IMPLEMENTASI PENGAMANAN *TEXT FILE* PADA *HYBRID SYSTEM* MENGGUNAKAN ALGORITMA VIGENÈRE DAN ALGORITMA *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT (*AMELSBR*)*

(Skripsi)

Oleh
Tryo Romadhoni Pujakusuma

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2018

ABSTRAK

IMPLEMENTASI PENGAMANAN *TEXT FILE* PADA *HYBRID SYSTEM* MENGGUNAKAN ALGORITMA *VIGENÈRE* DAN ALGORITMA *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT(*AMELSBR*)*

Oleh

Tryo Romadhoni Pujakusuma

Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data dan informasi. Masalah yang muncul ketika informasi tersebut bersifat rahasia, terutama bagi suatu perusahaan, institusi dan juga individu yang mempunyai dokumen dan data yang penting, sehingga perlu dijaga keamanan dari data tersebut. Keamanan merupakan hal yang terpenting dalam pengiriman suatu pesan rahasia. Dalam hal ini kriptografi yang berperan menyandikan pesan rahasia kedalam bentuk pesan yang tidak beraturan dan steganografi yang menyembunyikan pesan tidak beraturan tersebut ke dalam media gambar, sehingga menghasilkan keamanan ganda dalam pengiriman pesan rahasia. Dalam penelitian ini peneliti membangun sistem hibrid kriptografi dan steganografi menggunakan *Vigenere* dan AMELSBR berbasis *web* dengan media penampung berupa gambar dengan *format file* (.jpg) sebagai *input (cover),* gambar dengan jenis file (.png) sebagai *output (stegoimage)* serta data yang dapat disisipkan berupa berkas dengan *format file* (.txt). Kesimpulan yang didapat dari penelitian ini adalah Sistem *hybrid* dengan menggabungkan algoritma *Vigenere* dan metode AMELSBR ini dapat digunakan dengan baik untuk menyandikan pesan rahasia serta menyembunyikannya ke dalam media penampung gambar sehingga memperoleh keamanan ganda dalam pengiriman data. Tidak terlihat perbedaan yang signifikan antara *stegoimage* dengan gambar aslinya setelah dilakukan penyisipan. Oleh sebab itu penggunaan metode AMELSBR baik digunakan dalam steganografi. *Stegoimage* dapat tahan terhadap proses manipulasi *brightness* dan *contrast* dengan catatan gambar harus mempunyai nilai warna dominan hitam (rgb(0,0,0)) atau putih (rgb(255,255,255)) dan tidak banyak varian warna, dengan kata lain gambar yang dapat mengembalikan berkas tanpa mengalami pengurangan makna secara berlebihan setelah dilakukannya manipulasi *brightness* dan *contrast* adalah gambar dengan kualitas citra *biner* dan citra *grayscale*.

Kata Kunci: *hybrid*, kriptografi, steganografi, Vigenere, AMELSBR.

ABSTRACT

IMPLEMENTATION OF TEXT FILE SECURITY ON HYBRID SYSTEM USING VIGENÈRE ALGORITHM AND AMELSBR (ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT) ALGORITHM

By

Tryo Romadhoni Pujakusuma

The development of technology and the internet allows everyone to exchange data and information. Problems arise when the information is confidential, especially for a company, institution and also individuals who have important documents and data. Therefore, the security of the data is a must. In this case cryptography plays a role of encrypting secret messages into the form of unreadable messages and steganography that hides the irregular messages into the image media, resulting in double security in the delivery of secret messages. In this research we develop a hybrid system using Vigenere and AMELSBR with cover media in the form of (.jpg) format as input (cover), file type (.png) as output (stegoimage) and data be inserted as a file with text format. The conclusion of this research is that the hybrid system can be used to encrypt the secret message and hide it into the cover media to make it more secure in data transmission. Therefore, the use of AMELSBR method is good used in steganography. Stegoimage can withstand the process of manipulating the brightness and contrast with the image record must have the dominant black color value (rgb (0,0,0)) or white (rgb (255,255,255)) and not many color variants, in other words the image can restore the file without experiencing excessive reduction of meaning after the manipulation of brightness and contrast is an image with binary image quality and grayscale image.

Key word: Hybrid, Cryptography, Steganography, Vigenere, AMELSBR.

IMPLEMENTASI PENGAMANAN *TEXT FILE* PADA *HYBRID SYSTEM* MENGGUNAKAN ALGORITMA VIGENÈRE DAN ALGORITMA *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT (*AMELSBR*)*

Oleh :

TRYO ROMADHONI PUJAKUSUMA

Skripsi

Sebagai Salah Satu Syarat untuk Memperoleh Gelar
SARJANA KOMPUTER

pada

Jurusan Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam

JURUSAN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
2018

Judul Skripsi	:	**IMPLEMENTASI PENGAMANAN *TEXT FILE* PADA *HYBRID SYSTEM* MENGGUNAKAN ALGORITMA VIGENÈRE DAN ALGORITMA *ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT* (AMELSBR)**
Nama Mahasiswa	:	Tryo Romadhoni Pujakusuma
No. Pokok Mahasiswa	:	1117032058
Jurusan	:	Ilmu Komputer
Fakultas	:	Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Prof. Dra. Wamiliana, M.A., Ph.D.
NIP 19631108 198902 2 001

2. Mengetahui
Ketua Jurusan Ilmu Komputer
FMIPA Universitas Lampung

Dr. Ir. Kurnia Muludi, M.S.Sc.
NIP. 19640616 198902 1 001

MENGESAHKAN

1. Tim Penguji

   Ketua : **Prof. Dra. Wamiliana, M.A., Ph.D.** .....

   Penguji 1
   Bukan Pembimbing : **Febi Eka Febriansyah, S.T., M.T.** .....

   Penguji 2
   Bukan Pembimbing : **Dwi Sakethi, S.Si., M.Kom.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Prof. Warsito, S.Si. D.E.A., Ph.D.
NIP 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : **26 Februari 2018**

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul "Implementasi Pengamanan *Text File* Pada *Hybrid System* Menggunakan Algoritma Vigenère Dan Algoritma *Adaptive Minimum Error Least Significant Bit Replacement (*AMELSBR*)*" merupakan karya saya sendiri dan bukan karya orang lain. Semua tulisan yang tertuang di skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila di kemudian hari terbukti skripsi saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi berupa pencabutan gelar yang telah saya terima.

Bandar Lampung, 26 Februari 2018

Tryo Romadhoni Pujakusuma
NPM. 1117032058

RIWAYAT HIDUP

Penulis dilahirkan pada tanggal 18 Maret 1993 di Tanjung Karang, Bandar Lampung, sebagai anak ketiga dari empat bersaudara dari Ayah yang bernama Suhardoyo dan Ibu yang bernama Siti Zainab.

Penulis menyelesaikan pendidikan formal pertama kali di TK Al-Azhar tahun 1999, kemudian melanjutkan pendidikan dasar di SD Al-Azhar 2 dan selesai pada tahun 2005. Pendidikan menengah pertama di SMP Gajah Mada yang diselesaikan pada tahun 2008, kemudian melanjutkan ke pendidikan menengah atas di SMA Negeri 12 Bandar Lampung yang diselesaikan penulis pada tahun 2011.

Pada tahun 2011 penulis terdaftar sebagai mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Selama menjadi mahasiswa beberapa kegiatan yang dilakukan penulis antara lain:

1. Pada bulan Januari 2014 penulis melaksanakan Kuliah Kerja Nyata (KKN) di Desa Labuhan, Kecamatan Pulau Pisang, Kabupaten Pesisi Barat.
2. Pada bulan Februari 2015 penulis melaksanakan kerja praktek di PLN Persero Tanjung Karang.

PERSEMBAHAN

Dengan mengucap puji dan syukur kehadiarat Allah SWT

kupersembahkan karya kecilku ini untuk:

Ayahanda Suhardoyo dan Ibunda Siti Zainab tercinta yang telah memberi dorongan, kasih sayang serta menjadi motivasi terbesarku selama ini

M. Indra Pujakusuma, Ahmad Faizal Pujakusuma dan Rafli Ibrahim Pujakusuma yang selalu memberikan dukungan dan masukan agar menjadi lebih baik lagi

Dosen Pembimbing dan Penguji yang sangat berjasa

dalam membantu dan menyelesaikan karya kecil ini

Serta seluruh sahabat-sahabatku Ilmu Komputer 2011 dan Almamaterku yang kubanggakan Universitas Lampung

MOTO

“Whether You Think You Can, Or You Think You Can’t You’re Right"

(Henry Ford)

“Not Everything That Counts Can Be Counted And Not Everything That’s Counted Truly Counts ”

(Thomas Alfa Edison)

SANWACANA

Alhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT atas berkatrahmat, hidayah, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini.

Skripsi ini disusun sebagai syarat untuk memperoleh gelar Sarjana Komputer di Jurusan Ilmu Komputer Universitas Lampung. Penyelesaian skripsi ini tidak terlepas dari bantuan banyak pihak yang membantu baik secara materi, moril, saran,dan bimbingan. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Kedua orang tua tercinta, Ayah Suhardoyo dan Mamah Siti Zainab, serta Kakak-kakakku M. Indra Pujakusuma dan Ahmad Faizal Pujakusuma serta adikku Rafli Ibrahim Pujakusuma yang selalu memberi dukungan berupa materi, doa, motivasi dan kasih sayang yang tak terhingga.
2. Ibu Prof. Dra. Wamiliana, M.A., Ph.D sebagai pembimbing utama, yang telah membimbing penulis dan memberikan ide, kritik serta saran sehingga penulisan skripsi ini dapat diselesaikan.
3. Bapak Febi Eka Febriansyah, S.T., M.T dan Dwi Sakethi, S.Si., M.Kom. sebagai pembahas, yang telah memberikan masukan yang bermanfaat dalam perbaikan skripsi ini.
4. Bapak Prof. Warsito, S.Si., D.E.A., Ph.D selaku Dekan FMIPA Unila.

5. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc selaku Ketua Jurusan Ilmu Komputer dan Bapak Didik Kurniawan, S.Si., MT selaku Sekretaris Jurusan Ilmu Komputer FMIPA Universitas Lampung.
6. Bapak Dwi Sakethi, S.Si., M.Kom selaku Pembimbing Akademik, serta Bapak dan Ibu Dosen Jurusan Ilmu Komputer yang telah memberikan ilmu dan pengalaman dalam hidup untuk menjadi lebih baik.
7. Brother Ngobeg Amir, Ardye, Rico, Bayu, Bobby, Fathan, Harry, alm. Indra, Faisal, Pandya Panji, Pradana, Rahmat, Rizky, dan Rendra Rinaldi yang telah membantu dan memberikan motivasi dalam pengerjaan skripsi ini.
8. Kawan-kawan seperjuangan Buronan Skripsi: Panji, Basir Galih, Harry Okky, Gamma Adi, Bayu, Rudra dan Ade, dan seluruh keluarga Ilkom 2011
9. Kawan-kawan No Life: Rendra, Firman, Kiki, dan Diska yang memberikan masukan dan semangat dalam pengerjaan skripsi ini
10. Ibu Ade Nora Maela dan Ibu Wiwi yang telah membantu segala urusan administrasi dan Mas Nofal yang telah membukakan MIPA Terpadu dan ruang baca serta menyiapkan ruang seminar.

Penulis menyadari bahwa laporan ini masih jauh dari kata sempurna. Secara pribadi penulis mohon maaf yang sebesar-besarnya atas segala kekurangannya. Besar harapan agar skripsi ini dapat berguna bagi penulis dan semua pembacanya

Bandar Lampung, 26 Februari 2018

Penulis

Tryo Romadhoni Pujakusuma

DAFTAR ISI

Halaman

DAFTAR ISI xiii

DAFTAR GAMBAR xvii

DAFTAR TABEL xx

BAB I PENDAHULUAN 1

1.1 Latar Belakang 1

1.2 Rumusan Masalah 4

1.3 Batasan Masalah..... 4

1.4 Tujuan 5

1.5 Manfaat 5

BAB II TINJAUAN PUSTAKA..... 6

2.1 Kriptografi..... 6

2.1.1 Terminologi..... 7

2.1.2 Tujuan Kriptografi 10

2.2 Vigenere Cipher 11

2.3 Steganografi 14

2.3.1 Kriteria Steganografi..... 16

2.4 Citra Digital..... 16

2.4.1 Jenis File Citra Digital 17
2.4.2 Konsep Citra Warna *(True Color)* 19
2.4.3 Histogram 20
2.5 Teks Sederhana *(Plain Text)* 21
2.6 Metode AMELSBR 22
2.7 *Unified Modeling Language* (UML) 27
2.8 Metode Pengembangan Sistem *Waterfall* 30
BAB III Metode Penelitian 32
3.1 Tempat dan Waktu Penelitian 32
3.2 Perangkat 32
3.3 Metode Penelitian 33
3.4 Metode Pengembangan Sistem 33
3.4.1 Perencanaan Sistem 34
3.4.2 Analisis Kebutuhan 35
3.4.3 Desain 35
3.4.3.1 Diagram Sistem 36
3.4.3.2 Sequence Diagram 43
3.4.3.3 Rancangan Antarmuka 46
3.4.3.4 Testing (Pengujian) 48
BAB IV HASIL DAN PEMBAHASAN 49
4.1 Implementasi 49
4.1.1 Menu Kriptografi 49
4.1.1.1 Proses Enkripsi 50
4.1.1.2 Proses Dekripsi 51

4.1.2 Menu Steganografi 53
4.1.2.1 Proses Penyisipan atau Embedding 53
4.1.2.2 Proses Ekstraksi 55
4.1.3 Menu Bantuan 56
4.1.4 Menu Tentang 57
4.2 Pengujian *(Testing)* 58
4.2.1 Pengujian Enkripsi dan Dekripsi 59
4.2.1.1 Pengujian Enkripsi 59
4.2.1.2 Pengujian Dekripsi 60
4.2.2 Pengujian Terhadap Format *File* 61
4.2.3 Pengujian Terhadap Perubahan *Brightness* dan *Contrast* 63
4.2.3.1 Pengujian Perubahan *Brightness* 69
4.2.3.2 Pengujian Perubahan *Contrast* 80
4.2.4 Pengujian Terhadap Pemotongan Gambar *(Cropping)* 87
4.2.5 Pengujian Pengiriman *Stegoimage* Melalui Sosial Media 103
4.3 Pembahasan 105

