TEKNIK KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI ALGORITMA *VIGENERE* DAN STEGANOGRAFI AUDIO DENGAN METODE LSB

Skripsi Disusun Dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains Dan Teknologi Universitas Pembangunan Panca Budi Medan

SKRIPSI

OLEH

NAMA	: MUHAMMAD YUDHA PRATAMA
NPM	: 1514370182
PROGRAM STUDI	: SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020

ABSTRAK

MUHAMMAD YUDHA PRATAMA

TEKNIK KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI ALGORITMA *VIGENERE* DAN STEGANOGRAFI AUDIO DENGAN METODE LSB

2019

Dengan semakin berkembangnya teknologi informasi dan telekomunikasi, maka perhatian pada tingkat keamanan akan menjadi semakin penting. Salah satunya adalah tingkat keamanan penyisipan data atau informasi. Peningkatan kemanan penyisipan data dapat dilakukan dengan menggunakan Steganografi. Steganografi adalah teknik menyembunyikan pesan kedalam sebuah media. Media digital yang dapat digunakan adalah teks, gambar, suara dan video. Penelitian ini membahas tentang penerapan Steganografi untuk penyisipan pesan kedalam file audio. Jenis pesan yang dapat disisipkan adalah pesan teks dengan format (pdf dan doc), pesan gambar dengan format (jpg, png, gift dan bmp), pesan suara dengan format (mp3, wav dan wma), serta pesan video dengan format (3gp). Aplikasi ini dikembangkan dengan menggunakan bahasa pemrograman *Microsoft Visual Basic 2010*, dimana pemrograman ini dapat menyisipkan pesan. Pesan yang dapat disisipkan dengan format diatas. Dan aplikasi ini dapat berkombinasi dengan algoritma kriptografi dan steganografi dengan metode LSB.

Kata kunci : Kriptografi, *Vigenere*, Steganografi, LSB

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR ISI

Halaman

DAFTAR TABEL

Tabel **Halaman**

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat-Nya kepada peneliti, sehingga Skripsi ini dapat diselesaikan oleh peneliti tepat pada waktunya dengan judul Teknik Keamanan Data Menggunakan Kriptografi Algoritma Vigenere Dan Steganografi Audio Dengan Metode LSB. Skripsi ini dilakukan guna memenuhi salah satu syarat pemenuhan kurikulum dalam menyelesaikan pendidikan pada Program Studi S1 Sistem Komputer Fakultas Sains Dan Teknologi pada Universitas Pembangunan Panca Budi Medan. Pada kesempatan ini penulis mengucapkan rasa terima kasih dan penghargaan yang sebesar-besarnya kepada :

1. Teristimewa kepada Kedua Orang Tua dan Keluarga saya, yang telah banyak memberikan bimbingan dan bantuan baik moril maupun material selama penulis mengikuti pendidikan hingga selesainya Skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, SE, MM, selaku Rektor Universitas Pembangunan Panca Budi Medan.
3. Ibu Sri Shindi Indira selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
4. Bapak Eko Hariyanto, S.Kom., M.Kom selaku Ketua Program Studi Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
5. Bapak Andysah Putera Utama Siahaan, S.Kom., M.Kom., Ph.D, selaku Dosen Pembimbing I yang juga telah memberikan pengarahan dan petunjuk dalam Skripsi ini.

6. Bapak Supiyandi, S.kom., M.kom, selaku Dosen Pembimbing II yang juga telah memberikan pengarahan dan petunjuk dalam Skripsi ini.
7. Bapak/Ibu Dosen beserta seluruh staf Universitas Pembangunan Panca Budi Medan.
8. Kepada Ibu Roslaini Z, penulis mengucapkan banyak terima kasih untuk dukungan yang selama proses pembelajaran hingga selesainya Skripsi ini.
9. Kepada seluruh teman-teman penulis mengucapkan terima kasih atas dukungan kalian semua.
10. Kepada rekan-rekan di program Studi Teknik Komputer Universitas Pembangunan Panca Budi Medan yang selalu memberikan masukan serta kritik yang baik buat penulis. Penulis menyadari bahwa Skripsi ini tidaklah sempurna dan banyak kekurangan. Oleh karena itu, penulis sangat mengharapkan dan menghargai saran dari rekan-rekan dan dari semua pihak yang mengarah kepada perbaikan Tugas Akhir ini.

Medan. Desember 2019

Penulis,

MUHAMMAD YUDHA PRATAMA
(1514370182)

BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan, maupun individual. Begitu penting nya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang orang tertentu. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Berdasarkan penelitian sebelumnya ilmu sandi (kriptografi) sendiri telah ada sejak lama. Tercatat dalam sejarah bahwa julius caesar, seorang kaisar Romawi menggunakan penyandian untuk menyampaikan pesan rahasia perang.

Kriptografi merupakan ilmu untuk menjaga kerahasian pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Pesan yang disamarkan (teks jelas yang dapat dimengerti) dinamakan plainteks, sedangkan pesan hasil penyamaran (teks tersandi) dinamakan chiperteks. Proses kriptografi terdiri atas enkripsi dan dekripsi. Enkripsi merupakan proses penyamaran dari plainteks ke chiperteks. Sedangkan dekripsi merupakan proses pembalikan dari chiperteks ke plainteks. Teknik kriptografi akan lebih baik jika dikombinasikan dengan steganografi.

Berdasarkan uraian latar belakang diatas maka penulis mengambil judul penelitian "**Teknik Keamanan Data Menggunakan Kriptografi Algoritma *Vigenere* Dan Steganografi Audio Dengan Metode LSB***".*

1.2 Rumusan Masalah

Adapun masalah yang akan dibahas dalam skripsi ini yaitu:

1. Bagaimana kombinasi algoritma kriptografi *vigenere* dengan algoritma steganografi *least significant bit* LSB ?
2. Bagaimana cara menyisipkan sebuah data kedalam file audio ?
3. Bagaimana cara mengekstrak data yang telah disimpan ke dalam file audio ?

1.3 Batasan Masalah

Karena keterbatasan dan waktu maka penulis akan membatasi pokok permasalahan yang akan dibahas yaitu:

1. Bahasa pemograman yang digunakan adalah *Microsoft Visual Studio.*
2. Audio yang digunakan bertipe output mp3.
3. Besar data pesan adalah maksimal 500 KB plaint text.

1.4 Tujuan Penulisan

Untuk mengetahui kombinasi algoritma kriptografi *vigenere* dengan algoritma steganografi *least significant bit* LSB.

Untuk menyisipkan sebuah data file kedalam audio, serta untuk mengestrak data yang telah disimpan ke dalam file audio.

1.5 Manfaat Penulisan

Menghindari pencurian data melalui jaringan internet, dan mampu menjaga data yang dikirimkan menjadi lebih aman. Kemudian menghindari kecurigaan adanya informasi rahasia yang terkandung dalam suatu media.

1. Agar data dapat tersimpan dan tidak dapat diakses oleh pihak lain.
2. Dapat mengkombinasikan algoritma kriptografi dan steganografi.
3. Membuat sebuah kunci dalam sebuah data yang telah tersimpan.

BAB II

LANDASAN TEORI

2.1 Aplikasi

Menurut jogiyanto (1999:12) adalah penggunaan dalam suatu komputer, intruksi (instruction) atau pernyataan (statement) yang disusun sedemikian rupa sehingga komputer dapat memproses input menjadi output. Secara umum adalah alat terapan yang difungsikan secara khusus dan terpadu sesuai kemampuan yang dimilikinya. Cara kerja aplikasi, aplikasi tidak akan bekerja tanpa adanya sistem operasi, karena sistem operasi bertindak sebagai perantara antara hardware demgam program aplikasi. Pemutar media, pengola kata, serta lembar kerja merupakan salah satu contoh perangkat lunak aplikasi. Microsoft office yang merupakan penggabungan aplikasi lembar kerja, pengolah kata ataupun dengan aplikasi yang lainnya.. Kemampuan mereka yakni saling interaksi sesama yang saling menguntungkan, seperti satu dokumen pengolah kata terdapat satu lembar kerja meskipun dalam pembuatannya dibuat dalam aplikasi lembar kerja yang bebeda (Hasugian, 2013).

Dalam pengembangannya aplikasi dapat dikategorikan dalam tiga kelompok diantaranya;

1. Aplikasi Desktop, yaitu aplikasi yang hanya dijalankan di perangkat PC komputer atau laptop.

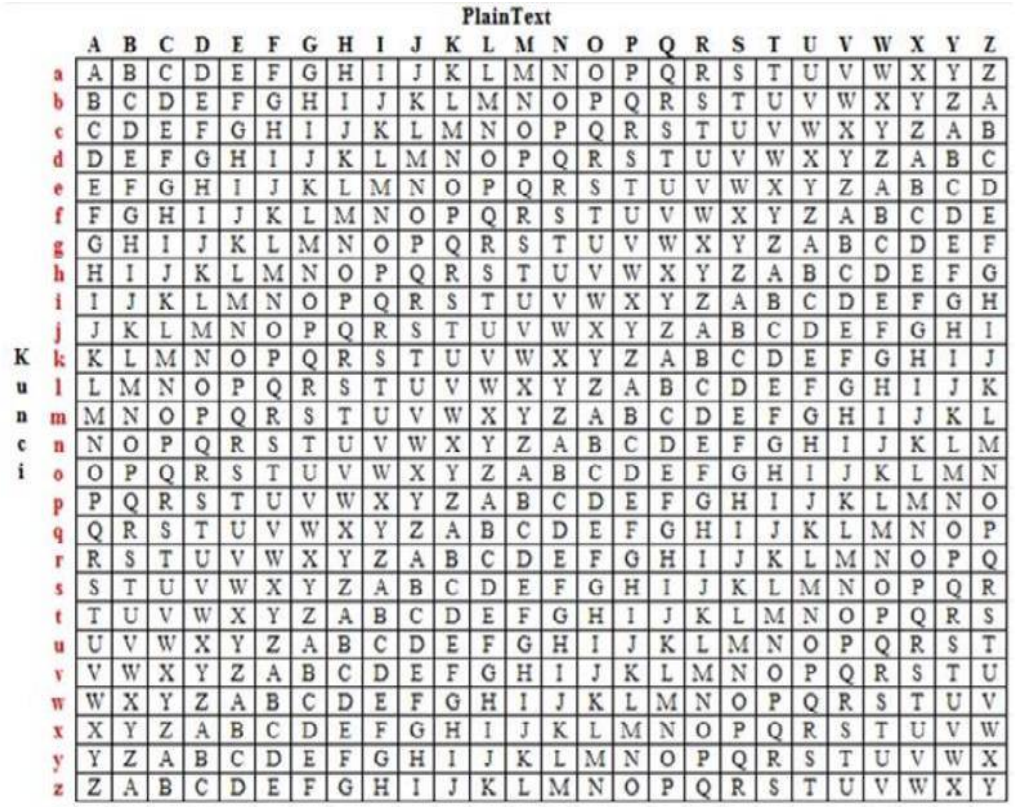
2. Aplikasi Web, yaitu aplikasi yang dijalankan menggunakan komputer dan koneksi internet.
3. Aplikasi Mobile, yaitu aplikasi yang dijalankan di perangkat mobile dimana untuk kategori ini penggunaannya sudah banyak sekali.

Umumnya suatu aplikasi dapat berjalan di berbagai perangkat yang dioperasikan oleh *operating system* (OS) yang ada di perangkat tersebut. Apliksi yang berkualitas dan bermanfaat bagi penggunaannya;

1. Aplikasi dapat memenuhi kebutuhan user
2. Aplikasi dapat berjalan di multi-platform.
3. Aplikasi dapat merespon intruksi dengan cepat serta membutuhkan *resource* (*procesor, memory, storage)* yang rendah.

2.2 *Vigenere Chiper*

Vigenere chiper merupakan metode untuk proses membuat kata sandi dari sebuah teks berdasarkan huruf-huruf pada kata kunci deretan sandi *caesar*. Metode ini pertama kali dikemukakan oleh Blaise de *Vigenere* yang merupakan seorang diplomat sekaligus kriptologi asal perancis pada tahun 1586. Bujur sangkar *vigenere* ditunjukan pada gambar (M Azman Maricar, 2018).



Kunci	PlainText																									
		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	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
u	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
n	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
c	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
i	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

Gambar 2.1 Pemetaan *Vigenere Cipher*

Sumber: M. Azman Maricar 2018

2.3 Algoritma

Algoritma adalah suatu urutan dari beberapa langkah yang logis guna menyelesaikan masalah. Pada saat kita memiliki masalah, maka kita harus dapat untuk menyelesaikan masalah tersebut dengan menggunakan langkah-langkah yang logis (Fairu Zabadi, 2010). Dalam ilmu matematika dan komputer, pengertian algoritma merupakan prosedur dari beberapa langkah demi langkah untuk perhitungan. Algoritma dipakai untuk perhitungan, penalaran otomatis, dan pemrosesan data. Algoritma adalah suatu metode yang efektif diekspresikan

sebagai rangkaian yang terbatas dari beberapa intruksi yang telah dijelaskan dengan baik guna menghitung sebuah fungsi. Susunan algoritma dimulai dari kondisi awal dan input awal, intruksi tersebut mendekripsikan komputasi yang apabila itu dieksekusi aerta diproses dengan melewati urusan-urusan kondisi terbatas yang terdefinisi dengan baik, sehingga dapat menghasilkan output atau keluaran dan kondisi yang telah ditentukan. Algoritma sangat diperlukan untuk mengolah data yang ada di komputer.

