Implementasi Steganografi Audio Menggunakan Teknik Masking untuk Menyisipkan Pesan ke dalam Spectrogram

Permadi Kusuma

23917007

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Informatika Program Magister

Fakultas Teknologi Industri

Universitas Islam Indonesia

2025

Lembar Pengesahan Pembimbing

Implementasi Steganografi Audio Menggunakan Teknik Masking untuk Menyisipkan Pesan ke dalam Spectrogram

Permadi Kusuma

23917007

Yogyakarta, Mei, 2025

Pembimbing I

Dr. Yudi Prayudi, S.Si., M. Kom

Lembar Pengesahan Penguji

Implementasi Steganografi dengan Menggunakan Teknik Masking untuk Menyisipkan Pesan ke dalam Spectrogram

Permadi Kusuma

23917007

Yogyakarta, Mei, 2025

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M. Kom.
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota I

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.
Anggota II

16/05/2025

Mengetahui,
Ketua Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D.

Abstrak

Implementasi Steganografi Audio Menggunakan Teknik Masking untuk Menyisipkan Pesan ke dalam Spectrogram

Pada saat mengirim pesan kepada pihak tertentu dan tidak ingin pesan tersebut diketahui oleh pihak lain, maka penting untuk menghindari kebocoran informasi. Steganografi audio merupakan teknik penyembunyian data dalam sinyal audio yang semakin relevan dalam konteks keamanan informasi digital. Namun masalah yang teridentifikasi adalah terdapat kekurangan pengetahuan untuk mendeteksi Steganografi audio yang membutuhkan teknik yang dapat membaca dan melihat pesan rahasia. Penelitian ini bertujuan untuk menerapkan teknik masking pada *spectrogram* audio sebagai media penyisipan pesan tersembunyi, serta menganalisis hasil steganografi menggunakan pendekatan pemrograman *Python* dengan pustaka *Librosa* yang dipakai untuk analisis sinyal audio. Proses penyisipan dilakukan dengan memanfaatkan area frekuensi tertentu pada *spectrogram* yang cenderung tidak sensitif terhadap persepsi manusia. Sampel audio yang digunakan dalam penelitian ini terdiri dari lagu *Bernadya - Hidup Harus Tetap Berjalan* dan nada dering *Samsung Galaxy S3* dan *Samsung Galaxy S20*. Analisis audio dilakukan melalui visualisasi *spectrogram*, ekstraksi fitur *Mel-Frequency Cepstral Coefficients (MFCC*), *Zero-Crossing Rate (ZCR)*, serta evaluasi metadata file audio. Tujuan dari analisis ini adalah untuk melihat apakah ada pola-pola aneh atau tidak wajar yang muncul akibat penyisipan pesan rahasia dalam file audio. Jadi ketika ada data disisipkan secara tersembunyi, biasanya akan muncul perbedaan kecil dalam bentuk garis, noise, atau perubahan struktur visual yang tidak alami. Hasil penelitian menunjukkan bahwa penyisipan pesan berhasil dilakukan menggunakan teknik masking, namun menimbulkan perubahan pada karakteristik visual dan statistik sinyal audio asli dengan hasil steganografi.

Kata kunci

Steganografi Audio, Spectrogram, Masking.

Abstract

Implementation of Audio Steganography Using Masking Technique to Insert Messages into Spectrograms

When sending a message to a specific party and do not want the message to be known by other parties, it is important to avoid information leakage. Audio Steganography is a technique for hiding data in audio signals that is increasingly relevant in the context of digital information security. However, the problem identified is that there is a lack of knowledge to detect audio Steganography which requires techniques that can read and view secret messages. This research aims to apply masking techniques to audio spectrograms as a medium for inserting hidden messages, as well as analyzing the results of steganography using the Python programming approach with the Librosa library used for audio signal analysis. The insertion process is done by utilizing certain frequency areas in the spectrogram that tend to be insensitive to human perception. The audio samples used in this study consisted of the song Bernadya - Life Must Go On and the ringtone built into the Samsung device and Samsung Galaxy S20. Audio analysis is done through spectrogram visualization, Mel-Frequency Cepstral Coefficients (MFCC) feature extraction, Zero-Crossing Rate (ZCR), and audio file metadata evaluation. The purpose of this analysis is to see if there are any strange or unnatural patterns that arise due to the insertion of a secret message in an audio file. So when there is data inserted in a hidden manner, it is common for small differences to appear in the form of lines, noise, or unnatural changes in visual structure. The results show that message insertion is successfully performed using masking techniques, but it causes changes in the visual characteristics and statistics of the original audio signal with the result of steganography.

Keywords

Steganography Audio, Spectrogram, Masking.

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Mei, 2025

Permadi Kusuma, S.Kom.

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Asian Journal of Innovation and Entrepreneurship (AJIE) Volume 9 Nomor 1 yang terakreditasi SINTA 4, Edisi 01 Januari 2025 dengan Judul "**Implementasi Steganografi dengan Menggunakan Teknik Masking untuk Menyisipkan Pesan ke dalam Spectrogram Audio**".

Kontributor	Jenis Kontribusi
Permadi Kusuma	Mendesain eksperimen (60%) Menulis *paper* (80%)
Yudi Prayudi	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (20%)

Halaman Kontribusi

Penelitian ini dapat berjalan dan diselesaikan berkat kontribusi dari berbagai pihak, beliau-beliau telah banyak memberikan saran dan masukan mulai dari pra penelitian, seminar proposal, sidang kemajuan, hingga sidang pendadaran:

1. Bapak Dr. Yudi Prayudi, S.Si., M.Kom. selaku Pembimbing I, dan Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D. selaku dosen penguji proposal dan progres. Ibu Erika Ramadhani, S.T., M.Eng dosen penguji proposal dan progres, yang telah memberikan arahan-arahannya kepada penulis, sehingga penulisan tesis ini bisa selesai dengan baik dan tepat waktu.
2. Dosen dan Seluruh pengurus Akademik MI UII yang berjasa serta bersedia memberikan waktu dan ilmu pengetahuan selama menempuh masa studi magister informatika.

Halaman Persembahan

Alhamdulillah, atas izin dan ridho Allah Subhannahu Wa Ta'ala, saya dapat menyelesaikan tesis ini. Hal ini tentu tidak lepas dari adanya dukungan dan do'a kedua orang tua saya. Untuk itu kupersembahkan karya ini kepada Bapak saya, Irwan dan Ibu saya, Haliah. Serta ketiga kakak yang bernama Sulkia, Asgar dan Fadly Abrianto. Terima kasih banyak, saya bersyukur menjadi bagian dari keluarga kalian.

Khusus kupersembahkan karya ini kepada orang-orang yang tersayang dan yang telah berjasa:

1. Kepada kedua orang tuaku Bapak Irwan dan Ibu Haliah yang selalu memberikan doa, motivasi, serta nasehat dalam hidupku.
2. Kepada kedua kakakku Sulkia dan Fadly Abrianto yang telah memberikan bantuan biaya selama masa studi dan memberikan doa, motivasi, serta nasehat dalam hidupku.
3. Teman-teman yang sedang menempuh pendidikan di Jogja yang berasal dari Kota Palopo, Sulawesi Selatan yang selalu memberikan saran dan motivasi selama menempuh masa studi Magister Informatika di UII.

Kata Pengantar

Assalamu'alaikum Wr. Wb.

Puji syukur penulis sampaikan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayahnya kepada penulis, sehingga dapat menyelesaikan laporan tesis yang berjudul **"Implementasi Steganografi Dengan Menggunakan Teknik *Masking* Untuk Menyisipkan Pesan ke Dalam *Spectrogram* Audio"** Tesis ini merupakan syarat wajib yang harus ditempuh dalam mencapai gelar Magister Komputer di bidang Forensika Digital.

Dalam prosesnya penulis mendapat banyak bantuan dari berbagai pihak. Untuk itu, penulis menyampaikan terima kasih kepada semua pihak yang telah membantu penulis dalam menyelesaikan laporan tesis ini.

1. Bapak Prof. Fathul Wahid, S.T., M.Sc., Ph.D., Selaku Rektor Universitas Islam Indonesia.
2. Bapak Yudi Prayudi, S.Si., M.Kom. selaku dosen pembimbing 1 yang telah banyak memberikan masukan dan arahan terhadap jalannya penelitian yang penulis lakukan.
3. Bapak Irving Vitra Paputungan, S.T., M.Sc., Ph.D yang menjadi dosen penguji ketika penulis melakukan sidang proposal, sidang progres dan sidang pendadaran
4. Ibu Erika Ramadhani, ST., M.Eng. yang menjadi dosen penguji ketika penulis melakukan sidang proposal dan progres.
5. Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom., sebagai dosen penguji ketika penulis melakukan sidang pendadaran.
6. Teman-teman dari Magister Informatika Fakultas Teknologi Industri Universitas Islam Indonesia dan juga khususnya Konsentrasi Forensika Digital Angkatan XXVIII, Terima kasih banyak sudah saling berjuang dan bekerjasama.

Penulis menyadari bahwa pada penyusunan laporan tesis ini masih terdapat banyak kekurangan, oleh karena itu kritik, saran, dan masukan yang membangun sangat diharapkan oleh penulis.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 16 Mei 2025

Penulis

Daftar Isi

Daftar Tabel

Daftar Gambar

Glosarium

Masking	- Menyembunyikan pesan di dalam audio.
Spectrogram	- Frekuensi dalam sinyal audio.
Audacity	- Software yang dipakai untuk melihat pesan yang sudah disisipkan ke dalam audio.
CoagulaLight1666	- Software untuk mengkonversi gambar menjadi suara.
Noise	- Gangguan atau sinyal tidak diinginkan pada audio.
BMP (Bitmap)	- File gambar format *BMP (Bitmap)*
Formant	- Puncak frekuensi tertentu dalam suara
WAV	- Format file audio
Cute Audio	- Memotong bagian audio
Python	- Bahasa pemrograman yang dipakai untuk analisis data pada audio asli dan stego
Google Colab	- Platform berbasis cloud yang dipakai menjalankan berbagi kode *Python*.
Librosa	- Paket python untuk analisis musik dan audio
MFCC	- Fitur audio yang mewakili karakteristik suara dalam bentuk angka-angka
ZCR	- Analisis sinyal audio dengan membandingkan perubahan pada gelombang audio
Metadata	- Berisi informasi tambahan tentang suatu data misalnya audio

BAB 1
Pendahuluan

1.1 Latar Belakang

Semakin maraknya pengguna internet di Indonesia membuat kasus kejahatan siber terus meningkat. Berdasarkan laporan dari *pusiknas.polri.go.id.* Jumlah kejahatan siber ditahun 2022 alami peningkatan dibanding periode tahun 2021 yang meningkat 14 kali lipat. Polri juga mengakui kejahatan siber yang semakin marak tidak mudah diatasi, misalnya pada kasus kejahatan yang memanfaatkan steganografi yang bisa menyembunyikan komunikasi ilegal, malware, atau informasi sensitif yang dicuri. Dengan berkembangnya teknologi saat ini membuat teknik steganografi juga ikut berkembang. Berbagai macam teknik yang digunakan untuk melindungi informasi yang dirahasiakan dari orang yang tidak berhak telah banyak dilakukan dengan upaya mengamankan suatu data penting [1]. Steganografi sudah bisa diterapkan pada media digital seperti audio, foto dan video. Steganografi merupakan ilmu untuk menyembunyikan pesan ke dalam media lain agar orang selain pengirim dan penerima tidak mengetahui keberadaan pesan tersebut [2]. Steganografi pada audio berperan penting dalam keamanan informasi seperti digunakan untuk menyembunyikan data rahasia perusahaan, data pribadi, atau informasi sensitif lainnya. Deteksi steganografi juga membantu mengidentifikasi jika ada pihak yang akan mencoba menyisipkan data tanpa izin.

