pilihan lebih dari satu.
Penggabungan / Join 	Asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu.

Status Akhir 	Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status akhir.
Swimlane 	Memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi.

(Sumber : Rosa A.S dan M. Shalahudin, 2014:162)

2.7. Perangkat Lunak Pendukung

Pada sub bab ini akan menjelaskan tentang perangkat lunak pendukung dalam penyelesaian penelitian skripsi ini.

2.7.1. *Microsoft Visual Studio* 2015

Microsoft Visual Studio merupakan sebuah Perangkat Lunak lengkap (*suite*) yang dapat digunakan untuk melakukan pengembangan aplikasi, baik itu aplikasi bisnis, aplikasi personal, ataupun komponen aplikasinya, dalam bentuk aplikasi *console*, aplikasi windows, ataupun aplikasi web. *Visual Studio* mencakup Kompiler, *SDK*, *Integrated Development Environment (IDE)*, dan dokumentasi (umumnya berupa *MSDN Library*).

Kompiler yang dimasukkan ke dalam paket *Visual Studio* antara lain *Visual C++, Visual C#, Visual Basic, Visual Basic .NET, Visual InterDev,Visual J++, Visual J#, Visual FoxPro,* dan *Visual SourceSafe*. *Microsoft Visual Studio* dapat digunakan untuk mengembangkan aplikasi dalam *native code* (dalam

bentuk bahasa mesin yang berjalan di atas *Windows*) ataupun *managed code* (dalam bentuk *Microsoft Intermediate Language* di atas *.NET Framework*). Selain itu, *Visual Studio* juga dapat digunakan untuk mengembangkan aplikasi *Silverlight*, aplikasi *Windows Mobile* (yang berjalan di atas *.NET Compact Framework*).

Microsoft visual studio 2015 Enterprise dapat membuat dan mengedit aplikasi lebih mudah dan cepat sehingga meningkatkan produktifitas dalam pembuatan aplikasi.

BAB III

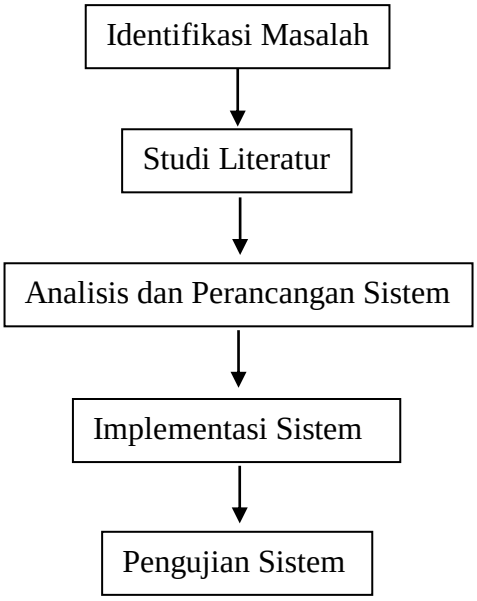
METODE PENELITIAN

3.1 Tahapan Penelitian

Penelitian yang dilakukan, diselesaikan melalui tahapan penelitian dalam lima tahapan yaitu:

1. Identifikasi masalah, yaitu mengidentifikasi masalah-masalah yang akan dibahas pada penelitian ini.
2. Studi literatur, yaitu mengumpulkan data-data melalui pembelajaran literatur pada sejumlah buku, artikel, paper, jurnal, makalah, maupun situs internet mengenai implementasi teknik steganografi LSB sebagai keamanan komunikasi data.
3. Analisis dan perancangan sistem, yaitu akan dilaksanakan perancangan antarmuka dan perancangan system keamanan teks pada citra bitmap dengan menggunakan algoritma LSB.
4. Implementasi sistem, yaitu mengimplementasikan tahapan penelitian sebelumnya kedalam sebuah program, dengan membangun aplikasi atau program sesuai kebutuhan sistem berdasarkan perancangan sistem yang telah dilakukan.
5. Pengujian sistem, yaitu melakukan ujicoba proses enkripsi dan deskripsi serta penyisispan dan ekstraksi.

Skema Tahapan Penelitian



Gambar 3.1. Skema Tahapan Penelitian

3.2 Metode Pengumpulan Data

Adapun metode pengumpulan data yang dilakukan pada penelitian ini yaitu:

1. Eksplorasi dan Studi Literatur

Eksplorasi dan studi literatur dilakukan dengan mempelajari konsep-konsep yang berkaitan dengan penelitian ini, seperti terori tentang teknik steganografi, metode-metode dalam steganografi, teknik enkripsi maupun struktur berkas audio melalui literatur-literatur seperti buku (textbook), paper, dan sumber ilmiah lain seperti situs internet ataupun asrtikel dokumen teks yang berhubungan.

2. Eksperimen

Setelah mendapatkan data secara studi pustaka, penulis melakukan eksperimen (ujicoba). Dalam eksperimen ini pengumpulan data dapat diambil secara langsung, sehingga penulis akan lebih mendalami dalam melakukan dan meminimalkan kesalahan dalam penelitian ini.

3.3 Analisis Sistem

Analisis sistem dapat didefinisikan sebagai penjabaran dari suatu sistem ke dalam bagian-bagian komponen dengan maksud untuk mengidentifikasi serta mengevaluasi hambatan dan permasalahan yang terjadi sehingga dapat diusulkan perbaikan sesuai kebutuhan yang diharapkan.

Sistem steganografi memerlukan semua jenis file gambar dan informasi atau pesan yang akan disembunyikan. Ini memiliki dua modul mengenkripsi dan mendekripsi. *Microsoft Visual Studio 2010* mempersiapkan sejumlah besar alat dan opsi untuk pemrograman yang menyederhanakan. Salah satu fungsinya untuk gambar dan gambarakan otomatis dikonversi ke jenis gambar format BMP.

Penulis menggunakan *software* tersebut dalam membangun perangkat lunak yang disebut "*Root Steganography*" yang ditulis dalam bahasa C # .Net dan diharapkan untuk dapat menyembunyikan informasi yang dibutuhkan. Adapun algoritma yang digunakan untuk enkripsi dan dekripsi dalam aplikasi ini menyediakan beberapa lapisan pengganti hanya menggunakan lapisan gambar *LSB*. Menulis data dimulai dari layer terakhir (layer 8st atau *LSB*) Karena lapisan ini sangat

penting dan lapisan atas memiliki dua kali lipat signifikan dari lapisan bawahnya. Jadi setiap langkah kita menuju ke lapisan gambar maka lapisan atas berkurang pada transpirasi *retouching* gambar.

Modul enkripsi digunakan untuk menyembunyikan informasi ke dalam gambar; tidak ada yang bisa melihat informasi atau file itu modul ini memerlukan semua jenis gambar dan pesan dan hanya memberi satu file gambar di tempat tujuan.

Modul dekripsi digunakan untuk mendapatkan informasi tersembunyi dalam file gambar. Ini mengambil file gambar sebagai output, dan memberi dua file pada folder tujuan, satu adalah file gambar yang sama dan yang lain adalah file pesan yang disembunyikan itu.

Kesimpulannya dalam skripsi ini akan dibangun aplikasi yang dapat digunakan sebagai sarana mengamankan komunikasi berupa data yang bertujuan untuk menjaga keaslian informasi yang akan disisipkan pada media penampung menggunakan teknik *steganography* dan penggunaan algoritma *LSB* (*least significant bit*) untuk menyembunyikan *file* didalam gambar digital yang akan mengekploitasi persepsi manusia ke pada gambar digital sehingga mengurangi kecurigaan pada data yang disisipi informasi.

Sebagai analisis sistem yang sedang bejalan, akan dibahas bagaimana prosedur dan aliran dokumen yang sedang berjalan digambarkan dalam bentuk *flowchart,* pengkodean dan analisis sistem non fungsional yang melputi perangkat keras dan perangkat lunak yang digunakan, serta analisis *user* yang terlibat.

3.3.1. Analisis Sistem Berjalan

Dari Rancangan Sistem yang diusulkan, diharapkan mampu menyembunyikan data kedalam gambar digital, tujuannya adalah untuk mengamankan data dari berbagai tindakan pencurian, penyadapan, modifikasi maupun fabrikasi data dari orang yang tidak memiliki wewenang tentang data tersebut. Adapun ukuran data yang mampu di tampung pada media penampung baiknya tidak lebih dari ukuran data tempat penampung itu sendiri untuk menghindari kecurigaan akibat perubahan warna yang terjadi pada media gambar yang telah disisipi data maupun informasi, terlebih jika media gambar penampung memiliki variasi warna yang banyak..

Media gambar penampung diharapkan memiliki kualitas gambar yang baik dengan pixel yang besar dengan tipe gambar *grayscale* untuk media menyimpan data, agar media penampung memiliki ruang yang besar pula untuk menyimpan berbagai data nantinya. Pemilihan tipe gambar *grayscale* lebih baik karena tidak memiliki banyak variasi warna, dan perubahan warna tidak terlalu signifikan pada tipe gambar jenis ini, karena penggunaan metode *LSB* (*least significant bit*) akan menyebabkan perubahan pada warna media gambar penampung, terlebih jika data yang disisipkan adalah data dengan ukuran yang sangat besar besar sedangkan media penampung memiliki variasi warna yang banyak.

