SKRIPSI

ANALISIS KOMBINASI KRIPTOGRAFI DAN STEGANOGRAFI AUDIO DALAM MENGAMANKAN INFORMASI

Disusun dan diajukan oleh:

WIRA SATYA TRI ALMI

D121181324

Logo

Description automatically generated with low confidence

PROGRAM STUDI SARJANA TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS HASANUDDIN

GOWA

2024

LEMBAR PENGESAHAN SKRIPSI

**JUDUL SKRIPSI DENGAN HURUF KAPITAL TIMES NEW ROMAN 14 BOLD SPASI SINGLE**

Disusun dan diajukan oleh

Logo

Description automatically generated with low confidence

**Nama Mahasiswa**

**NIM**

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka Penyelesaian Studi Program Sarjana Program Studi …………………

Fakultas Teknik Universitas Hasanuddin

Pada tanggal …………………

dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui,

|  |  |
| --- | --- |
| Pembimbing Utama,  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  NIP xxxxxxxxxxxxx | Pembimbing Pendamping,  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  NIP xxxxxxxxxxxxx |

Ketua Program Studi,

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NIP xxxxxxxxxxxxx

PERNYATAAN KEASLIAN

Yang bertanda tangan dibawah ini ;

Nama : Wira satya tri almi

NIM : D121181324

Program Studi : Teknik Informatika

Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul

{Judul Skripsi}

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

Semua informasi yang ditulis dalam skripsi yang berasal dari penulis lain telah diberi penghargaan, yakni dengan mengutip sumber dan tahun penerbitannya. Oleh karena itu semua tulisan dalam skripsi ini sepenuhnya menjadi tanggung jawab penulis. Apabila ada pihak manapun yang merasa ada kesamaan judul dan atau hasil temuan dalam skripsi ini, maka penulis siap untuk diklarifikasi dan mempertanggungjawabkan segala resiko.

Segala data dan informasi yang diperoleh selama proses pembuatan skripsi, yang akan dipublikasi oleh Penulis di masa depan harus mendapat persetujuan dari Dosen Pembimbing.

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

Gowa, tanggal bulan tahun

Yang Menyatakan

Materai

Nama Mahasiswa

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

[LEMBAR PENGESAHAN SKRIPSI i](#_Toc172717950)

[PERNYATAAN KEASLIAN ii](#_Toc172717951)

[ABSTRAK iii](#_Toc172717952)

[ABSTRACT iv](#_Toc172717953)

[DAFTAR ISI v](#_Toc172717954)

[DAFTAR GAMBAR vii](#_Toc172717955)

[DAFTAR TABEl viii](#_Toc172717956)

[DAFTAR SINGKATAN DAN ARTI SIMBOL ix](#_Toc172717957)

[DAFTAR LAMPIRAN x](#_Toc172717958)

[KATA PENGANTAR xi](#_Toc172717959)

[BAB 1 PENDAHULUAN 12](#_Toc172717960)

[1.1 Latar Belakang 12](#_Toc172717961)

[1.2 Rumusan Masalah 13](#_Toc172717962)

[1.3 Tujuan Penelitian/Perancangan 13](#_Toc172717963)

[1.4 Manfaat Penelitian/Perancangan 13](#_Toc172717964)

[1.5 Ruang Lingkup/Asumsi perancangan 13](#_Toc172717965)

[BAB 2 TINJAUAN PUSTAKA 14](#_Toc172717966)

[2.1 Audio 14](#_Toc172717967)

[2.2 Kriptografi 14](#_Toc172717968)

[2.2.1 Pengertian Kriptografi 14](#_Toc172717969)

[2.2.2 Konsep Dasar Kriptografi 15](#_Toc172717970)

[2.3 Algoritma AES (*Advanced Encryption Standard*) 15](#_Toc172717971)

[2.4 Stegnografi 17](#_Toc172717972)

[2.5 *Least Significant Bit* (LSB) 18](#_Toc172717973)

[BAB 3 METODE PENELITIAN/PERANCANGAN 20](#_Toc172717974)

[3.1 Tahapan Penelitian 20](#_Toc172717975)

[3.2 Gambaran Umum Sistem 21](#_Toc172717976)

[3.3 Instrument Penelitian 21](#_Toc172717977)

[3.4 Waktu dan Lokasi Penelitian 22](#_Toc172717978)

[3.5 Perancangan Sistem 22](#_Toc172717979)

[3.5.1 Flowchart Sistem 22](#_Toc172717980)

[3.5.2 *Wireframe* Sistem 24](#_Toc172717981)

[3.6 Pengembangan Sistem 28](#_Toc172717982)

[3.6.1 Menyembunyikan Pesan 28](#_Toc172717983)

[3.6.1.1 Pengimputan Data 29](#_Toc172717984)

[3.6.1.2 Enkripsi dengan AES 30](#_Toc172717985)

[3.6.1.3 Penyembunyian Data dengan Algoritma *Least Significant Bit* 30](#_Toc172717986)

[3.6.2 Menampilkan Pesan 31](#_Toc172717987)

[3.7 Pengujian Sistem 32](#_Toc172717988)

[3.8 Analisis Hasil Sistem 33](#_Toc172717989)

[BAB 4. HASIL DAN PEMBAHASAN 36](#_Toc172717990)

[4.1 Hasil Pengembangan Sistem 36](#_Toc172717991)

[4.2 Hasil Pengujian Sistem 40](#_Toc172717992)

[4.3 Hasil Analisis Hasil Sistem 42](#_Toc172717993)

[BAB 5. KESIMPULAN DAN SARAN 43](#_Toc172717994)

[5.1 Kesimpulan 43](#_Toc172717995)

[5.2 Saran 43](#_Toc172717996)

[DAFTAR PUSTAKA 44](#_Toc172717997)

DAFTAR GAMBAR

[Gambar 1. Algoritma AES 17](#_Toc174626300)

[Gambar 2. MSB dan LSB 20](#_Toc174626301)

[Gambar 3. Tahap Penelitian 21](#_Toc174626302)

[Gambar 4. Gambaran Umum Sistem 22](#_Toc174626303)

[Gambar 5. Flowchart Sederhana Sistem 24](#_Toc174626304)

[Gambar 6. *Wireframe* Halaman Utama 25](#_Toc174626305)

[Gambar 7. *Wireframe* Halaman Memilih Audio 25](#_Toc174626306)

[Gambar 8. *Wireframe* Halaman Memilih Audio Steganografi 26](#_Toc174626307)

[Gambar 9. *Wireframe* Halaman Menyembunyikan Pesan Rahasia 26](#_Toc174626308)