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan 111
5.2 Saran 112

DAFTAR PUSTAKA

DAFTAR GAMBAR

Halaman

Gambar 2.1. Kriptografi (Prayudi dan Kuncoro, 2005) 7

Gambar 2.2.Skema Enkripsi dan Dekripsi 8

Gambar 2.3. Blaise de Vigenere 12

Gambar 2.4. Steganografi (Prayudi dan Kuncoro, 2005)..... 15

Gambar 2.5. 4 Tipe Dasar Histogram (Hermawati, 2013) 21

Gambar 2.6. Gambaran Umum Metode AMELSBR (Gan, 2003)..... 24

Gambar 2.7. *Pixel* Tetangga dari *Pixel* P (Lee dan Chen, 1999) 25

Gambar 2.8. Proses MER (Lee dan Chen, 1999) 26

Gambar 2.9. *Use Case* Diagram (Satzinger, 2009) 28

Gambar 2.10. Diagram Aktivitas (Satzinger, 2009) 29

Gambar 2.11. Diagram Sekuensial (Satzinger, 2009)..... 30

Gambar 2.12 *Waterfall* (Satzinger et al, 2010) 31

Gambar 3.1 Tahap Penelitian dan Pengembangan Sistem..... 34

Gambar 3.2 *Use Case* Diagram..... 37

Gambar 3.3 Activity Diagram Pengirim pada Proses Enkripsi..... 39

Gambar 3.4 Activity Diagram Pengirim Proses Penyisipan 40

Gambar 3.5 *Activity* Diagram Penerima Proses Ekstraksi 41

Gambar 3.6 Activity Diagram Penerima Proses Dekripsi 42

Gambar 3.7 *Sequence* Diagram Pengirim Enkripsi..... 43

Gambar 3.8 *Sequence* Diagram Penyisipan(Encode) 44

Gambar 3.9 *Sequence* Diagram *Decode*..... 45

Gambar 3.10 *Sequence* Diagram Dekripsi 45

Gambar 3.11 Tampilan Kriptografi..... 46

Gambar 3.12 Tampilan Steganografi 47

Gambar 3.13 Tampilan Bantuan 47

Gambar 3.14 Tampilan Tentang 47

Gambar 4.1 Menu Kriptografi 50

Gambar 4.2 Proses Enkripsi..... 50

Gambar 4.3 Hasil Enkripsi..... 51

Gambar 4.4 Proses Dekripsi..... 52

Gambar 4.5 Hasil Dekripsi..... 52

Gambar 4.6 Menu Steganografi 53

Gambar 4.7 Proses Penyisipan atau *Embedding* 54

Gambar 4.8 Hasil Penyisipan atau *Stegoimage*..... 54

Gambar 4.9 Notifikasi Minimum *Pixel*..... 54

Gambar 4.10 Proses Ekstraksi..... 55

Gambar 4.11 Menu *Help*..... 57

Gambar 4.12 Menu Tentang 58

Gambar 4.13 Hasil Enkripsi atau *Ciphertext* 60

Gambar 4.14 Hasil Dekripsi atau *Plaintext*..... 61

Gambar 4.15 Notifikasi Format Gambar (.jpg)..... 62

Gambar 4.16 Notifikasi Format Gambar (.png)..... 63

Gambar 4.13 Proses Ekstraksi..... 66

Gambar 4.14 Menu *Help*..... 67

Gambar 4.15 Menu *About*..... 68

Gambar 4.16 Hasil Enkripsi atau *Ciphertext* 70

Gambar 4.17 Hasil Dekripsi atau *Plaintext*..... 71

Gambar 4.18 Notifikasi Format Gambar (.jpg)..... 72

Gambar 4.19 Notifikasi Format Gambar (.png)..... 73

DAFTAR TABEL

Halaman

Tabel 2.1. Vigenere Cipher dengan Angka (Arjana et al, 2012) 12

Tabel 2.2. Vigenere Cipher dengan Huruf 13

Tabel 4.1 8 *File* Gambar (.jpg)..... 64

Tabel 4.2. Pengujian 8 *File* Gambar dengan Berkas *Ciphertext*..... 66

Tabel 4.3 Histogram Pada *File* Citra Gambar..... 67

Tabel 4.4.Manipulasi *Stegoimage* Dengan *Brightnes* pada file png 70

Tabel 4.5 Manipulasi *Stegoimage* Dengan *Brightnes* pada file jpg 75

Tabel 4.6 Manipulasi *Stegoimage* Dengan *Contrast* pada png 81

Tabel 4.7 Manipulasi *Stegoimage* Dengan *Contrast* pada jpg..... 84

Tabel 4.8 Manipulasi *Stegoimage* Dengan Pemotongan Gambar pada png 87

Tabel 4.9 Manipulasi *Stegoimage* Dengan Pemotongan Gambar pada jpg 99

Tabel 4.10 Pengiriman *Stegoimage* png Melalui Sosial Media 104

Tabel 4.11 Pengiriman *Stegoimage* jpg Melalui Sosial Media 104

Tabel 4.12 Ulasan Pengujian Perubahan *Brightness*..... 107

Tabel 4.13 Ulasan Pengujian Perubahan *Contrast*..... 108

Tabel 4.14 Ulasan Pengujian Pemotongan Gambar..... 109

Tabel 4.15 Ulasan Pengujian Pengiriman *Stegoimage* png Melalui
Sosial Media.....110

I. PENDAHULUAN

1. Latar Belakang

Teknologi informasi dan komunikasi telah berkembang pesat, memberikan pengaruh yang besar bagi kehidupan manusia. Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Masalah yang muncul ketika informasi tersebut bersifat rahasia, terutama bagi suatu perusahaan, institusi atau organisasi dan juga individu yang mempunyai dokumen-dokumen rahasia dan data-data yang penting, sehingga, perlu dijaga keamanan dari dokumen-dokumen tersebut agar terhindar dari gangguan orang lain. Salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan tersebut adalah menggunakan teknik kriptografi.

Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi telah ada dan digunakan sejak berabad-abad yang lalu dikenal dengan istilah kriptografi klasik, yang bekerja pada mode karakter alfabet. Salah satu teknik kriptografi klasik

adalah algoritma *Vigenère Cipher* yang merupakan modifikasi dari *Caesar Cipher*.

Kriptografi memiliki dua konsep utama, yaitu enkripsi dan dekripsi. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Sedangkan proses untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*) (Sasongko, 2005).

Teknik menjaga kerahasiaan pesan tidak hanya menggunakan kriptografi. Teknik lain yang dapat digunakan yaitu steganografi. Teknik ini mempunyai cara kerja yang berbeda dengan kriptografi yaitu dengan menyisipkan data di dalam sebuah media. Media yang digunakan untuk menyembunyikan pesan pada umumnya berupa gambar, suara dan lain-lain.

Perbedaan antara teknik steganografi dan teknik kriptografi adalah pesan yang tersembunyi di dalam sebuah media (*cover object)* tidak terlihat secara kasat mata bahwa terdapat data yang telah disembunyikan pada media (*cover object*) tersebut. Dengan teknik steganografi ini dapat menyembunyikan data rahasia serta meningkatkan keamanan dalam proses pengiriman data. Steganogafi memiliki dua proses, yaitu *encoding* dan *decoding*. *Encoding* merupakan proses penyisipan pesan ke dalam media penampung *(covertext)* misalnya citra digital, sedangkan *decoding* adalah proses ekstraksi pesan dari gambar stego *(stegotext)*.

Salah satu teknik steganografi adalah AMELBSR *(Adaptive Minimun Error Least Significant Bit Replacement).* Dalam metode ini penyisipan pesan dilakukan dengan beberapa tahap yaitu *Capacity Evaluation*, *Minimun-Error Replacement* dan *Error Diffusion.* Ketiga tahap tersebut mempunyai fungsi yang berbeda-beda dan saling berhubungan satu dengan yang lainnya. Sifat dari metode AMELSBR ini adalah beradaptasi dengan karakteristik lokal dan media penampung sehingga tidak menimbulkan distorsi yang berlebihan pada citra penampung yang telah disisipkan data digital rahasia (Prayudi dan Kuncoro, 2005). Dalam penelitian ini juga tidak disertakan *stego key* atau kunci rahasia terhadap *stego image* karena *stego key* ini bersifat opsional dan steganografi sudah merupakan teknik keamanan data (Wang et al, 2006).

Wamiliana et al (2015) menggunakan metode AMELSBR dengan *input* data *file* berformat (.txt), *cover image* dengan format (.jpg/jpeg) dan *output stego image* adalah file dengan format (.png).

Kombinasi kriptografi dan steganografi dapat memberikan keamanan pada pesan rahasia. Pesan rahasia dienkripsi lalu disembunyikan dalam citra, dan pesan rahasia dapat diekstraksi dan didekripsi kembali persis sama seperti aslinya. Pesan rahasia terlebih dahulu dienkripsi dengan algoritma *Vigenère Cipher*, kemudian *ciphertext* hasil kriptografi tersebut disembunyikan di dalam media gambar/citra dengan metode steganografi AMELSBR. Implementasi algoritma kriptografi dan metode steganografi dapat lebih meningkatkan keamanan pesan rahasia. Implementasi

penggabungan ini dilakukan pada aplikasi berbasis *web* dipilih karena banyak pengguna yang bekerja dengan komputer/laptop sehingga data atau berkas rahasia yang akan dikirim dapat langsung disembunyikan dan dapat dimunculkan dengan cepat menggunakan satu alat saja. Aplikasi berbasis *web* ini dapat dikembangkan sesuai kebutuhan pengguna. Berdasarkan latar belakang yang telah disebutkan, maka penelitian ini akan mendiskusikan tentang *Implementasi Pengamanan File Text dengan Algoritma* Kriptografi *Vigenère dan Algoritma* Steganografi AMELSBR *(Adaptive Minimum Error Least Significant Bit Replacement).*

1.2. Rumusan Masalah

Rumusan masalah yang akan diselesaikan adalah bagaimana membangun aplikasi yang dapat mengenkripsi *file .txt* sebelum disisipkan ke citra dan mendekripsi *file* tersebut setelah diekstrak dari *file* citra dengan menggunakan metode Vigenère dan membangun aplikasi yang dapat menyisipkan *file .txt* pada citra dan mengekstrak *file* tersebut dengan menggunakan metode AMELSBR

1.3. Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut

1. Algoritma sistem ini hanya dapat mengenkripsi dan mendekripsi *file* yang berupa *file text* berformat *.txt* dan media untuk menyimpan *file text* adalah *file* citra dengan format *.jpg* sebagai *input* dan format *.png* sebagai *output*.

2. Algoritma yang digunakan untuk mengenkripsi dan mendekripsi *file* text adalah algoritma *Vigenère* dan untuk menyisipkan dan mengekstrak *file cirta* digunakan algoritma AMELSBR.
3. Aplikasi dibuat menggunakan bahasa pemrograman PHP.

1.4. Tujuan

Penelitian ini bertujuan untuk

1. Mengaplikasikan algoritma Vigenere dan AMELSBR dalam proses penyisipan.
2. Menguji aplikasi tersebut dengan melakukan perubahan *contrast*, *brightness* dan *cropping* terhadap stegano image untuk melihat sejauh mana aplikasi tersebut dapat digunakan terhadap distorsi.

1.5. Manfaat

Manfaat yang diperoleh dari penelitian ini adalah agar data berupa berkas ataupun *file-file* rahasia aman sampai tujuan. Sehingga, data tidak sampai pada pihak yang tidak bertanggung jawab ataupun digunakan untuk hal-hal kejahatan.

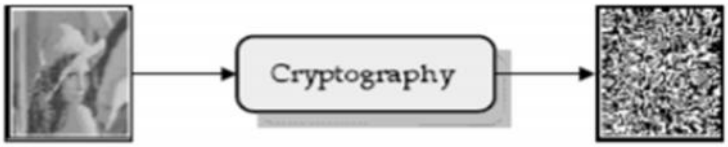
II. TINJAUAN PUSTAKA

2.1. Kriptografi

Kriptografi *(cryptography)* berasal dari Bahasa Yunani *cprytos* artinya "*secret* atau *hidden"* (rahasia), dan *graphein* artinya "*writing"* (tulisan). Jadi, kata kriptografi dapat diartikan sebagai "*secret writing*" (tulisan rahasia). Selain pengertian tersebut, kriptografi juga dapat diartikan sebagai ilmu dan seni untuk menjaga keamanan pesan yang dilakukan oleh *cryptographer*, sedangkan *cryptanalysis* adalah suatu ilmu dan seni membuka pesan yang diacak. Kata "seni" didalam definisi tersebut berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mempunyai cara-cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut berbeda-beda pada setiap pelaku kriptografi. Setiap cara menulis pesan rahasia, pesan tersebut mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan.

Algoritma teknik kriptografi adalah aturan untuk enkripsi dan deskripsi dimana enkripsi adalah proses penyandian *plainteks* atau pesan menjadi *ciphertext* (*enchiphering*) dan deskripsi adalah proses pengembalian

ciphertext menjadi *plaintext* (*deciphering)* (Munir, 2006). Ilustrasi kriptografi disajikan pada Gambar 2.1



Gambar 2.1 Kriptografi (Prayudi dan Kuncoro, 2005).

2.1.1 Terminologi

Dalam Kriptografi terdapat beberapa terminologi atau istilah yang penting untuk diketahui. Istilah tersebut adalah sebagai berikut (Munir, 2006).

1. Pesan, *Plaintext, dan Ciphertext*

   Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan asli biasanya disebut *plaintext.* Agar pesan tidak bisa dimengerti maknanya oleh pihak yang tidak berwewenang, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut *ciphertext.*

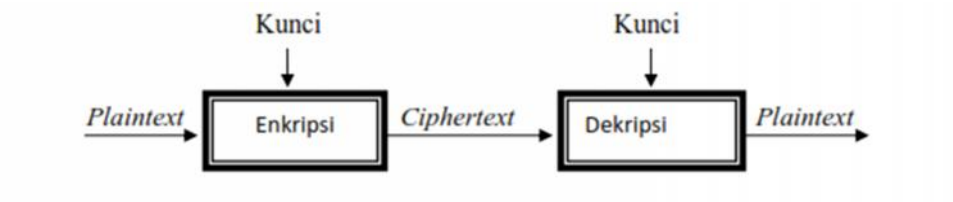
2. Pengirim dan penerima

   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim *(sender)* adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima *(receiver*) adalah entitas yang menerima pesan. Entitas disini dapat berupa orang, mesin (komputer), kartu kredit, dsb.

3. Enkripsi dan dekripsi

   Kriptografi mempunyai dua bagian yang penting, yaitu enkripsi dan dekripsi. Enkripsi adalah proses penyandian dari pesan asli *(plaintext)* menjadi pesan yang tidak dapat diartikan seperti pesan aslinya *(ciphertext)* dengan menggunakan aturan tertentu, sedangkan dekripsi merupakan kebalikannya yaitu mengubah pesan yang sudah disandikan menjadi pesan aslinya. Secara sederhana istilah-istilah tersebut dapat digambarkan sebagai berikut:

4. *Cipher* dan kunci



Gambar 2.2 Skema Enkripsi dan Dekripsi.

Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enCiphering* dan *deCiphering* atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Keamanan algoritma kriptografi sering diukur dari banyaknya kerja *(work)* yang dibutuhkan untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Kunci merupakan parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*. Kunci biasanya berupa *string* atau deretan bilangan.

5. Sistem kriptografi

   Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem kriptografi *(cryptosystem)* terdiri dari algoritma kriptografi, semua *plaintext, ciphertext,* dan kunci.

6. Penyadap *(Eavesdropper)*

   Penyadap adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk memperoleh informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan tujuan untuk memecahkan *ciphertext* menjadi *plaintext.*

7. Kriptanalisis dan kriptologi

   Kriptanalisis *(cryptanalysis)* adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer *(cryptographer)* mentransformasikan *plaintext* menjadi *ciphertext* dengan suatu algoritma dan kunci, maka sebaliknya seorang kriptanalis akan berusaha untuk memecahkan *ciphertext* tersebut untuk menemukan *plaintext* atau kunci. Studi mengenai kriptografi dan kriptanalisis disebut dengan Kriptologi *(cryptology)*.

2.1.2 Tujuan Kriptografi

Menurut Ariyus (2008) kriptografi bertujuan untuk memberi layanan keamanan (aspek-aspek keamanan) sebagai berikut:

1. Kerahasiaan *(confidentiality)* adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi tersebut. Untuk menjaga keamanan informasi dapat dilakukan dengan pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat informasi tidak dapat dipahami.

2. Integritas data *(data integrity)* adalah layanan yang menjamin bahwa pesan masih utuh atau belum pernah dimanipulasi selama pengiriman. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, seperti penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya.

3. Otentikasi (*authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasikan kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain, sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran

komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan.

4. Nir-penyangkalan *(non-repudiation)* adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2. Vigenère Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553. Karena yang memperkenalkan algoritma ini kepada publik adalah Blaise de Vigenère maka algoritma ini dinamakan Vigenère Cipher.

Gambar 2.3 Blaise de Vigènere.

Vigenère Cipher adalah metode menyandikan teks alphabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf-huruf pada kata kunci. *Vigenère Cipher* menggunakan tabel seperti pada tabel 2.1, *Vigenère Cipher* dengan angka dalam melakukan enkripsi (Arjana et al, 2012).

Teknik dari substitusi *Vigenère cipher* bisa dilakukan dengan dua cara:

1. Angka
2. Huruf

Table 2.2 Vigenère Cipher dengan Angka (Arjana et al, 2012)

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13

O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25

Jika ditukar dengan angka, maka kunci dengan huruf “ HARI”

K = (7, 0, 17, 8)

Plaintext nya “ SAYA HARIYANTO “ akan menjadi

P = (18, 0, 24, 0, 7, 0, 17, 8, 24, 0, 13, 19, 14).

S	A	Y	A	H	A	R	I	Y	A	N	T	O
18	0	24	0	7	0	17	8	24	0	13	19	14
7	0	17	8	7	0	17	8	7	0	17	8	7
25	0	15	8	14	0	8	16	5	0	4	1	21

Ciphertext yang dihasilkan:

Ciphertext = (25, 0, 16, 8, 14, 0, 8, 16, 5, 0, 4, 1, 21)

Ciphertext yang dihasilkan dengan huruf menjadi "ZAPIOAIQFAEBV".

Tabel 2.2, *Vigenère Cipher* dengan huruf berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser ke kiri dari baris sebelumnya membentuk ke-26 kemungkinan sandi *Caesar* setiap huruf disediakan dengan menggunakan baris yang berbeda-beda sesuai kunci yang diulang.

Table 2.2 Vigenère Cipher dengan Huruf

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B		B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C		C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D		D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E		E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F		F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G		G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H		H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I		I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J		J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K		K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L		L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M		M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N		N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O		O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P		P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q		Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R		R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S		S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T		T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U		U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V		V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W		W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X		X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y		Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z		Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Plantext: SAYA HARIYANTO

Kunci: HARI

Dari *Plaintext* dengan kata kunci di tabel didapatkan *Ciphertext* sebagai berikut:

Ciphertext: Zapioaiqfaebw

Proses dekripsi, dilakukan dengan mencari huruf *Ciphertext* pada baris *plaintext* dari kata kunci.

Dari proses/penjelasan tabel, maka dapat disimpulkan bahwa rumus dari enkripsi dan dekripsi data *Vigenère Cipher* adalah:

Enkripsi: Ci = (Pi + Ki) mod 26

Dekripsi: Pi = (Ci – Ki) mod 26; untuk Ci > = Ki

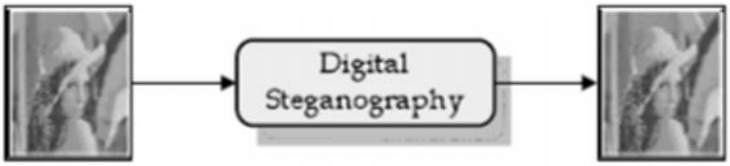
Pi = (Ci+ 26 – Ki) mod 26; untuk Ci < = Ki

2.3. Steganografi

*Steganography (*steganografi*)* merupakan seni untuk menyembunyikan pesan rahasia kedalam pesan lainnya sedemikian rupa sehingga membuat orang lain tidak menyadari adanya sesuatu di dalam pesan tersebut. Kata *Steganography* berasal dari bahasa Yunani, yaitu gabungan dari kata *steganos* (tersembunyi atau terselubung) dan *graphein* (tulisan atau menulis), sehingga makna *Steganography* kurang lebih bisa diartikan sebagai menulis tulisan yang tersembunyi (Sellars, 2006).

Sejalan dengan perkembangan maka konsep awal steganografi diimplementasikan pula dalam dunia komputer, yang kemudian dikenal dengan istilah steganografi digital. Dalam hal ini, steganografi digital memiliki dua properti dasar yaitu media penampung (*cover data* atau *data carrier*) dan data digital yang akan disisipkan (*secret data*), dimana media penampung dan data digital yang akan disisipkan dapat berupa file multimedia (teks/dokumen, citra, audio maupun video). Terdapat dua tahapan umum dalam steganografi digital, yaitu proses *embedding* atau *encoding* (penyisipan) dan proses *extracting* atau *decoding* (pemekaran atau pengungkapan kembali (*reveal*)). Hasil yang didapat setelah proses *embedding* atau *encoding* disebut *stego object* (apabila media penampung

hanya berupa data citra makadisebut s*tego image*) (Prayudi dan Kuncoro, 2005). Ilustrasi steganografi disajikan pada Gambar 2.4.



Gambar 2.4 Steganografi (Prayudi dan Kuncoro, 2005).

Provos dan Honeyman (2003) mendefinisikan steganografi adalah ilmu dan seni menyembunyikan dalam komunikasi. Sistem steganografi ini menyisipkan konten pada suatu media tanpa menimbulkan kecurigaan. Di masa lalu, orang-orang menggunakan tinta transparan untuk menggunakan teknik steganografi. Saat ini, komputer dan jaringan teknologi menyediakan saluran komunikasi yang mudah digunakan untuk steganografi. Pada dasarnya, proses informasi-bersembunyi dalam sistem steganografi dimulai dengan mengidentifikasi *bit* yang berlebihan pada media penutup (dapat dimodifikasi tanpa merusak integritas medium). Proses penyisipan menciptakan media stego dengan mengganti bit-bit yang berlebihan dengan data dari disembunyikan yaitu pesan. Tujuan modern steganografi adalah untuk menjaga data rahasia tidak terdeteksi dengan media penutup *(cover)*. Media tersebut dapat terlihat perbedaannya dengan menemukan distorsi pada media, proses menemukan distorsi ini disebut statistik steganalisis (Provos dan Honeyman, 2003).

2.3.1. Kriteria Steganografi

Kriteria steganografi menurut Munir (2004) adalah :

1. *Fidelity*.

   Mutu media penampung tidak jauh berubah. Setelah penambahan data rahasia, *stego object* dalam kondisi yang masih terlihat baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

2. *Robustness*.

   Data rahasia yang disembunyikan harus tahan *(robust)* terhadap berbagai operasi manipulasi atau *editing* pada media penampung. Apabila pada media penampung dilakukan operasi manipulasi atau *editing*, maka data yang disembunyikan seharusnya tidak rusak atau tetap valid.

3. *Recovery*.

   Data yang disembunyikan harus dapat di ungkapkan kembali *(reveal)*, karena dikaitkan dengan tujuan dari steganografi digital itu sendiri yaitu *data* sewaktu-waktu data rahasia di dalam media penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

2.4. Citra *Digital*

Citra atau gambar dapat didefinisikan sebagai sebuah fungsi yang terdiri dari dua variabel f(x,y), dengan x dan y adalah koordinat bidang datar, dan harga fungsi f disetiap pasangan koordinat (x,y) disebut intensitas atau *level*

keabuan (*grey level)* dari gambar di titik itu. Jika x,y dan f semuanya berhingga (*finite),* dan nilainya diskrit, maka gambarnya disebut citra *digital* (gambar *digital*). Sebuah citra *digital* terdiri dari sejumlah elemen berhingga, dimana masing-masing mempunyai lokasi dan nilai tertentu. Elemen-elemen ini disebut sebagai *picture element, image element, pels* atau *pixels* (Hermawati, 2013).

Purnomo dan Muntasa (2010) menjelaskan bahwa nilai dari intensitas bentuknya atau *level* keabuan adalah diskrit mulai dari 0 sanpai 255. Citra yang ditangkap oleh kamera dan telah dikuantisasi dalam bentuk nilai diskrit disebut dengan citra *digital* (*digital image*) (Purnomo dan Muntasa, 2010).

2.4.1. Jenis *File* Citra *Digital*

Bermacam-macam jenis file citra *digital* yaitu jpg/jpeg, png, gif, tiff dan lain sebagainya mempunyai ciri-ciri, karakteristik, keunggulan dan kelemahan dibagiannya. Disetiap jenis *file digital* terdapat kompresi atau dapat diartikan sebagai proses reduksi jumlah data yang diperlukan untuk menyatakan suatu jumlah informasi yang diberikan (Hermawati, 2013).

Teknik-teknik kompresi data dapat dibagi menjadi 2 yaitu (Widhiartha, 2008)

1. *Lossy compression.*

   Lossy compression menyebabkan adanya perubahan data dibandingkan sebelum dilakukan proses kompresi. Sebagai gantinya *lossy compression* memberikan derajat kompresi lebih

tinggi. Tipe ini cocok untuk kompresi file suara digital dan gambar digital. File suara dan gambar secara alamiah masih bisa digunakan walaupun tidak berada pada kondisi yang sama sebelum dilakukan kompresi.

2. *Lossless compression.*

   Sebaliknya *Lossless Compression* memiliki derajat kompresi yang lebih rendah tetapi dengan akurasi data yang terjaga antara sebelum dan sesudah proses kompresi. Kompresi ini cocok untuk basis data, dokumen atau *spreadsheet*. Pada *lossless compression* ini tidak diijinkan ada bit yang hilang dari data pada proses kompresi.

   Jenis-jenis file citra *digital* (Ichsan, 2011).

   1) JPG/JPEG (*Joint Photographic Experts Group).*

      Joint Photographic Experts Group (JPEG) adalah format gambar yang banyak digunakan untuk menyimpan gambar-gambar dengan ukuran lebih kecil. Beberapa karakteristik gambar JPEG adalah sebagai berikut :

      - Memiliki ekstensi .jpg atau .jpeg.
      - Mampu menayangkan warna dengan kedalaman 24-bit *true color*.
      - Mengkompresi gambar dengan sifat *lossy*.
      - Umumnya digunakan untuk menyimpan gambar-gambar hasil foto.

2) PNG (*Portable Network Graphics).*

PNG (*Portable Network Graphics*) adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut (*lossless compression*). PNG dibaca "ping", namun biasanya dieja apa adanya untuk menghindari kerancuan dengan istilah "ping" pada jaringan komputer. Format PNG ini diperkenalkan untuk menggantikan format penyimpanan citra GIF. Secara umum PNG dipakai untuk Citra Web.

2.4.2. Konsep Citra Warna (*True Color)*

Setiap *pixel* pada citra warna yang merupakan kombinasi dari tiga warna dasar (RGB=*Red Green Blue)*. Setiap warna dasar menggunakan penyimpanan 8 bit = 1 *byte*, yang berarti setiap warna mempunyai gradasi sebanyak 255 warna. Berarti setiap *pixel* mempunyai kombinasi warna sebanyak 16 juta warna lebih. Itulah sebabnya format ini dinamakan *true color* karena mempunyai jumlah warna yang cukup besar sehingga bisa dikatakan hampir mencakup semua warna di alam.

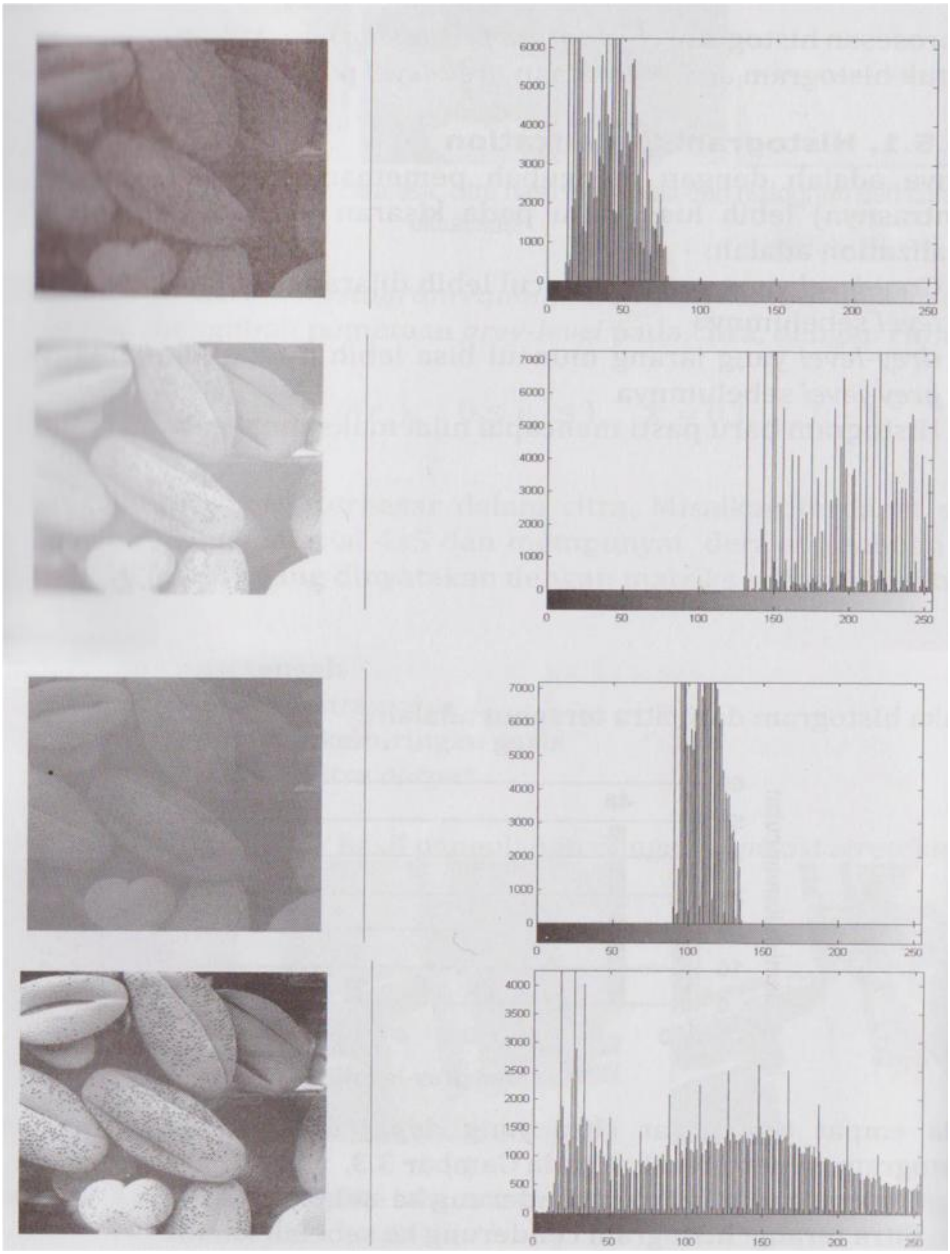
Penyimpanan citra *true color* di dalam memori berbeda dengan citra *grayscale*. Setiap *pixel* dari citra *grayscale* 256 gradasi warna diwakili oleh 1 *byte*. Sedangkan 1 *pixel* citra *true color* diwakili oleh 3 *byte*, dimana masing-masing *byte* mempresentasikan warna merah (*Red*), hijau (*Green*), dan biru (*Blue*) (Widhiartha,2008).