2.3.1 Kriteria Algoritma

Kriteria Algoritma menurut S.E. Goodman dan S.T. Hedetniemi, adalah urutan terbatas dari operasi-operasi yang terdefinisi dengan baik, dimana masing-masing membutuhkan memori dan waktu yang terbatas untuk menyelesaikan suatu masalah.

a. Input program minimal harus memiliki nol input atau lebih dari pengguna. Setiap program pasti memiliki input. Yang dimaksud dengan memiliki nol input berarti program tidak mendapat masukan data dari pengguna secara langsung, namun semua data akan digunakan oleh program yang sudah dideklarasikan didalam kode program yang akan dieksekusi .
b. Output program minimal harus memiliki satu output, setiap program pasti memiliki output karena progaram dibuat untuk tujuan tertentu. Output program bisa berbentuk file, video, teks, atau disimpan di clipboard ysng kemudian digunakan di program lain atau disimpan dalam basis data.

c. *Finite* (terbatas) Program yang dibuat harus pasti dan terbatas. Suatu program yang dieksekusi haruslah berhenti dan selesai, bukan harus berjalan terus-menerus hingga hang up atau not responding, dan ujung-ujungnya harus di-kill atau dimatikan dengan paksa. Suatu program dapat mengalami infinite (tak terbatas) karena kesalahan dari programmer. Walau sistem operasi tidak terbatas *(infinite),* tetapi sistem juga akan mati jika komputer di shutdown.

d. *Definite* (pasti) Program harus jelas arah dan tujuannya. Suatu program harus jelas kapan mulai dan kapan berakhir, apa tujuannya, dan memiliki logika yang jelas agar dapat menghasilkan output yang sesuai dengan yang diharapkan.

e. Efisien Artinya, Program harus efisien, tidak memakan banyak memory, tidak melakukan hal – hal yang tidak perlu.

2.4 Kriptografi

Kriptografi menjelaskan bahwa ”Kriptografi *(cryptography)* berasal dari Bahasa Yunani yaitu *“cryptós”* artinya “secret” (rahasia), sedangkan “gráphein” artinya “writing” (tulisan). Jadi, 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 (Miftakul Amin, 2016). 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 sekedar privacy, tetapi juga untuk tujuan data integrity, authentication, dan non-repudiation".

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai plaintext (teks biasa). Disebut demikian karena infomasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja (Wahidun Sipayung, 2014). Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah plaintext melibatkan pengguna suatu bentuk kunci. Plaintext yang telah dienkripsi (kodean) dikenal sebagai ciphertext (teks sandi). Pesan plaintext yang telah dienkripsi (atau dikodekan) dikenal sebagai ciphertext (teks sandi). Di dalam kriptografi kita akan sering menemukan istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :

a. Pesan, *Plainteks*, dan *Ciphertek*s

   Pesan *(message)* ialah data atau informasi yang dapat dibaca dan dimengerti arti dan maknanya. Biasa disebut untuk pesan adalah *(plaintext)* atau teks jelas *(cleartext).*

b. Pengirim dan Penerima

   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim *(sender)* ialah entitas yang mengirim pesan kepada entitas lainnya. Penerima *(receiver)* ialah entitas yang menerima pesan.

c. Enkripsi dan dekripsi

Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi *(encryption)* atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula disebut dekripsi *(decryption)* atau *deciphering* (standard nama menurut ISO 7498-2).

d. *Cipher* dan kunci

Algoritma kriptografi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* membutuhkan algoritma yang beda untuk enkripsi dan dekripsi. Konsep matematisnya yang didasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen *plaintext* dan himpunan yang berisi *ciphertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan cipherteks, maka :

E (P) = C fungsi enkripsi E memetakan P ke C

D(C) = P fungsi dekripsi D memetakan C ke P

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan D(E(P)) = P harus benar.

Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (key) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa stringatau deretan bilangan.

2.5 Aspek- aspek keamanan Komputer

a. Kerahasiaan *(confidentiality)* ialah fasilitas yang diarahkan untuk menjaga supaya pesan tidak mudah dibaca oleh pihak-pihak yang tidak berhak.

b. Integritas data *(data integrity)* ialah fasilitas yang mengamankan bahwa pesan masih asli atau belum pernah dipalsukan selama pengiriman.

c. Otentikasi *(authentication)* ialah fasilitas yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran bagian yang berkomunikasi *(user autehentication).*

d. *Non-repudiation* ialah fasilitas untuk menjaga entitas yang berkomunikasi melakukan penyangkalan *Advanced Encryption Standard (AES)*

e. *Authority* ialah informasi yang berbeda pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya

f. *privacy* lebih kearah data-data yang bersifat pribadi

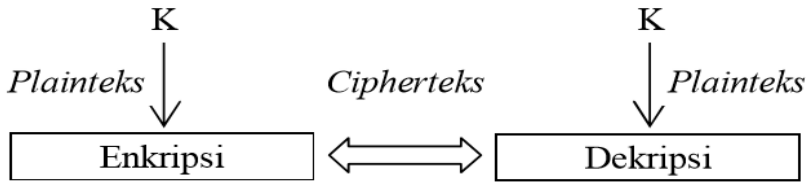
g. *Access Control* ialah Aspek ini berhubungan dengan cara pengaturan akses ke informasi. Ha ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi user id dan password ataupun dengan mekansme lain.

2.6 Macam-macam Algoritma Kriptografi

Berdasarkan kunci enkripsi dan dekripsi algoritma kriptografi dibagi menjadi tiga yaitu :

2.6.1 Algoritma kriptografi Simetris

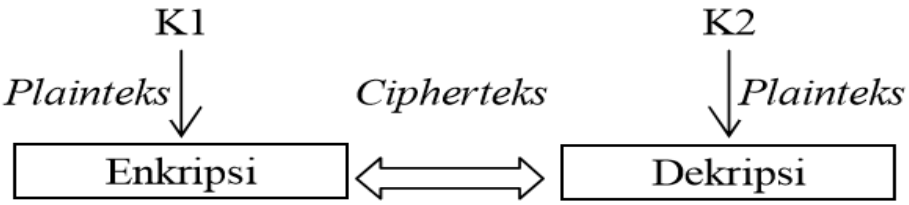
Konsep dasar kriptografi simetris adalah kunci enkripsi dan dekripsi yang sama. Nama lain kriptografi ini adalah kriptografi kunci privat, kriptografi kunci rahasia, atau kriptografi konvensional. Kriptografi ini mengasumsikan penerima dan pengirim pesan telah berbagi kunci tertentu sebelum pesan dikirim sehingga keamanan terletak pada kerahasiaan kunci. Umumnya cipher yang termasuk dalam kriptografi ini beroperasi dalam mode blok, yaitu setiap kali enkripsi atau dekripsi dilakukan pada satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran, yaitu setiap kali enkripsi atau dekripsi dilakukan terhadap satu bit atau satu byte data. Proses kriptografi ini sebagai berikut:



Gambar 2.2 Skema Kriptografi Simetris
Sumber: Indah Fitri Astuti, 2015

2.6.2 Algoritma Kriptografi Asimetris

Algoritma Asimetris adalah algoritma kriptografi yang mempergunakan kunci yang berbeda pada enkripsi dan dekripsinya. Pada kriptografi asimetris kunci untuk enkripsi tidak rahasia dan dapat diketahui siapapun (diumumkan ke publik), sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan (karena itu rahasia). Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan *(receiver)*. Hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri (Munir, 2006). Algoritma yang termasuk dalam algoritma asimetri adalah RSA, RSA-CRT, Elgamal, DSA, dsb. Skema kriptografi asimetri dapat dilihat pada gambar 2.



Gambar 2.3 Skema Kriptografi asimetris
Sumber: Indah Fitri Astuti, 2015

2.6.3 Hash Function

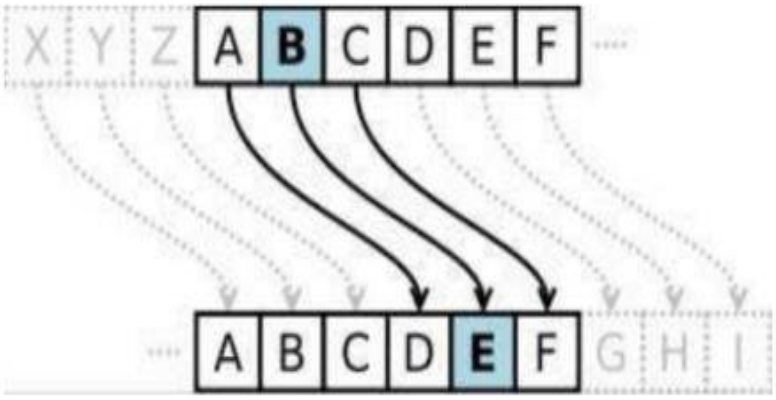
Fungsi Hash sering disebut dengan fungsi Hash satu arah (*one-way function*), *message disegt*, *fingerprint* fungsi kompresi dan message *authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukkan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap. Fungsi Hash biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan akan dibahas lebih lanjut pada bagian berikutnya.

2.7 Algoritma Kriptografi Klasik

Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Teknik substitusi adalah menggantikan karakter dalam plaintext menjadi karakter lain yang hasilnya adalah ciphertext. Sedangkan transposisi adalah teknik mengubah plaintext menjadi ciphertext dengan cara permutasi karakter. Kombinasi keduanya

secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: Caesar Cipher.

Caesar Cipher Metode penyandian ini dinamakan Caesar Chiper, setelah digunakan Julius Caesar untuk berkomunikasi dengan para panglimanya. Dalam kriptografi Caesar Chiper dikenal dengan beberapa nama seperti: shift cipher, Caesar's code atau Caesar shift. Caesar Chiper merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. Chiper ini berjenis chiper substitusi, dimana setiap huruf pada plaintextnya digantikan dengan huruf lain yang tetap pada posisi alfabet. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya.



Gambar 2.4 Proses Pergeseran Tiga Huruf
Sumber: Anita Hidayati, 2015

Transformasi Caesar Chiper dapat direpsentasikan dengan menyelaraskan plaintext dengan chipertext ke kiri atau kanan sebanyak jumlah pergeseran yang diinginkan. Sebagai contoh dengan jumlah pergeseran sebanyak 3.

Plaintex : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext : DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membaca pesan yang dienkripsi penerima dapat menyelaraskan huruf chipertext yang diterima dengan plaintext yang tepat berada di atasnya. Sebagai contoh dekripsinya sebagai berikut.

Ciphertext : VHPLQDU QDVLRQDO PDWHPDWLND

Plaintext : SEMINAR NASIONAL MATEMATIKA

Proses enkripsi pada Caesar Cipher dapat direperesentasikan menggunakan operator aritmetika modulo 26 setelah sebelumnya setiap huruf di transformasi kedalam angka, yaitu: A = 0, B = 1,…, Z = 25. Maka Caesar Cipher dirumuskan sebagai berikut: Proses enkripsi suatu huruf x dengan pergeseran n dapat dinyatakan secara matematis sebagai berikut:

Enkripsi: $C = E(P) = (P + 5) \bmod 26$ (1)

Dekripsi: $P = D(C) = (C - 5) \bmod 26$ (2)

Jika pergeseran huruf sebanyak x, maka dapat dijadikan dalam persamaan (3) dan (4):

$C = E(P) = (P + x) \bmod 26$ (3)

$P = D(C) = (C - x) \bmod 26$ (4)

dengan C adalah ciphertext, P adalah plaintext, x adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi. Untuk lebih menyulitkan kriptanalis

dapat digunakan perkalian dengan n, n adalah bilangan ganjil pada plaintext. Ini dijelaskan pada persamaan (5) dan (6):

$$C = E(P) = ((n * P) + x) \bmod 26 \quad (5)$$

$$P = D(C) = ((C - x)/ n) \bmod 26 \quad (6)$$

dengan n = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23,25. Tidak berlaku dengan n adalah bilangan negatif, karena akan menghasilkan huruf yang sama dalam enkripsi. Kelemahan dari *Caesar Cipher* adalah dapat dipecahkan dengan cara brute force attack, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci. Bisa juga menggunakan *exhaustive key search*, karena jumlah kunci sangat sedikit (hanya ada 26 kunci).

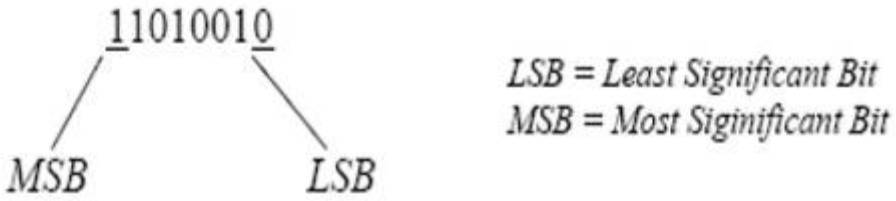
2.8 Algoritma Kriptografi Modern

Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter (seperti yang dilakukan pada cipher substitusi atau *cipher* transposisi dari algoritma kriptografi klasik). Operasi dalam mode bit berarti semua data dan informasi (baik kunci, plainteks, maupun ciphertext) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plaintext dienkripsi menjadi *ciphertext* dalam bentuk rangkaian bit, demikian sebaliknya. Enkripsi modern berbeda dengan enkripsi konvensional. Enkripsi modern sudah menggunakan komputer untuk pengoperasiannya, berfungsi untuk mengamankan data baik yang ditransfer

melalui jaringan komputer mauapun yang bukan. Hal ini sangat berguna untuk melindungi privacy, data integrity, authentication dan non-repudiation. Perkembangan algoritma kriptografi modern berbasis bit didorong oleh penggunaan komputer digital yang merepresentasikan data dalam bentuk biner.

2.9 Metode *Least Significant Bit* (LSB)

Metode LSB*(least significant bit),* merupakan metode yang bekerja pada bit yang terendah dari suatu deretan bit bit data. Penggunaan LSB ini dengan menyisipkannya pada bit rendah atau bit yang paling kanan (lsb) pada data pixel yang menyusun gambar tersebut (Sri Hartati, 2014). Seperti diketahui untuk *file bitmap* 24 bit di setiap *pixel* (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. (Munir Rinaldi 2006).



