IMPLEMENTASI STEGANOGRAFI LEAST SIGNIFIACTION BIT DAN KRIPTOGRAFI HILL CIPHER UNTUK KEAMANAN DATA KEPOLISIAN SEKTOR SELEBAR KOTA BENGKULU

SKRIPSI

OLEH :

JAKA YUNSAR
NPM : 18010016

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU
2023

IMPLEMENTASI STEGANOGRAFI LEAST SIGNIFIACTION BIT DAN KRIPTOGRAFI HILL CIPHER UNTUK KEAMANAN DATA KEPOLISIAN SEKTOR SELEBAR KOTA BENGKULU

PROPOSAL SKRIPSI

OLEH :

JAKA YUNSAR
NPM : 18010016

Diajukan Untuk Memperoleh Gelar Sarjana Komputer (S.Kom)
Pada Program Studi Informatika

PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN
BENGKULU
2023

IMPLEMENTASI STEGANOGRAFI LEAST SIGNIFIACTION BIT DAN KRIPTOGRAFI HILL CIPHER UNTUK KEAMANAN DATA KEPOLISIAN SEKTOR SELEBAR KOTA BENGKULU

SKRIPSI

OLEH :

JAKA YUNSAR
NPM : 18010016

Disetujui Oleh :

Pembimbing Utama	Pembimbing Pendamping
Sapri, S,Kom, M.Kom	**Juju Jumadi, S.Kom, M.Kom**
NIDN. 02.150171.02	**NIDN. 02.111282.01**

Mengetahui,
Ketua Program Studi Informatika

Liza Yulianti, S.Kom, M.Kom
NIDN : 02.160772.01

IMPLEMENTASI STEGANOGRAFI LEAST SIGNIFIACTION BIT DAN KRIPTOGRAFI HILL CIPHER UNTUK KEAMANAN DATA KEPOLISIAN SEKTOR SELEBAR KOTA BENGKULU

SKRIPSI

OLEH :

JAKA YUNSAR
NPM : 18010016

Telah dipertahankan di depan Tim Penguji Universitas Dehasen Bengkulu Pada :

Hari : Jumat
Tanggal : 16 Juni 2023
Tempat : Ruang Sidang Universitas Dehasen Bengkulu

Skripsi Telah Diperiksa dan Disahkan Oleh :

Penguji	Nama	NIDN	Tanda Tangan
Ketua	Sapri, S.Kom, M.Kom	02.150171.02	
Anggota	Juju Jumadi, S.Kom, M.Kom	02.111282.01	
Anggota	Khairil, S.Kom, M.Kom	02.130475.01	
Anggota	Eko Suryana, S.Kom, M.Kom	02.151174.01	

Mengetahui,

Dekan
Fakultas Ilmu Komputer

UNIVERSITAS DEHASEN UNIVED BENGKULU FAKULTAS ILMU KOM

Siswanto, SE, S.Kom, M.Kom
NIDN : 02.240363.01

DAFTAR RIWAYAT HIDUP

Penulis bernama Jaka Yunsar dilahirkan di Kota Bengkulu pada tanggal 25 Mei 1999. Anak kedua dari dua bersaudara. Ayah bernama Toni dan Ibu bernama Sariati.

Menyelesaikan pendidikan sekolah dasar (SD) Negeri 79 Kota Bengkulu pada tahun 2012. Kemudian penulis melanjutkan di sekolah menegah pertama (SMPN) negeri 08 kota Bengkulu dan lulus pada tahun 2015 dan menyelesaikan pendidikan Sekolah Menengah Atas (SMA) 3 kota Bengkulu pada tahun 2018 kemudian melanjut pendidikan keperguruan tinggi yaitu pada Universitas Dehasen (UNIVED) Bengkulu dengan mengambil jurusan Informatika pada Fakultas Ilmu Komputer, untuk jenjang Strata Satu (S-1)

MOTTO DAN PERSEMBAHAN

MOTTO DAN PERSEMBAHAN

MOTTO:

- Hidup itu untuk berguna bukan untuk sempurna

PERSEMBAHAN:

Terima Kasih Allah SWT karna RahmatNYA lah saya bisa menyelesaikan skripsi ini dan skripsi ini saya persembahkan kepada:

- Ayah dan ibuku (Toni dan Sariati) yang telah memberikan kasih sayang, memberi suport, tiada henti memberikan Do'a-Do'a, dan yang pastinya membiayai kuliah dari awal sampai selesai, yang selalu sabar sampai saya menyelesaikan pendidikan ini. Ibu dan ayah telah melalui banyak perjuangan dan rasa sakit. Tapi saya berjanji tidak akan membiarkan semua itu sia-sia. I love you amah abah
- Kakak ku Rio Demaensen yang selalu memberikan semangat. Makasih kakak ku sayang.
- Buat keluarga besar terima kasih selalu ada di saat keluarga saya butuhkan
- Buat kawan seperjuangan ku Carles, Agus, Rahmat, dan Farhan terima kasih kamu selalu siap menemani, membantu dan selalu mendukung dalam proses pengerjaan skripsi ini dari awal sampai akhir.
- Kakak ku Rio Demaensen terima kasih telah membantu dalam penyelesaain skripsi ini
- Para dosen dan pembimbingku (Bapak Sapri, M.Kom dan Bapak Juju Jumadi M.Kom) yang telah membantu saya dalam menyelesaikan skripsi ini.
- Buat teman-teman kelas Informatika angkatan 2018 yang selalu meberikan semangat dan motivasi
- Almamater kuning yang aku banggakan

ABSTRAK

IMPLEMENTASI STEGANOGRAFI LEAST SIGNIFIACTION BIT DAN KRIPTOGRAFI HILL CIPHER UNTUK KEAMANAN DATA KEPOLISIAN SEKTOR SELEBAR KOTA BENGKULU

Oleh :

Jaka Yunsar[1]
Sapri, M.Kom[2]
Juju Jumadi, M.Kom[2]

Keamanan menjadi faktor penting dalam proses pengiriman informasi, bahkan keamanan menjadi suatu kebutuhan agar dapat melindungi informasi dari orang yang tidak berhak untuk mengakses informasi tersebut,oleh karena itu, diperlukan adanya suatu mekanisme yang dapat menjaga kerahasiaan pesan dan salah satu metode untuk menjaga kerahasian pesan yaitu dengan cara melakukan penyandian teks melalui proses enkripsi dan dekripsi dengan menggunakan algoritma *Hill Cipher* dan penyisipan teks ke dalam gambar melalui proses *encode* dan *decode* dengan menggunakan metode *Least Significant Bit*. Algoritma Hill Cipher menggunakan sebuah matriks persegi sebagai kunci yang digunakan dan menerapkan aritmatika modulo.

Implementasi sistem menggunakan bahasa pemrograman Visual Basic 2010 dan metode yang digunakan dalam penelitian ini adalah waterfall, aplikasi ini dirancang menggunakan *UML* (*Unified Modelling Language*).

Hasil dari penelitian ini adalah sebuah aplikasi perangkat lunak yang berguna untuk menjaga kerahasiaan pesan dengan metode algoritma metode *least significant bit* dan *Hill Cipher*. Dengan adanya aplikasi Kripsteno ini dapat menjadi salah satu solusi dalam pengamanan data.

Kata kunci : Steganografi, Least Signifiaction Bit, Kriptografi, Hill Cipher

1. Mahasiswa
2. Pembimbing

ABSTRACT

THE IMPLEMENTATION OF LEAST SIGNIFIACTION BIT AND HILL CIPHER CRYPTOGRAPHIC STEGANOGRAPHY FOR POLICE DATA SECURITY AT SECTOR SELEBAR OF BENGKULU CITY

By :
Jaka Yunsar [1]
Sapri [2]
Juju Jumadi [2]

Security is an important factor in the process of sending information, even security becomes a necessity in order to be able to protect information from people who are not entitled to access the information. From encoding text through encryption and decryption processes using Hill Cipher algorithm and inserting text into images through encode and decode processes using the Least Signifiaction Bit method. The Hill Cipher algorithm used a square matrix as the key and applies modulo arithmetic. System implementation used Visual Basic 2010 programming language and the method used in this study is waterfall, this application is designed using UML (Unified Modeling Language). The result of this research is software application that is useful for maintaining the confidentiality of messages with the least Signifiaction bit and Hill Cipher algorithm methods. With Kripsteno application, it can be a solution in data security

Keywords : Steganography, Least Signifiaction Bit, Cryptography, Hill Cipher.

1. Student
2. Supervisors

SURAT PERNYATAAN ORISINILITAS DAN PERSETUJUAN AKADEMIK SKRIPSI

Yang bertanda tangan dibawah ini :

Nama : Jaka Yunsar

NPM : 18010016

Faktultas /Program Studi : Ilmu Komputer / Informatika

Dengan ini menyatakan dengan sesungguhnya bahwa Skripsi dengan Judul :

IMPLEMENTASI STEGANOGRAFI LEAST SIGNIFIACTION BIT DAN KRIPTOGRAFI HILL CIPHER UNTUK KEAMANAN DATA KEPOLISIAN SEKTOR SELEBAR KOTA BENGKULU

1. Adalah benar dibuat oleh saya sendiri untuk memenuhi persyaratan kelulusan akademik.
2. Pada bagian-bagian tertentu dalam penulisan skripsi ini yang saya kutip dari hasil karya orang lain telah ditulis sumbernya secara jelas sesuai dengan norma, kaidah dan cara penulisan ilmiah.
3. Jika dikemudian hari diketahui berdasarkan bukti-bukti yang kuat ternyata skripsi tersebut dibuat oleh orang lain atau diketahui bahwa skripsi tersebut merupakan *plagiat/mencontek/menjiblak* hasil karya tulis ilmiah orang lain, maka dengan inisaya bersedia menerima sanksi pencabutan gelar akademik yang saya peroleh dan sanksi-sanksi lainnya sesuai dengan peraturan yang berlaku.
4. Dan atas orisinilitas tersebut diatas, maka saya menyetujui untuk memberi kepada Universitas Dehasen Bengkulu hak atas bebas royalti non-eksklusif untuk menyimpan, mengalih mediakan, mendistribusikan dan mempublikasikan skripsi saya tanpa perlu meminta izin selama mencantumkan nama saya sebagai penulis/pencipta.
5. Saya bersedia menanggung secara pribadi tanpa melibatkan Universitas Dehasen Bengkulu segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam Karya Ilmiah saya ini

Demikian surat pernyataan ini dibuat dengan sebenarnya dan untuk dipergunakan sebagaimana mestinya.

Bengkulu, Juni 2023

Hormat Saya

Jaka Yunsar

KATA PENGANTAR

Puji Syukur saya panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan karunia-NYA, sehingga skripsi yang berjudul "**Implementasi Steganografi Least Signifiaction Bit Dan Kriptografi Hill Cipher Untuk Keamanan Data Kepolisian Sektor Selebar Kota Bengkulu**" dapat diselesaikan dalam waktu yang telah ditetapkan.

Pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah banyak membantu penulis selama penyusunan skripsi ini kepada :

1. Bapak Prof. Dr. Husaini, SE., M.Si, Ak, CA, CRP Selaku Rektor Universitas Dehasen (UNIVED) Bengkulu
2. Bapak Siswanto, SE, S.Kom, M.Kom selaku Dekan Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.
3. Ibu Liza Yulianti, M.Kom selaku Ketua Prodi Informatika Universitas Dehasen Bengkulu.
4. Bapak Sapri, S.Kom, M.Kom selaku pembimbing utama yang telah membimbing dengan sabar dan memberikan masukan serta saran kepada penulis
5. Bapak Juju Jumadi, S.Kom, M.Kom Selaku pembimbing pendamping yang telah memberikan masukan dan saran kepada penulis.
6. Pimpinan beserta seluruh Staf Polsek Selebar Kota Bengkulu yang telah membantu dalam penelitian ini.

7. Buat teman-teman yang tidak bisa disebutkan satu persatu baik formal dan non formal, terima kasih atas bantuannya selama penyelesaian penulisan skripsi ini

Penulis menyadari masih banyak kekurangan dalam penulisan skripsi ini, namun penulis mengharapkan saran dan kritik yang sifatnya membangun guna menunjang perkembangan ilmu pengetahuan khususnya ilmu komputer.

Bengkulu, Juni 2023

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Gambar **Halaman**

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting pada sistem informasi saat ini. Hal ini di sebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya suatu teknik-teknik yang baru yang disalah gunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut. Ironisnya, teknik yang digunakan untuk mengancam keamanan data selalu setingkat lebih maju daripada teknik yang digunakan untuk mengamankan data.

Kepolisian Sektor (Polsek) Kota Bengkulu memiliki banyak data yang harus dijaga kerahasiaannya, termasuk data mengenai kriminal yang terdapat di wilayah tersebut. Oleh karena itu, dibutuhkan suatu sistem keamanan yang efektif untuk melindungi data tersebut dari akses yang tidak sah.

Salah satu teknik yang dapat digunakan untuk menjaga kerahasiaan data adalah steganografi. Steganografi adalah teknik untuk menyembunyikan pesan atau informasi rahasia dalam suatu objek atau media yang mungkin tidak terlihat seperti gambar, audio, video, atau teks. Tujuan utama nya adalah untuk menyembunyikan keberadaan pesan tersebut sehingga pesan tersebut hanya diketahui oleh pihak yang dituju. Dalam steganografi, pesan yang akan disimpan di dalam media yang

digunakan tidak akan mengganggu informasi asli atau kualitas media tersebut. Teknik steganografi dapat dilakukan dengan berbagai cara, salah satunya adalah menggunakan teknik *Least Significant Bit* (LSB).

Teknik steganografi LSB memanfaatkan bit paling tidak signifikan dari sebuah gambar untuk menyimpan pesan rahasia. Dalam hal ini, gambar ikan atau laut dapat dijadikan media penyimpanan pesan rahasia. Pesan rahasia tersebut akan disembunyikan pada bit-bit yang tidak mempengaruhi kualitas gambar secara signifikan sehingga pesan tersebut tidak dapat dideteksi oleh mata manusia.

Namun demikian, pesan yang disembunyikan dengan teknik steganografi LSB masih rentan terhadap serangan kriptografi. Oleh karena itu, untuk meningkatkan keamanan data, teknik steganografi LSB dapat digabungkan dengan teknik enkripsi seperti *Hill Cipher*. *Hill Cipher* merupakan salah satu teknik enkripsi yang menggunakan matriks sebagai kunci enkripsi. Teknik ini dapat menghasilkan pesan terenkripsi yang sulit untuk dipecahkan.

Dengan menggabungkan teknik steganografi LSB dan *Hill Cipher*, pesan rahasia yang disembunyikan pada gambar akan lebih sulit diakses oleh pihak yang tidak berwenang. Oleh karena itu, implementasi kedua teknik tersebut dapat meningkatkan keamanan data pada Polsek Selebar Kota Bengkulu.

Berdasarkan latar belakang diatas, maka penulis tertarik untuk melakukan penelitian yang dituangkan dalam proposal skripsi dengan judul **"Implementasi Steganografi *Least Signification Bit* (LSB) dan**

Kriptografi *Hill Cipher* Untuk Keamanan Data Pada Kepolisian Sektor (Polsek) Selebar Kota Bengkulu".

1.2 Rumusan Masalah

Berdasarkan latar belakang yang diuraikan di atas, didapat suatu permasalahan yaitu bagaimana Implementasi Steganografi *Least Signification Bit* (LSB) dan *Hill Cipher* Untuk Keamanan Data Polsek Selebar Kota Bengkulu.

1.3 Batasan Masalah

Agar permasalahan tidak meluas dan menyimpang dari pembahasan, maka penulis membuat batasan masalah sebagai berikut :

1. File yang akan disisipkan adalah berbentuk teks.
2. Media digital penampungnya berupa file gambar (*image*) dengan ekstensi bmp.
3. Bahasa program yang digunakan untuk membuat aplikasi ini adalah Visual Studio 2010.

1.4 Tujuan Penelitian

1.4.1 Tujuan Umum

Tujuan umum dilakukannya penelitian ini adalah sebagai salah satu syarat untuk menyelesaikan pendidikan Strata Satu (S1) Pada Program Studi Informatika Fakultas Ilmu Komputer.

1.4.2 Tujuan Khusus

Tujuan penelitian ini adalah untuk merancang suatu perangkat lunak enkripsi-dekripsi dengan menggunakan steganografi LSB dan kriptografi *Hill Cipher* pada Polres Selebar Kota Bengkulu.

1.5 Manfaat Penelitian

Dari penjabaran diatas ada pula manfaat yang diberikan adalah :

1. Mempermudah dalam pengamanan data yang diinginkan dengan aman
2. Menambah pengetahuan dan wawasan penulis tentang steganografi LSB dan kriptografi khususnya enkripsi dan dekripsi di dalam pengamanan dan kerahasian suatu data *Hill Cipher*.
3. Perangkat lunak yang dibangun dapat menjadi salah satu alternatif untuk keamanan data.

BAB II

LANDASAN TEORI

2.1 Pengertian Steganografi

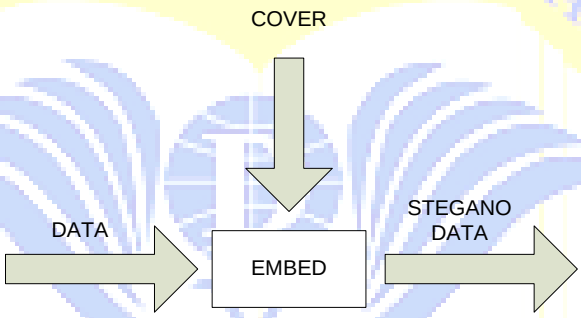
Steganografi (*covered writing*) didefinisikan sebagai ilmu dan seni untuk menyembunyikan pesan rahasia (*hiding message*) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Steganografi telah dikenal semenjak tahun 500 SM, dimana Herodotus (sejarawan Yunani) menuliskan pesan pada kepala budak dan menunggu sampai rambut kepalanya tumbuh kembali sehingga pesan tidak terlihat dan selanjutnya dia diutus untuk menyampaikan pesan tersebut tanpa menimbulkan kecurigaan oleh bangsa Persia (Lutfi & Rosihan, 2018)

Steganografi adalah salah satu alternatif solusi dalam mengamankan informasi yang bersifat penting dan pribadi. Istilah steganografi berasal dari bahasa Yunani, yaitu *steganos* yang berarti penyamaran atau penyembunyian dan *graphein* yang berarti tulisan. Jadi, steganografi bisa diartikan sebagai seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama (Wibisono, Waluyo, & Ujianto, 2020)

Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan atau informasi rahasia didalam informasi lainnya. Steganografi mempunyai sejarah yang hampir sama dengan

kriptografi, keduanya banyak digunakan ketika zaman perang (Syahril & Jaya, 2019)

Steganografi pada media digital file gambar digunakan untuk mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia dengan cara menurunkan kualitas warna pada file gambar yang belum disisipi pesan rahasia. Sehingga dengan keterbatasan tersebut manusia sulit menemukan gradasi penurunan kualitas warna pada file gambar yang telah disisipi pesan rahasia (Lutfi & Rosihan, 2018). Gambaran steganografi dapat ditunjukkan seperti pada gambar 2.1 berikut :



Gambar 2.1 Proses Steganografi
Sumber (Lutfi & Rosihan, 2018)

Didalam metode steganografi, memiliki beberapa kriteria yang harus dimiliki, antara lain (Gunawan & Sumarno, 2018) :

1. *Impercepbility*

   Keberadaan pesan tidak dapat dipersepsi oleh indra manusia, baik indra pendengaran maupun indra penglihatan

2. *Fidelity*

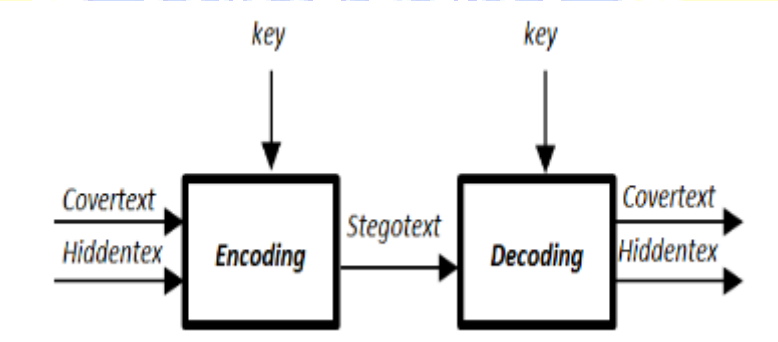
   Mutu dari citra penampung tidak jauh berubah. Setelah penambahan pesan rahasia, citra hasil steganografi masih terlihat dengan baik.

Pengamat tidak mengetahui kalau didalam citra tersebut masih terdapat teks rahasia.

3. *Recovery*

   Pesan rahasia yang disembunyikan didalam citra digital harus dapat diungkapkan kembali seperti aslinya

Steganografi yang menggunakan media gambar *hiddent text* atau *embedded text* yang sudah disisipkan merupakan pesan yang akan disisipkan kedalam *conver text* atau *cover object*, yaitu file gambar yang digunakan sebagai media penampung pesan kedalam file gambar yang dihasilkan *stego text* atau *stego-object* yang merupakan sebuah file gambar yang memiliki pesan *embedded* (Gunawan & Sumarno, 2018). Secara umum cara kerja steganografi dapat dilihat pada gambar 2.2 berikut :



Gambar 2.2 Cara Kerja Steganografi Secara Umum
Sumber (Wibisono, Waluyo, & Ujianto, 2020)

Pada Gambar 2.2, dijelaskan bahwa penyisipan pesan kedalam *cover text* dinamakan *encoding*, sedangkan ekstraksi pesan *stego text* dinamakan *decoding*. Kedua proses ini memerlukan kunci rahasia (*stegokey*) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Ada beberapa istilah penting dalam steganografi menurut (Wibisono, Waluyo, & Ujianto, 2020) antara lain :

1. *Cover-Object*

   Objek asli yang digunakan untuk menyembunyikan informasi

2. *Message*

   Informasi atau pesan aktual yang disembunyikan. Pesan dapat berupa teks atau gambar.