[Gambar 10. *Wireframe* Halaman Menampilkan Pesan Rahasia 27](#_Toc174626309)

[Gambar 11. *Wireframe* Pop up Menyembunyikan Pesan Berhasil 28](#_Toc174626310)

[Gambar 12. *Wireframe* Pop up Menampilkan Pesan Berhasil 28](#_Toc174626311)

[Gambar 13. Flowchart Menyembunyikan Pesan 29](#_Toc174626312)

[Gambar 14. Flowchart menampilkan pesan 32](#_Toc174626313)

[Gambar 15. Tangkapan Layar Halaman Utama 37](#_Toc174626314)

[Gambar 16. Tangkapan Layar Halaman Memilih Audio Input 38](#_Toc174626315)

[Gambar 17. Tangkapan Layar Halaman Menyembunyikan Pesan Rahasia 38](#_Toc174626316)

[Gambar 18. Tangkapan Layar Pop up Pesan Rahasia Berhasil Disembunyikan 39](#_Toc174626317)

[Gambar 19. Tangkapan Layar Halaman Memilih Audio Steganografi 39](#_Toc174626318)

[Gambar 20. Tangkapan Layar Halaman Menampilkan Pesan Rahasia 40](#_Toc174626319)

[Gambar 21. Tangkapan Layar *Pop up* Pesan Rahasia Berhasil Didapatkan 40](#_Toc174626320)

[Gambar 22. (a) spektogram audio1 sebelum disisipkan pesan dan (b) spektogram audio1 sesudah disisipkan pesan 43](#_Toc174626321)

[Gambar 23 (a) spektogram audio2 sebelum disisipkan pesan dan (b) spektogram audio2 sesudah disisipkan pesan 44](#_Toc174626322)

DAFTAR TABEl

[Tabel 1. Input Data Menyembunyikan Pesan 30](#_Toc172855757)

[Tabel 2. Skenario *Black Box Testing* 33](#_Toc172855758)

[Tabel 3. Sampel Audio 36](#_Toc172855759)

[Tabel 4. Black Box Testing 41](#_Toc172855760)

[Tabel 5. Hasil Nilai Peak Signal to Noise Ratio 43](#_Toc172855761)

DAFTAR SINGKATAN DAN ARTI SIMBOL

|  |  |
| --- | --- |
| Lambang/Singkatan | Arti dan Keterangan |
| AES  FIPS  *I*1[*i*]  *I2*[*i*]  IV  MSB  MSE  N  NIST  PSNR | *Advanced Encryption Standard*  *Federal Information Processing Standards* Nilai sampel ke-i dari file audio asli  Nilai sampel ke-i dari file audio hasil steganografi  *Initial Vector*  Nilai maksimal dari sampel audio, yaitu 32767 untuk data audio dengan format int16  *Most Significant Bit*  Nilai *Mean Squared Error*  Jumlah sampel audio  National Institute of Standards and Technology  *Peak Signal to Noise Ratio* |

DAFTAR LAMPIRAN

[Lampiran 1 Contoh lembar pengesahan untuk seminar proposal dan hasil 14](#_Toc124100022)

[Lampiran 2 Contoh kuesioner 15](#_Toc124100023)

KATA PENGANTAR

Puji syukur kehadirat 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 Patiroi yang telah banyak memberikan bantuan rohani dan meterial, 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 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. Teman – teman Synchronous 2018 atas dukungan ,bantuan serta semangatnya selama ini;
7. M. Emirat Millenium Try dan Maghfirah Tenri Sumpala Zani selaku teman yang telah banyak memberikan bimbingan dan motivasi dalam pengembangan sistem hingga penulisan skripsi ini;
8. Diri sendiri atas pencapaian, kerja keras, serta semangat pantang menyerah dalam menyelesaikan skripsi dan studi;
9. 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, July 2024

Penulis

BAB 1  
PENDAHULUAN

1.1 Latar Belakang

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, karenahanya mengganti nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya (Mulyono., 2018).

1.2 Rumusan Masalah

1. Bagaimana cara menyembunyikan sebuah pesan teks yang terkompresi dalam media cover berkas audio dengan algoritma *Least Significant Bit* (LSB) ?
2. Bagaimana membangun sistem steganografi audio menggunakan algoritma *Least Significant Bit* (LSB) ?

1.3 Tujuan Penelitian/Perancangan

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

1.4 Manfaat Penelitian/Perancangan

Memberikan pengetahuan terkait cara menyembunyikan sebuah pesan teks yang terkompresi dalam media cover berkas audio dengan menggunakan algoritma *Least Significant Bit* (LSB)

Memberikan pengetahuan terkait cara membangun sistem steganoragrafi audio menggunakan algoritma *Least Significant Bit* (LSB)

1.5 Ruang Lingkup/Asumsi perancangan

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

BAB 2  
TINJAUAN PUSTAKA

2.1 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. Kriptografi
     1. Pengertian 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 dienkripsi 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 melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (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. Konsep Dasar Kriptografi

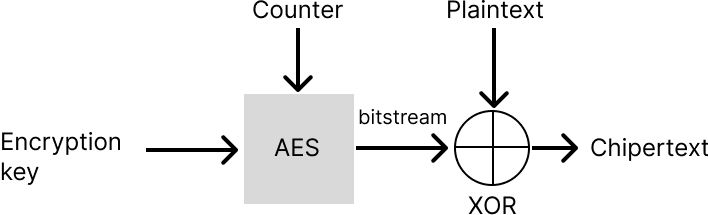
Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Confidelity* (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.
2. Data *integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
3. *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
4. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya)(Martono dkk, 2013).

2.3 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 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.



Gambar 1. Algoritma AES

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

1. *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 :

a. *Operasi Rotate*, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.

b. Operasi *SubBytes*, pada operasi ini 8 bit dari *subkey* disubstitusikan dengan nilai dari SBox.

c. 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.

d. Operasi XOR dengan *w[i-Nk]* yaitu word yang berada pada *Nk* sebelumnya.

2. *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.

3. 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.

4. 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.

5. MixColums 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 (x4+1), dimana c(x)=3x3+x2+x+2. Kebalikkan dari polinomial ini adalah c(x)=11x3+13x2+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, n.d.).

2.4 Stegnografi

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* “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 (P. Batarius and M. 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. *Fildelity*, keunggulan media penumpang setalah ditambahkan dengan media penumpang tidak jauh berbeda sebelum ditambahkan pesan rahasia.

3. *Recovery*, pesan rahasia yang disispkan 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 ahkir dalam steganografi dapat dihutung dengan menghitung nilai MSE dan PSNR.