Gambar 2.5 Deretan Bit

Sumber: Rahima, 2014

2.10 Steganografi

Steganografi berasal dari bahasa Yunani yaitu steganos yang artinya tersembunyi atau terselubung dan «graphein», yang artinya menulis, sehingga

kurang lebih artinya adalah “menulis tulisan yang tersembunyi atau terselubung” (Sellars, 1996), sedangkan kriptografi adalah merupakan teknik menyamarkan dari suatu pesan teks proses plaintext menjadi ciphertext dan sebaliknya (enkripsi dan deskrpisi) dengan pendekatan dikenal 2 (dua) algoritma simetrik dan asimetrik (Mara Husein, 2014). Penelitian ini akan lebih difokuskan pada teknik steganografi dengan metode LSB menggunakan platform aplikasi yang berbasis Matlab dengan tujuan;

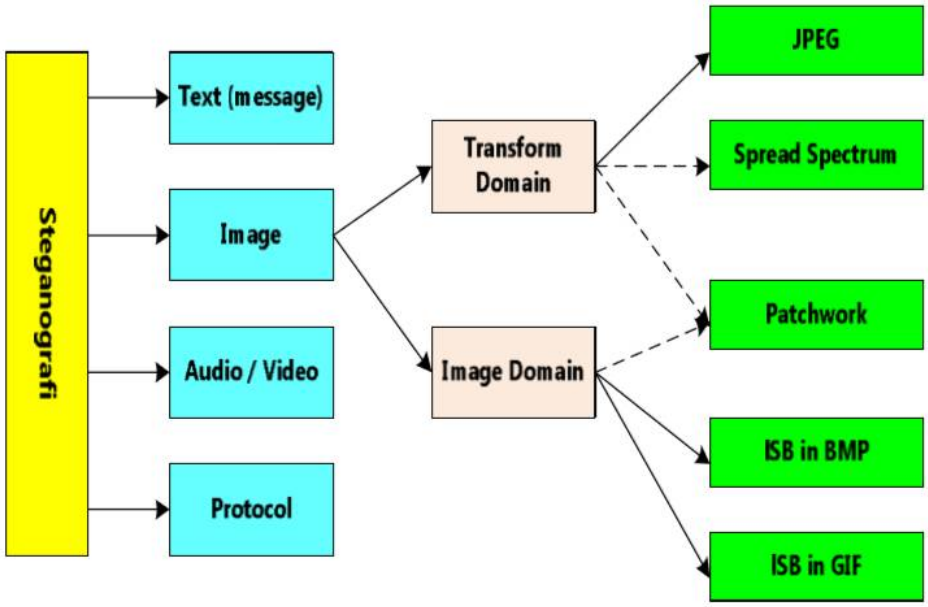
(a). Untuk melakukan pengamanan data dan kinerja (performance) dengan metode LSB agar data tersrbut tidak dapat di-akses orang lain dan dapat disembunyikan, dapat pula terjaga kerahasiaannya dari pihak yang tidak berwenang (pihak ketiga)

(b). Menguji dan menganalisa ukuran *(size)* proses file sebelum (cover) dan setelah *(stego)* steganografi dengan metode LSB.

(c). Menguji perubahan yang dialami oleh file master dan file pesan program dengan menggunakan aplikasi multi-purposes M-File (Matlab), baik ukuran dan kualitas data *(compressing)* – JPG dan BMP.

Steganografi adalah suatu teknik untuk menyembunyikan informasi yang bersifat pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, dimana disinilah fungsi dari teknik steganografi yaitu sebagai teknik penyamaran (incognito techniques) menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas oleh pihak ketiga. Dalam perang Dunia II, teknik

steganografi umum digunakan oleh tentara Jerman dalam mengirimkan pesan rahasia dari atau menuju Jerman[6]. Misalkan asumsikan terdapat gambar dengan piksel 100 x 100 dan colourencoding (embedded) 24 bits (R, G, dan B @ 8 bits) per piksel, maka colourencoding (embedded) akan mampu mewakili 0 .. 16.777.215 (mewakili 16 juta warna), dan ruang disk yang dibutuhkan = 100*100* 3 byte (karena RGB) = 30.000 bytes = 30 Kbyte atau 100*100* 24 bits = 240.000 bits.



Gambar 2.6 Kategori Steganografi

Sumber: Nizirwan Anwar, 2018

2.11 Visual Basic 2010

Visual Basic 2010 Visual Studio 2010 pada dasarnya adalah sebuah bahasa pemrograman komputer. Dimana pengertian dari bahasa pemrograman itu adalah perintah-perintah atau instruksi yang dimengerti oleh komp uter untuk

melakukan tugas-tugas tertentu (Citra Dewi, 2014). Visual Studio 2010 (yang sering juga disebut dengan VB .Net 2010) selain disebut dengan bahasa pemrograman, juga sering disebut sebagai sarana (tool) untuk menghasilkan program-progam aplikasi berbasiskan windows. Visual basic adalah sebuah bahasa pemrograman yang berpusat pada object (Object Oriented Programming) digunakan dalam pembuatan aplikasi Windows yang berbasis Graphical User Interface, hal ini menjadikan Visual Basic menjadi bahasa pemrograman yang wajib diketahui dan dikuasai oleh setiap programmer. Beberapa karakteristik obyek tidak dapat dilakukan oleh Visual Basic misalnya seperti Inheritance tidak bisa module dan Polymorphism secara terbatas bisa dilakukan dengan deklarasi class module yang mempunyai Interface tertentu. Beberapa kemampuan atau manfaat dari Visual Studio 2010 diantaranya seperti :

1. Untuk membuat program aplikasi berbasiskan windows.
2. Untuk membuat objek-objek pembantu program seperti, misalnya : kontrol *ActiveX, file Help,* aplikasi Internet dan sebagainya.
3. Menguji program *(debugging)* dan menghasilkan program berakhiran EXE yang bersifat *executable* atau dapat langsung dijalankan.

Visual studio 2010 adalah bahasa yang cukup mudah untuk dipelajari. Bagi programmer pemula yang baru ingin belajar program, lingkungan visual studio dapat membantu membuat program dalam sekejap mata. Sedangkan bagi programer tingkat lanjut, kemampuan yang besar dapat digunakan untuk membuat programprogram yang kompleks, misalnya lingkungan *net-working* atau *client server*. Bahasa Visual Studio cukup sederhana dan menggunakan kata-kata

bahasa Inggris yang umum digunakan. Kita tidak perlu lagi menghafalkan sintaks-sintaks maupun format-format bahasa yang bermacam-macam, di dalam Visual Basic semuanya sudah disediakan dalam pilihan-pilihan yang tinggal diambil sesuai dengan kebutuhan. Selain itu, sarana pengembangannya yang bersifat visual memudahkan kita untuk mengembangkan aplikasi berbasiskan Windows, bersifat mouse-driven (digerakkan dengan mouse) dan berdaya guna tinggi.

2.12 Mengenal UML

Unified Modelling Language (UML) adalah sebuah "bahasa" yang telah menjadi standar dalam industri untuk visualisasi, Pemodelan Visual dengan Menggunakan Uml dan mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Dengan menggunakan UML dapat dibuat model untuk semua jenis aplikasi piranti lunak, dimana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta ditulis dalam bahasa pemrograman apapun. Tetapi karena UML juga menggunakan class dan operation dalam konsep dasarnya, maka lebih cocok untuk penulisan piranti lunak dalam bahasa berorientasi objek seperti C++, Java, atau VB. NET.

2.13 Diagram UML

Setiap sistem yang kompleks seharusnya bisa dipandang dari sudut yang berbeda – beda sehingga bisa mendapatkan pemahaman secara menyeluruh . Untuk upaya tersebut UML menyediakan 9 jenis diagram yang dapat

dikelompokkan berdasarkan sifatnya statis atau dinamis. Ke 9 diagram dalam UML itu adalah :

a. Diagram Kelas

   Diagram kelas bersifat statis. Diagram ini memperlihatkan himpunan kelas-kelas, antarmuka-antarmuka, kolaborasi-kolaborasi serta relasi.

b. Diagram Objek

   Diagram objek bersifat statis. Diagram ini memperlihatkan objek-objek serta relasi antar objek. Diagram objek memperlihatkan instansiasi statis dari segala sesuatu yang dijumpai pada diagram kelas.

c. Use case Diagram

   Diagram ini bersifat statis. Diagram ini memperlihatkan himpunan use case dan aktor-aktor (suatu jenis khusus dari kelas). Diagram ini terutama sangat penting untuk mengorganisasi dan memodelkan perilaku dari suatu sistem yang dibutuhkan serta diharapkan pengguna.

d. *Sequence Diagram* (Diagram urutan)

   Diagram ini bersifat dinamis. Diagram *sequence* merupakan diagram interaksi yang menekankan pada pengiriman pesan *(message)* dalam suatu waktu tertentu.

e. Collaboration Diagram

   Diagram ini bersifat dinamis. Diagram kolaborasi adalah diagram interaksi yang menekankan organisasi struktural dari objek – objek yang menerima serta mengirim pesan *(message).*

f. Statechart Diagram

Diagram ini bersifat dinamis. Diagram ini memperlihatkan state – state pada sistem, memuat state, transisi, event, serta aktifitas. Diagram ini terutama penting untuk memperlihatkan sifat dinamis dari antarmuka, kelas, kolaborasi dan terutama penting pada pemodelan sistem – sistem yang reaktif.

g. Activity Diagram

Diagram ini bersifat dinamis. Diagram ini adalah tipe khusus dari diagram state yang memperlihatkan aliran dari suatu aktifitas ke aktifitas lainnya dari suatu sistem. Diagram ini terutama penting dalam pemodelan fungsi – fungsi dalam suatu sistem dan memberi tekanan pada aliran kendali antar objek.

h. Component Diagram

Diagram ini bersifat statis. Diagram ini memperlihatkan organisasi serta kebergantungan pada komponen – komponen yang telah ada sebelumnya. Diagram ini berhubungan dengan diagram kelas dimana komponen secara tipikal dipetakan ke dalam satu atau lebih kelaskelas, antarmuka – antarmuka serta kolaborasi – kolaborasi.

i. Deployment Diagram

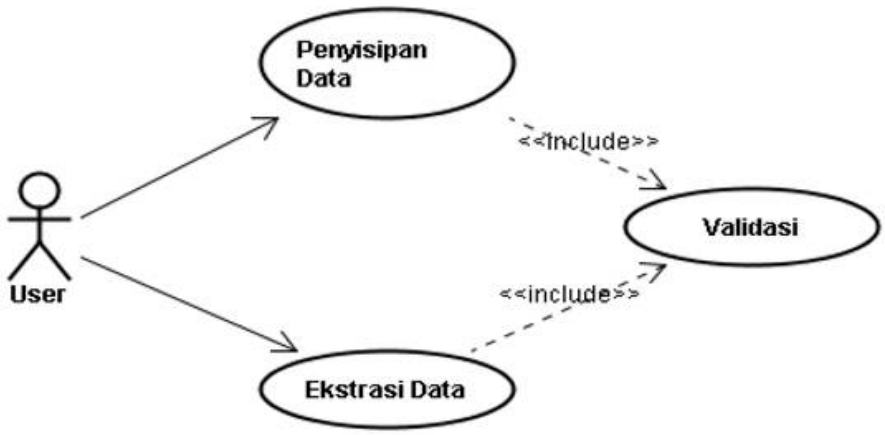
Diagram ini bersifat statis. Diagram ini memperlihatkan konfigurasi saat aplikasi dijalankan (saat run time). Dengan ini memuat simpul – simpul (node) beserta komponen – komponen yang ada di dalamnya. Deployment diagram berhubungan erat dengan diagram kompoen dimana deployment

diagram memuat satu atau lebih komponen – komponen. Diagram ini sangat berguna saat aplikasi berlaku sebagai aplikasi yang dijalankan pada banyak mesin *(distributed computing).*

Pemodelan sistem menggunakan UML dengan menggunakan *usecase* digaram. Aktor pada sistem adalah user dan terdapat dua fungsi dari penyisipan teks kedalam file audio yaitu, fungsi penyisipan data dan ekstrasi data.

2.14 *Use Case* Diagram

Use case diagram dapat mengetahui apa saja yang dapat dilakukan oleh pengguna terhadap sistem yang telah dibuat. *Use case* digaram steganografi dengan metode LSB.