3. *Stego-Object*

   Menyisipkan pesan atau informasi rahasia ke dalam *cover object*

4. *Stego-Key*

   Kunci yang digunakan untuk menyisipkan atau mengekstrasi pesan dari *cover object* dan *stego-object*, kunci dapat berupa huruf, angka ataupun simbol

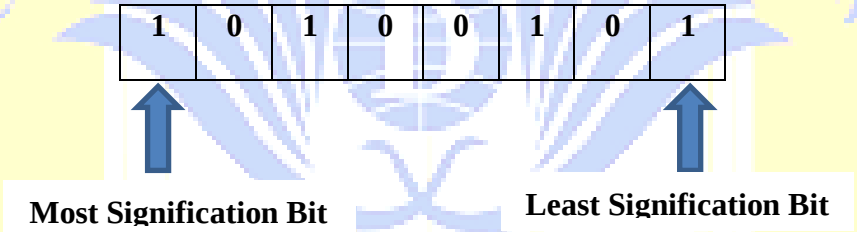
2.2 Metode *Least Significant Bit* (LSB)

Metode *Least Significant Bit* (LSB) atau biasa disebut dengan LSB suatu metode modifikasi steganografi suatu melakukan perubahan pada bit yang paling kanan atau bit yang kurang berarti. Media penampung LSB ini biasanya menggunakan citra digital atau gambar (Yusup, Carudin, & Purnamasari, 2020).

Penyembunyian pesan dilakukan dengan merubah bit-bit didalam segmen citra dengan bit-bit pesan rahasia. Metode yang paling sering digunakan adalah dengan modifikasi LSB (*Least Significant Bit*) pada citra penampung. Pada susunan bit didalam sebuah byte, ada bit yang paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling

kurang significant atau LSB (*Least Significant Bit*) (Gunawan & Sumarno, 2018).

Least sicnificant bit (LSB) merupakan sebuah algoritma dari metode steganografi yang sering digunakan dalam melakukan penyembunyian suatu data atau informasi, dimana langkah dari sebuah proses ini mengberikan suatu penyembunyian sebuah informasi kedalam suatu media, seperti citra atau sebuah gambar, dasar dari algoritma ini menggunakan sebuah bilangan biner dimana bilangannya terdiri dari dua angka, 0 dan 1, pada teknik ini kita mengganti bit pada posisi LSB pada data dengan bit dimana data yang akan disembunyikan, dan bit yang diganti adalah bit yang terakhir, sehingga walau data tersebut sudah diubah kita dapat mengenalinya.



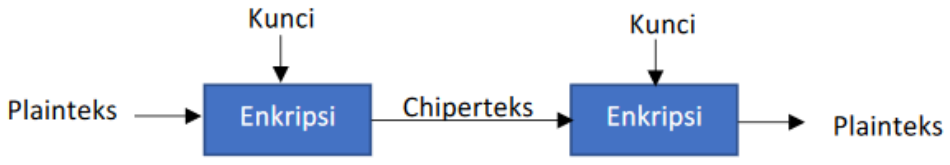
2.3 Kriptografi

Criptography berasal dari bahasa Yunani. Menurut bahasanya, istilah tersebut terdiri dari kata *kripto* dan *graphia*. *Kripto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan) (Fauzah & Iqbal, 2021). Menurut terminologinya, kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan, ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi dari pesan tersebut kemungkinan dapat disadap oleh pihak lain. Untuk menjaga keamanan pesan, maka pesan tersebut dapat *discreamble* / diacak atau diubah menjadi kode yang tidak dapat dimengerti oleh orang lain (Azlin et

al., 2018). Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu himpunan yang berisi elemen plainteks dan himpunan yang berisi elemen chipteks. Enkripsi dan dekripsi merupakan fungsi transformasi antara dua himpunan tersebut.

Enkripsi adalah proses menggunakan algoritma tertentu untuk mengubah data atau informasi menjadi format yang hampir tidak dapat diidentifikasi sebagai informasi asli. *Plaintext* atau teks biasa adalah informasi atau pesan yang dikirim dalam format yang mudah dibaca atau asli (Ziliwu, Maslan, & Kremer, 2022).

Dekripsi adalah kebalikan dari kegiatan enkripsi karena tujuan dari deskripsi mengembalikan pesan yang tersandi atau informasi palsu ke pesan asli. Pada proses mengembalikan isi pesan tersamar harus menggunakan kode yang telah disiapkan sebelumnya. Kegiatan perubahan isi pesan dari *plaintext* ke *ciphertext* disebut enkripsi, dan prosedur mengembalikan teks dari *ciphertext* ke *plaintext* disebut dekripsi (Ziliwu, Maslan, & Kremer, 2022).



Gambar 2.3 Diagram Enkripsi dan Dekripsi

2.3.1 Dasar Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari

pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga Prinsip-prinsip yang mendasari kriptografi yakni :

a. *Secrecy* (kerahasiaan), layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka maupun menghapus informasi yang telah disandi.
b. *Authentication*, berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Dimana informasi yang dikirimkan melalui kanal harus diautentifikasi keaslian, isi datanya, waktu pengiriman dan lain-lain
c. Hak Akses terhadap suatu *file* atau fasilitas lain dalam sebuah sistem pemrosesan informasi masih dalam area lain dimana gagasan kriptografi telah diterapkan.

2.3.2 Tujuan Kriptografi

a. *Authentication*

Layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi. Fasilitas yang berkaitan untuk melakukan identifikasi terlebih dahulu antara pengirim dan penerima pesan.

b. *Integrity*

Keuntungan yang didapatkan dalam menggunakan teknik kriptografi yaitu menjamin bahwa pesan akan diterima dalam keadaan masih utuh dan belom mengalamai perubahan selama proses pengiriman. Layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

c. *Confidelity*

Layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima/pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

d. Non-repudiation

Layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya.

2.3.3 Jenis Kriptografi

1. Kriptografi Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang (*plaintext*). Kriptografi ini hanya melakukan pengacakan pada huruf A-Z, dan

sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern (Pardede, Manurung, & Filina, 2017)

2. Kriptografi Modern

Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Algoritma kriptografi modern (Pardede, Manurung, & Filina, 2017)

a. Algoritma Simetris

Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital secara *real time*.

b. Algoritma Asimetris

Algoritma Asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi *deskripsi*. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (*Rivest, Shamir dan Adleman)*

2.4 Algoritma Hill Cipher

Algoritma kriptografi atau cipher, dan juga sering disebut dengan istilah sandi adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu algoritma simetris (*symmetric algorithms*) dan algoritma asimetris (*asymmetric algorithms*). *Hill cipher* yang merupakan *polyalphabetic cipher* dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses akan dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter lainnya dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pula (Ramadani, 2020).

Hill cipher termasuk jenis kriptografi klasik yang diciptakan oleh Lester S. Hill pada tahun 1929. Algoritma Hill cipher ini mengganti setiap abjad plainteks nya ke dalam bentuk angka numerik yang berkorespondensi

dengan 0 sampai 25. Dalam penerapannya algoritma ini yang menggunakan persamaan aritmatika modulo terhadap matriks, dengan perkalian dan teknik invers terhadap matriks. Kuncinya menggunakan matriks *n x n* dengan *n* merupakan ukuran blok (Haris & Ariyus, 2020). Plainteks terlebih dahulu dirubah kedalam bentuk angka seperti blok pada gambar 2.4

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Gambar 2.4 Hill Cipher

Berdasarkan jenis kunci yang dipakai, kriptografi Hill Cipher termasuk ke dalam Algoritma Simetrik (Symmetric Algorithms), karena algoritma ini menggunakan suatu kunci yang sama untuk proses enkripsi dan dekripsi pesan. Dalam melakukan proses enkripsi dan dekripsi, algoritma ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan dan menerapkan aritmatika modulo (Hasibuan, Isnarto, & Veronica, 2022).

Misalkan m=2, maka dapat ditulis suatu elemen plaintext sebagai x = (x1, x2) dan suatu elemen ciphertext sebagai y = (y1, y2). Disini (y1, y2) adalah kombinasi linier dari x1 dan x2. Misalkan :

$Y_1 = 1_{x1} + 5_{x2}$ ..... (1)

$Y_2 = 9_{x1} + 8_{x2}$ ..... (2)

Sehingga dapat dituliskan kedalam bentuk matrik sebagai berikut :

$$Y_1, Y_2 = X_1, X_2 = \begin{matrix} 1 & 5 \\ 9 & 8 \end{matrix} \quad \text{..... (3)}$$

Secara umum, algoritma Hill Cipher akan menggunakan matrik K m x m sebagai kunci untuk mengacak pesannya. Jika elemen pada baris i dan kolom j dari matriks K_{ij}. Dikatakan bahwa ciphertext diperoleh dari plaintext dengan cara transformasi linier. Untuk melakukan dekripsi, akan digunakan matrik invers K^{-1}. Jadi, dekripsi dilakukan jika matrik tersebut memiliki nilai invers dengan rumus :

1. Perkalian matrik memiliki sifat asosiat if, yaitu (AB)C = A(BC)
2. Matriks invers dari A adalah A-1 dimana AA-1 = A-1A = Im
3. Matriks invers dari A adalah A-1 dimana AA-1 = A-1A = Im Matriks invers dari A adalah A-1 dimana AA-1 = A-1A = Im

   Setelah ditetapkan kunci enkripsi dan pengembalian pesan maka terdapat lagi rumus yang digunakan untuk mengubah huruf asli kebentuk kode dapat dilihat pada persamaan berikut :

   $$C = (P \times K) mod\ 26 \quad \text{..... (4)}$$

   Serta rumus pengembalian pesan dapat dilihat pada persamaan berikut :

   $$P = K^{-1} \times C \quad \text{..... (5)}$$

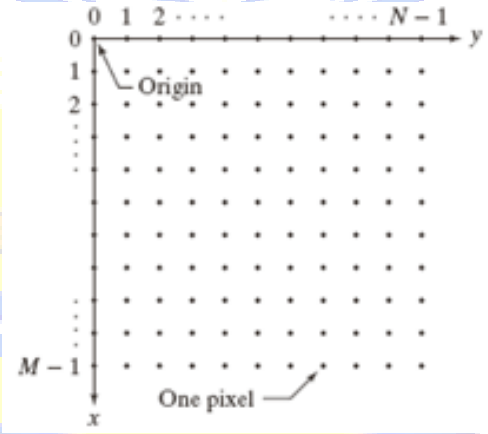
2.5 Pengertian Citra Digital

Citra (*image*) adalah gambar pada bidang dwimatra (dua dimensi). 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. (Arsy, Nurhayati, & Martono, 2016)

Citra yang ditangkap oleh kamera dan telah dikuantisasi dalam bentuk nilai diskrit sisebut sebagai citra digital (*digital image*). Foto hasil cetak dari printer tidak dapat disebut sebagai citra digital, namun foto yang tersimpan dalam *file* gambar (bmp, jpg, png atau format lainnya) pada komputer dapat disebut sebagai citra digital. (Sinaga, 2017).

