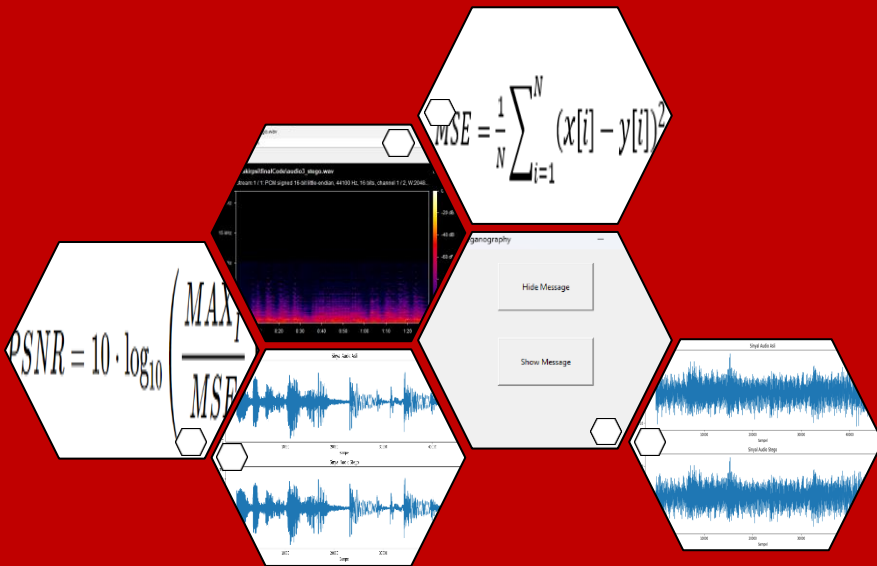


# ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO DALAM MENGAMANKAN INFORMASI

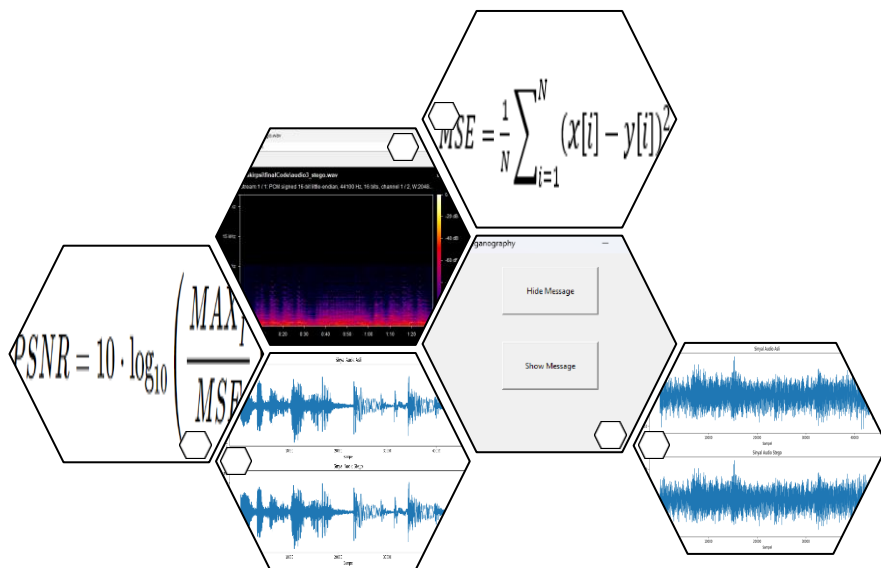


**WIRA SATYA TRI ALMI**  
**D121181324**



**PROGRAM STUDI TEKNIK INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS HASANUDDIN**  
**GOWA**  
**2025**

# ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO DALAM MENGAMANKAN INFORMASI



**WIRA SATYA TRI ALMI**  
**D121181324**



**PROGRAM STUDI TEKNIK INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS HASANUDDIN**  
**GOWA**  
**2025**

**HALAMAN JUDUL**

**ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO  
DALAM MENGAMANKAN INFORMASI**

**WIRA SATYA TRI ALMI  
D121181324**



**PROGRAM STUDI SARJANA TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS HASANUDDIN  
GOWA  
2025**

**PERNYATAAN PENGAJUAN SKRIPSI**

**ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO**  
**DALAM MENGAMANKAN INFORMASI**

Disusun dan diajukan oleh:

Wira Satya Tri Almi  
D121181324

Skripsi  
sebagai salah satu syarat untuk mencapai gelar sarjana

Pada

**PROGRAM STUDI SARJANA TEKNIK INFORMATIKA**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS HASANUDDIN**  
**GOWA**  
**2025**

**HALAMAN PENGESAHAN SKRIPSI****SKRIPSI****ANALISIS KRIPTOGRAFI DAN STEGANOGRAFI AUDIO DALAM  
MENGAMANKAN INFORMASI****WIRA SATYA TRI ALMI****D12118134**

Skripsi,  
Telah dipertahankan di hadapan Panitia Ujian Sarjana Teknik Informatika pada 07  
Februari 2025 dan dinyatakan telah memenuhi syarat kelulusan  
pada

Program Studi Teknik Informatika  
Departemen Teknik Informatika  
Fakultas Teknik  
Universitas Hasanuddin  
Makassar

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,

Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.  
NIP.197503132009121003

Mukarramah Yusuf, B.Sc., M.Sc., Ph.D  
NIP. 198310082012122003

Ketua Program Studi,

Prof. Dr. Ir. Indrabayu ST, MT,M.Bus.Sys.,IPM, ASEAN. Eng.  
NIP 19750716 200212 1 004

## PERNYATAAN KEASLIAN SKRIPSI

Dengan ini penulis menyatakan bahwa skripsi berjudul “Analisis Kriptografi dan Steganografi Audio Dalam Mengamankan Informasi” adalah benar karya penulis dengan arahan dari pembimbing bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T.dan ibu Mukarramah Yusuf, B.Sc., M.Sc., Ph.D Karya ilmiah ini belum diajukan dan tidak sedang diajukan dalam bentuk apa pun kepada perguruan tinggi manapun. Sumber informasi berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam daftar pustaka skripsi ini. Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini karya orang lain, maka penulis bersedia menerima sanksi atas perbuatan tersebut berdasarkan aturan yang berlaku.

Dengan ini penulis melimpahkan hak cipta (hak ekonomis) karya tulis penulis berupa skripsi ini kepada Universitas Hasanuddin.

Gowa, 19 Maret 2025

Materai

Wira Satya Tri Almi

D121181324

## ABSTRAK

**WIRA SATYA TRI ALMI.** Analisis Kombinasi Kriptografi dan Steganografi Audio dalam Mengamankan Informasi (dibimbing oleh Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. dan Ibu Mukarramah Yusuf, B.Sc., M.Sc.)

Dengan perkembangan teknologi internet saat ini, volume dan sensitivitas lalu lintas data elektronik meningkat secara signifikan, sehingga risiko kejahatan digital juga semakin besar. Dalam konteks pertukaran informasi jarak jauh atau pengiriman pesan, jalur transmisi yang aman dari penyadapan tidak selalu terjamin. Oleh karena itu, diperlukan metode yang efektif untuk melindungi data atau informasi. Salah satu teknik yang digunakan untuk mengamankan data adalah kriptografi dan steganografi, yang memungkinkan informasi disembunyikan dalam media seperti audio. Penelitian ini mengembangkan sistem yang menggabungkan algoritma steganografi Least Significant Bit (LSB) dengan algoritma kriptografi Advanced Encryption Standard (AES) untuk menyembunyikan pesan dalam audio. Sistem ini memiliki dua fitur utama: menyembunyikan pesan rahasia dalam audio dan mengekstrak pesan rahasia dari audio steganografi. Pengujian sistem steganografi audio menggunakan algoritma LSB dengan metode *black box testing* menunjukkan tingkat keberhasilan 100%. Analisis objektif menggunakan parameter *Peak Signal to Noise Ratio* (PSNR) pada audio steganografi menunjukkan bahwa kualitas audio tetap tinggi sebelum dan sesudah penyisipan pesan. Nilai PSNR yang dihasilkan berada dalam rentang yang baik, menunjukkan bahwa perubahan pada LSB tidak mempengaruhi kualitas audio secara signifikan. Selain itu, analisis subjektif menggunakan pendengaran manusia menunjukkan bahwa perbedaan antara audio asli dan audio yang telah disisipi pesan sangat sulit dideteksi karena perubahan dalam bentuk noise atau distorsi minimal.

**Kata Kunci:** Audio, Kriptografi, Steganografi.

## ABSTRACT

**WIRA SATYA TRI ALMI.** *Analysis of Combining Cryptography and Audio Steganography in Securing Information* (supervised by Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. dan Ibu Mukarramah Yusuf, B.Sc., M.Sc.)

*With the advancement of internet technology, the volume and sensitivity of electronic data traffic have increased significantly, leading to a greater risk of digital crimes. In long-distance information exchange or message transmission, secure transmission channels free from eavesdropping are not always guaranteed. Therefore, effective methods are required to protect data or information. One of the techniques used to secure data is cryptography and steganography, which allow information to be hidden within media such as audio. This study develops a system that combines the steganography algorithm Least Significant Bit (LSB) with the cryptography algorithm Advanced Encryption Standard (AES) to hide messages in audio. This system has two main features: hiding secret messages in audio and extracting secret messages from steganographic audio. The testing of the audio steganography system using the LSB algorithm with the black box testing method showed a 100% success rate. Objective analysis using the Peak Signal Noise Ratio (PSNR) parameter on steganographic audio indicated that the audio quality remained high before and after message insertion. The resulting PSNR values were within a good range, showing that the changes to the LSB did not significantly affect audio quality. Furthermore, subjective analysis using human hearing revealed that the differences between the original audio and the audio with hidden messages were challenging to detect due to minimal changes in the form of noise or distortion.*

**Keywords:** Audio, Cryptography, Steganography



## DAFTAR ISI

HALAMAN JUDUL .....	1
PERNYATAAN PENGAJUAN SKRIPSI .....	2
HALAMAN PENGESAHAN SKRIPSI .....	3
PERNYATAAN KEASLIAN SKRIPSI .....	4
ABSTRAK.....	5
ABSTRACT .....	6
DAFTAR ISI.....	7
DAFTAR GAMBAR.....	9
DAFTAR TABEL.....	10
DAFTAR SINGKATAN DAN ARTI SIMBOL.....	11
DAFTAR LAMPIRAN .....	12
KATA PENGANTAR .....	13
BAB I PENDAHULUAN .....	14
1.1 Latar Belakang .....	14
1.2 Rumusan Masalah .....	15
1.3 Tujuan Penelitian .....	15
1.4 Manfaat Penelitian .....	15
1.5 Ruang Lingkup/Asumsi perancangan.....	15
1.6 Teori.....	16
1.6.1 Audio.....	16
1.6.2 WAV .....	16
1.6.3 Kriptografi .....	16
1.6.4 <i>Algoritma AES</i> (Advanced Encryption Standard) .....	17
1.6.5 Konsep Dasar Kriptografi .....	18
1.6.4 Steganografi.....	19
1.6.5 Least Significant Bit (LSB) .....	20
BAB II METODE PENELITIAN .....	22
2.1 Tahapan Penelitian .....	22
2.2 Instrumen Penelitian .....	23
2.3 Waktu dan Lokasi Penelitian .....	23