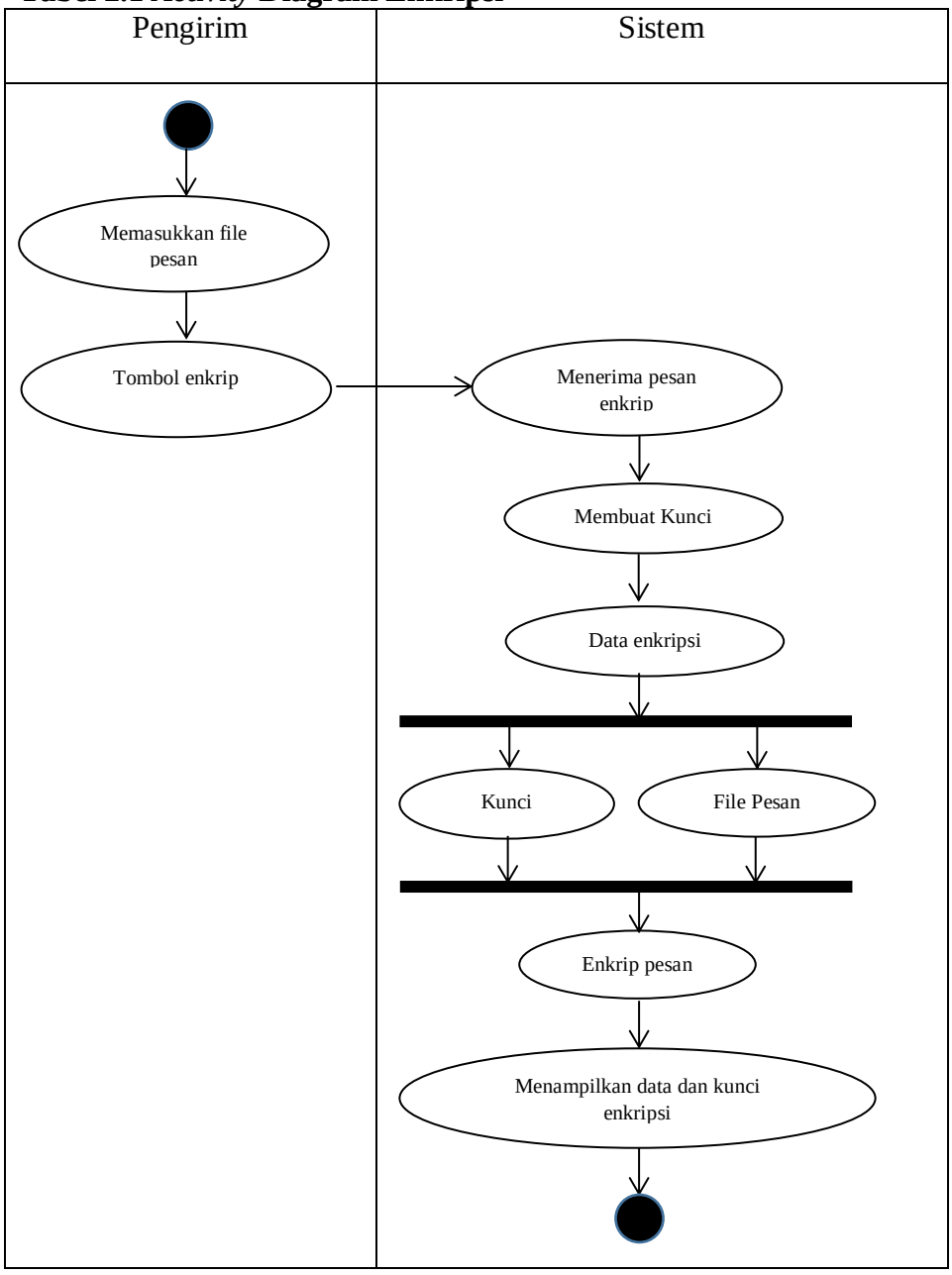
Gambar 2.7 *Use Case* Diagram

Sumber: Irwansyah, 2018

2.15 *Activity* Diagram Enkripsi

Activity diagram enkripsi menggambarkan aktivitas enkripsi yang dilakukan oleh pengirim dengan sistem pada gambar seperti berikut :

Tabel 2.1 *Activity* Diagram Enkripsi

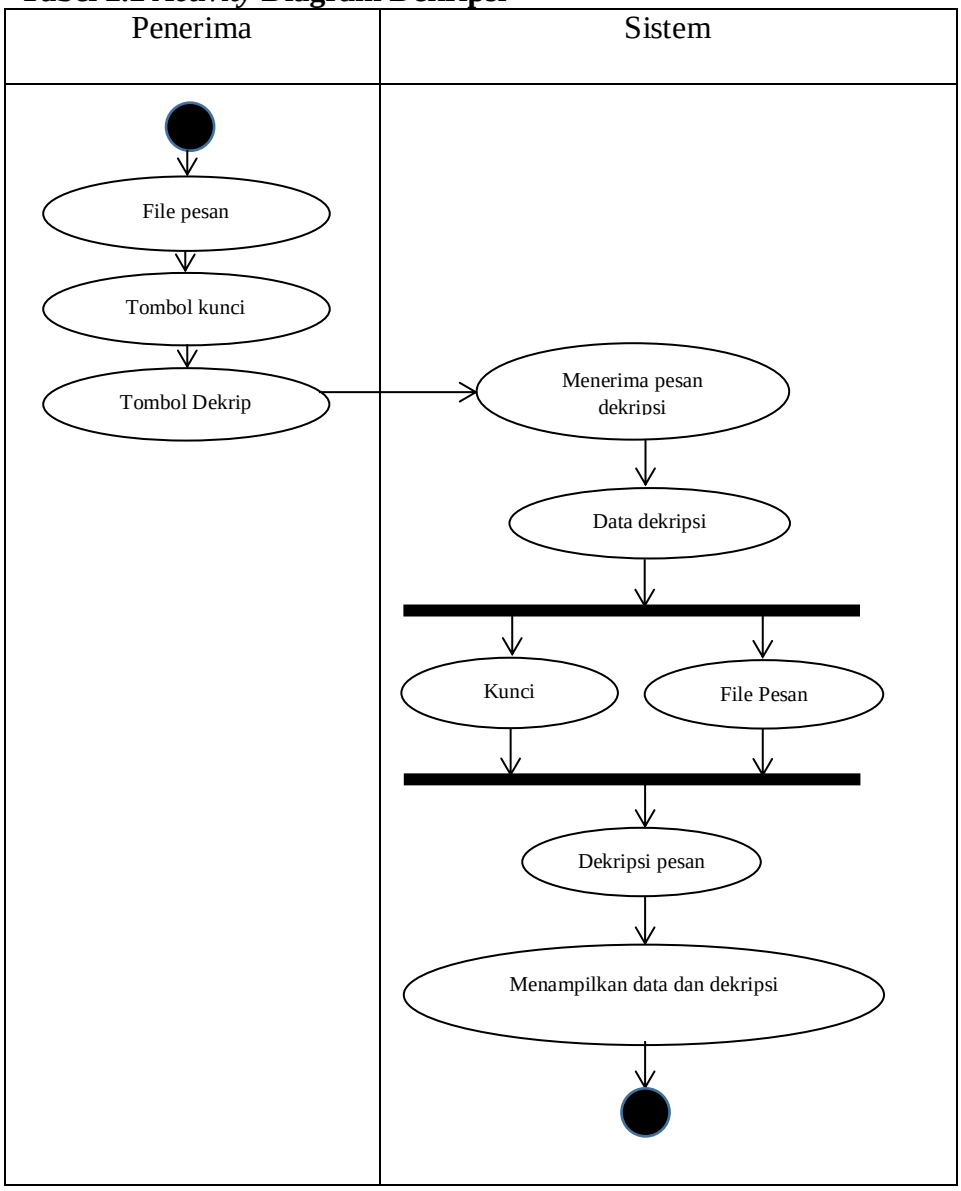


Sumber: Irwansyah, 2018

2.16 *Activity* Diagram Dekripsi

Activity diagram dekripsi menggambarkan data yang telah didekripsi antara penerima dengan sistem seperti gambar berikut :

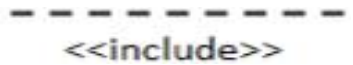
Tabel 2.2 *Activity* Diagram Dekripsi



Sumber: Irwansyah, 2018

Tabel 2.3 Simbol-simbol *Use case*

Gambar	Keterangan
	*Use case* menggambarkan fungsionalita yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktif, yang dinyatakan dengan menggunakan kata kerja
	*Actor* atau Aktor adalah Abstraction dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifika sikan aktir, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan Use Case, tetapi tidak memiliki kontrol terhadap *use case.*
	Asosiasi antara aktor dan use case, digambarkan dengan garis tanpa panah yang mengindikasika n siapa atau apa yang meminta interaksi secara langsung dan bukannya mengindikasikan data.
	Asosiasi antara aktor dan use case yang menggunakan panah terbuka untuk mengindikasikan bila aktor berinteraksi secara pasif dengan sistem.

	Include, merupakan di dalam *use case* lain (required) atau pemanggilan *use case* oleh *use case* lain, contohnya adalah pemanggilan sebuah fungsi program.
	*Extend*, merupakan perluasan dari *use case* lain jika kondisi atau syarat.

Sumber: Opik Taupik K. Mohamad Irfan, 2013

2.14 Flowchat

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

1. *System Flowchart*

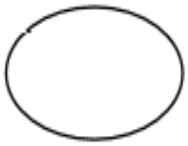
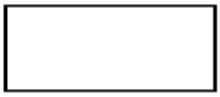
   System flowchart adalah urutan proses dalam system dengan menunjukkan alat. Media input, output, serta jenis media penyimpanan dalam proses pengolahan data. System f*lowchart* ini tidak digunakan untuk menggambar urutan langka untuk memecahkan masalah, tetapi hanya untuk menggambarkan prosedur dalam system yang di bentuk. Berikut ini adlah gambar dari simbol-simbol standar yang telah banyak digunakan pada penggunaan penggambaran system *flowchart.*

2. Program *Flowchart*

   Program flowchart adalah diagram alir yang menggambarkan urutan logika dari suatu prosedur pemecahan masalah. Untuk menggambarkan

program *flowchart* tersedia simbol-simbol standar, berikut ini adalah gambaran dari simbol-simbol standar yang digunakan program *flowchart.*

Tabel 2.4 Simbol Diagram *Flowchat*

No	Nama	Simbol	Fungsi
1	*Terminator*		Digunakan untuk mewakili simbol *start* dan *end*
2	*Arrow*		Menunjukkan alur proses
3	*Rectangle*		Menunjukkan langkah pemrosesan
4	*Trapezium*		Simbol untuk *input-output*
5	*Document*		Digunakan untuk mewakili *output*

6	*Decision*		Simbol yang berfungsi untuk menyatakan keputusan
7	*Preparation*		Simbol yang berfungsi untuk proses inisialisasi atau pemberian harga awal
8	*Connector*		Simbol untuk keluar-masuk atau penyambungan peoses pada halaman yang berbeda
9	*Manual input*		Simbol untuk memasukkan data secara manual melaui keyboard
10	*Manual operation*		Simbol yang menunjukkan pengolahan yang tidak dilakukan oleh komputer
11	*Predefine process*		Simbol untuk pelaksanaan suatu bagian
12	*Display*		Simbol yang menyatakan peralatan *output* yang digunakan seperti layar, printer, plotter dan sebagainya
13	*Magnetic disk*		Simbol yang digunakan untuk pemyimpanan data ke database
14	*Storage Data*		Simbol yang menyatakan input yang berasal dari disk atau disimpan ke disk

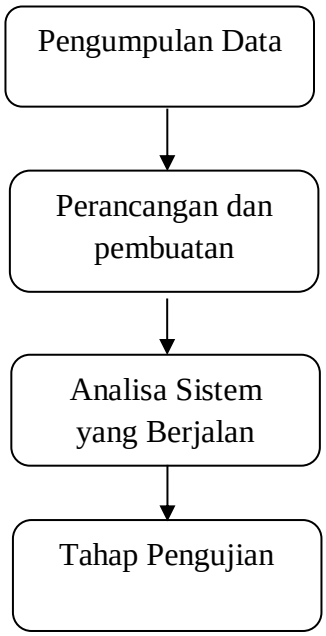
Sumber: Opik Taupik K. Mohamad Irfan, 2013

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Berikut ini adalah tahapan penelitian yang penulis lakukan:



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Adapun penjelasan dari metode pengumpulan data ialah :

3.2.1 Studi Literatur

Studi literatur dilakukan dengan melakukan pemahaman mengenai konsep dari kriptografi dan steganografi, serta file audio yang berkonsentrasi pada algoritma Twofish, metode Least Significant Bit (LSB), dan file audio mp3. Literatur pendukung ini dapat berupa jurnal, paper, makalah, artikel, buku, atau sumber lainnya. Hasil yang ingin diperoleh dari tahap ini adalah ringkasan dasar teori serta tinjauan penelitian sebelumnya berdasarkan masalah akhir.

3.2.2 Studi Pustaka

Pengumpulan data ini yang dilakukan menggunakan atau mengumpulkan sumber-sumber yang tertulis, dengan cara membaca, mempelajari dan mencatat hal yang penting sehubungan dengan penelitian tersebut. Untuk mendapatkan data yang diperlukan untuk melengkapi kesempurnaan tugas akhir ini adalah sebagai berikut :

a. Observasi

   Pada pengumpulan data atau informasi dilakukan dengan pengamatan pada objek kajian yang bertujuan untuk mendapatkan data tentang suatu masalah, sehingga mendapatkan hasil pemahaman atau sebagai pembuktian pada informasi atau keterangan yang di dapat dari sebelumnya.

b. Teknik Analisis Data

Analisis data ialah kegiatan yang dilakukan untuk mengubah data hasil dari suatu penelitian menjadi data atau informasi yang nantinya bisa dipergunakan untuk menjadikan sebuah kesimpulan.

3.3 Analisa Sistem yang Berjalan

Analisa ialah suatu kegiatan penguraian dan penyelidikan pada sebuah inti masalah agar mendapatkan suatu pemahaman, pengertian dan arti sebenarnya dari sebuah inti permasalahan tersebut. Pada sebuah keamanan komputer mempunyai sebuah istilah enkripsi, yang mana enkripsi ialah termasuk salah satu jenis yang menggunakan metode *ciphertext*. Agar memperoleh hasil teks yang sudah diubah *(ciphertext),* menggunakan angka dan table untuk konversi. Algoritma *Vigener Chiper* ialah sebuah metode keamanan informasi dengan menambah *plaintext* dengan kunci hingga menghasilkan *ciphertext* yang memiliki sifat *kongruen*.

3.4 Kelemahan Sistem Yang Berjalan

Pada system ini mempunyai kelemahan, kelemahan algoritma *vigenere cipher* muncul jika panjang kunci lebih pendek dari panjang plainteksnya sehingga terdapat perulangan kunci yang digunakan untuk mengenkripsi plainteks tersebut. Kunci yang berulang tersebut menimbulkan celah berupa jumlah pergeseran yang sama untuk setiap plainteks yang disubstitusi oleh huruf pada kunci yang sama sehingga huruf-huruf pesan atau plainteks dapat dikelompokkan berdasarkan kunci yang digunakan.