3.3.2. Analisis Masalah

Analisis masalah dilakukan untuk mengatahui masalah-masalah apa yang terjadi dalam pengembangan aplikasi *steganography*. Masalah yang terjadi ketika pembangunan *steganography* pada citra digital yaitu kapasitas citra penampung yang akan menyimpan data, kualitas citra digital yang telah disisipi data, dan keamanan informasi yang disisipkan ke dalam citra tidak terjamin, karena saat ini banyak aplikasi dengan berbagai teknik untuk menganalisis citra apakah terdapat informasi yang disembunyikan dan letak dari informasi yang disembunyikan. Jika letak dari informasi yang disisipkan pada citra dapat diketahui, maka informasi akan langsung dapat diketahui.

3.3.3. Analisis Kebutuhan Sistem

Tahapan ini meliputi analisis kebutuhan kebutuhan sistem secara fungsional maupun non-fungsional.

A. Analisis Kebutuhan Fungsional

Analisis kebutuhan fungsional adalah suatu gambaran dari rangkaian informasi yang dipakai pada sistem yang bersangkutan yang meliputi :

1. Perangkat Keras (*hardware*)

Berikut adalah perangkat keras yang digunakan dalam rancangan pembangunan aplikasi *steganography*.

Tabel 3.1. Spesifikasi Perangakat Keras (*Hardware)*

Laptop		
No	Spesifikasi Hardware	
1	Monitor	1366 x 768 (64 bit) (60 Hz) 14"
2	*Processor*	Intel® Core™ i5 CPU M 460 @ 2.53GHz (4 CPUs)
3	RAM	6144 MB
4	VGA	*AMD Mobility Radeon HD 5000 Series*
5	Hardisk	640 GB
6	Jaringan	*LAN Card / Wirelless Card*

2. Perangkat Lunak (*software*)

Analisis yang telah dilakukan dalam kebutuhan software untuk mengembangkan dan menjalankan perancangan sistem yang disarankan agar aplikasi ini dapat berjalan dengan baik adalah :

a. Microsoft Visual Studio 2013 Professional

Gambar 3.2. Splash Screen Visual Studio 2013

B. Analisis Kebutuhan Non-fungsional

Analisis non-fungsional adalah sebuah tahap dimana pembangunan sebuah perangkat lunak menganalisis sumber daya yang akan digunakan perangkat yang dibangunnya.

Kebutuhan non-fungsional yang harus dimiliki oleh sistemnya adalah:

1. Waktu pemrosesan data (*running time*) yang cepat sehingga efektif ketika digunakan oleh user.

   Tampilan antarmuka (*user interface*) yang mudah dipahami oleh pengguna (*user friendly*).

3.3.4. Analisis Teknik *Steganography*

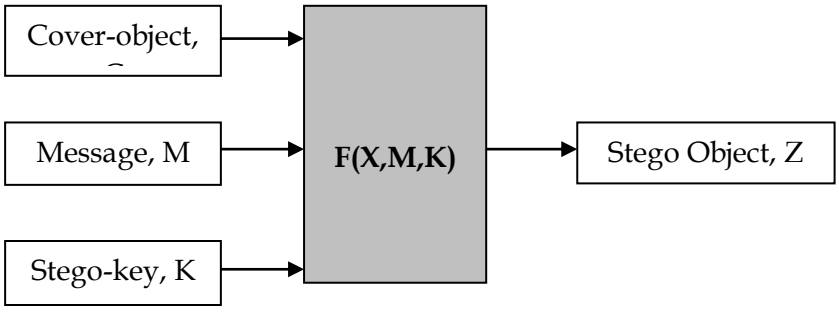
Teknik *steganography* adalah teknik komunikasi terselubung. Jadi,persyaratan mendasar dari sistem *stegarnography* ini adalah bahwa pesan yang dibawa oleh stego media seharusnya tidak masuk akal bagi manusia.

Adapun rancangan ini memiliki tujuan sebagai berikut:

1. Untuk alat keamanan produk berdasarkan teknik *steganography*.
2. Untuk mengekplorasi teknik penyembunyian data dengan menggunakan modul enkripsi dari rancangan ini.
3. Untuk mengektrak teknik mendapatkan data rahasia menggunakan modul dekripsi.

Steganography terkadang digunakan saat enkripsi tidak diijinkan, atau lebih umum lagi, *steganography* digunakan untuk melengkapi enkripsi. File terenkripsi mungkin masih menyembunyikan informasi menggunakan *steganography*, jadi walaupun file terenkripsi diuraikan, pesan tersembunyi tetap tidak dapat terlihat.

Pada dasarnya, model *steganography* ditujukan pada gambar berikut:



Gambar 3.3. Contoh model *steganography*

Pesan adalah data yang diinginkan pengirim agar tetap dirahasiakan. Bisa berupa teks biasa, *ciphertext*, gambar lain, atau apapun yang bisa disematkan dalam aliran kecil seperti tanda hak cipta, komunikasi terselubung, atau nomor seri. Password dikenal sebagai *stego-key*, yang memastikan bahwa hanya penerima yang mengetahui kunci decoding yang sesuai yang dapat mengekstrak pesan dari objek sampul. Objek sampul dengan pesan tersemat diam-diam kemudian disebut objek Stego.

Memulihkan pesan dari objek stego memerlukan objek sampulnya dan kunci decoding yang sesuai jika kunci stego digunakan selama proses pengkodean. Gambar asli mungkin atau mungkin tidak diperlukan di sebagian besar aplikasi untuk mengekstrak pesan.

Ada beberapa operator yang sesuai di bawah ini untuk menjadi objek sampul:

1. Audio yang menggunakan format audio digital seperti wav, midi, avi, mpeg, mpi dan voc
2. File dan Disk yang bisa menyembunyikan dan menambahkan file dengan menggunakan ruang kendur
3. Teks seperti karakter null, sama seperti kode morse termasuk html dan java
4. File gambar seperti bmp, gif dan jpg, di mana keduanya bisa berwarna dan abu-abu.

Secara umum, proses penyembunyian informasi mengekstrak bit redundansi dari objek sampul. Prosesnya terdiri dari dua tahap:

1. Identifikasi bit redundan pada *cover-object*. Bit *redundant* adalah bit yang dapat dimodifikasi tanpa merusak kualitas atau menghancurkan integritas objek sampul.

   Proses penyisipan kemudian memilih subset dari bit yang berlebihan untuk diganti dengan data dari pesan rahasia. Objek stego dibuat dengan mengganti bit redundan yang dipilih dengan bit pesan

3.3.5. Analisis Metode

Selama beberapa tahun terakhir, banyak teknik steganografi yang menanamkan pesan tersembunyi pada objek multimedia telah diajukan. Ada banyak teknik untuk menyembunyikan informasi atau pesan dalam gambar sedemikian rupa sehingga perubahan yang dibuat pada citra secara indual terbaca. Biasanya pendekatannya meliputi teknik LSB, *Masking* dan *Filtering* and *Transform*.

Penyisipan *least significant bit (LSB)* adalah pendekatan sederhana untuk menyematkan informasi pada file gambar. Teknik steganografi yang paling sederhana menyematkan bit pesan secara langsung ke bidang bit yang paling tidak penting dari *cover-image* dalam urutan deterministik. Modulasi bit paling signifikan tidak menghasilkan perbedaan yang dapat dirasakan manusia karena amplitudo perubahannya kecil.

Dalam teknik ini, kapasitas *embedding* dapat ditingkatkan dengan menggunakan dua atau beberapa bit paling signifikan. Pada saat yang sama, tidak hanya risiko membuat pesan tersemat yang terdeteksi secara statistik namun juga kesetiaan gambar menurun. Oleh karena itu, skema *embedding* LSB ukuran variabel disajikan, di mana jumlah LSB yang digunakan untuk penyisipan pesan / ekstraksi bergantung pada karakteristik piksel lokal. Kelebihan metode berbasis LSB mudah diimplementasikan dan *high pay-load.*

A. Algoritma dari LSB

Penyisipan dengan teknik *Least Bit Significant (LSB)* adalah pendekatan umum dan sederhana untuk menyematkan bit pesan pada piksel gambar sampul. Teknik ini bekerja dengan baik untuk *steganography* gambar.

Algoritma untuk menyematkan pesan teks menggunakan gambar seperti berikut:

Langkah 1 : Baca gambar sampul dan pesan teks, yang disembunyikan di gambar sampul.

Langkah 2 : Mengkonversi pesan teks menjadi biner.

Langkah 3 : Hitung LSB dari piksel gambar sampul.