2.4.3 Histogram

Histogram adalah diagram yang menunjukan jumlah kemunculan nilai *grey level (*Kecerahan) pada suatu citra, dimana sumbu-x dari diagram ini menggambarkan nilai *grey level (*Kecerahan) dan sumbu-y mewakili jumlah kemunculan *grey level (*Kecerahan) tertentu. Ada 4 tipe dasar citra yang dapat digambarkan dengan histogram yaitu (Hermawati, 2013) :

- Citra gelap: histogram cenderung ke sebelah kiri
- Citra terang: histogram cenderung ke sebelah kanan
- Citra *low contrast*: histogram mengumpul di suatu tempat
- Citra *high contrast*: histogram merata di semua tempat

Histogram pada citra digital disajikan pada Gambar 2.3.



Gambar 2.5 4 Tipe Dasar Histogram (Hermawati, 2013).

2.5. Teks Sederhana (*Plain Text)*

Format data teks (.txt) merupakan contoh format teks yang paling popular. Saat ini, perangkat lunak yang paling banyak digunakan untuk memanipulasi format data ini adalah Notepad. Format data teks (.txt) adalah format teks yang digunakan untuk menyimpan huruf, angka, karakter

kontrol (tabulasi, pindah baris, dan sebagainya) atau simbol-simbol lain yang biasa digunakan dalam tulisan seperti titik, koma, tanda petik, dan sebagainya. Satu huruf, angka, karakter kontrol atau simbol pada arsip teks memakan tempat satu byte. Berbeda dengan jenis teks terformat (.doc) yang satu huruf saja dapat memakan tempat beberapa byte untuk menyimpan format dari huruf tersebut seperti font, ukuran, tebal atau tidak dan sebagainya.

Kelebihan dari format data teks ini adalah ukuran datanya yang kecil karena tidak adanya fitur untuk memformat tampilan teks (Purnomo dan Zacharias, 2005).

2.6. Metode AMELSBR

Metode ini pertama kali diperkenalkan oleh Yeuan-Kuen Lee dan Ling-Hwei Chen pada tahun 1999 dalam dua makalahnya "*An Adaptive Image Steganographic Model Based on Minimum- Error LSB Replacement*" dan *"High Capacity Image Steganographic Model"* (Lee dan Chen, 1999). Di dalam kedua makalahnya, Lee dan Chen menerapkan citra hitam-putih *(grayscale image)* sebagai media penampung *(cover image)* dan kemudian pada tahun 2003, Mark David Gan pada tahun 2003 mengimplementasikan metode ini dengan citra berwarna *24 bit (true colors image)* sebagai media penampungnya.

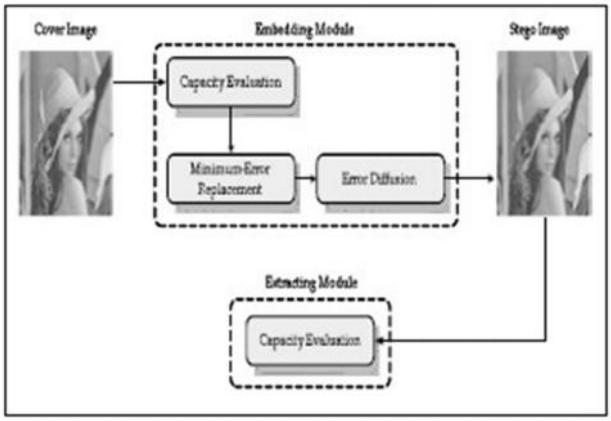
Dari hasil penelitian tersebut ternyata metode ini menawarkan beberapa kelebihan dibandingkan dengan metode LSB, yaitu *bit* data rahasia yang

akan disisipkan lebih banyak (pada metode LSB umumnya hanya 1 *bit*) tanpa menimbulkan banyak perubahan pada media penampung (dalam hal ini adalah data citra). Dengan metode ini, setiap *pixel* memiliki kapasitas penyembunyian yang berbeda-beda tergantung dari nilai toleransi *pixel* tersebut terhadap proses modifikasi atau penyisipan. Suatu *pixel* pada data citra bisa dikatakan dapat ditoleransi apabila dilakukan proses modifikasi (penyisipan) dengan skala yang tinggi terhadap nilainya adalah memungkinkan tanpa merubah tampak asli dari data citra tersebut, atau dengan kata lain area yang halus dan solid pada suatu data citra memiliki kadar toleransi yang rendah *(less tolerant)* terhadap proses modifikasi dibandingkan dengan area yang memiliki tekstur yang kompleks (Gan, 2003).

Metode *AMELSBR* yang diterapkan pada citra berwarna (*jpg/jpeg 24-bit*) memiliki beberapa langkah atau tahapan utama untuk melakukan proses penyisipan, antara lain *Capacity Evaluation, Minimum Error Replacement* dan *Error Diffusion* (Gan, 2003). Untuk proses pengungkapan, tahapan yang dilakukan yaitu *Capacity Evaluation* (Lee dan Chen, 1999).

Sebelum dilakukan proses penyisipan, maka langkah pertama yang harus dilakukan adalah mengevaluasi kapasitas penyisipan *(capacity evaluation)* dan mencari nilai *color variation*. Kemudian setelah mendapatkan nilai *color variation,* nilai tersebut diproses kembali untuk mendapatkan kapasitas penyisipan sejumlah *K-bit*. Setelah itu, untuk beradaptasi dengan karakteristik lokal *pixel,* maka sejumlah *K-bit* tersebut ditangani dengan

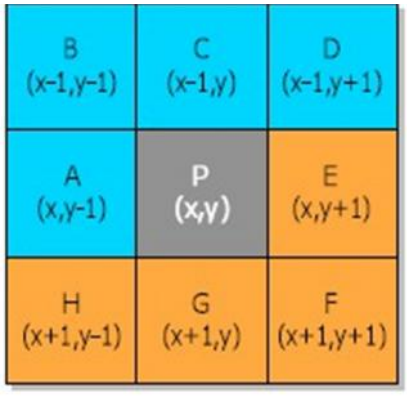
proses evaluasi kapasitas (*capacity evaluation*). Proses selanjutnya adalah mencari *MER*, dimana proses ini akan menentukan apakah *bit* ke *K+1* akan dilakukan perubahan atau tidak, dan yang akan menentukan itu adalah berdasarkan pada nilai *embedding error (Er)*. Proses tersebut disajikan pada Gambar 2.4.



Gambar 2.6 Gambaran Umum Metode AMELSBR (Gan, 2003).

Proses penyisipan *(embedding)* di dalam metode AMELSBR, prosesnya tidak sama dengan metode LSB. Apabila proses penyisipan di dalam metode LSB dilakukan langsung per *pixel* pada *byte*-nya, dimana 1 *bit* terakhir (LSB) per *byte*-nya diganti dengan 1 *bit* data rahasia yang akan disisipkan, tetapi tidak dengan metode AMELSBR. Di dalam metode ini, citra penampung *(cover image)* akan dibagi dulu menjadi beberapa blok. Setiap blok akan berukuran 3 x 3 *pixel* atau sama dengan 9 *pixel* (Curran dan Bailey, 2004).

Ketiga tahapan utama akan diterapkan per bloknya atau per operasi penyisipannya, dimana *bit-bit* data rahasia hanya akan disisipkan pada salah satu komponen warna di *pixel P*, dan disajikan pada Gambar 2.5.



Gambar 2.7 *Pixel* Tetangga dari *Pixel* P (Lee dan Chen, 1999).

Capacity evaluation, merupakan tahap pertama dan yang paling krusial dari metode penyisipan AMELSBR. Tahap ini mengacu pada karakterisitik *human visual system* (HVS) yang tidak sensitif terhadap *noise* dan perubahan warna yang terdapat di dalam citra (Lee dan Chen, 1999). Langkah pertama yang akan dilakukan pada evaluasi kapasitas adalah mencari nilai *color variation (V)* atau variasi warna yang melibatkan *pixel A, B, C* dan *D*. Adapun rumus dari *V* adalah sebagai berikut (Gan, 2003)

$$V = round\{(|C - A| + |A - B| + |B - C| + |C - D|)/4\}$$

dimana :

V = variasi warna *(color variation)*

Round = fungsi matematika untuk pembulatan

Rumus di atas akan menghasilkan ketentuan toleransi modifikasi yang akurat di setiap *pixel P*. Langkah ke-dua adalah mencari kapasitas penyisipan *(K)* pada *pixel P* dan dapat diterapkan rumus sebagai berikut (Gan, 2003)

$$K = round\,(|log2\,V|)$$

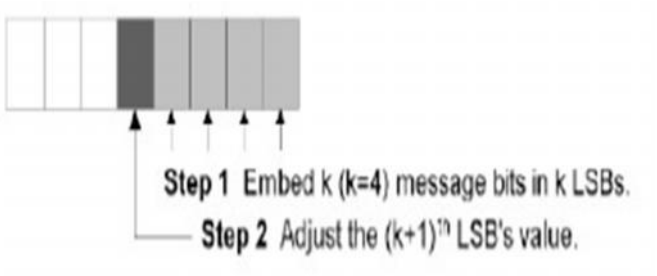
dimana :

K = kapasitas penyisipan pada *pixel P* dalam *bit*

V = variasi warna

Round = fungsi matematika untuk pembulatan

Tahap selanjutnya adalah mencari *Minimum-Error Replacement* (MER). Tahap ini berfungsi untuk meminimalkan terjadinya perubahan *pixel* pada citra penampung akibat dari proses penyisipan. Proses MER dilakukan dengan mengubah nilai *bit* ke *K+1* pada *pixel P*. Perubahan ini akan terjadi pada salah satu dari ke-tiga komponen warna (R, G atau B) yang terpilih (Lee dan Chen, 1999). Proses ini disajikan pada Gambar 2.6.



Gambar 2.8 Proses MER (Lee dan Chen, 1999).

Bila pada langkah sebelumnya (evaluasi kapasitas) didapat *K* = 4, maka *bit* yang ke-lima akan diubah nilainya, misal nilai awal adalah 1, maka akan diubah menjadi 0, begitu juga sebaliknya. Namun demikian pengubahan *bit* ke *K+1* belum tentu dilakukan, karena pada tahap MER juga dilakukan proses pengecekan nilai *embedding error*. *Embedding error (Er)* adalah selisih nilai (dalam desimal) pada komponen warna yang terpilih di *pixel P*, sebelum (original) dan sesudah dilakukan proses penyisipan, atau dengan rumus seperti di bawah ini

$$Er = Abs\left[P(x,y) - P'(x,y)\right]$$

dimana :

Abs = Nilai absolute
Er = Nilai *embedding error*
P(x,y) = *Pixel P* asli
P'(x,y) = *Pixel P* yang telah dimodifikasi

Pengubahan pada *bit* ke *K+1* akan dilakukan apabila nilai *embedding error* memenuhi syarat pada saat pengecekan, uraiannya bisa dijelaskan sebagai berikut. Asumsi *P(x,y)* adalah *pixel P* original, *P'(x,y)* adalah *pixel P* yang telah disisipkan sejumlah *K-bit* tanpa mengubah *bit* ke *K+1* dan *P"(x,y)* adalah *pixel P* yang telah disisipkan sejumlah *K-bit* sekaligus mengubah *bit* ke *K+1*. *Minimum error* yang dapat terjadi di *pixel P* haruslah *P'(x,y)* atau *P"(x,y)* (Lee dan Chen, 1999).

Kemudian proses pengecekan nilai *embedding error* dilakukan lewat rumus sebagai berikut

$$Er1 = Abs\,[P(x,y) - P'(x,y)]$$

$$Er2 = Abs\,[P(x,y) - P''(x,y)]$$

Apabila *Er1 < Er2*, maka *P'(x,y)* yang akan menggantikan *P(x,y)*. Jika sebaliknya maka *P"(x,y)* yang akan menggantikan *P(x,y)* (Lee dan Chen, 1999).