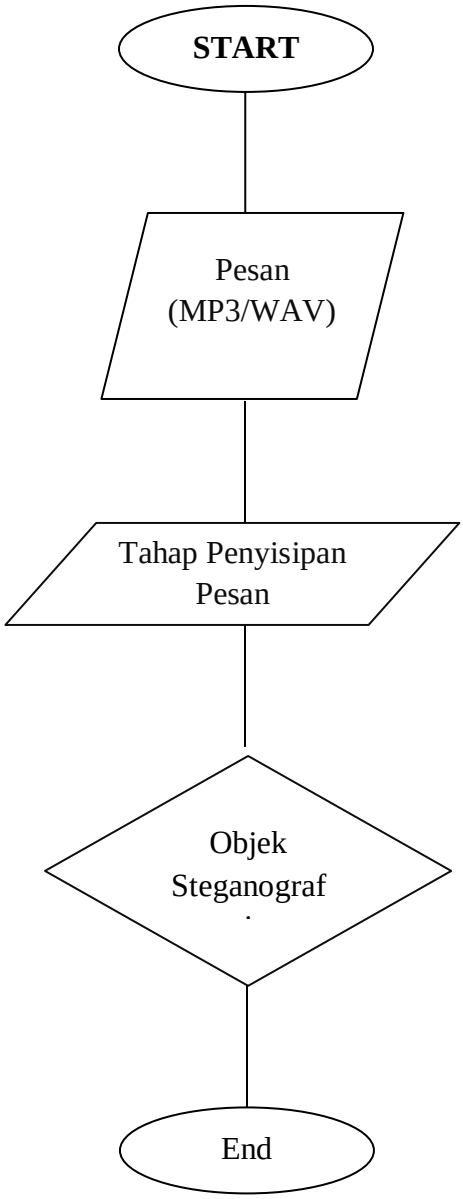
Karena terdapat kelompok huruf-huruf plainteks yang disubstitusi dengan huruf kunci yang sama karena perulangan kunci, maka tiap kelompok huruf-huruf tersebut dapat dikenakan metode analisis frekuensi terhadapnya. Sistem pengamanan tersebut masih mengalami kendala dalam mengamankan data. Salah satunya password mudah diretas karena mudah ditebak atau jumlah karakter yang minim.

3.5 Sistem Yang Diusulkan

Adapun system yang diusulkan berupa sebuah system keamanan pesan teks menggunakan kunci dengan teknik permutasi pada algoritma *vigenere chipper* yang berguna untuk sebuah pesan teks dimana hanya ada satu kunci dan menggunakan fungsi perulangan agar sulit untuk ditebaknya sebuah kunci.

3.6 Tahap Penyisipan Pesan

Tahap penyisipan pesan dilakukan pada *file audio* MP3 dengan menggunakan metode LSB. Tahap penyisipan pesan ini secara lebih rinci terdiri dari 2 proses, yaitu proses pencarian *byte* dan proses penggantian *byte* yang sama. Pada steganografi audio yang berbasis komputer, pesan rahasia tersebut ditanam dengan cara merubah urutan biner dari file suara. Steganografi audio dapat diterapkan pada file suara mp3, wav, menanam pesan rahasia pada suara digital pada umumnya. Skema tahapan penyisipan pesan secara umum dapat dilihat pada gambar 3.2.



Gambar 3.2 Flowchart Proses Penyisipan Pesan

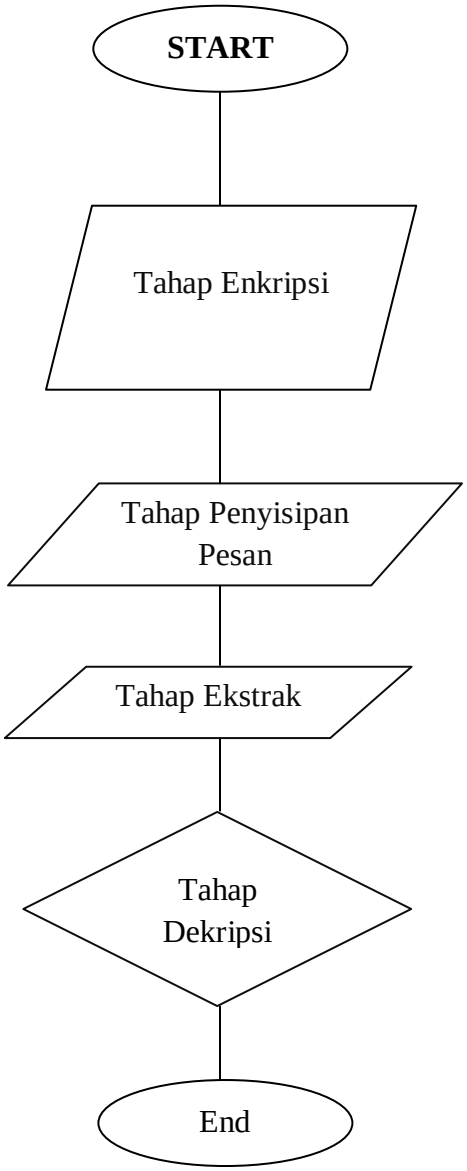
Keterangan Gambar 3.2

1. Masukan kunci yang digunakan sebagai kunci enkripsi, pesan rahasia dalam bentuk text, dan file mp3 sebagai media penampung.
2. Pesan text ditampung dalam temporary file kemudian dienkripsi menggunakan algoritma *Twofish* menghasilkan *chipertext*.
3. Dihitung jumlah *byte* homogen dalam mp3 kemudian dihitung kapasitas pesan yang mampu ditampung oleh file mp3 dengan perhitungan jumlah *byte* homogen dibagi 8. Jika ukuran chipertext lebih besar dari kapasitas yang mampu ditampung mp3 maka penyisipan pesan tidak dapat dilakukan.

3.7 Rancangan Penelitian

Ada 4 tahapan dalam implementasi aplikasi ini dengan mengkombinasikan kriptografi yang terdiri tahap enkripsi dan dekripsi pesan teks dari chiperteks menjadi plainteks serta steganografi yang terdiri dari tahap penyisipan pesan teks ke dalam file audio dan tahap ekstarsi audio steganografi sehingga menjadi file audio dan chipertext. Program ini menggunakan *Microsotf Visual Basic 2010* , kunci dan permutasi dapat mejaga dan membuat informasi lebih aman dan terjaga kerahasiaannya serta keasliannya sehingga sulit terdeteksi oleh pihak- pihak yang tidak berwenang dikarenakan penyandian tidak hanya bisa menyandikan huruf akan tetapi bisa juga digunakan untuk angka, symbol, tanda baca dan lain-lain. Dalam algoritma ini pemilihan kunci dilakukan secara acak dengan beberapa peluang agar dapat menemukan kunci yang sesuai dengan sifat algoritma *Vigenere Cipher* .

3.8 Tahap Implementasi



Gambar 3.3 *Flowchart* implementasi *kriptografi* dan *Steganografi*

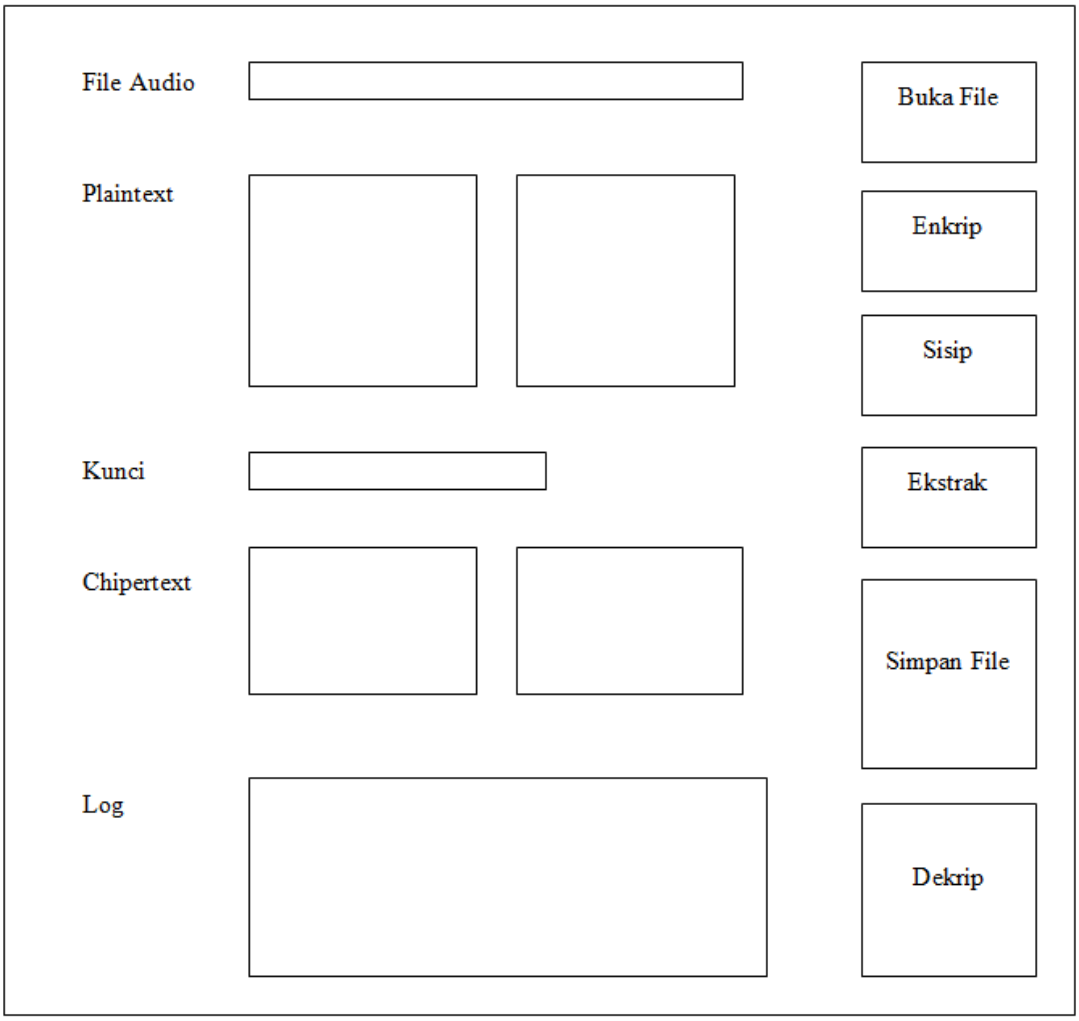
File audio menjadi masukan sebagai media penampung atau disebut file audio pembawa dan file teks menjadi masukan pesan rahasia yang akan dsisipkan. File teks terlebih dahulu melalui tahap enkripsi menghasilkan *chipertext,* kemudian chipertext disisipkan ke dalam file audio. Hasil dari proses penyisipan pesan tersebut adalah file audio steganografi. File audio mengandung psan teks rahasia didalamnya. File audio ini diharapkan mempunyai kualitas suara yang tidak jauh dengan file audio yang asli. Tahap ekstrak digunakan untuk memisahkan antara file audio pembawa dan pesan teks yang disisipkan. Pesan teks yang didapat masih dalam keadaan terenkripsi sehingga harus melalui tahap dekripsi terlebih dahulu agar menghasilkan pesan rahasia yang dapat diketahui maknanya. Proses ini dilakukan oleh orang yang akan mengirim pesan rahasia. Plaintext berupa pesan teks dienkripsi menjadi chipertext dengan menggunakan kunci publik. Kunci publik dibangkitkan dengan memasukkan password untuk keamanaan kunci. Pesan kemudian disisipkan kedalam file audio mp3 dengan menggunakan steganografi dengan metode LSB. Hasil dari proses sisipan pesan ini adalah file yang berbentuk bit dan biner. Sehingga pesan yang disisipkan tetap aman dalam file yang telah disimpan.

3.9 Perancangan Antarmuka

Adapun penjelasan dari perancangan antarmuka yaitu :

3.9.1 Perancangan Menu Steganografi LSB

Berikut adalah gambar menu steganografi :



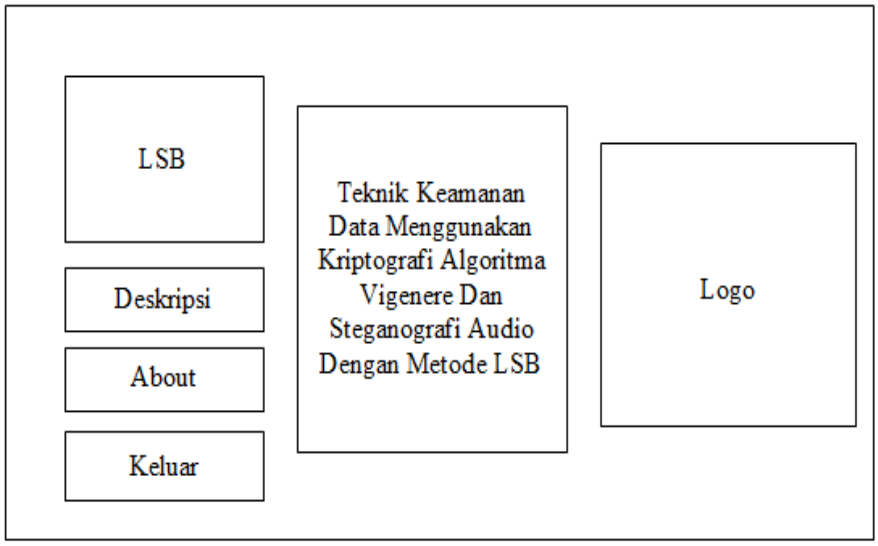
Gambar 3.4 Perancangan Steganografi LSB

Keterangan gambar 3.4

1. Nama file adalah yang akan digunakan untuk menyimpan berkas hasil sisipan.
2. Pesan adalah teks untuk menyimpan dan diketik untuk disisipkan.
3. Pesan ekstrak adalah tempat yang akan mengembalikan pesan teks yang telah diambil dari file audio.
4. Log adalah riwayat perhitungan dari metode algoritma LSB.
5. Buka file adalah tombol untuk memilih file untuk dijadikan penyimpanan.
6. Tombol ekstrak untuk melaksanakan pengambilan pesan dari file audio.
7. Tombol Sisip untuk menyembunyikan pesan dalam gambar
8. Tombol Simpan File untuk menyimpan hasil sisipan