Semakin rendah nilai MSE, maka akan semakin baik dan semakin tinggi nilai PSNR, maka akan semakin baik kualiatas hasil steganografi.

* 1. *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).

Dalam urutan bit dalam sebuat byte ( 1byte = 8 bit), Gambar 2, terdapat *Most Significant Bit* (MSB)dan *Least Significant Bit* (LSB). Sebagai contoh , byte dari 01111011, bit nomor 0 (pertama, digaris bawahi) adalah bit MSB dan bit nomor 1 (terakhir digasir bawahi) 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:

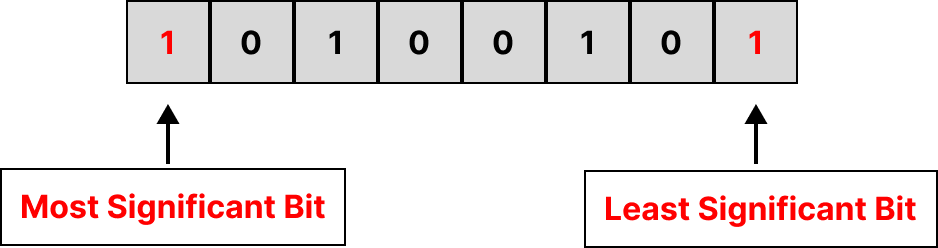
10100001 00101010 10101110 10101110 00100011

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 (digaris bawahi):

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).

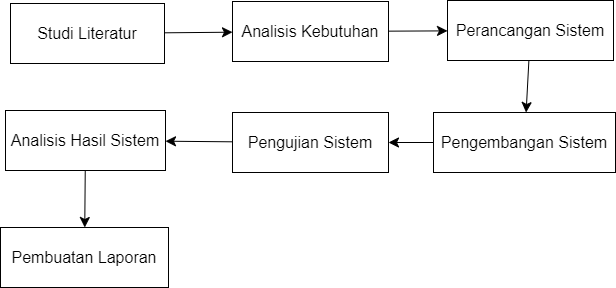
Gambar 2. MSB dan LSB

BAB 3  
METODE PENELITIAN/PERANCANGAN

3.1 Tahapan Penelitian

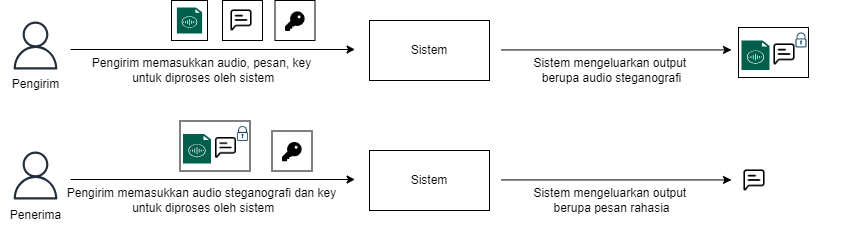
Penjelasan tahapan tersebut sebagai berikut:

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 dilakukantahapan pembuatan laporan skripsi berdasarkan penelitian yang telah dilakukan. Gambar 3 menunjukkan tahap penelitian yang dilakukan:



Gambar 3. Tahap Penelitian

3.2 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

* 1. Instrument Penelitian

Instrument 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

1. Perangkat Lunak

* Sistem operasi Windows 11 Home
* Visual Studio Code

1. Bahasa Pemrograman

* Python 3.11.4
  1. Waktu dan Lokasi Penelitian

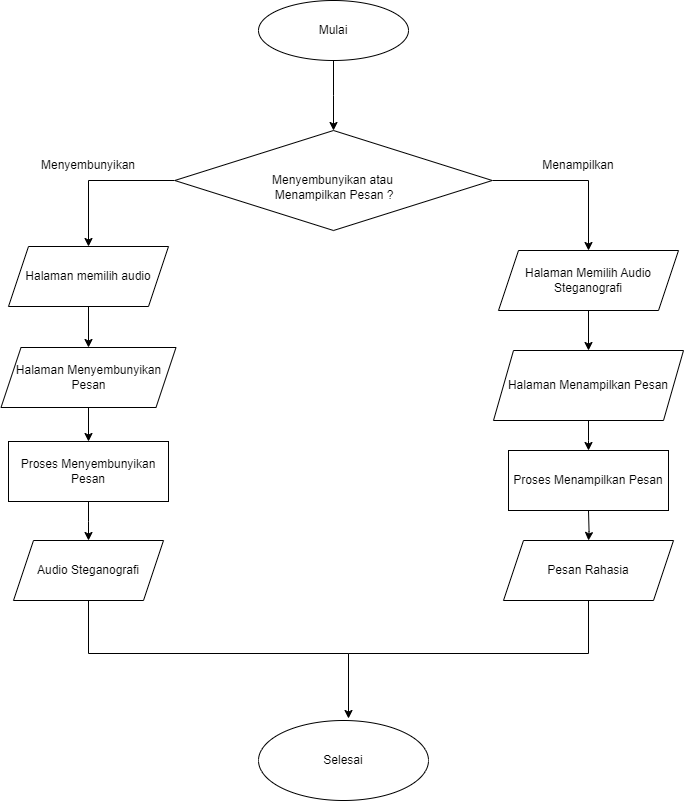
Penelitian ini dilakukan sejak disetujuinya proposal penelitian ini yaitu pada bulan November 2022. Penelitian ini dilakukan di Laboratorium *Cloud Computing* Departemen Teknik Informatika, Fakultas Teknik Universitas Hasanuddin yang terletak di Bontomarannu, Kabupaten Gowa, Sulawesi Selatan.

* 1. Perancangan Sistem

Sebelum sistem dikembangkankan, terlebih dahulu dibuat rancangan yang akan menjadi dasar dalam proses pengembangan sistem.

3.5.1 Flowchart Sistem

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

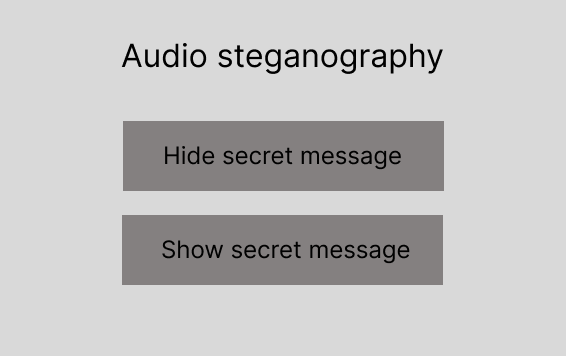


Gambar 5. Flowchart Sederhana Sistem

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.