2.4	Perancangan Sistem.....	23
2.4.1	Gambaran Umum Sistem.....	23
2.4.2	Flowchart.....	24
2.4.3	<i>Wireframe</i> .....	25
2.5	Pengembangan sistem.....	30
2.5.1	Menyembunyikan Pesan .....	30
2.5.2	Pengimputan Data.....	31
2.5.3	Pemeriksaan Tipe Data Audio .....	31
2.5.4	Enkripsi dengan AES.....	32
2.5.5	Hitung panjang pesan dan konversi ke Biner .....	32
2.5.6	Penyembunyian Data dengan Algoritma Least Significant Bit .....	33
2.6	Menampilkan Pesan .....	34
2.6.1	pengimputan data .....	35
2.6.2	Ekstraksi Least Significant Bit (LSB) dari Sampel Audio .....	35
2.6.3	Konversi Panjang Pesan.....	36
2.6.4	Ekstraksi Bit Pesan .....	36
2.6.5	Dekripsi dan Konversi ke Pesan Asli.....	36
2.7	Pengujian Sistem.....	37
3.8	Analisis Hasil Sistem.....	39
BAB III	.....	42
3.1	Hasil Pengembangan Sistem .....	42
3.2	Hasil Pengujian Sistem.....	46
3.3	Hasil Analisis Hasil Sistem .....	47
BAB IV	KESIMPULAN DAN SARAN .....	50
4.1	Kesimpulan .....	50
4.2	Saran .....	50
DAFTAR PUSTAKA	.....	51
LAMPIRAN	.....	53

## DAFTAR GAMBAR

Gambar 1 Algoritma AES .....	17
Gambar 2 MSB dan LSB .....	21
Gambar 3 Tahapan Penelitian .....	22
Gambar 4 Gambaran Umum Sistem .....	24
Gambar 5 Flowchart Sederhana Sistem .....	24
Gambar 6 Wireframe Halaman Utama .....	25
Gambar 7 Wireframe Halaman Memilih Audio .....	26
Gambar 8 Wireframe Halaman Memilih Audio .....	26
Gambar 9 Wireframe Halaman Menyembunyikan .....	27
Gambar 10 Wireframe Halaman Menampilkan Pesan .....	28
Gambar 11 Wireframe Pop up Menyembunyikan Pesan Berhasil .....	28
Gambar 12 Wireframe Pop up Menampilkan Pesan Berhasil .....	29
Gambar 13 Flowchart Menyembunyikan Pesan .....	30
Gambar 14 Flowchart Menampilkan pesan .....	34
Gambar 15 Flowchart PSNR .....	39
Gambar 16. Tangkapan Layar Halaman Utama .....	42
Gambar 17. Tangkapan Layar Halaman Memilih Audio Input .....	43
Gambar 18. Tangkapan Layar Halaman Menyembunyikan Pesan Rahasia .....	43
Gambar 19. Tangkapan Layar Pop up Pesan Rahasia Berhasil Disembunyikan .....	44
Gambar 20. Tangkapan Layar Halaman Memilih Audio Steganografi .....	44
Gambar 21. Tangkapan Layar Halaman Menampilkan Pesan Rahasia .....	45
Gambar 22. Tangkapan Layar Pop up Pesan Rahasia Berhasil Didapatkan .....	45
Gambar 23. (a) sinyal audio asli (sebelum disisipkan pesan) .....	48
Gambar 24. (a) sinyal audio asli sebelum disisipkan pesan dan (b) sinyal audio sesudah disisipkan pesan .....	49
Gambar 25. (a) sinyal audio asli sebelum disisipkan pesan dan (b) sinyal audio sesudah disisipkan pesan .....	49

## DAFTAR TABEL

Table 1 Input Data Menyembunyikan Pesan.....	31
Table 2 Input Data Menampilkan Pesan.....	35
Table 3 Skenario Black Box Testing .....	37
Table 4. Black Box Testing.....	46
Table 5. Hasil Nilai Peak Signal to Noise Ratio .....	47

## DAFTAR SINGKATAN DAN ARTI SIMBOL

Lambang/Singkatan	Arti dan Keterangan
AES	<i>Advanced Encryption Standard</i>
AIFF	<i>Audio Interchange File Format</i>
FIPS	<i>Federal Information Processing Standards</i>
$x[i]$	Nilai sampel dari sinyal audio asli pada indeks ke-i.
$y[i]$	Nilai sampel dari sinyal audio yang diproses pada indeks ke-i.
IV	<i>Initialitation Vector</i>
$MAX_1$	Nilai maksimal dari sampel audio, yaitu 32767 untuk data audio dengan format int16
MSB	<i>Most Significant Bit</i>
MSE	<i>Mean Squared Error</i>
N	Jumlah sampel audio
NIST	National Institute of Standards and Technology
PSNR	<i>Peak Signal to Noise Ratio</i>
RIFF	<i>Resource Interchange File Format</i>
WAV	<i>Waveform audio</i>

**DAFTAR LAMPIRAN**

Lampiran 1 Source Code Sistem .....	53
-------------------------------------	----

## KATA PENGANTAR

Puji syukur kehadiran Allah subhana wata'ala atas berkat rahmat dan karunia-Nya sehingga tugas akhir yang berjudul "**Analisis Kombinasi Kriptografi dan Steganografi Audio dalam Mengamankan Informasi**" 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. Allah subhana wata'ala, atas berkat rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini;
2. Kedua orang tua penulis, ibu Patima dan bapak Patiroid yang telah banyak memberikan bantuan rohani dan materi, semangat dan do'a serta kepercayaan kepada penulis;
3. Bapak Dr. Eng. Ady Wahyudi Paundu, S.T., M.T. dan Ibu Mukarramah Yusuf, B.Sc., M.Sc. selaku Pembimbing I dan Pembimbing II yang telah banyak memberi keyakinan, perhatian, bimbingan, motivasi, dan masukan yang bermanfaat kepada penulis;
4. Teman – teman SamjaTech dan Synchronous 2018 atas dukungan dan semangat yang telah diberikan selama ini;
5. Teman – teman Mawar atas segala dukungan, semangat dan tempat yang disediakan selama pengerjaan skripsi;
6. M. Emirath Millenium Try dan Maghfirah Tenri Sumpala Zani selaku teman yang telah banyak memberikan bimbingan dan motivasi dalam pengembangan sistem hingga penulisan skripsi ini;
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, 19 Maret 2025

Wira Satya Tri Almi

## BAB I PENDAHULUAN

### 1.1 Latar Belakang

Kemajuan ilmu pengetahuan dan teknologi sangatlah berpengaruh pada aspek kehidupan. Kebutuhan manusia akan alat canggih yang bekerja secara otomatis sangat meningkat. Sehingga alat otomatis mulai menggantikan alat manual, karena selain sistem kerja yang detail, kecepatan, akurasi, dan kuantitas yang dihasilkan sangat baik. Contohnya adalah kemajuan teknologi yang sangat dibutuhkan di bidang pertanian khususnya perkebunan lada (Nurdjannah, 2006). Perkembangan dunia digital saat ini membuat lalu lintas pengiriman data elektronik semakin ramai dan sensitif. Seiring dengan perkembangan tersebut, kejahatan teknologi komunikasi dan informasi juga turut berkembang. Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap penting, komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan, serta penyimpanan data belum tentu aman dari pencurian sehingga keamanan informasi menjadi bagian penting dalam dunia informasi. Seringkali seseorang yang hendak mengirim pesan kepada orang lain, tidak ingin orang yang tidak berwenang mengetahui pesan tersebut. Pesan yang bersifat rahasia yang ditujukan untuk kalangan terbatas. Salah satu upaya untuk mengantisipasi pesan agar tidak sampai kepada orang yang tidak berwenang dapat dilakukan dengan menyembunyikan pesan pada suatu media yang dapat ditelusuri oleh setiap orang. Data yang disembunyikan berupa data teks, gambar, audio, dan video (Rasyid Redha, 2020).

Terdapat teknik yang digunakan untuk mengamankan dan menjaga kerahasiaan data, yaitu kriptografi dan steganografi. Algoritma kriptografi merupakan salah satu metode pengamanan data yang digunakan untuk menjaga kerahasiaan data, keaslian data serta originalitas. Sedangkan, Steganografi adalah menyembunyikan informasi kedalam sebuah media seperti gambar, suara ataupun video. Dengan demikian, dapat disimpulkan bahwa kriptografi fokus pada bagaimana melindungi isi informasi agar tetap aman (*secure*) dan steganografi fokus bagaimana agar isi informasi tersebut tidak terlihat keberadaannya (Laia, 2020). Untuk menangani keamanan pertukaran informasi yang sifatnya rahasia maka dikembangkanlah metode pengamanan data pada audio menggunakan algoritma AES (*Advanced Encryption Standard*) dan Metode *Least Significant Bit* (LSB) merupakan metode steganografi yang bekerja menyisipkan pesan dengan mengganti bit terendah dalam sebuah byte media pembawa pesan. Dalam sebuah byte terdapat susunan bit, yang di dalamnya terdapat bit yang paling berarti (*Most Significant Bit*) dan bit yang paling kurang berarti (LSB). Bit yang sesuai untuk diganti adalah bit LSB, karenanya mengganti nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya (Mulyono., 2018). Berdasarkan hal inilah penulis, mengusulkan judul “**Analisis Kombinasi Kriptografi dan Steganografi Audio dalam Mengamankan Informasi**”.



## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat dirumuskan permasalahan pada penelitian ini yaitu:

- a. Bagaimana cara menyembunyikan sebuah pesan teks yang terenkripsi dalam media cover berkas audio dengan algoritma *Least Significant Bit* (LSB) ?
- b. Bagaimana membangun sistem steganografi audio menggunakan algoritma *Least Significant Bit* (LSB) ?
- c. Bagaimana perbedaan berkas audio sebelum dan sesudah disisipi pesan dengan algoritma *Least Significant Bit* (LSB)?

## 1.3 Tujuan Penelitian

Tujuan akhir yang ingin dicapai dari penelitian ini yaitu:

- a. Menemukan cara menyembunyikan sebuah pesan teks yang terkompresi dalam media cover berkas audio dengan algoritma *Least Significant Bit* (LSB)
- b. Membangun sistem steganografi audio menggunakan algoritma *Least Significant Bit* (LSB).

## 1.4 Manfaat Penelitian

Dengan dilakukannya penelitian ini, diharapkan manfaat yang didapatkan antara lain :

- a. Memberikan pengetahuan terkait cara menyembunyikan sebuah pesan teks yang terkompresi dalam media cover berkas audio dengan menggunakan algoritma *Least Significant Bit* (LSB)
- b. Memberikan pengetahuan terkait cara membangun sistem steganoragrafi audio menggunakan algoritma *Least Significant Bit* (LSB)

## 1.5 Ruang Lingkup/Asumsi perancangan

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut :

- a. Analisis yang akan dilakukan terhadap sistem hanya terkait dengan kualitas audio.
- b. Algoritma yang digunakan *Advanced Encryption Standard* (AES) dan steganografi *Least Significant Bit* (LSB).

## **1.6 Teori**

### **1.6.1 Audio**

Berdasarkan Kamus Besar Bahasa Indonesia edisi ketiga (Tim Penyusun, 2007: 76). Audio merupakan alat peraga yang bersifat dapat didengar (Daryanto 2010: 37). Audio berasal dari kata audible, yang artinya suaranya dapat diperdengarkan secara wajar oleh telinga manusia. Bahan ajar audio merupakan salah satu jenis bahan ajar noncetak yang di dalamnya mengandung suatu sistem yang menggunakan sinyal audio secara langsung, yang dapat dimainkan atau diperdengarkan oleh pendidik kepada peserta didiknya guna membantu mereka dalam menguasai kompetensi tertentu (Andi Prastowo, 2011: 264). Dari uraian tersebut, dapat disimpulkan bahwa media audio adalah salah satu bentuk perantara atau pengantar noncetak yang dapat digunakan untuk menyampaikan pesan dari pendidik kepada peserta didik dengan cara dimainkan atau diperdengarkan secara langsung sehingga peserta didik mampu menguasai kompetensi tertentu dari kegiatan pembelajaran yang dilakukan.

### **1.6.2 WAV**

WAV adalah singkatan dari istilah dalam bahasa Inggris waveform format audio ini adalah format file audio standar yang dikembangkan oleh Microsoft dan IBM, WAV adalah varian dari format bitstream RIFF dan mirip dengan format IFF dan AIFF yang digunakan computer Amiga dan Macintosh, Baik WAV dan AIFF kompatibel dengan sistem operasi Windows dan Macintosh, Meskipun begitu dapat mengakomodasi audio WAV dalam bentuk terkompresi, umumnya format WAV adalah audio yang tidak terkompresi (Lindawati, 2017).

