# SKRIPSI

# IMPLEMENTASI STEGANOGRAFI *MULTI-FRAME* PADA MEDIA VIDEO

**Disusun dan diajukan oleh:**

**M. EMIRAT MILLENIUM TRY**

**D121181516**

**DEPARTEMEN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS HASANUDDIN**

**MAKASSAR**

**2022**

**LEMBAR PENGESAHAN SKRIPSI**

**IMPLEMENTASI STEGANOGRAFI *MULTI-FRAME* PADA MEDIA VIDEO**

**Disusun dan diajukan oleh**

**M. EMIRAT MILLENIUM TRY**

**D121181516**

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi Teknik Informatika Fakultas Teknik Universitas Hasanuddin pada tanggal 30 November 2022 dan dinyatakan telah memenuhi syarat kelulusan.

Menyetujui,

| Pembimbing Utama, | Pembimbing Pendamping, |
|---|---|
| Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. | Iqra Aswad, S.T., M.T. |
| NIP. 19750313 200912 1 003 | NIP. 19901128 201904 3 001 |

Ketua Program Studi,

Dr. Indrabayu, S.T., M.T., M.Bus.Sys.
NIP. 19750716 200212 1 004

## PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : M. Emirat Millenium Try |
| Nim | : D121181516 |
| Program Studi | : Teknik Informatika |
| Jenjang | : S1 |

Menyatakan dengan ini karya tulisan saya berjudul:

**IMPLEMENTASI STEGANOGRAFI *MULTI-FRAME***

**PADA MEDIA VIDEO**

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilan alihan tulisan orang lain bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Gowa, 30 November 2022

Yang Menyatakan,


M. Emirat Millenium Try

# KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya sehingga tugas akhir yang berjudul "**Implementasi Steganografi *Multi-frame* pada Media Video**" ini dapat diselesaikan sebagai salah satu syarat dalam menyelesaikan jenjang Strata-1 pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Penulis menyadari bahwa dalam penyusunan dan penulisan laporan skripsi ini tidak lepas dari bantuan, bimbingan serta dukungan dari berbagai pihak, dari masa perkuliahan sampai dengan masa penyusunan skripsi. Oleh karena itu, penulis dengan senang hati menyampaikan terima kasih kepada:

1. Tuhan Yang Maha Esa atas semua berkat, karunia serta pertolongan-Nya yang tiada batas, yang telah diberikan kepada penulis di setiap langkah dalam pengembangan sistem hingga penulisan laporan skripsi ini;
2. Kedua orang tua penulis, Bapak Abdul Malik Pakambanan dan Ibu Lauradiah Djalle, serta keluarga besar yang senantiasa memberikan kekuatan, inspirasi, motivasi, bimbingan moral serta materi, kepercayaan, dan kasih sayang yang tidak terbatas kepada penulis;
3. Bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T., dan Bapak Iqra Aswad S.T, M.T., selaku Pembimbing I dan Pembimbing II yang telah banyak memberi keyakinan, perhatian, bimbingan, motivasi, dan masukan yang bermanfaat kepada penulis;
4. Teman-teman SamjaTech atas dukungan dan semangat yang telah diberikan selama ini;

5. Muh. Sandi Arista Ikhsan Yahmid, selaku teman yang telah banyak memberikan bimbingan dan motivasi dalam pengembangan sistem hingga penulisan laporan skripsi ini;
6. Diri penulis sendiri atas pencapaian, kerja keras, dan semangat pantang menyerah dalam menyelesaikan skripsi dan studi;
7. Serta seluruh pihak yang tidak sempat disebutkan satu persatu yang telah banyak meluangkan tenaga, waktu, dan pikiran selama penyusunan laporan skripsi ini.

Akhir kata, penulis berharap semoga Tuhan Yang Maha Esa berkenan membalas segala kebaikan dari semua pihak yang telah banyak membantu. Semoga skripsi ini dapat memberikan manfaat bagi pengembangan ilmu selanjutnya.

Makassar, November 2022

Penulis

# ABSTRAK

Seiring dengan kemajuan teknologi internet, media digital dapat dibagi dan dikirimkan melalui internet dengan lebih mudah. Namun, salah satu tantangan utama dalam berbagi dan mentransmisikan semua jenis informasi melalui internet adalah keamanan data. Oleh sebab itu, dibutuhkan cara untuk melindungi informasi. Dengan teknik steganografi, sebuah informasi dapat disembunyikan melalui sebuah media seperti video. Untuk memastikan informasi hanya dapat dibaca oleh penerima yang dituju, diterapkan teknik kriptografi untuk menyamarkan pesan sebelum dan sesudah pesan disembunyikan. Sistem yang dikembangkan menerapkan kombinasi dari Algoritma Least Significant Bit (steganografi) dan Vigenere Cipher (kriptografi) untuk menyembunyikan pesan rahasia pada nilai warna *pixel* dari *frame* video. Sistem memiliki 2 fitur utama, yaitu fitur menyembunyikan pesan rahasia pada sebuah video dan fitur menampilkan pesan rahasia dari sebuah video steganografi. Pengujian Sistem Steganografi *Multi-frame* pada video dengan Metode Black Box Testing berhasil dilakukan dengan tingkat keberhasilan 100%. Hasil analisis objektif dengan parameter nilai Peak Signal to Noise Ratio (PSNR) pada video steganografi dengan Metode *Multi-frame* lebih efektif 26.4% jika dibandingkan dengan Metode *Single-frame,* sedangkan hasil analisis subjektif dengan parameter kemampuan mata manusia pada video steganografi menunjukkan bahwa Metode *Multi-frame* dan *Single-frame* sama-sama tidak menunjukkan perubahan warna yang signifikan pada *frame*-nya.