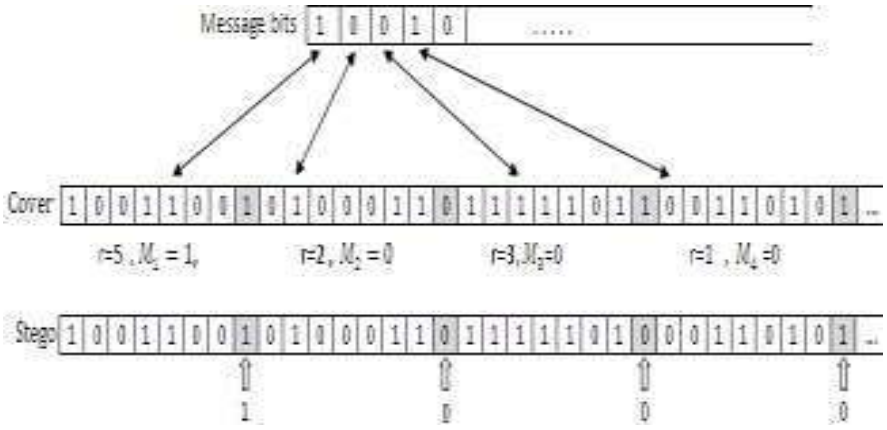
Langkah 4 : Ganti LSB dari piksel gambar sampul dengan setiap bit pesan rahasia satu per satu.

Langkah 5 : Tulis gambar stego.

Biasanya perubahan rata rata hanya separuh LSB yang perlu dirubah. Perbedaan gambar sampul (Asli) dengan dengan gambar stego hampir tidak terlihat oleh mata manusia. Karena intensitas cahaya pada masing masing sampul piksel-piksel terjadi 0 atau ± 1 unit.

Karena teknik LSB digunakan untuk menyembunyikan pesan ke dalam gambar, maka untuk meningkatkan sistem keamanan, digunakan teknik baru yang terdiri dari penyebaran bit secara acak pada gambar. Diusulkan dalam penyempurnaan ini bahwa penyisipan bit pesan kedalam gambar tidak hanya dalam bit paling tidak signifikan tetapi juga bit lainnya dalam piksel secara acak. Hal ini dapat dicapai dengan membandingkan bit pesan dengan bit piksel yang dipilih secara acak dari bit kedua sampai terakhir, (r), yang kita hasilkan dengan algoritma logaritma diskrit atau teknik lainnya.

Bedasarkan perbandingan ini, 1 masukan kedalam bitpaling sedikit jika bit pesan identik dengan gambar, sedangkan 0 dimasukan jika bit pesan tidak sesuai dengan bit yang dipilih dari gambar. Penulis menggunakan teknik LSB untuk menyematkan bit pesan tapi menggunakan teknik acak untuk pengkodean bit asli agar lebih aman dari teknik LSB.



Gambar 3.4. Menanamkan bit pesan dalam piksel cover gambar dengan Algoritma LSB.

1. Algoritma logaritma diskrit dan bilangan acak

Perhitungan logaritma diskrit dapat digunakan untuk memecahkan masalah pemetaan urutan. Ide utamanya disini adalah menghasilkan serangkaian bilangan acak panjang yang sama dengan panjang pesan, (m), yang berkisaran antara 3 sampai 8. Seri bilangan ini akan digunakan untuk pemetaan acak. Penulis mendefinisikan logaritma diskrit untuk menghasilkan bilangan acak. Angka-angka ini tergantung pada nilai kunci (k). Nilai dihitung dari persamaan berikut, dan angka-angka ini akan dibatasi pada panjang pesan :

x_i=a*x(i-1) (mod p) (1), i=1,….,m.

dimana

x_0= adalah jumlah panjang digit k

$a=3x_0$

p=K

Angka dibuat dari persamaan di atas kemudian digunakan menghasilkan angka lain mulai dari 3 sampai 8. Yang terakhir digunakan untuk menemukan digit gambar (dalam piksel) yang akan digunakan dalam perbandingan dengan bit pesan, seperti berikut :

$$r = p_i = x_i \ (mod\ 7) + 2 \quad (2)$$

Memulihkan pesan dari gambar stagano membutuhkan kunci decoding yang sesuai, k yang digunakan selama proses pengkodean. Oleh karena itu pengirim dan penerima harus berbagi kunci selama komunikasi. Kunci k kemudian digunakan untuk memilih posisi piksel tempat bit disematkan bersembunyi.

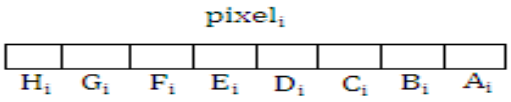
2. Algoritma untuk menyematkan pesan

Algoritma untuk menyematkan pesan menggunakan gambar *grayscale*adalah sebagai berikut:

Langkah 1: Ekstrak set bit dari pesan.

Langkah 2: Hitung piksel dari gambar sampul.

Piksel = {$piksel_1$,$piksel_2$,$piksel_3$,...,$piksel_n$}



Langkah 3: Ekstrak LSB pada gambar sampul. LSB={A_1,A_2,…,A_N}

Langkah 4: Ekstrak LSB pada gambar sampul. LSB ={B_1, B_2,..B_N}

Langkah 5: For i = 1 *to message length do*

{

If(M_i == B_i) *then do nothing*

Else

{

If(M_i == 1 and B_i == 0) *Then*

{

$B_i = M_i$;

A_i=0;

$pixel_i$=$Pixel_i$-1;

}

Else If (M_i = = 0 and B_i = = 1)Then

{

$B_i = M_i$;

A_i=1;

$pixel_i$=$Pixel_i$ +1;

}}

Tabel 3.2. Hasil Ekperimen dari teknik LSB

	Cover image $pixel_i$										Stego image $pixel'_i$								
i	H_i	G_i	F_i	E_i	D_i	C_i	B_i	A_i	decimal	M_i	H'_i	G'_i	F'_i	E'_i	D'_i	C'_i	B'_i	A'_i	decimal
1	1	0	0	1	0	0	0	0	144	1	1	0	0	1	0	0	0	1	145
2	1	0	0	1	1	0	1	0	154	0	1	0	0	1	1	0	1	0	154
3	1	0	0	1	1	1	0	0	156	0	1	0	0	1	1	1	0	0	156
4	1	0	0	1	0	0	1	0	146	0	1	0	0	1	0	0	1	0	146
5	1	0	0	1	0	1	0	1	150	0	1	0	0	1	0	1	0	1	150
6	1	0	0	1	1	1	0	1	157	0	1	0	0	1	1	1	0	1	157
7	1	0	1	0	1	1	1	1	175	0	1	0	1	0	1	1	1	0	174
8	1	0	1	0	0	1	0	1	165	1	1	0	1	0	0	1	0	1	165

3.3.6. Analisis Gambar *Staganography* dan Gambar Bitmap

Menggunakan gambar bitmap untuk menyembunyikan informasi rahasia adalah salah satu pilihan paling populer untuk *Steganography*. Banyak jenis perangkat lunak yang dibangun untuk tujuan ini, beberapa perangkat lunak ini menggunakan proteksi password untuk mengenkripsi informasi pada gambar. Untuk menggunakan perangkat lunak ini Anda harus memiliki format gambar 'BMP' untuk menggunakannya, namun menggunakan jenis gambar lainnya seperti "JPEG", "GIF" atau jenis lainnya agak atau tidak pernah digunakan, karena algoritma "BMP" Gambar untuk *Steganography* itu sederhana. Juga kita tahu bahwa di web yang paling populer adalah tipe "JPEG" dan tipe lainnya bukan "BMP", jadi kita harus punya solusi untuk masalah ini.

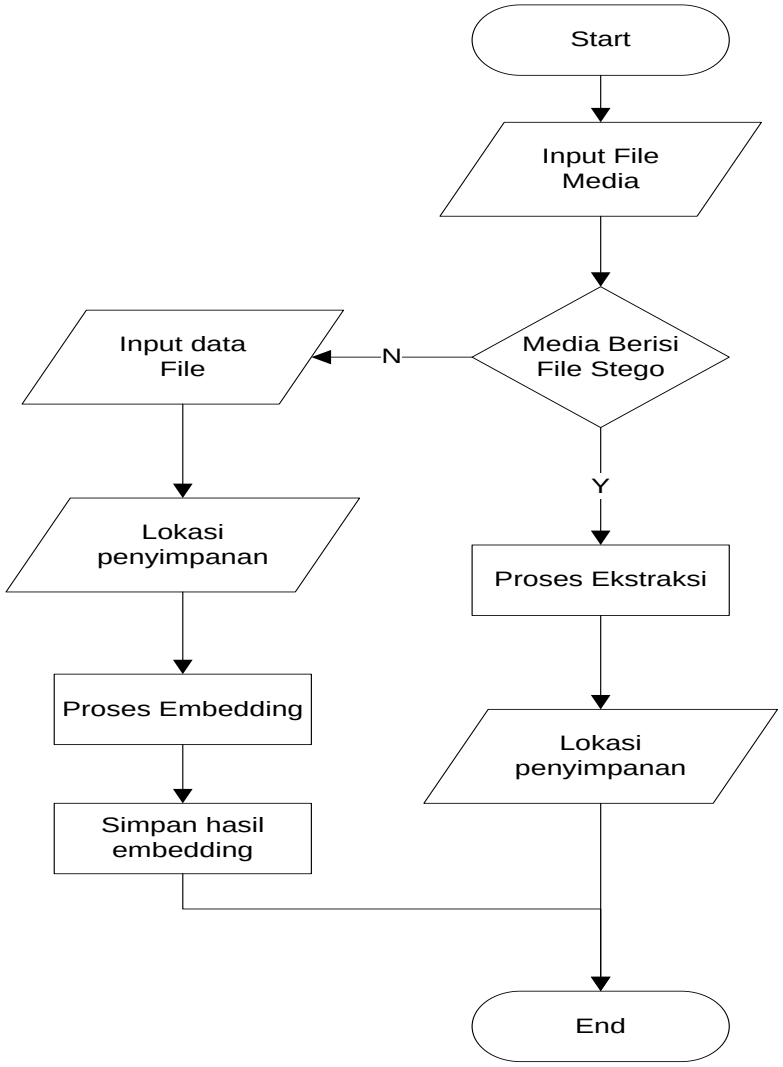
Rancangan perangkat lunak ini diharapkan memberikan solusi dari masalah ini, agar dapat menerima semua jenis gambar untuk menyembunyikan file informasi, namun akhirnya ia hanya memberi hasil satu foto "BMP" sebagai keluaran yang memiliki file tersembunyi di dalamnya.