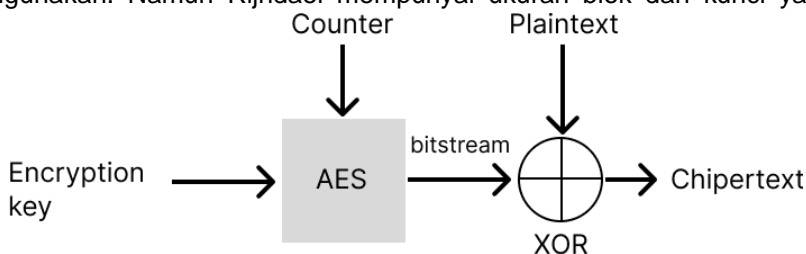
### **1.6.3 Kriptografi**

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkrpsi disebut sebagai plaintext (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah plaintext 16 melibatkan penggunaan suatu bentuk kunci. Pesan plaintext yang telah dienkrpsi (atau dikodekan) dikenal sebagai ciphertext (teks sandi) (Maharani & Agus, 2009) Kriptografi berasal dari kata Bahasa Yunani, yang berarti kryptos dan graphein. Kryptos berarti rahasia atau tersembunyi, sedangkan graphein artinya menulis. Jadi, secara umum kriptografi merupakan proses menulis atau menyampaikan pesan secara rahasia dan tersembunyi.

#### 1.6.4 Algoritma AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) adalah suatu algoritma enkripsi tipe simetrik block cipher yang dijadikan standard FIPS oleh NIST tahun 2001. Pada abad 21 di Amerika secara perlahan algoritme DES digantikan oleh AES. Algoritma AES merupakan algoritma terpopuler pada tipe simetrik yang digunakan saat ini AES merupakan algoritma block cipher dengan sistem permutasi dan substitusi. Ada tiga jenis algoritma AES, yaitu AES-128, AES-192, dan AES-256. Pengelompokan ini berdasarkan panjang kunci yang digunakan pada algoritma 17 AES. Selain itu ada beberapa hal lain yang membedakan antar jenis algoritma AES, yaitu round yang digunakan. AES-128 menggunakan 10 round, AES-192 menggunakan 12 round, dan AES-256 menggunakan 14 round (Visdya et al., 2019). Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya. Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan kunci yang tetap



Gambar 1 Algoritma AES

sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Proses enskripsi adalah kebalikkan dari deskripsi. Berikut penjelasannya :

- a. Key Schedule Proses key schedule diperlukan untuk mendapatkan subkey-subkey dari kunci utama agar cukup untuk melakukan enkripsi dan dekripsi. Proses ini terdiri dari beberapa operasi, yaitu :
  1. Operasi Rotate, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
  2. Operasi SubBytes, pada operasi ini 8 bit dari subkey disubstitusikan dengan nilai dari SBox.
  3. Operasi Rcon, operasi ini dapat diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari user. Operasi ini menggunakan nilai-

nilai dalam Galois field. Nilai nilai dari Rcon kemudian akan di-XOR dengan hasil operasi SubBytes.

4. Operasi XOR dengan  $w[i-Nk]$  yaitu word yang berada pada  $Nk$  sebelumnya.
- b. AddRoundKey Pada proses ini subkey digabungkan dengan state. Proses penggabungan ini menggunakan operasi XOR untuk setiap byte dari subkey dengan byte yang bersangkutan dari state. Untuk setiap tahap, subkey dibangkitkan dari kunci utama dengan menggunakan proses key schedule. Setiap subkey berukuran sama dengan state yang bersangkutan.
- c. SubBytes Rijndael hanya memiliki satu S-box. Kriteria desain untuk kotak S yang dibuat sedemikian rupa sehingga tahan terhadap diferensial linear yang dikenal sebagai pembacaan sandi dan menyerang menggunakan manipulasi aljabar. Koordinat  $x$  merupakan digit pertama sedangkan  $y$  yang kedua dari bilangan hexadecimal.
- d. ShiftRows Proses ShiftRows akan beroperasi pada tiap baris dari tabel state. Proses ini akan bekerja dengan cara memutar byte-byte pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbedabeda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar.
- e. MixColumns Proses MixColumns akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 bytes dari setiap kolom tabel state dan menggunakan transformasi linier Operasi Mix Columns memperlakukan setiap kolom sebagai polinomial 4 suku dalam Galois field dan kemudian dikalikan dengan  $c(x)$  modulo  $(x^4+1)$ , dimana  $c(x)=3x^3+x^2+x+2$ . Kebalikkan dari polinomial ini adalah  $c(x)=11x^3+13x^2+9x+14$ . 7 Operasi MixColumns juga dapat dipandang sebagai perkalian matrix. Sebagai varian dari Square Cipher, Rijndael memiliki kemampuan untuk bekerja sangat baik pada platform apapun. Ditambah dengan operasi yang menggunakan table lookup dan operasi XOR membuat prosesnya menjadi tidak terlalu rumit (Clara & Budi, 2021).

### 1.6.5 Konsep Dasar Kriptografi

Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

- a. Confidentiality (kerahasiaan) yaitu 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.
- b. Data integrity (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, perubahan

atau penambahan) data yang tidak sah (oleh pihak lain).

- c. Authentication (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
- d. Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya) (Martono, 2013).

#### 1.6.4 Steganografi

Steganografi “steganography” adalah ilmu, teknik atau seni menyembunyikan pesan rahasia “hiding message” atau tulisan rahasia “covered writing” sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi berasal dari bahasa Yunani yaitu steganos 19 “tersembunyi/menyembunyikan” dan graphy “tulisan”, sehingga secara lengkap bermakna tulisan yang disembunyikan. Secara umum steganografi merupakan teknik untuk menyisipkan informasi kedalam media yang tidak dapat diduga oleh orang biasa, sehingga tidak menimbulkan suatu kecurigaan kepada orang yang melihatnya (Batarius & Maslim, 2012). Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi steganografi. Hari ini, teknologi jaringan dan komputer menyediakan cara easy-to-use jaringan komunikasi untuk steganografi. Proses penyembunyian informasi di dalam suatu sistem Steganografi dimulai dengan mengidentifikasi suatu sampul media yang mempunyai bit berlebihan (yang dapat dimodifikasi tanpa menghancurkan integritas media). Proses menyembunyikan (embedding) menciptakan suatu proses stego medium dengan cara menggantikan bit yang berlebihan ini dengan data dari pesan yang tersembunyi (Satriya & Prayudi, 2011).

Cara kerja steganografi :

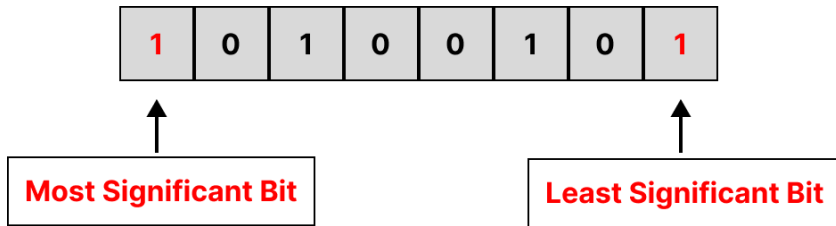
1. Imperceptibility, keberadaan pesan rahasia dalam media penumpang tidak dapat di deteksi.
2. Fidelity, keunggulan media penumpang setelah ditambahkan dengan media penumpang tidak jauh berbeda sebelum ditambahkan pesan rahasia.
3. Recovery, pesan rahasia yang disisipkan dapat di ungkap kembali.
4. Robustness, pesan yang disembunyikan harus tahan terhadap operasi manipulasi yang dilakukan pada media penumpang. Perbedaan antara berkas awal dan berkas akhir dalam steganografi dapat dihitung dengan menghitung nilai MSE dan PSNR. Semakin rendah nilai MSE, maka akan semakin baik dan semakin tinggi nilai PSNR, maka akan semakin baik kualitas hasil steganografi.

### 1.6.5 Least Significant Bit (LSB)

Metode Least Significant Bit (LSB) merupakan metode steganografi yang bekerja menyisipkan pesan dengan mengganti bit terendah dalam sebuah byte media pembawa pesan. Dalam sebuah byte terdapat susunan bit, yang di dalamnya terdapat bit yang paling berarti (Most Significant Bit) dan bit yang paling kurang berarti LSB. Bit yang sesuai untuk diganti adalah bit LSB, karena hanya mengganti nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya (Mulyono et al., 2018). 20 Dalam urutan bit dalam sebuah byte ( 1byte = 8 bit), terdapat Most Significant Bit (MSB) dan Least Significant Bit (LSB). Sebagai contoh , byte dari 01111011, bit nomor 0 (pertama, digaris bawah) adalah bit MSB dan bit nomor 1 (terakhir digaris bawah) adalah bit LSB. Bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Sehingga hanya beberapa bit yang signifikan yang berubah dan secara visual tidak terlihat oleh manusia. Contoh sebelum menambahkan bit adalah:

```
10100001 00101010 10101110 10101110 00100011
00110010 11001011 11001000 10101010 10100011
```

Pesan rahasia (yang telah dikonversi ke sistem biner) misalnya '1010111010', maka setiap bit dari pesan tersebut menggantikan posisi LSB menjadi:



*Gambar 2* MSB dan LSB

```
10100001 00101010 10101110 10101110 00100011
00110011 11001011 11001000 10101011 10100010
```

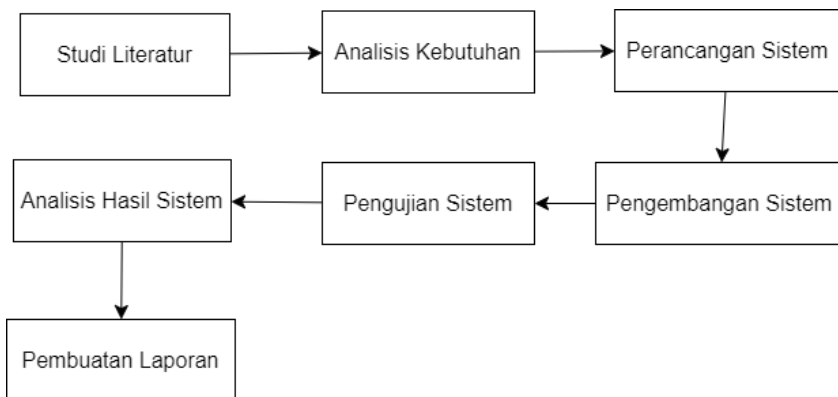
Dalam hal ini, hanya empat bit yang perlu diubah. Rata-rata, hanya setengah dari bit dalam audio yang perlu di modifikasi untuk menyembunyikan pesan rahasia dengan menggunakan ukuran penyamaran maksimum. Perubahan yang dihasilkan yang dilakukan pada bit yang paling tidak signifikan terlalu kecil untuk dikenali oleh mata manusia, sehingga pesan secara efektif disembunyikan (Mulyono et als., 2018).