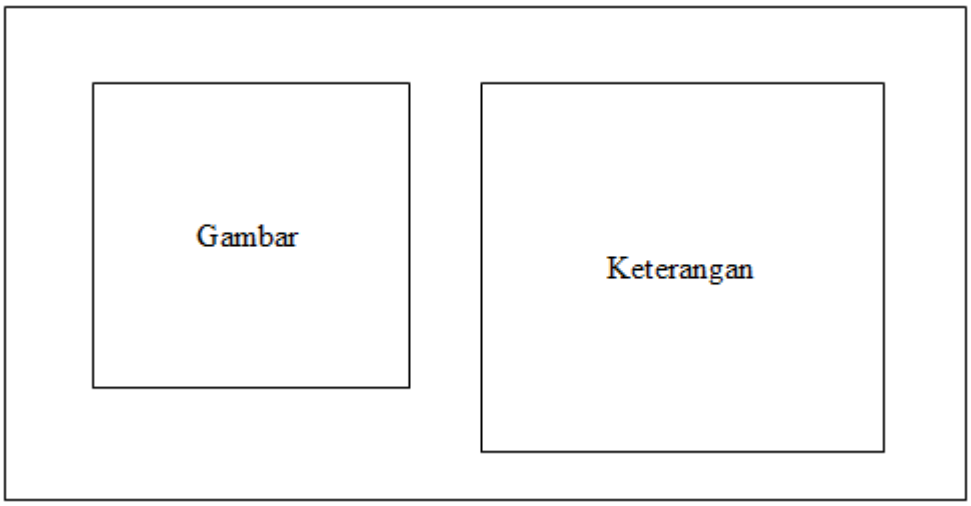
3.9.2 Perancangan Menu Utama

Berikut adalah gambar perancangan menu utama :



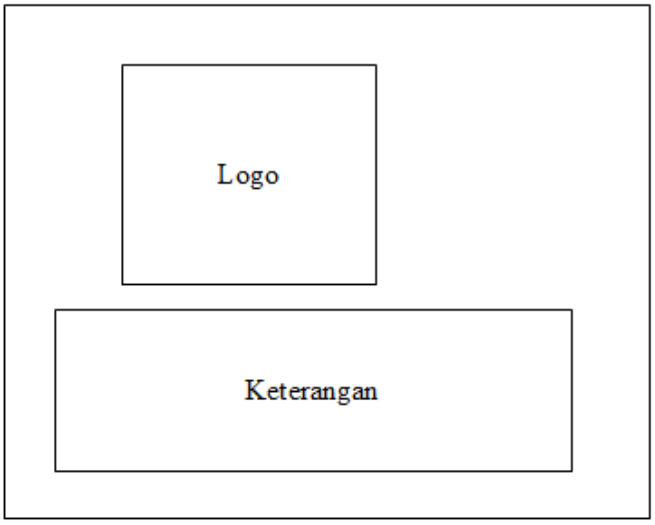
Gambar 3.5 Perancangan Menu Utama

3.9.3 Perancangan Menu Deskripsi



Gambar 3.6 Perancangan Menu Deskripsi

3.9.4 Perancangan Menu About



Gambar 3.7 Perancangan Menu About

3.10 Tahap Pengujian

Pengujian dilakukan pada 12 data *sample* yang terdiri dari 4 buah *plaintext* dan 8 buah *file audio. Plaintext* yang diujikan menggunakan format .txt dan ukuran tiap *plaintext* dinaikan kelipatan 5 KB. *File audio* terdiri dari file musik mp3.

Musik adalah kumpulan data bunyi atau suara dan keadaan diam, dalam alur waktu dan ruang tertentu. Musik instrumen merupakan musik yang mengalun tanpa lirik, hanya berupa alunan alat musik saja. Masing-masing *file audio* dibedakan berdasarkan ukuran kapasitas pesan yang mampu ditampung file mp3 dan di dalam pengujian ini ditentukan dua cakupan ukuran kapasitas pesan yang berbeda yaitu antara 10000 *byte* – 35000 *byte* dan 50000 *byte* – 75000 *byte*. Ukuran kapasitas pesan yang mampu ditampung file mp3 diperoleh dari banyaknya *byte* yang sama dibagi 8, karena dalam metode LSB, 1 *byte file audio* digunkan untuk 1 bit karakter pesan.

Aspek pertama yang diuji kapasitas pesan teks yang mampu ditampung oleh file mp3, tiap file mp3 disisipkan pesan teks dengan ukuran kelipatan 5 KB. File mp3 terakhir yang masih mampu menampung pesan berarti mempunyai kapasitas yang paling besar. Aspek kedua yang diuji adalah perhitungan waktu eksekusi. Waktu eksekusi yang dihitung antara lain : waktu enkripsi, waktu dekripsi, waktu penyisipan pesan ke dalam *file audio,* dan waktu ektraksi file mp3 stego. Aspek ketiga yang diuji adalah perhitungan kualitas suara file mp3 stego yang dihasilkan. Kualitas suara file mp3 stego diui secara obyektif dengan terlebih dahulu mengukur kekuatan sinyal file audio menggunakan alat berupa Sound Level Meter Extechtipe 407736, lalu dihitung nilai Peak Signal to Note Ratio (PSNR).

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

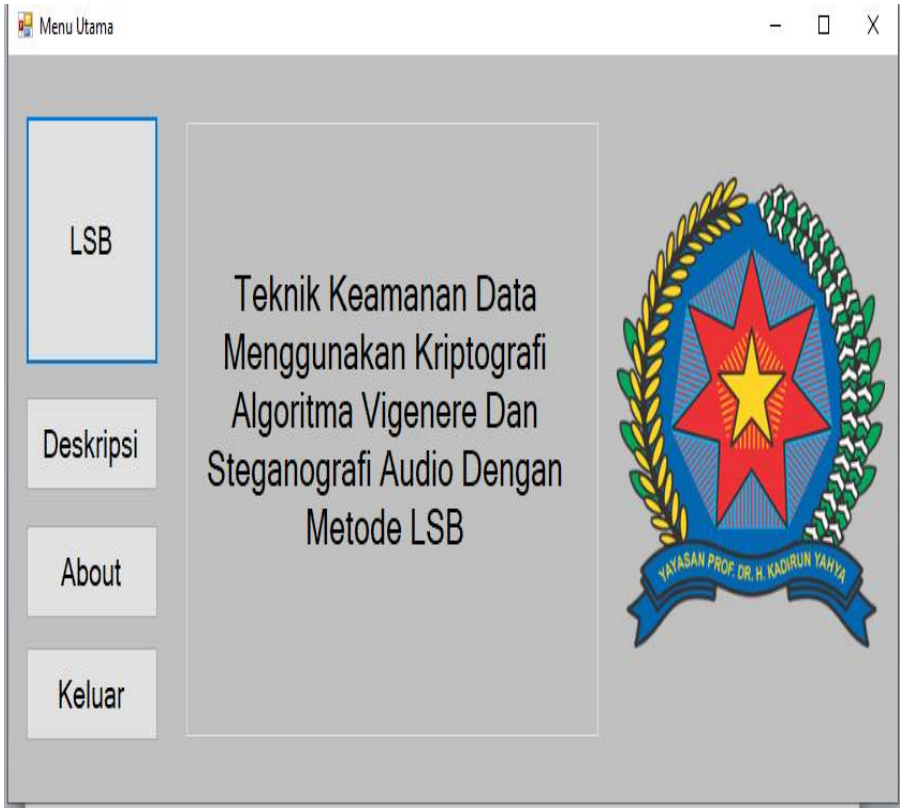
Pada tahap implementasi sistem ini adalah sebuah tahap aplikasi yang sudah dirancang dan dijalankan. Tahap tersebut menunjukkan setiap proses yang sedang berjalan dan mempu bekerja seperti yang diinginkan. Proses perancangan ini menggunakan *microsoft visual basic 2010* yang ditampilkan melalui form – form agar menjadi sarana bagi penggunanya dalam melakukan proses implementasi.

4.2 Pengujian Sistem

Dalam pengujian sebuah sistem memiliki tujuan untuk menemukan kesalahan pada aplikasi yang dibangun dan memperbaikinya, selain itu pengujian sistem ini dilakukan untuk mengetahui apakah sistem dapat berjalan sesuai yang diharapkan.

4.2.1 Tampilan Menu Utama

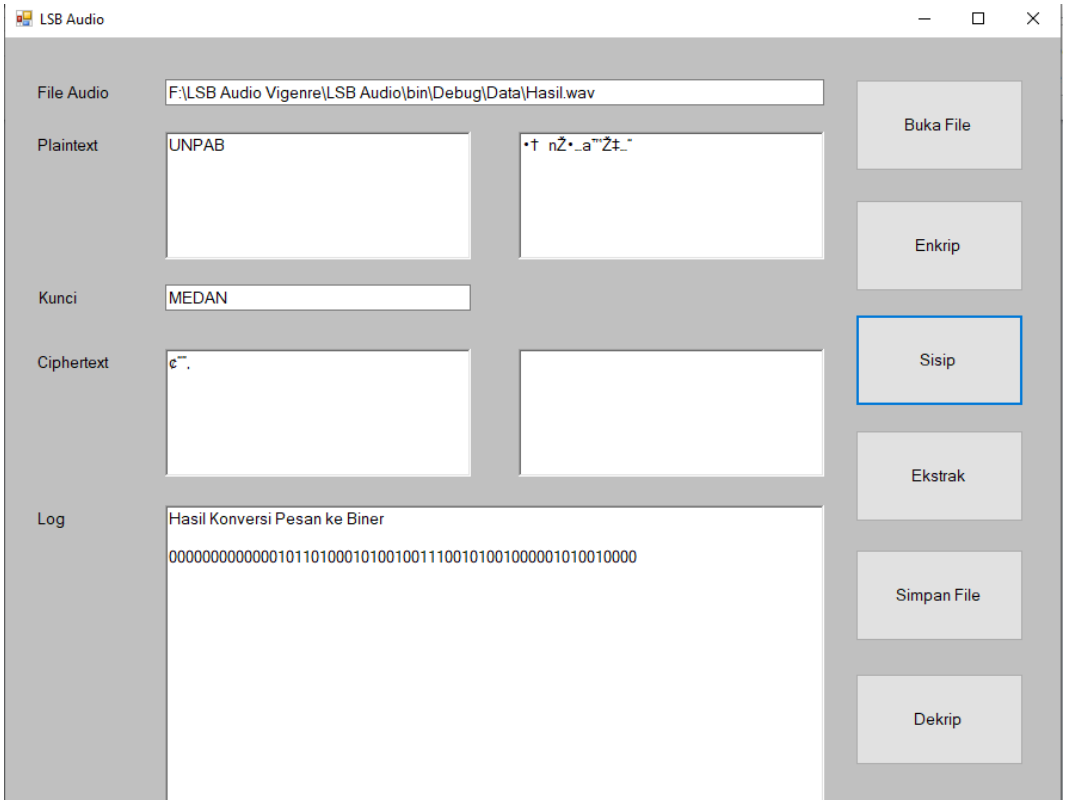
Pada tampilan gambar dibawah ini adalah tampilan awal ketika aplikasi ini dijalankan. Pada form ini terdapat form dengan fungsi masing-masing, selain itu juga terdapat tombol yaitu : LSB, Deskripsi, About, dan tombol keluar yang memiliki fungsi masing-masing yang juga memiliki fungsi berbeda.



Gambar 4.1 Tampilan Menu Utama

4.2.2 Tampilan Menu LSB (*least significant bit)*

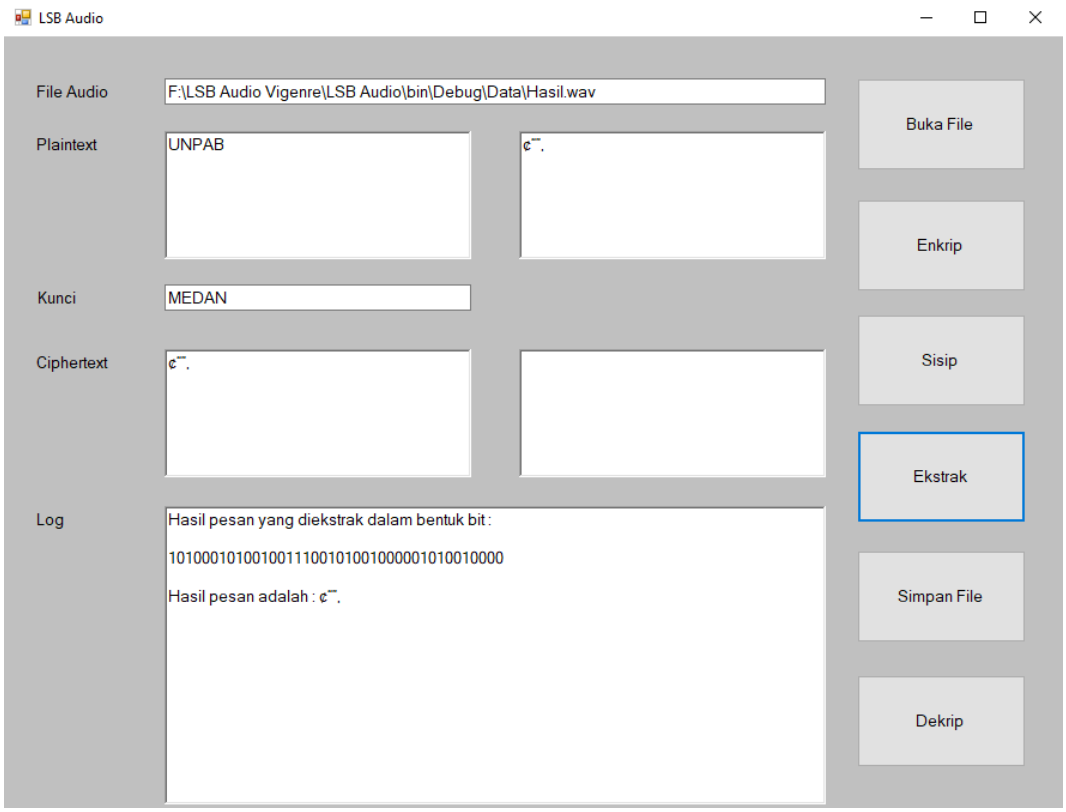
Tombol ini menampilkan menu untuk menyisipkan data kedalam file audio, kemudian akan di sisipkan kedalam sebuah pesan yang telah dituliskan, dan kemudian akan menjadi hasil konvensi pesan biner. Kemudian pesan akan di ekstrak menjadi pesan berupa bit.