**Kata kunci**: video, *frame*, steganografi, kriptografi.

# DAFTAR ISI

**HALAMAN PENGESAHAN** ..... ii
**HALAMAN PERNYATAAN KEASLIAN** ..... iii
**KATA PENGANTAR** ..... iv
**ABSTRAK** ..... vi
**DAFTAR ISI** ..... vii
**DAFTAR TABEL** ..... ix
**DAFTAR GAMBAR** ..... x
**BAB I PENDAHULUAN** ..... 1
1.1 Latar Belakang ..... 1
1.2 Rumusan Masalah ..... 3
1.3 Tujuan Penelitian ..... 3
1.4 Manfaat Penelitian ..... 4
1.5 Batasan Masalah ..... 4
1.6 Sistematika Penulisan ..... 4
**BAB II TINJAUAN PUSTAKA** ..... 6
2.1 Video Digital ..... 6
2.2 Kompresi Video ..... 7
2.3 Warna RGB ..... 8
2.4 Steganografi ..... 8
2.5 Kriptografi ..... 9
2.6 Least Significant Bit ..... 10
2.7 Vigenere Cipher ..... 11
2.8 Peak Signal to Noise Ratio ..... 12
2.9 American Standart Code for Information Interchange ..... 13
**BAB III METODOLOGI PENELITIAN** ..... 15
3.1 Tahapan Penelitian ..... 15
3.2 Gambaran Umum Sistem ..... 16
3.3 Waktu dan Lokasi Penelitian ..... 17
3.4 Analisis Kebutuhan ..... 18
3.5 Perancangan Sistem ..... 19
3.6 Pengembangan Sistem ..... 24

3.7 Pengujian Sistem ..... 47
3.8 Analisis Hasil Sistem..... 49
**BAB IV HASIL DAN PEMBAHASAN** .....53
4.1 Hasil Pengembangan Sistem ..... 53
4.2 Hasil Pengujian Sistem..... 56
4.3 Hasil Analisis Hasil Sistem ..... 59
**BAB V PENUTUP**.....67
5.1 Kesimpulan..... 67
5.2 Saran..... 67
**DAFTAR PUSTAKA**.....69
**LAMPIRAN**.....72
Lampiran 1 *Source Code* Sistem..... 72
Lampiran 2 Sampel Pesan Rahasia ..... 73
Lampiran 3 Keseluruhan Perbandingan Nilai PSNR Hasil Steganografi dengan Metode 1-LSB, 2-LSB, dan 3-LSB ..... 76
Lampiran 4 Keseluruhan Perbandingan Nilai PSNR Hasil Steganografi dengan Metode *Single-frame* dan *Multi-frame* ..... 91

# DAFTAR TABEL

Tabel 3.1 Input Data Menyembunyikan Pesan .....26
Tabel 3.2 *Delimiter* .....31
Tabel 3.3 Input Data Menampilkan Pesan .....39
Tabel 3.4 Skenario Black Box Testing .....47
Tabel 3.5 Sampel Video .....51
Tabel 4.1 Hasil Black Box Testing .....57
Tabel 4.2 Perbandingan Ukuran *File Video Codec* .....59
Tabel 4.3 Perbandingan Ukuran *File* Video Sebelum dan Setelah Steganografi dengan *Video Codec* dan *Preset* yang sama .....61
Tabel 4.4 Hasil Nilai Peak Signal to Noise Ratio antara 1-LSB, 2-LSB, dan 3-LSB .....62
Tabel 4.5 Hasil Nilai Peak Signal to Noise Ratio antara *Single-frame* dan *Multi-frame* .....62