## BAB II METODE PENELITIAN

### 2.1 Tahapan Penelitian

Penjelasan tahapan tersebut sebagai berikut:

Studi Literatur merupakan tahap awal sebuah penelitian dimana dilakukan pencarian literatur-literatur berkaitan dengan kriptografi, steganografi, serta bagaimana cara mengimplementasikan pada media audio. Analisis Kebutuhan, tahap ini membahas apa saja kebutuhan yang diperlukan selama penelitian ini dilakukan seperti hardware/software. Perancangan Sistem, tahap ini menjelaskan pembuatan rancangan flowchart pada sistem serta Wireframe yang menjadi dasar pembuatannya. Pengembangan sistem, pengembangan dilakukan sesuai dengan studi literatur, analisis kebutuhan, dan perancangan sistem untuk menghasilkan sistem steganografi pada media audio yang dapat menyembunyikan pesan. Pengujian sistem, tahap ini dilakukan pengujian agar dapat memastikan sistem yang dibuat sesuai dengan yang diharapkan. Analisis sistem, file audio yang telah disisipkan pesan akan dianalisis apakah ada perubahan kualitas dengan file audio asal. Pembuatan laporan, setelah menyelesaikan semua tahapan maka akan dilakukan tahapan pembuatan laporan skripsi berdasarkan penelitian yang telah dilakukan. Gambar 3 menunjukkan tahap penelitian yang dilakukan:



Gambar 3 Tahapan Penelitian



## 2.2 Instrumen Penelitian

Instrumen penelitian dimulai dengan menyimpulkan hasil dari studi literatur yang telah dilakukan, dilanjutkan dengan melakukan persiapan untuk pengembangan dimulai dari perangkat keras, perangkat lunak, bahasa pemrograman, serta library yang akan digunakan. Berikut ialah instrument penelitian yang digunakan pada penelitian meliputi:

1. Perangkat Keras
  - Laptop Acer Aspire E5-476G dengan Prosesor Intel i5-8250U (1.60GHz - 1.80 GHz), RAM 12GB, HDD 700GB dan SSD 500GB
2. Perangkat Lunak
  - Sistem operasi Windows 11 Home
  - Visual Studio Code
3. Bahasa Pemrograman
  - Python 3.11.4

## 2.3 Waktu dan Lokasi Penelitian

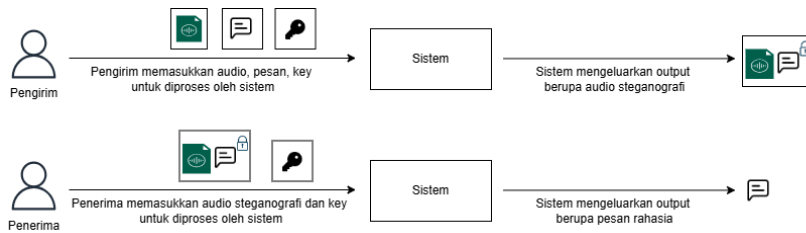
Penelitian ini dilakukan sejak disetujuinya proposal penelitian ini yaitu pada bulan November 2022. Penelitian ini dilakukan di Laboratorium Cloud Computing Departemen Teknik Informatika, Fakultas Teknik Universitas Hasanuddin yang terletak di Bontomarannu, Kabupaten Gowa, Sulawesi Selatan.

## 2.4 Perancangan Sistem

### 2.4.1 Gambaran Umum Sistem

Secara umum, terdapat dua peran dalam pengoperasian sistem ini, yaitu pengirim dan penerima. Pengirim memiliki kemampuan untuk menyembunyikan pesan dalam audio, sementara penerima dapat mengungkapkan pesan tersebut. Sistem yang akan dikembangkan bertujuan membantu pengguna dalam menyembunyikan dan mengungkapkan pesan rahasia dalam media audio, sehingga pengirim dapat mengirimkan pesan melalui saluran publik tanpa diketahui oleh orang lain, kecuali penerima yang dituju dengan persetujuan dari kedua belah pihak. Pada peran pengirim, pengirim harus memasukkan file audio yang akan digunakan sebagai wadah pesan rahasia, memasang kunci untuk menyembunyikan pesan tersebut, pesan rahasia itu sendiri. Sistem akan memproses informasi ini dan menghasilkan output berupa file audio steganografi yang berisi pesan rahasia yang telah disisipkan. Pada peran penerima, langkahnya akan berkebalikan. Penerima perlu memasukkan file audio steganografi yang berisi pesan rahasia dan kunci untuk mengungkapkan pesan tersebut, sesuai dengan kesepakatan antara pengirim dan penerima. Sistem akan memproses informasi ini dan menghasilkan output berupa pesan rahasia yang telah diungkapkan dari

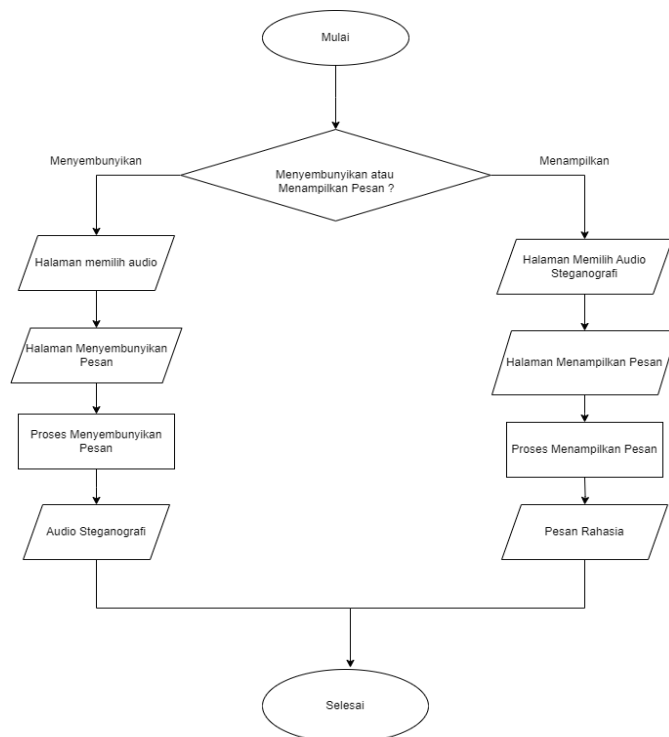
dalam file audio steganografi tersebut. Pada Gambar 4 menunjukkan gambaran umum sistem sebagai berikut:



**Gambar 4** Gambaran Umum Sistem

## 2.4.2 Flowchart

Flowchart sederhana yang mencakup keseluruhan system dapat dilihat pada Gambar 5.



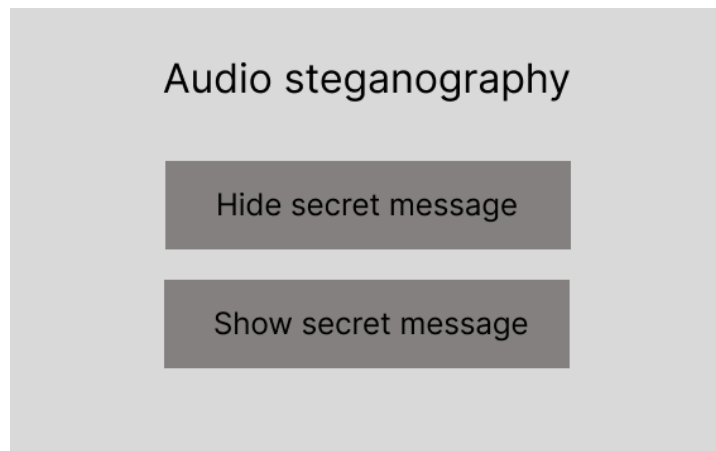
**Gambar 5** Flowchart Sederhana Sistem

Sistem secara umum memiliki dua fungsi utama, yaitu kemampuan untuk menyisipkan pesan rahasia dalam media audio dan kemampuan untuk menampilkan pesan rahasia dari sebuah media audio. Fitur menyisipkan pesan rahasia dalam media audio akan menghasilkan keluaran berupa audio steganografi, sementara fitur menampilkan pesan rahasia dari media audio akan menghasilkan keluaran berupa pesan rahasia dalam bentuk teks.

### **2.4.3 Wireframe**

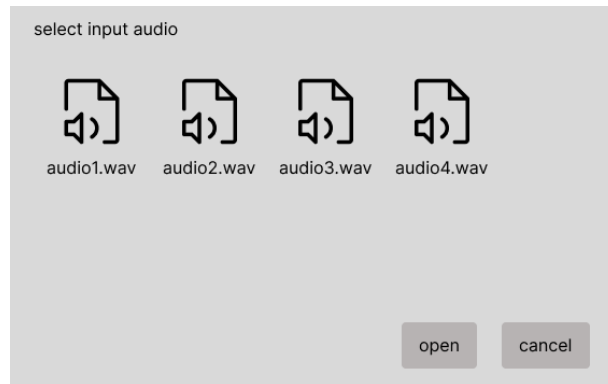
Adapun tahap sebelum mengembangkan sistem, terlebih dahulu dibuat sebuah Wireframe sebagai kerangka yang dapat memberikan gambaran kasar pada setiap halaman sistem.

1. Halaman utama, yaitu halaman yang berisikan button untuk memilih fitur yang akan digunakan. Wireframe halaman utama dapat dilihat pada Gambar 6.



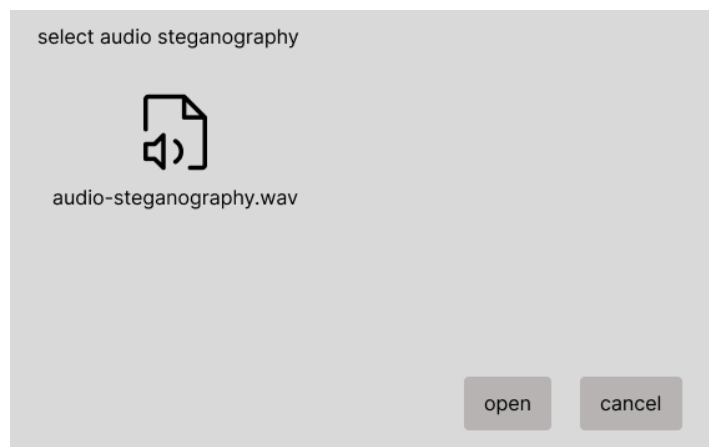
*Gambar 6 Wireframe Halaman Utama*

2. Halaman memilih audio input, yaitu halaman untuk memilih audio yang akan disisipi pesan. Wireframe untuk halaman memilih audio dapat dilihat pada Gambar 7.



*Gambar 7 Wireframe Halaman Memilih Audio*

3. Halaman memilih audio steganografi, yaitu halaman untuk memilih audio yang telah disisip pesan. Wireframe untuk halaman memilih audio steganografi dapat dilihat pada Gambar 8.



*Gambar 8 Wireframe Halaman Memilih Audio*

4. Halaman menyembunyikan pesan rahasia, yaitu halaman yang berisikan informasi audio yang telah diinput dan data-data yang diperlukan untuk menyembunyikan pesan rahasia. Wireframe untuk halaman menyembunyikan pesan rahasia dapat dilihat pada Gambar 9.

**Hide Secret Message**

Audio specification

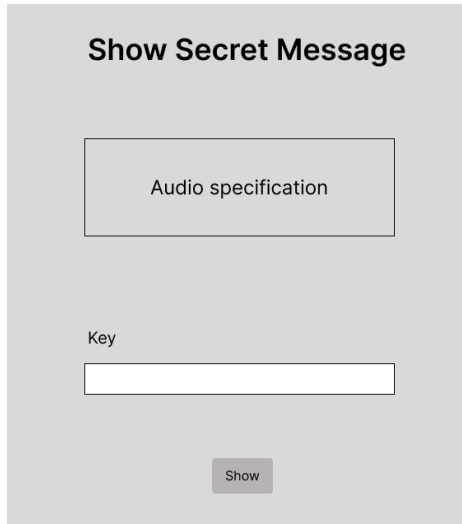
Message

Key

Hide

*Gambar 9 Wireframe Halaman Menyembunyikan*

5. Halaman menampilkan pesan, yaitu halaman yang berisikan informasi audio yang telah diinput dan data-data yang diperlukan untuk menampilkan pesan rahasia. Wireframe untuk halaman menampilkan pesan rahasia dapat dilihat pada Gambar 10.