Gambar 4.2 Tombol Sisip Pada Menu LSB

Berikut ini adalah pesan yang disisipkan adalah Universitas pembanunan panca budi, kemudian pesan akan berubah menjadi hasil konvensi pesan ke biner seperti yang tertulis dibawah ini :

000000000010001001010101010011100100100101010110010001010101001001
010011010010010101010001000001010100110010000001010000010001010100
110101000010010000010100111001000111010101010100111001000001010011
100010000001010000010000010100111001000011010000010010000001000010
010101010100010001001001.

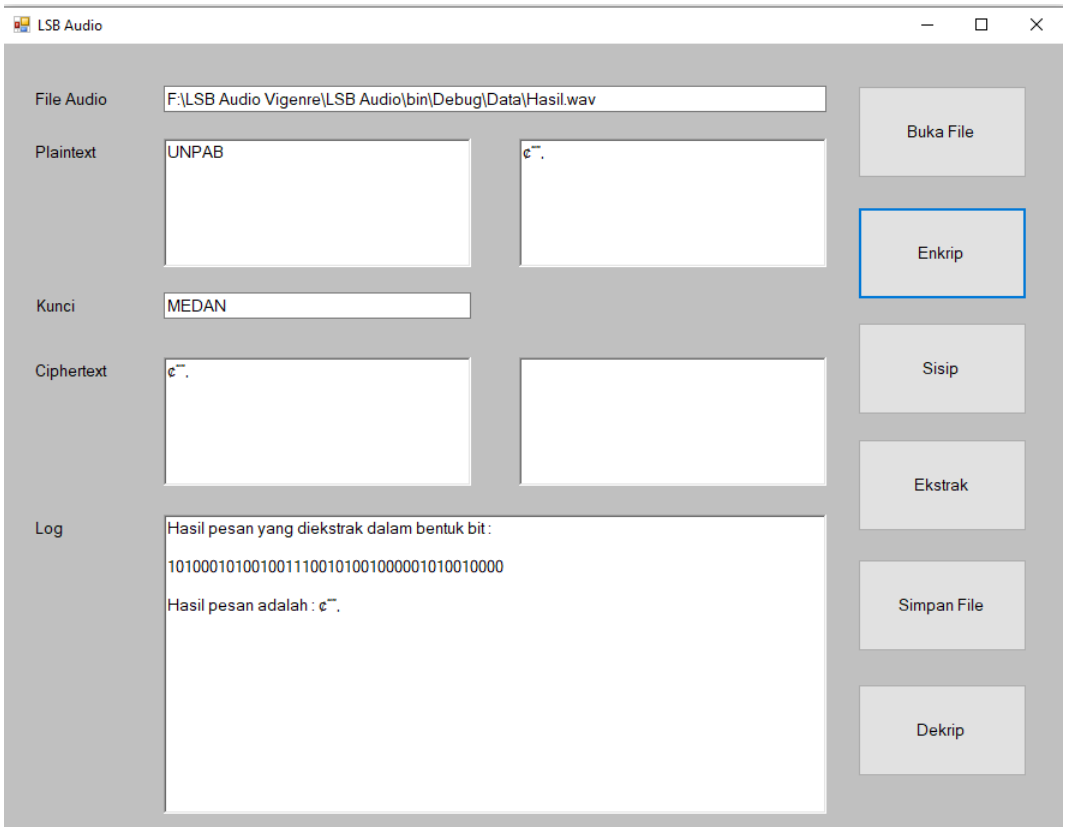


Gambar 4.3 Tombol Ekstrak Pada Menu LSB

Berikut ini adalah pesan yang akan di ekstrak kedalam bentuk bit seperti yang tertulis dibawah ini :

01010101010011100100100101010110010001010101001001010011010010010101000100000101010011001000000101000001000101010011010100001001000001010011100100011101010101010011100100000101001110001000000101000001000001010011100100001101000001001000000100000100101010101000100001001001.

Dan hasil pesan yang diekstrak kedalam bentuk bit adalah sebuah pesan yang tertulis, Universitas Pembangunan panca budi. Setelah data sudah disisipkan dan diekstrak maka data disimpan kedalam file. Kemudian data akan tersimpan didalam sebuah documen project LSB audio.



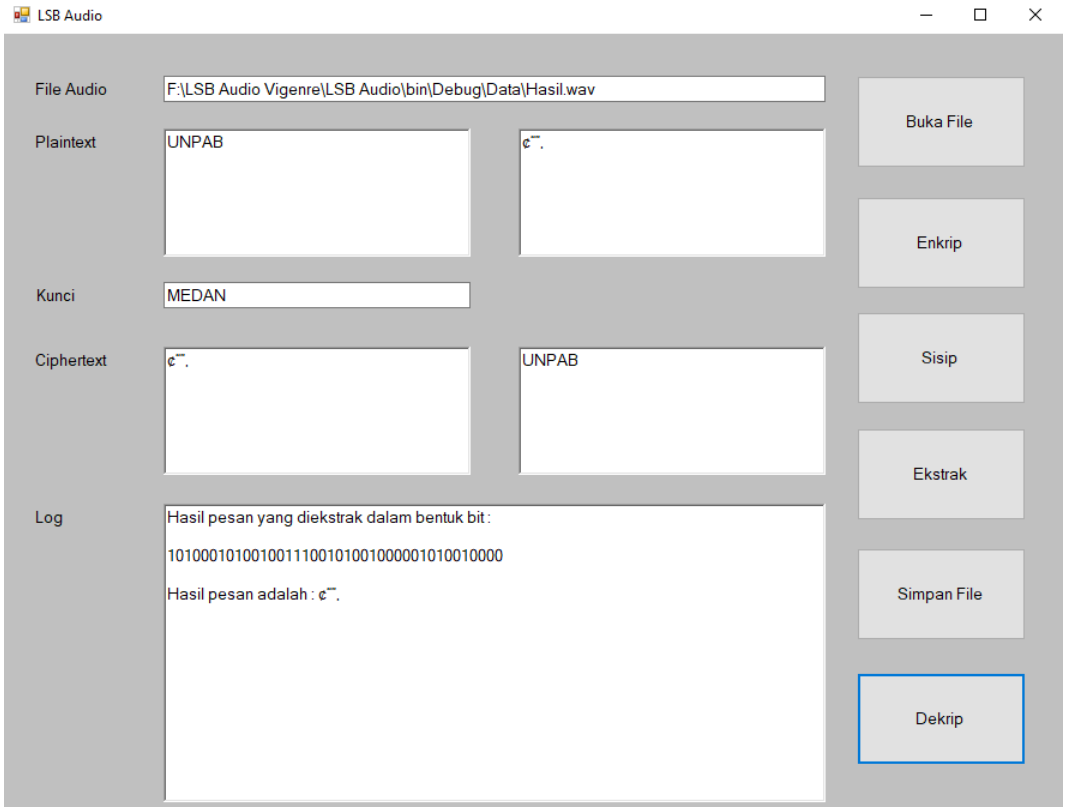
Gambar 4.4 Tombol Enkrip Pada LSB

Berikut ini adalah pesan yang akan dienkrip adalah Universitas Pembangunan Panca Budi. Dan pesan yang disisipkan akan menghasilkan konvensi pesan ke biner.

Hasil pesan yang dienkrip dalam bentuk bit :

10100010100100111001010010000010100100000

Hasil pesan adalah : ¢“”,•
0101010000100101010101000001010010000010000001010000010010010100110001001001010010000100000101001110.



Gambar 4.5 Tombol Dekrip Pada LSB

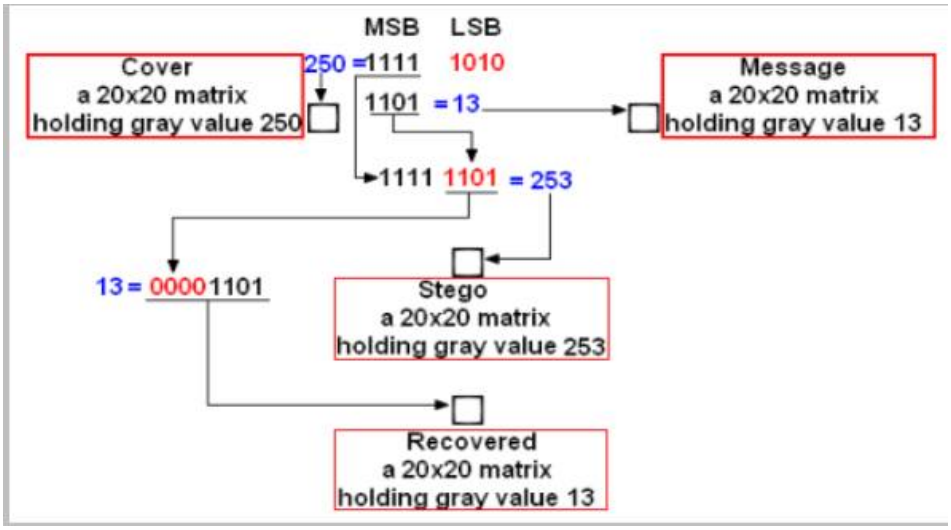
Berikut ini adalah sebuah pesan yang telah didekrip kedalam bentuk bit. Hasil pesan yang diekstrak dalam bentuk bit :

10100010100100111001010010000010100100000

Hasil pesan adalah : ¢“”,•

0100100001001001010001000101010101010000001000000100000101000100010000010100110001000001010010000010000001010011010001010100001001010100001010010000010000001010000010010010100110001001001010010000100000101001110.

4.2.3 Tampilan Menu Deskripsi Steganografi



Gambar 4.6 Menu Deskripsi Steganografi

Steganografi *(information hiding)* adalah sebuah teknik untuk menyembunyikan pesan rahasia pada sebuah host media atau disebut juga cover media. Steganografi berasal dari bahasa yunani yang memiliki arti "menulis tersembunyi". Digunakan dalam beragam bentuk selama ribuan tahun. Pada abad ke-5 sebelum masehi, histaiacus mencukur kepala seorang budak kemudian menuliskan pesan dikepalanya dan membiarkan rambut tumbuh untuk menutupi pesan yang ditulis. Sehingga untuk membaca pesan tersebut rambut pembawa pesan harus dicukur kembali. Perkembangan teknologi turut membawa perubahan pada steganografi baik teknik dan media yang digunakan.

4.2.4 Tampilan Menu About

Gambar 4.7 Menu About

Menu about beriisikan sebuah data kelengkapan diri pada seorang penulis dan pembuat program yang telah dimsukan kedalam sebuah aplikasi steganografi. Kemudian setelah semua aplikasi berjalan dengan baik maka di akhiri dengan tombol keluar yang ada pada menu utama.

4.3 Perhitungan *Vigenere*

Pada Algoritma *Vigenere Chiper* hanya memiliki satu kunci rahasia saja untuk mengubah *plaintext* menjadi *chipertext* pembangkitan kunci pergeseran kemudian enkripsi. Kunci tersebut dapat dibangkitkan apabila kunci yang akan digunakan memenuhi syarat tukar posisi yaitu :

$$XY = 0sp\ (jtp - 1)$$

Dimana pertukaran posisi dilakukan secara acak, pada jumlah tukar posisi jumlah pertukaran posisi akan sepanjang dengan kunci tersebut. Pemilihan kunci tidak hanya berupa huruf, akan tetapi bisa juga dengan angka ataupun simbol dengan demikian semakin sulit kuncinya maka akan semakin sulit seorang kriptanalis membaca kunci tersebut.

4.4 Validasi Sistem

ASCII *(American Standard Code for Information Interchange).* Merupakan kode standar untuk pertukaran informasi dalam pengkodean huruf dan simbol seperti *unicode* dan *hex* tetapi ASCII lebih bersifat *universal*. Dalam bahasa komputer 0 dan 1 tidak ada cara lain untuk mewakili huruf dan karakter yang bukan nomor. Semuanya harus menggunakan 0 dan 1 salah satu jalan untuk berbahasa dengan komputer lain dengan cara menggunakan tabel ASCII. Tabel ASCII merupakan tabel atau daftar yang berisi semua huruf dalam alfabet romawi ditambah beberapan karakter tambahan. Dalam tabel akan ada karakter yang diwakili oleh sejumlah kode. Berikut adalah tabel ASCII.