# DAFTAR GAMBAR

Gambar 2.1 Proses Enkripsi dan Dekripsi .....9
Gambar 2.2 Most Significant Bit dan Least Significant Bit .....10
Gambar 2.3 Tabel Vigenere Cipher .....12
Gambar 2.4 Tabel ASCII .....14
Gambar 3.1 Diagram Tahapan Penelitian .....15
Gambar 3.2 Gambaran Umum Sistem .....16
Gambar 3.3 *Flowchart* Sederhana Sistem.....19
Gambar 3.4 *Wireframe* Halaman Utama.....20
Gambar 3.5 *Wireframe* Halaman Memilih Video Input .....21
Gambar 3.6 *Wireframe* Halaman Memilih Video Steganografi .....21
Gambar 3.7 *Wireframe* Halaman Menyembunyikan Pesan Rahasia .....22
Gambar 3.8 *Wireframe* Halaman Menampilkan Pesan Rahasia .....23
Gambar 3.9 *Wireframe Pop up* Menyembunyikan Pesan Berhasil .....23
Gambar 3.10 *Wireframe Pop up* Menampilkan Pesan Berhasil .....24
Gambar 3.11 *Flowchart* Menyembunyikan Pesan.....25
Gambar 3.12 Proses Pemisahan Pesan menjadi List.....28
Gambar 3.13 *Flowchart* Enkripsi dengan Algoritma Vigenere Cipher .....29
Gambar 3.14 Proses Enkripsi Vigenere Cipher .....30
Gambar 3.15 Proses Penyisipan *Delimiter*.....31
Gambar 3.16 *Raw* Data Nilai Warna *Frame*.....32
Gambar 3.17 *Flowchart* Menyembunyikan Data dengan Algoritma Least Significant Bit.....33
Gambar 3.18 Proses Konversi ASCII & Konversi Biner dari *Ciphertext*.....34
Gambar 3.19 Proses Konversi Biner dari Nilai Warna *Pixel*.....35
Gambar 3.20 Proses Substitusi Biner.....35
Gambar 3.21 Contoh Hasil Citra Setelah Proses Substitusi Least Significant Bit .....36
Gambar 3.22 *Flowchart* Menampilkan Pesan Rahasia .....38
Gambar 3.23 Flowchart Mendapatkan *Ciphertext* Metadata dengan Algoritma Least Significant Bit .....41
Gambar 3.24 *Flowchart* Mendapatkan *Ciphertext* Pesan dengan Algoritma Least Significant Bit .....42
Gambar 3.25 Proses Pengambilan Data dari *Frame* .....43
Gambar 3.26 *Flowchart* Dekripsi dengan Algoritma Vigenere Cipher.....45
Gambar 3.27 Proses Dekripsi Vigenere Cipher .....46
Gambar 3.28 Proses Penggabungan Kata .....47
Gambar 4.1 Tangkapan Layar Halaman Utama.....53
Gambar 4.2 Tangkapan Layar Halaman Memilih Video Input .....54
Gambar 4.3 Tangkapan Layar Halaman Menyembunyikan Pesan Rahasia ....54
Gambar 4.4 Tangkapan Layar *Pop up* Pesan Rahasia Berhasil Disembunyikan .....55
Gambar 4.5 Tangkapan Layar Halaman Memilih Video Steganografi .....55
Gambar 4.6 Tangkapan Layar Halaman Menampilkan Pesan Rahasia .....56

Gambar 4.7 Tangkapan Layar *Pop up* Pesan Rahasia Berhasil Didapatkan....56
Gambar 4.8 Perbandingan Citra *Frame* pada Video1.....63
Gambar 4.9 Perbandingan Citra *Frame* pada Video2.....64
Gambar 4.10 Perbandingan Citra *Frame* pada Video3.....65

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Seiring dengan kemajuan teknologi internet, media digital seperti gambar, audio, video dan teks dapat dibagi dan dikirimkan melalui internet dengan lebih mudah. Namun, salah satu tantangan utama dalam berbagi dan mentransmisikan semua jenis informasi melalui saluran publik adalah keamanan data (Widianto, 2018). Dengan berbagai teknik seseorang bisa mengakses informasi secara ilegal, sehingga banyak yang mencoba untuk mengakses informasi yang bukan haknya (Hafiz, 2019). Pada tahun 2021, sekitar 51.829 orang menjadi korban insiden keamanan di mana data sensitif, dilindungi, atau rahasia seseorang disalin, dikirim, dilihat, dicuri, atau digunakan oleh pihak yang tidak berwenang (Federal Bureau of Investigation, 2021). Oleh karena itu, beberapa cara untuk melindungi informasi yang dikirimkan terhadap pihak yang tidak berwenang menjadi sebuah kebutuhan (Widianto, 2018).

Berbagai macam teknik digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berwenang, diantaranya ialah teknik steganografi dan teknik kriptografi. Steganografi memiliki alur yang searah dengan kriptografi, dimana steganografi memiliki tujuan untuk menyembunyikan pesan-pesan rahasia melalui sebuah perantara yaitu media, sedangkan kriptografi memiliki tujuan untuk memberikan samaran dari sebuah pesan (Gunawan, 2018).

Untuk memberikan kepercayaan dan keamanan kepada pengguna untuk melindungi informasinya, kita dapat menggabungkan teknik steganografi dan kriptografi (Al-Juaid dkk., 2018). Sebagai salah satu bentuk implementasinya, sebuah data berbentuk teks dapat disamarkan lalu disembunyikan ke dalam sebuah video (media) (Gunawan, 2018).

