APLIKASI PENYEMBUNYIAN FILE DENGAN VIGENERE CHIPER DAN STEGANOGRAPHY (LSB)

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

SKRIPSI

OLEH

NAMA	:	**ENDRAT FUJIYANTO**
N.P.M	:	**1624370457**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
2019

LEMBAR PENGESAHAN

APLIKASI PENYEMBUNYIAN FILE DENGAN VIGENERE CHIPER DAN STEGANOGRAPHY (LSB)

Disusun Oleh

NAMA : ENDRAT FUJIYANTO
NPM : 1624370457
PROGRAM STUDI : SISTEM KOMPUTER

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal : 07 November 2019

Dosen Pembimbing I	Dosen Pembimbing II
Andysah Putera Utama Siahaan, S.Kom., M.Kom	Leni Marlina, S.Kom,M.Kom

Mengetahui,

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi
Hamdani, ST., MT	Eko Hariyanto, S.Kom, M.Kom

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Endrat Fujiyanto
NPM	: 1624370457
Prodi	: Sistem Komputer
Konsentrasi	: Sistem Komputer
Judul Skripsi	: Aplikasi Penyembunyian File Dengan Vigenere Chiper dan Steganography (LSB)

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Sayat 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, 25 November 2019

Yang membuat pernyataan

Endrat Fujiyanto

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 ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

ya yang bertanda tangan di bawah ini :

ma Lengkap	: ENDRAT FUJIYANTO
mpat/Tgl. Lahir	: MEDAN / 18 Juli 1993
mor Pokok Mahasiswa	: 1624370457
gram Studi	: Sistem Komputer
sentrasi	: Sistem Kendali Komputer
mlah Kredit yang telah dicapai	: 141 SKS, IPK 3.10
mor Hp	: 082365656711

ngan ini mengajukan judul sesuai bidang ilmu sebagai berikut :

o.	Judul
1.	APLIKASI PENYEMBUNYIAN FILE DENGAN VIGENERE CHIPER DAN STEGANOGRAPHY

an : Diisi Oleh Dosen Jika Ada Perubahan Judul

t Yang Tidak Perlu
r I,

Medan, 15 Mei 2018

Pemohon,

(Endrat Fujiyanto)

Cahyo Pramono, SE., MM

Tanggal : .....
Disetujui oleh :
Dosen Pembimbing I :

(Andysah Putera Utama Siahaan S.Kom. MKom)

Tanggal : .....
Disetujui oleh:
Dosen Pembimbing II:

(Leni Marlina. M.Kom.)

Tanggal : .....
Disetujui oleh:
Ka. Prodi Teknik Komputer

(Eko Hariyanto, S.Kom, M.Kom)

Tanggal : .....
Diketahui oleh :
Dekan

(Hamdani, ST., MT.)

No. Dokumen: FM-LPPM-18-02	Revisi: 0	Tgl. Eff: 15 Oktober 2020

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Jend. Gatot Subroto Km 4,5 ☎ 06150200508 – 20122 Medan
Email : fst@pancabudi.ac.id website : www.pancabudi.ac.id

or : 1120 /17/FST/2018
o : 1 (satu) eks.
: **Tugas Bimbingan Skripsi/Tugas Akhir**

da : Yth. Bapak/Ibu
1. **Andysyah Putera Utama Siahaan, S.Kom.,M.kom** (Pembimbing I)
2. **Leni Marlina S.Kom.,M.Kom** (Pembimbing II)

Di -
Tempat

Dengan hormat, sehubungan permohonan mahasiswa untuk melaksanakan pembuatan Skripsi/ Tugas Akhir, yang diajukan oleh :

N a m a	: **Endrat Fujiyanto**
N.P.M	: 1624370457
Prog. Studi	: Sistem Komputer
Judul	: Aplikasi Penyembunyian File Dengan Metode Pailier dan RGB Intensity Based Staganography (VB Net)
Jadwal Seminar	:
Jadwal Sidang	:

Sehubungan dengan hal tersebut, maka kami menugaskan Bapak/Ibu sebagai dosen pembimbing guna penyelesaian Skripsi/Tugas Akhir mahasiswa tersebut. Dalam proses bimbingan tidak dibenarkan menawarkan bantuan untuk pembuatan skripsi, tata cara penulisan Skripsi/Tugas Akhir sesuai dengan ketentuan yang ditetapkan oleh Fakultas.

Demikian disampaikan, atas perhatian dan kerja sama Bapak/Ibu diucapkan terima kasih.

Medan, 28 Maret 2018
Dekan,

Sri Shindi Indira, ST.,M.Sc

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 : Andysyah Putera Utama Siahaan, S.Kom, M.Kom
Dosen Pembimbing II : Leni Marlina, S.Kom., M.Kom
Nama Mahasiswa : ENDRAT FUJIYANTO
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1624370457
Jenjang Pendidikan :
Judul Tugas Akhir/Skripsi : Aplikasi Penyembunyian File dengan Metode Paillier dan RGB Intensity Based Steganography

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
16-02-2018	perbaiki Bab I, Buat metode penelitian	Leni	
26-08-2018	Acc bab I dan II. lanjutkan ke Bab berikutnya-	Leni	
15-09-2018	perbaiki Bab III. perbaiki penulisannya.	Leni	
02-10-2018	lanjutkan Bab Implementasi.	Leni	
10-10-2018	Sistematika antar dengan dgn Implementasi.	Leni	
15-10-2018	lengkapi Seminar	Leni	
24-10-2018	Lengkapi Seminar. -kata pengantar, D-isi, D-gbr, D-tbl D-pustaka-	Leni	
31-10-2018	perbaiki kelengkapan Skripsi Acc Seminar	Leni	
19-03-2019	Acc sidang	Leni	

Medan, 13 Agustus 2018
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira

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

iversitas	: Universitas Pembangunan Panca Budi
kultas	: SAINS & TEKNOLOGI
sen Pembimbing I	: Andysyah Putera Utama Siahaan, S.Kom., M.Kom
sen Pembimbing II	: Leni Marlina S.Kom., M.Kom
ma Mahasiswa	: ENDRAT FUJIYANTO
rusan/Program Studi	: Sistem Komputer
mor Pokok Mahasiswa	: 1624370457
njang Pendidikan	:
dul Tugas Akhir/Skripsi	: Aplikasi Penyembunyian File dengan Metode Pairter dan RGB Intensity Based Steganography

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
12/4 2018	Revisi Bab I		
14/8 2018	Revisi Bab II		
3/9 2018	Revisi Bab I, II		
10/9	Revisi Bab III		
20/9	Revisi Bab II, III		
30/9	Revisi Bab IV, V		
1/10	Acc Seminar / Revisi Judul		
27/3	Acc Sidang		

Medan, 18 April 2018
Diketahui/Disetujui oleh :
Dekan,

TANDA BEBAS PUSTAKA
No. 2100/perp/ISP/2019
Dinyatakan tidak ada sangkut paut dengan UPT. Perpustakaan
Medan, 18 APR 2019
Ka. UPT. Perpustakaan
Elfyana, S.Sos

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 10 April 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di - .
Tempat

Telah Diperiksa oleh LPMU
dengan Plagiarisme..... 36 %
Medan, 27 JULI 2019
AN Ka. LPMU
THAMRIN HAKIM
~~Galih Pramono, SE, MM~~

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: ENDRAT FUJIYANTO
Tempat/Tgl. Lahir	: MEDAN / 18 Juli 1993
Nama Orang Tua	: SURATNO
N. P. M	: 1624370457
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 082365656711
Alamat	: Jl. Bilal Ujung

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Aplikasi penyembunyian file dengan vigenere chiper dan steganography (LSB).**, 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.	750.000
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.	~~1,605,000~~ 2.355.000
	5. Uk. Termin Ganjil	Rp	4.200.000
			6.555.000

16/8/19

Ukuran Toga : L

Hormat saya

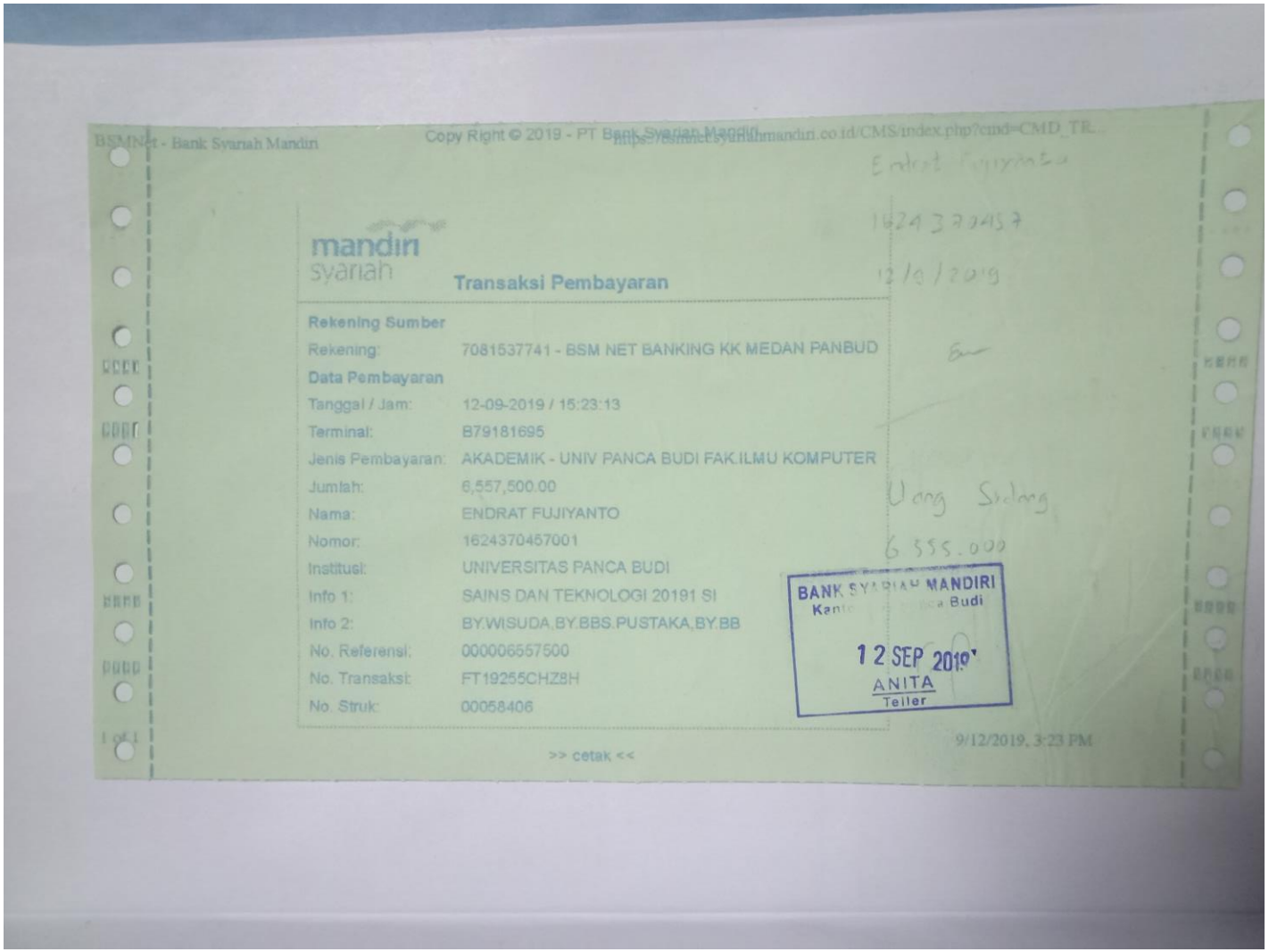
ENDRAT FUJIYANTO
1624370457

Diketahui/Disetujui oleh :
Dekan Fakultas SAINS & TEKNOLOGI
Sri Shinta Mahmud, S.T., M.Sc.

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.

Telah di terima
berkas persyaratan
dapat di proses
Medan, 16-08-2019
Ka. BPAA
an.
TEGUH WARYONO, SE., MM.



BSMNet - Bank Syariah Mandiri Copy Right © 2019 - PT Bank Syariah Mandiri https://bsmnet.syariahmandiri.co.id/CMS/index.php?cmd=CMD_TR...

Endrat Fujiyanto

1624370457

12/9/2019

mandiri syariah

Transaksi Pembayaran

Rekening Sumber	
Rekening:	7081537741 - BSM NET BANKING KK MEDAN PANBUD
Data Pembayaran	
Tanggal / Jam:	12-09-2019 / 15:23:13
Terminal:	B79181695
Jenis Pembayaran:	AKADEMIK - UNIV PANCA BUDI FAK.ILMU KOMPUTER
Jumlah:	6,557,500.00
Nama:	ENDRAT FUJIYANTO
Nomor:	1624370457001
Institusi:	UNIVERSITAS PANCA BUDI
Info 1:	SAINS DAN TEKNOLOGI 20191 SI
Info 2:	BY.WISUDA,BY.BBS.PUSTAKA,BY.BB
No. Referensi:	000006557500
No. Transaksi:	FT19255CHZ8H
No. Struk:	00058406

Uang Sidang

6.555.000

BANK SYARIAH MANDIRI Kantor Panca Budi

12 SEP 2019

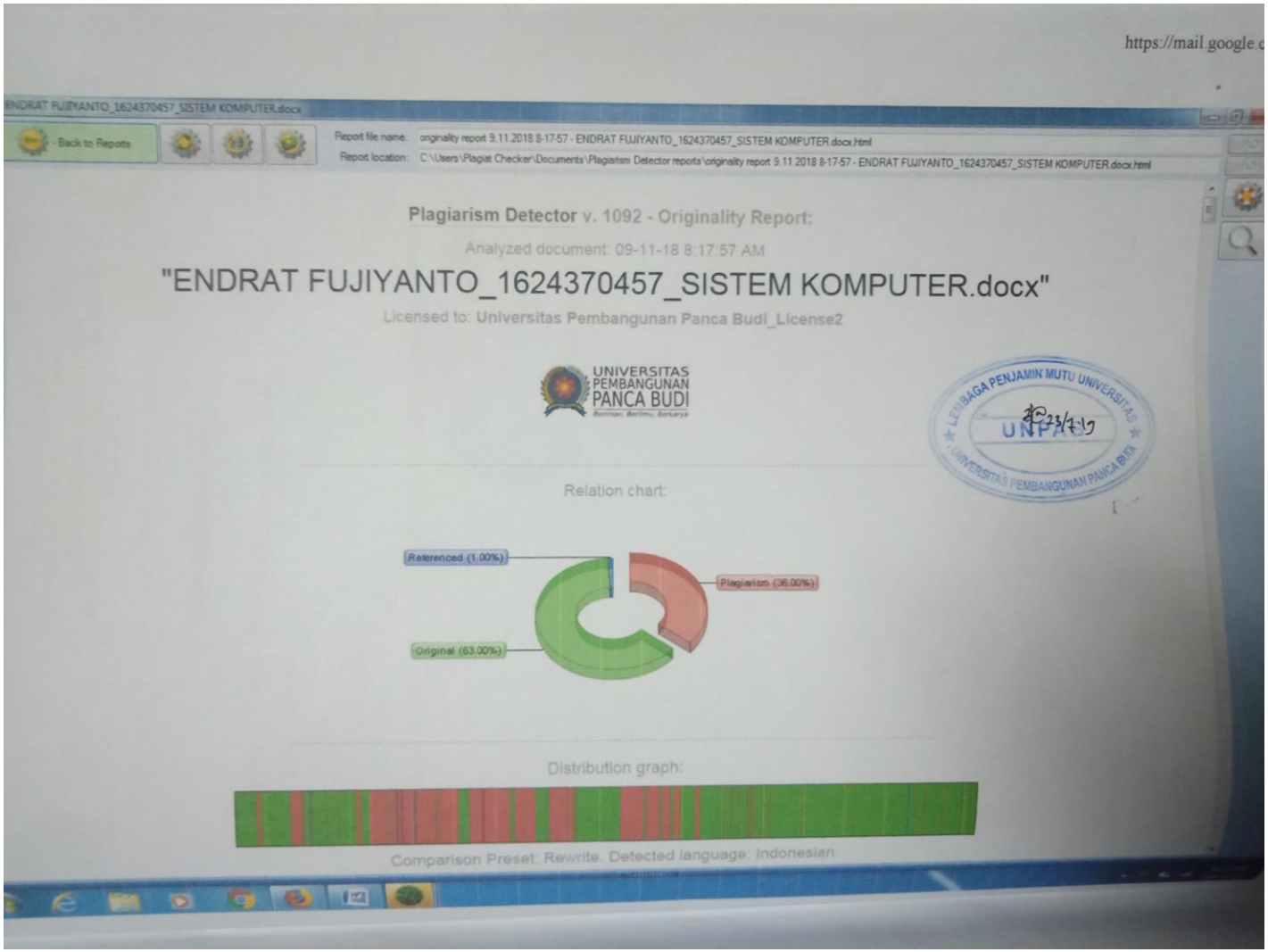
ANITA

Teller

>> cetak <<

9/12/2019, 3:23 PM

1 of 1


https://mail.google.c
ENDRAT FUJIYANTO_1624370457_SISTEM KOMPUTER.docx
- Back to Reports
Report file name: originality report 9.11.2018 8-17-57 - ENDRAT FUJIYANTO_1624370457_SISTEM KOMPUTER.docx.html
Report location: C:\Users\Plagiat Checker\Documents\Plagiarism Detector reports\originality report 9.11.2018 8-17-57 - ENDRAT FUJIYANTO_1624370457_SISTEM KOMPUTER.docx.html
Plagiarism Detector v. 1092 - Originality Report:
Analyzed document: 09-11-18 8:17:57 AM
"ENDRAT FUJIYANTO_1624370457_SISTEM KOMPUTER.docx"
Licensed to: Universitas Pembangunan Panca Budi_License2
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LEMBAGA PENJAMIN MUTU UNIVERSITAS
UNPAB
23/7-19
UNIVERSITAS PEMBANGUNAN PANCA BUDI
Relation chart:
Referenced (1.00%)
Plagiarism (36.00%)
Original (63.00%)
Distribution graph:
Comparison Preset: Rewrite. Detected language: Indonesian

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	:	ENDRAT FUJIYANTO
N.P.M.	:	1624370457
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, 18 April 2019
Ka. Laboratorium

Fachrid Wadly, S. Kom

Tgl. Efektif : 04 Juni 2015

ABSTRAK

Steganografi berhubungan dengan penambahan informasi pada sebuah media yang diberikan (disebut sebagai media sampul) tanpa membuat perubahan yang kelihatan kasat mata padanya. Kebanyakan teknik steganografi yang dikemukakan tidak dapat diterapkan untuk menyimpan data dalam skala besar. Dalam teknik baru untuk steganografi citra RGB, intensitas warna (R-G-B) digunakan untuk menentukan jumlah bit yang ingin disimpan pada setiap piksel. Sementara itu, untuk meningkatkan keamanan dari *file* rahasia yang disimpan, maka akan diterapkan metode kriptografi. *Paillier cryptosystem* yang ditemukan oleh Pascal Paillier pada tahun 1999 merupakan sebuah algoritma asimetris *probabilistic* untuk kriptografi kunci publik. Sekuritas dari algoritma *Paillier* ini bergantung pada problema perhitungan n-*residue class* yang dipercaya sangat sulit untuk dikomputasi. Problema ini dikenal dengan asumsi *Composite Residuosity* (CR) dan merupakan dasar dari kriptosistem *Paillier* ini. Kelebihan dari algoritma *Paillier* ini terletak pada sifat probabilistiknya sehingga susah dipecahkan *ciphertext*-nya. Perangkat lunak yang dibuat dapat menyimpan *file* rahasia ke dalam sebuah citra digital menjadi sebuah citra stego. *File* rahasia tersebut dapat diekstrak keluar melalui proses ekstraksi.

Kata kunci : citra digital, ekstraksi, *file* rahasia, kritografi, metode *Paillier*, metode RGB *steganography*, penempelan, steganografi.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Skripsi yang berjudul "Aplikasi Penyembunyian File Dengan Vigenere Chiper Dan Steganography (Lsb)".

Skripsi disusun sebagai salah satu syarat yang harus ditempuh untuk menyelesaikan Program Sarjana (S1) pada Program Studi Sistem Komputer Fakultas Sains & Teknologi Universitas Pembangunan Panca Budi.

Skripsi ini dapat disusun dengan baik karena banyak masukan, dukungan dan bantuan baik tenaga, materi maupun dorongan semangat dari berbagai pihak oleh karena itu penulis mengucapkan terima kasih kepada:

1. Bapak Dr. H. Muhammad Isa Indrawan, S.E, M.M., selaku Rektor Universitas Pembangunan Panca Budi.
2. Ibu Sri Shindi Indira, ST., M.Sc., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi.
3. Bapak Eko Hariyanto, S. Kom., M. Kom selaku Ketua Program Studi Sistem Komputer Universitas Pembangunan Panca Budi.
4. Bapak Andysah Putera Utama Siahaan, S.Kom., M.Kom., Ph.D selaku Dosen Pembimbing I.
5. Ibu Leni Marlina, S.Kom., M.Kom., selaku Dosen Pembimbing II.
6. Seluruh Keluarga penulis, terutama untuk kedua orang tua penulis, yang banyak memberi dukungan moril dan materil serta doa yang tiada henti diberikan kepada penulis dalam menyelesaikan Skripsi penulis.