4.5 Tabel ASCII *(American Standard Code for Information Interchange).*

Dec	Hex	Name	Char	Ctrl-char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	0	Null	NUL	CTRL-@	32	20	Space	64	40	@	96	60	`
1	1	Start of heading	SOH	CTRL-A	33	21	!	65	41	A	97	61	a
2	2	Start of text	STX	CTRL-B	34	22	"	66	42	B	98	62	b
3	3	End of text	ETX	CTRL-C	35	23	#	67	43	C	99	63	c
4	4	End of xmit	EOT	CTRL-D	36	24	$	68	44	D	100	64	d
5	5	Enquiry	ENQ	CTRL-E	37	25	%	69	45	E	101	65	e
6	6	Acknowledge	ACK	CTRL-F	38	26	&	70	46	F	102	66	f
7	7	Bell	BEL	CTRL-G	39	27	'	71	47	G	103	67	g
8	8	Backspace	BS	CTRL-H	40	28	(	72	48	H	104	68	h
9	9	Horizontal tab	HT	CTRL-I	41	29	)	73	49	I	105	69	i
10	0A	Line feed	LF	CTRL-J	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	VT	CTRL-K	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	FF	CTRL-L	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage feed	CR	CTRL-M	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	SO	CTRL-N	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	SI	CTRL-O	47	2F	/	79	4F	O	111	6F	o
16	10	Data line escape	DLE	CTRL-P	48	30	0	80	50	P	112	70	p
17	11	Device control 1	DC1	CTRL-Q	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	DC2	CTRL-R	50	32	2	82	52	R	114	72	r
19	13	Device control 3	DC3	CTRL-S	51	33	3	83	53	S	115	73	s
20	14	Device control 4	DC4	CTRL-T	52	34	4	84	54	T	116	74	t
21	15	Neg acknowledge	NAK	CTRL-U	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	SYN	CTRL-V	54	36	6	86	56	V	118	76	v
23	17	End of xmit block	ETB	CTRL-W	55	37	7	87	57	W	119	77	w
24	18	Cancel	CAN	CTRL-X	56	38	8	88	58	X	120	78	x
25	19	End of medium	EM	CTRL-Y	57	39	9	89	59	Y	121	79	y
26	1A	Substitute	SUB	CTRL-Z	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	ESC	CTRL-[	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	FS	CTRL-\	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	GS	CTRL-]	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	RS	CTRL-^	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	US	CTRL-_	63	3F	?	95	5F	_	127	7F	DEL

.

4.6 Coding Form LSB *(least significant bit)*

```
Public Class frmLSBAudio
    Dim Log, LogBit As String
    Dim JlhPesan, JlhSample As Integer
    Dim Data_WAV(), PT_ASCII() As Byte
    Dim Pesan, Pesan_Bit As String
    Dim K1, K2 As Byte
```

Berikut ini adalah kode program untuk membuka file tempat informasi disisipkan.

```
    Private Sub btnBukaFile_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnBukaFile.Click
        Dim openFileDialog As OpenFileDialog = New
OpenFileDialog()
        openFileDialog.Title = "Buka File Audio"
        openFileDialog.InitialDirectory =
Application.StartupPath & "\Data"
        openFileDialog.Filter = "WAV files (*.wav)|*.wav|All
files (*.*)|*.*"
        openFileDialog.FilterIndex = 1
        openFileDialog.RestoreDirectory = True


        If (openFileDialog.ShowDialog() <> DialogResult.OK)
Then
            Exit Sub
        End If

        txtFile.Text = openFileDialog.FileName
        Data_WAV =
System.IO.File.ReadAllBytes(openFileDialog.FileName)
        JlhSample = Data_WAV.Length - 44

        txtLog.Text = "File Sukses dibuka!"
    End Sub
```

Berikut ini adalah kode program untuk menyimpan file tempat informasi disisipkan.

```
   Private Sub btnSimpanFile_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnSimpanFile.Click
        Dim saveFileDialog As SaveFileDialog = New
SaveFileDialog()
        saveFileDialog.Title = "Simpan File Audio"
        saveFileDialog.InitialDirectory =
Application.StartupPath & "\Data"

        saveFileDialog.Filter = "WAV files (*.wav)|*.wav|All
files (*.*)|*.*"
        saveFileDialog.FilterIndex = 1
        saveFileDialog.RestoreDirectory = True

        If (saveFileDialog.ShowDialog() <> DialogResult.OK)
Then
            Exit Sub
        End If
System.IO.File.WriteAllBytes(saveFileDialog.FileName,
Data_WAV)
    End Sub

    Private Sub btnEmbed_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnSisip.Click
        Log = ""
        LogBit = ""
        Pesan_Bit = ""
        Pesan = txtPesan.Text
        JlhPesan = Pesan.Length

        If JlhPesan > 255 Then
            K1 = JlhPesan / 256
            K2 = JlhPesan Mod 256
        Else
```

```
            K1 = 0
            K2 = JlhPesan
        End If

        'Penambahan Kunci 2 karakter pertama
        Pesan = Convert.ToChar(K1) & Convert.ToChar(K2) &
Pesan
        JlhPesan = Pesan.Length

        'Membuat array bit dari pesan
        For i = 0 To Pesan.Length - 1
            Dim Bin As String
            Bin = Convert.ToString(Convert.ToByte(Pesan(i)),
2)

            For h = 0 To 8 - Bin.Length - 1
                Bin = "0" & Bin
            Next

            Pesan_Bit &= Bin
            LogBit &= Bin & vbCrLf
        Next
        Log &= "Hasil Konversi Pesan ke Biner" & vbCrLf &
vbCrLf & Pesan_Bit & vbCrLf & vbCrLf

        'Simpan pesan ke audio
        Dim Sinyal As Byte = 0
        Dim SinyalBin As String = ""

        For i = 0 To (JlhPesan * 8) - 1

            Sinyal = Data_WAV(i + 44)
            SinyalBin = Convert.ToString(Sinyal, 2)
'toBiner(Sinyal)

            SinyalBin = SinyalBin.Remove(SinyalBin.Length -
1, 1)
            SinyalBin &= Pesan_Bit(i)
            Sinyal = Convert.ToByte(SinyalBin, 2)
'toDecimal(SinyalBin)
            Data_WAV(i + 44) = Sinyal
        Next

        txtLog.Text = Log
    End Sub

    Private Sub btnEkstrak_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnEkstrak.Click
        Log = ""
```

```
        'Ambil panjang pesan dari audio
        Pesan_Bit = ""
        For i = 0 To 15
            Dim Bin As String = Convert.ToString(Data_WAV(i
+ 44), 2)

            Bin = Bin(Bin.Length - 1)
            Pesan_Bit &= Bin
        Next

        JlhPesan = Convert.ToInt16(Pesan_Bit, 2)

        'Ambil pesan dari audio
        Pesan = ""
        Pesan_Bit = ""

        For i = 0 To (JlhPesan * 8) - 1
            Dim Bin As String

            Bin = Convert.ToString(Data_WAV(i + 44 + 16), 2)
            Bin = Bin(Bin.Length - 1)
            Pesan_Bit &= Bin
        Next

        For i = 0 To JlhPesan - 1
            Pesan &=
Convert.ToChar(Convert.ToByte(Pesan_Bit.Substring((i * 8),
8), 2))
        Next

        Log &= "Hasil pesan yang diekstrak dalam bentuk bit
: " & vbCrLf & vbCrLf & Pesan_Bit & vbCrLf & vbCrLf
        Log &= "Hasil pesan adalah : " & Pesan & vbCrLf
        txtPE.Text = Pesan
        txtLog.Text = Log
    End Sub

    Private Sub btnKeluar_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs)
        Application.Exit()
    End Sub

End Class
```

4.6.1 Coding form menu utama

Berikut ini adalah tampilan coding menu utama :

```
Public Class frmMenu
    Private Sub btnGronfeld_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnGronfeld.Click
        frmLSBAudio.ShowDialog()
    End Sub

    Private Sub btnDeskripsi_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnDeskripsi.Click
        frmDeskripsi.ShowDialog()
    End Sub

    Private Sub btnAbout_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnAbout.Click
        frmAbout.Show()
    End Sub
    Private Sub btnKeluar_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnKeluar.Click
        Application.Exit()
    End Sub

End Class
```

4..6.2 Coding Form Menu Deskripsi

Berikut ini adalah tampilan coding tombol deskripsi :

```
Public Class frmMenu

    Private Sub btnGronfeld_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnGronfeld.Click
        frmLSBAudio.ShowDialog()
    End Sub

    Private Sub btnDeskripsi_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnDeskripsi.Click
        frmDeskripsi.ShowDialog()
    End Sub
```

```
    Private Sub btnAbout_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnAbout.Click
        frmAbout.Show()
    End Sub
    Private Sub btnKeluar_Click(ByVal sender As
System.Object, ByVal e As System.EventArgs) Handles
btnKeluar.Click
        Application.Exit()
    End Sub

End Class
```

4.6.3 Coding Form Menu About

Berikut ini adalah tampilan coding tombol about :

```
Public Class frmMenu

    Private Sub btnGronfeld_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnGronfeld.Click
        frmLSBAudio.ShowDialog()
    End Sub

    Private Sub btnDeskripsi_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles btnDeskripsi.Click
        frmDeskripsi.ShowDialog()
    End Sub

    Private Sub btnAbout_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnAbout.Click
        frmAbout.Show()
    End Sub

    Private Sub btnKeluar_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnKeluar.Click
        Application.Exit()
    End Sub

End Class
```

4.6.4 Coding Form Menu Keluar

Berikut ini adalah tampilan coding tombol keluaar :

```
Public Class frmMenu

    Private Sub btnGronfeld_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnGronfeld.Click
        frmLSBAudio.ShowDialog()
```

```
    End Sub

    Private Sub btnDeskripsi_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles btnDeskripsi.Click
        frmDeskripsi.ShowDialog()
    End Sub
```

```
    Private Sub btnAbout_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnAbout.Click
        frmAbout.Show()
    End Sub

    Private Sub btnKeluar_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnKeluar.Click
        Application.Exit()
    End Sub

End Class
```

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat diambil kesimpulan sebagai berikut:

1. Pesan dapat dikombinasikan dengan algoritma steganografi dengan metode LSB, dan pesan dapat disisipkan kedalam file audio sebagai media penampung pesan dan pesan rahasia.
2. Proses ekstrasi pesan untuk mendapatkan data yang tersembunyi dengan menggunakan steganografi bisa dilakukan dengan baik tanpa kehilangan sedikit data pun.
3. Perancangan penyisipan pesan kedalam file audio mp3 ini menggunakan *Microsoft Visual Studio 2010.*

5.2 Saran

Adapun saran-saran yang dapat penulis berikan sebagai berikut:

1. Dalam pembuatan aplikasi kriptografi dan steganografi, sistem ini diharapkan dapat berguna untuk menjaga dan menjamin kerahasiaan data.
2. Pesan teks tidak terbatas pada format .txt atau file pesan yang dapat berupa audio dan dapat menggunakan media berformat mp3 atau wav.

DAFTAR PUSTAKA

Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIf). Vol. 1. No. 1. 2017.

Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol. 300, No. 1, p. 012067). IOP Publishing.

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.

Batubara, Supina, Sri Wahyuni, and Eko Hariyanto. "Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam." Seminar Nasional Royal (SENAR). Vol. 1. No. 1. 2018.

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

Fachri, B. (2018, September). APLIKASI PERBAIKAN CITRA EFEK NOISE SALT & PAPPER MENGGUNAKAN METODE CONTRAHARMONIC MEAN FILTER. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 87-92).

Fachri, B., Windarto, A. P., & Parinduri, I. (2019). Penerapan Backpropagation dan Analisis Sensitivitas pada Prediksi Indikator Terpenting Perusahaan Listrik. JEPIN (Jurnal Edukasi dan Penelitian Informatika), 5(2), 202-208.

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

Hasugian, H. A. (2013). Implementasi Algoritma Hill Chiper Dalam Penyandian Data.*Jurnal Pelita Informatika Budi Darma*. Volume 4 Nomor 2.

INDRA PERMANA, A. M. I. N. U. D. D. I. N. "SISTEM PAKAR MENDETEKSI HAMA DAN PENYAKIT TANAMAN KELAPA SAWIT PADA PT. MOEIS KEBUN SIPARE-PARE KABUPATEN BATUBARA." (2013).

Fairu Zabadi, M. 2010. Implementasi Kriptografi Klasik Menggunakan Borland Delphi. *Jurnal Dinamika Informatika* Volume 4 Nomor 2.

M. Miftakul Amin, (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. *Jurnal Pseudocode* Volume III Nomor 2.

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

Permana, Aminuddin Indra. "Kombinasi Algoritma Kriptografi One Time Pad dengan Generate Random Keys dan Vigenere Cipher dengan Kunci EM2B." (2019).

Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." Seminar Nasional Teknologi Informasi Dan Multimedia, ISSN. 2015.

Wahidun Sipayung, (2014). Perancangan Citra Watermaking Pada Citra Digital Menggunakan Metode Discrete Cosine Transform (DCT). *Pelita Informatika Budi Darma.* Volume VII Nomor 3.

Sri Hartati Monalisa, (2014). Steganografi Pada File Citra Untuk Pengamanan Data Menggunakan Spread Spectrum. *Pelita Informatika Budi Darma.* Volume VII Nomor 3.

Mara Husein, (2014). Implementasi Caesar Cipher Untuk Pemyembunyian Pesan Teks Rahasia Pada Citra Dengan Menggunakan Metode Least Significant Bit (LSB). *Pelita Informatika Budi Darma.* Volume VII Nomor 2.

Citra Dewi Astuti Br, Tarigan, 2014. Steganografi Pada File Audio Mp3 Untuk Pengamanan Data Menggunakan Metode Least Significant Bit (LSB). *Pelita Informatika Budi Darma.* Volume VI Nomor 3.

Nizirwan Anwar, 2018. Perancangan Steganografi Hidden Message Dengan Metode LSB Berbasis Matlab. *Jurnal Algoritma, Logika dan Komputasi.* Volume I Nomor 1.

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

Putra, Randi Rian. "IMPLEMENTASI METODE BACKPROPAGATION JARINGAN SARAF TIRUAN DALAM MEMPREDIKSI POLA PENGUNJUNG TERHADAP TRANSAKSI." JurTI (Jurnal Teknologi Informasi) 3.1 (2019): 16-20.

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