Perkembangan teknologi internet menunjukkan kemungkinan penggunaan video steganografi sebagai metode yang ampuh dan aman untuk berbagi data rahasia seperti informasi perbankan, informasi hak cipta, informasi intelijen militer, dll (Hussein dkk., 2020). Video steganografi menjadi area penelitian penting dalam teknologi penyembunyian data dan telah menjadi alat yang menjanjikan karena kebutuhan keamanan transmisi pesan rahasia yang menjadi lebih ketat serta media video yang lebih digemari (Liu dkk., 2019). Menurut survei, konsumsi video online masyarakat mengalami peningkatan sebesar 73%, paling besar dibandingkan media lainnya (Global Web Index, 2020). Video pada dasarnya adalah kumpulan dari beberapa citra digital individu yang biasa disebut dengan *frame* (Pangaribuan dkk., 2020). Salah satu metode teknik steganografi yang dapat dilakukan untuk menyisipkan teks ke dalam sebuah video ialah Least Significant Bit (LSB), yaitu substitusi bit yang paling kurang berpengaruh dalam nilai warna RGB setiap *pixel* pada *frame* dengan bit pesan yang ingin disisipkan sehingga tidak memberikan perbedaan signifikan pada *pixel* tersebut dan dapat mengeksploitasi keterbatasan kekuatan sistem penglihatan manusia (Nur'aini, 2019). Untuk memastikan pesan yang disembunyikan hanya dapat dibaca oleh penerima yang dituju, digunakan teknik kriptografi dengan algoritma Vigenere Cipher sebelum dan sesudah pesan

disembunyikan pada video. Vigenere Cipher menerjemahkan karakter pada pesan berdasarkan *key* yang diberikan. Algoritma ini menerapkan mekanisme transfer yang menggeser setiap karakter pada pesan dengan jumlah yang berbeda pada tabel yang disebut "Vigenere Table" (Nahar dkk., 2020).

Penyembunyian pesan pada beberapa *frame* (*multi-frame*) untuk meminimalkan perubahan warna *pixel* pada satu *frame* diharapkan dapat meningkatkan keamanan dari teknik steganografi jika dibandingkan dengan metode *single-frame* pada penelitian sebelumnya. Oleh karena itu, penulis ingin mengajukan penelitian berjudul "Implementasi Steganografi *Multi-frame* pada Media Video" sebagai cara untuk melindungi informasi teks (pesan) pada saluran publik (internet) dari pihak yang tidak berwenang.

## 1.2 Rumusan Masalah

a. Bagaimana melindungi pesan rahasia pada saluran internet dari pihak yang tidak berwenang dengan Video Steganografi *Multi-frame* menggunakan kombinasi Algoritma Least Significant Bit dan Vigenere Cipher?
b. Bagaimana perbandingan kualitas citra antara video steganografi dengan metode *multi-frame* dan *single-frame*?

## 1.3 Tujuan Penelitian

a. Mengetahui cara untuk melindungi pesan rahasia pada saluran internet dari pihak yang tidak berwenang dengan Video Steganografi *Multi-frame*

menggunakan kombinasi Algoritma Least Significant Bit dan Vigenere Cipher.

b. Mengetahui perbandingan kualitas citra antara video steganografi dengan Metode *Multi-frame* dan *Single-frame*.

## 1.4 Manfaat Penelitian

a. Memberikan informasi tentang kombinasi Algoritma Least Significant Bit dan Vigenere Cipher dapat menyembunyikan pesan pada media video.
b. Membantu masyarakat untuk melindungi pesannya dalam media video agar pesannya hanya dapat dibaca oleh penerima yang dituju.

## 1.5 Batasan Masalah

a. Sistem hanya dapat mengkompres video pada *lossless video codec*.
b. Video hanya dikirimkan melalui layanan tanpa kompresi.
c. Sistem hanya dapat menerima karakter ASCII.
d. Pengirim dan penerima yang dituju sudah mengetahui *key* yang digunakan untuk menyamarkan pesan.

## 1.6 Sistematika Penulisan

**BAB I PENDAHULUAN:** Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan.

**BAB II TINJAUAN PUSTAKA:** Pada bab ini akan dijelaskan teori-teori yang menunjang penelitian yang dilakukan.

**BAB III METODOLOGI PENELITIAN:** Bab ini berisi tahapan-tahapan yang dilakukan selama proses penelitian.

**BAB IV HASIL DAN PEMBAHASAN:** Bab ini berisi hasil penelitian dan pembahasan dari penelitian yang dilakukan.

**BAB V PENUTUP:** Bab ini berisi kesimpulan dari hasil penelitian dan saran untuk penelitian kedepannya.

# BAB II

# TINJAUAN PUSTAKA

## 2.1 Video Digital

Video digital pada dasarnya tersusun atas serangkaian *frame*. Rangkaian *frame* tersebut ditampilkan pada layar dengan kecepatan tertentu, tergantung pada *frame* rate yang diberikan (dalam *frame* per second). Jika *frame* rate cukup tinggi, mata manusia tidak dapat menangkap gambar atau *frame*, melainkan menangkapnya sebagai rangkaian yang kontinu/berlanjut (video) (Anti dkk., 2017).