7. Seluruh teman-teman penulis diprodi Sistem Komputer KK MLM L2A atau REG MLM L3A Angkatan 2016. Terima kasih atas bantuan, dukungan dan hiburan yang sudah kalian berikan kepada penulis.
8. Semua pihak yang telah membantu dalam menyelesaikan Skripsi ini.

Dalam skripsi ini, penulis menyadari bahwa masih jauh dari kata sempurna baik dari segi materi, pengolahan mau pun penyajiannya. Untuk itu penulis mengharapkan kritik dan saran yang bersifat membangun bagi penulis demi kesempurnaan skripsi ini. Penulis berharap semoga skripsi ini dapat bermanfaat bagi semua pihak.

Medan, 08 Oktober 2019
Penulis,

Endrat Fujiyanto
NPM. 1624370457

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Nomor **Judul** **Halaman**

BAB I

PENDAHULUAN

1. Latar Belakang

Steganografi berhubungan dengan penambahan informasi pada sebuah media yang diberikan (disebut sebagai media sampul) tanpa membuat perubahan yang kelihatan kasat mata padanya. Sasarannya adalah untuk menyembunyikan sebuah *file* yang ditempelkan diantara media sampul sedemikian sehingga keberadaan *file* yang ditempelkan menjadi tersembunyi. Steganografi dapat digunakan untuk menyembunyikan pesan pada citra ataupun berfungsi sebagai pemberian hak paten pada citra. Steganografi berbasis citra menggunakan citra sebagai media sampul. Beberapa metode telah diperkenalkan untuk steganografi berbasis citra, seperti metode LSB (*Least Significant Bits*), *Masking* dan *Filtering*, *Transformations* dan *Spread Spectrum Image Steganography*, dimana LSB adalah salah satu metode paling sederhana.

Kebanyakan teknik steganografi yang dikemukakan tidak dapat diterapkan untuk menyimpan data dalam skala besar. Teknik steganografi untuk citra RGB baru dikemukakan dalam paper '*RGB Intensity Based Variable-Bits Image Steganography*' (Parvez, T. dan A.A.A., Gutub, 2008). Dalam teknik baru untuk steganografi citra RGB, intensitas warna (R-G-B) digunakan untuk menentukan jumlah bit yang ingin disimpan pada setiap piksel. *Channel* (saluran) yang terdiri dari nilai warna rendah dapat menyimpan jumlah data bit yang lebih besar. Deretan dari *channel* dipilih secara acak berdasarkan pada sebuah kunci yang

digunakan bersama. Teknik ini menjamin sebuah kapasitas minimum dan dapat mengakomodasikannya untuk menyimpan data berukuran besar. Para pengembang algoritma ini mengklaim bahwa algoritmanya memiliki performansi yang lebih bagus daripada algoritma sebelumnya. Algoritma ini juga dapat digunakan untuk menyimpan jumlah bit yang berbeda per *channel*, tetapi tetap dapat menyediakan kapasitas sangat tinggi untuk media sampul. (Parvez, T. dan A.A.A., Gutub, 2008)

Kriptografi memungkinkan orang meninggalkan pesan rahasia yang dijumpai dalam dunia fisik ke dalam dunia elektronik, sehingga memungkinkan orang melakukan bisnis secara elektronik tanpa keraguan atas pemalsuan, pencurian dan penipuan. Setiap hari ratusan ribu orang yang berinteraksi secara elektronik, apakah melalui *e-mail*, *e-commerce*, mesin ATM atau telepon seluler. Peningkatan penyebaran informasi secara elektronik telah mengakibatkan ketergantungan yang meningkat terhadap kriptografi. Salah satu peranan dari kriptografi adalah untuk melakukan pengamanan data yaitu dengan menggunakan algoritma kriptografi. *Paillier cryptosystem* yang ditemukan oleh Pascal Paillier pada tahun 1999 merupakan sebuah algoritma asimetris *probabilistic* untuk kriptografi kunci publik. Dengan enkripsi *probabilistic*, seorang *crypanalyst* tidak dapat lagi mengenkripsi *plaintext* acak untuk mencari *ciphertext* yang benar. Algoritma *Paillier* ini merupakan suatu algoritma enkripsi *probabilistic* yang lebih efisien karena proses enkripsi per karakter dan bukan per bit.

Penggabungan metode kriptografi dan steganografi ini akan menghasilkan sebuah sistem dengan tingkat keamanan yang sangat tinggi. Oleh karena itu, penulis tertarik untuk membahas dan mempelajari proses kerja dari algoritma

kriptografi dan steganografi tersebut dengan mengambil skripsi yang berjudul "**Aplikasi Penyembunyian File dengan Vigenere Chiper dan Steganography (LSB)**".

2. Rumusan Masalah

Berdasarkan uraian latar belakang sebelumnya, maka permasalahannya adalah:

a. Pengamanan data rahasia dengan menggunakan metode kriptografi dapat mengamankan data tersebut sehingga pihak lain tidak dapat mengetahui isi data, namun pihak lain dapat mengetahui bahwa ada informasi yang dirahasiakan.
b. Kebanyakan metode steganografi tidak efisien dalam menyembunyikan data, dimana tidak dapat dilakukan penyimpanan data dalam skala besar pada sebuah citra
c. Beberapa metode kriptografi akan selalu menghasilkan *ciphertext* yang sama untuk input plaintext dan kunci yang sama, sehingga rentan terhadap penyerangan.

3. Batasan Masalah

Batasan masalah yang akan dibahas dalam skripsi ini mencakup :

a. *Input* citra sampul dalam format JPG, BMP dan PNG.
b. *Input* dokumen teks sebagai pesan rahasia yang akan disisipkan memiliki format TXT, RTF dan DOCX dimana data yang terbaca hanya data *plaintext* saja, tanpa adanya format dan tidak mencakup gambar ataupun tabel.
c. Ukuran citra yang dapat diproses merupakan citra persegi.

d. Data yang disisipkan berupa pesan rahasia bertipe data *string* yang mencakup ASCII Code yang terdapat pada *keyboard* komputer.

4. Tujuan Penelitian

Tujuan dari penyusunan skripsi ini adalah untuk membuat sebuah perangkat lunak untuk mengamankan dan menyembunyikan data rahasia pada citra digital dengan menggunakan algoritma kriptografi dan steganografi citra, sehingga dapat mempermudah pengamanan data rahasia agar tidak diketahui orang lain.

5. Manfaat Penelitian

Kontribusi yang dapat diberikan adalah sebagai berikut:

a. Bagi dunia akademik dan ilmu pengetahuan khususnya Universitas Pembangunan Panca Budi.
    1. Sebagai bahan referensi tambahan dalam hal menyelesaikan sebuah permasalahan yang mirip dengan latar belakang pembuatan sistem ini.
    2. Sebagai modul praktikum dalam pembelajaran tentang visual basic.
b. Bagi pembaca
    1. Sistem ini diharapkan memberi manfaat dalam keamanan dan kemudahan dalam penyembunyian data.
    2. Bagi dunia pekerjaan, dapat digunakan sebagai sistem yang akan meningkatkan keamanan dan kenyamanan karyawan dengan membatasi dan menghindari tindak kejahatan dalam perusahaan.
    3. Perangkat lunak dapat digunakan untuk mengamankan dan menyembunyikan data rahasia pada citra digital dengan menggunakan algoritma kriptografi dan steganografi citra.

c. Bagi penulis

1. Untuk mengaplikasikan ilmu yang telah diperoleh selama perkuliahan, serta menambah wawasan mengenai sistem aplikasi penyembunyian file dengan metode Paillier dan RGB.
2. Untuk kontribusi penulis dalam dunia pendidikan agar berguna bagi kehidupan sehari-hari dan bisa dikembangkan lagi dikemudian hari.

6. Metode Penelitian

Metodologi pengembangan sistem adalah metode-metode, prosedur-prosedur, konsep-konsep pekerjaan, aturan-aturan, postulat-postulat yang akan digunakan untuk mengembangkan sebuah sistem. Langkah kerja dalam menyusun skripsi ini adalah sebagai berikut :

a. Kajian Teoritis

Studi lapangan, observasi dan wawancara mengenai teori-teori yang berhubungan dengan topik yang dibahas.

b. Analisis

Melakukan analisis masalah dan menetapkan algoritma untuk menyimpulkan lebih rinci masalah yang akan diselesaikan. Proses kerja akan digambarkan dengan menggunakan *activity diagram*. Aplikasi yang dibuat akan dimodelkan dengan menggunakan *use case diagram*.

c. Perancangan

Rancangan *interface* (*input* dan *output*) dari perangkat lunak) menggunakan *Microsoft Visual Basic 2010*.

d. Pemrograman (*coding*)

Membuat kode program dari perangkat lunak dengan menggunakan *Microsoft Visual Basic 2010*.

e. Pengujian

Pada tahap ini dilakukan pengujian terhadap atas aplikasi yang dibuat.

f. Membuat kesimpulan dan menyusun laporan tugas akhir.

7. Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam penyusuan laporan penelitian :

BAB 1 PENDAHULUAN

Pada bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bab ini berisi tentang teori-teori dasar yang berhubungan dengan objek penelitian.

BAB 3 ANALISA DAN PERANCANGAN

Pada bab ini berisi tentang analisa proses kerja dari metode *Paillier* dan *RGB Intensity Based Steganography*, perancangan aplikasi yang dibangun menggunakan alat bantu permodelan yaitu : UML, *flowchart*, *interface* serta user *interface.*

BAB 4 HASIL DAN PEMBAHASAN

Pada bab ini diuraikan tentang implementasi dari aplikasi yang di buat serta kelebihan dan kelemahan aplikasi yang di hasilkan.

BAB 5 PENUTUP

Bab ini menjelaskan kesimpulan dan saran hasil akhir dari semua penulisan yang dikerjakan yaitu yang berisi masukan-masukan untuk mengembangkan dan melengkapi sistem yang sudah dibangun di masa yang mendatang.

BAB II

LANDASAN TEORI

1. Kriptografi

a. Definisi Kriptografi

Kata kriptografi (*cryptography*) berasal dari bahasa Yunani, yaitu *kriptos* yang artinya *secret* (rahasia), dan *graphein*, yang artinya *writing* (tulisan). Kriptografi berarti *secret writing* (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat dan mata-mata. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan *data integrity*, *authentication*, dan *non-repudiation* (Schneier, B., 1996).

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*cryptography is the art and science of keeping messages secure*) (Schneier, B., 1996).

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi (Menezes, A., dkk, 1996).

Kata ”seni” di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang

unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (Schneier, B., 1996).

b. Tujuan Kriptografi

Kriptografi bertujuan untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan) sebagai berikut:

1. Kerahasiaan (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi *ciphertext*. Misalnya pesan "Harap datang pukul 8" disandikan menjadi "TrxC#45motyptre!%". Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy*.
2. Integritas data (*data integrity*) , adalah layanan yang menjamin bahwa pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?". Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain ke dalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Pesan yang telah ditandatangani menyiratkan pesan yang dikirim adalah asli.

3. Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *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. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar ?".

   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. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Tanda tangan digital menyatakan 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. Sebagai contoh misalkan seorang pemilik emas mengajukan tawaran kepada toko mas bahwa ia akan menjual emasnya. Tetapi, tiba-tiba harga emas turun drastis, lalu ia membantah telah mengajukan tawaran menjual emas. Dalam hal ini, pihak toko emas perlu prosedur nirpenyangkalan untuk membuktikan bahwa pemilik emas telah melakukan kebohongan (Schneier, B., 1996).

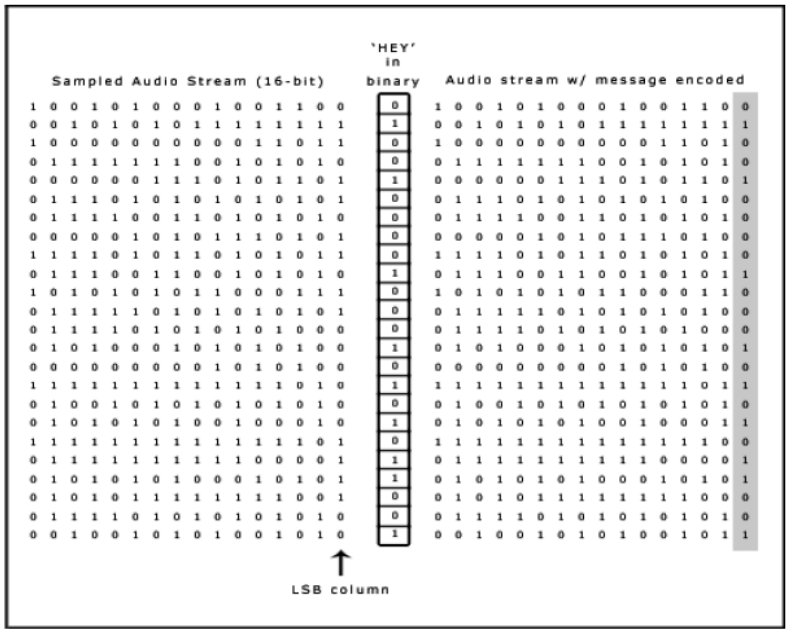
2. Steganografi

Metode-Metode Steganografi

Metode-metode umum yang digunakan untuk menyembunyikan data dalam sebuah *digital images* antara lain:

a. Least Significant Bit Insertion (*LSB*)

Metode ini adalah metode yang sangat popular dimana *LSB* dari setiap *byte* dalam sebuah citra digunakan untuk menyimpan data rahasia (Gambar 2.8). Perubahan yang dihasilkan terlalu kecil, sehingga sulit dikenali oleh mata manusia. Kekurangan dari teknik ini adalah karena teknik ini menggunakan setiap *pixel* dalam sebuah citra, format kompresi yang menjaga keutuhan data seperti *bmp* atau *gif* harus digunakan sebagai citra. Apabila format kompresi yang tidak menjaga keutuhan data digunakan, beberapa informasi tersembunyi dapat hilang.



Gambar 1. *Least Significant Bit*

Sumber : Cun-Cun. 2008.

b. Masking* and *Filtering

Kedua metode ini menyembunyikan informasi dengan cara mirip dengan penanda kertas. Hal ini dapat dilakukan, contohnya dengan memodifikasi luminance sebagian dari citra, tetapi apabila dilakukan dengan hati-hati distorsi baru dapat terlihat.

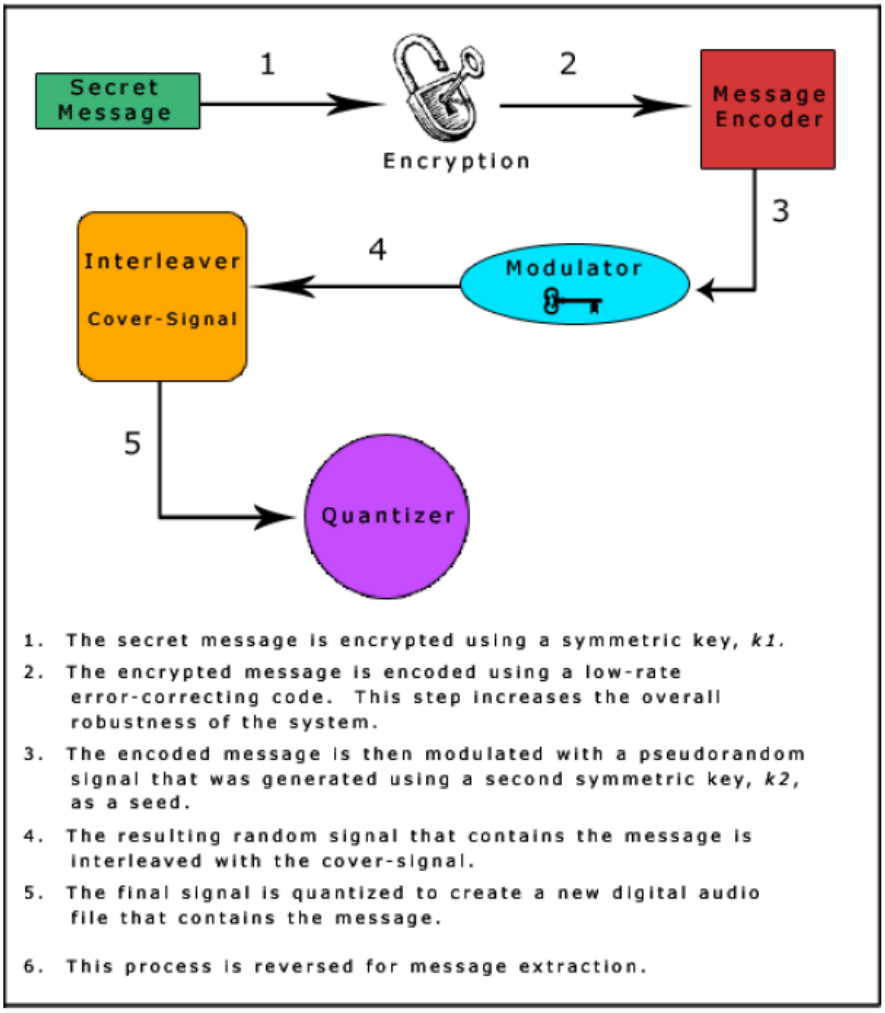
c. Transformations

Discrete Cosine Transformation (DCT) adalah salah satu metode transformasi untuk mentransformasi 8*8 blok pixel dari sebuah citra secara berurutan kedalam masing-masing koefisien DCT. Alat steganografi dapat menggunakan LSB dari koefisien DCT yang terbagi-bagi utnuk menyembunyikan informasi (metode JSteg). Sebagai tambahan DCT, citra dapat diproses dengan FFT atau dengan *Wavelet Transformation*. Properti citra yang lain seperti *luminance* juga dapat dimanipulasi.

d. Spread Spectrum Image Steganography

Metode-metode yang didasari oleh teknologi ini menyandikan pesan yang diinginkan agar tersembunyi. Untuk menyandikan, digunakan sebuah *pseudorandom noise generator* yang lebar untuk membuat sebuah barisan yang tersebar. Kemudian, sebuah skema modulasi digunakan untuk memperluas spektrum yang sempit dari sebuah pesan dengan barisan yang tersebar, dengan demikian menyusun sinyal yang dibawa yang masuk ke dalam interleave dan ruang penyebar. Inner leaver juga dapat mempergunakan kunci untuk mendikte algoritma *interleaving*. Sinyal ini sekarang digabungkan dengan *cover* dari citra untuk menghasilkan citra stego, yang sudah dibagi-bagi dengan layak untuk

memelihara *dynamic range* awal dari cover citra. Citra stego tersebut kemudian diteruskan kepada penerima pesan. Untuk lebih jelasnya, lihat gambar berikut:



Gambar 2. *Spread Spectrum*

Sumber : Cun-Cun, 2008.

e. Algoritma *Image Steganography* Berbasis Intensitas Citra.

Pada tahun 2008, Mohammad Tanvir Parvez dan Adnan Abdul-Aziz Gutub memperkenalkan sebuah algoritma baru yang mampu menjamin kapasitas minimum untuk setiap citra sampul dan jumlah bit yang tersimpan pada setiap

channel dapat berbeda yang tergantung pada intensitas. Hal ini dapat memberikan kapasitas yang sangat tinggi untuk beberapa citra sampul.

Ide algoritma ini adalah bahwa nilai warna yang lebih rendah dari sebuah *channel* memiliki efek yang lebih rendah pada keseluruhan warna dari piksel dibandingkan dengan nilai yang lebih tinggi. Oleh karena itu, lebih banyak bit dapat diubah pada sebuah *channel* yang memiliki nilai ‘rendah’ daripada sebuah channel yang memiliki nilai ‘tinggi’.

3. Citra

Data atau informasi tidak hanya disajikan dalam bentuk teks, tetapi juga dapat berupa gambar, audio (bunyi, suara, musik), dan video. Keempat macam data atau informasi ini sering disebut multimedia. Era teknologi informasi saat ini tidak dapat dipisahkan dari multimedia. Situs web (*website*) di Internet dibuat semenarik mungkin dengan menyertakan visualisasi berupa gambar atau video yang dapat diputar. Beberapa waktu lalu istilah SMS (*Short Message Service*) begitu populer bagi pengguna telepon genggam (*handphone* atau HP). Tetapi, saat ini orang tidak hanya dapat mengirim pesan dalam bentuk teks, tetapi juga dapat mengirim pesan berupa gambar maupun video, yang dikenal dengan layanan MMS (*Multimedia Message Service*).

Citra (*image*) – istilah lain untuk gambar – sebagai salah satu komponen multimedia memegang peranan sangat penting sebagai bentuk informasi visual. Citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu citra kaya dengan informasi. Ada sebuah peribahasa yang berbunyi “sebuah gambar bermakna lebih dari seribu kata” (*a picture is more than a thousand words*). Maksudnya tentu sebuah gambar dapat memberikan informasi yang lebih banyak

daripada informasi tersebut disajikan dalam bentuk kata-kata (tekstual) (Munir, R., 2008).