Citra digital dibentuk oleh kumpulan titik yang dinamakan piksel (*pixel* atau "*picture element*"). Setiap piksel digambarkan sebagai satu kotak kecil. Setiap piksel mempunyai koordinat posisi. Sistem koordinat yang dipakai untuk menyatakan citra digital ditunjukkan pada Gambar 2.1 berikut



Gambar 2.5 Ilustrasi Citra Digital

Ada banyak cara untuk menyimpan citra digital di dalam memori. Cara penyimpanan menentukan jenis citra digital yang terbentuk. Format citra digital yang banyak dipakai adalah sebagai berikut :

A. Citra Biner

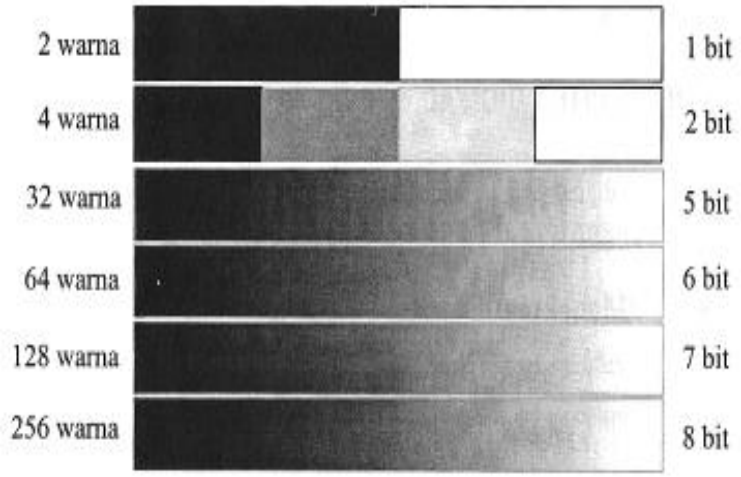
Citra biner adalah citra digital yang hanya memiliki dua kemungkinan nilai pixel yaitu hitam dan putih. Citra biner juga disebut sebagai citra *B&W (black and white)* atau citra monokrom. hanya dibutuhkan 1 bit untuk mewakili nilai setiap pixel dari citra biner. Citra biner (*monochrome*) atau disebut juga *binary image*, merupakan citra digital yang setiap *pixel*-nya hanya memiliki 2 kemungkinan derajat keabuan, yaitu 0 dan 1 (Sinaga, 2017). Nilai 0 mewakili warna hitam, dan nilai 1 mewakili warna putih, di mana setiap *pixel*-nya membutuhkan media penyimpanan sebesar 1 bit

Gambar 2.6 Citra Biner

B. Citra Grayscale

Citra *grayscale* menangani gradasi warna hitam dan putih, yang tentu saja menghasilkan warna abu-abu. Dalam hal ini intensitas berkisar antara 0 sampai dengan 255. Nilai 0 menyatakan hitam dan nilai 255 menyatakan putih. Banyaknya warna tergantung pada jumlah bit yang disediakan dimemori untuk menampung kebutuhan warna ini. Semakin besar jumlah bit warna yang disediakan di memori, semakin

halus gradasi warna yang terbentuk. Gambar 2.3 menunjukkan perbandingan gradasi warna untuk jumlah bit tertentu



Gambar. 2.7 Citra Perbandingan Gradasi Warna 1 bit, 2 bit, 5 bit, 6 bit, 7bit, 8bit

C. Citra Warna

Setiap piksel pada citra warna memiliki warna yang merupakan kombinasi dari tiga warna dasar RGB (*Red, Green, Blue*). Setiap warna dasar menggunakan penyimpanan 8 bit = 1 byte, yang berarti setiap warna mempunyai gradasi sebanyak 255 warna. Berarti setiap piksel mempunyai kombinasi warna sebanyak 28 . 28 . 28 = 224 = 16 juta warna lebih. Itulah yang menjadikan alasan format ini disebut dengan *true color* karena mempunyai jumlah warna yang cukup besar sehingga bias dikatakan hampir mencakup semua warna di alam. Penyimpanan citra *true color* di dalam memori berbeda dengan citra *grayscale*. Setiap piksel dari citra *grayscale* 256 gradasi warna diwakili oleh 1 byte. Sedangkan 1 piksel citra *true color* diwakili oleh 3 byte, dimana masing-masing byte merepresentasikan warna merah, hijau dan biru

Gambar. 2.8 Citra Warna

2.5.1 Pengolahan Citra Digital

Pengolahan citra adalah disiplin ilmu yang mempelajari hal-hal yang berkaitan dengan perbaikan kualitas gambar (peningkatan kontras, transformasi warna, restorasi), transformasi gambar (rotasi, translasi, skala, transformasi geometrik), melakukan pemilihanciri citra (*feature extraction*) yang optimal untuk bertujuan analisis, melakukan proses penarikan informasi atau deskripsi objek atau pengenalan objek yang terkandung pada citra, melakukan kompresi atau reduksi data untuk tujuan penyimpanan, transmisi dan waktu proses data. (Sinaga, 2017).

Pengolahan citra merupakan cabang ilmu dalam Artifical Intelegence yang menggunakan objek citra dalam bentuk digital untuk penyelesaian kasusnya. Metode dalam citra dapat digunakan baik perhitungan matematis pada objek secara piksel ataupun geometris. Masing-masing objek citra memiliki nilai perbedaan yang dapat diperhitungkan secara matematis, sehingga menunjukkan ciri yang berbeda antara objek satu dengan yang lain. Penciri dari perbedaan setiap objek dapat ditentukan dari warna, tekstur, ataupun bentuk

(Widyaningsih, 2017). Dengan memanfaatkan informasi digital ini pengelompokkan atau clustering dapat di implementasikan terhadap objek.

2.5.2 Tujuan Pengolahan Citra Digital

Pengolahan citra digital banyak dimanfaatkan oleh berbagai bidang mulai dari kemanan, kesehatan, pendidikan dan bidang – bidang yang lain. Berikut beberapa tujuan dari kegiatan pengolahan citra digital

1. Memperbaiki kualitas gambar dilihat dari aspek *radiometric* (peningkatan kontras, tranformasi warna, restorasi citra) dan dari aspek *geometric* (rotasi, translasi, skala, transformasi geometrik).
2. Melakukan proses penarikan informasi atau deskripsi objek atau pengenalan objek yang terkandung pada citra.
3. Melakukan kompresi atau reduksi data untuk tujuan penyimpanan data, transmisi data, dan waktu proses data.

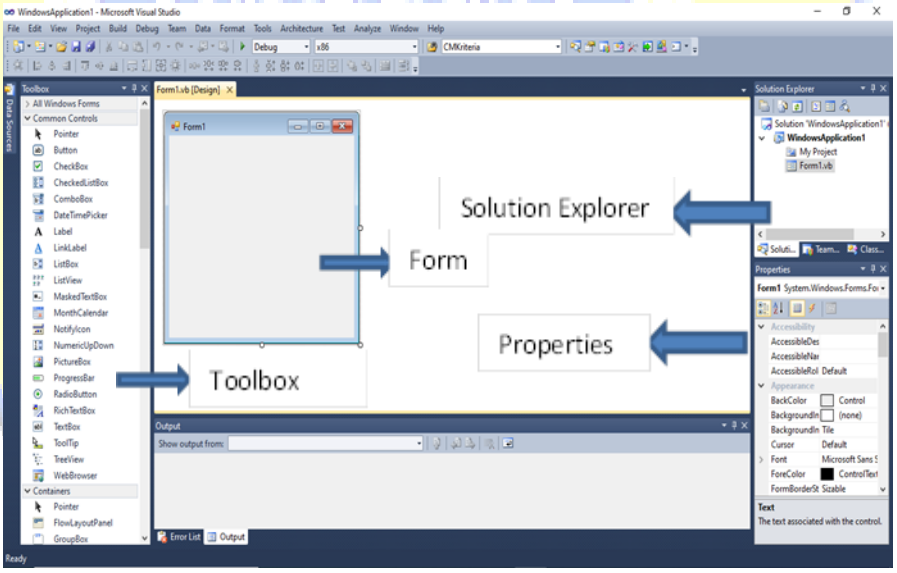
2.6 Tinjauan Umum Visual Basic.Net 2010

Microsoft Visual Basic.Net adalah sebuah alat untuk mengembangkan dan membangun aplikasi yang bergerak di atas sistem .NET Framework, dengan menggunakan bahasa BASIC. Dengan menggunakan alat ini, para programmer dapat membangun aplikasi *Windows Forms*, Aplikasi web berbasis ASP.NET, dan juga aplikasi *command-line*. Alat ini dapat diperoleh secara terpisah dari beberapa produk lainnya (seperti *Microsoft Visual C++, Visual C#, atau Visual J#),* atau juga dapat diperoleh secara terpadu dalam Microsoft Visual Studio (R.H Sianipar, 2017).

Visual Basic.Net merupakan salah satu *Development Tool* yaitu alat bantu untuk membuat berbagai macam program komputer, khususnya yang menggunakan sistem operasi *Windows*. Visual Basic merupakan salah satu bahasa pemrograman komputer yang mendukung object (*Object Oriented Programming* = OOP)

2.6.1 Menu Utama *Integrated Development Environment*

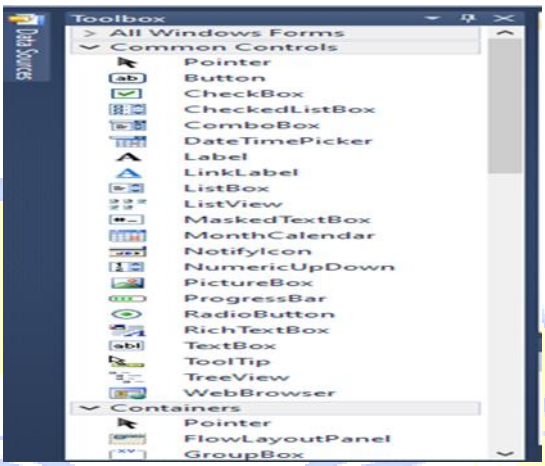
Di dalam menu utama *Integrated Development Environment* (IDE) tersedia perintah-perintah dan disertai pula dengan submenu-submenunya. Pada umumnya menu juga dapat ditampilkan dalam bentuk toolbar, tetapi tidak semua opsi tersedia pada saat itu juga. Ada kalanya opsi-opsi tersebut tidak dapat diterapkan pada tempat IDE. Ini berarti opsi tersebut dalam keadaan *invisible* atau *disabled*



Gambar 2.9 Komponen Visual Basic 2010

2.6.2 *Toolbox Windows Form*

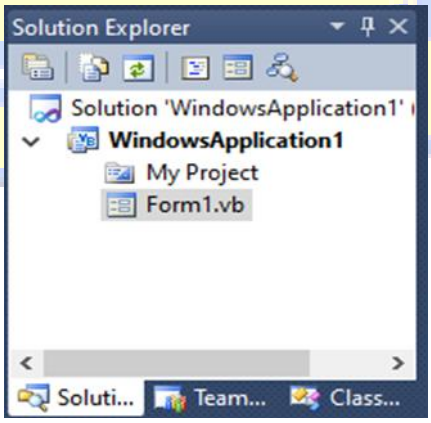
Toolbox berisi berbagai control yang dapat anda gunakan untuk mendesain antarmuka grafis. *Toolbox* mempunyai pengaturan automatic hiding sehingga akan tertutup jika tidak diperlukan