Namun sering kali ditemukan kasus kejahatan yang memanfaatkan Steganografi. Menurut situs *cyberthreat.id,* kejahatan steganohrafi audio pernah terjadi pada tahun 2019 yaitu perusahaan keamanan siber *Symantec* dan *BlackBerry Cylance* melaporkan bahwa kelompok peretas menggunakan file audio *WAV* untuk menyembunyikan kode berbahaya. Dalam kasus ini, malware disisipkan ke dalam file audio menggunakan teknik steganografi, memungkinkan kode berbahaya tersebut untuk menghindari deteksi oleh perangkat lunak keamanan yang biasanya tidak memeriksa file audio secara mendalam. Teknik ini digunakan dalam operasi spionase siber dan penambangan mata uang kripto ilegal. Temuan pertama steganografi dilakukan *Symantec* pada Juni 2019. Peneliti keamanan *Symantec* mengatakan telah melihat kelompok spionase siber diduga berasal dari Rusia yang dikenal sebagai *Waterbug* (atau *Turla*) menggunakan file *WAV*.[3].

Dalam konteks audio forensik, teknik *Masking* pada steganografi audio dipilih karena menawarkan beberapa keuntungan, seperti pesan steganografi yang ada pada audio aman

dari modifikasi dan bisa menampung pesan dengan jumlah kata atau kalimat yang bisa disesuaikan dengan kebutuhan. Cara kerja teknik *Masking* yaitu memanfaatkan kelemahan telinga manusia dalam mendeteksi perubahan kecil pada suara tersembunyi pada frekuensi tertentu. Suara yang disembunyikan dengan cara *Masking* akan ditutupi oleh suara lain yang lebih keras atau lebih dominan, sehingga informasi yang tersembunyi tersebut tidak terdengar oleh manusia. Selain itu, teknik ini memanfaatkan cara telinga dan otak memproses suara, sehingga sulit dideteksi melalui pendengaran normal.

Dalam bidang forensik digital. Penerapan steganografi audio menggunakan *Teknik Masking* dapat memberikan manfat berupa pengetahuan baru bagi seorang investigasi digital bahwa pesan rahasia bisa dimasukkan di *Spectrogram Audio*. Dengan kata lain petugas investigasi digital dapat memanfaatkan steganografi audio menggunakan teknik *Masking* untuk mendukung proses penyelidikan, pengumpulan bukti digital, dan pelacakan kejahatan.

Selain menyembunyikan informasi, penting juga untuk memastikan bahwa informasi tersebut tidak bisa diakses dengan mudah.. Adapun alasan ilmiah kenapa penulis tertarik untuk meneliti steganografi audio terutama menggunakan sampel musik adalah musik memiliki spektrum frekuensi yang kompleks dengan berbagai nada, harmoni, dan dinamika. Selain itu, musik adalah media yang sering dipertukarkan di internet, membuatnya ideal untuk komunikasi rahasia tanpa menimbulkan kecurigaan. Sehingga proses penyisipan pesan rahasia pada lagu dan nada dering dapat dikirim sebagai file biasa tanpa menarik perhatian.

1.2 Rumusan Masalah

Berdasarkan latar belakang penelitian, rumusan masaIah yang diangkat dalam penelitian ini adalah sebagai berikut:

1. Bagaimana cara mengimplementasikan teknik masking dalam steganografi audio untuk menyisipkan pesan tersembunyi ke dalam spectrogram audio?
2. Bagaimana karakteristik hasil audio steganografi dibandingkan dengan audio asli, ditinjau dari aspek visual spectrogram, parameter akustik, dan metadata file?
3. Sejauh mana teknik masking pada steganografi audio dapat digunakan dalam konteks investigasi forensik digital, khususnya dalam proses deteksi atau identifikasi pesan tersembunyi pada audio digital?

1.3 Batasan Masalah

Adapun batasan masalah pada penelitian ini adalah sebagai berikut:

1. Steganografi audio disembunyikan dalam cover audio digital berformat MP3.
2. Menyisipkan pesan rahasia dilakukan melalui Spektrogram audio.
3. Penelitian ini menggunakan Teknik *Masking* untuk menyisipkan audio.
4. Sampel audio penelitian berformat *MP3* yaitu lagu Bernadya, nada dering *Samsung Galaxy S3* dan nada dering *Samsung Galaxy S20.*

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah sebagai berikut

1. Mengimplementasikan teknik masking dalam steganografi audio untuk menyisipkan pesan tersembunyi ke dalam spectrogram
2. Membandingkan karakteristik hasil audio steganografi dengan audio asli melalui visualisasi Spektrogram, parameter akustik, dan metadata file.
3. Penelitian ini dilakukan untuk mengetahui sejauh mana teknik masking pada steganografi audio dapat digunakan dalam konteks investigasi forensik digital, khususnya dalam proses deteksi atau identifikasi pesan tersembunyi pada audio digital.

1.5 Manfaat Penelitian

Dari uraian yang sudah dijelaskan maka dari penelitian ini diharapkan mampu memberikan kontribusi pada penerapan steganografi audio yang terkait dengan penyimpanan pesan rahasia agar kedepannya teknik steganografi audio bisa digunakan dalam hal positif seperti kebutuhan untuk keamanan perusahaan yaitu melindungi data penting misalnya rencana bisnis dan informasi pada dokumen rahasia yang rawan dari penyadapan atau kebocoran. Penelitian tentang steganografi audio menggunakan teknik masking memberikan kontribusi terhadap Forensik Digital (FD), terutama dalam deteksi dan analisis pesan tersembunyi. Teknik ini memungkinkan pesan disisipkan dalam audio dengan cara memasukkan pesan ke area spectrogram yang dimana untuk menampilkan area tersebut membutuhkan software khusus yang tidak semua orang tahu. Selain itu, teknik masking ini bisa meningkatkan keamanan komunikasi tersembunyi yang tahan dari modifikasi seperti kompresi dan mengubah format audio.

Penelitian ini diharap juga bisa membantu para ahli investigasi digital dalam mengungkap kejahatan digital yang memanfaatkan teknik steganografi audio yang disembunyikan pada Spectrogram. Secara keseluruhan, penelitian ini berperan dalam mengembangkan metode steganografi yang lebih efisien dan aman, serta memperkuat kemampuan analisis forensik digital. Penelitian ini juga diharapkan mampu mengatasi celah pengetahuan dan memberikan pemahaman baru terhadap masalah yang dibahas pada penelitian terdahulu sehingga bisa menutupi kekurangan penelitian sebelumnya.

1.6 Metodologi Penelitian

Langkah langkah yang ditempuh dalam penelitian adalah sebagai berikut

1. Identifikasi Masalah

Pada tahapan ini peneliti melakukan identifikasi masalah yang ditemukan pada jurnal-jurnal terbaru, media massa dan laporan statistik resmi yang terkait kejahatan yang memanfaatkan teknik steganografi untuk menyisipkan pesan ke dalam media digital seperti foto, video dan audio.

2. Menetapkan Tujuan Penelitian

Tahapan selanjutnya menentukan tujuan dari penelitian ini yang sesuai dengan latar belakang masalah yang terkait dengan penggunaan steganografi audio. Seperti perbandingan audio asli dengan hasil stego dan juga.

3. Menentukan Objek Penelitian

Pada tahapan ini peneliti menentukan objek penelitian. Objek penelitian yang dimaksud adalah sampel audio yang akan dilakukan proses steganografi menggunakan teknik Masking.

4. Studi Literatur

Tahapan selanjutnya dilakukan studi literatur untuk mengumpulkan, meninjau, dan menganalisis informasi dari berbagai sumber yang sudah ada, seperti buku, artikel, jurnal, dan dokumen lainnya. Dengan meninjau literatur yang ada, peneliti dapat menemukan area yang belum banyak diteliti atau aspek tertentu yang masih membutuhkan penjelasan lebih lanjut.

5. Pengujian dan Analisis Sistem

Tahapan selanjutnya adalah pengujian dan analisis sistem. Pada penelitian ini menggunakan aplikasi Audacity untuk menyisipkan pesan. Untuk analisis audio stego menggunakan pemrograman Python. Hasil analisis dapat dilihat dari perbedaan *MFCC (Mel-Frequency*

Cepstral Coefficients), ZCR (Zero-Crossing Rate), Spectrogram dan metadata file audio asli dan stego.

6. Melakukan Pembahasan Hasil

Pada tahap ini peneliti membahas, mengevaluasi, dan menginterpretasikan hasil dari eksperimen atau pengujian yang telah dilakukan. Pada tahapan ini peneliti melakukan pembahasan berupa hasil analisis dan implenetasi steganografi audio menggunakan teknik Masking pada lagu dan nada dering berformat mp3.

7. Memberikan Kesimpulan dan Saran

Pada bagian ini akan menjelaskan kesimpulan dari hasil steganografi audio menggunakan teknik Masking. Pada tahapan ini, peneliti juga menjelaskan saran untuk mengembangkan penelitian selanjutnya khususnya pada steganografi audio yang diharap kedepannya semakin berkembang.

1.7 Sistematika Penulisan

Untuk memudahkan proses pembahasan dalam penelitian yang dibuat ini, maka peneliti membuat sistematika penulisan pada penelitian sebagai berikut:

BAB I Pendahuluan

Bab ini memuat uraian pengantar terkait masalah yang akan diteliti. Secara detail bab ini berisi latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II Tinjauan Pustaka

Pada bab ini memuat mengenai teori-teori yang melandasi dan terkait serta digunakan dalam penelitian ini.

BAB III Metodologi Penelitian

Bab metodologi penelitian berisi langkah-langkah atau alur jalannya penelitian dari awal sampai akhir.

BAB IV Pembahasan

Berisi hasil penelitian terkait uji coba dari implementasi teknik yang dipakai.

BAB V Penutup

Pada bab ini dijelaskan mengenai kesimpulan akhir yang didapat dari hasil penelitian untuk menjawab rumusan masalah. Disini juga dijelaskan mengenai penelitian lanjutan yang diharapkan dapat dilakukan di masa depan.

BAB 2
Tinjauan Pustaka

2.1 Penelitian Terdahulu

Teknik steganografi sudah dikenal sejak lama walaupun belum menggunakan media digital. Steganografi digunakan untuk menyembunyikan data di dalam data lain. Banyak teknik yang dapat digunakan untuk menyembunyikan informasi di dalam gambar, audio, dan video di antaranya adalah *Teknik LSB (Least Significant Byte), Discrete Cosine Transform (DCT),* dan *Masking and Filtering*. Teknik *LSB* bisa menyisipkan data dalam jumlah besar karena memanfaatkan hampir setiap piksel namun rentan terhadap manipulasi dan mudah rusak oleh kompresi atau pengeditan kecil seperti cropping dan diresize seperti pada penelitian [4] yang melakukan penelitian steganografi pada gambar dan audio. Begitupun dengan penelitian [5] yang memakai teknik *LSB* pada citra digital, hasilnya berhasil menyembunyikan data rahasia dengan baik. Namun tingkat keberhasilan dan kualitas citra stego sangat tergantung pada pengolahan citra yang dilakukan. Untuk teknik steganografi *Discrete Cosine Transform (DCT)* pada penelitian [2] suara yang dihasilkan audio stego tidak berbeda jauh dengan file audio awal, sehingga pesan yang tersembunyi di dalamnya tersimpan dengan baik. Proses penyisipan hanya dapat dilakukan jika ukuran data pada file pesan lebih kecil dari ukuran data file audio. Jika ukuran file pesan lebih besar dari file audio, maka aplikasi akan menampilkan hasil error atau proses penyisipan gagal dilakukan.