Masing-masing *frame* merupakan citra digital. Suatu citra digital direpresentasikan dengan sebuah matriks yang masing-masing elemennya merepresentasikan nilai intensitas. Jika I adalah matriks dua dimensi, I (x,y) adalah nilai intensitas yang sesuai pada posisi baris x dan kolom y pada matriks tersebut. Titik-titik ditempatkan image di sampling disebut picture elements, atau sering dikenal sebagai piksel. *Pixel* atau piksel (picture element / unsur gambar) adalah titik–titik kecil. Gambar apapun yang tampak pada layar komputer sebenarnya tersusun dari titik-titik kecil (Anti dkk., 2017).

Jika beberapa piksel diletakkan berderet maka yang tampak adalah sebuah garis. Jadi semua garis, sehalus apapun tampaknya pada layar komputer, sebenarnya adalah deretan piksel (Anti dkk., 2017).

### 2.1.1 *Frame* Per Second

Ketika serangkaian gambar mati yang bersambung dilihat oleh mata manusia, maka suatu keajaiban terjadi. Jika gambar-gambar tersebut dimainkan dengan cepat maka akan terlihat sebuah pergerakan yang halus, inilah prinsip dasar film, video dan animasi. Jumlah gambar yang terlihat setiap detik disebut dengan *frame* rate. Diperlukan *frame* rate minimal sebesar 10 fps (*frame* rate per second) untuk menghasilkan gambar pergerakan yang halus (Anti dkk., 2017).

### 2.1.2 *Frame* Size dan Resolusi

Lebar dan tinggi *frame* video disebut dengan *frame* size, yang menggunakan satuan *pixel*, misalnya video dengan *frame* size 640x480 *pixel*. Dalam dunia digital video, *frame* size disebut juga dengan resolusi. Semakin tinggi resolusi gambar maka semakin besar pula informasi yang dimuat, berarti akan semakin besar pula kebutuhan memory untuk membaca informasi tersebut (Anti dkk., 2017).

## 2.2 Kompresi Video

Lossy compression yaitu suatu metode kompresi data yang menghilangkan sebagian “informasi” dari data asli selama proses kompresi dengan tidak menghilangkan secara signifikan informasi yang ada dalam data secara keseluruhan, sedangkan lossless compression yaitu suatu metode kompresi data

dengan tidak ada “informasi” data yang hilang atau berkurang jumlahnya selama proses kompresi (Pangesti dkk., 2020).

## 2.3 Warna RGB

Kepekaan mata manusia terhadap warna merah, hijau, dan biru mendasari teori citra RGB. Bila dilakukan pencampuran ketiga unsur warna tersebut dapat menghasilkan warna lain yang disebut additive color. Pengaturan warna RGB (Red, Green, Blue) menggunakan skala mulai dari 0 sampai dengan 255. Warna dari tiap piksel ditentukan dengan kombinasi intensitas red, green dan blue yang disimpan di tiap saluran warna di lokasi piksel tertentu. Format *file* grafik menyimpan RGB image sebagai 24-bit image, dengan komponen red, green, dan blue masing-masing 8 bit (Himmah dkk., 2020).

## 2.4 Steganografi

Steganografi berasal dari bahasa Yunani yaitu Steganos yang berarti menyembunyikan dan Graptos yang artinya tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan. Secara umum steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia (Hafiz, 2019).

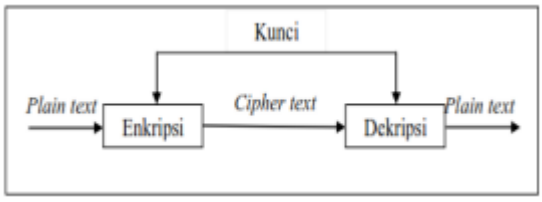
Dalam praktiknya, agar data menjadi lebih aman, data diacak terlebih dahulu menggunakan kriptografi, kemudian baru dilakukan proses steganografi agar lebih maksimal dalam mengamankan dan menjaga kerahasiaan. Steganografi membutuhkan dua properti, yaitu data dan wadah penampung data. wadah

penampung yang umumnya digunakan berupa teks, suara, gambar, atau video. Sedangkan data yang disembunyikan dapat berupa teks, gambar, atau data yang lainnya (Hafiz, 2019).

Keuntungan menggunakan steganografi adalah memungkinkan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim karena pesan tersembunyi. Ini membuat pihak ketiga tidak menyadari keberadaan pesan (Hafiz, 2019).

## 2.5 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu kryptos yang memiliki arti tersembunyi atau rahasia dan graphein artinya menulis. Kriptografi adalah ilmu untuk mengenkripsi atau mengacak, dimana data asli atau plaintext diacak menggunakan kunci enkripsi untuk menjadi naskah acak yang sulit dibaca atau yang disebut dengan *ciphertext* (Hafiz, 2019). Proses enkripsi dan dekripsi dapat dilihat pada Gambar 2.1.