3.4 Perancangan Sistem

Dalam penyusunan suatu program diperlukan suatu model data yang berbentuk diagram sebagai upaya untuk memperjelas kebutuhan fungsional bentuk data yang dibutuhkan oleh sistem agar dapat berjalan sesuai dengan prosedur yang dibangun. Aplikasi yang di bangun akan di modelkan menggunakan *flowchart* maupun *unifield modeling language (UML).*

3.4.1. Perancangan *Flowchart*

Pada Perancangan *Flowchart* ini merupakan perancangan yang digunakan untuk menjelaskan urutan langkah-langkah cara kerja rancangan aplikasi *steganography* ketika di jalankan.

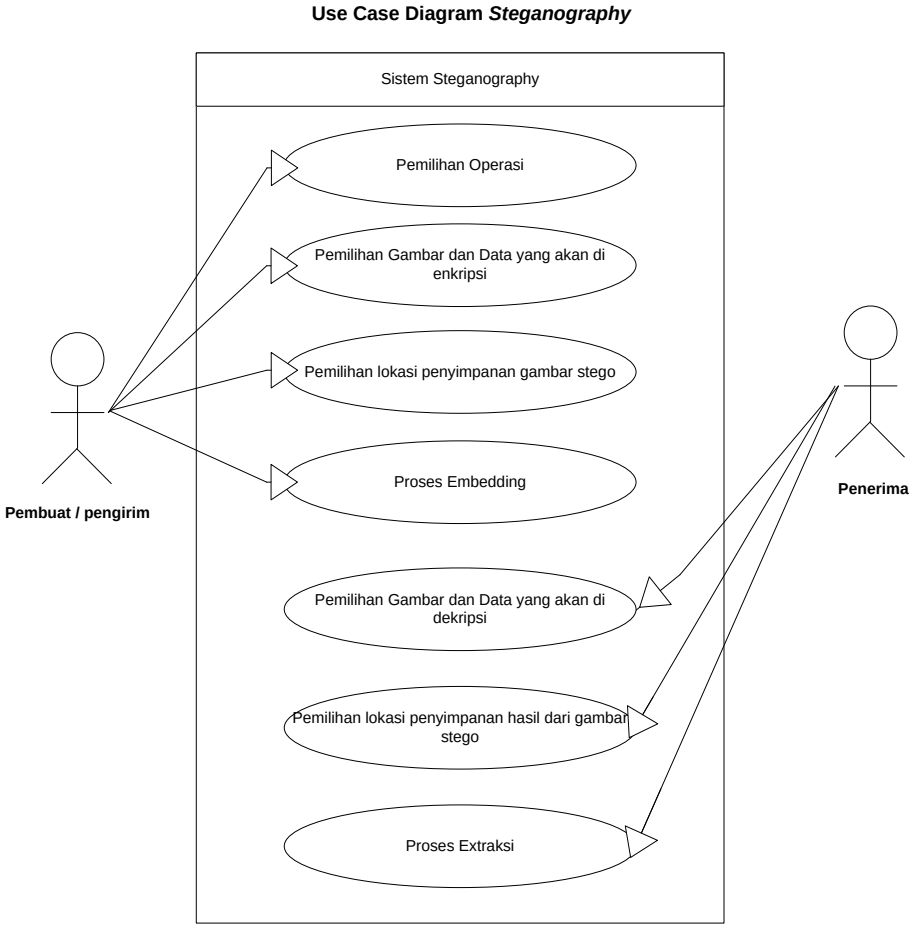


Gambar 3.5. flowchart perancangan sistem *steganography*

3.4.2. *Unifield Modeling Language (UML)*

A. *Use Case Diagram*

Diagram *use case* merupakan bagian tertinggi dari fungsionalitas yang dimiliki sistem yang akan menggambarkan bagaimana seorang aktor akan menggunakan dan memanfaatkan fungsionalitas sistem yang terdapat pada aplikasi *steganography*.



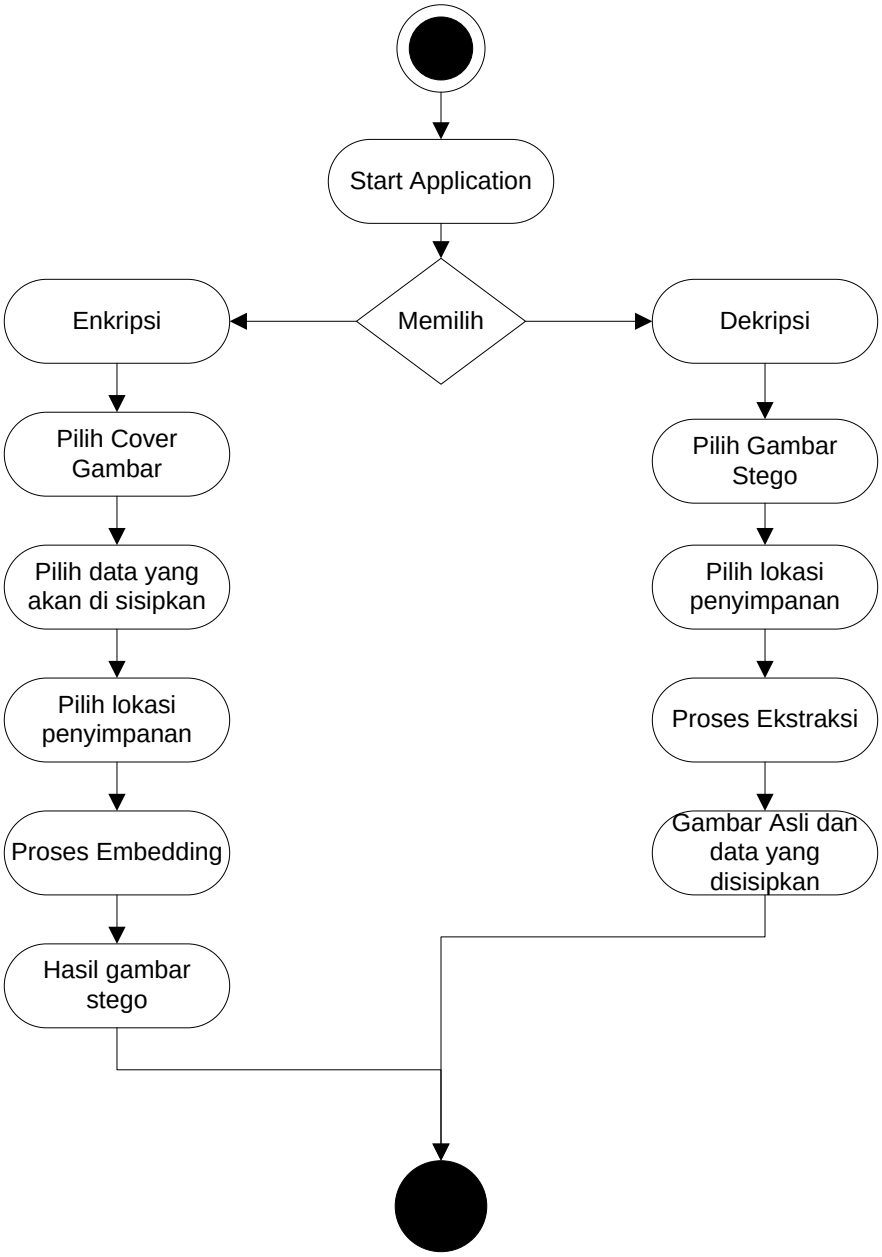
Gambar 3.6. ***Use Case Diagram Steganography***

Adapun Skenario yang terdapat pada diagram *Use Case* pada aplikasi ini yaitu :

Pengirim menekan tombol *browse* untuk menentukan media gambar penampung data, lalu sistem akan menampilkan dialog *open file*, lalu pengirim memilih media penampung, lalu memilih data yang akan di sisipkan. Maka sistem akan menampilkan informasi citra sebelum pengirim menekan tombol enkripsi untuk menyisipkan data yang akan disisipkan pada media gambar penampung.