Teknik *Masking* membuat informasi sulit ditemukan tanpa alat atau teknik khusus. Barang bukti audio kerap muncul sebagai temuan barang bukti digital dalam berbagai perkara. Tidak menutup kemungkinan terdapat pesan tersembunyi dalam setiap audio temuan tersebut [6]. Pada penelitian [7] mengusulkan teknik *Masking and Filtering* dengan melakukan pengujian memasukkan pesan rahasia ke dalam gambar berformat JPG, tujuannya agar pesan rahasia dapat dibaca dan dimengerti oleh orang tertentu saja, cara untuk menyembunyikan pesan tersebut, yaitu dengan steganografi menggunakan teknik *Masking and Filtering* dimana proses *Masking* nantinya menjadi media penanda pada gambar yang dapat menyisipkan pesan. *Filtering* memberikan nilai pada bagian yang sudah diberikan tanda. Penyembunyian pesan dilakukan dengan memanipulasi nilai pencahayaan dari gambar.

Sama halnya dengan penelitian [8] yang menggunakan teknik *Masking and Filtering*. Secara komprehensif mempelajari bagaimana menerapkan Steganografi dengan menyisipkan gambar sebagai pesan rahasia ke media yang juga berupa gambar. Hasil yang diperoleh adalah kualitas gambar setelah disisipi dengan informasi rahasia tidak mengalami perubahan yang berarti, setelah dilakukan proses penyisipan informasi rahasia kedalam gambar dan dilakukan proses ekstraksi. Pesan disisipkan ke dalam file gambar sehingga pesan tersebut tidak dapat diketahui orang lain. Hal ini disebabkan adanya perbedaan susunan warna antara warna gambar asli dan warna Stego Image.

Kekurangan dari penelitian sebelumnya yaitu teknik pemfilteran *masking* ini dibatasi pada gambar yang menampilkan warna abu-abu. Pada penelitian sebelumnya, teknik *Masking and Filtering* dilakukan pada steganografi gambar. Selain itu beberapa penelitian juga menggunakan teknik yang berbeda seperti teknik *LSB* dan *DCT*. Teknik Masking menawarkan kualitas audio yang baik dan ketahanan terhadap manipulasi, namun dengan kapasitas penyisipan yang terbatas [9]. Metode *LSB* memiliki kapasitas penyisipan yang besar, tetapi kurang tahan terhadap manipulasi. Sementara itu, metode *DCT* menawarkan keseimbangan antara kualitas dan ketahanan, namun dengan kompleksitas yang lebih tinggi dibandingkan LSB. [10]. Alasan peneliti menggunakan teknik *masking* dikarenakan bisa tahan dari serangan modifikasi seperti kompresi, cute audio, konvert audio ke format lain dan pengeditan lainnya. Teknik *masking* juga bisa menyisipkan kalimat panjang dan gambar yang bisa disesuaikan dengan kebutuhan.

Pada penelitian ini melakukan implementasi steganografi pada file audio dengan menggunakan teknik *Masking* yang bisa memasukkan pesan teks format *Bitmap* yang sudah diubah menjadi audio ke dalam media audio yaitu lagu yang berformat *MP3*. Penelitian ini menganalisis tiga audio yang sudah dilakukan penyisipan pesan steganografi. Adapun aplikasi yang digunakan untuk menyisipkan pesan rahasia adalah *Audacity* dan aplikasi yang dipakai membuat pesan rahasia ialah *CoagulaLight1666* yang bisa mengubah file gambar menjadi audio berformat *WAV*. Sedangkan untuk menganalisis audio menggunakan pemrograman *Python* melalui *Google Colab*.

Peneliti akan membuat skenario dalam penyisipan pesan dan juga dilakukan proses Analisis dan validasi perbandingan audio asli dan audio yang sudah dilakukan proses steganografi.. Untuk mengetahui perbedaan audio setelah disisipi pesan yaitu dengan menganalisis perbedaan *spectrogram, Mel-Frequency Cepstral Coefficients (MFCC), Zero-*

Crossing Rate (ZCR), dan *metadata* file audio. Berikut ini beberapa penelitian terdahulu yang terkait dengan steganografi audio yang dapat dilihat pada tabel di bawah ini.

Tabel 1.1 Rangkuman penelitian terdahulu

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
1	F. Ro'isa and I. M. Suartana (2019)	1) Penelitian ini menggunakan Teknik *Masking* untuk menyisipkan informasi rahasia ke dalam gambar. Pada proses ini dibagi menjadi dua yaitu penyisipan pesan dan pengekstrakan pesan. 2) Teknik *Masking* ini terbatas dalam gambar 24 bit warna atau berskala keabuan *(Grayscale).* Teknik tersebut hampir sama dengan teknik *Watermark,* yang mana sebuah gambar ditandai yang akan digunakan sebagai penyembunyian suatu pesan rahasia.	**Kelebihan:** Hasil yang diperoleh dari penelitian ini yaitu setelah informasi rahasia dimasukkan ke dalam gambar, kualitas gambar tidak mengalami perubahan yang signifikan. Namun, setelah proses ekstraksi dan penyisipan, informasi rahasia dapat diungkap kembali. **Kekurangan:** jika gambar diubah, informasi rahasia yang telah dimasukkan dapat rusak, yang berarti informasi rahasia tidak dapat dideteksi atau diekstraksi. Waktu yang dibutuhkan untuk proses penyisipan (Encoding) lebih lama daripada proses ekstraksi.
2	B. Yanti Fitri and Khairi (2023)	1) Pada penelitian ini Eksperimen ini dilakukan pada gambar digital *RGB* dalam format *BMP,* yang kemudian dimasukkan pesan teks. Implementasi akan dilakukan	**Kelebihan:** Penyisipan dan penyembunyian pesan menggunakan teknik steganografi LSB *(Least Significant Byte),* dan algoritma

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
		menggunakan software *MATLAB*. 2) Embedding (penyisipan pesan) dan ekstraksi (mengembalikan pesan seperti semula) adalah dua tahapan yang dilakukan selama proses implementasi steganografi *LSB*.	Vigenere Cipher pada gambar digital berjalan baik. Tidak ada perubahan yang signifikan dari gambar aslinya ke gambar yang dilakukan penyisipan pesan (stego image). **Kekurangan:** Pesan yang sudah disisipkan pada citra dapat diperoleh kembali. Kecuali jika pesan atau informasi yang disisipkan pada gambar diubah formatnya, dicrop, atau diresize ukurannya, pesan dan informasi di dalamnya akan rusak.
3	A. D. Hendrata and A. Prihanto (2021)	1) Pada penelitian ini, Perangkat lunak yang dibangun menggunakan Bahasa Matlab memiliki kemampuan untuk menyembunyikan pesan rahasia di dalam file teks ke dalam format audio *WAV*. 2) Teknik *LSB* dipakai untuk menanamkan bit pesan rahasia pada bit yang kurang signifikan dari file audio. Teknik ini memiliki kelemahan, yaitu tidak tahan terhadap serangan dan kemudahan	**Kelebihan:** 1. Sistem yang dibangun dapat melakukan dua proses yaitu proses encoding pesan rahasia ke dalam suara dan proses decoding untuk mengekstrak pesan rahasia dari suara. 2. Pengujian untuk membandingkan grafik sinyal audio asli dengan sinyal audio stego menunjukkan bahwa keduanya memiliki grafik

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
		untuk mengekstrak dan menghancurkan pesan yang telah disisipkan ke dalam file.	sinyal yang hampir identik secara visual. **Kekurangan:** Teknik LSB memiliki kelemahan pada sisi ketahanan terhadap serangan dan menghancurkan pesan yang telah disisipkan pada file.
4	Moh Azhar Ulum (2023)	1) Teknik *Discrete Cosine Transform (DCT)* dipilih karena kemampuannya untuk menjaga keutuhan dari file pembawa pesan, yang membuat pesan sulit dikenali pada file hasil steganografi. Matlab digunakan untuk menerapkannya. 2) Penelitian ini melakukan pengujian teknik black box testing dan perhitungan nilai Peak Sinyal to Noise Ratio (*PSNR*) dilakukan dengan menggunakan kombinasi tiga rekaman suara dan delapan file audio dalam berbagai ukuran. Pesan yang disisipkan terdiri dari enam sample pesan dalam format txt dan dua pesan yang diketikkan langsung pada form yang disediakan.	**Kelebihan:** 1. Hasil pengujian black box menunjukkan bahwa semua fitur dan tombol aplikasi dapat berfungsi dengan baik. 2. Suara yang dihasilkan audio stego tidak berbeda jauh dengan file audio awal, sehingga pesan yang tersembunyi di dalamnya tersimpan dengan baik. **Kekurangan:** Proses penyisipan hanya dapat dilakukan jika ukuran data pada file pesan lebih kecil dari ukuran data file audio. Jika ukuran file pesan lebih besar dari file audio, maka aplikasi akan menampilkan hasil error atau proses penyisipan gagal dilakukan.

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
5	Sunardi, I. Riadi, and M. Hajar Akbar (2020)	1) Pada penelitian ini, tahapan penelitian yang dilakukan untuk pengambilan bukti digital adalah metodologi static forensics yang merupakan teknik konvensional untuk melakukan penanganan barang bukti elektronik . Teknik ini berfokus memeriksa salinan duplikasi atau image. 2) Metodologi penelitian dimulai dengan tinjauan literatur, yang mengumpulkan referensi dari berbagai sumber. Setelah itu, perancangan skenario kasus, persiapan alat dan bahan untuk simulasi kasus, investigasi dan analisis kasus, dan diskusi dan pemberian kesimpulan.	**Kelebihan:** 1.Penelitian ini berhasil melakukan proses ekstraksi file steganografi pada bukti digital sehingga penerapan teknik static forensics bisa diterapkan. 2.Dengan menggunakan *FTK Imager*, proses akuisisi data dapat menghasilkan sembilan salinan bukti digital dengan nilai hash yang sama dengan nilai file aslinya. Akibatnya, hasil ekstraksi file steganografi pada bukti digital dapat dianggap sebagai bukti yang sah. **Kekurangan:** Beberapa format file lebih rentan terhadap pengeditan dan kompresi, yang dapat merusak informasi yang disembunyikan.
6	G. M. Marevson (2024)	Penelitian ini memakai teknik *LSB* untuk mengurangi noise pada audio steganografi. Penelitian ini menggunakan file audio berformat	**Kelebihan:** Audio steganografi menggunakan teknik LSB berhasil diimplementasi untuk

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
		.wav yang dipakai sebagai cover dalam audio steganografi.	menyembunyikan pesan berupa teks dalam cover file audio berformat.wav. Program berhasil melakukan encoding dan decoding pesan. **Kekurangan:** Program yang dibuat memiliki noise yang masih dapat didengar karena LSB yang diimplementasi tidak memiliki step (jarak).
7	D. El Rezen Purba and Desinta Purba (2021)	1) Teknik yang diterapkan pada penelitian ini adalah Masking yaitu melakukan pengujian memasukkan pesan rahasia ke dalam gambar berformat JPG. Agar pesan rahasia dapat dibaca dan dimengerti oleh orang tertentu saja. 2) Masking berfungsi sebagai penandaan tempat pada gambar dimana pesan dapat disisipkan. Teknik ini mirip dengan watermark, dimana sebuah gambar ditandai *(watermark)* untuk menyembunyikan pesan rahasia.	**Kelebihan:** Data teks disisipkan ke dalam file gambar sehingga data tersebut tidak dapat diketahui orang lain. Hal ini disebabkan adanya perbedaan susunan warna antara warna gambar asli dan warna Stego Image. **Kekurangan:** Teknik pemfilteran masking ini terbatas pada gambar dengan 24bit warna atau gambar mode skala abu-abu.
8	A. Permana (2020)	Penelitian ini menggunakan teknik *End Of File* yang cocok memasukkan data pada ujung file.	**Kelebihan:** Penelitian ini mencapi hasil yang signifikan dimana teknik ini

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
		Teknik Ini dapat digunakan untuk melakukan penyisipan data yang ukurannya sama dengan ukuran file asli dan yang mau disisipkan.	memproses data dengan mengubahnya menjadi bilangan desimal dan menyisipkannya di akhir file audio. **Kekurangan:** Ukuran file tidak dapat diubah secara signifikan, karena tidak mengubah suara.
9	M. Assyahid, R. Rihartanto, and D. S. B. Utomo (2018)	Penelitian ini menggunakan audio dengan format *WAV*, sementara pesan yang sisipkan data dalam bentuk teks. Nantinya data teks disebar ke dalam audio untuk menghasilkan stego-audio sehingga memiliki kualitas audio yang tidak jauh berbeda dibandingkan dengan audio aslinya.	**Kelebihan:** 1. Penyisipan pesan menggunakan teknik Spread Spectrum menjadikan pesan yang disisipkan menjadi lebar dan acak. 2. Semakin rendah nilai MSE maka semakin baik, dan semakin besar nilai PSNR maka kualitas stego-audio juga semakin. **Kekurangan:** Pada penelitian ini, data yang digunakan adalah audio sebagai media cover dan text sebagai pesan yang disembunyikan. Sehingga data awal harus direpresentasikan menjadi bentuk data biner.