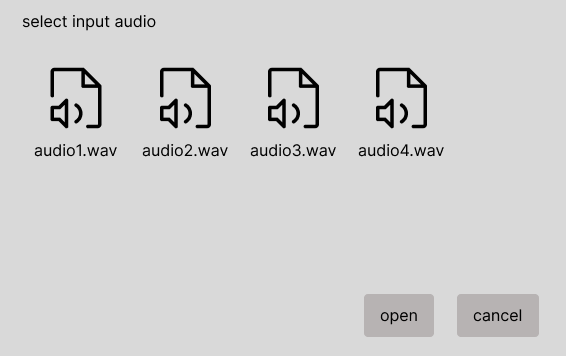
3.5.2 *Wireframe* Sistem

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

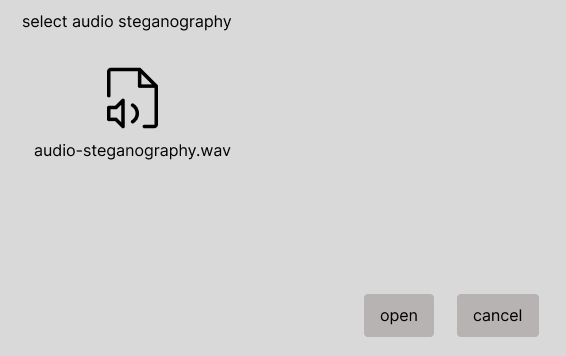
1. Halaman utama, yaitu halaman yang berisikan button untuk memili fitur yang akan digunakan. *Wireframe* halaman utama dapat dilihat pada Gambar 6.

Gambar 6. *Wireframe* Halaman Utama

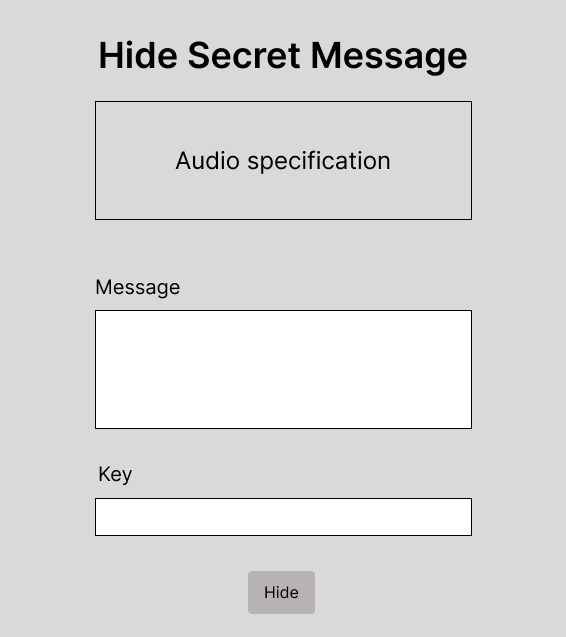
1. Halaman memilih audio input, yaitu halaman untuk memilih audio yang akan disisipi pesan. *Wireframe* untuk halaman memilih audio dapat dilihat pada Gambar 7.



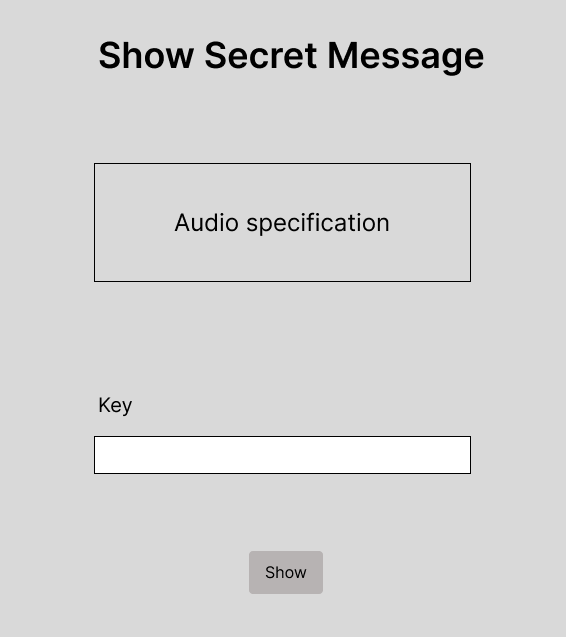
Gambar 7. *Wireframe* Halaman Memilih Audio

1. 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 Steganografi

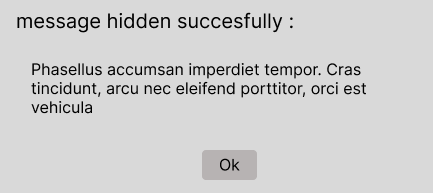
1. Halaman menyembunyikan pesan rahasia, yaitu halaman yang berisikan informasi audio yang telah diinput dan data-data yang diperlukan untuk menyembunyikan pesan rahasia. *Wireframe* untuk alaman menyembunyikan pesan rahasia dapat dilihat pada Gambar 9.

Gambar 9. *Wireframe* Halaman Menyembunyikan Pesan Rahasia

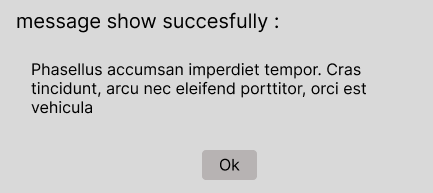
1. Halaman menampilkan pesan, yaitu halaman yang berisikan informasi audio yang telah diinput dan data-data yang diperlukan untuk menampilkan pesan rahasia. *Wireframe* untuk halaman menampilkan pesan rahasia dapat dilihat pada Gambar 10.

Gambar 10. *Wireframe* Halaman Menampilkan Pesan Rahasia

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

1. Berhasil menyembunyikan pesan rahasia ke media audio dan menampilakan informasi bahwa pesan telan berhasil disembnyikan. *Wireframe* untuk *pop up* menyembunyikan pesan berhasil, dilihat pada Gambar 11.