**Show Secret Message**

Audio specification

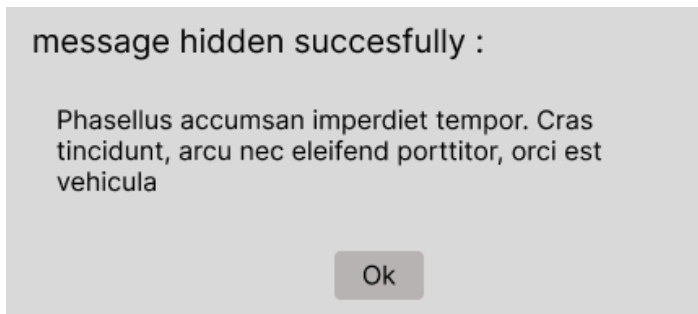
Key

Show

*Gambar 10 Wireframe Halaman Menampilkan Pesan*

Sistem akan menampilkan sebuah pop up ketika fitur berhasil dijalankan, seperti berikut:

1. Berhasil menyembunyikan pesan rahasia ke media audio dan menampilkan informasi bahwa pesan telah berhasil disembunyikan. Wireframe untuk pop up menyembunyikan pesan berhasil, dilihat pada Gambar 11.



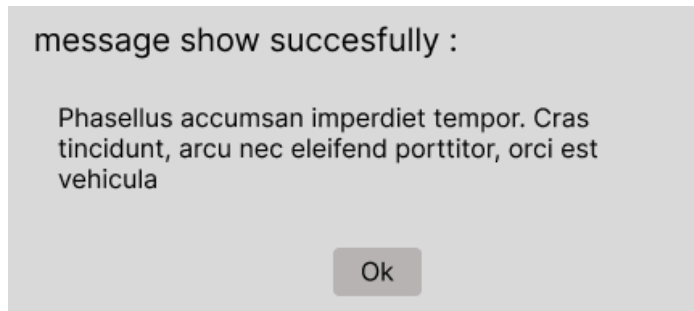
**message hidden succesfully :**

Phasellus accumsan imperdiet tempor. Cras tincidunt, arcu nec eleifend porttitor, orci est vehicula

Ok

*Gambar 11 Wireframe Pop up Menyembunyikan Pesan Berhasil*

2. Berhasil menampilkan pesan rahasia dari media audio akan menampilkan informasi bahwa pesan telah berhasil didapatkan. Wireframe untuk pop up menampilkan pesan dapat dilihat pada Gambar 12.



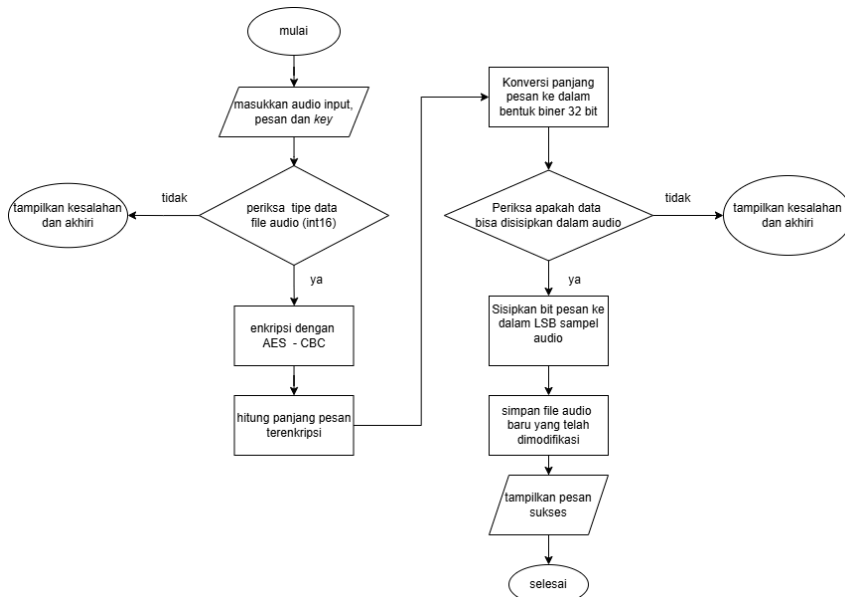
*Gambar 12 Wireframe Pop up Menampilkan Pesan Berhasil*

## 2.5 Pengembangan sistem

Sistem yang dibuat memiliki dua fitur utama yaitu menyembunyikan pesan dan menampilkan pesan.

### 2.5.1 Menyembunyikan Pesan

Alur dalam menyembunyikan pesan terdapat pada Gambar 13.



Gambar 13 Flowchart Menyembunyikan Pesan

Pada fitur penyembunyian pesan dalam audio, pengguna perlu menginput file audio sebagai media cover, pesan teks yang akan disisipkan, serta kunci enkripsi (key). Sistem pertama-tama memeriksa apakah format file audio sesuai, yaitu harus bertipe int16. Jika tidak, sistem akan menampilkan kesalahan dan menghentikan proses. Jika file audio valid, sistem akan melakukan enkripsi pesan menggunakan algoritma AES-CBC dengan kunci yang telah dimasukkan. Sebelum dienkripsi, pesan teks akan dikonversi ke byte dan diberikan padding agar sesuai dengan ukuran blok enkripsi. Setelah dienkripsi, hasil enkripsi akan digabungkan dengan Initialization Vector (IV) sepanjang 16 byte, lalu dikonversi menjadi biner. Selanjutnya, sistem menghitung panjang pesan terenkripsi dan mengonversinya ke biner 32 bit, yang akan disisipkan terlebih dahulu dalam audio sebagai metadata agar dapat dibaca saat proses ekstraksi nanti. Sistem kemudian memeriksa



apakah file audio memiliki kapasitas yang cukup untuk menyimpan pesan yang telah dikonversi ke biner. Jika kapasitas tidak mencukupi, sistem akan menampilkan kesalahan dan menghentikan proses. Jika memadai, sistem melakukan proses penyisipan dengan teknik Least Significant Bit (LSB). Dalam proses ini, setiap bit dari pesan biner yang telah digabungkan akan menggantikan bit paling tidak signifikan (LSB) dari setiap sampel audio. Setelah seluruh bit pesan berhasil disisipkan, sistem menyimpan file audio yang telah dimodifikasi sebagai file baru, lalu menampilkan notifikasi bahwa proses penyisipan berhasil. Hasil akhirnya adalah file audio yang tampak tidak berubah tetapi telah berisi pesan tersembunyi di dalamnya.

### 2.5.2 Pengimputan Data

Tahap pertama dalam penyembunyian pesan adalah menginput data yang akan disisipkan ke dalam file audio. Berikut adalah field yang perlu diinput:

Table 1 Input Data Menyembunyikan Pesan

<b>Nama <i>Field</i></b>	<b>Tipe Data</b>
Audio Input	String
Pesan	String
<i>Key</i>	String

Penjelasan masing-masing field:

- Audio Input, yaitu File audio yang digunakan sebagai media untuk menyimpan pesan rahasia.
- Pesan, yaitu Pesan rahasia dalam bentuk teks yang akan disembunyikan dalam audio. Sebelum disisipkan, pesan akan dienkripsi untuk menjaga kerahasiaannya. Panjang pesan yang dapat disisipkan bergantung pada kapasitas bit paling kurang berpengaruh (LSB) dalam sampel audio.
- Key, yaitu Kunci enkripsi yang digunakan untuk mengamankan pesan dengan algoritma AES. Key ini akan di-hash menggunakan MD5 untuk menghasilkan kunci enkripsi 16-byte yang diperlukan dalam proses enkripsi dan dekripsi.

### 2.5.3 Pemeriksaan Tipe Data Audio

Proses ini memeriksa format file audio yang akan digunakan. File audio harus dalam format WAV dengan tipe data sampel int16 untuk memastikan kompatibilitas dengan algoritma LSB. Jika format tidak sesuai, sistem akan

memberikan notifikasi kesalahan. Tahap ini penting karena LSB steganografi bekerja dengan mengubah bit-bit audio dalam sampel audio dan tipe data int16 memastikan bahwa setiap sampel terdiri dari 16 bit.

#### 2.5.4 Enkripsi dengan AES

Sebelum pesan disisipkan ke dalam audio, pesan akan dienkrpsi menggunakan algoritma AES (Advanced Encryption Standard) dalam mode CBC (Cipher Block Chaining). Langkah-langkah enkripsi adalah sebagai berikut:

1. Konversi Pesan ke Byte: Pesan diubah menjadi bentuk byte menggunakan encoding UTF-8.
2. Hashing Key: Key yang diinput oleh pengguna di-hash menggunakan algoritma MD5 untuk menghasilkan kunci enkripsi 16-byte.
3. Pembuatan IV (Initialization Vector): IV acak sepanjang 16 byte dibuat untuk memastikan bahwa setiap enkripsi memiliki nilai unik.
4. Padding Pesan: Pesan dipadding agar panjangnya menjadi kelipatan 16 byte sesuai dengan persyaratan AES.
5. Enkripsi dengan AES-CBC: Pesan dienkrpsi menggunakan AES dalam mode CBC dengan key hasil hashing dan IV yang dihasilkan.

Setelah pesan berhasil dienkrpsi, hasil enkripsi dikonversi ke dalam bentuk biner. Konversi ini dilakukan dengan mengubah setiap byte dari ciphertext menjadi representasi biner 8-bit. Proses ini memastikan bahwa pesan dapat dengan mudah disisipkan ke dalam sampel audio menggunakan teknik LSB.

#### 2.5.5 Hitung panjang pesan dan konversi ke Biner

Sebelum menyisipkan pesan ke dalam audio, Panjang pesan dihitung agar sistem mengetahui jumlah bit yang akan disisipkan ke dalam audio. Kemudian Panjang pesan ini kemudian dikonversi ke dalam representasi biner 32-bit agar dapat disisipkan di awal audio dan digunakan saat proses ekstraksi untuk menentukan batas pesan yang disisipkan. Setelah panjang pesan dikonversi ke dalam biner, langkah selanjutnya adalah menggabungkan panjang pesan (32-bit) dengan pesan terenkrpsi dalam format biner. Kombinasi ini akan membentuk satu rangkaian biner yang siap untuk disisipkan ke dalam file audio. Struktur data biner yang dihasilkan adalah sebagai berikut:

Bagian Data	Panjang
Panjang Pesan	32-bit
Pesan Terenkripsi	Variabel

Dengan struktur ini, sistem dapat mengenali batas pesan saat proses ekstraksi dan menghindari kesalahan dalam pembacaan data.

### **2.5.6 Penyembunyian Data dengan Algoritma Least Significant Bit**

Proses ini bertujuan untuk menyisipkan bit pesan yang telah dienkripsi ke dalam bit paling kurang berpengaruh dari sampel audio. Langkah-langkahnya adalah sebagai berikut:

1. Membaca File Audio: File audio yang digunakan harus dalam format WAV dengan tipe data sampel int16.
2. Mengekstrak Data Sampel: Data sampel audio diambil dalam bentuk array numerik yang berisi amplitudo suara.
3. Menyisipkan Panjang Pesan: 32 bit pertama dari pesan disisipkan untuk menyimpan informasi panjang pesan terenkripsi.
4. Menyisipkan Pesan Terenkripsi: Pesan yang telah dikonversi ke biner disisipkan ke dalam LSB dari setiap sampel audio.
5. Penyimpanan File Audio Baru: Setelah penyisipan selesai, file audio yang telah dimodifikasi disimpan dengan pesan yang tersembunyi di dalamnya.