Secara harfiah, citra (*image*) adalah gambar pada bidang dwimatra (dua dimensi). Gambar 2.1 adalah citra seorang gadis model yang bernama Lena, dan gambar di sebelah kanannya adalah citra kapal di sebuah pelabuhan. Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh oleh alat-alat optik, misalnya mata pada manusia, kamera, pemindai (*scanner*), dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam.

Citra sebagai keluaran dari suatu sistem perekaman data dapat bersifat:

1. optik berupa foto,
2. analog berupa sinyal video seperti gambar pada monitor televisi,
3. digital yang dapat langsung disimpan pada suatu pita magnetik.

Citra yang dimaksudkan di dalam keseluruhan isi buku ini adalah “citra diam” (*still images*). Citra diam adalah citra tunggal yang tidak bergerak. Gambar 2.1 adalah dua buah citra diam. Untuk selanjutnya, citra diam disebut citra saja.

(a) Lena

(b) Kapal

Gambar 3. Citra Lena dan Citra Kapal

Sumber : Munir, R., 2008

Citra bergerak (*moving images*) adalah rangkaian citra diam yang ditampilkan secara beruntun (sekuensial) sehingga memberi kesan pada mata sebagai gambar yang bergerak. Setiap citra di dalam rangkaian itu disebut *frame*. Gambar-gambar yang tampak pada film layar lebar atau televisi pada hakikatnya terdiri atas ratusan sampai ribuan frame (Munir, R., 2008).

Meskipun sebuah citra kaya informasi, namun seringkali citra yang kita miliki mengalami penurunan mutu (degradasi), misalnya mengandung cacat atau derau (*noise*), warnanya terlalu kontras, kurang tajam, kabur (*blurring*), dan sebagainya. Tentu saja citra semacam ini menjadi lebih sulit diinterpretasi karena informasi yang disampaikan oleh citra tersebut menjadi berkurang.

a. Citra Analog

Citra Analog adalah citra yang terdiri dari sinyal-sinyal frekuensi elektromagnetis yang belum dibedakan sehingga pada umumnya tidak dapat ditentukan ukurannya. Dimana fungsinya adalah kontinu sehingga belum dapat dideteksi titik per titik (piksel) bagian terkecil dari citra tersebut (Murni, 1992).

b. Citra Digital

Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada pita magnetik. Menurut presisi yang digunakan untuk menyatakan titik-titik koordinat pada domain spasial atau bidang dan untuk menyatakan nilai keabuaan atau warna suatu citra, maka secara teoritis citra dapat dikelompokkan menjadi empat kelas citra, yaitu citra kontinu-kontinu, kontinu-diskrit, diskrit-kontinu, dan diskrit-diskrit, di mana label pertama menyatakan presisi dari titik-titik koordinat pada bidang citra sedangkan label kedua menyatakan presisi nilai keabuan atau warna. Kontinu dinyatakan dengan presisi angka tak terhingga, sedangkan diskrit dinyatakan dengan presisi angka terhingga.

Komputer digital bekerja dengan angka-angka presisi terhingga, dengan demikian hanya citra dari kelas diskrit-diskrit yang dapat diolah dengan komputer,

citra dari kelas tersebut lebih dikenal sebagai citra digital. Citra digital merupakan suatu array dua dimensi atau suatu matriks yang elemen-elemennya menyatakan tingkat keabuan dari elemen gambar, jadi informasi yang terkandung bersifat diskrit. Citra digital tidak selalu merupakan hasil langsung data rekaman suatu sistem. Kadang-kadang hasil rekaman data bersifat kontinu seperti gambar pada monitor televisi, foto sinar-X, dan lain sebagainya. Dengan demikian untuk mendapatkan suatu citra digital diperlukan suatu proses konversi, sehingga citra tersebut selanjutnya dapat diproses dengan komputer (Murni, 1992).

c. RGB

Salah satu sistem yang digunakan untuk mewakili gambar yaitu sistem warna RGB (*Red, Green, Blue*). Sistem RGB adalah sistem yang menggabungkan warna primer gabungan (*additive primary colours*) untuk memperoleh gabungan-gabungan warna. Mode warna RGB megunakan nilai antara 0 – 255 untuk masing-masing komponen warna penyusunnya atau disebut juga chanel warna. Nilai 0 mengacu pada warna hitam, sedangkan nilai 255 menunjukkan warna putih sehingga untuk menyusun sebuah warna mode RGB menggunakan kombinasi nilai antara 0- 255 pada masing-masing chanelnya (Yoga, 2005).

Setiap elemen dalam sistem ini disebut sebagai channel, sehingga sistem ini memiliki 3 channel yaitu *channel* R (mewakili warna merah), *channel* G (mewakili warna hijau) dan *channel* B (mewakili warna biru) Berikut ini adalah tabel warna yang merupakan gabungan warna primer (Munir, R., 2008).

Tabel 1. Kode warna

Warna	Red	Green	Blue
Black	0	0	0
Blue	0	0	255
Green	0	255	0
Red	255	0	0
Cyan (Green + Blue)	0	255	255
Magenta (Red + Blue)	255	0	255
Yellow (Red + Green)	255	255	0
White (Red + Green + Blue)	255	255	255

Sumber : Munir, R., 2008

4. Pengolahan Citra

Agar citra yang mengalami gangguan mudah diinterpretasi (baik oleh manusia maupun mesin), maka citra tersebut perlu dimanipulasi menjadi citra lain yang kualitasnya lebih baik. Bidang studi yang menyangkut hal ini adalah pengolahan citra (*image processing*).

Pengolahan citra adalah pemrosesan citra, khususnya dengan menggunakan komputer, menjadi citra yang kualitasnya lebih baik. Sebagai contoh, citra burung nuri pada Gambar 2.4 (a) tampak agak gelap, lalu dengan operasi pengolahan citra kontrasnya diperbaiki sehingga menjadi lebih terang dan tajam (b). Umumnya, operasi-operasi pada pengolahan citra diterapkan pada citra bila :

1. perbaikan atau memodifikasi citra perlu dilakukan untuk meningkatkan kualitas penampakan atau untuk menonjolkan beberapa aspek informasi yang terkandung di dalam citra,
2. elemen di dalam citra perlu dikelompokkan, dicocokkan, atau diukur,
3. sebagian citra perlu digabung dengan bagian citra yang lain : (Munir, R., 2008).

(a) (b)

Gambar 4. (a) Citra Burung Nuri yang Agak Gelap

(b) Citra Burung yang Telah Diperbaiki Kontrasnya sehingga Terlihat Jelas & Tajam.

Sumber : Munir, R. 2008

Di dalam bidang komputer, sebenarnya ada tiga bidang studi yang berkaitan dengan data citra, namun tujuan ketiganya berbeda, yaitu:

1. Grafika Komputer (*computer graphics*).
2. Pengolahan Citra (*image processing*).
3. Pengenalan Pola (*pattern recognition/image interpretation*).

Pengubahan kontras citra seperti pada Gambar 5. adalah contoh operasi pengolahan citra. Contoh operasi pengolahan citra lainnya adalah penghilangan derau (*noise*) pada citra Lena. Citra Lena yang di sebelah kiri mengandung derau berupa bintik-bintik putih (derau). Dengan operasi penapisan (*filtering*), derau pada citra masukan ini dapat dikurangi sehingga dihasilkan citra Lena yang kualitasnya lebih baik (Munir, R., 2008).

(a) (b)

Gambar 5. (a) Citra Lena yang mengandung derau, (b) Hasil dari operasi penapisan derau

Sumber : Munir, R. 2008.

5. Steganografi Berbasis Intensitas RGB

Kata Steganografi berasal dari bahasa Yunani Steganos yang artinya tersembunyi atau terselubung. Steganograpi merupakan proses penyimpanan pesan rahasia berupa teks dan gambar dalam bentuk lain sehingga tidak mudah di ketahui oleh orang lain (Zam, 2013).

a. Skema Partisi

Pada algoritma ini, sebuah skema partisi didefinisikan sebagai deretan menurun secara monoton [a_i], i = 1 sampai 8. Asumsikan nilai warna dari sebuah *channel* adalah c. Kemudian *channel* tersebut dengan nilai c menyimpan i buah data bit jika c >= a_i, dan untuk semua j, j < i, c < a_j. Agar algoritma berjalan dengan benar, maka hanya digunakan skema partisi yang valid.

Sebuah skema partisi yang valid dapat didefinisikan sebagai berikut:

Anggap [a_i] adalah sebuah skema partisi dimana i buah bit yang lebih rendah dari a_i semuanya bernilai 0. Anggap [b_i], i = 1 sampai 8, adalah deretan lainnya, dimana b_i dihasilkan dengan mengubah semua nilai dari i buah bit yang lebih rendah dari a_i menjadi 1. Jika a_i > b_{i+1}, i = 1 sampai 7, maka [ai] adalah sebuah skema partisi yang valid. Kondisi sederhana ini memastikan bahwa jumlah data bit yang dibaca dari sebuah *channel* pada sisi penerima adalah sama dengan yang tersimpan pada sisi pengirim (Parvez, T. dan A.A.A. Gutub, 2008).

b. Algoritma Steganografi Berbasis Intensitas RGB

Ide di balik algoritma ini adalah bahwa untuk warna yang tidak signifikan, jumlah bit yang dapat diubah secara signifikan per *channel* dapat menjadi lebih banyak dari sebuah citra RGB. Gambar 3.4 menunjukkan salah satu contohnya. Pada (a) warna WHITE (R = 255, G = 255, B = 255). Pada (b) hanya diubah 4 bit terakhir dari R menjadi nol, menghasilkan sebuah warna dimana perubahan dapat kelihatan. Pada (c), komposisi warna adalah sama seperti (a), kecuali R = 55. Pada (d), kembali dilakukan perubahan 4 bit terakhir dari R menjadi 0, menghasilkan sebuah warna yang kelihatan hampir sama dengan (c).

Ide algoritma ini adalah bahwa nilai warna yang lebih rendah dari sebuah *channel* memiliki efek yang lebih rendah pada keseluruhan warna dari piksel dibandingkan dengan nilai warna yang lebih tinggi. Oleh karena itu, lebih banyak bit dapat diubah pada sebuah *channel* yang memiliki nilai ‘rendah’ darpiada sebuah *channel* yang memiliki nilai ‘tinggi’.

Oleh karena itu, algoritma ini dapat dijabarkan sebagai berikut:

1. Gunakan salah satu dari tiga *channel* sebagai indikator. Deretan indikator dapat dibuat acak, berdasarkan pada sebuah kunci yang digunakan bersama antara pengirim dan penerima.
2. Data disimpan pada salah satu dari dua *channel* selain indikator. *Channel* dengan nilai warna terendah diantara dua buah *channel* selain indikator akan menyimpan data pada *least significant bit*-nya.
3. Jumlah bit yang akan disimpan tergantung pada nilai warna dari *channel*. Semakin rendah nilai warna, maka semakin banyak data bit yang dapat disimpan. Oleh karena itu, diperlukan partisi dari nilai warna. Melalui eksperimen yang dilakukan oleh pengembang algoritma, diketahui bahwa partisi optimal tergantung pada citra sampul yang digunakan.
4. Untuk mengembalikan data, perlu untuk mengetahui *channel* mana yang menyimpan data bit. Hal ini dapat dilakukan dengan melihat *least significant bit* dari kedua *channel* selain indikator:
    a. Jika bit sama, maka *channel* yang mengikuti indikator pada urutan siklis menyimpan data.
    b. Jika bit tidak sama, *channel* yang mendahului indikator pada urutan siklis yang menyimpan data (Parvez, T. dan A.A.A. Gutub, 2008).

6. Paillier Cryptosystem

Paillier Cryptosystem yang ditemukan oleh Pascal Paillier pada tahun 1999 merupakan sebuah algoritma asimetris *probabilistic* untuk kriptografi kunci publik. Problema dari perhitungan n-*residue class* dipercaya sangat sulit untuk dikomputasi. Problema ini dikenal dengan asumsi *Composite Residuosity* (CR) dan merupakan dasar dari kriptosistem Paillier ini. Skema ini merupakan *additive homomorphic cryptosystem*, yang berarti bahwa diberikan kunci publik dan enkripsi dari m_1 dan m_2, seseorang akan mampu menghitung enkripsi dari $m_1 + m_2$.

a. Notasi yang Digunakan

Seperti pada algoritma RSA, diperlukan nilai n = pq dimana p dan q adalah bilangan prima besar. Selain itu, juga perlu dideklarasikan fungsi Totient dari Euler, $\phi(n) = (p - 1)(q - 1)$ dan fungsi Carmichael, $\lambda(n) = \text{lcm}(p - 1, q - 1)$.

Asumsikan $|\mathbb{Z}_{n^2}^*| = n\phi(n)$ maka untuk semua $w \in \mathbb{Z}_{n^2}^*$:

$$w^{\lambda} = 1 \bmod n$$

$$w^{n\lambda} = 1 \bmod n^2$$

Teorema ini dinamakan teorema Carmichael.

Sedangkan, sebuah bilangan z dikatakan sebagai residu modulo ke-n dari n^2 jika terdapat sebuah bilangan $y \in \mathbb{Z}_{n^2}^*$ sedemikian sehingga :

$$z = y^n \bmod n^2$$

Teorema ini dikenal dengan teorema *Composite Residuosity* (CR) yang menjadi dasar dari algoritma Paillier.

Sementara itu, jika diambil sebuah set $S_n = \{u < n^2 \mid u = 1 \bmod n\}$ yang merupakan sebuah subgrup perkalian dari integer modulo n^2 melalui sebuah fungsi L, maka persamaan berikut:

$$\forall u \in S_n \qquad L(u) = (u - 1) / n$$

b. Algoritma

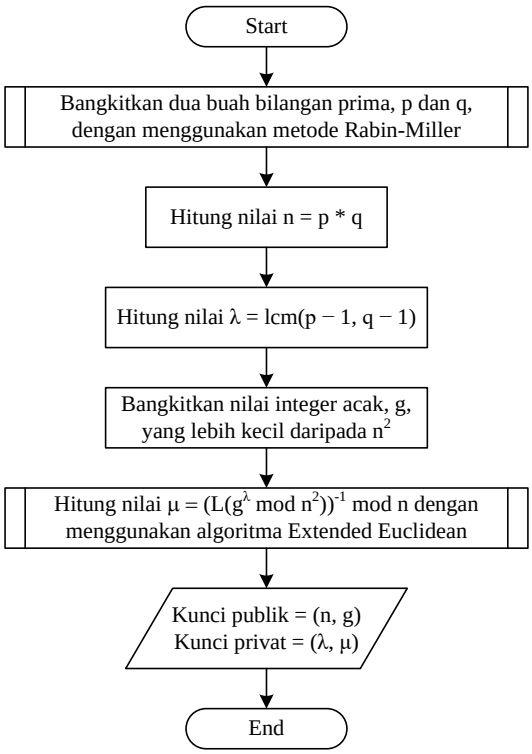
Algoritma dari skema ini dapat dirincikan sebagai berikut:

1. Proses Pembentukan Kunci
   a. Pilihlah dua buah bilangan prima besar p dan q secara acak dan unik.
   b. Hitung nilai n = pq dan λ = lcm(p − 1, q − 1).
   c. Pilih bilangan integer acak g dimana $g \in \mathbb{Z}_{n^2}^*$
   d. Pastikan n membagi *order* dari g dengan mengecek eksistensi dari invers perkalian modular berikut:

$$\mu = (L(g^{\lambda} \mod n^2))^{-1} \mod n$$

   dimana fungsi L didefinisikan sebagai:
   e. Kunci publik adalah (n, g).
   f. Kunci privat adalah (λ,μ).

Flowchart dari proses pembentukan kunci dapat dilihat pada gambar berikut:



Gambar 6. *Flowchart* Proses Pembentukan Kunci *Paillier cryptosystem*

Sumber : Menezes, A., van Oorschot, P. & Vanstone, S. 1996.

Agar dapat lebih memahami mengenai proses pembentukan kunci dari kriptosistem *Paillier* ini, maka diberikan sebuah contoh sederhana berikut ini:

a. Pilih dua buah bilangan prima besar, misalkan dipilih p = 19 dan q = 149.

b. Hitung nilai :

- $n = p * q$

  $= 19 * 149 = 2831$

- $\lambda = LCM(p - 1, q - 1)$

  $= LCM(18, 148)$

  $= 1332.$

c. Pilih sebuah *integer acak* g, dimana g berada dalam *range* nilai antara 0 sampai n^2. Agar memiliki nilai invers, maka nilai dari hasil fungsi L harus

relatif prima dengan nilai n. Selain itu, nilai dari operasi (g^{λ} mod n^2) mod n harus sama dengan 1. Agar lebih mudah memenuhi semua ketentuan di atas, pilihlah nilai g berupa bilangan prima. Misalkan dipilih g = 79.

d. Hitung nilai u, fungsi L dan μ :

- $u = g^{\lambda} \bmod n^2$

  $= 79^{1332} \bmod 2831^2$

  $= 3790710$

- $L(u) = (u - 1) / n$

  $= (3790710 - 1) / 2831$

  $= 1339$

- $\mu = 1339^{-1} \bmod 2831$

  $= 74$

e. Kunci privat : (λ,μ) = (1332, 74).

f. Kunci publik : (n, g) = (2831, 79).

2. Proses Enkripsi

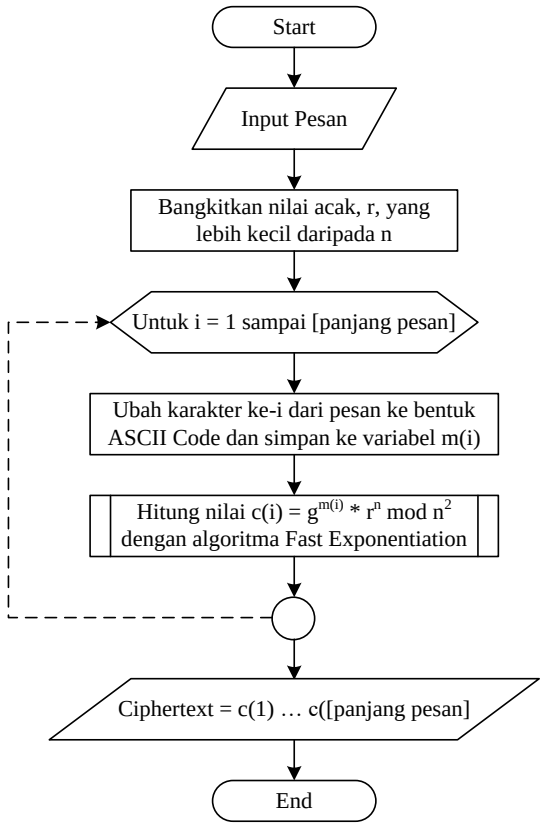
a. Misalkan m adalah pesan yang akan dienkripsikan dimana $m \in \mathbb{Z}_n$

b. Pilih nilai r dimana $r \in \mathbb{Z}_n^*$

c. Hitung *ciphertext* dengan rumusan berikut:

$$c = g^m \cdot r^n \mod n^2$$

Flowchart dari proses enkripsi dapat dilihat pada gambar berikut:



Gambar 7. *Flowchart* Proses Enkripsi *Paillier cryptosystem.*

Sumber : Menezes, A., van Oorschot, P. & Vanstone, S. 1996.

Agar dapat lebih memahami mengenai proses enkripsi dari kriptosistem *Paillier* ini, maka diberikan sebuah contoh sederhana berikut ini dimana kunci publik yang diperlukan diambil dari contoh perhitungan proses pembentukan kunci di atas:

a. Misalkan pesan m = ‘A’, dengan nilai ASCII Code = 65.
b. Pilih nilai r, dengan ketentuan nilai r harus lebih kecil daripada n dan tidak boleh sama dengan nilai p dan q. Selain itu nilai r harus relatif prima terhadap n. Agar lebih mudah, pilih nilai r berupa bilangan prima. Misalkan r = 31.
c. Hitung *ciphertext* dengan rumusan berikut:

   $c = g^m . r^n \bmod n^2$

$= 79^{65} \cdot 31^{2831} \bmod 2831^2$

$= 686094$

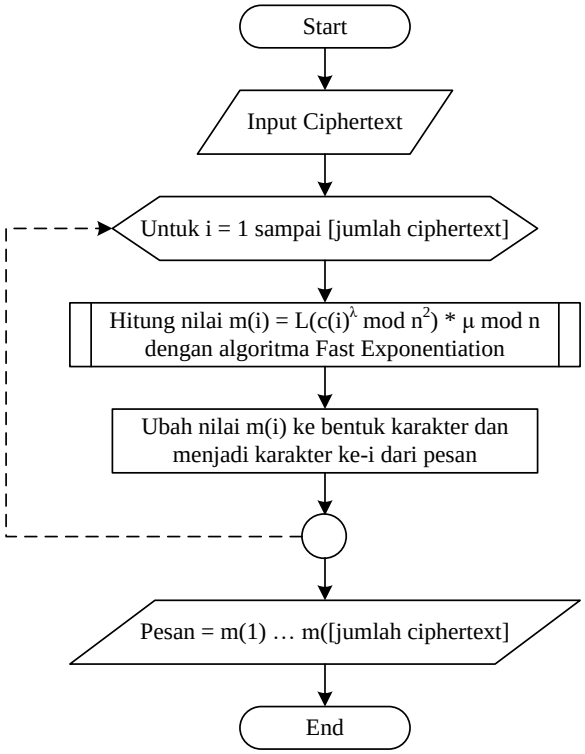
3. Proses Dekripsi

a. Misalkan c adalah *ciphertext* dimana $c \in \mathbb{Z}_{n^2}^*$

b. Hitung pesan dengan rumusan berikut:

$$m = L(c^{\lambda} \mod n^2) \cdot \mu \mod n$$

Flowchart dari proses dekripsi dapat dilihat pada gambar berikut:



Gambar 8. *Flowchart* Proses Dekripsi *Paillier cryptosystem.*

Sumber : Menezes, A., van Oorschot, P. & Vanstone, S. 1996.