Gambar 2.1 Proses Enkripsi dan Dekripsi

Kriptografi memiliki 4 komponen utama yaitu:

1. *Plaintext*, yaitu pesan yang dapat dibaca.
2. *Ciphertext*, yaitu pesan sandi/pesan acak yang tidak bisa dibaca.
3. *Key*, yaitu kunci untuk melakukan teknik kriptografi.

4. Algoritma, yaitu metode untuk melakukan enkripsi dan dekripsi (Irawan, 2017).

## 2.6 Least Significant Bit

Penyembunyian pesan dilakukan dengan menggantikan bit-bit didalam segmen citra dengan bit-bit pesan rahasia. Metode yang paling sering digunakan adalah metode modifikasi LSB (Least Significant Bit) pada citra penampung. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit paling signifikan yang disebut MSB (Most Significant Bit) dan bit yang paling kurang signifikan atau LSB (Least Significant Bit) (Anti dkk., 2017). Perbedaan antara Most Significant Bit dan Least Significant Bit dapat dilihat pada Gambar 2.2.


Gambar 2.2 Most Significant Bit dan Least Significant Bit

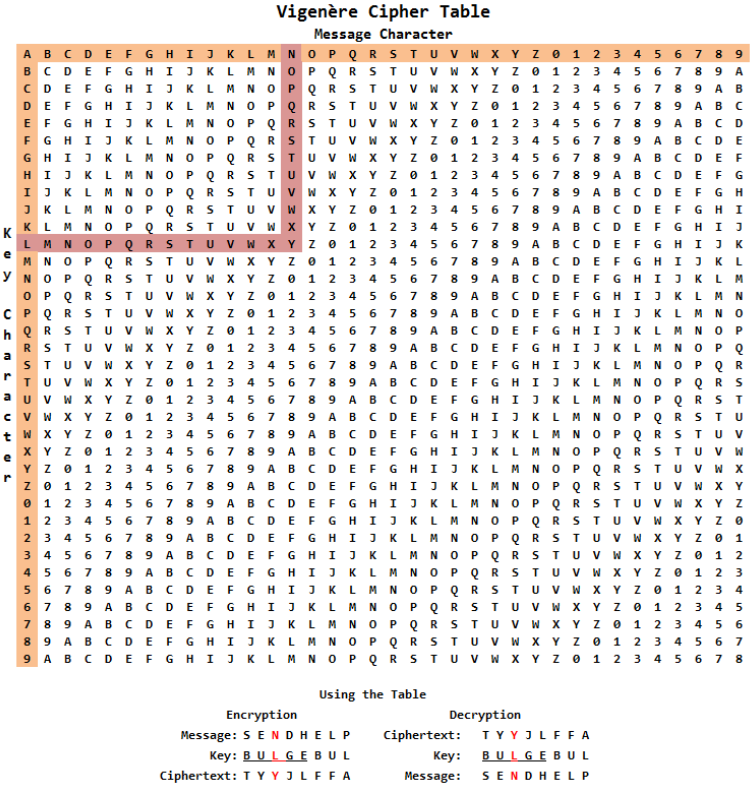
Contoh susunan bit pada byte yang menjelaskan bit yang cocok untuk diganti adalah bit LSB, sebab penggantian hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte di dalam gambar menyatakan warna tertentu, maka perubahan pada bit LSBnya tidak mengubah warna secara signifikan. Sebelum melakukan penggantian bit-bit LSB, semua data citra yang tidak bertipe 24 bit diubah terlebih dahulu menjadi format 24 bit. Jadi setiap data piksel sudah mengandung komponen warna merah, hijau dan biru (RGB). Nilai dari bit-bit yang kurang signifikan atau LSB dari setiap byte di dalam

bitmap digantikan dengan bit-bit pesan yang akan disembunyikan. Jika byte merupakan komponen hijau (G), maka penggantian satu bit LSB-nya hanya mengubah sedikit kadar warna hijau, dan perubahannya tak terdeteksi oleh mata manusia (Anti dkk., 2017).

## 2.7 Vigenere Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 (Irawan, 2017).

Cara kerja dari Vigenère cipher yaitu dengan mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. Vigenère cipher adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda (Irawan, 2017). Tabel Vigenere dan cara kerjanya dapat dilihat pada Gambar 2.3.




Gambar 2.3 Tabel Vigenere Cipher

Kunci pada Vigenère cipher berbentuk deretan huruf. Kunci yang berbetuk deretan huruf tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui (Irawan, 2017).

## 2.8 Peak Signal to Noise Ratio

Istilah peak signal-to-noise ratio (PSNR) adalah ekspresi untuk rasio antara nilai (daya) maksimum yang mungkin dari suatu sinyal dan kekuatan distorsi noise yang memengaruhi kualitas representasinya. Karena banyak sinyal memiliki rentang

dinamis yang sangat luas, (rasio antara nilai terbesar dan terkecil dari kuantitas yang dapat diubah), PSNR biasanya dinyatakan dalam skala desibel logaritmik (Ni, 2020).