Gambar 11. *Wireframe* Pop up Menyembunyikan Pesan Berhasil

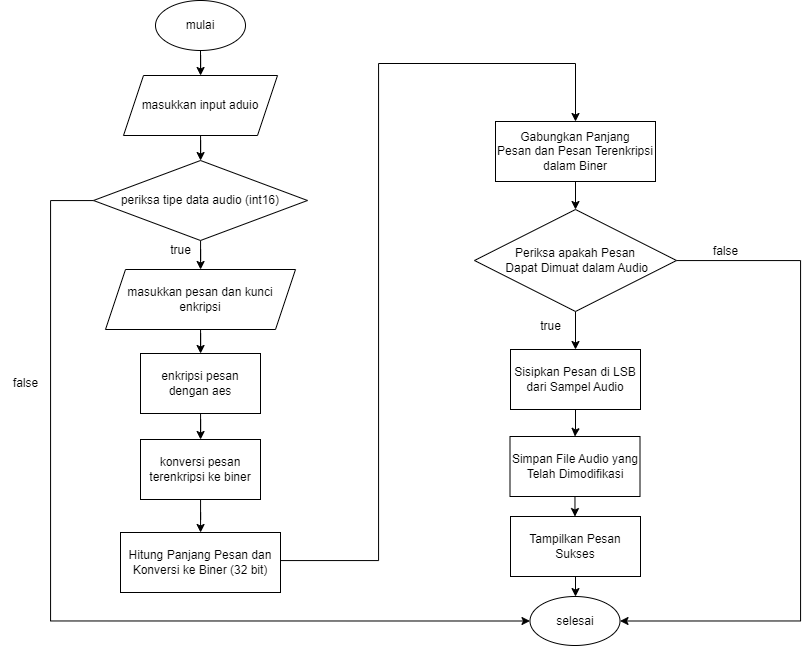
1. Berhasil menampilkan pesan rahasia dari media audio akan menampilkan informasi bahwa pesan telah berhasil didapatkan. *Wireframe* untuk *pop up* menampilkan pesan dapat dilihat pada Gambar 12.

Gambar 12. *Wireframe* Pop up Menampilkan Pesan Berhasil

* 1. Pengembangan Sistem

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

3.6.1 Menyembunyikan Pesan

 Alur dalam menyembunyikan pesan terdapat pada gambar 13 sebagai berikut.

Gambar 13. Flowchart Menyembunyikan Pesan

Pada fitur menyembunyikan pesan dalam audio, pengguna perlu menginput file audio yang akan disisipi pesan, pesan yang ingin disembunyikan, dan *key*. Sistem kemudian memeriksa apakah tipe data file audio tersebut sesuai (harus int16). Pesan yang diinput akan dienkripsi menggunakan kunci yang telah diinput dengan algoritma AES dalam mode CBC, setelah pesan dikonversi menjadi byte dan ditambahkan padding. Hasil enkripsi digabungkan dengan IV *(Initialization Vector)* sepanjang 16 *byte* dan dikonversi menjadi biner, bersama dengan panjang pesan yang dikonversi ke biner 32 bit.

Sistem memastikan bahwa pesan dapat dimuat dalam file audio. Jika tidak, proses akan dihentikan. Jika ya, sistem melakukan *looping* pada setiap bit dari pesan biner yang telah digabungkan, mensubstitusi bit paling kurang berpengaruh (LSB) dari setiap sampel audio dengan bit pesan tersebut. Setelah proses substitusi selesai, file audio yang telah dimodifikasi disimpan sebagai file baru, dan sistem menampilkan pesan bahwa proses penyisipan pesan telah berhasil atau lebih tepatnya output yang dikeluarkan itu audio input.

* + - 1. Pengimputan Data

Pada fitur penyembunyian pesan, tahap pertama yaitu dengan menginput data, Adapun *field* yang akan diinput dilihat pada table 1.

Tabel 1. Input Data Menyembunyikan Pesan

|  |  |
| --- | --- |
| **Nama *Field*** | **Tipe Data** |
| Audio Input | String |
| Pesan | String |
| *Key* | String |

1. Audio Input, yaitu video yang dijadikan media untuk menampung sebuah pesan rahasia.
2. Pesan, yaitu pesan rahasia dalam bentuk teks yang akan disembunyikan dalam file audio. Pesan ini akan dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sebelum disisipkan ke dalam audio. Panjang pesan yang dapat disembunyikan bergantung pada kapasitas bit paling kurang berpengaruh (LSB) dari sampel audio.
3. *Key,* yaitu teks yang digunakan untuk mengenkripsi pesan rahasia menggunakan algoritma AES. *Key* ini di-hash menggunakan MD5 untuk menghasilkan kunci enkripsi yang digunakan dalam proses enkripsi. *Key* yang sama diperlukan untuk dekripsi pesan saat diambil kembali dari audio.
   * + 1. Enkripsi dengan AES

Proses enkripsi dalam sistem penyembunyian pesan pada audio melibatkan beberapa langkah utama. Pertama, pesan yang diinput dikonversi menjadi byte menggunakan encoding UTF-8. Selanjutnya, kunci enkripsi dihasilkan dengan meng-hash *key* yang diinput menggunakan algoritma MD5 untuk menghasilkan kunci enkripsi 16-byte. Setelah itu, sistem menghasilkan IV (*Initialization Vector*) acak sepanjang 16 byte untuk digunakan dalam mode operasi CBC pada AES, memastikan bahwa setiap enkripsi unik. Pesan kemudian dipadding agar panjangnya menjadi kelipatan 16 byte sebelum dienkripsi menggunakan AES-CBC dengan kunci hasil *hashing* dan IV yang dihasilkan. Hasil enkripsi ini digabungkan dengan IV dan dikonversi ke dalam bentuk biner. Panjang pesan terenkripsi juga dikonversi ke biner 32-bit dan digabungkan dengan pesan terenkripsi biner. Sistem kemudian memastikan bahwa panjang pesan biner tidak melebihi kapasitas LSB dari sampel audio, sebelum melakukan looping pada setiap sampel audio dan menyisipkan bit pesan terenkripsi ke dalam LSB dari setiap sampel audio. Setelah semua bit pesan disisipkan, file audio yang telah dimodifikasi disimpan sebagai file baru yang mengandung pesan rahasia.

* + - 1. Penyembunyian Data dengan Algoritma *Least Significant Bit*

Dalam tahap ini penyisipan pesan rahasia ke dalam bit paling kurang berpengaruh (LSB) dari sampel audio. Pada proses ini dilakukan setelah pesan rahasia telah dienkripsi dan dikonversi ke dalam bentuk biner. Adapun beberapa langkah dalam proses ini sebagai berikut. Langkah pertama dalam proses penyembunyian pesan adalah membaca file audio yang akan digunakan. File audio harus dalam bentuk format wav dan tipe data sampelnya harus *int16.* 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. Setelah file audio diperiksa, maka Langkah selanjutnya yaitu menyisipkan pesan ke dalam LSB dari sampel audio. Pesan yang disisipkan terdiri dari panjang pesan terenkripsi (32 bit) dan pesan terenkripsinya dalam bentuk biner. Proses penyisipan pesan dilakukan dengan mengganti bit paling kurang berpengaruh (bit paling kanan) dari setiap sampel audio dengan bit-bit dari pesan biner.