Agar dapat lebih memahami mengenai proses dekripsi dari kriptosistem *Paillier* ini, maka diberikan sebuah contoh sederhana berikut ini dimana kunci privat yang diperlukan diambil dari contoh perhitungan proses pembentukan kunci di atas dan nilai *ciphertext* diambil dari proses enkripsi di atas :

a. Nilai *cipher* = 686094.

b. Hitunglah nilai u dan m :

- $u = c^{\lambda} \bmod n^2 = 686094^{1332} \bmod 2831^2 = 5959256$
- $L(u) = (5959256 - 1) / 2831 = 2105$
- $m = 2105 * 74 \bmod 2831 = 65$ → karakter 'A'

7. MSE

Proses pengujian akan menggunakan rumusan MSE (*Mean Square Error*). MSE dapat secara langsung merefleksikan perbedaan kualitas diantara dua buah citra digital. MSE digunakan sebagai standar untuk menghitung kualitas dari dua buah citra digital yang di-*decode*. MSE diantara dua buah citra dapat dihitung dengan menggunakan rumusan berikut:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M} \sum_{j=0}^{N} \left(P_1(i,j) - P_2(i,j) \right)^2$$

Disini, M, N adalah lebar dan tinggi dari citra digital, $P_1(i, j)$ adalah nilai piksel dari citra digital asli dan $P_2(i, j)$ adalah nilai piksel dari citra digital ter-*decode*.

Dalam penelitian ini, P_1 akan merupakan nilai piksel dari pengujian 1 dan P_2 akan merupakan nilai piksel dari pengujian 2. Biasanya, jika nilai MSE ≥ 30 db, maka kualitas perbedaan antara dua buah citra digital dikatakan bagus (Zhu Liehuang, Li Wenzhou, Liao Lejian dan Li Hong, 2006).

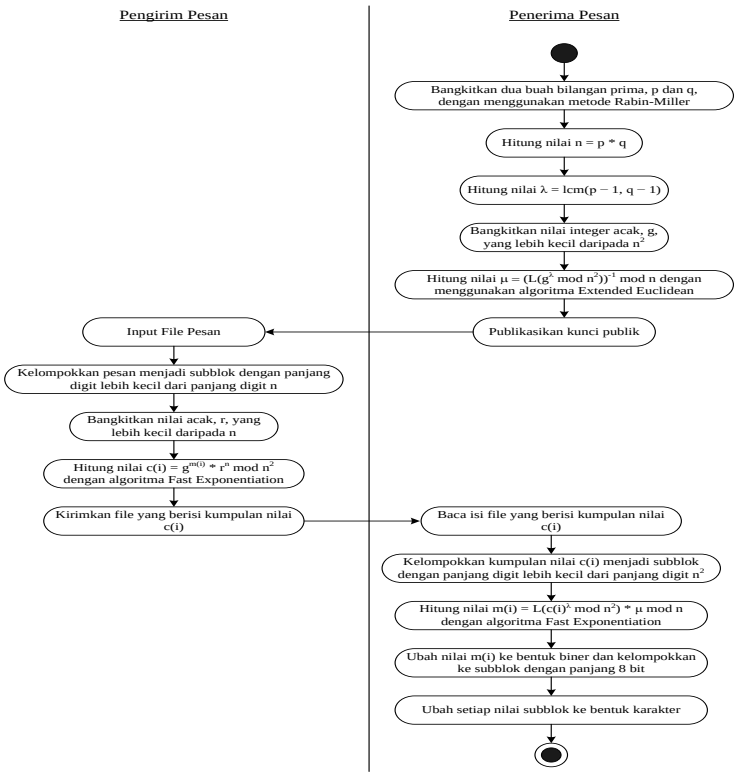
BAB III

ANALISIS DAN PERANCANGAN

1. Analisis

Sebelum melakukan perancangan sebuah sistem untuk menyelesaikan suatu permasalahan, terlebih dahulu harus dilakukan analisis terhadap sistem tersebut, untuk mendeskripsikan alur kerja dari proses yang terdapat dalam sistem, merumuskan prasyarat desain sistem dan pemodelan sistem.

a. Analisis Proses



Gambar 9. *Activity Diagram* dari Metode Paillier

Sumber : Munir, R. 2006.

Metode Paillier merupakan sebuah algoritma asimetris *probabilistic* untuk kriptografi kunci publik. Metode Paillier ini menggunakan konsep dari problema

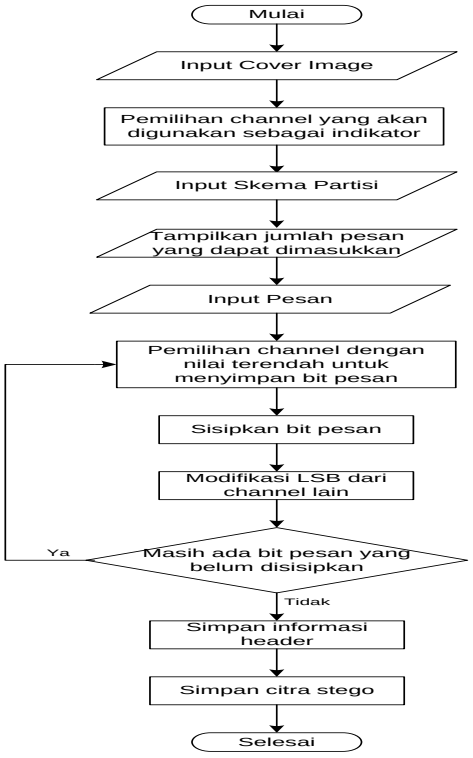
perhitungan n-*residue class* yang dikenal dengan asumsi *Composite Residuosity* (CR).

Agar dapat lebih memahami mengenai prosedur kerja dari metode Paillier, maka diberikan sebuah *activity diagram* yang menjelaskan prosedur kerja dari Metode Paillier, seperti terlihat pada gambar 10. Sementara itu, steganografi citra RGB merupakan suatu konsep untuk menyisipkan suatu data ke dalam citra sehingga informasi data tersebut tersembunyi dan hanya pihak yang berhak yang dapat mengekstraksi keluar informasi tersebut. Dalam proses kerja steganografi citra RGB, terdapat dua buah proses yaitu proses *encoding* dan proses *decoding*.

Gambar 10. menunjukkan proses *encoding* pada sisi pengirim bentuk *flowchart*. Perlu dicatat bahwa diasumsikan bahwa kunci yang digunakan bersama dan skema partisi telah disepakati antara kedua pihak.

Seperti terlihat pada *flowchart* bagian *encoding* dari algoritma pada gambar 10, proses kerja akan dimulai dari proses penginputan *cover image* dan penentuan skema partisi yang akan digunakan. Skema partisi ini akan digunakan untuk menentukan jumlah bit yang dapat disisipkan ke dalam sebuah piksel pada citra. Setelah itu, proses dilanjutkan dengan penentuan *channel* yang akan digunakan sebagai indikator. Kemudian proses dilanjutkan pengisian *file* pesan yang akan disisipkan. Panjang pesan yang dapat disisipkan telah ditentukan pada saat pengisian partisi diatas, sehingga pengisian pesan tidak dapat melebihi panjang yang telah ditentukan tersebut. Proses akan dilanjutkan dengan memilih *channel* yang memiliki nilai terendah selain *channel* indikator untuk menyimpan bit pesan.

Setelah itu, maka akan digunakan skema partisi untuk menentukan jumlah bit yang dapat disimpan dalam *channel* tersebut. Kemudian, sisipkan sejumlah bit pesan ke dalam *channel* tersebut dan modifikasi LSB dari *channel* lainnya sesuai dengan ketentuan dari algoritma. Proses diatas akan diulangi hingga semua bit pesan ditempelkan pada citra sampul. Setelah semua proses selesai, maka harus disisipkan juga informasi *header* yang berisi jumlah piksel yang akan dibaca.



Gambar 10. *Flowchart* dari Proses *Encoding*

Sumber : Munir, R. 2006.

Agar dapat lebih memahami mengenai prosedur kerja dari proses *encoding*, maka diberikan sebuah contoh sederhana berikut ini:

Misalkan terdapat sebuah citra berukuran 2 x 3 dengan perincian warna piksel sebagai berikut:

R = 115, G = 135 dan B = 141	R = 72, G = 35 dan B = 81	R = 72, G = 35 dan B = 81
R = 82, G = 45 dan B = 91	R = 182, G = 145 dan B = 141	R = 95, G = 135 dan B = 101

Pesan yang akan disisipkan adalah M (ASCII Code = 77 = 0100 1101) dan skema partisi yang digunakan adalah ‘256, 256, 256, 256, 0, 0, 0, 0’, maka proses kerjanya adalah sebagai berikut:

1. Proses pembacaan piksel selalu dimulai dari kiri atas ke kanan bawah, yaitu mulai dari kiri ke kanan dan dari atas ke bawah.
2. Piksel pertama dan kedua selalu digunakan sebagai *header* untuk menyimpan informasi jumlah piksel yang digunakan untuk melakukan penyisipan data, sehingga tidak boleh disisipkan data pesan. Hal ini dikarenakan proses pembacaan selalu dimulai dari kiri atas, dan pada saat awal proses, harus diketahui terlebih dahulu jumlah piksel yang harus dibaca. Hal inilah yang menjadi alasan pemilihan piksel pertama dan kedua sebagai *header*. Sesuai dengan proses pembacaan piksel citra yang dimulai dari kiri ke kanan dan dari atas ke bawah, maka proses dilanjutkan dengan membaca piksel berikutnya, yaitu piksel ketiga pada citra yang terletak di sebelah kanan dari piksel pertama dan kedua.
3. Skema partisi yang digunakan adalah ‘256, 256, 256, 256, 0, 0, 0, 0’, maka proses penentuan jumlah bit yang dapat disisipkan dalam setiap piksel pada citra adalah sebagai berikut:

a. Nilai pertama yaitu 256, merupakan nilai yang lebih besar daripada nilai terbesar piksel citra yaitu 255, sehingga maka jumlah bit yang disisipkan adalah 1 bit.
b. Proses dilanjutkan dengan mengecek nilai kedua yaitu 256, yang merupakan nilai yang lebih besar daripada nilai terbesar piksel citra yaitu 255, maka jumlah bit yang dapat disisipkan ditambah satu menjadi 2 bit.
c. Proses dilanjutkan dengan mengecek nilai ketiga yaitu 256, yang merupakan nilai yang lebih besar daripada nilai terbesar piksel citra yaitu 255, maka jumlah bit yang dapat disisipkan ditambah satu menjadi 3 bit.
d. Proses dilanjutkan dengan mengecek nilai keempat yaitu 256, yang merupakan nilai yang lebih besar daripada nilai terbesar piksel citra yaitu 255, maka jumlah bit yang dapat disisipkan ditambah satu menjadi 4 bit.
e. Proses dilanjutkan dengan mengecek nilai kelima yaitu 0, yang merupakan nilai terkecil dari warna piksel, sehingga tidak dapat disisipkan bit pesan lagi. Proses dihentikan.

4. Proses kerja untuk piksel 3:
   a. *Channel* yang dipilih sebagai indikator dapat ditentukan secara acak. Channel yang dipilih sebagai *indikator* hanya diketahui oleh pengirim dan penerima. Misalkan *channel* yang dipilih sebagai indikator adalah G.
   b. Nilai terendah selain indikator adalah R = 72, maka R dipilih untuk menyimpan bit pesannya.
   c. R = 72 = 0100 1000. Bit akan disisipkan di LSB-nya. LSB dari R adalah 1000, sedangkan bit yang akan disisipkan adalah 0100, maka ganti LSB

dari R dengan bit yang akan disisipkan, sehingga R menjadi 0100 0100 = 68

d. Sekarang bit terakhir dari R adalah 0 dan bit terakhir dari B adalah 1. Karena pada contoh ini, digunakan *channel* R yang mendahului indikator G untuk menyimpan data, maka kedua bit lainnya tidak boleh sama. Ketentuan ini telah terpenuhi untuk piksel ini.

e. Hasil yang diperoleh adalah :

   R = 68 G = 35 B = 81

5. Proses kerja untuk piksel 4:

   a. Misalkan *channel* yang dipilih sebagai indikator adalah G.

   b. Nilai terendah selain indikator adalah R = 82, maka R dipilih untuk menyimpan bit pesannya.

   c. R = 82 = 0101 0010. Bit akan disisipkan di LSB-nya. LSB dari R adalah 0010, sedangkan bit yang akan disisipkan adalah 1101, maka ganti LSB dari R dengan bit yang akan disisipkan, sehingga R menjadi 0101 1101 = 93

   d. Sekarang bit terakhir dari R adalah 1 dan bit terakhir dari B adalah 1. Karena pada contoh ini, digunakan *channel* R yang mendahului indikator G untuk menyimpan data, maka kedua bit lainnya tidak boleh sama. Karena bit R menyimpan data, maka tidak boleh diubah lagi. Oleh karena itu, bit terakhir dari B diubah menjadi 0, sehingga diperoleh B = 0101 1010 = 90

   e. Hasil yang diperoleh adalah :

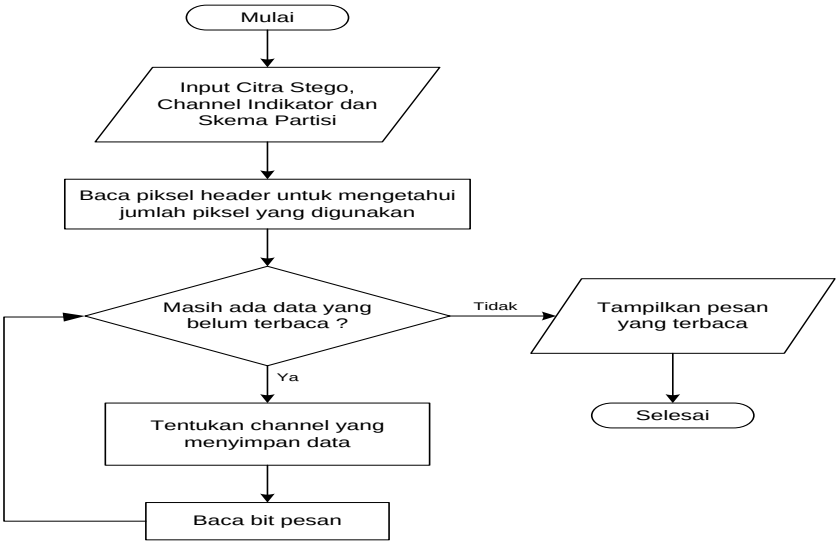
      R = 93 G = 45 B = 90

6. Setelah selesai melakukan penyisipan data, langkah terakhir adalah melakukan proses penyisipan data *header*. Jumlah piksel yang digunakan adalah 2 buah, maka data 0000 0000 0000 0000 0000 0010 harus disisipkan sebagai *header*. Data tersebut akan dimasukkan pada piksel 1 dan 2. Langkahnya adalah sebagai berikut:
   a. Setiap *channel* pada piksel 1 dan piksel 2 akan disisipkan bit tersebut.
   b. Nilai R = 115 = 0111 0011. LSB-nya = 0011 diubah menjadi 0000, sehingga nilai R menjadi 0111 0000 = 112.
   c. Nilai G = 135 = 1000 0111. LSB-nya = 0111 diubah menjadi 0000, sehingga nilai G menjadi 1000 0000 = 128.
   d. Nilai B = 141 = 1000 1101. LSB-nya = 1101 diubah menjadi 0000, sehingga nilai B menjadi 1000 0000 = 128.
   e. Nilai R = 68 = 0100 0100. LSB-nya = 0100 diubah menjadi 0000, sehingga nilai R menjadi 0100 0000 = 64.
   f. Nilai G = 35 = 0010 0011. LSB-nya = 0011 diubah menjadi 0000, sehingga nilai G menjadi 0010 0000 = 32.
   g. Nilai B = 81 = 0101 0001. LSB-nya = 0001 diubah menjadi 0010, sehingga nilai B menjadi 0101 0010 = 82.

Nilai warna piksel untuk citra hasil:

R = 112, G = 128 dan B = 128	R = 64, G = 32 dan B = 82	R = 68, G = 35 dan B = 81
R = 93, G = 45 dan B = 90	R = 182, G = 145 dan B = 141	R = 95, G = 135 dan B = 101

Gambar 11. menunjukkan proses *decoding* pada sisi penerima dalam bentuk *flowchart*. Perlu dicatat bahwa diasumsikan bahwa kunci yang digunakan bersama dan skema partisi telah disepakati antara kedua pihak.



Gambar 11. *Flowchart* dari Proses *Decoding*

Sumber : Munir, R. 2006.

Berdasarkan gambaran *flowchart* pada gambar diatas, diketahui bahwa proses *decoding* dimulai pembacaan deretan indikator dan jumlah piksel yang digunakan untuk menyimpan pesan. Kemudian, proses dilanjutkan dengan penentuan *channel* mana yang menyimpan data. Setelah itu, proses dilanjutkan dengan pembacaan data bit yang disisipkan pada piksel citra. Setelah semua piksel terbaca, maka akan diperoleh deretan bit pesan yang akan dikelompokkan menjadi subblok berukuran 8 bit dan diubah ke bentuk bilangan desimal yang merupakan ASCII Code dari karakter pesan.

Agar dapat lebih memahami mengenai prosedur kerja dari proses *decoding*, maka diberikan sebuah contoh sederhana berikut ini:

Nilai warna piksel untuk citra hasil:

Tabel

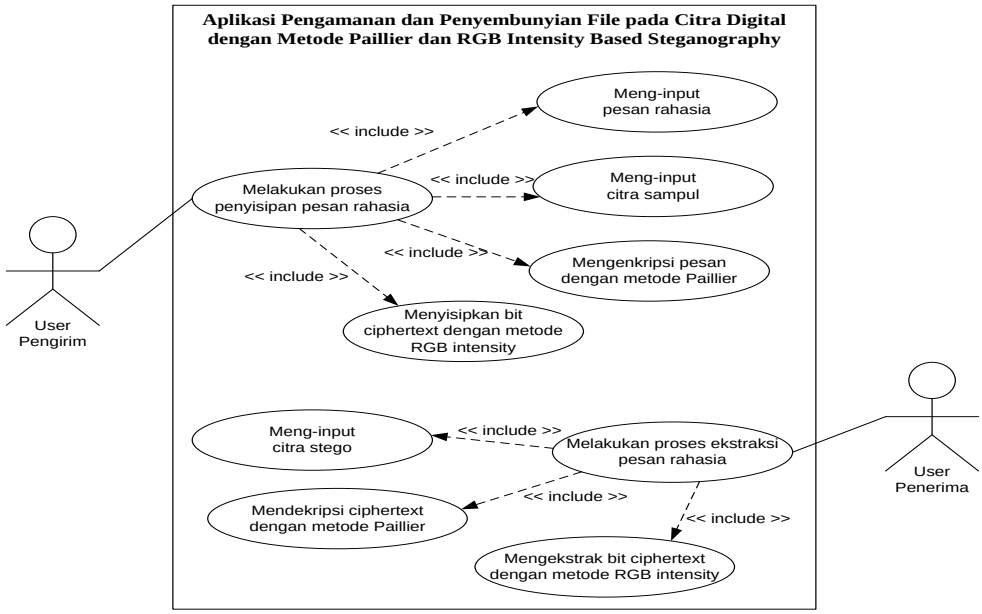
R = 112, G = 128 dan B = 128	R = 64, G = 32 dan B = 82	R = 68, G = 35 dan B = 81
R = 93, G = 45 dan B = 90	R = 182, G = 145 dan B = 141	R = 95, G = 135 dan B = 101

1. Lacak jumlah piksel yang digunakan untuk melakukan penyisipan bit pesan. Nilai tersebut dapat diketahui dari LSB piksel pertama dan piksel kedua. Langkah kerjanya adalah sebagai berikut:
   a. Ambil 4 bit LSB dari semua *channel* warna pada piksel pertama dan piksel kedua.
   b. Nilai R = 112 = 0111 0000. LSB-nya = 0000.
   c. Nilai G = 128 = 1000 0000. LSB-nya = 0000.
   d. Nilai B = 128 = 1000 0000. LSB-nya = 0000.
   e. Nilai R = 64 = 0100 0000. LSB-nya = 0000.
   f. Nilai G = 32 = 0010 0000. LSB-nya = 0000.
   g. Nilai B = 82 = 0101 0010. LSB-nya = 0010.
   h. Bit yang diperoleh : 0000 0000 0000 0000 0000 0010 = 2. Hal ini berarti 2 buah piksel digunakan untuk menyimpan data.
2. *Channel* yang digunakan sebagai indikator telah disepakati bersama antara pengirim dan penerima, yaitu *channel* G. Oleh karena itu, *channel* yang digunakan untuk menyimpan bit pesan adalah *channel* R atau *channel* B.