Nilai PSNR ≥ 40 dB menggambarkan perbedaan antara dua citra dengan 8 bit per channel hampir tidak terlihat oleh mata manusia, sedangkan nilai PSNR = ∞ untuk citra identik (Chervyakov dkk., 2020).

## 2.9 American Standart Code for Information Interchange

Kode ASCII adalah representasi numerik komputer untuk karakter keyboard. Ini berkisar dari 0-255. Karakter dikodekan dalam 1 byte, sebenarnya dalam 7 bit dan bit ke-8 digunakan untuk menyimpan simbol bahasa lain seperti á atau ñ (Elshoush dkk., 2021).

Kode ASCII dengan nilai 0-127 adalah kode untuk memanipulasi teks. Kode ASCII cukup banyak digunakan untuk meningkatkan keamanan informasi, seperti keamanan informasi pada e-voting, dan menghasilkan suatu deretan karakter yang tidak mudah untuk ditebak dan memberikan kemungkinan yang luas pada lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet, tetapi juga mencakup karakter-karakter seperti ., ”, ‘, =, @, #, %, dan sebagainya (Hamdani dkk., 2020). Tabel ASCII dapat dilihat pada Gambar 2.4.

# ASCII TABLE

| Decimal | Hexadecimal | Binary | Octal | Char |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | *[NULL]* |
| 1 | 1 | 1 | 1 | *[START OF HEADING]* |
| 2 | 2 | 10 | 2 | *[START OF TEXT]* |
| 3 | 3 | 11 | 3 | *[END OF TEXT]* |
| 4 | 4 | 100 | 4 | *[END OF TRANSMISSION]* |
| 5 | 5 | 101 | 5 | *[ENQUIRY]* |
| 6 | 6 | 110 | 6 | *[ACKNOWLEDGE]* |
| 7 | 7 | 111 | 7 | *[BELL]* |
| 8 | 8 | 1000 | 10 | *[BACKSPACE]* |
| 9 | 9 | 1001 | 11 | *[HORIZONTAL TAB]* |
| 10 | A | 1010 | 12 | *[LINE FEED]* |
| 11 | B | 1011 | 13 | *[VERTICAL TAB]* |
| 12 | C | 1100 | 14 | *[FORM FEED]* |
| 13 | D | 1101 | 15 | *[CARRIAGE RETURN]* |
| 14 | E | 1110 | 16 | *[SHIFT OUT]* |
| 15 | F | 1111 | 17 | *[SHIFT IN]* |
| 16 | 10 | 10000 | 20 | *[DATA LINK ESCAPE]* |
| 17 | 11 | 10001 | 21 | *[DEVICE CONTROL 1]* |
| 18 | 12 | 10010 | 22 | *[DEVICE CONTROL 2]* |
| 19 | 13 | 10011 | 23 | *[DEVICE CONTROL 3]* |
| 20 | 14 | 10100 | 24 | *[DEVICE CONTROL 4]* |
| 21 | 15 | 10101 | 25 | *[NEGATIVE ACKNOWLEDGE]* |
| 22 | 16 | 10110 | 26 | *[SYNCHRONOUS IDLE]* |
| 23 | 17 | 10111 | 27 | *[ENG OF TRANS. BLOCK]* |
| 24 | 18 | 11000 | 30 | *[CANCEL]* |
| 25 | 19 | 11001 | 31 | *[END OF MEDIUM]* |
| 26 | 1A | 11010 | 32 | *[SUBSTITUTE]* |
| 27 | 1B | 11011 | 33 | *[ESCAPE]* |
| 28 | 1C | 11100 | 34 | *[FILE SEPARATOR]* |
| 29 | 1D | 11101 | 35 | *[GROUP SEPARATOR]* |
| 30 | 1E | 11110 | 36 | *[RECORD SEPARATOR]* |
| 31 | 1F | 11111 | 37 | *[UNIT SEPARATOR]* |
| 32 | 20 | 100000 | 40 | *[SPACE]* |
| 33 | 21 | 100001 | 41 | **!** |
| 34 | 22 | 100010 | 42 | **"** |
| 35 | 23 | 100011 | 43 | **#** |
| 36 | 24 | 100100 | 44 | **$** |
| 37 | 25 | 100101 | 45 | **%** |
| 38 | 26 | 100110 | 46 | **&** |
| 39 | 27 | 100111 | 47 | **'** |
| 40 | 28 | 101000 | 50 | **(** |
| 41 | 29 | 101001 | 51 | **)** |
| 42 | 2A | 101010 | 52 | ***** |
| 43 | 2B | 101011 | 53 | **+** |
| 44 | 2C | 101100 | 54 | **,** |
| 45 | 2D | 101101 | 55 | **-** |