Misalkan kita memiliki sampel audio dengan nilai int16 sebagai berikut:

* Sampel Audio: 10010 (biner)
* Pesan Rahasia Bit: 1

Proses LSB steganografi akan menggantikan bit paling kurang berpengaruh (bit paling kanan) dari sampel audio dengan bit pesan rahasia:

* Sampel Audio (sebelum): 10010
* Bit Rahasia: 1
* Sampel Audio (sesudah): 10011
  + 1. Menampilkan Pesan

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

Gambar 14. Flowchart menampilkan pesan

Pada tahap menampilkan pesan, user menginput file audio yang telah disisipi pesan (audio steganografi), dan *key* yang dipakai dalam menyamarkan pesan.

Proses ini dimulai dengan membaca file audio steganografi yang mengembalikan laju sampel dan array sampel audio. Bit paling kurang berpengaruh (*Least Significant Bit* atau LSB) dari 32 sampel audio pertama diekstraksi untuk mendapatkan panjang pesan terenkripsi, yang diambil dari 32 bit pertama yang disimpan dalam file audio. Panjang pesan dalam format biner dikonversi ke desimal untuk mengetahui berapa banyak byte yang harus diekstrak dari audio. Setelah panjang pesan diketahui, bit-bit berikutnya sesuai dengan panjang pesan diekstraksi dari LSB sampel audio. Kemudian bit-bit pesan yang telah diekstraksi kemudian dikonversi kembali menjadi byte untuk mendapatkan pesan terenkripsi. Pesan terenkripsi didekripsi menggunakan kunci yang sama seperti saat penyembunyian, dan pesan asli diperoleh dengan menghilangkan padding dan mengubah byte kembali ke string.

* 1. Pengujian Sistem

Pengujian sistem menggunakan metode *Black Box Testing* dengan beberapa skenario, dapat dilihat pada Tabel 2.

Tabel 2. Skenario *Black Box Testing*

|  |  |  |
| --- | --- | --- |
| **No** | **Aksi** | **Hasil yang diharapkan** |
|  | * 1. **Halaman Utama** | |
| 1.1 | Menekan tombol*“ Hide Secret Message*” | Halaman “memilih audio input” terbika |
| 1.2 | Menekan tombol ”*Show Secret Message”* | Halaman “memilih audio steganografi” terbuka |
| * 1. **Halaman Memilih Audio Input** | | |
| 2.1 | Memilih audio lalu menekan tombol “Open” | Halaman “menyembunyikan pesan rahasia” |
| 2.2 | Memilih tombol “Cancel” | Halaman memilih audio tertutup |
| 1. **Halaman Memilih Audio Steganografi** | | |
| 3.1 | Memilih audio lalu menekan tombol “Open” | Halaman “menyembunyikan pesan rahasia” |
| 3.2 | Memilih tombol “Cancel” | Halaman memilih audio tertutup |
| 1. **Halaman Menyembunyikan Pesan Rahasia** | | |
| 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 |
| 1. **Halaman Menampilkan Pesan Rahasia** | | |
| 5.1 | Menekan tombol “*Show”* tanpa mengisi *field* “K*ey”* | 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* |

* 1. 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. 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:

……………………………..(1)

Keterangan:

N = jumlah sampel audio.

*x*[*i*] = nilai amplitudo dari file audio asli.

*y*[*i*] = nilai amplitudo dari file audio hasil steganografi.

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

………………………………..(2)

Keterangan:

= Nilai maksimal dari sampel audio, yaitu 32767 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.

Data yang digunakan dalam penelitian ini ada 4\*.wav audio sebagai wadah atau cover audio dan masing-masing memiliki pesan teks yang berbeda sebagai pesan yang akan disisipkan kedalam media cover audio. Dapat dilihat pada tabel 3.

Tabel 3. Sampel Audio

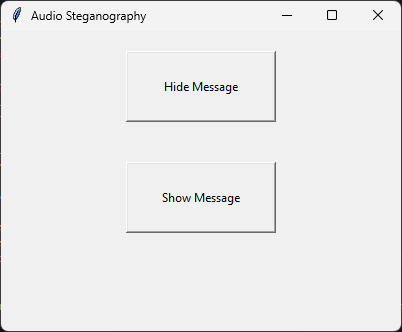
|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Audio sampel** | **Durasi** | **Ukuran file (MB)** |
| 1. | audio1.wav | 30 detik | 5.14 MB |
| 2. | audio2.wav | 60 detik | 10.1 MB |
| 3. | audio3.wav | 90 detik | 15.1 MB |

Sampel pertama adalah **audio1.wav** yang memiliki durasi 30 detik dan ukuran file sebesar 5.14 MB. Sampel kedua adalah **audio2.wav** dengan durasi yang lebih panjang yaitu 60 detik dan ukuran file sebesar 10.1 MB. Sampel ketiga adalah **audio3.wav** yang memiliki durasi 90 detik dan ukuran file sebesar 15.1 MB. Tabel ini memberikan gambaran mengenai karakteristik dari masing-masing sampel audio yang digunakan dalam penelitian. Adapun perhitungan yang akan dilakukan dengan merujuk pada persamaan (1) dan (2) sebagai berikut.

BAB 4. HASIL DAN PEMBAHASAN

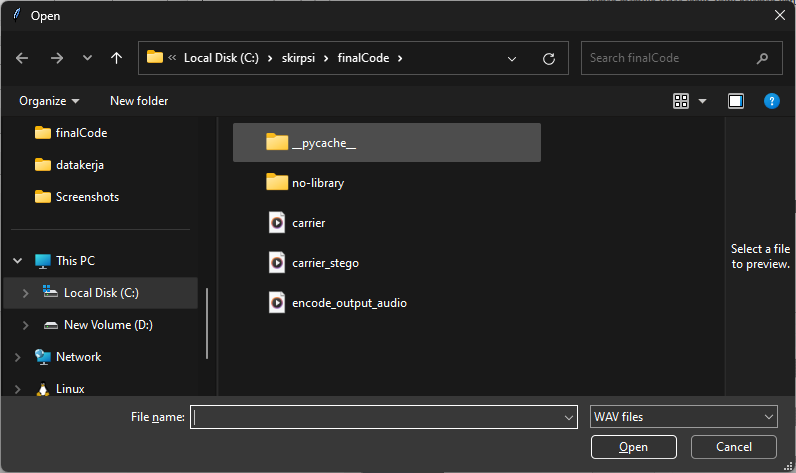
4.1 Hasil Pengembangan Sistem

Berikut adalah hasil dari pengembangan system berdasarkan perancangan system:

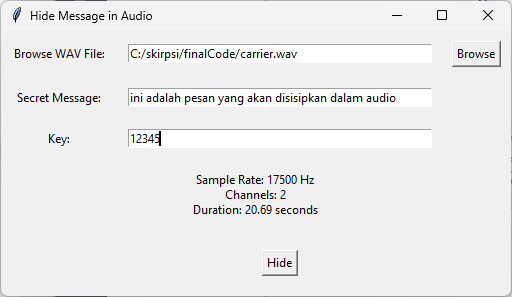
1. Halaman utama, menampilkan sebuat *button* untuk memilih fitur apa yang akan dijalankan. Tangkapan layar untuk halaman utama terdapat pada Gambar 15.