No	Peneliti	Pendekatan/Teknik Penelitian	Hasil Penelitian
10	Yang diusulkan peneliti	Pada penelitian ini akan mencoba mengimplementasi steganografi audio menggunakan teknik *Masking*. Pada penelitian sebelumnya, teknik *Masking* dilakukan pada steganografi gambar dan beberapa penelitian sebelumnya menggunakan teknik berbeda seperti memakai teknik *LSB* dan *DCT*. Metode *DCT* menyisipkan pesan ke dalam koefisien frekuensi secara langsung, kekurangan dari metode *DCT* yaitu proses stego dapat menyebabkan penurunan kualitas suara. Sedangkan *LSB* mengubah bit terakhir pada sinyal audio di domain waktu. Kekurangan metode *LSB* yaitu hasil stego mudah rusak terhadap proses kompresi atau modifikasi. Sebaliknya, pendekatan masking dalam *spectrogram* bisa menjaga kualitas suara dan aman dari proses modifikasi. Dengan keunggulan ini, metode yang diusulkan memiliki potensi untuk digunakan dalam komunikasi rahasia yang lebih aman dan tahan terhadap gangguan atau deteksi. Pada penelitian ini akan mencoba melakukan implementasi steganografi audio menggunakan teknik *Masking* yang bisa memasukkan pesan teks dan gambar format *Bitmap* yang sudah diubah menjadi audio ke dalam media audio.	

2.2 Steganografi

Steganografi menyembunyikan data rahasia di file lain sedemikian rupa sehingga hanya penerima yang tahu adanya pesan. Dahulu kala, data dilindungi dengan menyembunyikannya di belakang lilin, menulis meja, perut kelinci atau di kulit kepala para budak. Tapi hari ini sebagian besar orang mengirimkan data berupa teks, gambar, video, dan audio di atas medium. Agar transmisi data rahasia aman, objek multimedia seperti audio, video, gambar digunakan sebagai sumber cover untuk menyembunyikan data.[11]. Steganografi merupakan salah satu teknik yang dapat digunakan untuk menyembunyikan pesan dengan menggunakan media digital. Steganografi digital menggunakan media digital sebagai wadah penampung misalnya gambar, suara, teks, maupun video. Data rahasia yang disembunyikan juga dapat berupa gambar, suara, teks, maupun video.[12]. Pesan rahasia tidak diubah menjadi bentuk karakter unik seperti halnya kriptografi. Pesan tersebut hanya

disembunyikan ke dalam suatu media berupa musik, gambar, teks, atau media tampung digital lainnya dan terlihat seperti pesan atau berkas biasa. [5].

Pada penelitian ini akan mengimplementasikan steganografi audio dengan menyisipkan pesan ke dalam area Spectrogram audio. Penerapan steganografi pada file audio dianggap lebih rumit dibandingkan pada file video. Hal ini dikarenakan kemampuan pendengaran manusia (*Human Auditory System*) lebih peka daripada kemampuan pengelihatan manusia *(Human Visual System)*. [13]. Tujuan utama dari Steganografi adalah menyembunyikan informasi di dalam file atau media lain sehingga tidak terlihat mencurigakan. Pesan yang disembunyikan tidak bisa dilihat oleh orang-orang yang tidak berwenang. Dengan steganografi, informasi disembunyikan di tempat yang tidak terlihat atau tidak terduga, seperti dalam gambar, video, atau audio, sehingga hanya pihak yang tahu cara mengekstrak informasi tersebut yang bisa membaca pesan tersebut. Teknik steganografi dapat diterapkan pada beberapa tipe media yang berbeda seperti text, audio, dan video. file audio dan video dianggap sebagai media yang baik pada teknik steganografi karena banyaknya redundansi.

2.3 Audio

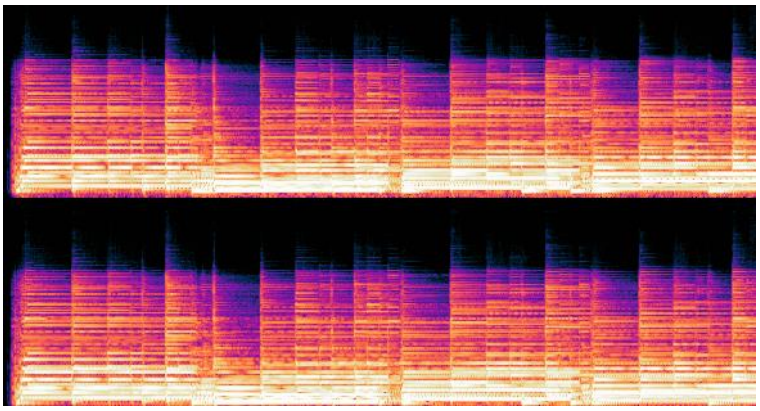
Media audio menurut [14], adalah media yang hanya dapat didengar saja atau dengan kata lain hanya memiliki unsur suara. Seperti radio, kaset, telepon, dan rekaman suara. Media audiovisual menyatakan seperangkat alat yang dapat memproyeksikan ganbar bergerak dan bersuara, alat-alat tersebut seperti televisi, *PC-speaker active, VCD* dan media sound slide. Media audio, merupakan media yang hanya dapat dinikmati dengan pendengaran saja, hanya mempunyai unsur bunyi dan lain sebagainya seperti radio atau rekaman berbunyi. Media audio juga hanya dapat melayani si pendengar atau penerima pesan yang sudah mampu dapat berfikir apa arti atau esensi dari audio yang di dapatkan. Biasanya menggunakan media ini seperti di acara radio biasanya serempak dan tidak dapat terkontrol atau sulit melakukannya. [15].

Pada penelitian ini akan mencoba menyisipkan pesan ke dalam audio berformat MP3. Audio adalah salah satu istilah yang digunakan dalam fonetik dan fonologi yang merupakan kekhasan suatu bahasa [14]. Sedangkan menurut [16] , media audio merupakan media yang menyajikan pesan secara auditif. Atau dengan kata lain, yang dimaksud dengan media audio adalah semua media yang pemanfaatannya menggunakan unsur dengar (audio). Keterampilan yang dapat dicapai dengan penggunaan media audio meliputi pemusatan perhatian dan mempertahankan perhatian, mengikuti pengarahan, melatih daya analisis, menentukan arti dari konteks, memilah- milah informasi atau gagasan yang relevan dan

informasi yang tidak relevan, merangkum, mengemukakan kembali atau mengingat kembali informasi [17].

2.4 *Spectrogram*

Spectrogram adalah bentuk visualisasi dari masing-masing nilai Formant yang dilengkapi dengan level energi yang bervariasi terhadap waktu. Level energy ini dikenal dengan istilah Formant Bandwidth. Dikarenakan *Spectrogram* memuat hal-hal yang bersifat detail, maka Spectrogram oleh beberapa ahli juga dikenal dengan istilah sidik jari suara (*voice fingerprint*). Spectrogram membentuk pola umum yang khas dalam pengucapan kata dan pola khusus masing-masing *Formant* dalam pengucapan suku kata, sehingga Spectrogram juga digunakan untuk melakukan Analisis identifkasi suara seseorang. [18]. Penelitian steganografi audio ini menyisipkan pesan ke area Spectrogram sehingga pada kasus yang melakukan pemalsuan audio dimana subyek berusaha untuk menghilangkan karakter suara aslinya, maka *Formant Bandiwidth* dapat berperan untuk mengidentifikasi audio aslinya. Sehingga bisa membedakan mana yang asli dan manipulasi.



Gambar 2.1 Tampilan *Spectogram* di aplikasi *Audacity*

Menurut [19] Analisis *Spectrogram* ini didasarkan pada perbandingan pola yang dihasilkan dari kata-kata yang diucapkan oleh suara sampel dengan kata-kata yang diucapkan oleh suara barang bukti. *Spectrogram* membentuk pola-pola yang khas, sehingga dapat dijadikan sebagai salah satu analisis untuk audio forensik, dapat juga untuk mengidentifikasi dan memahami informasi tersembunyi maupun pola komunikasi guna membantu dalam investigasi digital. Pada *Spectrogram* terkadang juga menghasilkan kata yang memiliki pola yang tidak jelas dan berbeda dengan barang bukti. Hal tersebut dapat terjadi karena suara yang ada di rekaman suara tidak jelas pengucapannya dan tidak sama dengan rekaman barang bukti. Tahapan ini untuk mendapatkan gambaran pada rekaman suara yang memiliki

ciri khas tersendiri. *Spectrogram* menunjukkan sebaran energi yang terdapat pada *formant* yang sebelumnya telah didapatkan. [20].

2.5 Masking

Teknik steganografi sendiri sudah dikenal sejak lama walaupun belum menggunakan media digital. Steganografi digunakan untuk menyembunyikan data di dalam data lain. Banyak teknik yang dapat digunakan untuk menyembunyikan informasi di dalam gambar, audio, dan video di antaranya adalah *Teknik LSB (Least Significant Byte), Masking and Filtering* dan *Discrete Cosine Transform (DCT).*

Teknik masking berkembang dari konsep yang didasarkan pada psikoakustik dan teori sistem pendengaran manusia *(Human Auditory System, HAS).* Teknik masking dalam psikoakustik pertama kali diperkenalkan oleh *Hermann von Helmholtz*, seorang ilmuwan Jerman abad ke-19. Dalam karyanya yang berjudul "*On the Sensations of Tone as a Physiological Basis for the Theory of Music*" yang diterbitkan pada tahun 1863. Dalam buku ini, *Helmholtz* menjelaskan fenomena di mana suara tertentu dapat menutupi atau "mem-mask" suara lain, sehingga suara yang ditutupi menjadi tidak terdengar oleh pendengaran manusia [21].

Dalam steganografi audio, *masking* digunakan untuk menyembunyikan informasi rahasia dalam sinyal suara tanpa mengubah kualitas audio yang dapat didengar manusia. Sebelum menyisipkan pesan, peneliti mencoba mendeteksi bagian audio yang keras atau dominan, seperti suara drum atau vokal yang terdapat pada musik. Suara yang lebih lemah di sekitar bagian ini tertutup secara alami, sehingga ideal untuk menyisipkan informasi. Inilah mengapa peneliti memilih media musik karena memberikan beragam nada dan irama yang bisa dimanfaatkan untuk proses penyisipan pesan. Misalnya sebuah musik yang menyajikan beragam bunyi yang sangat keras. Jika terdapat suara pelan di belakang musik tersebut, kemungkinan besar tidak bisa mendengar karena tertutup oleh suara dominan yang keras.