2.7. *Unified Modeling Language* (UML)

Unified Modeling Language (UML) adalah salah satu alat bantu yang sangat handal di dunia pengembangan sistem berorientasi objek. Hal ini disebabkan karena UML menyediakan Bahasa pemodelan visual yang memungkinkan bagi pengembang sistem untuk membuat cetak biru atas visi mereka dalam bentuk baku, mudah dimengerti serta dilengkapi dengan mekanisme yang efektif untuk berbagi (*sharing)* dan mengkomunikasikan rancangan mereka dengan yang lain. UML adalah sistem notasi yang sudah dibakukan di dunia pengembangan sistem, hasil kerja bersama dari Grady Booch, James

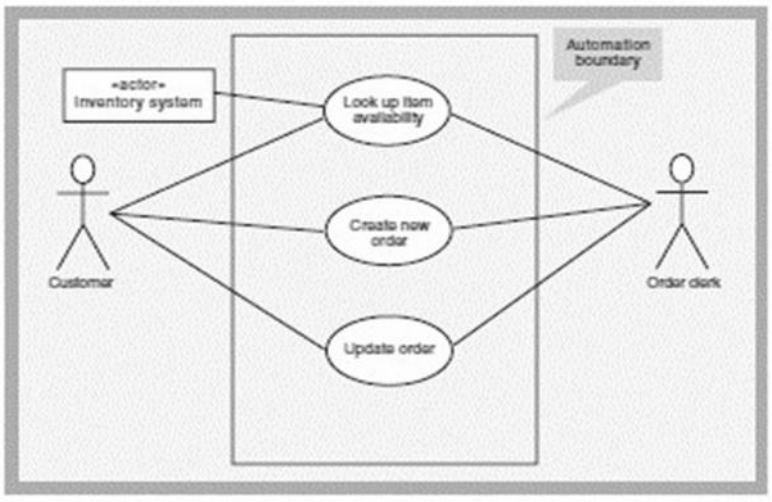
Rumbaugh dan Ivar Jacob-son. Dengan UML dapat diceritakan apa yang seharusnya dilakukan oleh suatu sistem bukan bagaimana yang seharusnya dilakukan oleh suatu sistem (Munawar, 2005).

Unified Modeling Language (UML) dideskripsikan oleh beberapa diagram yaitu :

1. *Use case* diagram.

   Diagram *use case* menyajikan interaksi antara *use case* dan actor, dimana actor berupa orang, peralatan, atau sistem lain yang berinteraksi dengan sistem yang sedang dibangun. *Use case* menggambarkan fungsionalitas sistem atau persyaratan-persyaratan yang harus dipenuhi sistem dari pandangan pemakai (Sholiq, 2006).

   Berikut contoh diagram *use case* yang disajikan pada Gambar 2.9.

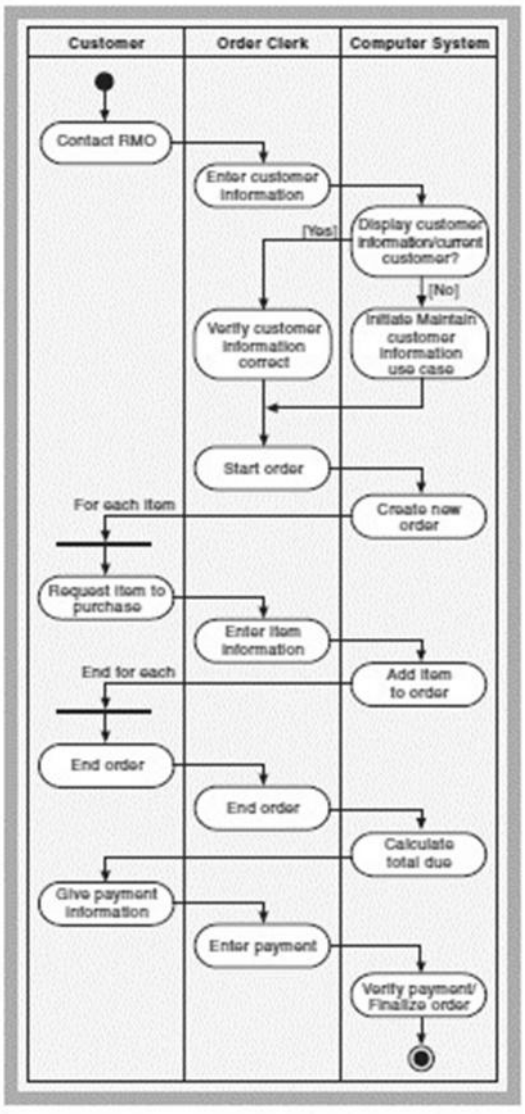


Gambar 2.9 *Use Case* Diagram (Satzinger et al, 2010).

2. Diagram aktivitas.

   Diagram aktivitas atau *Activity Diagram* menggambarkan aliran fungsionalitas sistem. Pada tahap pemodelan bisnis, diagram aktivitas dapat digunakan untuk menunjukkan aliran kerja bisnis (*business work*

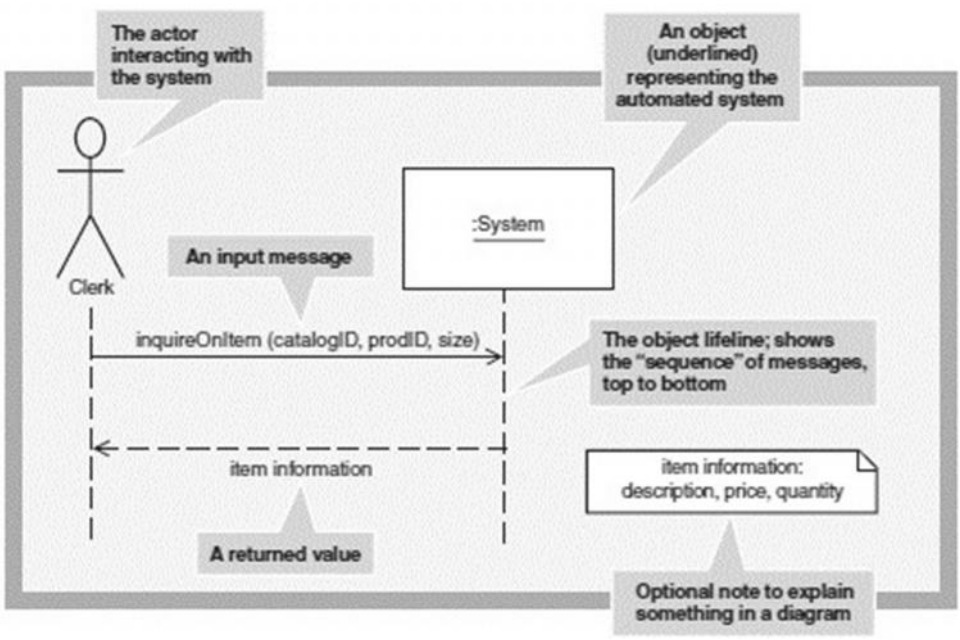
flow serta dapat digunakan untuk menggambarkan aliran kejadian (*flow of events)* dalam *use case*. Aktivitas dalam diagram dipresentasikan dengan bentuk bujur sangkar bersudut tidak lancip, yang didalamnya berisi langkah-langkah apa saja yang terjadi dalam aliran kerja. Ada keadaan mulai (*start state)* yang menunjukkan dimulainya aliran kerja, dan keadaan selesai (*end state)* yang menunjukkan akhir diagram, dan titik keputusan dipresentasikan dengan *diamond* (Sholiq, 2006). Contoh diagram aktivitas disajikan pada Gambar 2.10.



Gambar 2.10 Diagram Aktivitas (Satzinger, 2009).

3. Diagram sekuensial.

   Diagram sekuensial atau *sequence diagram* digunakan untuk menunjukkan aliran fungsionalitas dalam *use* case. Misalkan, pada *use case* "menarik uang" mempunyai beberapa kemungkinan, seperti penarikan uang secara normal, percobaan penarikan uang tanpa kecukupan ketersediaan dana, penarikan dengan penggunaan PIN yang salah, dan lainnya (Sholiq, 2006). Contoh diagram sekuensial disajikan pada Gambar 2.11.

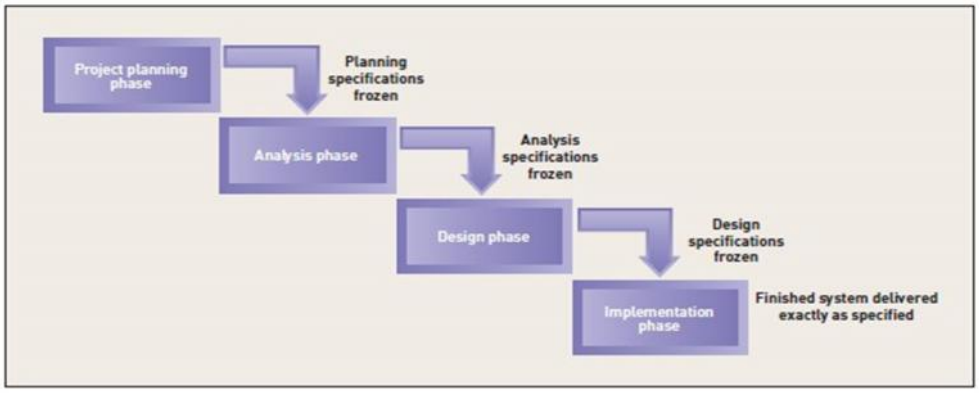


Gambar 2.11 Diagram Sekuensial (Satzinger, 2009).

2.8 Metode Pengembangan Sistem *Waterfall*

Metode pengembangan sistem *waterfall* adalah pendekatan SDLC yang penyelesaian proyeknya diselesaikan dengan tahapan-tahapan yang berurutan. Tahap-tahap pada metode *waterfall* adalah perencanaan sistem, analisis kebutuhan, desain dan implementasi (Satzinger et al, 2010).

Tahapan-tahapan dalam metode pengembangan sistem *Waterfall* disajikan pada Gambar 2.12.



Gambar 2.12 *Waterfall* (Satzinger et al, 2010).

BAB III
METODE PENELITIAN

3.1 Tempat dan Waktu Penelitian

Peneliti melakukan penelitian di Jurusan Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Lampung. Waktu penelitian dilakukan pada semester Ganjil tahun ajaran 2015-2016.

3.2 Perangkat

Perangkat keras yang digunakan pada penelitian implementasi aplikasi ini adalah satu unit laptop dengan spesifikasi sebagai berikut :

- Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz (8 CPUs).
- Memory: 4096MB RAM.
- DirectX Version: DirectX 11.
- Card name: Intel(R) HD Graphics Family 4000.
- Display Memory: 1696 MB.

Perangkat lunak yang digunakan peneliti adalah sebagai berikut :

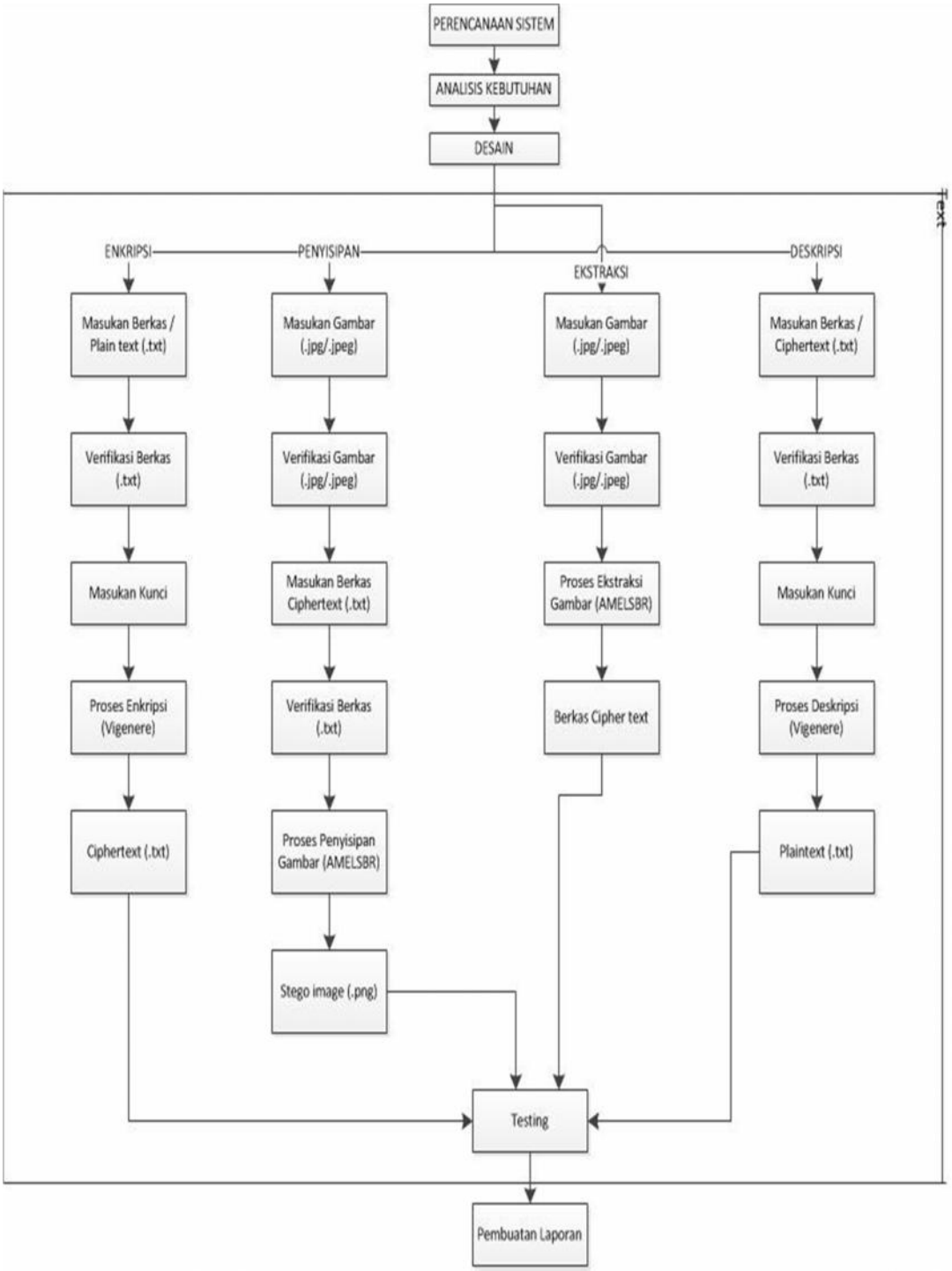
- Windows 7 Ultimate.
- Adobe Photoshop CS5.
- Notepad++ Versi 6.3.0
- XAMPP 1.0.0
- Google Chrome(Browser) Versi 41.0.2272.118

3.3 Metode Penelitian

Metode penelitian yang dilakukan adalah studi literatur. Dengan membaca buku-buku dan jurnal-jurnal yang berkaitan dengan teknik steganografi dan pengolahan citra. Tujuan metode literatur adalah untuk memperoleh sumber referensi sehingga memudahkan dalam penelitian ini.

3.4 Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan adalah metode *Waterfall.* Tahap-tahap pada metode *Waterfall* adalah perencanaan sistem, analisis kebutuhan, desain dan implementasi. Tahap penelitian dan pengembangan sistem disajikan pada Gambar 3.1.



Gambar 3.1 Tahap Penelitian dan Pengembangan Sistem.