Gambar 2.10 *Toolbox*

2.6.3 Jendela *Explorer*

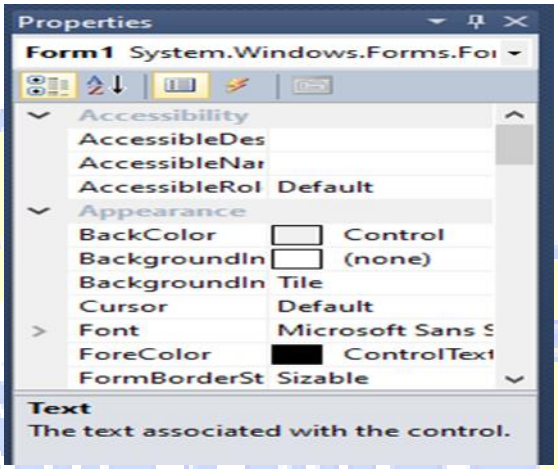
Jendela *explorer* merupakan tempat ditampilkannya daftar-daftar komponen secara hirarki. Dalam Jendela explorer dimungkinkan adanya beberapa proyek, dan dalam proyek ini masih ada beberapa item lagi seperti *form*, *module*, dan lain-lain



Gambar 2.11 Jendela *Explorer*

2.6.4 Jendela *Properties*

Jendela propertis ini berfungsi untuk menampilkan semua *property* dari komponen yang dipilih beserta settingannya. Dengan jendela ini kita dapat mengatur *property* dari masing-masing kontrol yang telah dibuat



Gambar 2.12 Jendela *Properties*

2.7 UML (*Unified Modeling Laguange*)

UML adalah salah satu *tool* atau model untuk merancang pengembangan software yang berbasis *object-oriented*. UML sendiri juga memberikan standar penulisan sebuah sistem *blueprint*, yang meliputi konsep proses bisnis, penulisan kelas-kelas dalam bahasa program yang spesifik, skema database, dan komponen yang diperlukan dalam sistem *software* (Sonata & Sari, 2019)

UML merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung". Beberapa pemodelan yang termasuk kedalam pemodelan UML seperti *use case diagram*, *class diagram*, *activity diagram*, dan *sequence diagram* (Syarif & Nugraha, 2020)

Adapun tujuan dari UML adalah:

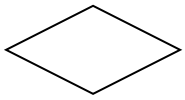
1. Merancang perangkat lunak.
2. Sarana komunikasi antara perangkat lunak dengan proses bisnis.
3. Menjabarkan sistem secara rinci untuk analisa dan mencari apa yang diperlukan sistem.
4. Mendokumentasi sistem yang ada, proses-proses dan organisasinya

2.7.1 *Activity* Diagram

Diagram aktivitas atau *activity diagram* menggambarkan *work flow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak (Syarif & Nugraha, 2020). Pada dasarnya, *activity* diagram merupakan variasi dari statechart diagram. *Activity* diagram mempunyai peran seperti halnya *flowchart*, akan tetapi perbedaannya dengan *flowchart* adalah *activity* diagram bisa mendukung perilaku paralel sedangkan *flowchart* tidak bisa. Berikut adalah notasi *activity* diagram.

Tabel 2.1 Notasi *Activity* Diagram

Gambar	Nama Simbol	Keterangan
	Status Awal	Sebuah diagram aktivitas memiliki sebuah status awal
	Status Akhir	Status akhir yang dilakukan sistem sebuah diagram aktivitas memiliki sebuah status akhir
	Aktivitas	Aktivitas yang dilakukan sistem biasanya diawali dengan kata kerja

Gambar	Nama Simbol	Keterangan
	Decision / Percabangan	Percabangan dimana ada pilihan aktivitas yang lebih dari satu
	*Fork*	Digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabungkan dua kegiatan paralel menjadi satu

2.7.2 *Use Case* Diagram

Use case atau *diagram use case* merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat (Syarif & Nugraha, 2020). *Use case* merupakan sebuah pekerjaan tertentu, misalnya login ke sistem, meng-*create* sebuah daftar belanja, dan sebagainya.

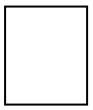
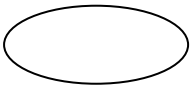
Seorang/sebuah aktor adalah sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu. *Use case diagram* dapat sangat membantu bila kita sedang menyusun *requirement* sebuah sistem, mengkomunikasikan rancangan dengan klien, dan merancang *test case* untuk semua *feature* yang ada pada sistem. Sebuah *use case* dapat meng-*include* fungsionalitas *use case* lain sebagai bagian dari proses dalam dirinya.

Secara umum diasumsikan bahwa *use case* yang di-*include* akan dipanggil setiap kali *use case* yang meng-*include* dieksekusi secara normal. Sebuah *use case* dapat di-*include* oleh lebih dari satu

use case lain, sehingga duplikasi fungsionalitas dapat dihindari dengan cara menarik keluar fungsionalitas yang *common*. Sebuah *use case* juga dapat meng-*extend use case* lain dengan *behaviour*-nya sendiri. Sementara hubungan generalisasi antar *use case* menunjukkan bahwa *use case* yang satu merupakan spesialisasi dari yang lain.

Tabel 2.2 Simbol *Use Case* Diagram

Gambar	Nama Simbol	Keterangan
	*Actor*	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinterasi dengan *Use Case*.
	*Depedency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (*independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*Independent)*
	Generalization	Hubungan dimana objek anak(*Descended)* berbagi prilaku dan struktur data dari objek yang diatasnya objek induk.
	*Include*	Menspesifikasikan bahwa use case sumber secara explicit.
	Extend	Menspesifikasikan bahwa use case target memperluas prilaku pada use case sumber pada sebuah titik diberikan.
	Assosiation	Apa yang memhubungkan objek satu dengan objek yang lainnya.

Gambar	Nama Simbol	Keterangan
	*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
	*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur dari sebuah *actor*.
	*Colaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya.
	*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi.

2.7.3 *Class* Diagram

Diagram kelas atau *class diagram* menggambarkan struktur sistem dari segini pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem (Syarif & Nugraha, 2020). *Class diagram* membantu dalam memvisualisasikan struktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, *class* diagram berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat.

Class diagram memiliki tiga area pokok:

1. Nama (dan *stereotype*)
2. Atribut
3. Metode

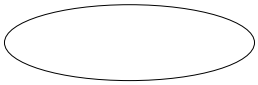
Tabel 2.3 Simbol Class Diagram

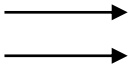
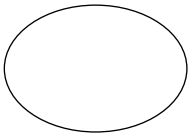
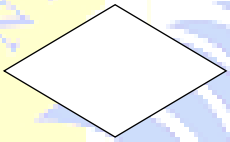
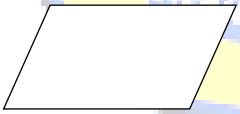
Gambar	Nama Simbol	Keterangan
	*Class*	Himpunan dari objek- objek yang berbagi atribut serta operasi yang sama.
	Associatiom	Apa yang menghubungkan antara objek satu dengan objek lainnya

2.8 Flowchart

Flowchart adalah representasi secara simbolik dari suatu algoritma atau prosedur untuk menyelesaikan suatu masalah, dengan menggunakan *flowchart* akan memudahkan pengguna melakukan pengecekan bagian-bagian yang terlupakan dalam analisis masalah, disamping itu *flowchart* juga berguna sebagai fasilitas untuk berkomunikasi antara pemrogram yang bekerja dalam tim suatu proyek. *Flowchart* membantu memahami urutan-urutan logika yang rumit dan panjang. *Flowchart* membantu mengkomunikasikan jalannya program ke orang lain (bukan pemrogram) akan lebih mudah (Santoso & Nurmalina, 2017).

Tabel 2.4 Simbol dan Fungsi *Flowchart*

Gambar	Nama Simbol	Keterangan
	*Start / Mulai* *End / Selesai*	Simbol yang digunakan untuk memulai / selesai

Gambar	Nama Simbol	Keterangan
	*Flow*	Simbol arus/ *flow* yang menyatakan jalannya proses
	*Connector*	Simbol *connector*, (menyatakan sambungan dari proses ke proses lainnya dalam hal yang sama
	*Process*	Simbol proses yaitu menyatakan suatu tindakan
	*Manual Operation*	Simbol manual, manyatakan suatu tindakan
	*Decision*	Simbol *decision*, menunjukkan suatu kondisi tertentu yang akan menghasilkan dua kemungkinan
	*Keying Operation*	Simbol *keying* operation menyatakan segala jenis operasi yang diproses dengan menggunakan suatu mesin yang mempunyai keyboard.
	*Input/Output*	Simbol *input* atau *output* menyatakan proses *input* atau *output*
	*Document*	Simbol dokumen mencetak keluaran dalam bentuk dokumen

BAB III

METODOLOGI PENELITIAN

3.1 Subjek Penelitian

3.1.1 Gambaran Umum Polsek Selebar Kota Bengkulu

Sejarah yang menorehkan tinta emas Hari Depan Polisi dimulai setelah proklamasi Kemerdekaan, dimana Panitia Persiapan Kemerdekaan Indonesia (PPKI) pada sidangnya hari kedua tgl 19 Agustus 1945 memasukkan kepolisian dalam lingkungan Departemen Dalam Negeri. Dengan demikian status Djawatan Kepolisian Negara (DKN) secara administratif mempunyai kedudukan yang sama dengan Dinas Polisi Umum pada masa penjajahan Belanda".

Visi :

Terwujudnya Polsek Selebar Kota Bengkulu yang Profesional, Modern dan Terpercaya sebagai pelindung, pengayom serta pelayan masyarakat yang terpercaya dalam memelihara Kamtibmas dan menegakkan hukum

Misi :

1. Memberikan perlindungan, pengayoman dan pelayanan kepada masyarakat sehingga masyarakat merasa aman, tentram dalam kehidupan sehari-hari
2. Memberikan bimbingan kepada masyarakat melalui upaya preemtif dan preventif yang dapat meningkatkan kesadaran dan kekuatan serta kepatuhan hukum masyarakat

3. Menegakkan hukum secara profesional dan proporsional dengan menjunjung tinggi supremasi hukum dan hak asasi manusia menuju kepada adanya kepastian hukum dan rasa keadilan
4. Memelihara keamanan dan ketertiban masyarakat dengan tetap memperhatikan norma-norma dan nilai-nilai yang berlaku dalam bingkai integritas wilayah hukum Polsek Selebar Kota Bengkulu
5. Mengelola profesionalisme sumberdaya manusia dengan dukungan sarana prasarana serta meningkatkan upaya konsolidasi dan soliditas Polsek Selebar Kota Bengkulu untuk mewujudkan keamanan di wilayah Kota Bengkulu sehingga dapat mendorong meningkatnya gairah kerja guna mencapai kesejahteraan masyarakat; dan
6. Polsek Selebar Kota Bengkulu berkomitmen melayani dengan hati, tulus, ikhlas dan simpatik

3.1.2 Struktur Organisasi

Struktur organisasi merupakan salah satu sarana untuk mencapai tujuan organisasi atau perusahaan melalui fungsi-fungsi manajemen yang dilakukan oleh seorang pemimpin. Adapun struktur Polsek Selebar Kota Bengkulu terdapat pada lampiran 1 (terlampir).