B. Activity Diagram

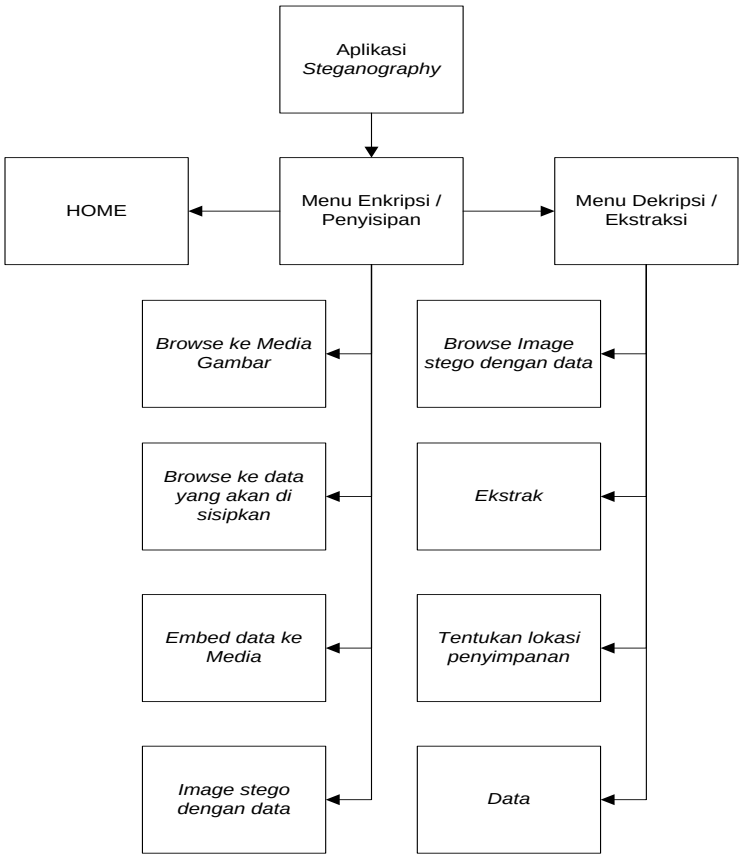
Activity Diagram menggambarkan bagaimana alir aktifitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana aplikasi hingga berakhir.



Gambar 3.7. Perancangan *Activity Diagram*

3.4.3. Perancangan Antarmuka

Program simulasi ini mempunyai sebuah layer utama dan mempunyai beberapa menu. Hirarki menu menu yang terdapat dalam program simulasi ini dapat dilihat pada gambar :



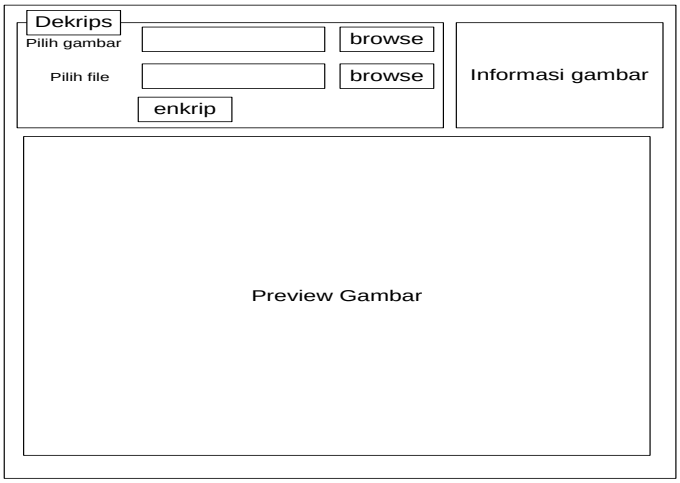
Gambar 3.8. Struktur aplikasi *steganography*

3.4.4. Perancangan antarmuka Home

Perancangan antarmuka adalah tahapan pembuatan rancangan untuk digunakan pada pengembangan aplikasi *steganography* yang dibagi menjadi beberapa bagian.

1. Perancangan antarmuka penyisipan

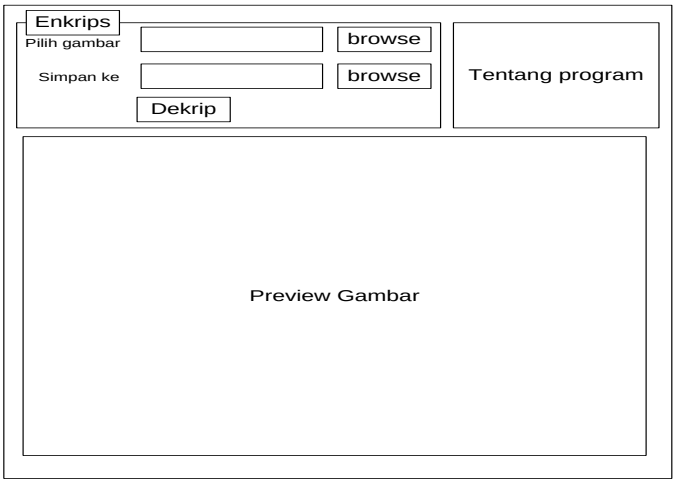
   Pada layer penyisipan ini berfungsi untuk proses penyisipan.



Gambar 3.9. perancangan antarmuka layar penyisipan

2. Perancangan antarmuka ekstraksi

   Pada layer ekstraksi ini berfungsi untuk proses ekstraksi dari gambar stego.



Gambar 3.10. perancangan antarmuka layer ekstraksi

BAB IV

HASIL DAN PEMBAHASAN

4.1. Implementasi Sistem

4.1.1. Definisi Implementasi Sistem

Pada bab ini akan dilakukan implementasi dan pengujian terhadap sistem. Tahapan ini dilakukan setelah perancangan selesai dilakukan dan selanjutnya akan di implementasikan pada Bahasa pemograman. Setelah di implementasikan maka akan dilakukan pengujian sistem untuk melihat kekurangan-kekurangan paada aplikasi untuk pengembangan sistem selanjutnya.

Setelah sistem di analisis dan didesain, maka akan menuju tahap implementasi. Implementasi merupakan tahapan untuk menilai dan menkonfirmasi modul-modul perancangan, sehingga pengguna dapat memberikan masukan kepada pembangunan sistem.

Langkah-langkah yang dibutuhkan dalam implementasi sistem adalah sebagi berikut :

1. Menyelesaikan desain sistem yaitu desain *interface,* desain *input,* desain *output.*
2. Menyediakan perangkat lunak (*software*), perangkat keras (*hardware*) dan pemakai (*brainware*) untuk mendukung pengembangan sistem.
3. Menulis, menguji, mengontrol dan mendokumentasi aplikasi computer.
4. Menguji sistem apakah sistem yang dibuat telah sesuai dengan perancangan yang dibutuhkan.

4.1.2. Tujuan Implementasi Sistem

Adapun tujuan implementasi dari sistem adalah untuk menerapkan perancangan yang telah dilakukan, sehingga pengguna dapat memberi masukan demi berkembangnya sistem yang telah dibangun.

4.1.3. Kebutuhan implementasi sistem

Setiap sistem yang dirancang memerlukan sarana pendukung yaitu berupa peralatan atau aplikasi pendukung yang berperan penting dalam menunjang penerapan sistem yang di desain.

Beberapa kebutuhan pada umumnya dibutuhkan oleh sistem antara lain adalah:

1. Perangkat keras yang digunakan

Berikut adalah spesifikasi perangkat keras yang digunakan saat proses implementasi.

Perangkat Keras	Spesifikasi
Processor	Core i5 M460@2.53GHz
RAM	6 GB
Hardisk	640 GB
VGA	AMD Radeon 5000 S
Monitor	14"
Mouse	Standar
Keyboard	Standar

Tabel 4.1. Perangkat keras yang digunakan

2. Perangkat lunak yang digunakan

Berikut adalah spesifikasi perangkat lunak yang digunakan saat proses implementasi.

Tabel 4.2. Perangkat lunak yang digunakan

Perangkat Lunak	Keterangan
Sistem Operasi	*Microsoft Windows 7 Ultimate*
Perancangan tampilan	*Microsoft Visual Studio 2010*
Net Framework	*Net framework* dengan versi 4.0

4.2. Implementasi Antarmuka (*interface*)

Implementasi antarmuka akan diambil dari *screenshoot* aplikasi ketika aplikasi dijalankan.

4.2.1. Tampilan utama dan tampilan menu enkripsi

Tampilan utama dan tampilan menu enkripsi sesuai dengan rancangan sebelumnya dimana tampilan utama dari aplikasi bukanlah halaman *login*, karena aplikasi sederhana ini tidak membutuhkan halaman *login.* Adapun fungsi dan keterangan dari tampilan adalah:

1. Tab menu *encrypt Image* adalah fungsional dari program dalam proses enkripsi.
2. Tombol *browse* pilih gambar untuk memilih media gambar yang sesuai untuk di jadikan media untuk menyisipkan berbagai data.