Pada penelitian ini menggunakan teknik *masking*, teknik ini biasanya terbatas pada gambar 24 bit atau gambar grayscale. Teknik ini mirip dengan watermarking pada kertas yang akan memberikan tanda pada gambar. Hal ini diperoleh dengan memodifikasi bagian cahaya gambar. Informasi tidak disimpan pada "*noise*" level tetapi disimpan di bagian gambar yang terlihat jelas, sehingga lebih cocok digunakan dalam kasus *lossy compression algorithm* seperti pada gambar JPEG [12]. Melalui teknik steganalisis ini pesan rahasia mampu dideteksi dan diketahui ada tidaknya pesan tersembunyi tersebut. Teknik masking

lebih bagus daripada teknik *LSB* dikarenakan teknik masking membolehkan adanya kompresi, pemotongan, dan sebagian proses yang dilakukan dalam gambar. Teknik masking melewatkan informasi ke dalam tempat tertentu sehingga pesan tersebut dapat semakin terselubung dibanding hanya sekedar menutupi tingkatan noise pada gambar [8].

Pada steganografi audio, Proses masking dilakukan pada *Spectrogram* audio yang mempunyai tujuan untuk menandai area pada audio yang akan disisipi dengan pesan. Pada penyisipan pesan dilakukan dengan menyisipkan pesan rahasia ke dalam audio. Kemudian membandingkan antara audio sesudah dan sebelum disisipi dengan informasi rahasia. Dengan begitu bisa mengetahui kualitas audio setelah disisipi dengan informasi yang sudah diubah dalam format audio.

2.6 Teknik *LSB (Least Significant Byte)*

Selain teknik masking, terdapat juga Teknik *LSB (Least Significant Byte) dan Discrete Cosine Transform (DCT).* Audio Steganografi menggunakan teknik *LSB* memiliki keuntungan berupa kemudahan implementasi dan kecepatan algoritma. Kelemahan dari *LSB* adalah adanya noise yang dapat didengar telinga manusia. Beberapa solusi yang dapat digunakan untuk mengurangi noise tersebut adalah dengan membuat step (jarak) di tiap byte yang diganti atau dengan memilih lagu sedemikian rupa sehingga noise berada di bagian audio yang diam [22].

LSB merupakan metode yang paling sederhana untuk menyembunyikan data dalam file citra , dikarenakan metode ini memiliki komputasi yang tidak terlalu rumit dalam penyembunyian pesannya. *LSB* ini menggunakan citra digital sebagai convertext,yaitu dengan mengubah bit yang tidak begitu berpengaruh pada redundan cover image dengan bit dar pesan rahasia. Terdapat bilangan 8 bit pada tiap -tiap susunan , dari 0 sampai dengan 255 atau jika dengan biner dari 00000000 sampai 11111111. Dan pada setiap pixel pada berkas gambar bitmap 24 bit dapat disisipkan 3 bit data.[10].

2.7 Teknik *DCT (Discrete Cosine Transform)*

(DCT) Discrete Cosine Transform (DCT) adalah sebuah teknik untuk mengubah sebuah sinyal ke dalam komponen frekuensi dasar, teknik *Discrete Cosine Transform (DCT)* memiliki kelebihan yakni pesan rahasia pada gambar akan tetap terjaga terhadap kompresi pada gambar akan tetapi memiliki kelemahan yaitu penurunan kualitas citra stego jika dibandingkan dengan citra aslinya [11].

Pada tahapan *DCT* ini dapat merubah suatu informasi dari area waktu ke dalam area frekuensi tersebut. Dimana perubahan ini bertujuan untuk mempersingkat perpindahan suatu informasi, dapat memangkas suatu penyimpanan yang ada pada memori. Pada *DCT* tersebut menggambarkan sebuah gambar dengan penambahan senosida dari jarak dan juga perubahan dalam frekuensi itu. *DCT* adalah skema *Lossy Compression* yang dipakai *JPEG* kompresi citra digital *NxN* diubah dari domain spasial ke domain *DCT*. [10].

Tabel 2.1 Perbandingan teknik *Masking, LSB dan DCT*

Teknik	**Kapasitas**	**Ketahanan**			**Penyisipan Pesan**
		Cute audio	**Kompresi**	**Mengubah Format audio**	
Masking	Terbatas	✓	✓	✓	✓
LSB	Kapasitas lebih tinggi	×	×	×	✓
DCT	Terbatas	×	×	✓	✓

Pada tabel perbandingan diatas menunjukan teknik masking lebih kuat dalam pengujian ketahanan pesan seperti memotong bagian audio, melakukan kompresi dan mengubah format audio, seperti yang sudah dilakukan pada penelitian [9]. Namun teknik masking terbatas pada kapasitas pesan yang disisipkan, dikarenakan semakin panjang kalimat, maka pesan yang tampil pada spectrogram akan sulit untuk dibaca. Sedangkan teknik *LSB (Least Significant Bit)* bisa menyisipkan data dalam jumlah besar, namun rentan terhadap manipulasi dan mudah rusak oleh kompresi atau pengeditan kecil, seperti pada penelitian [4] dengan judul *"Implementasi Teknik Steganography Pada File Gambar dan Audio Dengan Menggunakan Metode LSB"*. Untuk pesan yang disisipkan dapat diperoleh kembali, namun jika pesan pada media diubah formatnya, *dicrop,* atau *diresize*, maka pesan di dalamnya akan rusak. Seperti pada penelitian [13] dengan judul *"Analisis Kualitas Suara Stego Audio Penyisipan Informasi Tersembunyi dengan Metode Least Significant Bit"*.

Sedangkan pada metode *DCT (Discrete Cosine Transform)*, kapasitas pesan yang disisipkan lebih kecil dibanding *LSB* namun lebih besar dibanding teknik Masking dikarenakan proses penyisipan hanya dapat dilakukan jika ukuran data pada file pesan lebih kecil dari ukuran data file audio. Jika tidak maka akan menampilkan hasil error atau proses

penyisipan gagal dilakukan, seperti pada penelitian [2] dengan judul *"Implementasi Audio Steganografi Menggunakan Algoritma Discrete Cosine Transform"*. Pada penelitian [23] dengan judul *"Steganografi Audio Berbasis Qr Code Menggunakan Metode Least Significant Bit (Lsb), Discrete Cosine Transform (Dct), Dan Discrete Wavelet Transform (Dwt)"* Stego file tidak tahan pada pengujian ketahanan kompresi diakibatkan oleh kompresi yang menghilangkan sebagian informasi sehingga pesan menjadi rusak.

2.8 Pemrograman *Python*

Python adalah bahasa pemrograman yang menggunakan interpreter untuk menjalankan kode programnya. Interpreter tersebut dapat menerjemahkan kode secara langsung, dan Python dapat dijalankan di berbagai platform seperti *Windows, Linux,* dan lain-lain. Python mengadopsi paradigma pemrograman dari beberapa bahasa lain, termasuk paradigma pemrograman prosedural seperti bahasa *C*, pemrograman berorientasi objek seperti Java, dan bahasa fungsional seperti *Lisp*. Kombinasi paradigma ini memudahkan para programmer dalam mengembangkan berbagai proyek menggunakan Python.

Banyak programmer dan peneliti beralih ke penggunaan bahasa pemrograman *Python*. Python dapat digunakan untuk berbagai keperluan, seperti pengembangan aplikasi web, aplikasi desktop, *IoT*, dan berbagai aplikasi lainnya. *Python* juga memiliki integrasi dengan sistem database dan mampu membaca serta mengubah file, sehingga sering digunakan untuk prototyping atau pengembangan perangkat lunak dengan cepat dan reliabel. Selain itu, *Python* juga digunakan secara luas oleh para peneliti karena kemampuannya dalam menangani data besar dan perhitungan matematika yang kompleks [24]

Bahasa pemrograman *Python* merupakan bahasa pemrograman populer yang memiliki keunggulan sebagai berikut :

1. Mudah untuk digunakan dalam mengembangkan sebuah produk perangkat lunak, perangkat keras, *Internet of Things*, aplikasi web, maupun video game.
2. Selain memiliki keterbacaan kode yang tinggi, sehingga kode mudah dipahami, bahasa pemrograman ini memiliki library yang sangat banyak dan luas.
3. Merupakan bahasa yang mendukung ekosistem Internet of Things dengan sangat baik [25]

Bahasa *Python* dirancang pada tahun 1990 oleh *Guido van Rossum*. Seperti banyak bahasa skrip lainnya, bahasa ini gratis, bahkan untuk penggunaan komersial, dan dapat dijalankan di hampir semua komputer modern. [26]**.**

2.9 *Librosa*

Librosa adalah paket *Python* untuk pemrosesan musik dan audio yang memungkinkan pengguna untuk memuat audio di notebook sebagai array numpy untuk analisis dan manipulasi. Melakukan pemeriksaan data untuk setiap pola secara visual dengan menggunakan librosa untuk mengimplementasikan file audio *(.mav*) dan matplotlib untuk menampilkan bentuk gelombang.[27] **.** Secara umum, fungsi librosa cenderung mengekspos semua parameter yang relevan kepada pemanggil. Pada tingkat tinggi, librosa menyediakan implementasi berbagai fungsi umum yang digunakan di seluruh bidang pencarian informasi musik. [28]**.**

Librosa difokuskan untuk memfasilitasi solusi yang layak untuk kasus uji ini, di mana pengguna dapat memutar not audio pada antarmuka musik yang kemudian dievaluasi berdasarkan kinerjanya dengan file yang dipilih. *Librosa* mempertimbangkan beberapa variabel dan faktor seperti faktor kenyaringan, tempo, dan jumlah frekuensi dengan instrumen musik untuk tujuan validasi. Proses validasi dilakukan melalui serangkaian fase seperti normalisasi fitur, teks, dan pencocokan pola audio untuk mengambil spektrograf yang efisien dari audio yang diputar. Keterbatasan seperti deteksi urutan musik serta awal kebisingan diabaikan dengan penggunaan model pencocokan pola. Elemen kinerja didasarkan pada not musik yang terlewatkan oleh pengguna, dan not audio asing yang dimainkan oleh pengguna. [29]**.**

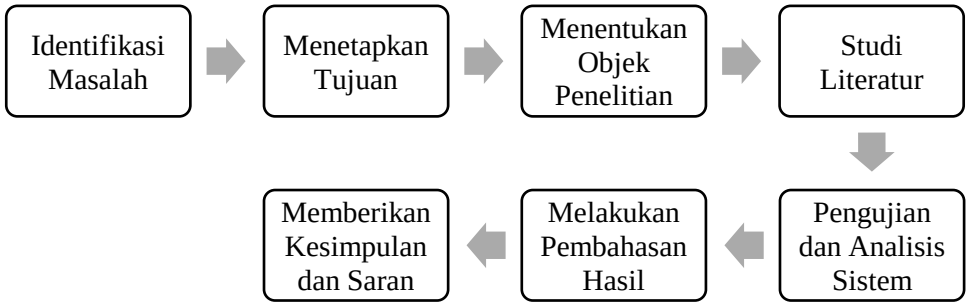
2.10 Digital Forensik

Forensik digital adalah praktik pengumpulan, analisis, dan pelaporandata digital. Investigasi forensik digital memiliki peranan yang sangat beragam. Forensik adalah istilah yang diberikan untuk penyelidikan kejahatan menggunakan sarana ilmiah atau digunakan untuk menggambarkan deteksi kejahatan secara umum. [30]**.** Dalam berbagai kasus *Cyber Crime*, ilmu digital forensik kerapkali membantu pihak kepolisian dan hakim dalam mengidentifikasi adanya manipulasi pada data atau rekaman suara, sehingga dapat membuktikan keaslian data tersebut. Peran lainnya yaitu menyediakan bukti yang dapat digunakan di pengadilan karena bukti digital yang dikumpulkan melalui proses forensik dapat dihadirkan di pengadilan untuk mendukung argumen dan keputusan dalam persidangan.