3. Skema partisi yang digunakan telah disepakati bersama antara pengirim dan penerima,skema partisi yang digunakan adalah ‘256, 256, 256, 256, 0, 0, 0, 0’
4. Piksel ketiga memiliki nilai R dan B yang berbeda tipenya (R berupa bilangan genap dan B berupa bilangan ganjil). Sesuai ketentuan algoritma, apabila bit terakhir dari R dan B tidak sama, maka *channel* yang mendahului *channel* indikator yang menyimpan data. Karena bit terakhir dari nilai R dan B pada piksel kedua tidak sama, maka *channel* R yang mendahului *channel* G yang menyimpan data. Nilai R = 68 = 0100 0100. Bit pesan merupakan LSB dari nilai R yaitu 0100.
5. Karena jumlah piksel yang digunakan untuk menyimpan bit pesan ada dua buah, maka proses dilanjutkan untuk piksel keempat. Piksel keempat memiliki nilai R dan B yang berbeda tipenya (R berupa bilangan ganjil dan B berupa bilangan genap). Sesuai ketentuan algoritma, apabila bit terakhir dari R dan B tidak sama, maka *channel* yang mendahului *channel* indikator yang menyimpan data. Karena bit terakhir dari nilai R dan B pada piksel keempat tidak sama, maka *channel* R yang mendahului *channel* G yang menyimpan data. Nilai dari *channel* R adalah 93 = 0101 1101. Bit pesan merupakan LSB dari nilai R yaitu 1101.
6. Bit pesan yang diperoleh adalah 0100 1101 = 77 yang merupakan ASCII Code dari karakter ‘M’.

b. Pemodelan Sistem

Aplikasi Pengamanan dan Penyembunyian File pada Citra Digital dengan Metode Paillier dan RGB Intensity Based Steganography ini dapat dimodelkan dengan menggunakan *use case diagram* seperti terlihat pada gambar berikut:



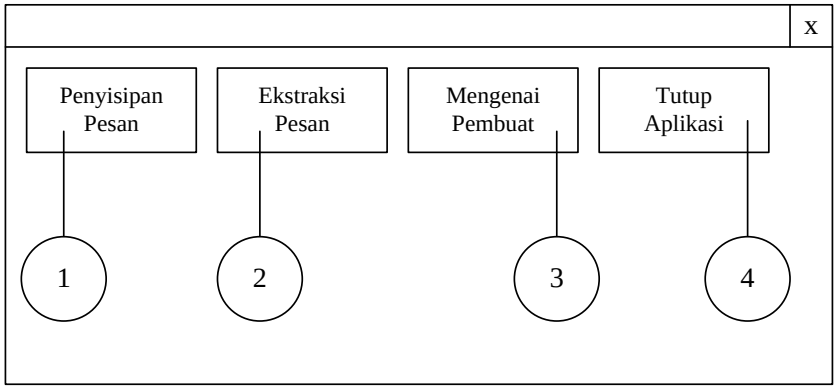
Gambar 12. *Use Case* Diagram dari Sistem

Sumber : Munir, R. 2008.

c. Perancangan

1. Form 'Main'

Form ini merupakan *form* inti dari perangkat lunak yang berfungsi untuk menghubungkan *form-form* yang ada pada perangkat lunak. Rancangan tampilan dari *form* 'Main' ini dapat dilihat pada gambar 3.6 berikut:



Gambar 13. Rancangan *Form* 'Main'

Sumber : Sumber : Munir, R. 2008.

Keterangan :

1 : *Button* ’Penyisipan Pesan’, yang berfungsi untuk menampilkan *form* Penyisipan.

2 : *Button* ’Ekstraksi Pesan’, yang berfungsi untuk menampilkan *form* Ekstraksi.

3 : *Button* ’Mengenai Pembuat’, yang berfungsi untuk menampilkan *form* Mengenai.

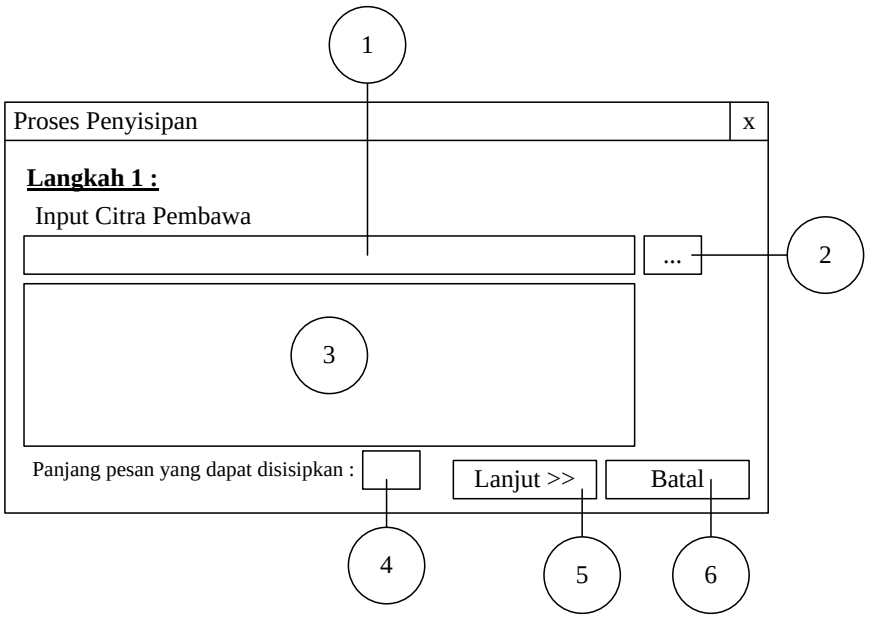
4 : *Button* ’Tutup Aplikasi’, yang berfungsi untuk menutup aplikasi.

***2. Form* ‘Penyisipan’**

Form ini berfungsi untuk melakukan penyisipan pesan rahasia ke dalam sebuah citra sampul. Rincian dari proses penyisipan adalah sebagai berikut:

a. Input Citra Pembawa

Rancangan tampilan dari *form* ‘Penyisipan – Input Citra Pembawa’ dapat dilihat pada gambar 3.7 berikut:



Gambar 14. Rancangan *Form* ‘Penyisipan – Input Citra Pembawa’

Sumber : Sumber : Munir, R. 2008.

Keterangan :

1 : *Label*, yang berisi lokasi dari *file* citra pembawa yang dipilih.

2 : *Button*, berfungsi untuk menampilkan kotak dialog *open* sebagai tempat pemilihan *file* citra pembawa yang diinginkan.

3 : *Picturebox*, digunakan untuk menampilkan gambar citra pembawa yang dipilih.

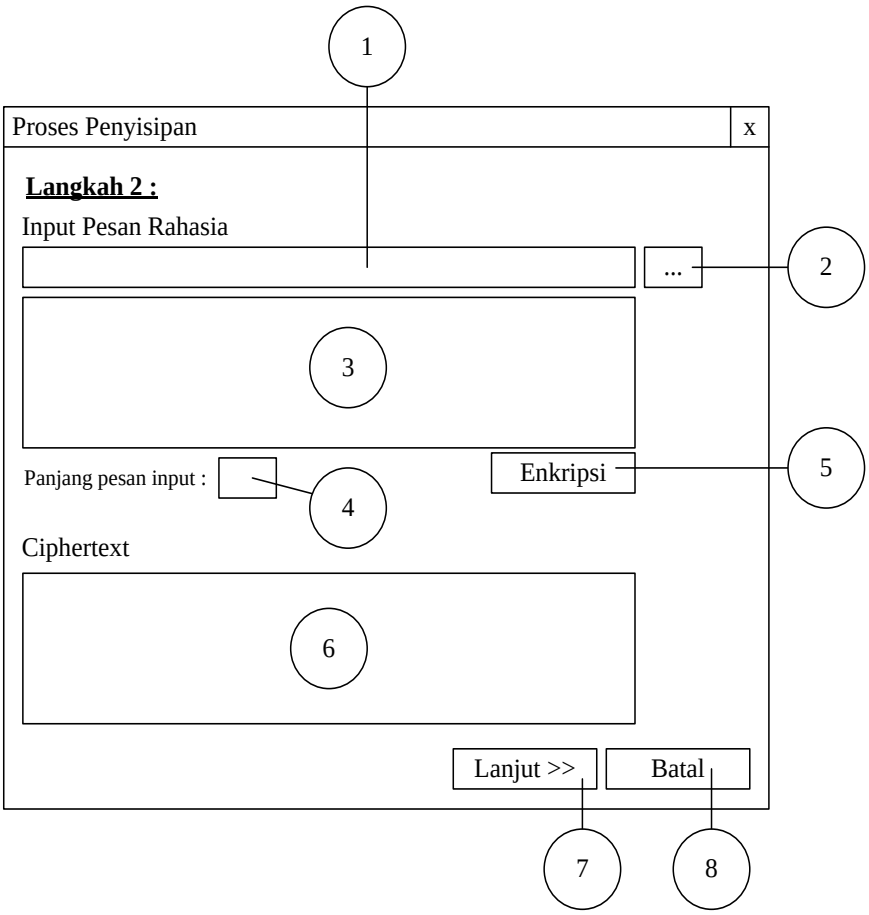
4 : *Label*, yang berfungsi untuk menampilkan total panjang pesan yang dapat disisipkan pada citra pembawa.

5 : *Button* ’Lanjut’, yang berfungsi untuk melanjutkan ke langkah berikutnya, yaitu input pesan rahasia dan enkripsi.

6 : *Button* ’Keluar’, yang berfungsi untuk menutup *form* dan kembali ke *form* ’Main’.

7. Input Pesan Rahasia dan Enkripsi

   Rancangan tampilan dari *form* ‘Penyisipan – Input Pesan Rahasia dan Enkripsi’ dapat dilihat pada gambar 3.8 berikut:



Gambar 15. Rancangan *Form* 'Penyisipan – Input Pesan Rahasia dan Enkripsi'

Sumber : Munir, R. 2008.

Keterangan :

1 : *Label*, yang berisi lokasi dari *file* pesan rahasia yang dipilih.

2 : *Button*, berfungsi untuk menampilkan kotak dialog *open* sebagai tempat pemilihan *file* pesan rahasia yang diinginkan.

3 : *Richtextbox*, digunakan untuk menampilkan isi *file* pesan rahasia ataupun sebagai tempat pengisian pesan rahasia.

4 : *Label*, yang berfungsi untuk menampilkan total panjang pesan yang dimasukkan.

5 : *Button* ’Enkripsi’, yang berfungsi untuk melakukan proses enkripsi terhadap pesan rahasia yang dimasukkan.

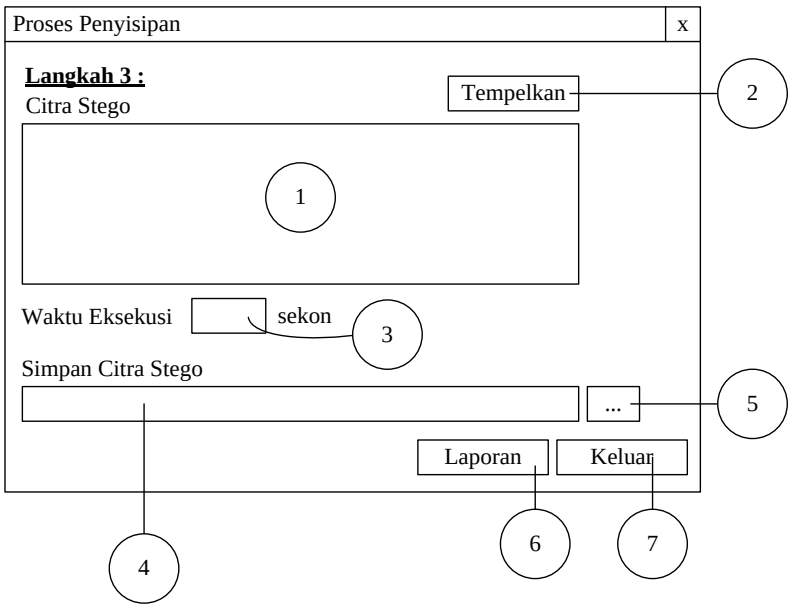
6 : *Richtextbox,* digunakan untuk menampilkan hasil enkripsi terhadap pesan rahasia.

7 : *Button* ’Tempelkan’, yang berfungsi untuk melanjutkan ke langkah berikutnya, yaitu tempelkan *ciphertext* ke citra pembawa.

8 : *Button* ’Keluar’, yang berfungsi untuk menutup *form* dan kembali ke *form* ’Main’.

8. Tempelkan *Ciphertext* ke Citra Pembawa

Rancangan tampilan dari *form* ‘Penyisipan – Tempelkan *Ciphertext* ke Citra Pembawa’ dapat dilihat pada gambar 3.9 berikut:



Gambar 16. Rancangan *Form* ‘Penyisipan – Tempelkan *Ciphertext* ke Citra Pembawa’

Sumber : Munir, R. 2008.

Keterangan :

1 : *Picturebox*, digunakan untuk menampilkan gambar citra stego yang dihasilkan.

2 : *Button*, berfungsi untuk melakukan proses penempelan *ciphertext* ke citra pembawa.

3 : *Label*, berfungsi untuk menampilkan waktu eksekusi dari proses penyisipan.

4 : *Label*, yang berisi lokasi dari *file* citra stego yang dipilih.

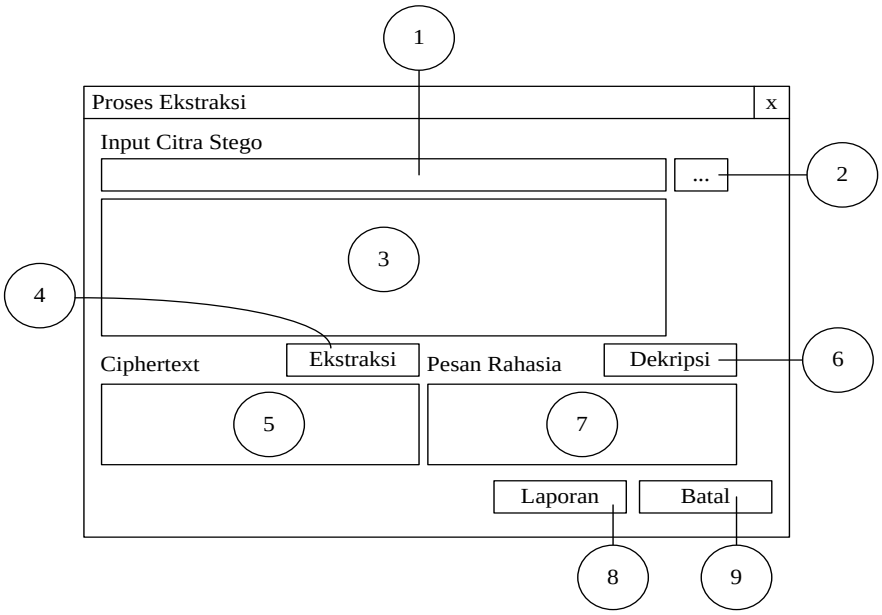
5 : *Button*, berfungsi untuk menampilkan kotak dialog *save* sebagai tempat pemilihan *file* citra stego.

6 : *Button* ’Laporan’, yang berfungsi untuk menampilkan detail perhitungan dari proses penyisipan.

7 : *Button* ’Keluar’, yang berfungsi untuk menutup *form* dan kembali ke *form* ’Main’.

***3. Form* ‘Ekstraksi’**

Form ini berfungsi untuk melakukan ekstraksi pesan rahasia dari citra stego. Rancangan tampilan dari *form* ‘Ekstraksi’ dapat dilihat pada gambar 3.10:



Gambar 17. Rancangan *Form* ‘Ekstraksi’

Keterangan :

1 : *Label*, yang berisi lokasi dari *file* citra stego yang dipilih.

2 : *Button*, berfungsi untuk menampilkan kotak dialog *open* sebagai tempat pemilihan *file* citra stego yang diinginkan.

3 : *Picturebox*, digunakan untuk menampilkan gambar citra stego yang dihasilkan.

4 : *Button*, berfungsi untuk mengektrak *ciphertext* keluar dari citra stego.

5 : *Richtextbox*, digunakan untuk menampilkan *ciphertext* yang terekstrak keluar.

6 : *Button*, berfungsi untuk mendekripsi *ciphertext* terekstrak.

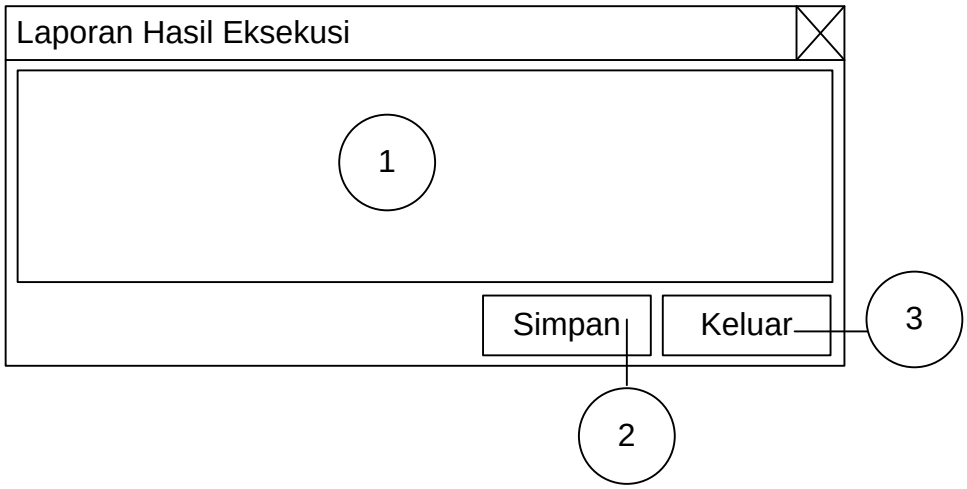
7 : *Richtextbox*, digunakan untuk menampilkan pesan rahasia hasil dekripsi.

8 : *Button* ’Laporan’, yang berfungsi untuk menampilkan detail perhitungan dari proses ekstraksi.

9 : *Button* ’Batal’, yang berfungsi untuk menutup *form* dan kembali ke *form* ’Main’.

***4. Form* ‘Laporan Hasil Eksekusi’**

Form ‘Laporan Hasil Eksekusi’ berfungsi untuk menampilkan perincian hasil eksekusi dari pencarian citra. Rancangan tampilan dari *form* ‘Laporan Hasil Eksekusi’ dapat dilihat pada Gambar 18:



Gambar 18. Rancangan Form Laporan Hasil Eksekusi

Keterangan :

1 : *RichTextBox,* yang berfungsi untuk menampilkan laporan hasil eksekusi.

2 : *Button* ’Simpan’, yang berfungsi untuk menyimpan laporan hasil eksekusi.