3.4.1 Perencanaan Sistem

Tahap awal yaitu pendefinisian masalah yang akan diselesaikan dari sistem yang akan dibangun yaitu bagaimana mengirimkan berkas rahasia

dengan aman tanpa terlihat mencurigakan bagi orang lain yang tidak berkepentingan dengan berkas tersebut. Dari masalah tersebut maka akan dibangun suatu sistem penyisipan berkas yang sudah dienkripsi dengan metode Vigenere kemudian disisipkan ke media gambar sebagai *cover* atau disebut teknik steganografi dengan metode AMELSBR.

3.4.2 Analisis Kebutuhan

Terdapat analisis kebutuhan yang digunakan dalam pengembangan sistem ini yaitu berupa perangkat keras laptop berserta spesifikasi sebagai berikut : Processor: Intel(R) Core(TM) i7-3610QM CPU @ 2.30GHz (8 CPUs), memory: 4096MB RAM, directX Version: DirectX 11, card name: Intel(R) HD Graphics Family 4000 dan display, memory: 1696 MB serta perangkat lunak atau software yaiutu Windows 7 Ultimate, Adobe Photosop CS5, Notepad++ versi 6.3.0, XAMPP versi 1.0.0, Google Chrome (browser) very 41.0.2272.118.

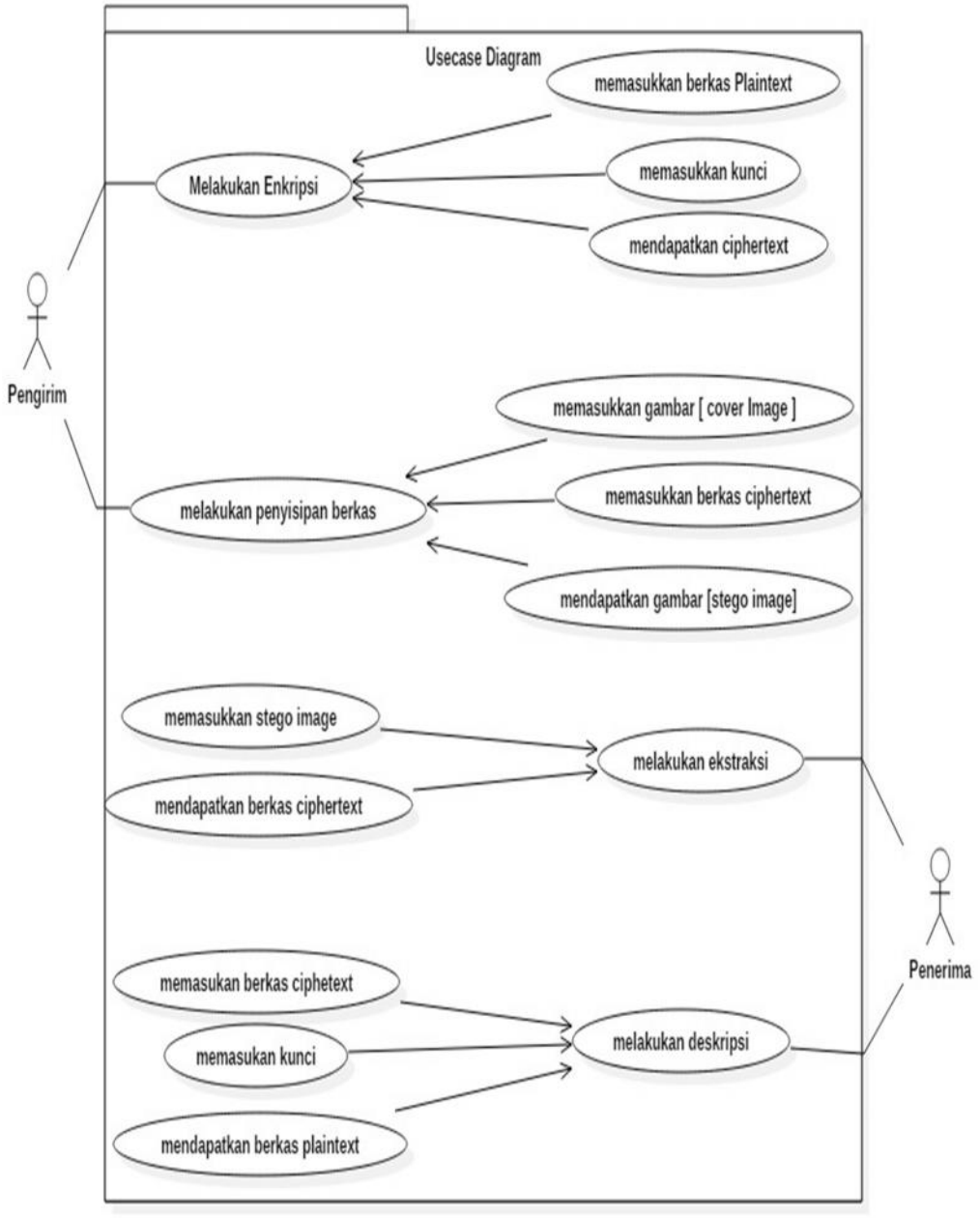
3.4.3 Desain

Proses desain yaitu proses alur kerja sistem, tahap-tahap pengerjaan sistem serta tahap-tahap berjalannya sistem dengan baik. Berikut adalah penjabaran dari tahap-tahap tersebut disajikan dalam bentuk diagram serta rancangan antarmuka sistem.

3.4.3.1 Diagram Sistem

1. *Use Case* Diagram.

   Use Case diagram berikut ini menjelaskan bagaimana pengguna menggunakan sistem. Pengguna yang terdapat di dalam sistem teknik steganografi ini adalah pengirim dan penerima. Pada bagian pengirim dilakukan 6 interaksi yaitu memasukkan berkas berupa *plaintext*, memasukkan password/kunci, mendapatkan berkas *Ciphertext*, kemudian memasukkan gambar (*cover image*), memasukkan berkas *Ciphertext*, dan mendapatkan gambar (stego image). Sedangkan di bagian penerima dilakukan 5 interaksi yaitu memasukkan gambar (stego image), mendapatkan berkas *ciphertext*, memasukkan berkas *ciphertext*, memasukkan password/kunci, dan mendapatkan berkas *plaintext*. *Use Case* diagram disajikan pada Gambar 3.2.



Gambar 3.2 *Use Case* Diagram.

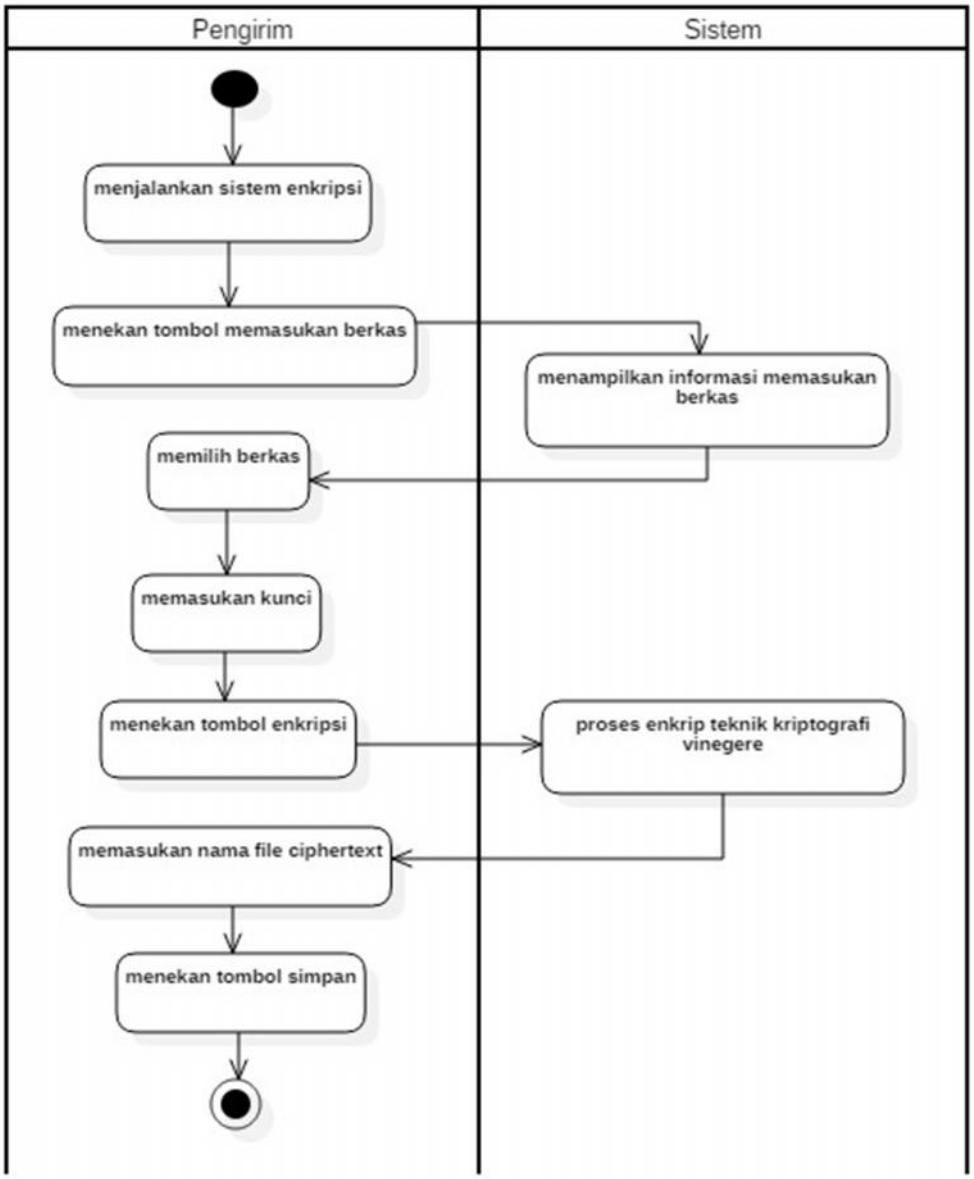
2.*Activity* Diagram

Activity diagram digunakan untuk menggambarkan aliran kerja (*workflow)* dari kejadian *use case* sistem. Gambar 3.3, Gambar 3.4 , Gambar 3.5 dan Gambar 3.6 adalah diagram aktivitas yang

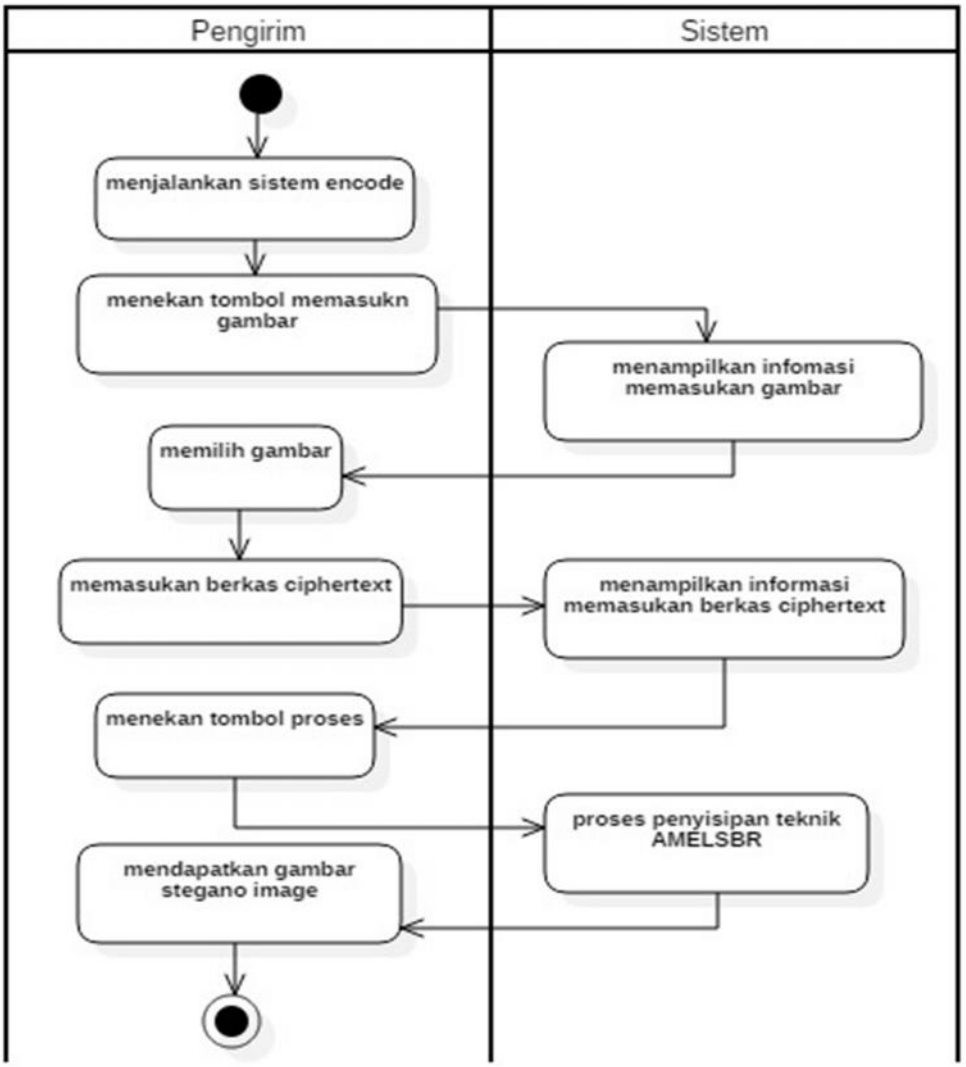
berhubungan dengan aliran kejadian untuk *use case* sistem teknik Kriptografi dengan metode Vigenère Cipher dan teknik steganografi dengan metode *AMELSBR (Adaptive Minimun Error Least Significant Bit Replacement)*. *Activity* diagram pada sistem ini terbagi atas 4 bagian yaitu 2 *activity* diagram untuk pengirim dan 2 *activity* diagram untuk penerima.

a. *Activity* Diagram Pengguna Sebagai Pengirim

Pada *activity diagram* pengirim dimulai dengan menjalankan sistem kemudian pengirim memasukkan berkas *plaintext* sedangkan sistem menampilkan infromasi memasukkan gambar sebagai media penampung sedangkan sistem menampilkan informasi untuk memasukkan gambar. Begitu juga dengan proses pemasukan berkas yang dimulai dengan memasukkan berkas dan sistem menampilkan informasi memasukkan berkas serta setelah semua proses selesai maka sistem memproses gambar dan berkas tadi dengan teknik steganografi menggunakan metode AMELSBR. Terakhir pengguna mendapatkan gambar (*stego image)*. Proses ini disajikan pada Gambar 3.3 dan Gambar 3.4.



Gambar 3.3 *Activity* Diagram Pengirim pada Proses Enkripsi.