Gambar 15. Tangkapan Layar Halaman Utama

1. Halaman memilih audio input, yaitu halaman memilih audio yang akan disisipi sebuah pesan. Tangkapan layar untuk halaman memilih audio dapat dilihat pada Gambar 16.

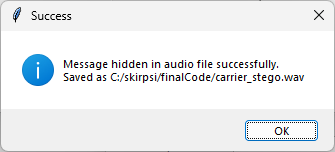


Gambar 16. Tangkapan Layar Halaman Memilih Audio Input

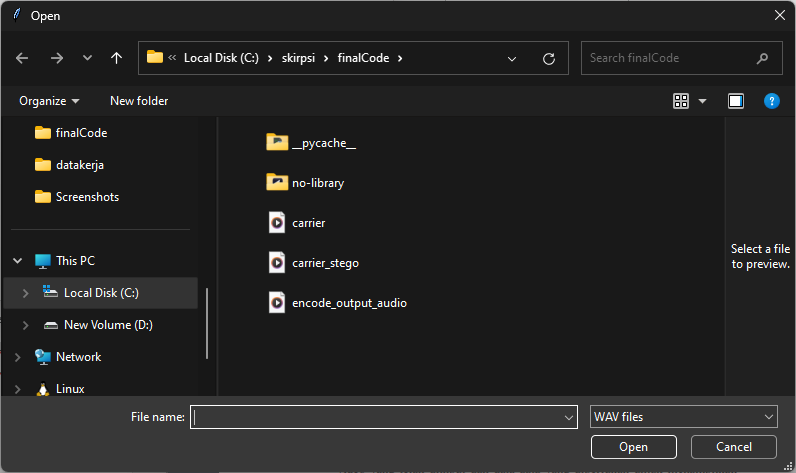
1. Halaman menyembunyikan pesan rahasia, yaitu halaman yang berisi informasi audio yang telah diinput dan data-data yang akan diinput masuk ke dalam audio. Tangkapan layar untuk halaman menyembunyikan pesan rahasia dapat dilihat pada Gambar 17.

Gambar 17. Tangkapan Layar Halaman Menyembunyikan Pesan Rahasia

1. Berhasil menyembunyikan pesan rahasia ke media audio akan menampilkan sbuah *pop up* menyembunyikan pesan berhasil dapat dilihat pada Gambar 18.

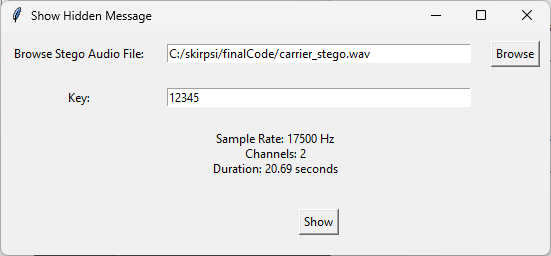


Gambar 18. Tangkapan Layar Pop up Pesan Rahasia Berhasil Disembunyikan

1. Halaman memilih audio steganografi, yaitu halaman untuk memilih audio yang telah disisipi pesan. Tangkapan layar untuk halaman memilih audio steganografi dapat dilihat pada Gambar 19.

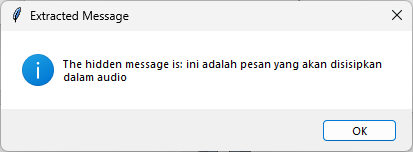
Gambar 19. Tangkapan Layar Halaman Memilih Audio Steganografi

1. 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 20.



Gambar 20. Tangkapan Layar Halaman Menampilkan Pesan Rahasia

1. 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 21.



Gambar 21. Tangkapan Layar *Pop up* Pesan Rahasia Berhasil Didapatkan

* 1. Hasil Pengujian Sistem

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

Tabel 4. *Black Box Testing*

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Aksi** | **Hasil yang diharapkan** | **Hasil yang sebenarnya** |
|  |  | 1. **Halaman Utama** |  |
| 1.1 | Menekan tombol*“ Hide Secret Message*” | Halaman “memilih audio input” terbika | Seperti yang diharapkan |
| 1.2 | Menekan tombol ”*Show Secret Message”* | Halaman “memilih audio steganografi” terbuka | Seperti yang diharapkan |
|  | 1. **Halaman Memilih Audio Input** | | |
| 2.1 | Memilih audio lalu menekan tombol “*Open*” | Halaman “menyembunyikan pesan rahasia” | Seperti yang diharapkan |
| 2.2 | Memilih tombol “*Cancel*” | Halaman memilih audio tertutup | Seperti yang diharapkan |
|  | 1. **Halaman Memilih Audio Steganografi** | | |
| 3.1 | Memilih audio lalu menekan tombol “*Open*” | Halaman “menyembunyikan pesan rahasia” | Seperti yang diharapkan |
| 3.2 | Memilih tombol “*Cancel*” | Halaman memilih audio tertutup | Seperti yang diharapkan |
|  | 1. **Halaman Menyembunyikan Pesan Rahasia** | | |
| 4.1 | Menekan tombol “*Hide”* tanpa mengisi *field “Browse wav file”* | Muncul error dengan pesan semua harus terisi | Seperti yang diharapkan |
| 4.2 | Menekan tombol “*Hide”* tanpa mengisi *field “Message”* | Muncul error dengan pesan semua harus terisi | Seperti yang diharapkan |
| 4.3 | Menekan tombol “*Hide”* tanpa mengisi *field “Key”* | Muncul error dengan pesan semua harus terisi | Seperti yang diharapkan |
| 4.4 | Menekan tombol “*Hide”* dengan semua *field* terisi | Muncul informasi penyembunyian berhasil beserta pesan yang berhasil disembunyikan | Seperti yang diharapkan |
|  | 1. **Halaman Menampilkan Pesan Rahasia** | | |
| 5.1 | Menekan tombol “*Show”* tanpa mengisi *field* “K*ey”* | Muncul *error* dengan pesan semua *field* harus terisi | Seperti yang diharapkan |
| 5.2 | Menekan tombol “*Show”* dengan semua *field* terisi | Muncul informasi pesan berhasil didapatkan beserta pesannya | Seperti yang diharapkan |
| 5.3 | Menekan tombol “*Show”* namun *key* yang dimasukkan salah | Muncul *error* dengan pesan *invalid* | Seperti yang diharapkan |