3 : *Button* ’Keluar’, yang berfungsi untuk menutup *form.*

BAB IV

IMPLEMENTASI PERANGKAT LUNAK

1. Spesifikasi Perangkat Keras dan Perangkat Lunak

Untuk menjalankan sistem yang dirancang, diperlukan beberapa faktor pendukung sebagai berikut :

a. Kebutuhan Perangkat Keras (*Hardware*)

Untuk bisa menjalankan sistem, maka *hardware* yang direkomendasikan adalah satu set lengkap perangkat komputer yang memiliki spesifikasi sebagai berikut:

1. Intel Core 2 Duo Processor T6600.
2. RAM 1 GB
3. Harddisk 160 GB
4. Monitor 14,0 HD LED LCD

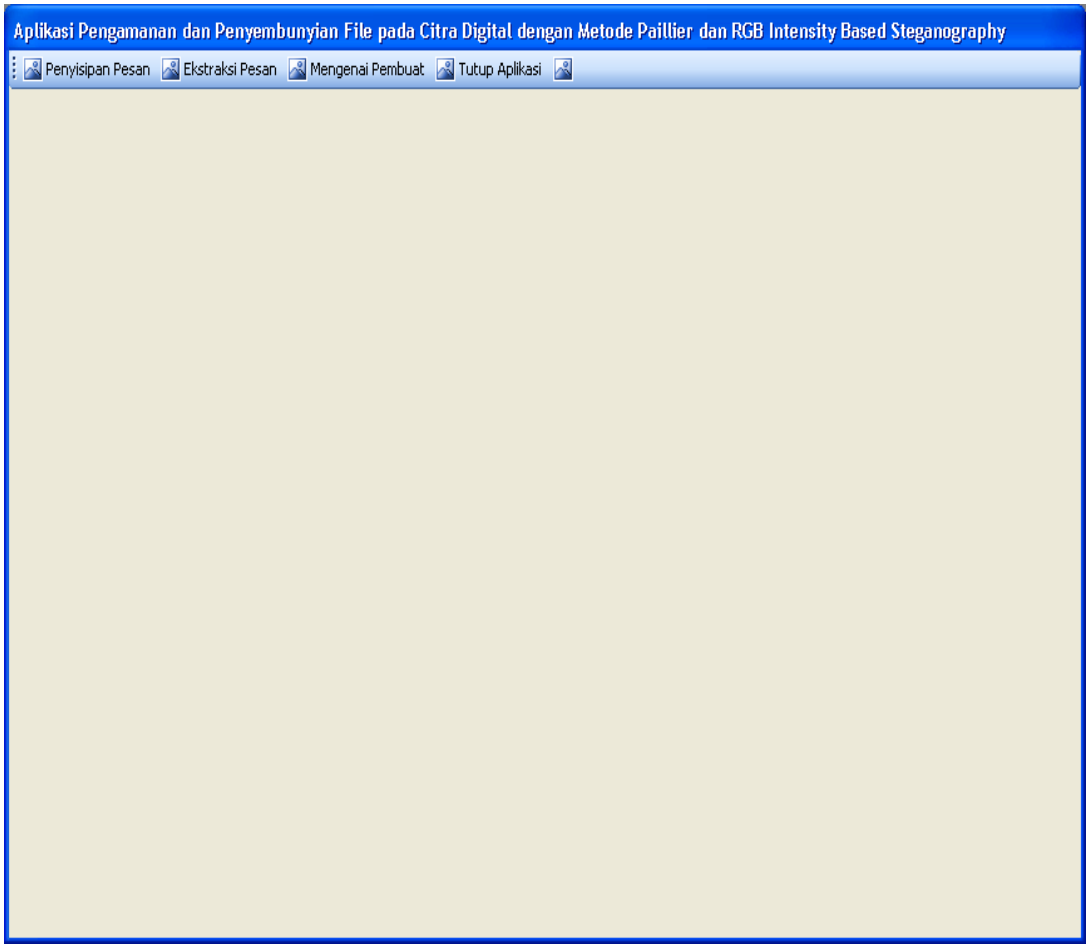
b. Kebutuhan Perangkat Lunak (*Software*)

Adapun perangkat lunak untuk menjalankan program ini adalah:

1. Sistem operasi Windows 98/2000/Me/XP ke atas.
2. *Microsoft.NET Framework* 3.5 untuk menjalankan program.

2. Hasil

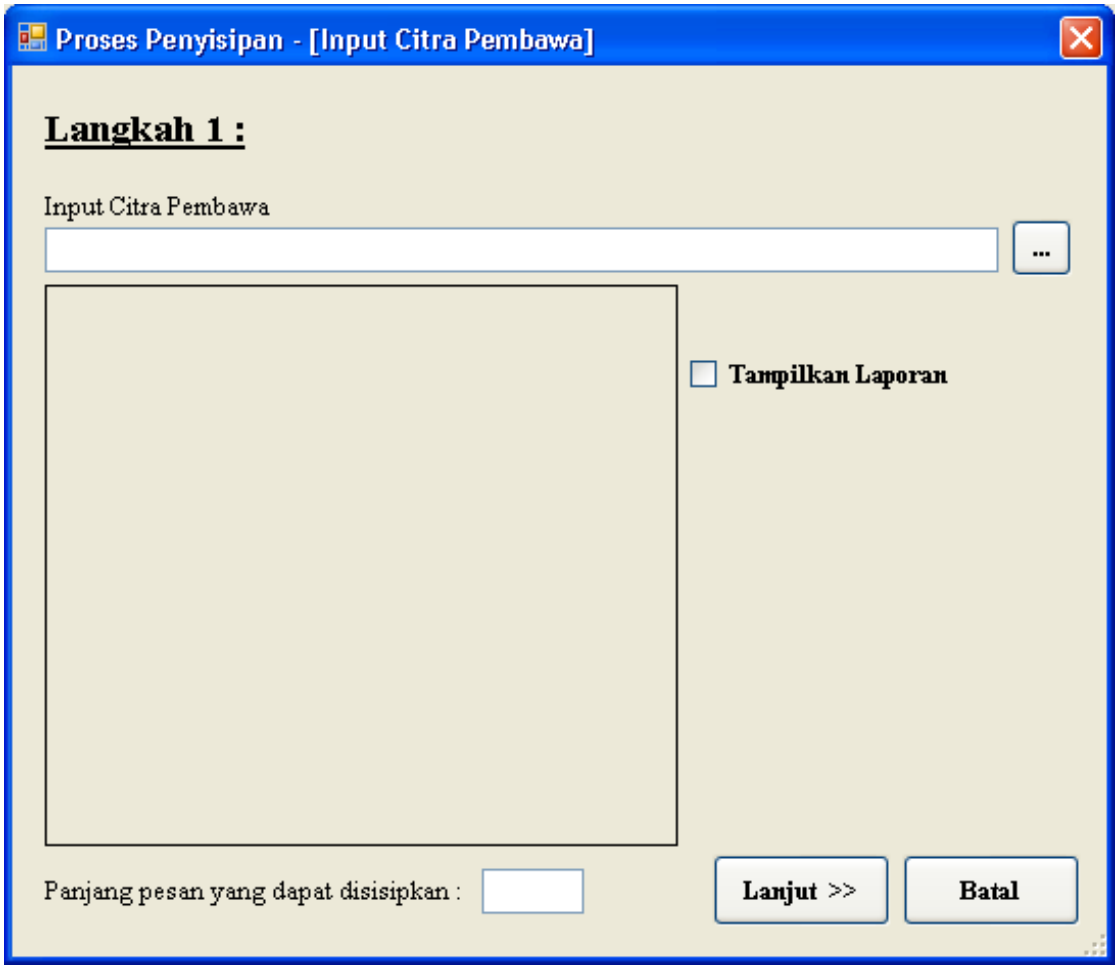
Untuk menggunakan perangkat lunak ini, jalankan *file* ”12SquareStego.exe”, maka akan ditampilkan tampilan utama dari program seperti terlihat pada gambar berikut:



Gambar 19. Tampilan Utama

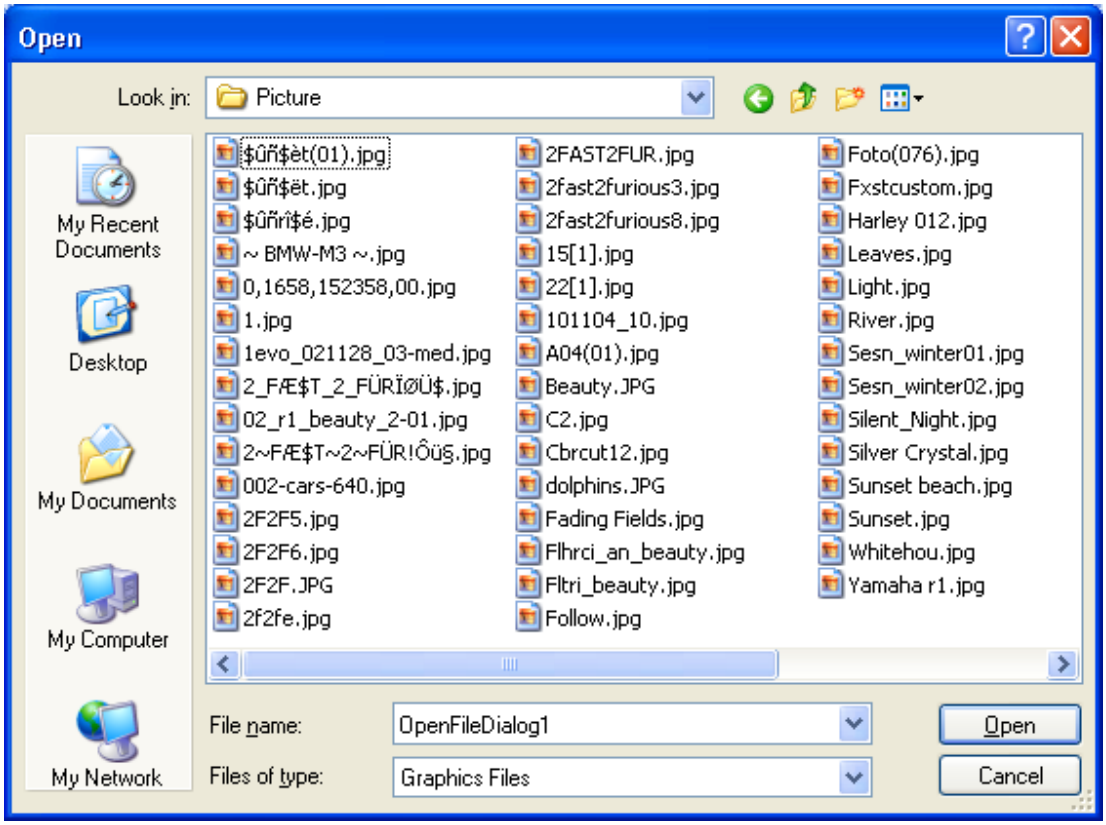
Pada tampilan utama ini terdapat beberapa *link* utama yang berfungsi untuk mengakses *form-form* yang terdapat dalam sistem.

1. *Link* ‘Penyisipan Pesan’ digunakan untuk melakukan proses penyisipan pesan. Tampilan *form* ‘Penyisipan Pesan’ dapat dilihat pada gambar berikut:



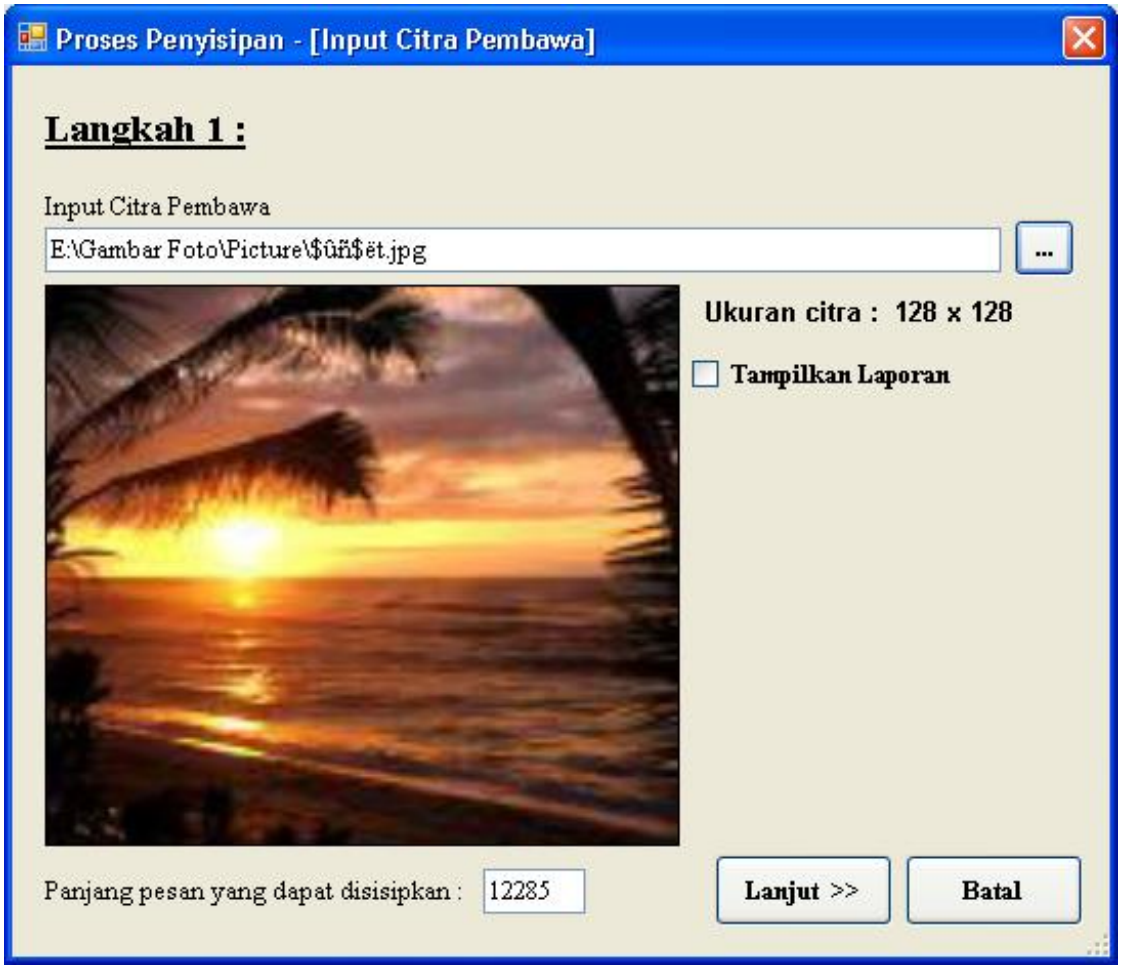
Gambar 20. Tampilan *Form* Penyisipan Pesan

Pilih citra yang akan digunakan untuk menyimpan data pesan rahasia. Untuk membuka kotak dialog Open untuk pemilihan *file* citra, maka kliklah *link* '…'. Tampilan kotak dialog Open dapat dilihat pada gambar berikut:



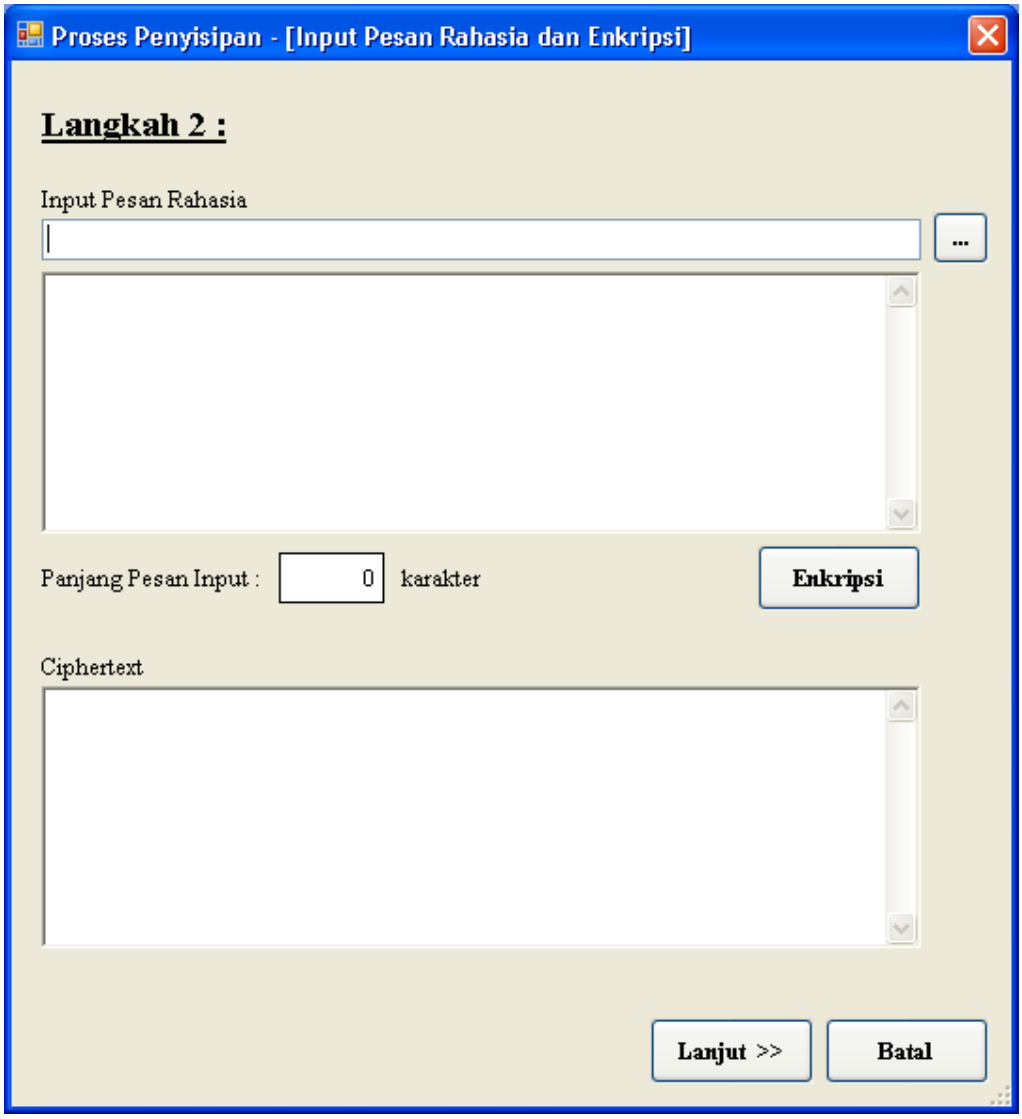
Gambar 21. Tampilan Kotak Dialog Open untuk *File* Citra

Pilihlah *file* citra yang diinginkan. Setelah itu, klik tombol ‘Open’. Sedangkan, untuk membatalkan proses pemilihan *file* citra, maka klik tombol ‘Cancel’. Tampilan *form* Tempel Pesan Rahasia dapat dilihat pada gambar berikut:



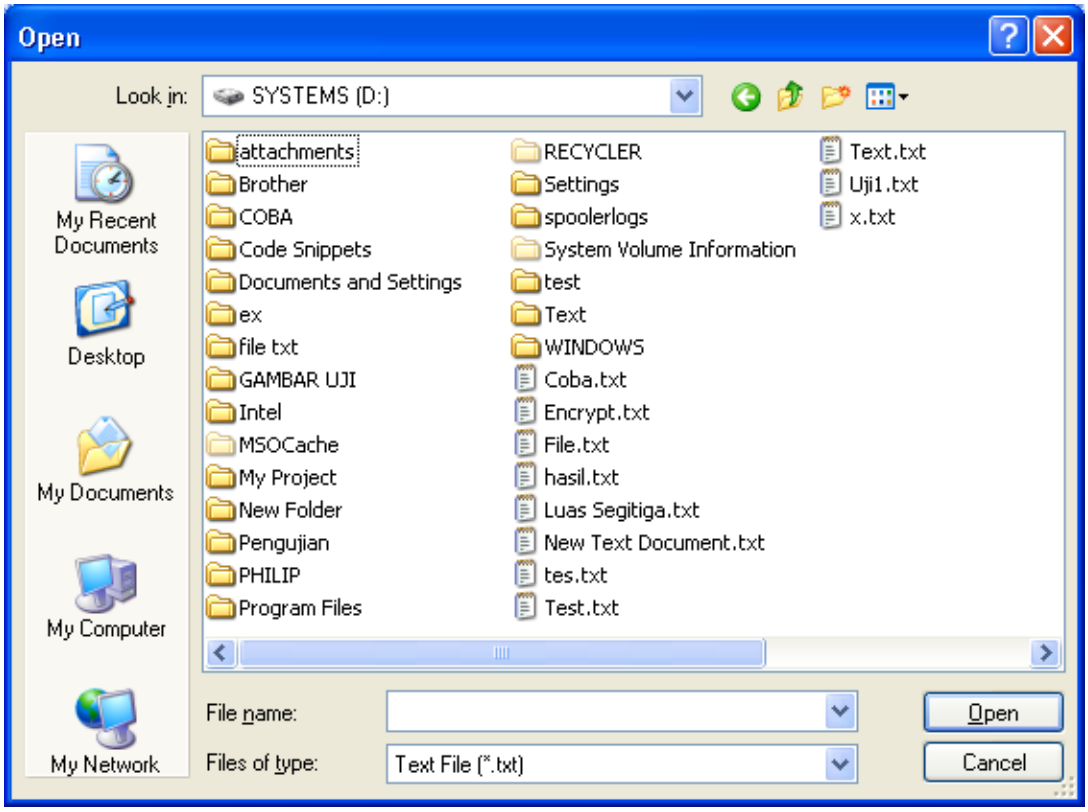
Gambar 22. Tampilan Tempel Pesan Rahasia Setelah Input Data

Setelah semua data dimasukkan, klik *link* ‘Lanjut >>>’ sehingga sistem akan menampilkan langkah selanjutnya dari proses penyisipan yaitu proses pengisian pesan rahasia dan enkripsi. Tampilan system dilihat pada gambar :