BAB 3

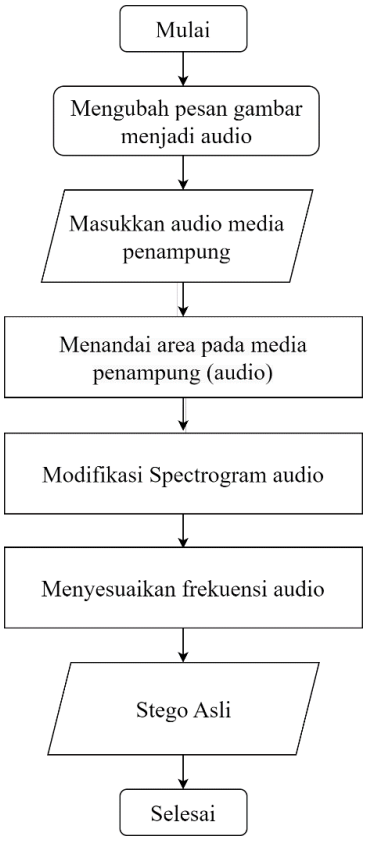
Metodologi

Secara garis besar tahapan metodologi penelitian ini dapat dilihat pada Gambar 3.1.



Gambar 3.1 Metodologi yang Diusulkan

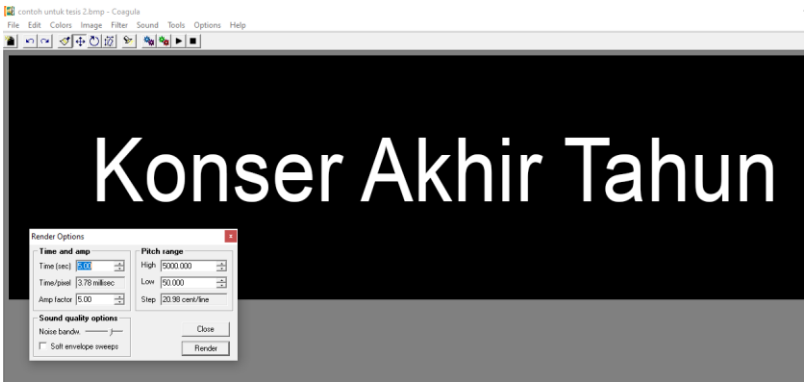
Penelitian ini dilaksanakan sesuai alur yang telah direncanakan dan terkait dengan tahapan dalam teknik penelitian yang kemudian diimplementasikan. Adapun langkah-langkah steganografi dalam penelitian ini bisa dilihat pada gambar 3.2.



Gambar 3.2 Flowchart Teknik Masking

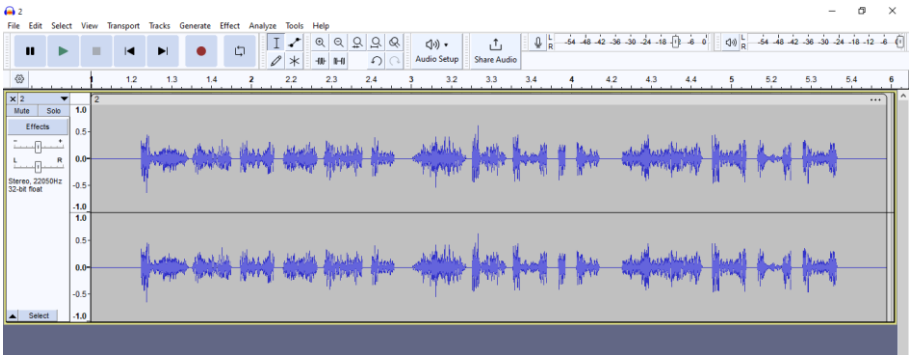
3.1 Pemilihan File Audio

Pada penelitian ini memilih file audio yang digunakan sebagai media penyembunyian (*cover audio*). File ini harus memiliki kualitas dan ukuran yang cukup besar untuk bisa menyembunyikan pesan dengan baik. Penelitian ini akan mencoba memilih audio berformat MP3 sebagai cover audio. Untuk audio yang dijadikan sampel yaitu lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*", *"Nada Dering Samsung Galaxy S3* dan nada dering *Samsung Galaxy S20*". Didalam audio ini sudah dilakukan penyisipan pesan rahasia yang nanti dianalisis.



Gambar 3.3 Aplikasi *CoagulaLight1666*

Pada gambar 3.3 menampilkan layar aplikasi *CoagulaLight1666* yang berfungsi mengubah gambar yang menampilkan teks **"*Konser Akhir Tahun*"** menjadi audio berformat *WAV*. Untuk membuka file gambar yang sudah diubah menjadi audio dapat dibuka melalui aplikasi *Audacity* dan melalui *Google Colab* dengan menggunakan kode *Python*.



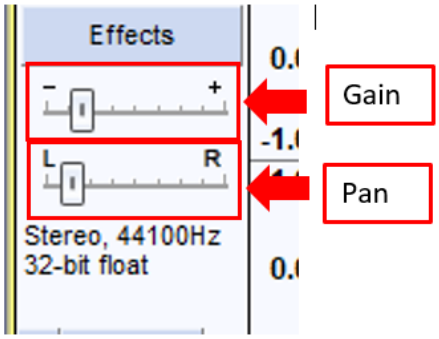
Gambar 3.4 Pesan Dalam Bentuk Audio

Pada gambar 3.4 menampilkan pesan "***Konser Akhir Tahun***" yang sudah diubah menjadi audio. Audio yang berisikan pesan ini akan disisipkan pada file audio media penampung melalui *spectrogram* dengan cara dimasking.

3.2 Penyisipan Pesan

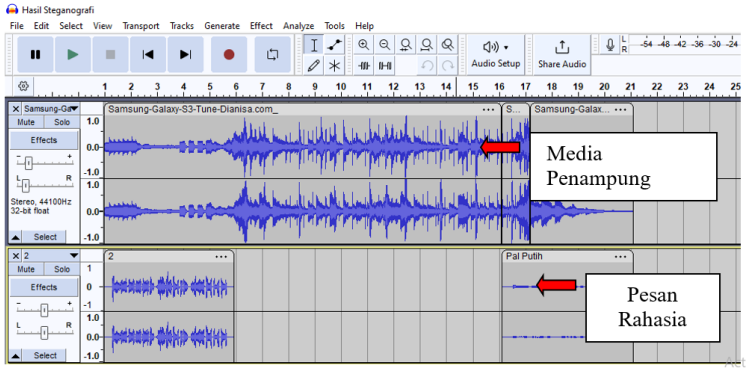
Peneliti menentukan bagian dari spektrum audio di mana suara tambahan dapat dimasukkan tanpa terdeteksi oleh pendengaran manusia. Biasanya, suara dengan frekuensi yang lebih tinggi atau yang berada di belakang suara yang lebih keras dipilih untuk penyisipan. Dengan begitu suara tertentu pada audio bisa menutupi suara lain yang lebih lemah, sehingga tidak terdengar oleh telinga manusia. Adapun pesan yang akan dijadikan steganografi adalah yang merupakan gambar yang sudah diubah ke bentuk audio sehingga pesan dapat disisipkan ke dalam musik dengan cara dimasking.

Terdapat tiga pesan yang akan disisipkan pada tiga file audio. Pesan yang pertama bertuliskan *"Konser Akhir Tahun, Pal Putih, dan 31 Desember"* yang disisipkan pada audio dari lagu *Bernadya - Untungnya, Hidup Harus Tetap Berjalan*. Pesan kedua bertuliskan *"nama saya permadi kusuma konsentrasi forensika digital universitas islam indonesia"* yang disisipkan pada nada dering *Samsung Galaxy S3*. Untuk pesan yang ketiga dalam bentuk gambar yaitu gambar *Flashdisk* merk *Sandisk* yang disisipkan pada nada dering *Samsung Galaxy S20*. Proses penyisipan pesan stego menggunakan aplikasi *Audacity*.



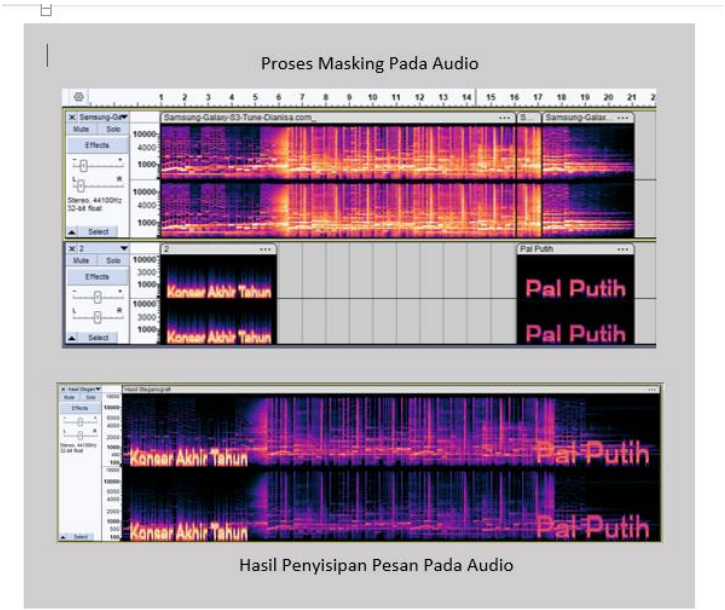
Gambar 3.5 Proses Penurunan Efek *Gain* dan *Pan* di *Audacity*

Pada tahapan ini dilakukan pengaturan *Gain* (penguatan) yang berfungsi mengatur tingkat kekuatan sinyal audio seperti efek atau mixing. Dengan menurunkan efek *Gain*, maka suara menjadi lebih rendah sehingga bisa menghindari distorsi. Sementara itu, pengaturan *Pan* (panorama) berfungsi untuk mengatur posisi suara dalam bidang stereo, yaitu antara kiri dan kanan. Misalnya, jika pan digeser ke kiri, suara lebih terdengar dari speaker kiri, dan sebaliknya. Kombinasi gain dan pan digunakan untuk mengontrol keseimbangan dan kejelasan suara dalam sebuah mix. Penggunaan *Gain* dan *Pan* yang tepat dapat membantu dalam optimasi steganografi audio, baik dalam hal menyembunyikan pesan secara efektif maupun memastikan bahwa pesan tetap dapat diekstraksi dengan baik tanpa terdistorsi oleh proses pengolahan audio.



Gambar 3.6 Proses penyisipan Steganografi pada Audio

Selanjutnya pesan rahasia kemudian disisipkan ke dalam file audio pada bagian yang sudah dipilih dan difilter sebelumnya. Teknik penyisipan bisa menggunakan berbagai teknik, seperti menyisipkan pesan ke dalam area *Spectrogram* audio sebagai area yang ingin di masking. Dengan memasukkan nada pada frekuensi tingkat daya yang rendah, penyisipan data tersembunyi yang diekstraksi tercapai. [31]



Gambar 3.7 Tampilan Proses Steganografi Audio di *Audacity*

Pada gambar 3.7 merupakan proses steganografi audio dengan menggunakan teknik masking melalui area *Spectrogram*. File audio yang berisikan pesan disatukan dengan audio penampung yaitu file audio berformat mp3.