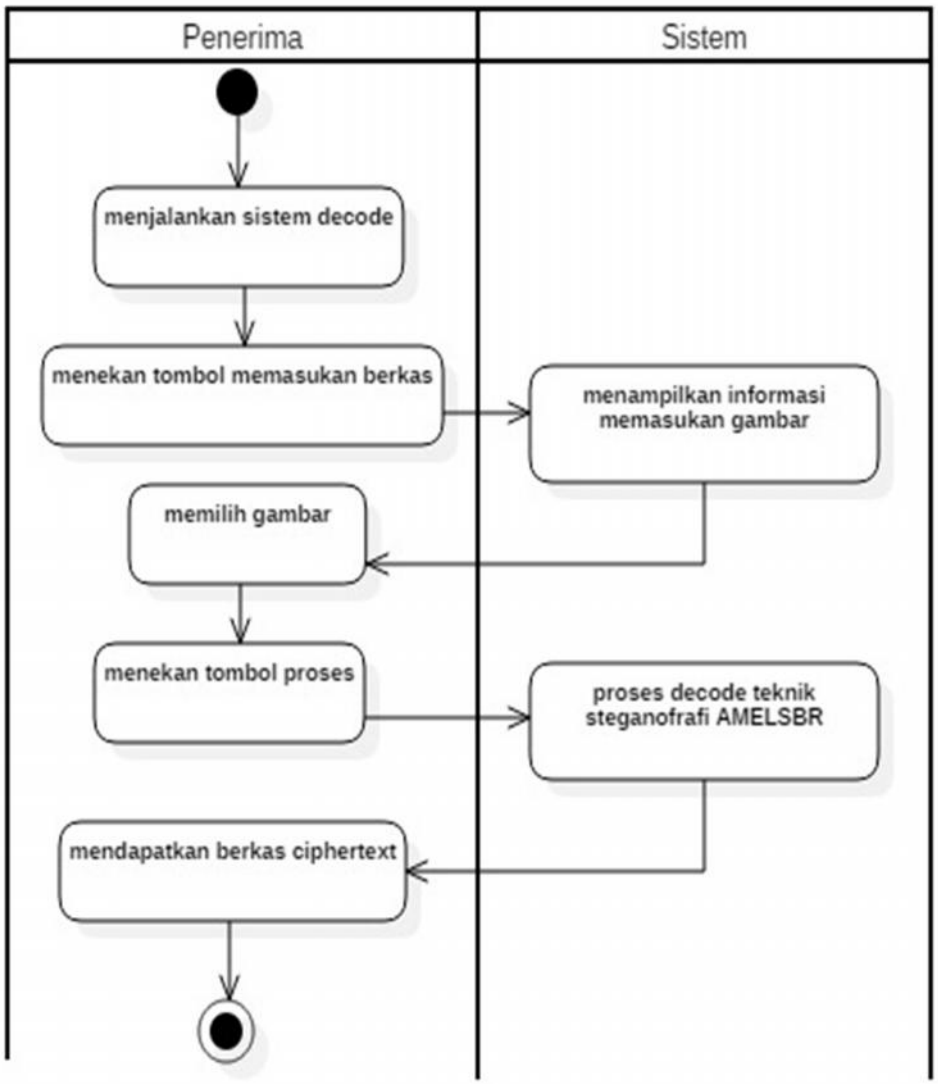


Gambar 3.4 *Activity* Diagram Pengirim Proses Penyisipan.

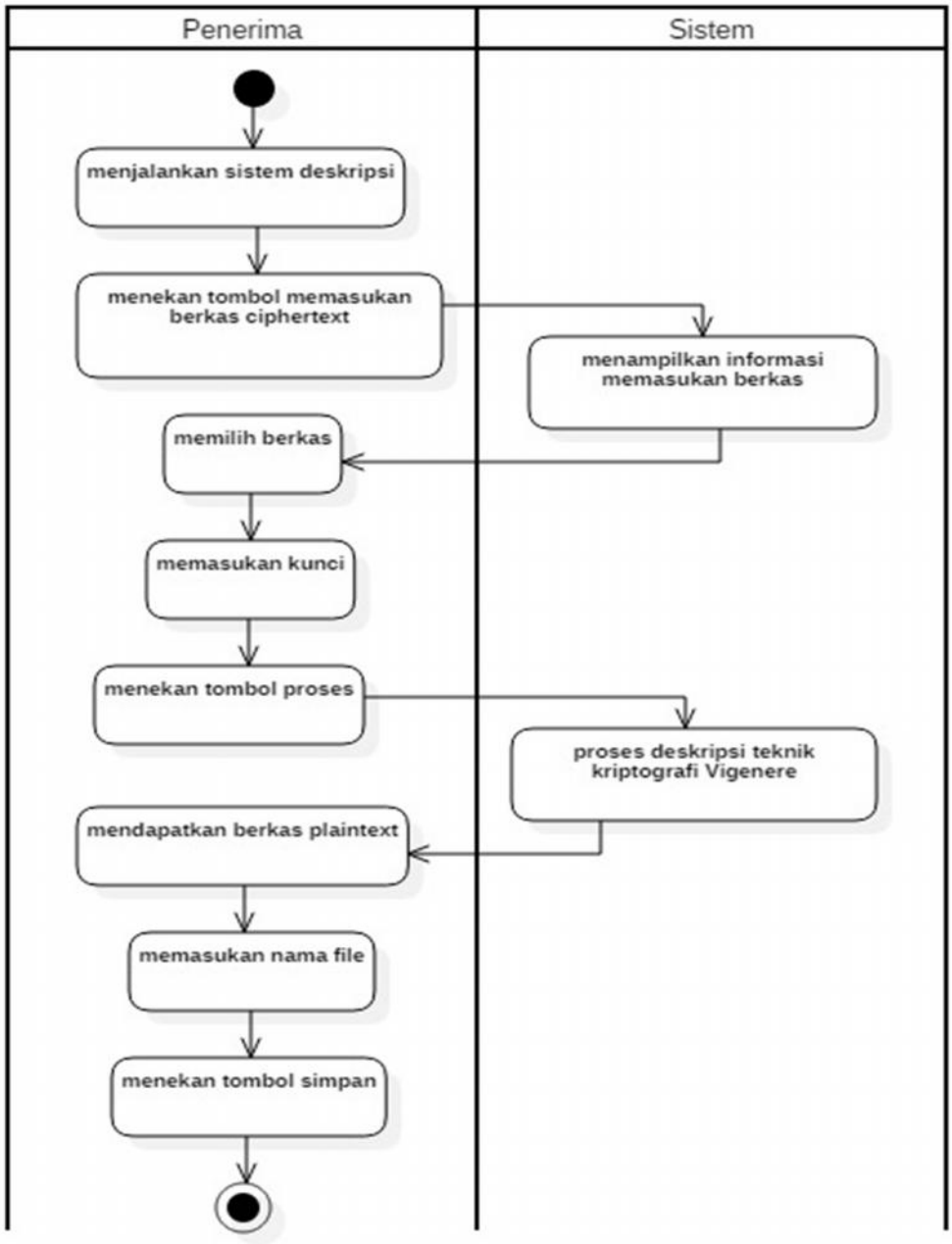
b. *Activity* Diagram Pengguna sebagai Penerima

Pada *activity diagram* penerima dimulai dengan menjalankan sistem kemudian memasukkan gambar (*stego image)* ke dalam sistem dengan sistem menampilkan informasi untuk memasukkan gambar. Proses selanjutnya yaitu proses ekstraksi dari gambar tersebut dengan teknik steganografi menggunakan metode AMELSBR, dan mendapatkan file *ciphertext* dari hasil ekstraksi. Kemudian jalankan

sistem deskripsi dengan memasukkan *Ciphertext* ke dalam sistem, masukkan kunci, dan proses selanjutnya yaitu proses deskripsi dari *ciphertext* tersebut dengan teknik kriptografi Vigenere dan mendapatkan file *Plaintext* sebagai hasil Deskripsi. Proses ini disajikan pada Gambar 3.5 dan Gambar 3.6.



Gambar 3.5 *Activity* Diagram Penerima Proses Ekstraksi.

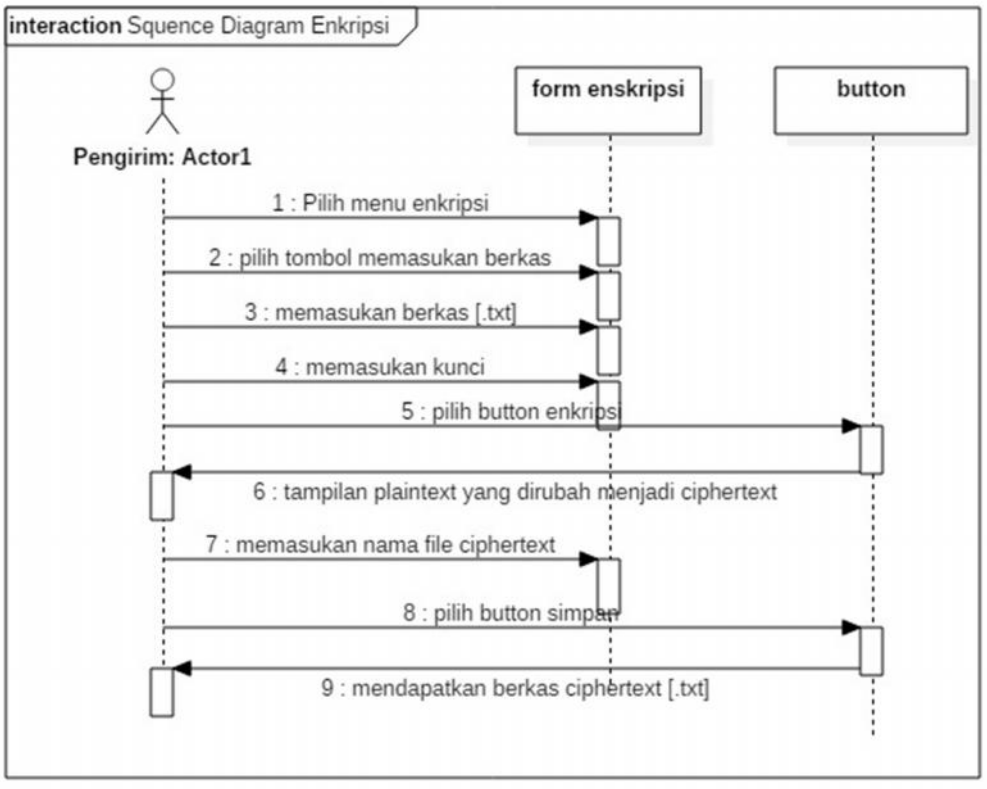


Gambar 3.6 *Activity* Diagram Penerima Proses Deksripsi.

3.4.3.2 Sequence Diagram.

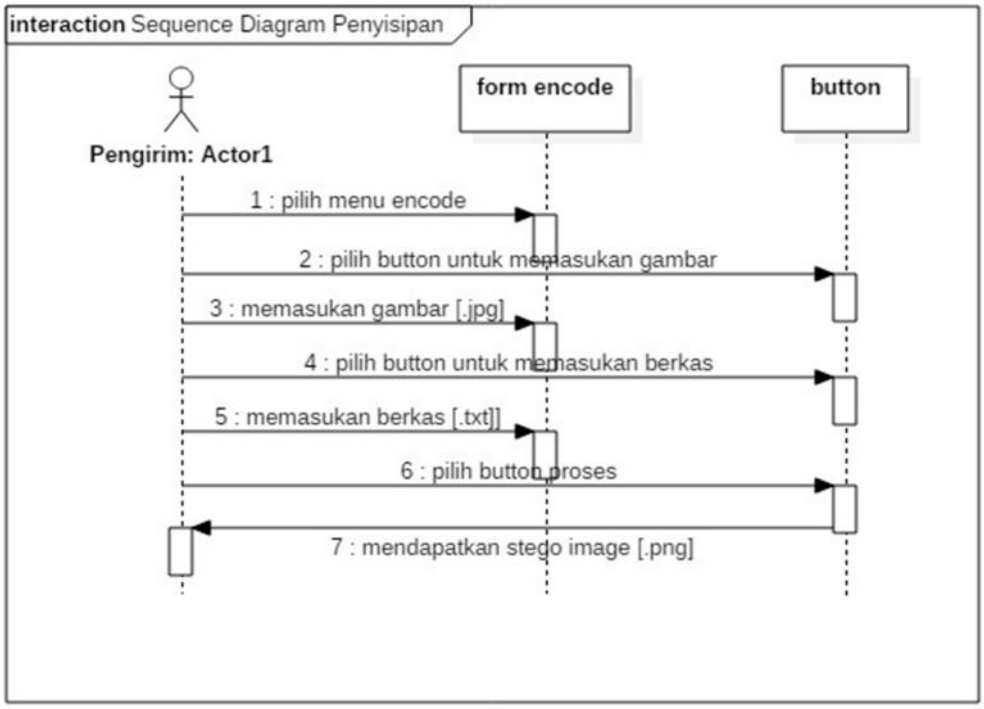
Sequence diagram digunakan untuk menunjukkan aliran fungsionalitas dalam *use case.* Pada sistem ini terdapat 4 bagian *sequence* diagram yaitu diagram untuk enkripsi dan diagram untuk decode, diagram untuk decode, dan diagram untuk deskripsi, sesuai dengan *use case* diagram yang telah digambarkan. *Sequence* diagram sistem disajikan pada Gambar 3.7, Gambar 3.8, Gambar 3.9, dan Gambar 3.10

1. Sequence Diagram Enkripsi dan Sequence Diagram Penyisipan (Encode)



Gambar 3.7 Sequence Diagram Pengirim Enkripsi.

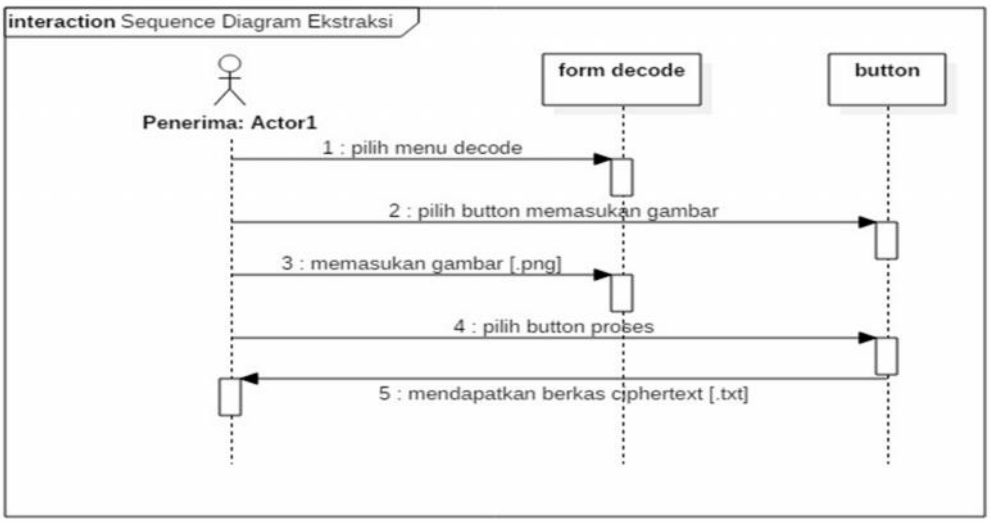
Dari Gambar 3.7 dijelaskan bahwa terdapat 13 proses memasukkan berkas *plaintext* yang akan diubah, memasukkan kunci sebagai kunci untuk membuka file yang telah diubah, menulis nama file *Ciphertext*, setelah terpenuhi maka proses enkripsi dilakukan proses di lanjutkan pada Gambar 3.8.