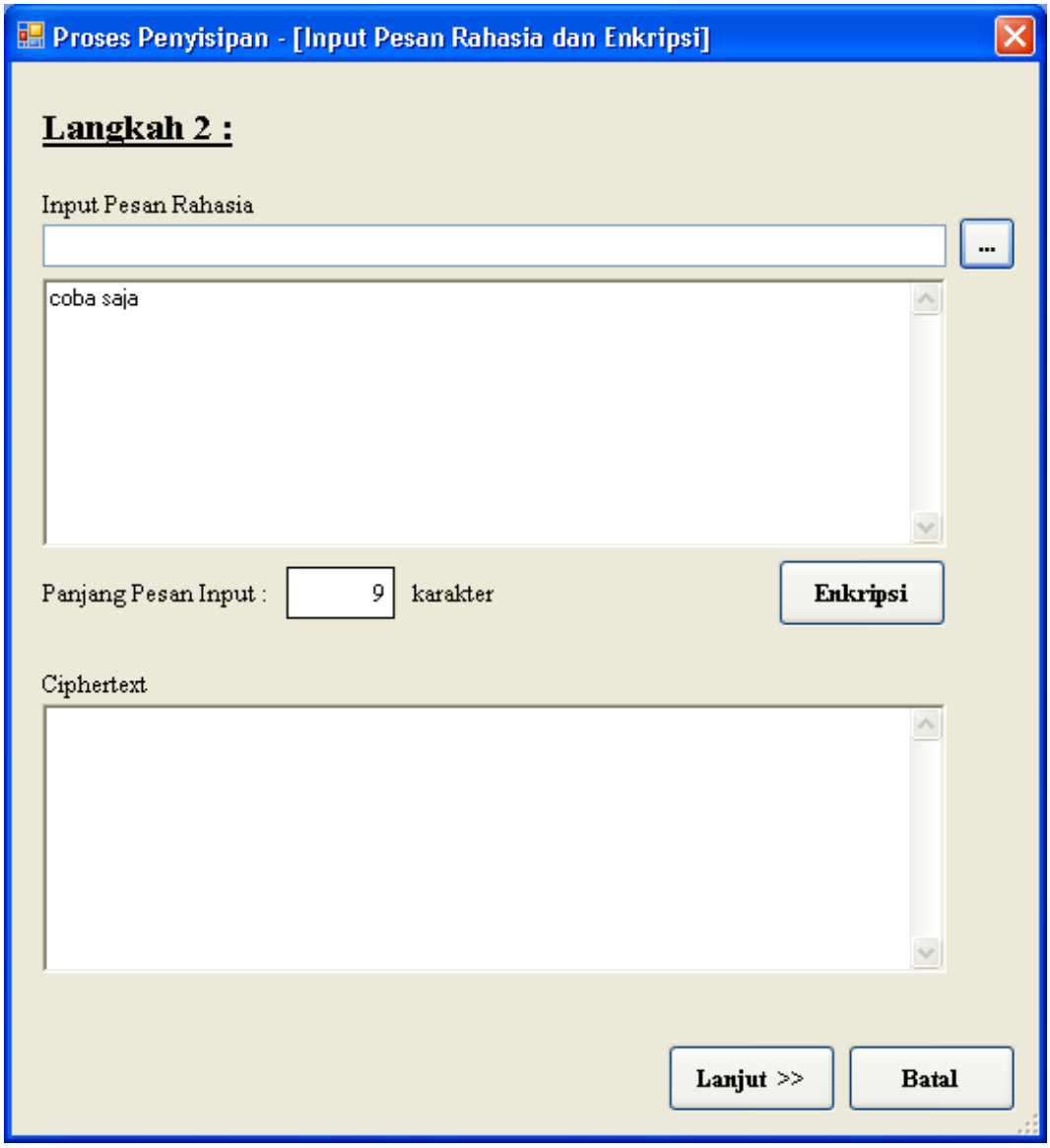
Gambar 23. Tampilan Form Input Pesan Rahasia

Pilih *file* pesan rahasia yang akan disisipkan ke dalam citra sampul. Untuk membuka kotak dialog Open untuk pemilihan *file* pesan rahasia, maka kliklah *link* '…'. Tampilan kotak dialog Open dapat dilihat pada gambar berikut:



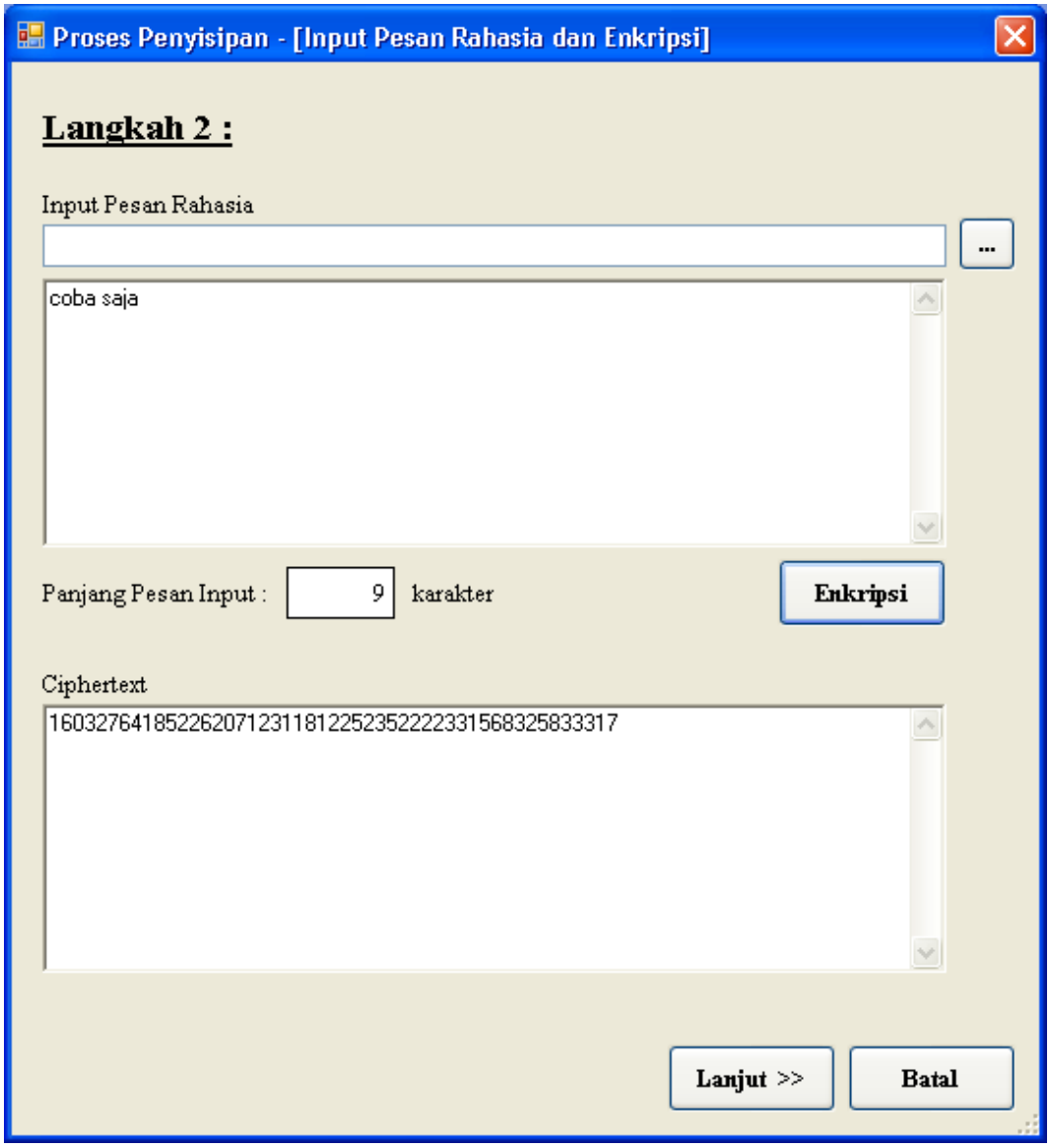
Gambar 24. Tampilan Kotak Dialog Open untuk *File* Pesan Rahasia

Pilihlah *file* pesan rahasia yang diinginkan. Setelah itu, klik tombol ‘Open’. Sedangkan, untuk membatalkan proses pemilihan *file* citra, maka klik tombol ‘Cancel’. Tampilan *form* Input Pesan Rahasia dapat dilihat pada gambar berikut:



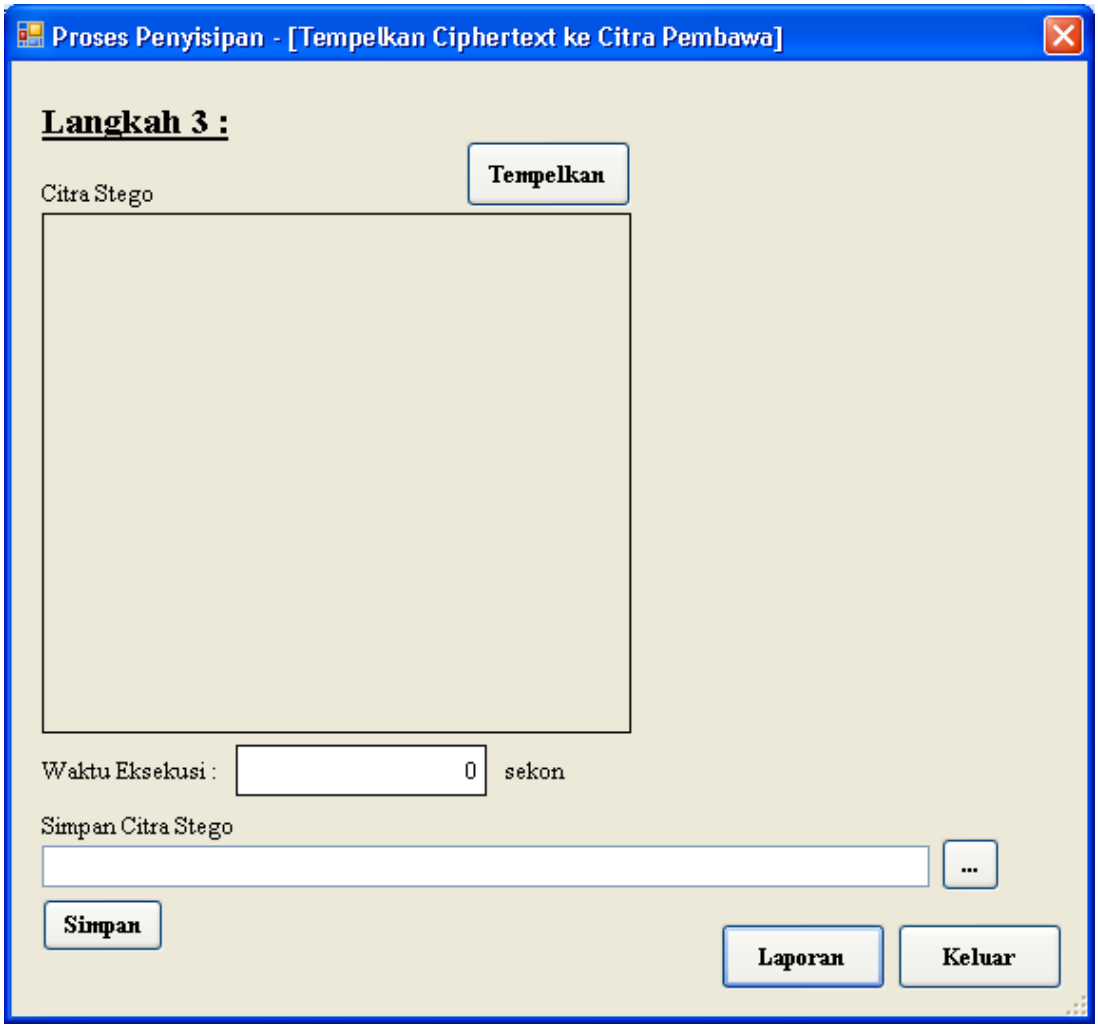
Gambar 25. Tampilan *Form* Input Pesan Rahasia Setelah Input

Setelah itu, klik tombol ‘Enkripsi’ untuk mengenkripsi pesan rahasia yang dimasukkan sehingga sistem akan mengenkripsi pesan rahasia dan menampilkan hasil *ciphertext* yang diperoleh. Tampilan *form* Input Pesan Rahasia akan terlihat seperti gambar berikut:



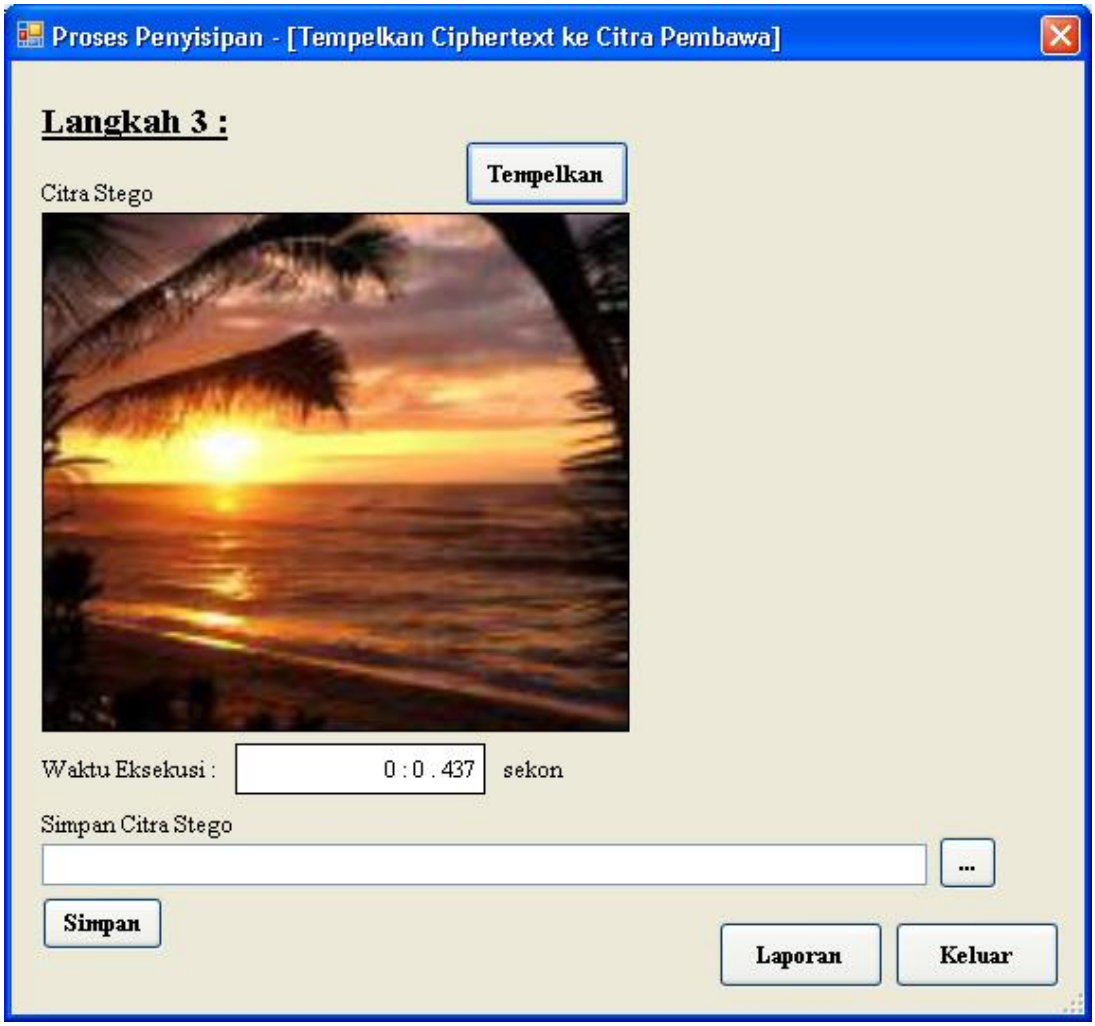
Gambar 26. Tampilan *Form* Input Pesan Rahasia Setelah Enkripsi

Setelah itu, klik tombol ‘Lanjut’ sehingga sistem akan menampilkan proses penempelan pesan rahasia ke citra sampul. Tampilan *form* Tempelkan *Ciphertext* ke Citra Pembawa dapat dilihat pada gambar berikut:



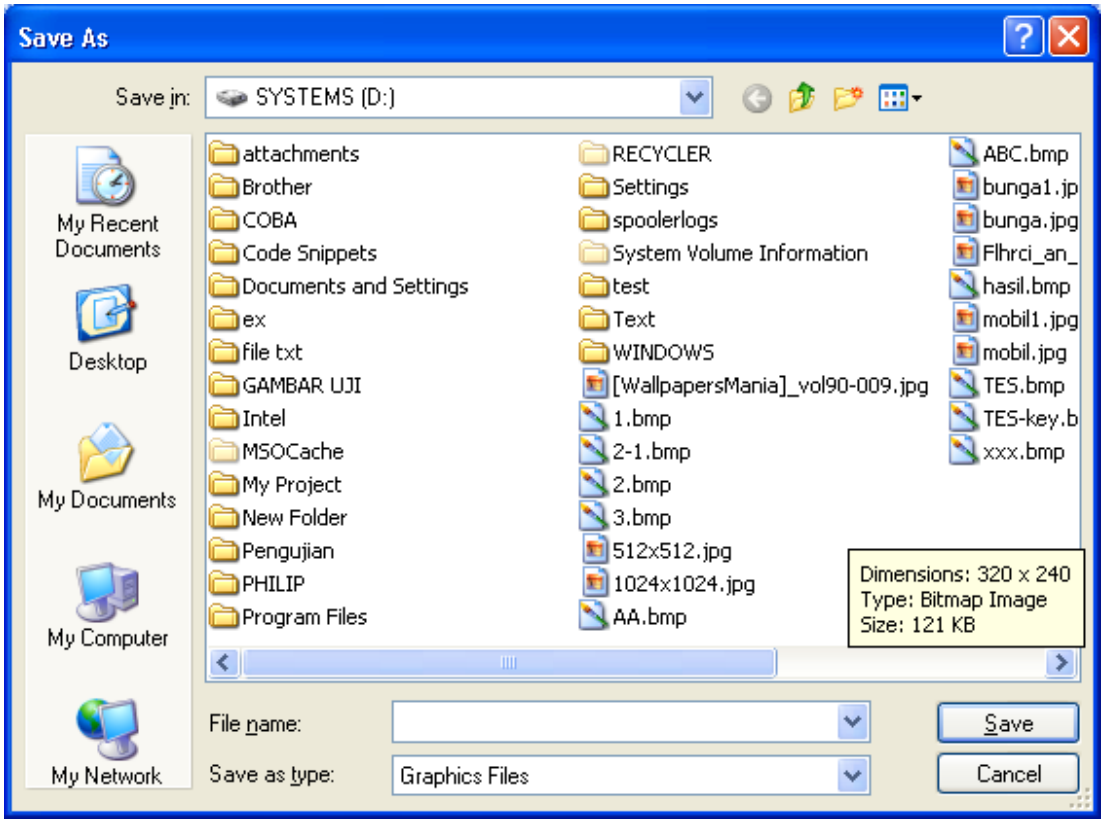
Gambar 27. Tampilan *Form* Tempelkan *Ciphertext* ke Citra Pembawa

Klik tombol ‘Tempelkan’ untuk melakukan proses penyisipan pesan rahasia ke citra sampul. Tampilan *form* Tempelkan *Ciphertext* ke Citra Pembawa setelah proses penempelan dapat dilihat pada gambar berikut:



Gambar 28. Tampilan *Form* Tempelkan *Ciphertext* ke Citra Pembawa Setelah Proses Penempelan

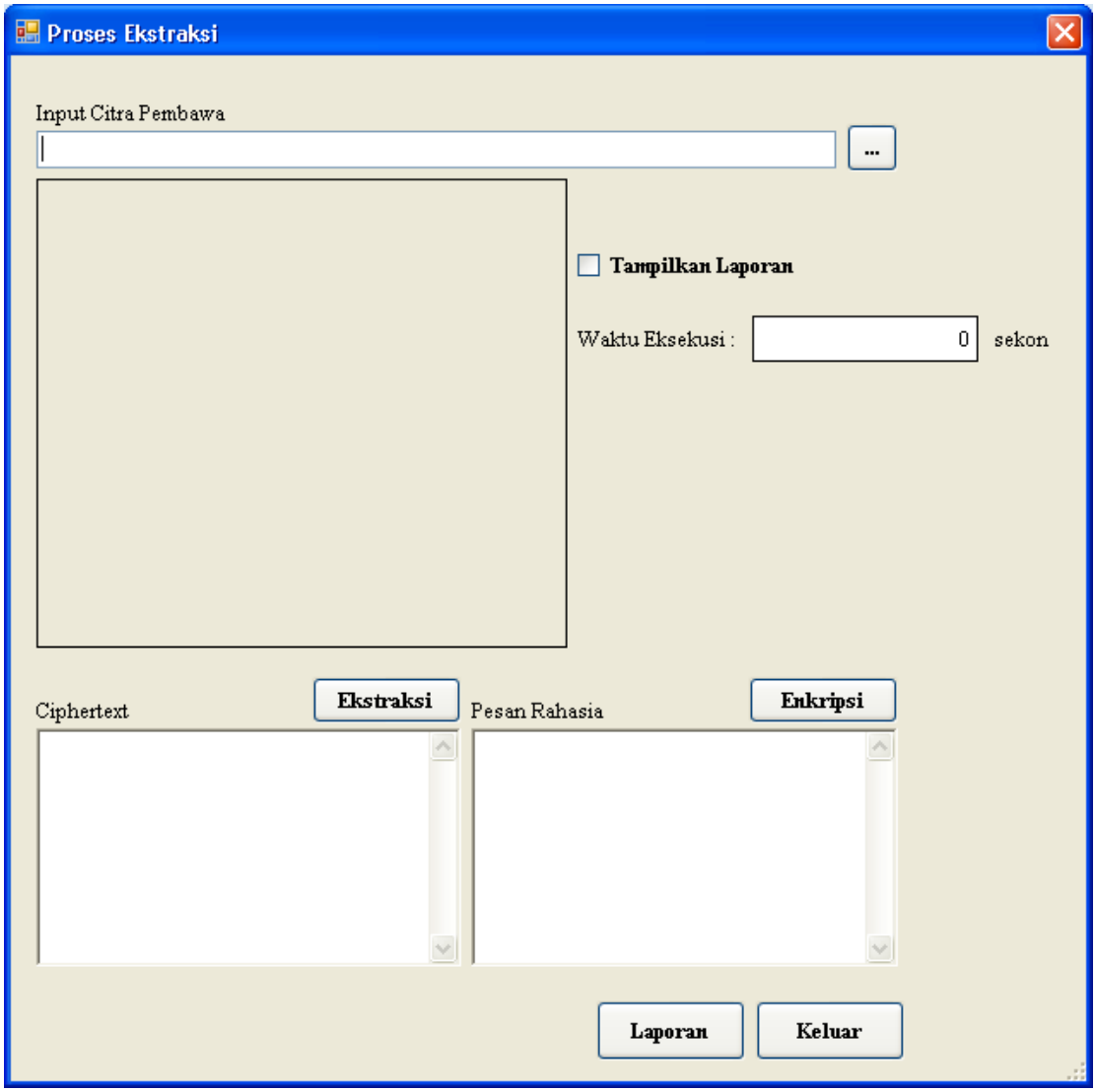
Klik tombol '…' untuk memilih lokasi penyimpanan *file* citra. Apabila *user* mengklik tombol '…', maka sistem akan menampilkan kotak dialog *Save* seperti terlihat pada gambar berikut:



Gambar 29. Tampilan Kotak Dialog *Save*

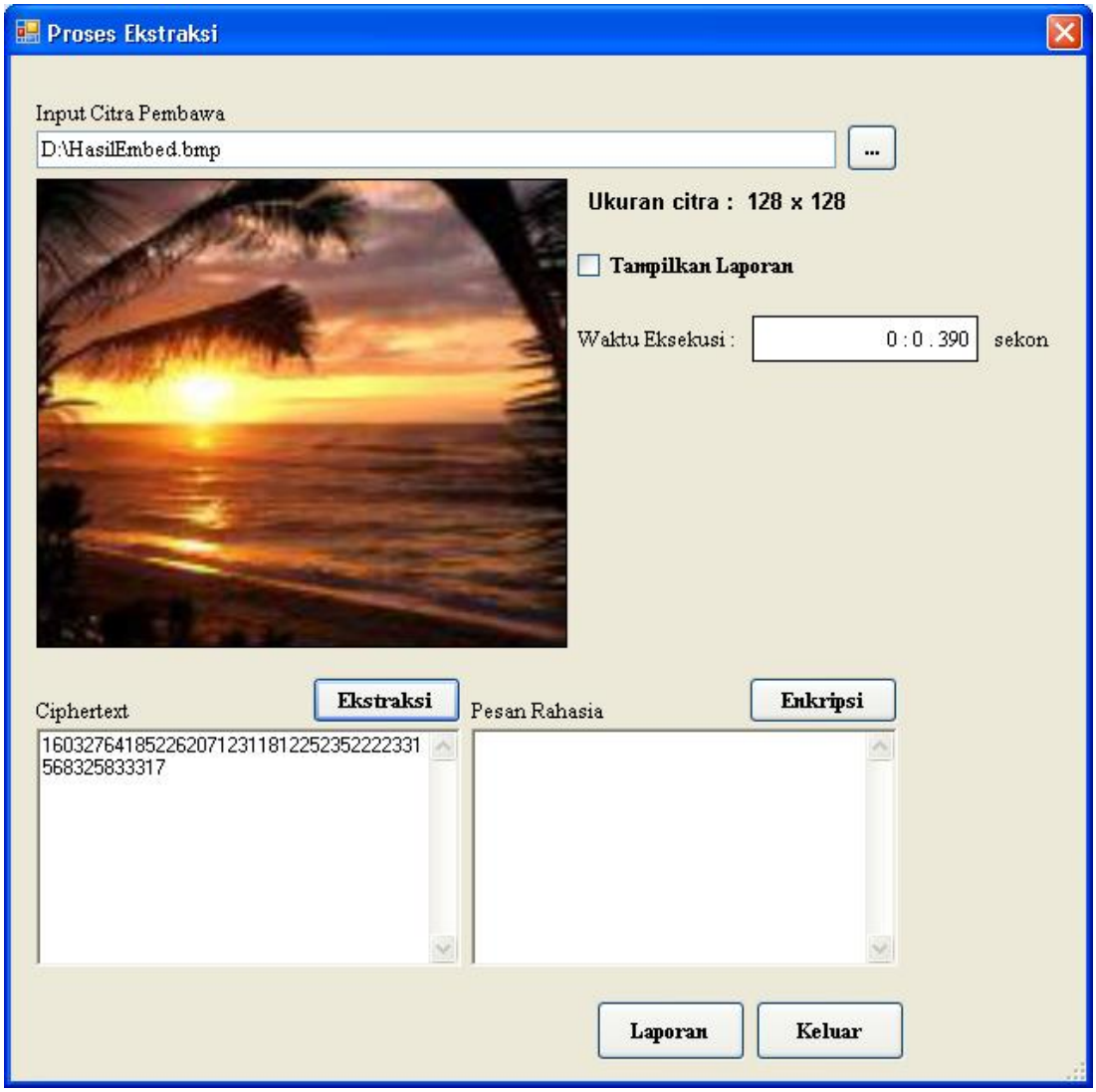
Isikan nama *file* pada *textbox File name* dan klik tombol ‘Save’. Sistem akan menyimpan *file* citra tersebut pada lokasi yang dipilih.

2. *Link* ‘Ekstraksi’ digunakan untuk melakukan proses ekstraksi pesan rahasia dari media citra stego. Tampilan *form* Ekstraksi Pesan Rahasia dapat dilihat pada gambar berikut:



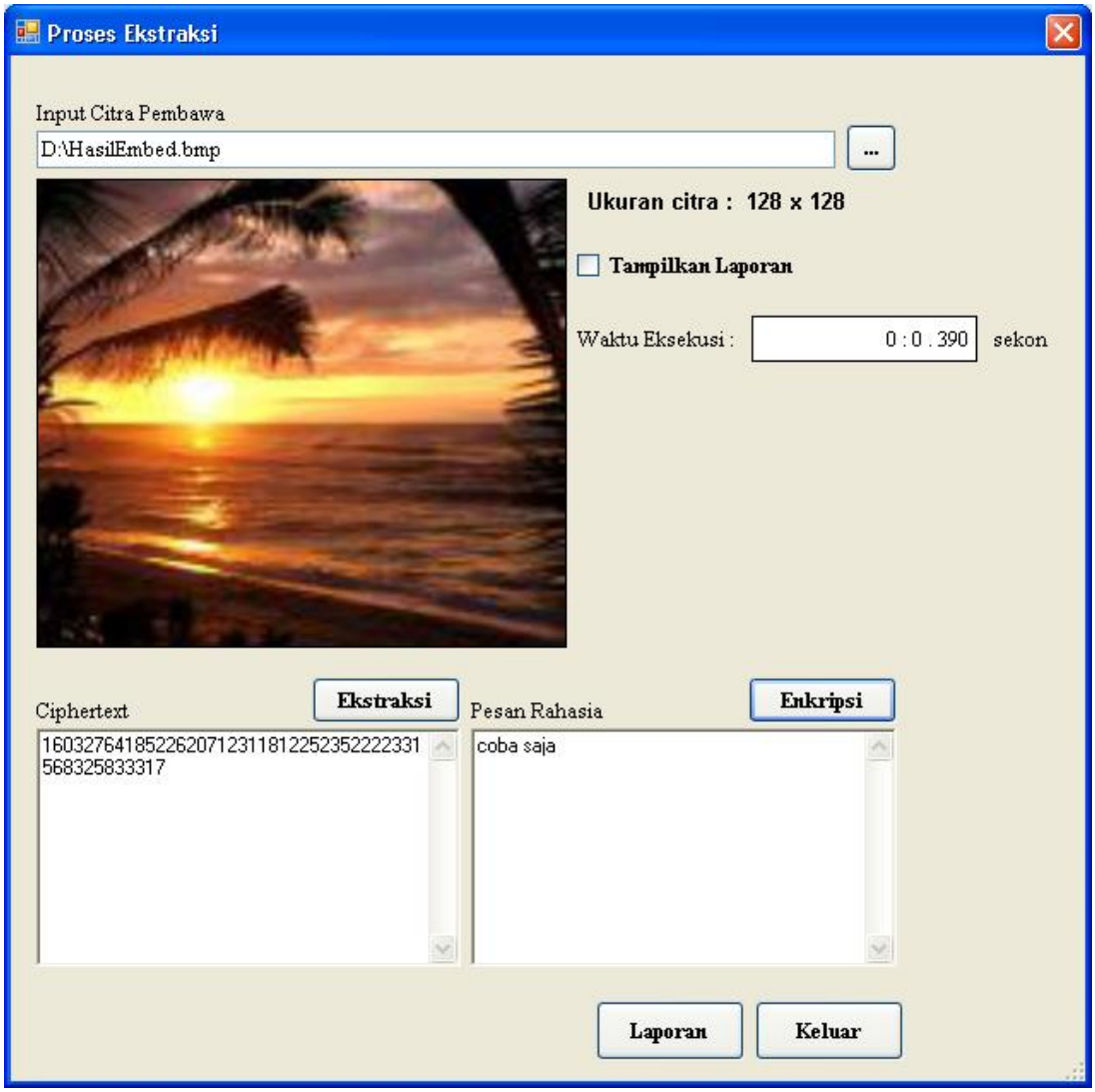
Gambar 30. Tampilan *Form* Ekstraksi Pesan Rahasia

Kliklah *link* ‘Buka’ untuk memilih *file* citra steganografi yang akan diekstrak keluar pesan rahasianya. Setelah itu, klik tombol ‘Ekstraksi’ untuk mengekstrak *ciphertext* keluar dari citra stego. Tampilan form setelah proses ekstraksi dapat dilihat pada gambar berikut:



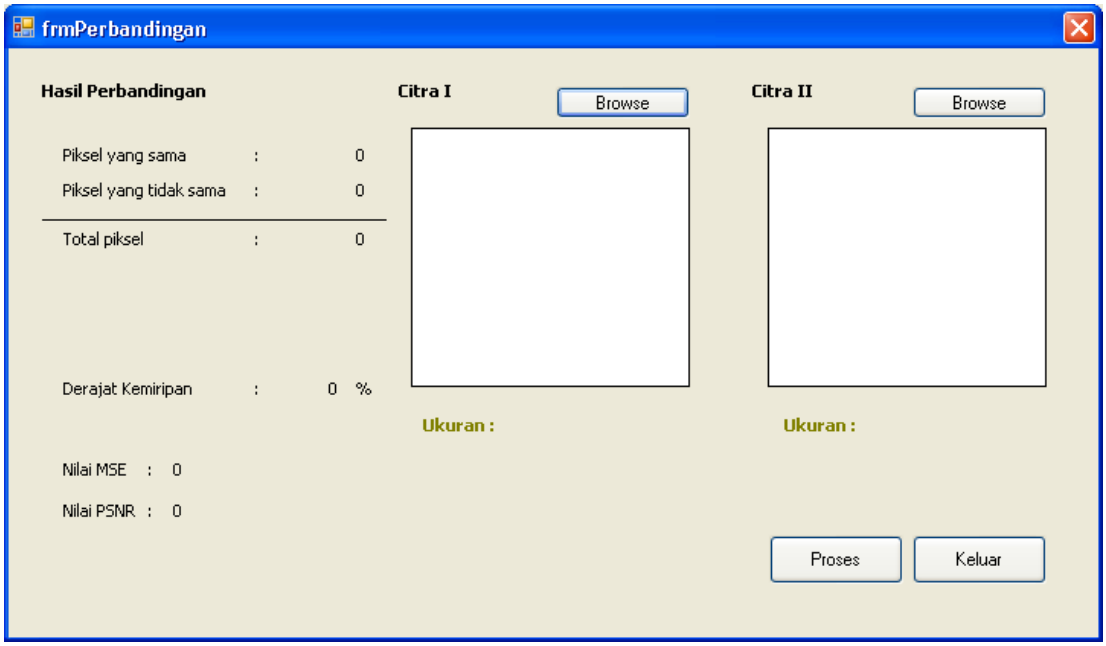
Gambar 31. Tampilan *Form* Ekstraksi Pesan Rahasia Setelah Proses Ekstraksi

Setelah itu, klik tombol dekripsi untuk melakukan proses dekripsi terhadap *ciphertext* yang diperoleh. Setelah selesai proses ekstraksi pesan rahasia, maka tampilan *form* Ekstraksi Pesan Rahasia akan terlihat seperti gambar berikut:



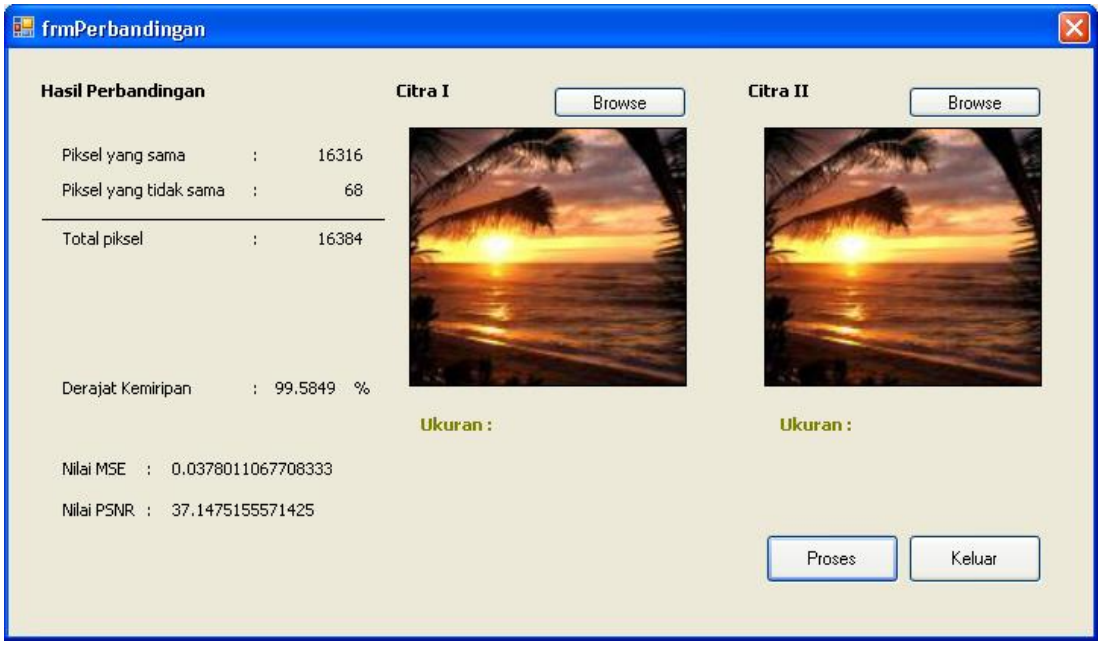
Gambar 32. Tampilan *Form* Ekstraksi Pesan Rahasia Setelah Proses Dekripsi Pesan

3. *Link* 'Hasil Perbandingan' digunakan untuk menampilkan proses perbandingan antara dua buah citra dengan menggunakan rumusan MSE. Tampilan *form* 'Perbandingan' dapat dilihat pada gambar berikut:



Gambar 33. Tampilan *Form* Hasil Perbandingan

Pilihlah file citra pertama dan kedua yang ingin dibandingkan. Setelah itu, klik tombol ‘Proses’ sehingga sistem akan menampilkan hasil perbandingan, seperti terlihat pada gambar berikut:



Gambar 34. Tampilan *Form* Hasil Perbandingan Setelah Proses

BAB V

PENUTUP

1. Kesimpulan

Setelah menyelesaikan pembuatan perangkat lunak ini, penulis dapat menarik beberapa kesimpulan sebagai berikut:

a. Berdasarkan hasil pengujian, tidak tampak adanya perbedaan antara citra asli dengan citra stego secara kasat mata. Hal ini dapat dilihat pada nilai MSE yang relatif kecil, dimana semakin kecil nilai MSE antara dua buah citra digital berarti bahwa kedua citra tersebut semakin mirip.
b. Proses perubahan / penghapusan bagian tertentu pada citra tidak berdampak pada pesan yang disisipkan, dengan kemungkinan terjadinya perubahan terhadap isi pesan relatif kecil.

2. Saran

Penulis ingin memberikan beberapa saran yang mungkin berguna untuk pengembangan lebih lanjut pada perangkat lunak, yaitu :

a. Aplikasi dapat dimodifikasi lagi sehingga dapat digunakan untuk menyisipkan pesan rahasia pada audio, video ataupun gambar animasi berformat *.gif.
b. Pengembangan lebih lanjut dapat dilakukan dengan menganalisis sekuritas dari algoritma yang dibahas dan membandingkannya dengan skema steganografi berbasis teks lainnya yang sejenis.

DAFTAR PUSTAKA

Cun-Cun (2008). **Perancangan Program Aplikasi Steganography pada Media *Audio File* dengan Metode *Direct Sequence Spread Spectrum***, Jakarta: BINUS

Menezes, A., van Oorschot, P. & Vanstone, S. (1996). ***Handbook of Applied Cryptography***, CRC Press

Munir, R. (2008). **Pengantar Pengolahan Citra**, Jakarta: PT. Elex Media Komputindo,

Munir, R., (2006), **Kriptografi**, Bandung: Informatika.

Murni, A. (1992). **Pengantar Pengolahan Citra**, Jakarta: PT. Elex Media Komputindo,

Parvez, T. dan A.A.A. Gutub (2008). ***RGB Intensity Based Variabel-Bits Image Steganography***, IEEE Asia-Pasific Services Computing Conference

Schneier, B. (1996). ***Applied Crytography***, *Second Edition*, John Willey & Sons Inc., 1996.

William Stallings, (2011), ***Cryptography and Network Security : Principle and Practice***, *Second Edition*, Prentice Hall.

Zhu Liehuang, Li Wenzhou, Liao Lejian dan Li Hong (2006). ***A Novel Image Scrambling Algorithm for Digital Watermarking Based on Chaotic Sequence***. IJCSNS, International Journal of Computer Science and Network Security, Vol 6, No. 8B.

Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.

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.

Bahri, S. (2018). Metodologi Penelitian Bisnis Lengkap Dengan Teknik Pengolahan Data SPSS. Penerbit Andi (Anggota Ikapi). Percetakan Andi Ofsset. Yogyakarta.

Diantoro, M., Maftuha, D., Suprayogi, T., Iqbal, M. R., Mufti, N., Taufiq, A., ... & Hidayat, R. (2019). Performance of Pterocarpus Indicus Willd Leaf Extract as Natural Dye TiO2-Dye/ITO DSSC. Materials Today: Proceedings, 17, 1268-1276.

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).

Fitriani, W., Rahim, R., Oktaviana, B., & Siahaan, A. P. U. (2017). Vernam Encypted Text in End of File Hiding Steganography Technique. Int. J. Recent Trends Eng. Res, 3(7), 214-219.

Hardinata, R. S. (2019). Audit Tata Kelola Teknologi Informasi menggunakan Cobit 5 (Studi Kasus: Universitas Pembangunan Panca Budi Medan). Jurnal Teknik dan Informatika, 6(1), 42-45.

Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 1(1).

Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10), 1363-1365.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. Int. J. Sci. Res. Sci. Technol, 3(6), 504-509.

Marlina, L., Muslim, M., Siahaan, A. U., & Utama, P. (2016). Data Mining Classification Comparison (Naïve Bayes and C4. 5 Algorithms). Int. J. Eng. Trends Technol, 38(7), 380-383.

Muttaqin, Muhammad. "ANALISA PEMANFAATAN SISTEM INFORMASI E-OFFICE PADA UNIVERSITAS PEMBANGUNAN PANCA BUDI MEDAN DENGAN MENGGUNAKAN METODE UTAUT." Jurnal Teknik dan Informatika 5.1 (2018): 40-43.

Ramadhan, Z., Zarlis, M., Efendi, S., & Siahaan, A. P. U. (2018). Perbandingan Algoritma Prim dengan Algoritma Floyd-Warshall dalam Menentukan Rute Terpendek (Shortest Path Problem). JURIKOM (Jurnal Riset Komputer), 5(2), 135-139.

Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. Int. J. Eng. Technol., 7(2.13), 345-347.

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." Jurnal Abdi Ilmu 10.2 (2018): 1899-1902.

BIOGRAFI PENULIS

Penulis dilahirkan di Kota Medan pada tanggal 18 Juli 1993 sebagai anak pertama dari tiga bersaudara dari Keluarga Bapak Suratno dan Ibu Endang Kumoratih. Pada tahun 2005 lulus di SDN 064964 Medan, tahun 2008 lulus di SMP Sinar Husni Medan dan tahun 2011 lulus di SMA Sinar Husni Medan.

Pada tahun 2011, Penulis melanjutkan kuliah di Program Diploma III Jurusan Manajemen Informatika di Politeknik LP3M Medan, Kemudian pada tahun 2016 penulis kembali melanjutkan studi S-1 nya di Universitas Pembangunan Panca Budi dengan memilih Program Studi Sitem Komputer, selama menjadi mahasiswa Universitas Pembangunan Panca Budi, penulis aktif di organisasi kemahasiswaan, Himpunan Mahasiswa Sistem Komputer.

Penulis dinyatakan lulu pada ujian sidang meja hijau pada Program Studi Sistem Komputer pada tanggal 07 November 2019 dengan Tugas Akhir berjudul "APLIKASI PENYEMBUNYIAN FILE DENGAN VIGENERE CHIPER DAN STEGANOGRAPHY (LSB)"