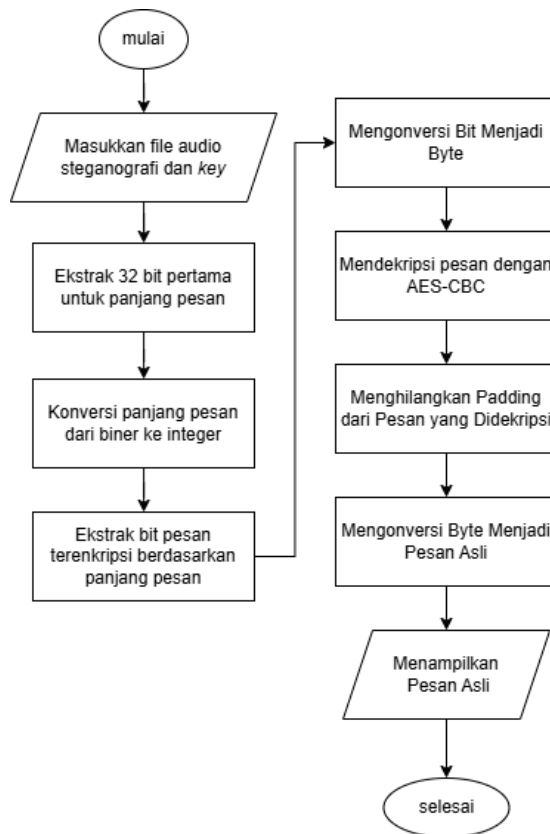
Contoh perubahan bit dalam proses LSB:

- Sampel Audio Sebelum: 10010 (biner)
- Bit Rahasia: 1
- Sampel Audio Sesudah: 10011

Setelah proses ini selesai, file audio tetap dapat diputar seperti biasa, tetapi telah mengandung pesan rahasia yang tersembunyi di dalamnya.

## 2.6 Menampilkan Pesan

Alur dalam menampilkan pesan rahasia dapat kita lihat pada Gambar 14.



Gambar 14 Flowchart Menampilkan pesan

Pada tahap menampilkan pesan, pengguna menginput file audio steganografi yang telah disisipkan pesan rahasia serta *key* yang digunakan dalam proses enkripsi. Proses ini dimulai dengan membaca file audio steganografi, lalu mengekstrak Least Significant Bit (LSB) dari 32 sampel audio pertama. 32 bit ini berisi informasi panjang pesan terenkripsi yang tersembunyi dalam file audio. Setelah 32 bit ini diekstraksi, data tersebut dikonversi dari biner ke desimal untuk menentukan panjang pesan dalam satuan byte. Informasi panjang pesan ini digunakan untuk menentukan jumlah bit yang harus diekstraksi dari LSB sampel audio berikutnya. Selanjutnya, bit-bit pesan tersembunyi diekstraksi dari LSB sampel audio sesuai dengan panjang yang telah ditentukan. Setelah semua bit pesan berhasil dikumpulkan, data tersebut dikonversi menjadi byte untuk mendapatkan pesan terenkripsi. Pesan terenkripsi ini kemudian didekripsi menggunakan

algoritma AES-CBC dengan key yang sama seperti saat penyisipan pesan. Proses dekripsi mencakup penghapusan padding agar format pesan kembali sesuai. Terakhir, setelah pesan berhasil didekripsi, data dalam bentuk byte dikonversi kembali menjadi teks asli yang dapat dibaca oleh pengguna, lalu ditampilkan sebagai hasil akhir dari proses ekstraksi.

### 2.6.1 pengimputan data

Pada alur menampilkan pesan, hal pertama yang akan dilakukan ialah pengimputan data, adapun data yang akan diinput dapat dilihat pada tabel 2.

Table 2 Input Data Menampilkan Pesan

<b>Nama field</b>	<b>Type data</b>
Audio steganografi	String
Key	String

#### a. Audio Steganografi

Merupakan file audio yang telah disisipkan pesan rahasia menggunakan metode steganografi LSB. File ini berisi data suara dalam bentuk array numerik yang merepresentasikan nilai amplitudo setiap sampel audio. Sistem akan membaca dan mengekstrak bit tersembunyi dari file ini untuk mendapatkan pesan terenkripsi.

#### b. Key (Kunci Enkripsi)

Sebuah teks yang digunakan untuk mendekripsi pesan yang telah dienkripsi menggunakan algoritma AES-CBC pada proses penyisipan. Kunci ini harus sesuai dengan kunci yang digunakan saat enkripsi agar pesan dapat diuraikan dengan benar. Key yang diinput akan di-hash menggunakan algoritma MD5 untuk menghasilkan kunci 16-byte yang sesuai dengan kebutuhan dekripsi AES.

### 2.6.2 Ekstraksi Least Significant Bit (LSB) dari Sampel Audio

Setelah data diinput, langkah selanjutnya adalah mengekstrak bit tersembunyi dari Least Significant Bit (LSB) di setiap sampel audio. LSB merupakan bit dengan pengaruh terkecil dalam representasi biner suatu nilai amplitudo suara. Proses ekstraksi dilakukan dengan mengambil LSB dari setiap sampel audio. Khusus untuk 32 sampel pertama, LSB yang diekstraksi digunakan untuk mendapatkan panjang pesan terenkripsi yang tersembunyi dalam file audio. Informasi panjang pesan ini sangat penting karena menentukan jumlah byte yang harus diekstraksi untuk memperoleh pesan asli.



## 2.7 Pengujian Sistem

Pengujian sistem menggunakan metode *Black Box Testing* dengan beberapa skenario, dapat dilihat pada tabel 3.

Table 3 Skenario *Black Box Testing*

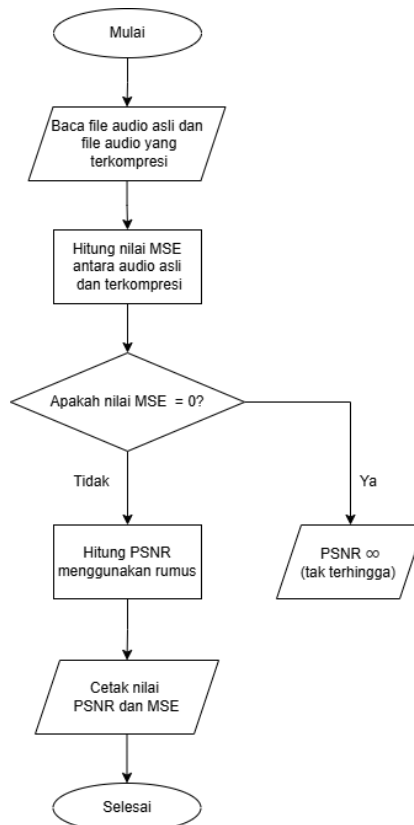
No	Aksi	Hasil yang diharapkan
<b>1. Halaman Utama</b>		
1.1	Menekan tombol "Hide Secret Message"	Halaman "memilih audio input" terbuka
1.2	Menekan tombol "Show Secret Message"	Halaman "memilih audio steganografi" terbuka
<b>2. Halaman Memilih Audio Input</b>		
2.1	Memilih audio lalu menekan tombol "Open"	Halaman "menyembunyikan pesan rahasia"
2.2	Memilih tombol "Cancel"	Halaman memilih audio tertutup
<b>1. Halaman Memilih Audio Steganografi</b>		
3.1	Memilih audio lalu menekan tombol "Open"	Halaman "menyembunyikan pesan rahasia"
3.2	Memilih tombol "Cancel"	Halaman memilih audio tertutup
<b>2. Halaman Menyembunyikan Pesan Rahasia</b>		
4.1	Menekan tombol "Hide" tanpa mengisi field "Browse wav file"	Muncul error dengan pesan semua harus terisi
4.2	Menekan tombol "Hide" tanpa mengisi field "Message"	Muncul error dengan pesan semua harus terisi
4.3	Menekan tombol "Hide" tanpa mengisi field "Key"	Muncul error dengan pesan semua harus terisi

4.4	Menekan tombol "Hide" dengan semua field terisi	Muncul informasi penyembunyian berhasil beserta pesan yang berhasil disembunyikan
<b>3. Halaman Menampilkan Pesan Rahasia</b>		
5.1	Menekan tombol "Show" tanpa mengisi field "Key"	Muncul error dengan pesan semua field harus terisi
5.2	Menekan tombol "Show" dengan semua field terisi	Muncul informasi pesan berhasil didapatkan beserta pesannya
5.3	Menekan tombol "Show" namun key yang dimasukkan salah	Muncul error dengan pesan invalid



### 3.8 Analisis Hasil Sistem

Karena sistem steganografi audio yang dibangun dengan format file audio WAV yang tidak terkompresi, maka dari itu audio hasil dari steganografi akan dianalisis dengan cara membandingkan kualitas audio antara file audio asli (*sebelum disisipi pesan*) dan file audio hasil steganografi (*setelah disisipi pesan*). Untuk mengetahui apakah ada perubahan yang signifikan dalam kualitas audio setelah proses penyisipan, maka akan dilakukan analisis objektif audio hasil dari sistem ini (*audio steganografi*) dengan menggunakan parameter *Peak Signal to Noise Ratio* (PSNR). PSNR sendiri adalah metrik yang digunakan dalam pengukur kualitas perubahan file audio asli dan file audio hasil steganografi. Flowchart sistem pada PSNR dapat dilihat pada Gambar 15.



Gambar 15 Flowchart PSNR

Penelitian ini dimulai dengan membaca file audio asli dan file audio terkompresi. Setelah file audio terbaca maka akan dilanjutkan dengan proses perhitungan nilai MSE antara audio asli dan terkompresi. Nilai MSE sebagai nilai rata – rata perbedaan antara kedua sinyal, dimana nilai MSE yang rendah menunjukkan kemiripan tinggi antara sinyal audio asli dan terkompresi. Jika nilai MSE sama dengan nol, maka kedua sinyal akan dianggap identik dan PSNR akan dianggap sebagai tak terhingga. Namun, jika MSE tidak sama dengan nol, maka prosesnya akan berlanjut dengan PSNR dihitung menggunakan rumus yang ditetapkan. Selanjutnya sistem akan menampilkan nilai PSNR dan MSE.

Adapun langkah awal dalam menghitung PSNR yaitu dengan mencari nilai dari *Mean Squared Error* MSE antara file audio asli dan file audio steganografi dengan rumus:

$$MSE = \frac{1}{N} \sum_{i=1}^N (x[i] - y[i])^2 \dots\dots\dots(1)$$

Keterangan:

N = jumlah sampel audio.

$x[i]$  = nilai sampel dari sinyal audio asli pada indeks ke-i.

$y[i]$  = nilai sampel dari sinyal audio yang diproses pada indeks ke-i.

Setelah nilai MSE diperoleh, maka nilai PSNR dapat dihitung dengan rumus sebagai berikut:

$$PSNR = 10 \times \log_{10} \left( \frac{MAX^2}{MSE} \right) \dots\dots\dots(2)$$

Keterangan:

$MAX_I$  = Nilai maksimal dari sampel audio, yaitu 32767 (Gunarto et al., 2018) untuk data audio dengan format int16.

MSE = Nilai *Mean Squared Error* yang telah dihitung sebelumnya.

Analisis dengan parameter PSNR dilakukan untuk membandingkan kualitas audio. Semakin tinggi nilai PSNR, semakin sedikit perubahan yang terjadi pada kualitas audio asli. Selain analisis objektif, dilakukan juga analisis subjektif dengan parameter kemampuan pendengaran manusia untuk mengetahui apakah ada perbedaan signifikan antara audio asli dan audio setelah disisipkan pesan.