3. Tombol *browse* pilih file adalah untuk memilih data yang akan disembunyikan dan akan disisipkan pada media gambar.
4. *Image information* berfungsi menampilkan informasi dari media gambar.
5. *Image Preview* berfungsi untuk menampilkan media gambar yang nantinya akan digunakan untuk menyimpan data sisipan.

Gambar 4.1. Tampilan dari menu enkripsi

4.2.2. Tampilan menu dekripsi

Tampilan dari menu dekripsi hampir sama dengan tampilan menu enkripsi dan sesuai dengan rancangan sebelumnya. Adapun fungsi dan keterangan dari tampilan adalah:

1. Tombol *browse* pilih gambar untuk memilih media gambar stego yang telah disisipi oleh data untuk melakukan proses ekstraksi.

2. Tombol *browse* simpan ke adalah untuk memilih lokasi penyimpanan file setelah proses ekstraksi data.
3. Tentang programberfungsi menampilkan informasi dari judul penulis.
4. *Image Preview* berfungsi untuk menampilkan media gambar stego yang nantinya akan melakukan proses ekstraksi.

   Berikut adalah gambar dari menu dekripsi:

Gambar 4.2. Tampilan dari menu dekripsi

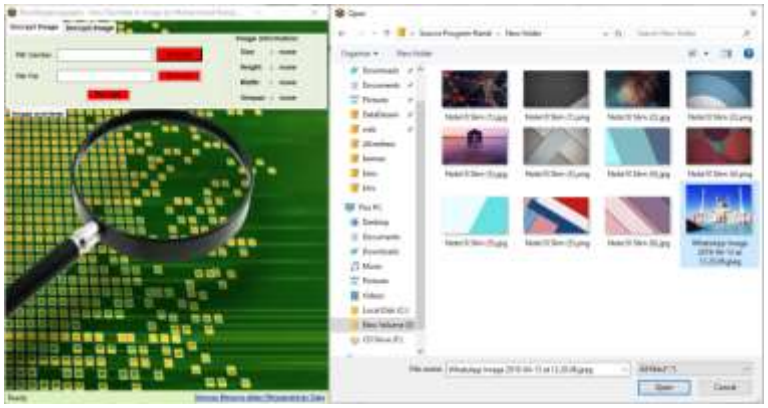
4.3. Pengujian Sistem dan Analisa Hasil

Pada tahapan pengujian sistem, penulis akan melakukan pengujian terhadap program yang telah dibuat. Pengujian dilakukan untuk mengetahui kemampuan perangkat lunak.

4.3.1. Pengujian proses enkripsi

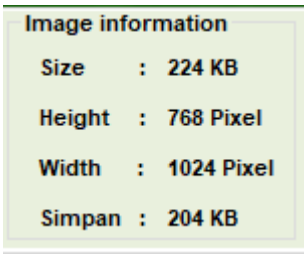
Adapun tahapan pada proses pengujian ini dilakukan adalah:

Tahap 1. Melakukan pemilihan pada gambar sebagai media penyimpanan.



Gambar 4.3. Proses pemilihan gambar.

Klik *browse*lalu pilih gambar yang akan digunakan. Setelah tahap ini informai tentang gambar akan di tampilkan pada sisi sebelah kanan.



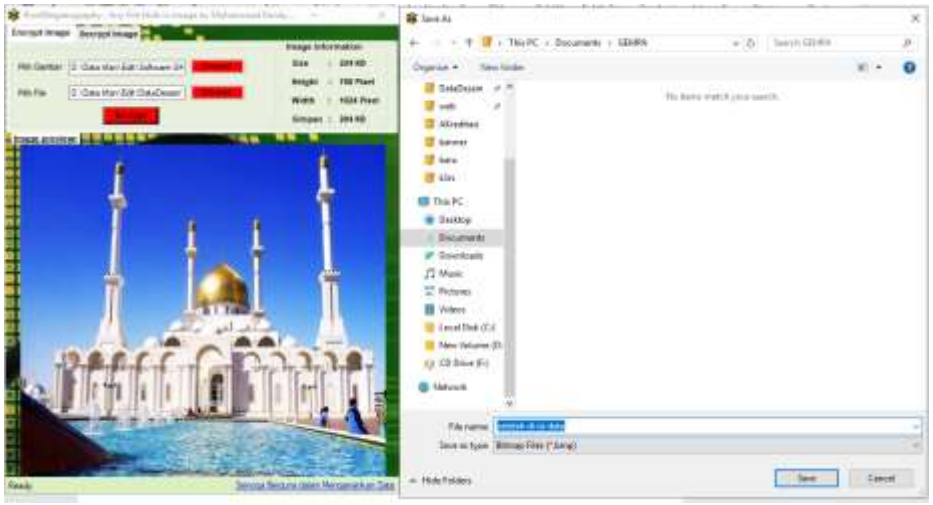
Gambar 4.4. informasi gambar

Informasi simpan dibutuhkan seberapa besar media mampu menampung data.

Tahap 2. Melakukan pemilihan data yang akan di sisipkan pada media dengan mengklik pilih file pada *browse* lalu tentukan file yang akan di sisipkan.

Gambar 4.5. Pemilihan data yang akan disisipkan

Tahap 3.Sebelum proses enkripsi, program akan menampilkan lokasi penyimpanan hasil gambar stego yang membawa data.



Gambar 4.6. Memilih lokasi penyimpanan

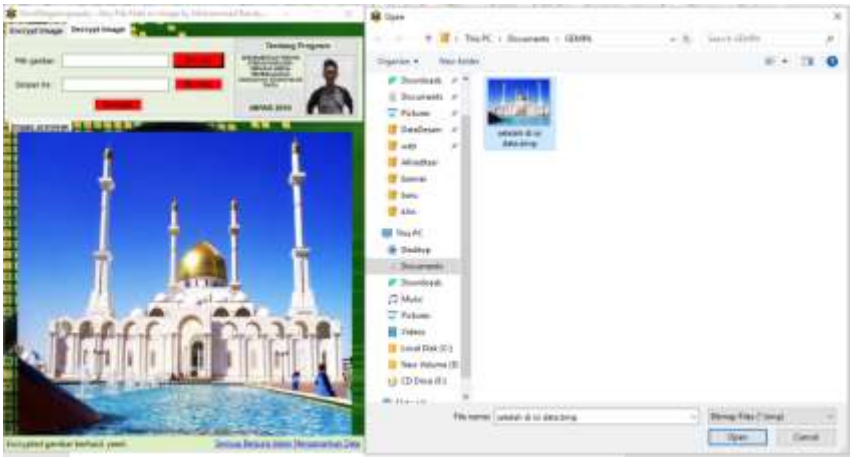
Tahap 4. Proses embedding data ke media gambar dengan format .BMP.

4.3.2. Pengujian Proses Dekripsi

Pengujian ini dilakukan untuk melihat ketersediaan data yang telah di sisipkan sebelumnya kedalam media gambar, apakah masih dapat dikembalikan atau tidak.

Adapun tahapan dari proses pengujian ini adalah:

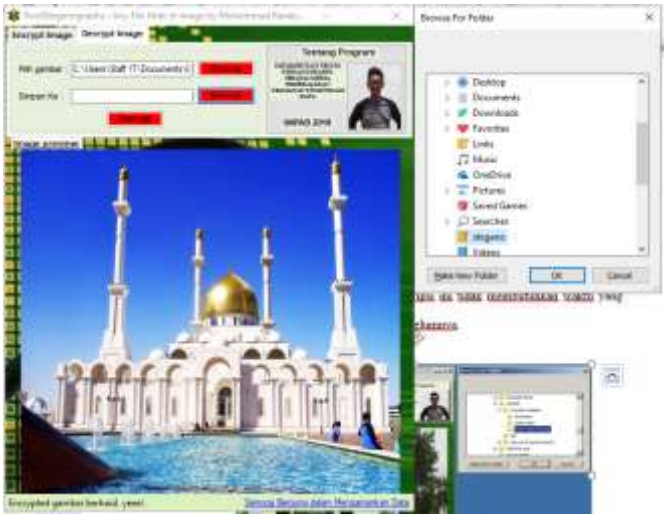
Tahap 1. Pemilihan gambar stego yang membawa data rahasia, secara *default* gambar stego ini memiliki format file bitmap (.bmp) setelah tahap ini gambar akan ditampilkan pada *image preview* pada aplikasi.



Gambar 4.7. Proses pemilihan gambar stego

Tahap 2. Pemilihan lokasi ekstraksi data rahasia dari dalam gambar stego ke lokasi penyimpanan yang ditentukan. Proses dekripsi ini tidak membutuhkan waktu yang begitu lama, seperti proses enkripsi data sebelumnya.