3.1.3 Tempat dan Waktu Penelitian

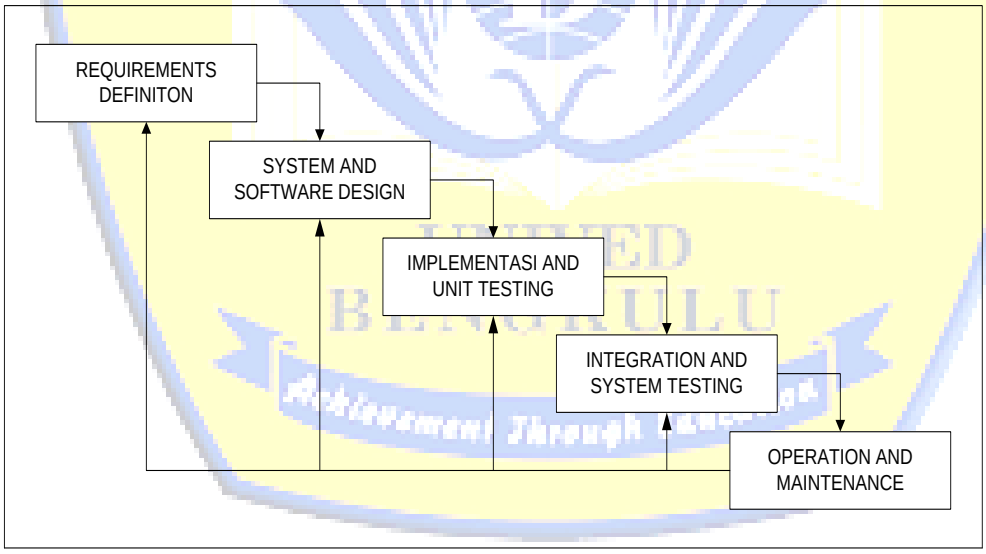
Penulis melakukan penelitian pada Polsek Selebar Kota Bengkulu yang beralamat di Bumiayu, Selebar, Bengkulu City, Bengkulu 38216, Indonesia.

Penelitan ini dilaksanakan pada bulan Oktober 2022 sampai dengan bulan Mei 2023.

3.2 Metode Penelitian

Metode penelitian yang digunakan pada penelitian ini adalah metode *waterfall.* Dengan metode *waterfall* mampu melakukan analisa bertahap. Analisa kebutuhan digunakan untuk mengetahui dari kelemahan sistem yang lama, kemudian membuat desain dari rancangan tersebut dan dilanjutkan dengan pembuatan rancangan sistem baru yang meliputi kode-kode program. Setelah sistem baru selesai di ujikan sistem tersebut. Jika tidak ada kesalahan, maka sistem akan diimplementasikan dan pemeliharaan sistem.

Tahap penelitian yang dilakukan akan digambarkan dengan diagram alir seperti gambar dibawah ini :



Gambar 3.1 Metode Penelitian *Waterfall*

Keterangan :

1. *Requirement Definition*(Identifikasi Masalah)

Mengumpulkan kebutuhan secara lengkap kemudian kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh program yang akan dibangun. Fase

ini harus dikerjakan secara lengkap untuk bisa menghasilkan desain yang lengkap.Pada tahap ini pengembang sistem diperlukan suatu komunikasi yang bertujuan untuk memahami software yang diharapkan pengguna dan batasan *software*.Informasi ini biasanya dapat diperoleh melalui wawancara, survey atau diskusi.Informasi tersebut dianalisis untuk mendapatkan data yang di butuhkan oleh pengguna.

2. ***System And Software Design*** **(Desain Perangkat Lunak)**

Desain dikerjakan setelah kebutuhan selesai dikumpulkan secara lengkap. Kebutuhan dari tahap pertama akan dipelajari dalam fase ini dan desain sistem disiapkan. Desain Sistem membantu dalam menentukan perangkat keras dan sistem persyaratan dan juga membantu dalam mendefinisikan arsitektur sistem secara keseluruhan.

3. ***Implementation and Unit Testing*****(Implementasi dan Testing)**

Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut unit, yang terintegrasi dalam tahap berikutnya.Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman yang sudah ditentukan.

4. ***Integration and System Testing*** **(Integrasi System)**

Penyatuan unit-unit program kemudian diuji secara keseluruhan (s*ystem testing*).Semua unit yang dikembangkan dalam tahap implementasi diintegrasikan ke dalam sistem setelah pengujian masing-masing unit. Pasca integrasi seluruh sistem diuji untuk mengecek setiap kesalahan dan kegagalan.

5. ***Operation and Maintenance*** **(Operasi dan Perbaikan)**

Ini merupakan tahap terakhir dalam model waterfall. *Software* yang sudah jadi dijalankan serta dilakukan pemeliharaan. Pemeliharaan termasuk dalam memperbaiki kesalahan yang tidak ditemukan pada langkah sebelumnya.Perbaikan implementasi unit sistem dan peningkatan jasa sistem sebagai kebutuhan baru.

3.3 Perangkat Keras (*Hardware*) dan Perangkat Lunak (*Software*)

3.3.1 Perangkat Keras (*Hardware*)

Perangkat keras yang digunakan dalam penelitian ini adalah menggunakan komputer dengan spesifikasi sebagai berikut :

a. Laptop Acer.
b. RAM 4 Gb
c. Flashdisk Kingstone 8Gb
d. Harddisk 500 Gb

3.3.2 Perangkat Lunak (*Software*)

Adapun perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut :

a. Sistem Operasi Window 10
b. Visual Basic.Net 2010
c. Crystal Report 13

3.4 Metode Pengumpulan Data

Adapun metode pengumpulan data yang penulis gunakan pada penelitian ini adalah sebagai berikut :

1. Observasi

Dalam pengumpulan data melalui observasi, penulis mengamati dan menganalisa bagaimana tahapan atau langkah-langkah dari metode steganografi dan kriptografi pada objek citra digital.

2. Studi Pustaka

Metode dimana penulis mempelajari dan mencari data yang berasal dari buku dan referensi yang berhubungan dengan masalah yang ditulis.

3.5 Analisa Perancangan Sistem

Analisis perancangan sistem merupakan analisis yang dilakukan untuk mengamati dan menentukan kebutuhan – kebutuhan yang diperlukan dalam pengembangan sistem. Analisis sistem dibagi menjadi beberapa sub bagian yaitu analisis spesifikasi sistem dan analisis arsitektur sistem. Berikut penjabaran dari tahap – tahap analisis sistem

3.5.1 Analisa Sistem Aktual

Polsek Selebar Kota Bengkulu memiliki banyak data yang harus dijaga kerahasiaannya, termasuk data kriminal yang terdapat di wilayah tersebut. Oleh karena itu, dibutuhkan suatu sistem keamanan yang efektif untuk melindungi data tersebut dari akses yang tidak sah. Salah satu teknik yang dapat digunakan untuk menjaga kerahasiaan data adalah steganografi. Dalam steganografi, pesan yang akan disimpan di dalam media yang digunakan tidak akan mengganggu informasi asli atau kualitas media tersebut. Namun demikian, pesan yang disembunyikan dengan steganografi masih rentan terhadap serangan kriptografi. Oleh karena itu, untuk meningkatkan keamanan data, teknik steganografi LSB dapat digabungkan dengan teknik enkripsi seperti *Hill Cipher* .

3.5.2 Analisa *Steganografi LSB* dan *Hill Cipher*

Sebelum masuk kedalam proses penyandian terlebih dahulu ditetapkan pesan yang akan disandikan dan kunci matriks 2x2. Berikut langkah-langkah enkripsi pesan pada algoritma Hill Cipher dengan menggunakan matrik 2x2 :

1. Siapkan pesan

   P = JAKA

   Kunci :

   $K = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}$

2. Mengubah pesan menjadi kode dan matrik 2x2

   Setelah diketahui masing-masing kode huruf maka pesan teks yang akan di sandikan diubah kedalam kode-kode angka seperti terlihat pada gambar 2.4 pada bab sebelumnya, yaitu :

   P = 9 0 10 0

3. Lakukan perkalian matrik

   $JA = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 9 \\ 0 \end{bmatrix} = \begin{bmatrix} (4 * 9) + (3 * 0) \\ (3 * 9) + (3 * 0) \end{bmatrix} = \begin{bmatrix} 36 \\ 27 \end{bmatrix}$

   Mod : 36 mod 26 = 10 = K

   27 mod 26 = 1 = B

   $KA = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix} \begin{bmatrix} 10 \\ 0 \end{bmatrix} = \begin{bmatrix} (4 * 10) + (3 * 0) \\ (3 * 10) + (3 * 0) \end{bmatrix} = \begin{bmatrix} 40 \\ 30 \end{bmatrix}$

   Mod : 40 mod 26 = 14 = O

   30 mod 26 = 4 = E

   Cipherteks yang dihasilkan adalah : *KBOE*

4. Dekripsi Hill Cipher

Berikut ini adalah rumus dekripsi metode Hill Cipher beserta contohnya : P = K^{-1}.C mod 26

Cipherteks : *KBOE*

Untuk melakukan dekripsi, maka kunci enkripsi diubah menjadi :

$K = \begin{bmatrix} 4 & 3 \\ 3 & 3 \end{bmatrix}$ ⟹ det K = (4*3) – (3*3) = 3

Invers modulo

3^{-1} mod 26 ⟹ 3_x = 1 mod 26 ⟹ 3_x = 1 + 26K

x = (1+26K)/3

Cari K = n sehingga hasil x adalah bilangan bulat

K = 0 ⟹ x = (1+26K)/3 = 1/3 (bukan bilangan bulat)

K = 0 ⟹ x = (1+26K)/3 = 27/3 = 9 (bilangan bulat)

$$Jika\ K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\ maka\ K^{-1} = deteminan \begin{bmatrix} d & -b \\ -d & a \end{bmatrix}$$

$$sehingga\ K^{-1} = 9\begin{bmatrix} 3 & -3 \\ -3 & 4 \end{bmatrix} = \begin{bmatrix} 27 & -27 \\ -27 & 36 \end{bmatrix} mod 26$$

$$= \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix}$$

Untuk modulo bilangan negatif dapat dikerjakan sebagai berikut :

-27 mod 26 = -n mod x

Maka : -n mode x = x-(n mod x) ⟹ 26 – (27 mod 26) = 25

Proses dekripsi :

$$KB = \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix}\begin{bmatrix} 36 \\ 27 \end{bmatrix} = \begin{bmatrix} (1 * 36) + (25 * 27) \\ (25 * 36) + (10 * 27) \end{bmatrix} = \begin{bmatrix} 711 \\ 1170 \end{bmatrix}$$

Mod : 711 mod 26 = 9 = J

1170 mod 26 = 0 = A

$$OE = \begin{bmatrix} 1 & 25 \\ 25 & 10 \end{bmatrix} \begin{bmatrix} 40 \\ 30 \end{bmatrix} = \begin{bmatrix} (1 * 40) + (25 * 30) \\ (25 * 40) + (10 * 30) \end{bmatrix} = \begin{bmatrix} 790 \\ 1300 \end{bmatrix}$$