Adapun contoh pemakaian rumus sebagai berikut. Terdapat sinyal audio dengan 3 sampel sebagai berikut:

- **Sinyal audio asli:**  $x = [10000, 15000, 20000]$
- **Sinyal audio modifikasi:**  $y = [10010, 14990, 20020]$

**Hitung Nilai MSE:**

- $(10000 - 10010)^2 = 100$
- $(12000 - 11990)^2 = 100$
- $(20000 - 20020)^2 = 400$
- $MSE = \frac{100+100+400}{3} = 200$

**Nilai Maksimum (MAX):**

- Untuk sinyal audio 16-bit, MAX = 32767

**Hitung Nilai PSNR:**

- $PSNR = 10 \times \log_{10} \left( \frac{32767^2}{200} \right)$
- $PSNR = 10 \times \log_{10} \left( \frac{1073676289}{200} \right)$
- $PSNR = 10 \times \log_{10} (5368381.445)$
- $PSNR = 10 \times 6.7305 \text{ dB}$
- $PSNR = 67.305 \text{ dB}$

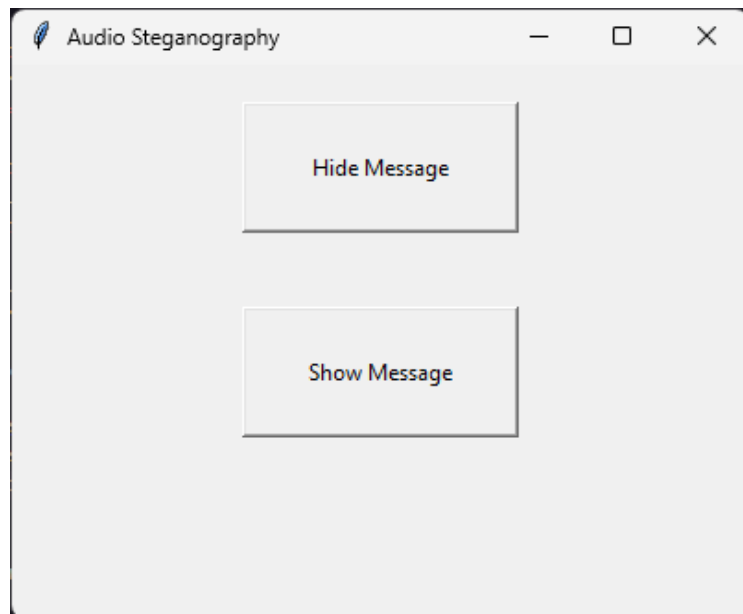
## BAB III

### HASIL DAN PEMBAHASAN

#### 3.1 Hasil Pengembangan Sistem

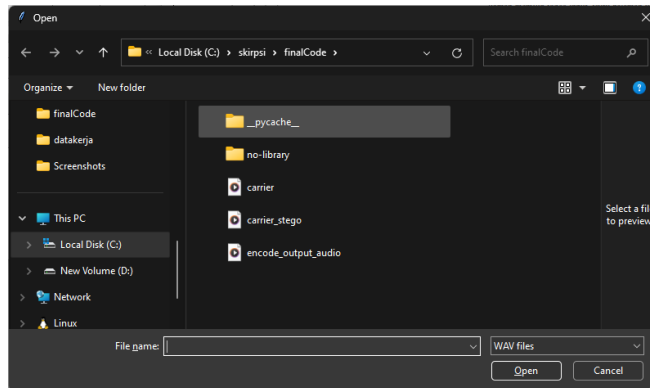
Berikut adalah hasil dari pengembangan system berdasarkan perancangan system:

1. Halaman utama, menampilkan sebuah *button* untuk memilih fitur apa yang akan dijalankan. Tangkapan layar untuk halaman utama terdapat pada Gambar 16.



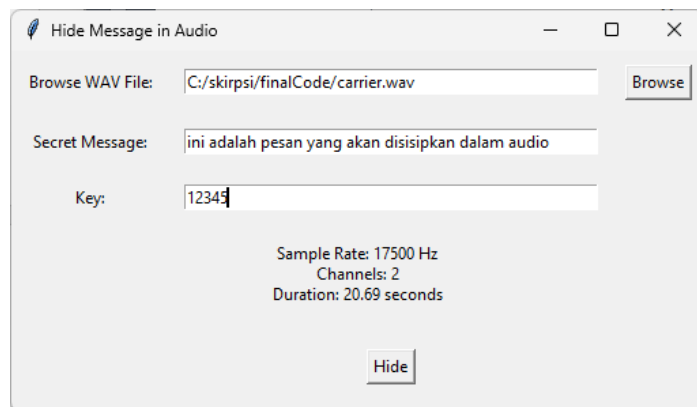
Gambar 16. Tangkapan Layar Halaman Utama

2. Halaman memilih audio input, yaitu halaman memilih audio yang akan disisipi sebuah pesan. Tangkapan layar untuk halaman memilih audio dapat dilihat pada Gambar 17.



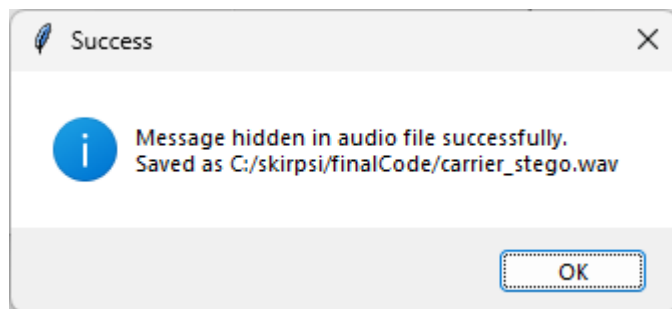
*Gambar 17. Tangkapan Layar Halaman Memilih Audio Input*

3. Halaman menyembunyikan pesan rahasia, yaitu halaman yang berisi informasi audio yang telah diinput dan data-data yang akan diinput masuk ke dalam audio. Tangkapan layar untuk halaman menyembunyikan pesan rahasia dapat dilihat pada Gambar 18.



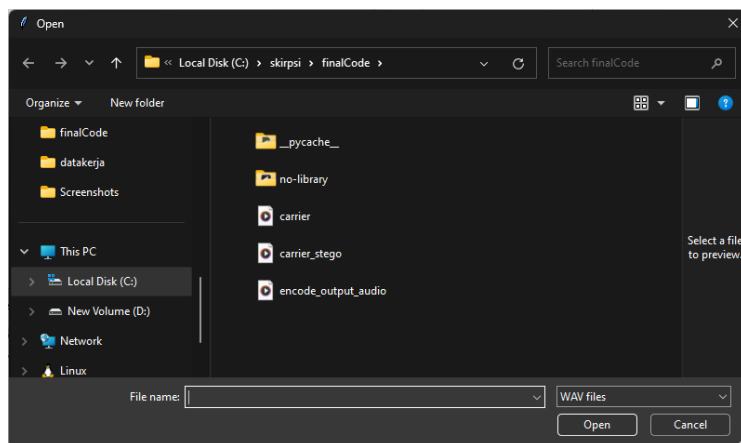
*Gambar 18. Tangkapan Layar Halaman Menyembunyikan Pesan Rahasia*

4. Berhasil menyembunyikan pesan rahasia ke media audio akan menampilkan sebuah *pop up* menyembunyikan pesan berhasil dapat dilihat pada Gambar 19.



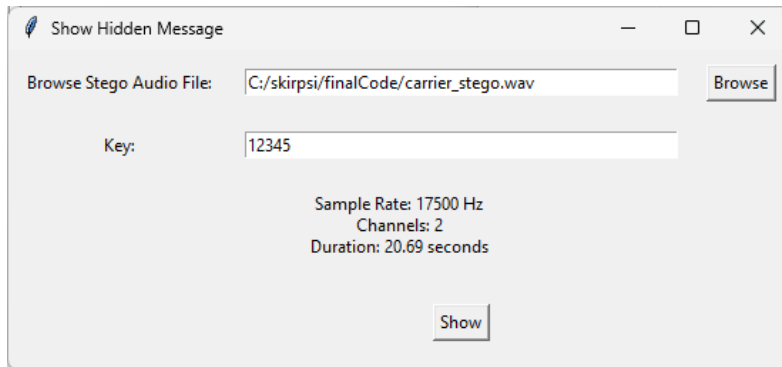
*Gambar 19. Tangkapan Layar Pop up Pesan Rahasia Berhasil Disembunyikan*

5. Halaman memilih audio steganografi, yaitu halaman untuk memilih audio yang telah disisipi pesan. Tangkapan layar untuk halaman memilih audio steganografi dapat dilihat pada Gambar 20.



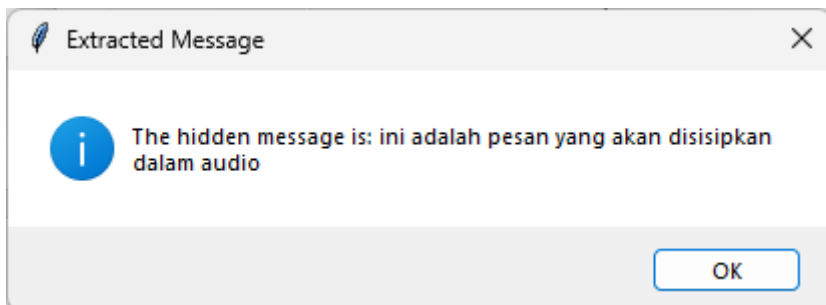
*Gambar 20. Tangkapan Layar Halaman Memilih Audio Steganografi*

6. Halaman menampilkan pesan rahasia, yaitu halaman yang berisi informasi audio yang telah diinput dan data-data yang diperlukan untuk menampilkan pesan rahasia. Tangkapan layar untuk halaman menampilkan pesan rahasia dapat dilihat pada Gambar 21.



*Gambar 21. Tangkapan Layar Halaman Menampilkan Pesan Rahasia*

7. Berhasil menampilkan pesan rahasia dari media audio akan menampilkan informasi pesan yang telah didapatkan. Tangkapan layar untuk *pop up* pesan yang berhasil dapat dilihat pada Gambar 22.



*Gambar 22. Tangkapan Layar Pop up Pesan Rahasia Berhasil Didapatkan*

### 3.2 Hasil Pengujian Sistem

Berdasarkan *Black Box Testing* yang telah dilakukan, hasilnya dapat dilihat pada tabel 4.

Table 4. *Black Box Testing*

No.	Aksi	Hasil yang diharapkan	Hasil yang sebenarnya
	<b>1. Halaman utama</b>		
1.1	Menekan tombol " <i>Hide Secret Message</i> "	Halaman "memilih audio input" terbuka	Seperti yang diharapkan
1.2	Menekan tombol " <i>Show Secret Message</i> "	Halaman "memilih audio steganografi" terbuka	Seperti yang diharapkan
	<b>1. Halaman Memilih Audio Input</b>		
2.1	Memilih audio lalu menekan tombol " <i>Open</i> "	Halaman "menyembunyikan pesan rahasia"	Seperti yang diharapkan
2.2	Memilih tombol " <i>Cancel</i> "	Halaman memilih audio tertutup	Seperti yang diharapkan
	<b>2. Halaman Memilih Audio Steganografi</b>		
3.1	Memilih audio lalu menekan tombol " <i>Open</i> "	Halaman "menyembunyikan pesan rahasia"	Seperti yang diharapkan
3.2	Memilih tombol " <i>Cancel</i> "	Halaman memilih audio tertutup	Seperti yang diharapkan
	<b>3. Halaman Menyembunyikan Pesan Rahasia</b>		
4.1	Menekan tombol " <i>Hide</i> " tanpa mengisi <i>field</i> " <i>Browse wav file</i> "	Muncul error dengan pesan semua harus terisi	Seperti yang diharapkan
4.2	Menekan tombol " <i>Hide</i> " tanpa mengisi <i>field</i> " <i>Message</i> "	Muncul error dengan pesan semua harus terisi	Seperti yang diharapkan
4.3	Menekan tombol " <i>Hide</i> " tanpa mengisi <i>field</i> " <i>Key</i> "	Muncul error dengan pesan semua harus terisi	Seperti yang diharapkan



4.4	Menekan tombol “ <i>Hide</i> ” dengan semua <i>field</i> terisi	Muncul informasi penyembunyian berhasil beserta pesan yang berhasil disembunyikan	Seperti yang diharapkan
<b>4. Halaman Menampilkan Pesan Rahasia</b>			
5.1	Menekan tombol “ <i>Show</i> ” tanpa mengisi <i>field</i> “ <i>Key</i> ”	Muncul <i>error</i> dengan pesan semua <i>field</i> harus terisi	Seperti yang diharapkan
5.2	Menekan tombol “ <i>Show</i> ” dengan semua <i>field</i> terisi	Muncul informasi pesan berhasil didapatkan beserta pesannya	Seperti yang diharapkan
5.3	Menekan tombol “ <i>Show</i> ” namun <i>key</i> yang dimasukkan salah	Muncul <i>error</i> dengan pesan <i>invalid</i>	Seperti yang diharapkan

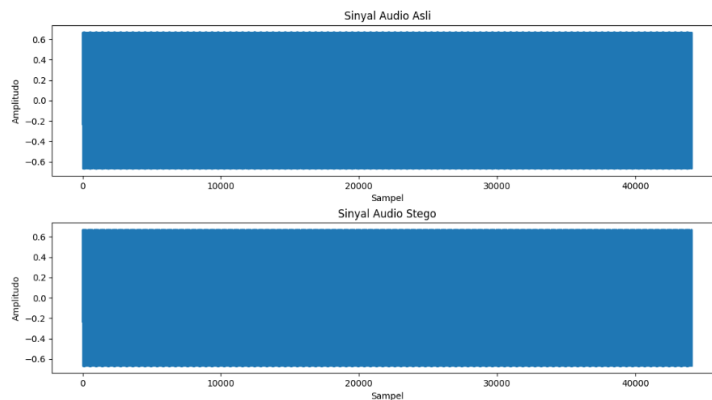
### 3.3 Hasil Analisis Hasil Sistem

Berdasarkan data hasil uji steganografi, ditemukan bahwa file .wav yang dijadikan sebagai objek file yang disisipkan tidak mengalami perubahan kualitas suara yang signifikan. Maka hal ini tentunya membuat teks yang berada dalam file audio berformat wav tetap aman, karena tidak akan menimbulkan kecurigaan dari suara audio .wav steganografi. Oleh karena itu, kerahasiaan file yang telah disisipi yang akan dikirim ke penerima tidak akan bocor. Hasil pengujian dengan 3 sampel audio dapat dilihat pada tabel 5.