Tahap 3. Proses ekstraksi



Gambar 4.8.Pemilihan lokasi ekstraksi

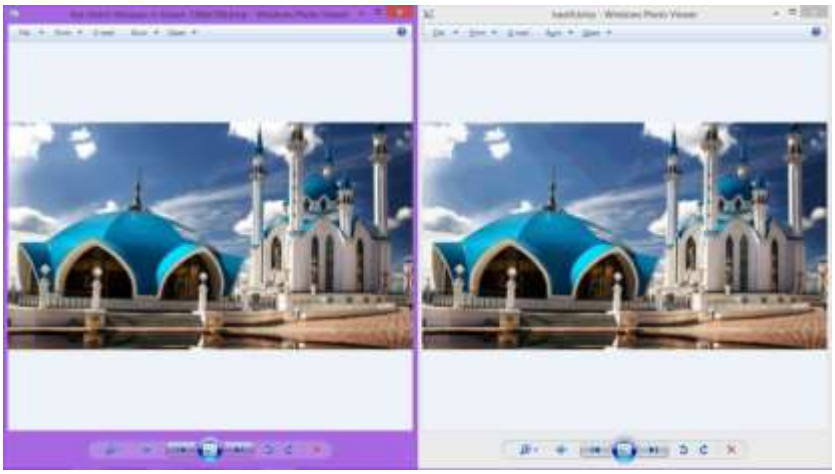
4.3.3. Analisa Perbandingan

Pada tahapan ini berbagai Analisa penulis lakukan untuk melihat berbagai perbedaan gambar setelah melalui proses penyisipan (*embedding)* maupun ekstraksi (*extract*) data.

Adapun Analisa yang penulis lakukan adalah :

1. Analisa Warna

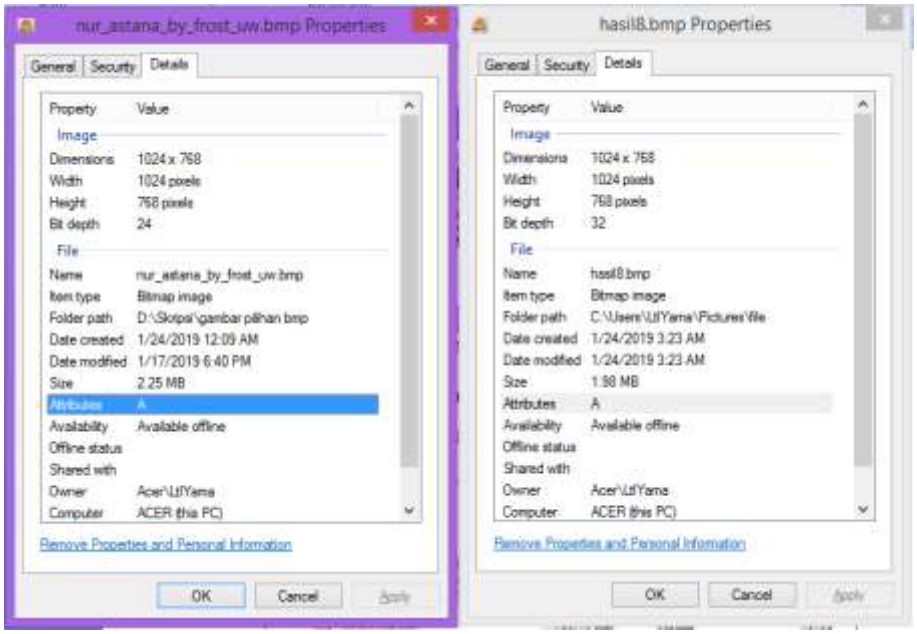
Pada tahapan ini penulis akan menganalisa gambar sebelum di sisipkan data dengan gambar yang sudah disisipkan data untuk menguji berbagai perbedaan yang mungkin terjadi.



Gambar 4.9. Gambar asli (kiri) dan gambar stego (kanan)

Pada gambar diatas menjelaskan bahwa tidak terdapat perubahan warna antara gambar asli dan gambar stego yang telah disisipi data. Jadi dapat disimpulkan bahwa data yang disisipkan tidak dapat diketahui.

2. Analisa Ukuran

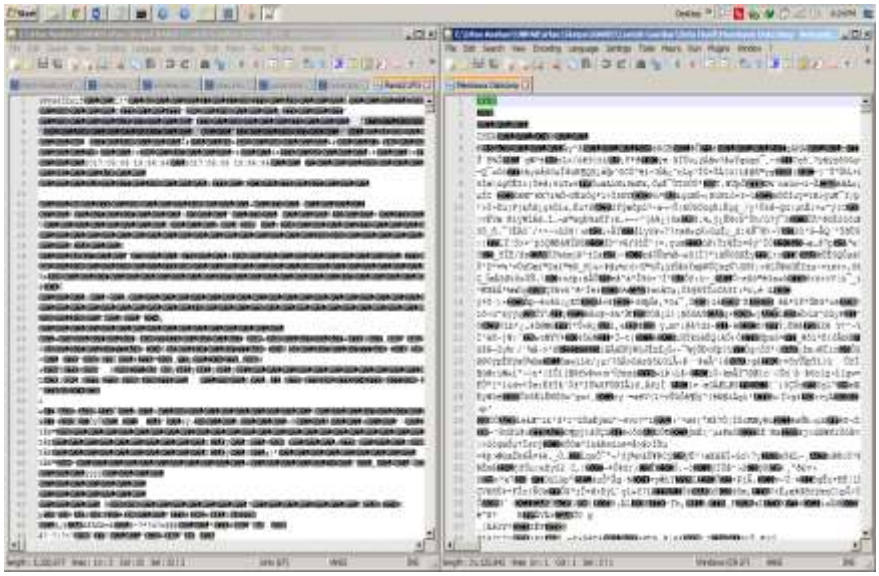


Gambar 4.10. Ukuran dari gambar stego (kanan) lebih besar dari gambar asli (kiri)

Pada gambar diatas memperlihatkan perbedaan yang sangat signifikan dimana gambar stego ukuran nya lebih kecil dari gambar aslinya.

3. Analisa isi dari gambar

Pada Analisa jenis ini penulis membuka gambar asli dan gambar stego menggunakan aplikasi Notepad++ untuk melihat perbedaan isi dari kedua gambar tersebut.

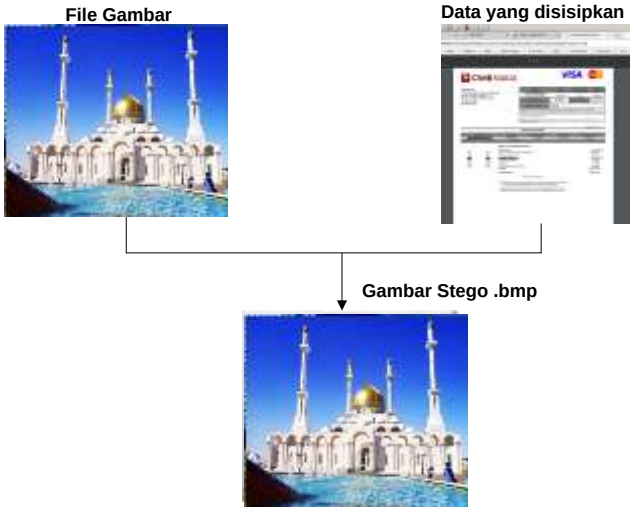


Gambar 4.11. perbedaan isi gambar asli (kiri) dengan gambar stego (kanan)

4.4. Analisa Proses

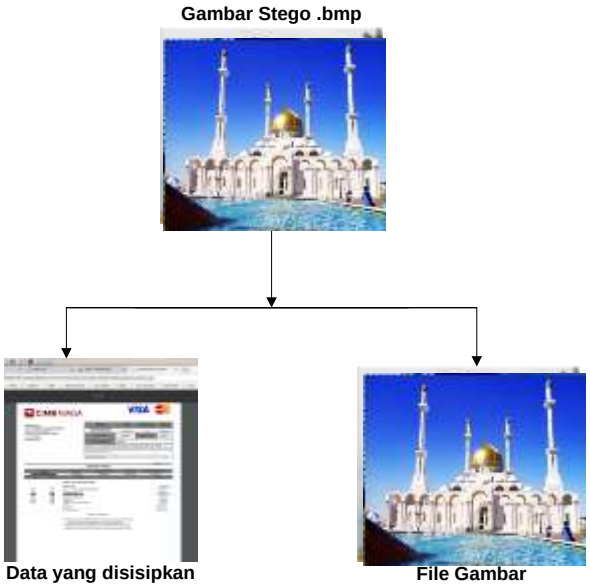
Pada Analisa proses penulis menggambarkan gambaran sederhana bagaimana aplikasi bekerja dalam proses enkripsi dan proses dekripsi.Berikut adalah gambaran sederhana dari Analisa proses.

4.4.1. Analisa Proses Enkripsi



Gambar 4.12. Analisa proses enkripsi

4.4.2. Analisa Proses Dekripsi



Gambar 4.13. Analisa proses dekripsi

4.5. Pengujian

Pada penelitian ini menguji gambar *cover* yang sudah ditetapkan berukuran sebesar 300kb dengan menyisipkan file gambar yang berbeda dengan proses enkripsi dan menganalisa perbedaannya.