| 46 | 2E | 101110 | 56 | **.** |
| 47 | 2F | 101111 | 57 | **/** |
| 48 | 30 | 110000 | 60 | **0** |
| 49 | 31 | 110001 | 61 | **1** |
| 50 | 32 | 110010 | 62 | **2** |
| 51 | 33 | 110011 | 63 | **3** |
| 52 | 34 | 110100 | 64 | **4** |
| 53 | 35 | 110101 | 65 | **5** |
| 54 | 36 | 110110 | 66 | **6** |
| 55 | 37 | 110111 | 67 | **7** |
| 56 | 38 | 111000 | 70 | **8** |
| 57 | 39 | 111001 | 71 | **9** |
| 58 | 3A | 111010 | 72 | **:** |
| 59 | 3B | 111011 | 73 | **;** |
| 60 | 3C | 111100 | 74 | **<** |
| 61 | 3D | 111101 | 75 | **=** |
| 62 | 3E | 111110 | 76 | **>** |
| 63 | 3F | 111111 | 77 | **?** |
| 64 | 40 | 1000000 | 100 | **@** |
| 65 | 41 | 1000001 | 101 | **A** |
| 66 | 42 | 1000010 | 102 | **B** |
| 67 | 43 | 1000011 | 103 | **C** |
| 68 | 44 | 1000100 | 104 | **D** |
| 69 | 45 | 1000101 | 105 | **E** |
| 70 | 46 | 1000110 | 106 | **F** |
| 71 | 47 | 1000111 | 107 | **G** |
| 72 | 48 | 1001000 | 110 | **H** |
| 73 | 49 | 1001001 | 111 | **I** |
| 74 | 4A | 1001010 | 112 | **J** |
| 75 | 4B | 1001011 | 113 | **K** |
| 76 | 4C | 1001100 | 114 | **L** |
| 77 | 4D | 1001101 | 115 | **M** |
| 78 | 4E | 1001110 | 116 | **N** |
| 79 | 4F | 1001111 | 117 | **O** |
| 80 | 50 | 1010000 | 120 | **P** |
| 81 | 51 | 1010001 | 121 | **Q** |
| 82 | 52 | 1010010 | 122 | **R** |
| 83 | 53 | 1010011 | 123 | **S** |
| 84 | 54 | 1010100 | 124 | **T** |
| 85 | 55 | 1010101 | 125 | **U** |
| 86 | 56 | 1010110 | 126 | **V** |
| 87 | 57 | 1010111 | 127 | **W** |
| 88 | 58 | 1011000 | 130 | **X** |
| 89 | 59 | 1011001 | 131 | **Y** |
| 90 | 5A | 1011010 | 132 | **Z** |
| 91 | 5B | 1011011 | 133 | **[** |
| 92 | 5C | 1011100 | 134 | **** |
| 93 | 5D | 1011101 | 135 | **]** |
| 94 | 5E | 1011110 | 136 | **^** |
| 95 | 5F | 1011111 | 137 | **_** |
| 96 | 60 | 1100000 | 140 | **`** |
| 97 | 61 | 1100001 | 141 | **a** |
| 98 | 62 | 1100010 | 142 | **b** |
| 99 | 63 | 1100011 | 143 | **c** |
| 100 | 64 | 1100100 | 144 | **d** |
| 101 | 65 | 1100101 | 145 | **e** |
| 102 | 66 | 1100110 | 146 | **f** |
| 103 | 67 | 1100111 | 147 | **g** |
| 104 | 68 | 1101000 | 150 | **h** |
| 105 | 69 | 1101001 | 151 | **i** |
| 106 | 6A | 1101010 | 152 | **j** |
| 107 | 6B | 1101011 | 153 | **k** |
| 108 | 6C | 1101100 | 154 | **l** |
| 109 | 6D | 1101101 | 155 | **m** |
| 110 | 6E | 1101110 | 156 | **n** |
| 111 | 6F | 1101111 | 157 | **o** |
| 112 | 70 | 1110000 | 160 | **p** |
| 113 | 71 | 1110001 | 161 | **q** |
| 114 | 72 | 1110010 | 162 | **r** |
| 115 | 73 | 1110011 | 163 | **s** |
| 116 | 74 | 1110100 | 164 | **t** |
| 117 | 75 | 1110101 | 165 | **u** |
| 118 | 76 | 1110110 | 166 | **v** |
| 119 | 77 | 1110111 | 167 | **w** |
| 120 | 78 | 1111000 | 170 | **x** |
| 121 | 79 | 1111001 | 171 | **y** |
| 122 | 7A | 1111010 | 172 | **z** |
| 123 | 7B | 1111011 | 173 | **{** |
| 124 | 7C | 1111100 | 174 | **\|** |
| 125 | 7D | 1111101 | 175 | **}** |
| 126 | 7E | 1111110 | 176 | **~** |
| 127 | 7F | 1111111 | 177 | *[DEL]* |

Gambar 2.4 Tabel ASCII