Mod : 790 mod 26 = 10 = K

1300 mod 26 = 0 = A

Pada studi kasus ini digunakan adalah gambar dengan warna 24 bit yaitu yang terdiri dari 3 warna R,G,B dimana masing-masing warna mempunyai kedalam 8 bit. Karena masing-masing warna bernilai 8 bit, maka pesan akan disisipkan kedalam bit R, bit G dan bit B tiap-tiap pixel. Misalkan pesan yang akan disisipkan sebanyak 8 bit, maka pesan yang 8 bit tersebut hanya akan disisipkan pada dua 3 pixel, karena tiap pixel memiliki kapasitas 24 bit dan masing-masing bit pesan hanya disisipkan pada 8 bit citra gambar. Dibawah ini adalah langkah-langkah proses steganografi untuk menyisipkan pesan kedalam citra gambar, Berikut ini merupakan bagaimana cara kerja dari algoritma LSB dimana teks **JAKA** akan disisipkan kedalam gambar, namun terlebih dahulu teks tersebut diubah kedalam biner dengan nilai sebagai berikut :

Tabel 3.1 Kode ASCII Teks/Pesan Yang Akan Disisip

Teks	Desimal	Biner
J	74	0100 1010
A	65	0100 0001
K	75	0100 1011
A	65	0100 0001

Setelah diubah kedalam biner lalu pesan akan disisipkan kedalam gambar pada warna (RGB) dengan nilai citra atau gambar awal sebagai berikut :

196	10	97	182
67	200	100	50
25	150	45	200
176	56	77	100
101	34	40	40
40	200	55	28
28	30	60	45
44	66	99	125

Nilai piksel citra diubah menjadi biner sehingga menjadi :

Tabel 3.2 Nilai Biner Citra

11000100	00001010	01100000	10110110
01000011	11001001	01100101	00110011
00011000	10010110	00101100	11001000
10110000	00111000	01001100	01100101
01100100	00100010	00101000	00101000
00101001	11001001	00110110	00011100
00011101	00011110	00111101	00101101
00101100	01000011	01100010	01111100

Untuk selanjutnya, setiap bit kode biner pesan digunakan untuk menggantikan bit terakhir dari kode biner citra. Proses penggantian dilakukan terurut menurut baris ataupun kolom. Pada contoh ini digunakan baris. Setelah proses penggantian, maka kode biner untuk citra menjadi :

Tabel 3.3 Nilai Biner Citra Yang Disisipkan Pesan

11000010	00001010	01100000	10110110
01000011	11001001	01100101	00110011
00011000	10010110	00101100	11001000
10110000	00111000	01001100	01100100
01100101	00100010	00101001	00101000
00101000	11001000	00110110	00011100
00011101	00011110	00111101	00101100
00101100	01000011	01100011	01111101

Tabel 3.4 Nilai Desimal Citra Setelah Disisipkan Pesan

196	10	96	182
67	201	101	51
24	150	44	200
176	56	76	100
101	34	41	40
40	200	54	28
29	30	61	44
54	67	99	125

Untuk hasil ekstraknya dapat dengan mudah dilakukan dengan mengambil bit terakhir dari kode biner citra yang telah disisipkan pesan. Data biner yang telah diambil isi pesannya dimana nilai tersebut adalah sebagai berikut

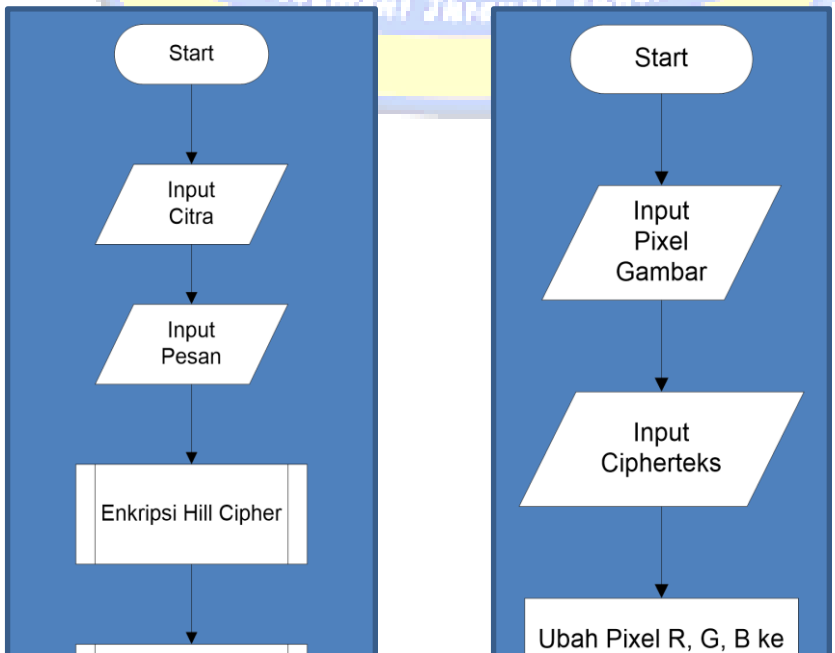
Tabel 3.4 Kode ASCII Hasil Ekstrak

Teks	Desimal	Biner
J	74	0100 1010
A	65	0100 0001
K	75	0100 1011
A	65	0100 0001

3.5.3 Perancangan Sistem Baru

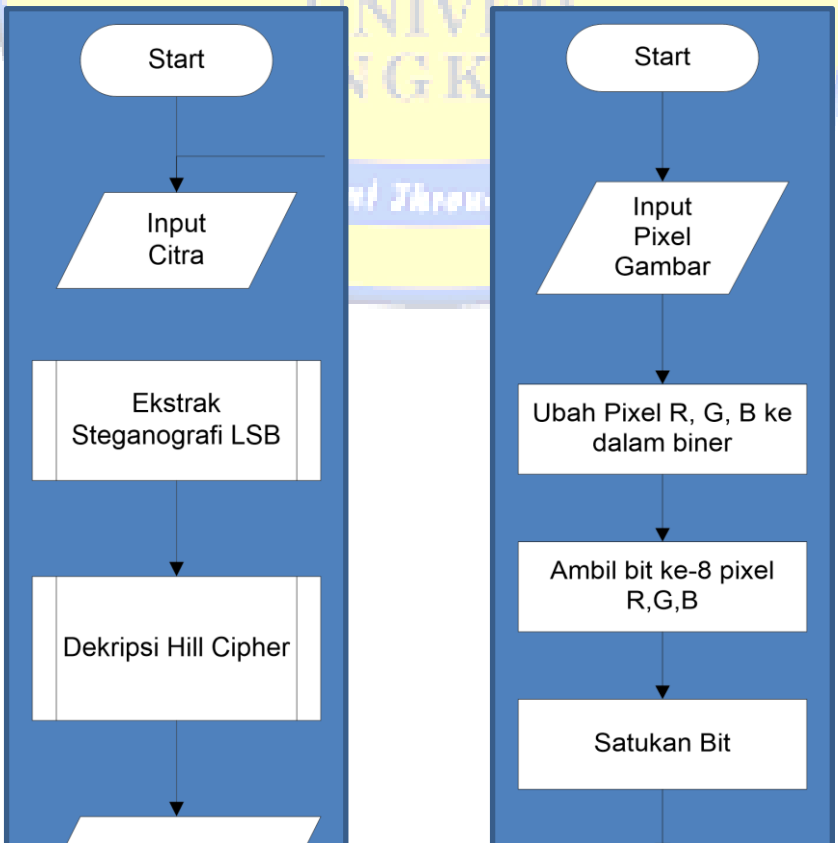
Perancangan sistem yang akan dilakukan pada penelitian ini yaitu perancangan *flowchart, use case diagram* dan perancangan antarmuka. Perancangan perancangan *flowchart diagram, use case diagram* bertujuan untuk memberikan gambaran mengenai proses dan alur penggunaan dari sistem yang dikembangkan. Sedangkan perancangan antarmuka dilakukan untuk memberikan gambaran tampilan antar muka dari sistem yang dikembangkan. Berikut penjabaran dari masing – masing perancangan yang dilakukan pada penelitian ini

A. Flowchart Penyisipan



Gambar 3.2 Sisip Pesan *Hill Cipher* dan Steganografi LSB

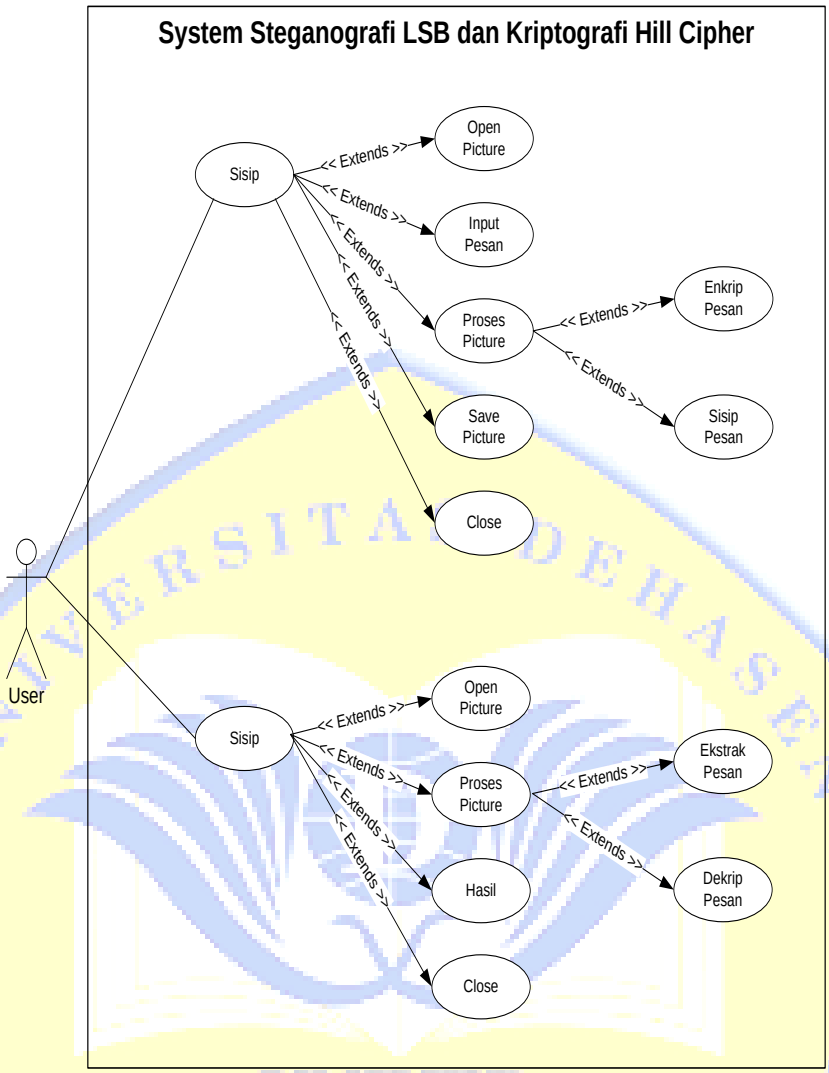
B. Flowchart Ekstrak Pesan



Gambar 3.3 Ekstrak Pesan *Hill Cipher* dan Steganografi LSB

C. Use Case Diagram

Kegiatan interaksi antara aktor terhadap sistem ditunjukan pada *use case diagram*, Aktor yang terlibat dalam kegiatan tersebut adalah *user*. User memiliki dua *use case*, yaitu form sisip dan form ekstrak dan yang kemudian keduanya memilki beberapa *use case* lagi. Use case diagram perangkat lunak yang dibangun terlihat pada gambar 3.4 berikut :