3.3 Penyimpanan dan Analisis

Setelah proses steganografi berhasil, file audio disimpan dan dilakukan analisis untuk mengidentifikasi perubahan dari audio asli dengan audio stego. Dalam penelitian ini,

dilakukan analisis *MFCC (Mel-Frequency Cepstral Coefficients), ZCR (Zero-Crossing Rate),* dan analisis *spectrogram*. Sehingga nantinya akan dianalisis menggunakan pemrograman *Python* melalui *Google Colab*. Sedangkan analisis metadata file menggunakan *Software Mediainfo*. Analisis yang digunakan ini mengacu pada pendekatan secara umum yang telah dilakukan oleh penelitian sebelumnya.

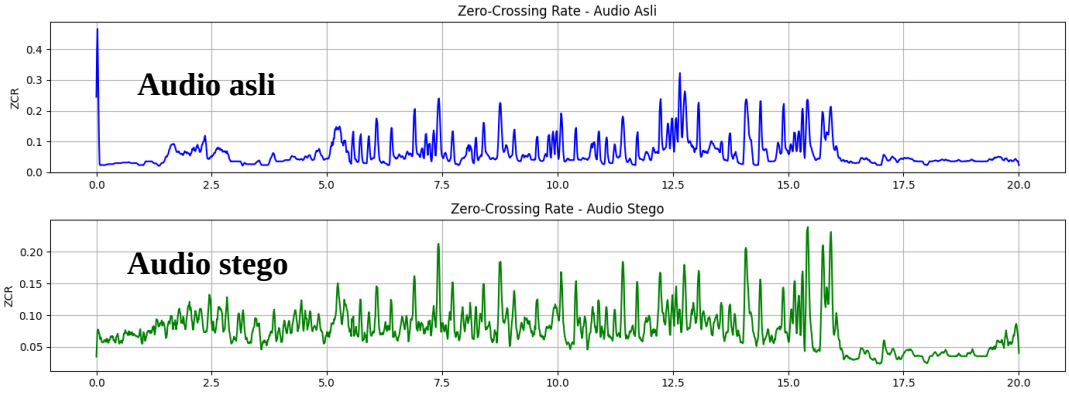
3.3.1 Analisis *MFCC (Mel-Frequency Cepstral Coefficients)*

Pada tahapan analisis *MFCC* dapat digunakan untuk mendeteksi perubahan kecil yang terjadi pada karakteristik frekuensi audio akibat penyisipan pesan tersembunyi. Dengan menggunakan *MFCC*, proses analisis dimulai dengan membandingkan grafik audio asli dan stego. Setelah itu, pola frekuensi yang tampil dalam bentuk grafik diubah menjadi angka-angka (koefisien *MFCC*) yang bisa dibandingkan antara audio asli dan audio stego. Jika terjadi perubahan akibat penyisipan pesan, maka nilai *MFCC*-nya juga akan mengalami pergeseran. Sehingga dengan adanya perbandingan nilai-nilai *MFCC* Mean dan *STD*, penyelidik dapat mengidentifikasi adanya perbedaan meskipun perubahan itu tersembunyi dari pendengaran manusia. Analisis ini merujuk pada penelitian yang ditulis oleh [32] dengan judul *Perbandingan Steganalisis Sinyal Wicara Berformat WAV Antara Metode Analisis Cepstral dan Mel-Frequencycepstral Coefficient (MFCC)* yang melakukan analisis *cepstral* dan *MFCC* dalam mendeteksi pesan tersembunyi pada sinyal wicara berformat .wav.

3.3.2 Analisis *ZCR (Zero-Crossing Rate)*

Pada tahapan ini, analisis *ZCR (Zero-Crossing Rate)* didasarkan pada seberapa sering sinyal audio melintasi garis nol dalam satuan waktu. Ini berguna untuk melihat karakteristik dasar dari suara, misalnya suara tersebut lebih banyak mengandung nada halus atau suara bising. Dalam sinyal yang bersih dan stabil, *ZCR* menampilkan grafik yang rendah, sedangkan pada sinyal yang terdapat gangguan atau noise akan menunjukan grafik lebih tinggi. Dengan melihat grafik *ZCR* audio asli dan stego, peneliti bisa mengidentifikasi perubahan kecil dalam pola gelombang suara. Dalam konteks steganografi audio, perubahan *ZCR* antara audio asli dan audio stego bisa menunjukkan adanya penyisipan pesan tersembunyi, karena proses penyisipan biasanya sedikit mengubah pola gelombang asli. Analisis *ZCR* yang digunakan peneliti merujuk pada penelitian *Audio Features Based Steganography Detection in WAV File the Creative Commons Attribution License (CC BY 4.0)* yang ditulis

oleh [33] yang melakukan analisis *MFCC* dan *ZCR* untuk membedakan antara sinyal audio asli dan yang telah disisipi pesan tersembunyi.



Gambar 3.8 Tampilan Grafik *ZCR (Zero-Crossing Rate)*

3.3.3 Analisis *Spectrogram*

Pada tahapan ini analisis perbedaan *Spectrogram* antara audio asli dan audio yang telah disisipi pesan dilakukan agar bisa melihat adanya pesan yang disisipkan pada media lagu dan nada dering. Meskipun perubahan suara mungkin tidak terdengar oleh telinga manusia, perbedaan ini dapat terlihat jelas pada *spectrogram*, yaitu gambar visual dari frekuensi suara terhadap waktu. Dengan membandingkan dua *spectrogram*, maka dapat melihat adanya pola yang tidak biasa yang menunjukkan adanya pesan tersembunyi. Analisis ini juga membantu memastikan keaslian sebuah file audio dan bisa menjadi bukti bahwa file tersebut telah dimodifikasi. Selain itu, perbedaan spektral juga bisa menunjukkan bagian mana dari audio yang telah disisipi pesan. Pada penelitian [34] melakukan analisis audio stego menggunakan metode *LSB* dengan menganalisis area *spectrogram* yang terdapat perubahan akibat adanya proses steganografi.

3.3.4 Analisis Metadata

Pada tahapan ini dilakukan pemeriksaan informasi spesifik yang tersimpan dalam file audio asli dan stego seperti ukuran file, bitrate, dan format file. Metadata ini bisa berubah saat pesan disisipkan ke dalam audio, misalnya ukuran file menjadi lebih besar atau penambahan bitrate yang melebihi standar lagu dan nada dering yang berformat *MP3*. Dalam konteks steganografi, perubahan metadata bisa menjadi petunjuk awal bahwa file telah dimanipulasi. Dengan membandingkan metadata file asli dan file stego, peneliti atau penyidik dapat mendeteksi adanya anomali teknis yang mendukung adanya modifikasi file

yang merujuk pada kecurigaan terdapat pesan rahasia, meskipun perubahan tersebut tidak langsung nampak pada suara audionya. Pada penelitian [35] dengan judul *A Novel Hybrid Method for Effective Identification and Extraction of Digital Evidence Masked by Steganographic Techniques in WAV and MP3 Files* melakukan analisis metadata untuk mengidentifikasi tanda-tanda manipulasi pada file audio yang mengandung steganografi.

3.4 Analisis Kebutuhan

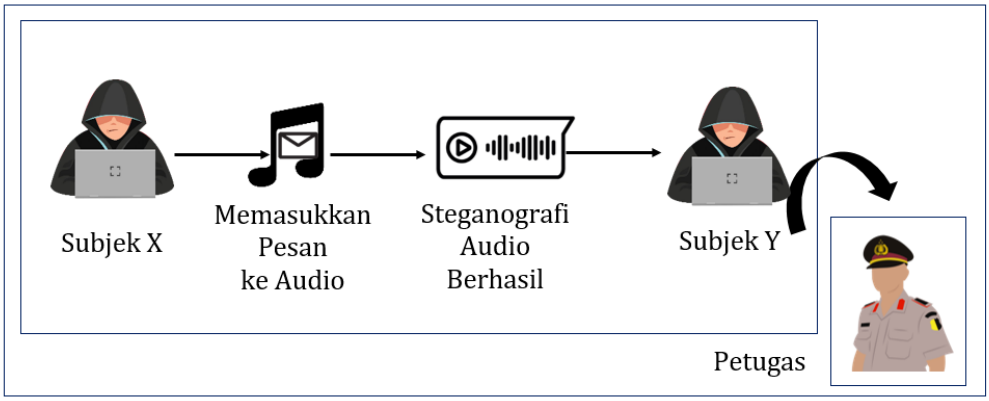
Peneliti akan melakukan analisis dari implementasi teknik steganografi *Masking*. Disini dibutuhkan beberapa *software* dan *hardware* agar bisa membantu proses analisis terhadap teknik yang digunakan. Penelitian ini menggunakan Laptop *Acer* yang sudah terinstal *Tools* yang digunakan untuk menguji keberhasilan steganografi. Peneliti menggunakan perangkat keras dan perangkat lunak sebagai berikut:

a) Perangkat Keras menggunakan Laptop *Acer* dengan spesifikasi:
   - *Ram DDR 3 6gb.*
   - *HDD 500 GB.*
   - *VGA Intel® HD Graphics.*
   - *Processor Intel® Core™ i3.*

b) Perangkat Lunak untuk penelitian:
   - Tools *Adobe Photoshop* dipakai untuk membuat gambar yang menampilkan tulisan untuk disisipkan ke audio.
   - Tools *CoagulaLight1666* adalah *tools* yang bisa digunakan untuk mengubah gambar menjadi audio.
   - Tools *Audacity* dipakai untuk menyisipkan dan mendeteksi steganografi pada audio.
   - *Google Colab* dipakai untuk menulis dan menjalankan kode *Python* untuk Analisis steganografi audio.
   - *Librosa* pustaka *Python* digunakan untuk menganalisis dan memproses data steganografi audio.
   - *Software Mediainfo* digunakan untuk analisis metadata audio asli dan stego.

3.5 Skenario Kasus

Melakukan analisis terhadap teknik steganografi *Masking*. Disini diperlukan skenario kasus dengan melibatkan file audio yang sudah dilakukan penyisipan pesan tersembunyi sehingga bisa menemukan pesan tersembunyi pada audio tersebut. Ilustrasi kasus dapat dilihat Gambar 3.8.



Gambar 3.9 Skenario kasus

Deskripsi kegiatan dimana subjek X merupakan orang yang membuat pesan rahasia. Kemudian menyisipkan pesan ke dalam audio untuk dikirim ke temannya yaitu subjek Y, petugas investigas menemukan file audio tersebut dan mencoba mendeteksi dan menganalisis isi pesan yang tersimpan di dalam file audio menggunakan Pemrograman *Python* melalui *Google Colab*.

3.6 Peran Teknik Masking dalam Investigasi Forensik Digital

Teknik masking dalam steganografi audio digunakan untuk menyisipkan pesan rahasia ke dalam bagian audio yang tidak terdengar oleh manusia, biasanya dengan menyembunyikan pesan di balik suara yang lebih keras. Dalam konteks forensik digital, teknik ini dapat menjadi tantangan karena perubahan suara sulit dikenali secara kasat telinga dan tidak semua petugas investigas mengetahui irama lagu atau audio yang dijadikan stego. Namun, dengan analisis audio seperti *MFCC (Mel-Frequency Cepstral Coefficients)* dan *ZCR (Zero-Crossing Rate)*, perubahan halus tersebut dapat terdeteksi secara grafik dan numerik, misalnya melalui perbandingan nilai mean dan standar deviasi antara audio asli dan stego. Dengan begitu pendekatan analisis grafik dan data numerik sangat berguna dalam mengungkap steganografi audio. Begitupun dengan analisis *spectrogram* audio asli dengan stego yang dapat mendeteksi adanya modifikasi area spectrogram yang dilakukan dengan cara dimasking.