Table 5. Hasil Nilai Peak Signal to Noise Ratio

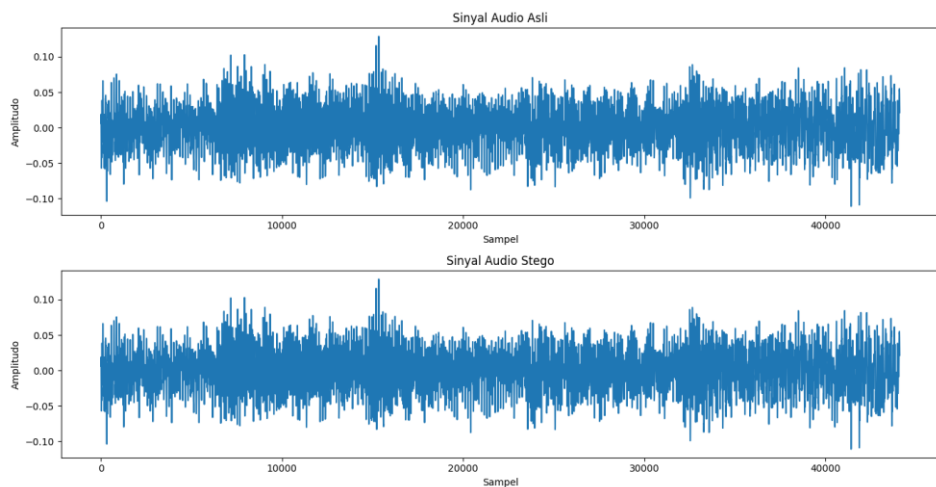
No.	Nama File	Durasi	Jumlah Kata	Ukuran Data		PSNR (dB)
				Awal	Stego	
1.	audio1.wav	30 detik	1000	5.05 MB/ (5,299,278) bytes	5.05 MB / (5,299,244) bytes	107.2067984 0443478 dB
2.	audio2.wav	60 detik	1000	10.1 MB/(10,593,870 bytes)	10.1MB (10,593,836 bytes)	110.3173478 6999581 dB
3.	audio3.wav	90 detik	1000	15.1 MB (15,884,366 bytes)	15.1 MB (15,884,332 bytes)	112.0542226 1075567 dB

Penampakan sinyal audio1 sebelum dan sesudah penyisipan pesan (steganografi audio) dapat dilihat pada Gambar 23. Sinyal pertama merupakan sinyal audio asli sebelum adanya penyisipan data, sedangkan sinyal kedua menunjukkan sinyal audio steganografi yang sudah disisipi pesan rahasia.



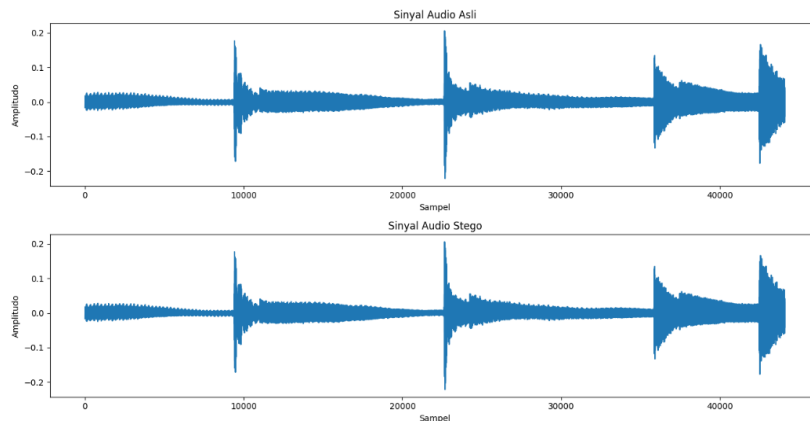
*Gambar 23. (a) sinyal audio asli (sebelum disisipkan pesan)  
dan (b) sinyal audio sesudah disisipkan pesan*

Penampakan dari sinyal audio2 sebelum dan sesudah penyisipan pesan (audio steganografi) dapat dilihat pada Gambar 24. Gambar ini menampilkan perbandingan antara sinyal audio asli dan audio steganografi setelah penyisipan.



*Gambar 24. (a) sinyal audio asli sebelum disisipkan pesan dan (b) sinyal audio sesudah disisipkan pesan*

Penampakan dari sinyal audio sebelum dan sesudah penyisipan pesan (steganografi audio) pada audio3 ditampilkan pada Gambar 25. Gambar ini memberikan perbandingan antara sinyal audio asli dan audio stego setelah proses penyisipan pesan.



*Gambar 25. (a) sinyal audio asli sebelum disisipkan pesan dan (b) sinyal audio sesudah disisipkan pesan*

Perubahan yang dilakukan pada Least Significant Bit (LSB) tidak menyebabkan perubahan signifikan pada frekuensi utama maupun amplitudo sinyal audio. Oleh karena itu, karakteristik keseluruhan audio tetap hampir sama dengan sinyal aslinya. Namun, karena perubahan ini dilakukan pada tingkat yang sangat halus, pendengar yang sangat sensitif mungkin dapat mendeteksi sedikit perubahan berupa noise atau distorsi yang sangat minimal. Hal ini menegaskan bahwa teknik steganografi audio menggunakan algoritma LSB sangat efektif dalam menyembunyikan pesan tanpa menyebabkan penurunan kualitas audio yang signifikan, baik secara visual melalui analisis amplitudo maupun secara auditori melalui pendengaran.

## **BAB IV KESIMPULAN DAN SARAN**

### **4.1 Kesimpulan**

Berdasarkan hasil penelitian dalam implementasi steganografi menggunakan metode least significant bit untuk menyembunyikan pesan tersembunyi sebagai file audio berformat wav, dapat diambil kesimpulan berdasarkan uraian – uraian pada bab – bab sebelumnya. Kesimpulan dari hasil penelitian ini sebagai berikut.

1. Sistem steganografi audio berbasis Least Significant Bit (LSB) menyembunyikan pesan teks terenkripsi dengan cara mengonversi teks terenkripsi menjadi biner, lalu menyisipkan bit – bit tersebut ke dalam bit paling tidak signifikan (LSB) dari sampel audio tanpa menyebabkan perubahan kualitas suara.
2. Sistem steganografi ini dibangun dalam bentuk aplikasi berbasis dekstop dengan algoritma LSB untuk menyisipkan dan mengekstrak pesan. Aplikasi ini memproses file audio sesuai dengan metode yang dijelaskan pada nomor 1.
3. Hasil analisis menggunakan parameter Peak Signal to Noise Ratio (PSNR) menunjukkan bahwa kualitas audio sebelum dan sesudah penyisipan pesan tetap baik. Nilai PSNR yang diperoleh berada dalam rentang yang menunjukkan bahwa perubahan pada LSB tidak secara signifikan memengaruhi kualitas audio. Selain itu, hasil spektrogram menunjukkan bahwa perbedaan antara audio asli dan audio yang telah disisipkan pesan sangat sulit dideteksi secara visual.

### **4.2 Saran**

Saran untuk penelitian yang akan datang dari penulis diharapkan:

1. Sistem dapat dikembangkan pada platform web atau mobile.
2. Dapat dilakukan penelitian hal serupa menggunakan algoritma yang berbeda seperti F5, parity coding.
3. Pertimbangkan untuk memperluas dukungan sistem untuk format audio lainnya selain WAV, seperti MP3 atau FLAC, sehingga sistem dapat lebih fleksibel dan berguna bagi berbagai kebutuhan pengguna.

## DAFTAR PUSTAKA

- Batarius, P., & Maslim, M. (2012). PERBANDINGAN METODE DALAM TEKNIK STEGANOGRAFI. In Seminar Nasional Teknologi Informasi & Komunikasi Terapan..
- Clara, L., & Budi, A. (2021). IMPLEMENTASI METODE ALGORITMA AES PADA PERLINDUNGAN DATA SISTEM LOGIN.
- Gunarto, P., Abdullah, A., & Irawan, D. (2018). 9 Gunarto, dkk; Model Matematis Turbin Pelton Dengan Menggunakan Bahasa. Jurnal Teknik Mesin, 4(2).
- Laia, R. (2020). Implementasi Algoritma Aes 256 Bit Dan Lsb Untuk Pengamanan Dan Penyisipan Pesan Teks Pada File Audio. In Jurnal Pelita Informatika (Vol. 8, Issue 4).
- Lindawati, S. R. (2017). *Steganography Implementation on Android Smartphone Using the LSB* (Least Significant Bit) to MP3 and WAV Audio. IEEE.
- Maharani, S., & Agus, F. (2009). Implementasi Perangkat Lunak Penyandian Pesan Menggunakan Algoritma RSA. In Jurnal Informatika Mulawarman (Vol. 4, Issue 1).
- Martono, I. (2013). Penggunaan Steganografi dengan Metode End of File (EOF) pada Digital Watermarking.
- Mulyono, I. U. W., Susanto, A., Anggraeny, T., & Sari, C. A. (2018a). Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit). Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 63–74. <https://doi.org/10.22219/kinetik.v4i1.701>
- Susanto, A., Anggraeny, T., & Sari, C. A. (2018b). Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit). Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 63–74. <https://doi.org/10.22219/kinetik.v4i1.701>

- Rasyid Redha, M. (2020). IMPLEMENTASI LEAST SIGNIFICANT BIT (LSB) DAN ALGORITMA VIGENERE CIPHER PADA AUDIO STEGANOGRAFI. *Jurnal Sains Dan Teknologi*, Vol. 20. 52
- Satriya, E., & Prayudi, W. Y. (2011). KONSEP HIDDEN MESSAGE DENGAN MENGGUNAKAN TEKNIK STEGANOGRAFI DYNAMIC CELL SPREADING. In *Media Informatika* (Vol. 9, Issue 9).
- Visdya, R., Chandra, H., Kusyanti, A., & Data, M. (2019). Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File (Vol. 3, Issue 1). <http://j-ptiik.ub.ac.id>


## LAMPIRAN

:

*Lampiran 1* Source Code Sistem

Source code penelitian tersedia untuk public pada tautan berikut:

<https://github.com/historia11/Steganografi-LSB.git>

 historia11	file code	f31ca42 · 4 minutes ago	 1 Commit
 Audio	file code	4 minutes ago	
 image	file code	4 minutes ago	
 finaCode.py	file code	4 minutes ago	
 psnr2.py	file code	4 minutes ago	