Gambar 3.8. Sequence Diagram Penyisipan(Encode).

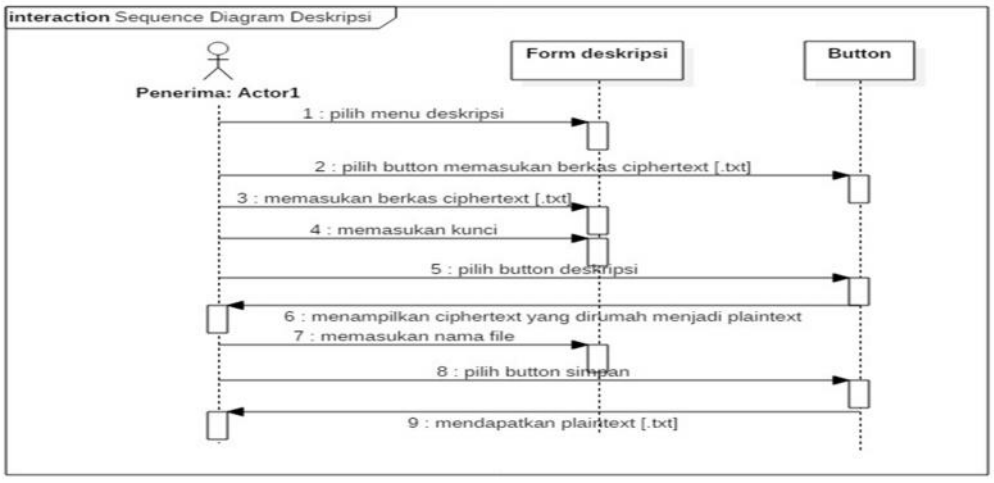
Pada proses ini memasukkan gambar sebagai media penampung dan memasukkan berkas *Ciphertext* yang akan disisipkan. Pada sistem terdapat verifikasi berkas jenis (.txt) dan verifikasi gambar Jenis file (.jpg/jpeg). Setelah semua terpenuhi maka proses penyisipan dilakukan sehingga akhirnya didapatkan gambar *stegoimage*.

d. *Sequence* Diagram Ekstraksi(Decode) dan Diagram Deskripsi.



Gambar 3.9 Sequence Diagram Decode.

Dari Gambar 3.9 dijelaskan bahwa terdapat proses pemasukan gambar (*stego image*) ke dalam sistem kemudian dilakukan verifikasi gambar berjenis *file* (.png). Selanjutnya dilakukan proses ekstraksi gambar dan pada akhirnya diterima kembali berkas yang telah disisipi sebelumnya yaitu *ciphertext*. Kemudian dilanjutkan pada proses Gambar 3.10.



Gambar 3.10 Sequence Diagram Deskripsi.

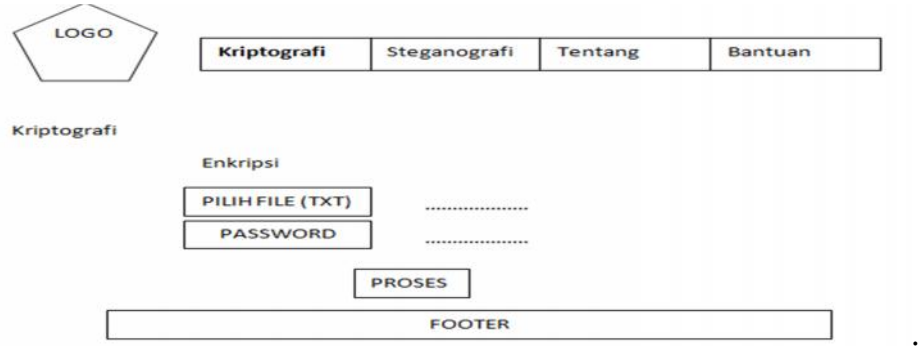
Proses ini memasukkan berkas *ciphertext* , kemudian memasukkan kunci untuk deskripsi *ciphertext* dan kemudian mendapatkan berkas *plaintext* (.txt).

3.4.3.3 Rancangan Antarmuka

Perancangan antarmuka implementasi teknik kriptografi dan steganografi menggunakan metode Vigenere dan AMELSBR*)* ini dirancang dengan tampilan yang *user friendly*, sehingga diharapkan dapat mempermudah pengguna dalam menggunakan sistem ini. Berikut rancangan antarmuka sistem.

1. Tampilan Kriptografi

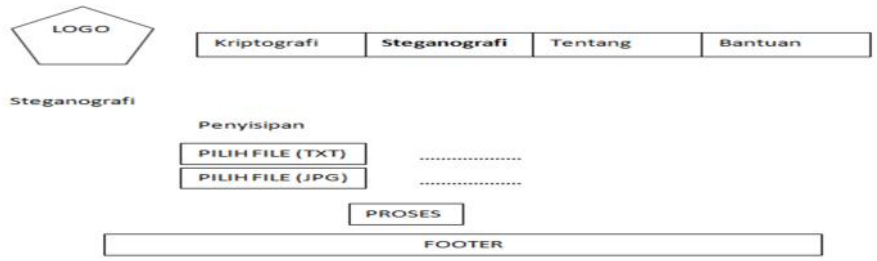
Tampilan kriptografi, pada tampilan ini pengguna dapat melakukan pross enkripsi dan dekripsi dengan membaca aturan penggunaan dibagian bantuan. Tampilan Kriptogafi disajikan pada Gambar 3.11.



Gambar 3.11 Tampilan Kriptografi.

2. Tampilan Steganografi

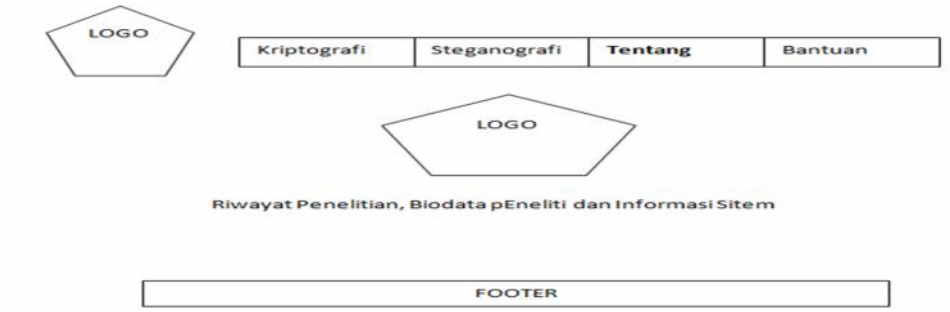
Tampilan Steganografi, pada tampilan ini pengguna dapat melakukan pross penyisipan dan ekstraksi dengan membaca aturan penggunaan dibagian bantuan. Tampilan Kriptogafi disajikan pada Gambar 3.12.



Gambar 3.12 Tampilan Steganografi.

3. Tampilan Bantuan

Tampilan Bantuan adalah tampilan yang memberikan pengarahan kepada pengguna sistem agar pengguna dapat menggunakan sistem dengan baik dan benar. Tampilan Bantuan disajikan pada Gambar 3.13.



Gambar 3.13 Tampilan Bantuan.

4. Tampilan Tentang

Tampilan Tentang adalah tampilan yang menyajikan informasi biodata dan nomor kontak pengembang sistem dan instansi. Tampilan Tentang disajikan pada Gambar 3.14

Gambar 3.13 Tampilan Tentang.

3.4.3.4 *Testing* (Pengujian)

Tahap *testing* atau pengujian adalah tahap untuk memastikan seluruh kebutuhan yang telah diimplementasikan serta mengidentifikasi kekurangan pada sistem. Pada pengujian sistem terdapat rencana pengujian atau sekenario pengujian yaitu.

1. Pengujian terhadap gambar berjenis *file* (.jpg/.jpeg) sebagai *input* dan gambar berjenis *file* (.png) sebagai *output*.

Proses ini untuk membuktikan bahwa gambar berjenis *file* (.jpg/.jpeg) sebagai *input* dan gambar berjenis *file* (.png) sebagai *output* adalah jenis *file* yang baik dalam teknik steganografi menggunakan metode AMELSBR.

2. Pengujian terhadap perubahan *brightness* dan *contrast.*

Proses ini untuk membuktikan bahwa perubahan *brightness* dan *contrast* pada *stego image* mempengaruhi berkas yang telah disisipi.

3. Pengujian terhadap pemotongan gambar pada hasil proses penyisipan (*stegoimage).*

Proses ini untuk membuktikan bahwa melakukan pemotongan gambar pada *stego image* mempengaruhi berkas yang telah disisipi.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut.

1. Sistem *hybrid* dengan menggabungkan algoritma Vigenere dan metode AMELSBR ini berhasil untuk menyandikan pesan rahasia serta menyembunyikannya ke dalam media penampung gambar sehingga memperoleh keamanan ganda dalam pengiriman data.
2. Tidak terlihat perbedaan yang signifikan antara *stegoimage* dengan gambar aslinya setelah dilakukan penyisipan. Dengan demikian penggunaan metode AMELSBR baik digunakan dalam steganografi.
3. *Stegoimage* dapat tahan terhadap proses manipulasi *brightness* dan *contrast* dengan catatan gambar harus mempunyai nilai warna dominan hitam (rgb(0,0,0)) atau putih (rgb(255,255,255)) dan tidak banyak varian warna, dengan kata lain gambar yang dapat mengembalikan berkas tanpa mengalami pengurangan makna secara berlebihan setelah dilakukannya manipulasi *brightness* dan *contrast* adalah gambar dengan kualitas citra *biner* dan citra *grayscale*.

4. Proses penyisipan pesan ke dalam gambar terjadi dari kiri ke kanan pada bagian atas gambar, sehingga pemotongan *stegoimage* pada bagian kiri dan atas mempunyai resiko kehilangan data lebih besar, sebaliknya pemotongan pada bagian bawah dan kanan mempunya resiko yang kecil terjadinya kehilangan data tergantung ukuran gambar dan jumlah *pixel*.

5.2. Saran

Setelah melakukan pengujian ini, maka saran yang diberikan untuk penelitian selanjutnya adalah sebagai berikut.

1. Pada penelitian selanjutnya dapat menggunakan metode lain agar dapat mengetahui kelemahan dan kelebihan masing-masing metode.
2. Pada penelitian selanjutnya media penampung yang akan disisipkan pesan dapat berupa audio, video ataupun media lain.
3. Pada pengembangan sistem yang akan dibangun dapat menggunakan bahasa pemrograman lain.

DAFTAR PUSTAKA

Ariyus, Doni. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi. ANDI: Yogyakarta.

Arjana, Putu H.,Rahayu Tri Puji, Hariyanton Yakub. 2012. Implementasi Enkripsi Data Dengan Algoritma Vigenere Cipher. Yogyakarta. Stmik Dharma Putra..

Curran, K., Bailey, K. 2004. An Evaluation of Image Based Steganography Methods. *International Journal of Digital Evidence*. Vol.2, Issue.1.

Gan, M. D. 2003. Chameleon Image Steganography, http://chameleonstego. tripod.com/downloads/Chameleon_Technical_Paper.pdf

Hermawati, Fajar A. 2013. *Pengolahan Citra Digital.* Yogyakarta : Andi Offset.

Ichsan. 2011. Implementasi Teknik Kompresi Gambar Dengan Algoritma Set Partitioning In Hierarchical Trees Pada Perangkat Bergerak. DepartemenTeknik Elektro Fakultas Teknik Universitas Sumatera Utara Medan, Medan.

Lee, Y. K., dan Chen, L. H. 1999. An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement. National Science Council, ROC. NSC87-2213-E-009-006.

Munawar. 2005. *Pemodelan Visual Dengan UML.* Yogyakarta: Graha Ilmu.

Munir, Rinaldi. 2004. *Pengolahan Citra Digital dengan Pendekatan Algoritmik*. Bandung : Penerbit Informatika Bandung.

Munir, Rinaldi. 2006. *Kriptografi*. Bandung: Penerbit Informatika Bandung.

Prayudi, Y. dan Kuncoro, P.S. 2005. Implementasi Steganografi Menggunakan Teknik Adaptive Minumum Error Least Significant Bit Replacement. Seminar Nasional Aplikasi Teknologi Informasi. Vol 1, G1-G6.

Provos, N and Honeyman, P. 2003. *Hide and Seek: An Introduction to Steganography.* University of Michigan.

Purnomo, Herry dan Zacharias, Theo. 2005. *Pengenalan Informatika Perspektif Teknik dan Lingkungan* . Yogyakarta: Andi.

Purnomo, Mauridhi H dan Muntasa A. 2010. *Konsep Pengolahan Citra Digital dan Ekstrasi Fitur*. Yogyakarta : Graha Ilmu.

Sasongko, Jati. 2005. Pengamanan Data Informasi Menggunakan Kriptografi Klasik. *Jurnal Teknologi Informasi DINAMIK*. Volume X, No.3, 160-167.

Satzinger, John W. Robert Jackson. and Stephen D. Burd. 2010. *Systems analysis and design in a changing world, Five Edition* . Course Technology, Cengage Learning, Boston, Massachusetts. Canada.

Sellars, D. 2006. *An Introduction to Steganography,* , http:// www.cs.uct.ac.za/ courses/ CS400W/NIS/papers99/dsellars/ stego.html

Sholiq. 2006.*Pemodelan Sistem Informasi Berorientasi Objek dengan UML*. Yogyakarta: Graha Ilmu.

Wamiliana., Mustofa. Usman., M. Azram., F.A. Elfaki., Astria. Hijriani., dan Pandya. Panditatwa. 2015. Adaptive Minimum Error Least Significant Bit Replacement Method for Steganography Using jpg/jpeg and Files. *Science International (Lahore)*, 27(6),4987-4990. ISSN: 1013-5316.

Wang, A. J., Armstrong, T., dan Yetsko, K. 2006. *Steganography*, http:// cse.spsu. edu/jwang/ research/security/steganography.pdf

Widhiartha, Putu. 2008. *Pengantar Kompresi Data*, http://nyoman.staf. narotama.ac.id/files/2012/01/widhiartha_kompresidata.pdf