4.5.1. Pengujian data menggunakan file gambar .Jpg

Tabel 4.3. Pengujian Data Gambar

GAMBAR *COVER*	FILE YANG DISISIPKAN	HASIL STEGO	KELUARAN
 **Cover.bmp** **301kb**	 **Data1.jpg** **11kb**	 **310kb**	 **11kb**
	 **Data2.jpg** **24kb**	 **311kb**	 **24kb**
	 **Data3.jpg** **34kb**	 **311kb**	 **34kb**

 **Cover.bmp** **301kb**	 **Data4.jpg** **42kb**	 **312kb**	 **42kb**
	 **Data5.jpg** **51kb**	 **310kb**	 **51kb**
	 **Data6.jpg** **61kb**	 **312kb**	 **61kb**
	 **Data7.jpg** **70kb**	 **313kb**	 **70kb**
	 **Data8.jpg** **81kb**	 **314kb**	 **81kb**

	 **Data9.jpg** **90kb**	 **311kb**	 **90kb**
	 **Data10.jpg** **100kb**	 **311kb**	 **100kb**
	 **Data11.jpg** **254kb**	 **262kb**	 **254kb**

Pada tabel 4.3. diatas didapat bahwa, gambar *cover* yang digunakan dalam penyisipan file ukuran 10kb sampai 100kb tidak mengalami perbedaan gambar yang signifikan. Namun, pada penyisipan file dengan ukuran 250kb, gambar *cover* menjadi rusak akibatnya gambar tersebut mengalami perbedaan yang signifikan dari sebelum disisipkan file. Jika dilihat dari hasil keluaran proses deskripsi, gambar yang telah disisipkan mengalami perubahan gambar sedikit demi sedikit dengan bertambahnya ukuran file yang disisipkan. Hal ini dapat dilihat jelas dari tabel 4.3. tersebut bahwa gambar keluaran dengan ukuran 11kb tidak mengalami perubahan dari sebelum

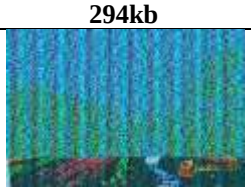
disisipkan, sedangkan gambar keluaran dengan ukuran 254kb mengalami perubahan dari sebelum disisipkan.

Selain itu, pada hasil *stego* juga didapat bahwa terdapat perbedaan ukuran file gambar cover sebelum dan sesudah disisipkan file. Ukuran hasil *stego* rata-rata mengalami pertambahan ukuran file namun tidak signifikan. Misalnya, pada penyisipan file dengan ukuran 11kb, gambar *cover* yang mulanya 301kb menjadi 310kb. Namun pada penyisipan file dengan ukuran 254kb, hasil *stego* mengalami penurunan ukuran file karna pada gambar *cover* dan gambar yang disisipkan menjadi rusak.

4.5.2. Pengujian data menggunakan file text

Tabel 4.4. Pengujian Data Text

GAMBAR *COVER*	FILE YANG DISISIPKAN	HASIL STEGO
 **Cover.bmp 301kb**	**data1.txt 10kb**	 **308kb**
	Data2.txt 20kb	 **307kb**
	Data3.txt 30kb	 **307kb**

 **Cover.bmp 301kb**	**Data4.txt 40kb**	 **305kb**
	Data5.txt 50kb	 **302kb**
	Data6.txt 60kb	 **301kb**
	Data7.txt 70kb	 **300kb**
	Data8.txt 80kb	 **297kb**
	Data9.txt 90kb	 **294kb**
	Data10.txt 100kb	 **294kb**
	Data11.txt 250kb	 **248kb**

Pada tabel 4.4. diatas didapat bahwa, gambar *cover* yang digunakan dalam penyisipan file ukuran 10kb sampai 100kb tidak mengalami perbedaan gambar yang signifikan. Namun, pada penyisipan file dengan ukuran 250kb, gambar *cover* menjadi rusak akibatnya gambar tersebut mengalami perbedaan yang signifikan dari sebelum disisipkan file. Jika dianalisa dari perbedaan ukuran gambar cover sebelum dan sesudah disisipkan file tampak terjadi penurunan ukuran. Hal ini berbeda pada pengujian menggunakan data sisipan gambar. Pada data sisipan *text*, ukuran gambar *cover* menurun dengan naiknya ukuran file text yang disisipkan. Semakin tinggi ukuran file *text* yang disisipkan maka semakin rendah ukuran hasil *stego*.

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan hasil tinjauan teoritis, analisa serta desain sistem aplikasi *steganography* yang telah diuraikan dari bab sebelumnya, maka penulis dapat mengambil kesimpulan :

1. Penggunaan *steganography* dapat bermanfaat dan mencegah kebocoran informasi dari proses penyadapan karna proses penyimpanan data pada *steganography* dengan metode LSB pada citra digital dilakukan dengan mengganti bit bit redudansi yang telah dikonversi menjadi bilangan biner.
2. Teknik pengamanan data *steganography* sangat berguna untuk mengamankan data karena perbedaan antara gambar asli dan gambar stego sangat sulit di bedakan.
3. Ukuran *stage image* dari *steganography* metode LSB rata-rata mengalami pertambahan ukuran file namun tidak signifikan.

5.2. Saran

Berdasarkan hasil penelitian dan pembahasan serta kesimpulan yang penulis kemukanan, terdapat saran yang ingin penulis sampaikan dalam pengembangan aplikasi ini lebih lanjut.

1. Diharapkan selalu mengamankan data-data penting pada media yang aman dan sulit untuk ditemukan.

2. Disarankan menggunakan kualitas gambar terbaik agar media penyimpanan semakin besar dan data yang dapat di amankan juga lebih besar.
3. Disarankan mengenkripsi terlebih dahulu jika data yang diamankan berupa teks, untuk meningkatkan keamanan data.
4. Penulis memberikan saran kepada pembaca yang masih ragu dalam memanfaatkan kemajuan teknologi dalam kehidupan sehari-hari agar segera memanfaatkan fasilitas tersebut untuk mengamankan data penting dan mempermudah segala yang berkaitan.

DAFTAR PUSTAKA

Anonim, E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," Jurnal Techno. Com, vol. 14, no. 2, pp. 329-335, 2014.

Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).

Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11

Bishop, Rosdiana, "Sekuritas Sistem Dengan Kriptografi," in Prosiding Sendi_U 2013, Semarang, 2013.

FACHRI, Barany. Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 2018, 3: 98-102.

Fresly, Faizal Zuli1, Ari Irawan, "Implementasi Kriptografi Dengan Algoritma Blowfish dan Riverst Shamir Adleman (RSA) Untuk Proteksi File," Jurnal Format Volume 6 nomor 2 Tahun 2016.

Gede Angga Pradipta " Penerepan Kombinasi metode Enkripsi Vigenere Cipher Dan Trasposisi Pada Aplikasi Client Server Chatting, " Jurnal Sistem Dan Informatika Vol. 10, Nomor 2, 2016.

Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). Implementasi Augmented Reality Sebagai Media Promosi Penjualan Rumah. In Seminar Nasional Royal (Senar) (Vol. 1, No. 1, pp. 429-434).

Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. Jurnal Teknik dan Informatika, 5(2), 13-19

Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." Int. J. Recent Trends Eng. Res 2.12 (2016): 140-151.

Nandar Pabokory, Indah Fitri Astuti, Awang Harsa Kridalaksana, " Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Jurnal Informatika Mulawarman Vol. 10. Nomor 1, 2015.

Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. Int. J. Secur. Its Appl, 10(8), 173-180.

Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." INTECOMS: Journal of Information Technology and Computer Science 1.1 (2018): 72-77.

Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In Journal of Physics: Conference Series (Vol. 1028, No. 1, p. 012052). IOP Publishing.

Ramadhan, A., & Mohd. Awal Hakimi. (2006). Pemprograman Web Database dengan PHP dan MySQL. Synergy Media.

Ramadhan, M., & Nugroho, N. B. (2009). Desain web dengan php. Jurnal Saintikom, 6(1).

Renddy, Teady Matius, Surya Mulyana, Fresly, " Steganografi Dengan Deret Untuk Mengacak Pola Penempatan Pada Rgb," Jurnal Teknologi Informasi, 2015.

Rhee, C. A. Sari, E. H. Rachmawanto, Y. P. Astuti and L. Umaroh, "Optimasi Penyandian File Kriptografi Shift Cipher," in Prosiding Sendi_U 2013, Semarang, 2013.

Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. Int. J. Sci. Res. Sci. Technol, 3(6), 470-473.

Siahaan, A. P. U., Aryza, S., Nasution, M. D. T. P., Napitupulu, D., Wijaya, R. F., & Arisandi, D. (2018). Effect of matrix size in affecting noise reduction level of filtering.

Siahaan, MD Lesmana, Melva Sari Panjaitan, and Andysah Putera Utama Siahaan. "MikroTik bandwidth management to gain the users prosperity prevalent." Int. J. Eng. Trends Technol 42.5 (2016): 218-222.

Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.

Suriski Sitinjak, Yuli Fauziah, Juwairiah, " Aplikasi Kriptografi File Menggunakan Algoritma Blowfish," Jurnal Informatika Mulawarman Vol. 10. Nomor 1, 2015.

Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 100-109.