* 1. Hasil Analisis Hasil Sistem

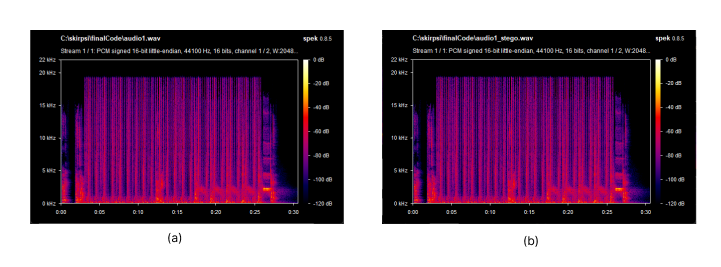
Berdasarkan data hasil uji steganografi, ditemukan bahwa file .wav yang dijadikan sebagai objek file yang disisipkan tidak mengalami perbahan kualitas suara yang signifikan. Maka hal ini tentunya membuat file teks dalam file audio berformat wav tetap aman, karena tidak akan menimbulkan kecurigaan dari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

Tabel 5. Hasil Nilai *Peak Signal to Noise Ratio*

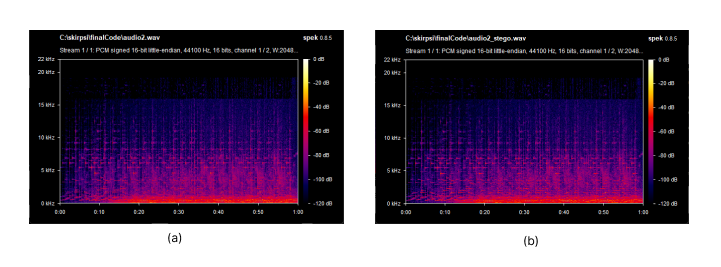
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Nama File** | **Durasi** | **Jumlah Kata** | **Ukuran Data** | | **PSNR (dB)** |
| **Awal** | **Stego** |
| 1. | audio1.wav | 30 detik | 200 | 5.14 MB | 5.14 MB | 86.691 |
| 2. | audio2.wav | 60 detik | 300 | 10.1 MB | 10.1 MB | 111.705 |
| 3. | audio3.wav | 90 detik | 100 | 15.1 MB | 15.1 MB | 121.881 |

Penampakan dari spektogram audio sebelum disisipkan pesan (audio asli) dan setelah disisipkan pesan (audio steganografi) pada audio1 dapat dilihat pada Gambar 22.

Gambar 22. (a) spektogram audio1 sebelum disisipkan pesan dan (b) spektogram audio1 sesudah disisipkan pesan

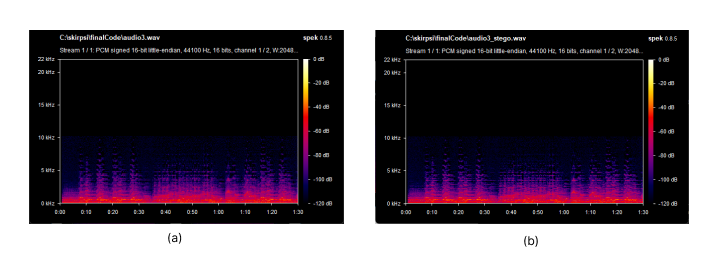


Penampakan dari spektogram audio sebelum disisipkan pesan (audio asli) dan setelah disisipkan pesan (audio steganografi) pada audio2 dapat dilihat pada Gambar 23.



Gambar 23. (a) spektogram audio2 sebelum disisipkan pesan dan (b) spektogram audio2 sesudah disisipkan pesan

Penampakan dari spektogram audio sebelum disisipkan pesan (audio asli) dan setelah disisipkan pesan (audio steganografi) pada audio2 dapat dilihat pada Gambar 24.



Gambar 24. (a) spektogram audio3 sebelum disisipkan pesan dan (b) spektogram audio3 sesudah disisipkan pesan

Perubahan yang dilakukan pada LSB tidak mengubah frekuensi utama dan amplitudo secara signifikan, sehingga karakteristik audio secara keseluruhan tetap hampir sama. Namun, karena perubahan tersebut dilakukan pada level yang sangat halus, pendengar yang sangat teliti mungkin merasakan sedikit perubahan dalam bentuk noise atau distorsi minimal. Ini menunjukkan bahwa teknik steganografi audio dengan algoritma LSB sangat efektif dalam menyembunyikan pesan tanpa mempengaruhi kualitas audio secara signifikan, baik secara visual pada spektogram maupun secara auditory melalui pendengaran.

BAB 5. KESIMPULAN DAN SARAN

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. Berhasilnya sistem yang dicitpatakan sesuai dengan tahapan dan rancangan yang telah disusun.
  2. Hasil dari skenario pengujian sistem menggunakan metode *Black Box Testing* pada 13 skenario berjalan sukses dengan tingkat keberhasil sebesar 100%
  3. Hasil analisis menggunakan parameter *Peak Signal to Noise Ratio* (PSNR) menunjukkan bahwa kualitas dari audio awal dan setelah penyisipan pesan tetap baik. Nilai PSNR yang didapatkan berada dalam rentang yang menunjukkan bahwa perubahan pada LSB tidak mempengaruhi kualitas audio dengan signifikan.
  4. Hasil dari spektogram menunjukkan bahwa perbedaan antara audio awal dan audio yang telah disisipi pesan sangat sulit dideteksi secara visual.

1. 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

Clara, L., & Budi, A. (n.d.). *IMPLEMENTASI METODE ALGORITMA AES PADA PERLINDUNGAN DATA SISTEM LOGIN*.

Laia, R. (2020). Implementasi Algoritma Aes 256 Bit Dan Lsb Untik Pengamanan Dan Penyisipan Pesan Teks Pada File Audio. In *Jurnal Pelita Informatika* (Vol. 8, Issue 4).

Maharani, S., & Agus, F. (2009). Implementasi Perangkat Lunak Penyandian Pesan Menggunakan Algoritma RSA. In *Jurnal Informatika Mulawarman* (Vol. 4, Issue 1).

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

Mulyono, I. U. W., 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*.

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