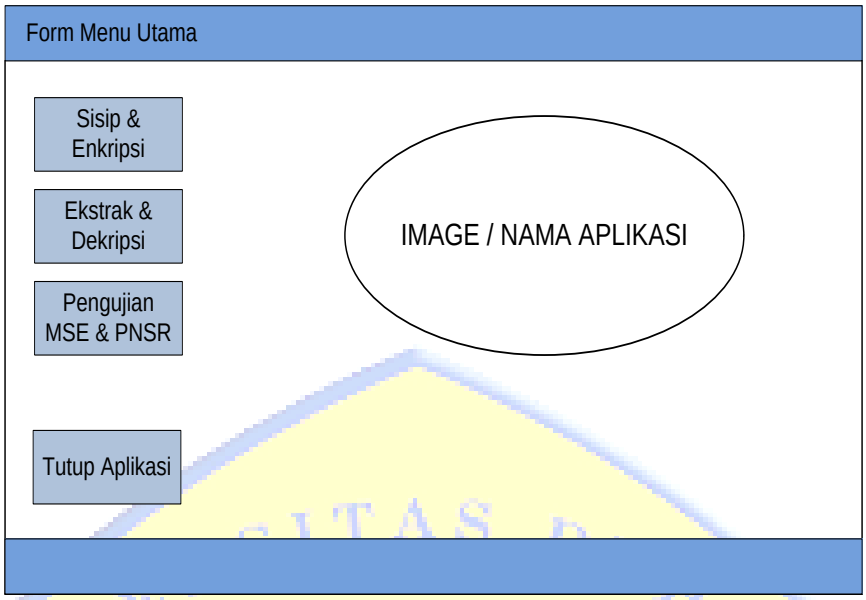


Gambar 3.4 Use Case Diagram Aplikasi

D. Rancangan *Interface* (Antarmuka) Aplikasi

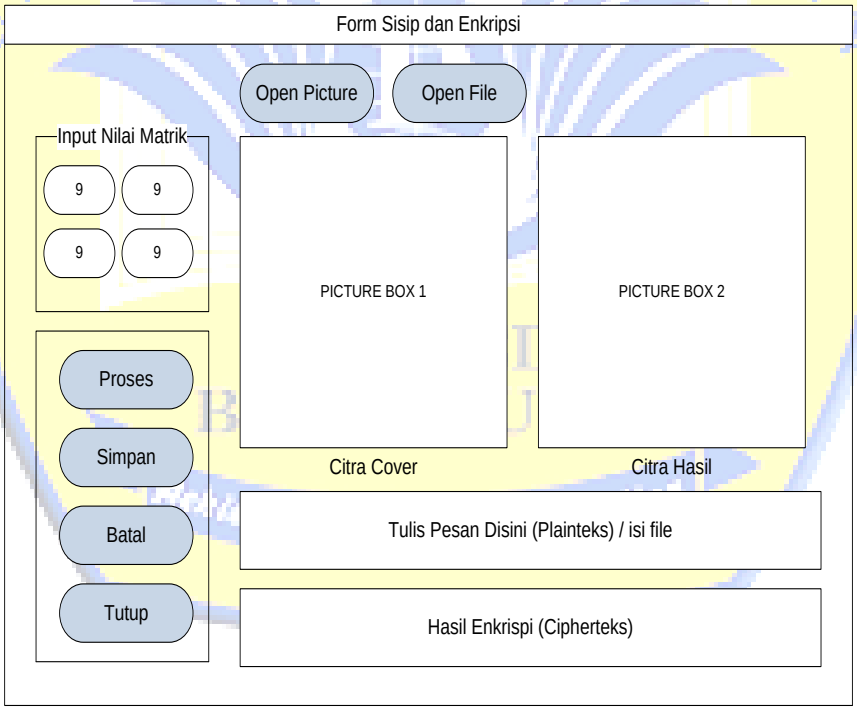
Perancangan ini bertujuan untuk merancang tampilan dari suatu perangkat lunak yang akan di buat yang sesuai dengan kebutuhan pengguna. Berikut perancangan antarmuka aplikasi steganografi LSB dan Hill Cipher :

1. Menu Utama Aplikasi



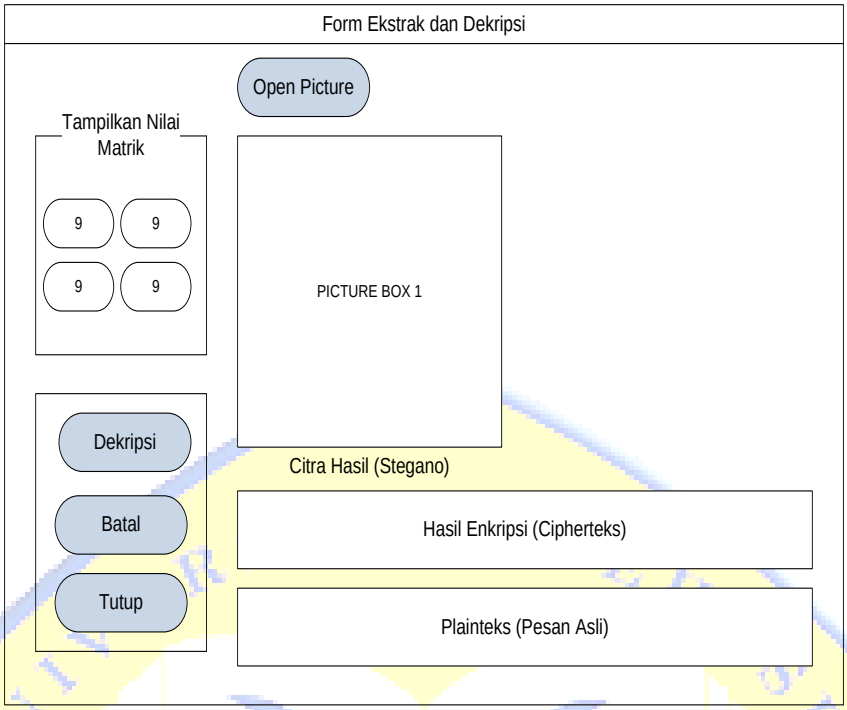
Gambar 3.5 Rancangan Menu Utama Aplikasi

2. Rancangan Form Sisip dan Enkripsi



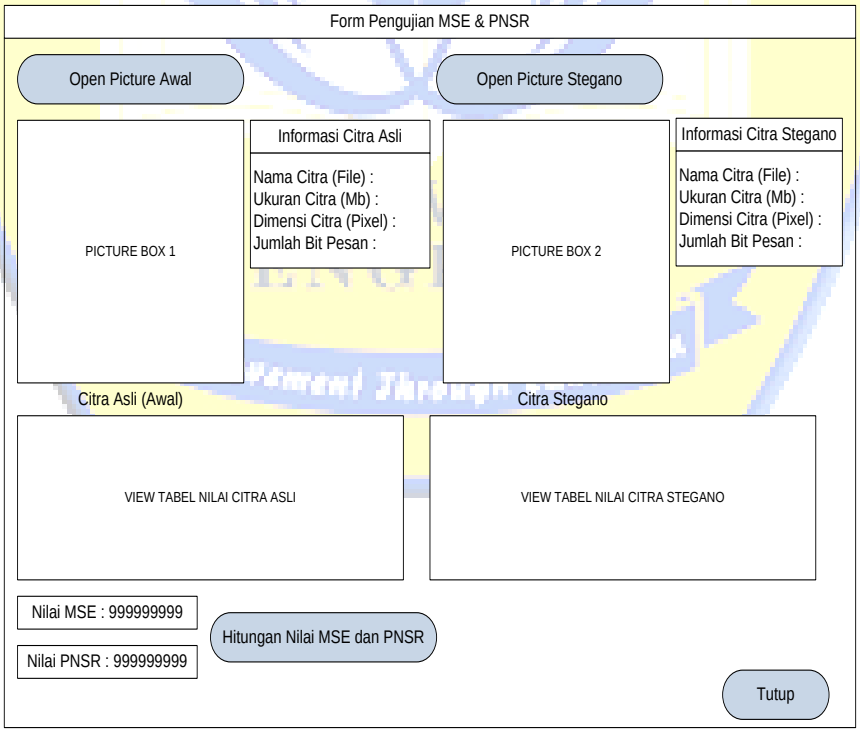
Gambar 3.6 Rancangan Form Sisip dan Enkripsi Pesan

E. Rancangan Form Ektrak dan Dekripsi Pesan



Gambar 3.7 Rancangan Form Ekstrak dan Dekripsi Pesan

F. Rancangan Pengujian MSE & PNSR



Gambar 3.8 Rancangan Pengujian MSE dan PNSR

3.6 Perancangan Pengujian

A. Pengujian Blackbox

Pengujian sistem merupakan proses eksekusi sistem dengan tujuan mencari kesalahan atau kelemahan dari program tersebut. Proses tersebut dilakukan dengan mengevaluasi kemampuan program. Suatu program yang diuji akan dievaluasi apakah keluaran atau output yang dihasilkan telah sesuai dengan yang diinginkan atau tidak. Metode pengujian yang dipakai dalam sistem ini adalah metode *black box*. Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak. Pengujian ini memungkinkan analisis sistem memperoleh kumpulan kondisi input yang akan mengerjakan seluruh keperluan fungsional program. Tujuan metode ini mencari kesalahan pada:

1. Fungsi yang salah atau hilang.
2. Kesalahan pada *interface*.
3. Kesalahan pada struktur data atau akses database.
4. Kesalahan performansi.
5. Kesalahan inisialisasi dan tujuan akhir

B. Pengujian MSE (*Mean Square Error*)

MSE merupakan tolak ukur analisis kuantitatif yang digunakan untuk menilai kualitas sebuah citra keluaran dan keunggulan sebuah metode yang digunakan. Ukuran matriks citra m * n, B1 dan B2 merupakan matriks citra. Dengan kata lain *Mean Square Error* (MSE) adalah kesalahan kuadrat rata- rata sinyal-sinyal piksel citra hasil pemrosesan sinyal terhadap sinyal asli. Untuk nilai terbaik MSE adalah sama dengan nol. MSE dapat dirumuskan sebagai berikut

$$MSE_{AVG} = \frac{MSE_R + MSE_G + MSE_B}{X.Y}$$

C. Pengujian PNSR (*Peak Signal to Noise Ratio*)

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut, dalam satuan desibel (dB). Semakin besar parameter PSNR semakin mirip dengan citra asli. Untuk menentukan nilai PSNR digunakan persamaan berikut ini :

$$PNSR = 10log_{10}\frac{255^2}{MSE}$$