BAB 4
Hasil dan Pembahasan

Pada bab ini, membahas tentang hasil implementasi dan analisis terhadap lagu *Bernadya,* nada dering *Samsung Galaxy S3,* dan nada dering *Samsung Galaxy S20* yang telah melalui proses steganografi. Berdasarkan hasil evaluasi tersebut maka dapat dilihat bagaimana karateristik audio setelah dilakukan proses steganografi.

4.1 Analisis Steganografi Audio

Untuk mendukung hasil implementasi steganografi audio pada Spectrogram, maka dilakukan analisis karateristik audio yang secara umum sudah dilakukan oleh penelitian sebelumnya seperti, analisis perbedaan *Spectrogram*, *MFCC (Mel-Frequency Cepstral Coefficients)*, *Zero-Crossing Rate (ZCR)* dan analisis metadata. Tujuan dari analisis ini adalah untuk melihat apakah ada pola-pola aneh atau tidak wajar yang muncul akibat penyisipan pesan rahasia dalam file audio. *Spectrogram* memvisualisasikan bagaimana energi suara tersebar dalam frekuensi dan waktu, jadi ketika ada data disisipkan secara tersembunyi, biasanya akan muncul perbedaan kecil dalam bentuk garis, noise, atau perubahan struktur visual yang tidak alami. Dengan membandingkan *spectrogram* file asli dan stego, maka bisa mencoba mengungkap apakah ada manipulasi yang tidak terdengar langsung tapi bisa terlihat secara visual.

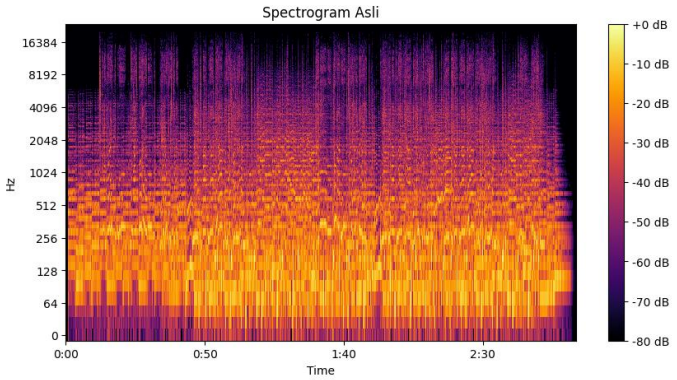
4.1.1 Analisis Steganografi Perbedaan Spectrogram

Analisis *spectrogram* dilakukan guna melihat pola perbedaan *spectrogram* audio asli dan audio yang telah disisipi pesan. Meskipun perubahan suara tidak terdengar oleh telinga manusia, namun perbedaan dapat dilihat jelas pada *spectrogram* yang menampilkan gambar visual dari frekuensi suara. Dengan begitu, peneliti dapat mendeteksi perbedaan pola atau intensitas warna antara audio asli dan audio stego yang menunjukkan adanya pesan tersembunyi. Analisis ini juga membantu memastikan keaslian sebuah file audio dan bisa menjadi bukti bahwa file tersebut telah dimodifikasi. Selain itu, perbedaan spektral juga bisa menunjukkan bagian mana dari audio yang telah disisipi pesan.

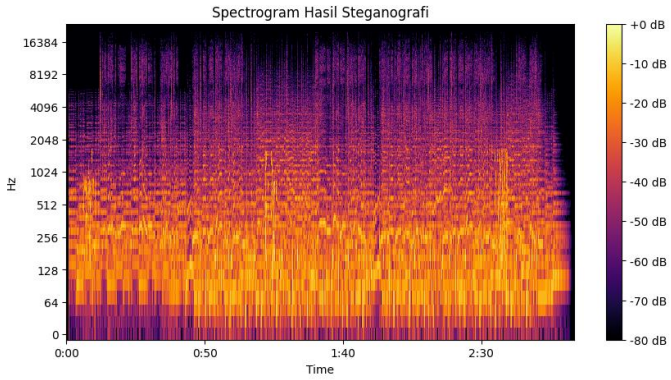
a. Tampilan *Spectrogram* Lagu Bernadya

Pada tahapan ini analisis *Spectrogram* dilakukan guna melihat pola gelombang suara yang diucapkan dari formant setiap kalimat. Pada tampilan *Spectrogram* terlihat perbedaan tingkat energi masing-masing audio. Sehingga bisa mengidentifikasi pola suara dan

gangguan atau anomali dalam sinyal audio. Dikarenakan *Spectrogram* memperlihatkan hal-hal yang bersifat detail, maka sebagian ahli berpendapat bahwa *Spectrogram* merupakan sidik jari suara (*voice fingerprint*). Pada *source code Python* yang dipakai menggunakan fitur *Librosa* untuk menganalisis karateristik *spectrogram* audio asli dengan hasil steganografi.



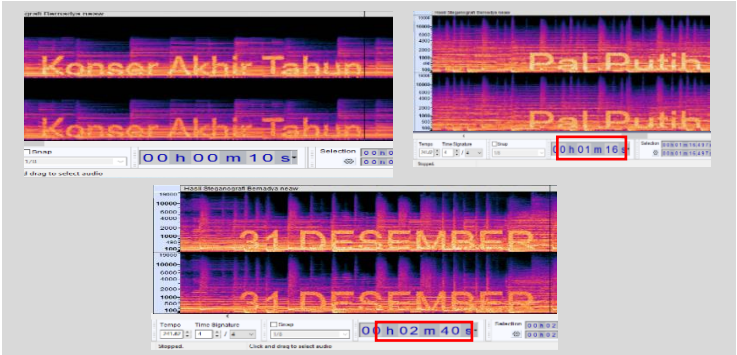
Gambar 4.1 *Spectrogram* audio asli



Gambar 4.2 *Spectrogram* hasil stego

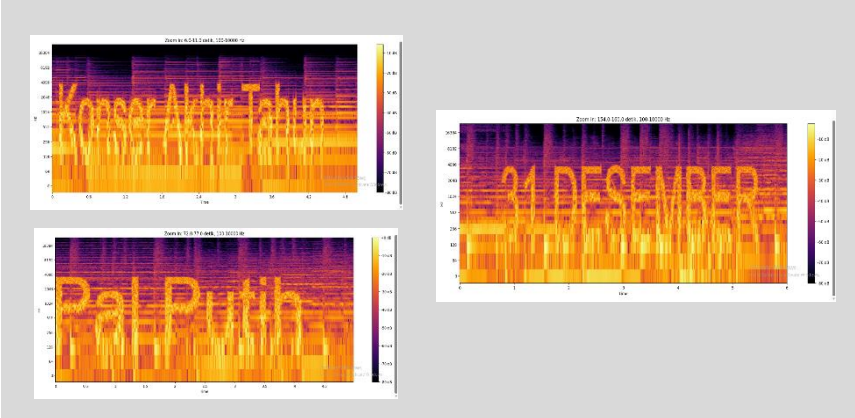
b. Melakukan *Zoom In* ke area *Spectrogram*

Untuk menemukan pesan yang disisipkan di area *spectrogram.* Dilakukan *Zoom In* untuk memperbesar area *spectrogram* audio supaya dapat dengan jelas melihat isi pesan. Seperti pada gambar 4.3 dibawah ini.



Gambar 4.3 *Zoom In Spectrogram* hasil stego menggunakan *Audacity*

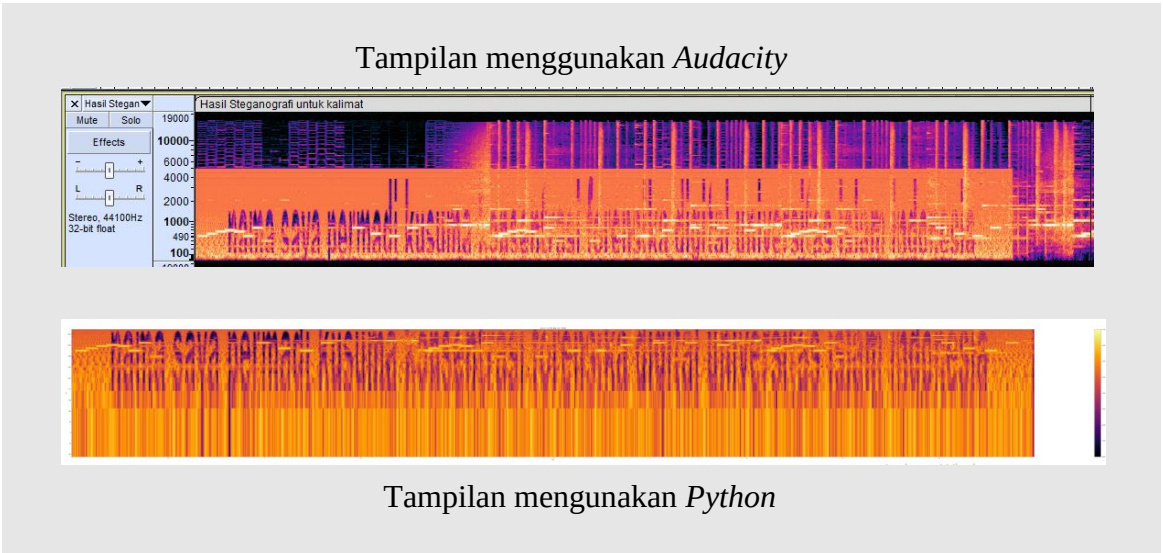
Pada gambar 4.3 menampilkan pesan rahasia pada spectrogram dari lagu *Bernadya*. Pesan tersebut akan nampak jika melalui proses *Zoom in*. Selain menggunakan aplikasi *Audacity*, proses menampilkan pesan rahasia juga dilakukan menggunakan pemrograman *Python* dengan memakai fitur *Librosa* seperti pada gambar 4.4 di bawah ini.



Gambar 4.4 *Zoom In Spectrogram* hasil stego menggunakan *Python*

c. Tampilan Spectrogram Nada Dering Samsung

Implementasi steganografi dilakukan pada nada dering *Samsung Galaxy S3*. Adapun pesan yang disisipkan bertuliskan **"*nama saya permadi kusuma konsentrasi forensika digital universitas islam indonesia*"** dengan jumlah 10 kata, untuk tampilan pesan yang sudah disisipkan dapat dilihat menggunakan fitur *zoom in* pada aplikasi *Audacity* dan melalui *Google Colab* dengan menggunakan script Pemrograman *Python*. Seperti pada gambar di bawah ini.

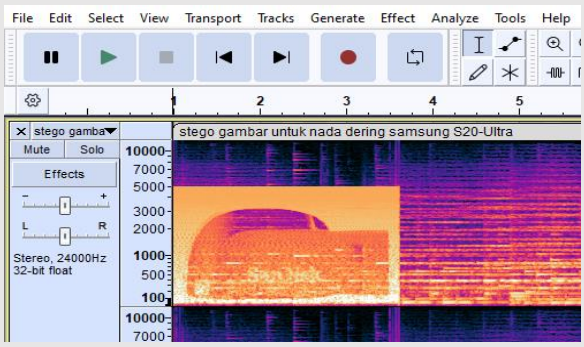


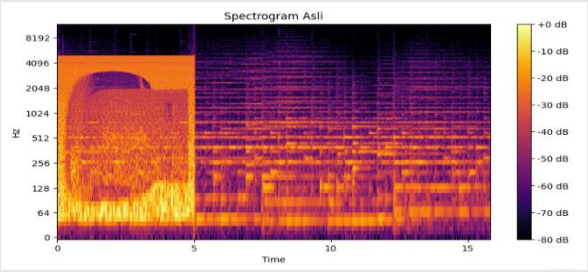
Gambar 4.5 *Zoom In Spectrogram* nada dering Samsung

d. Tampilan *Spectrogram* Nada Dering *Samsung Galaxy S20*

Selain kalimat. Peneliti juga menyisipkan pesan gambar Flashdisk ke area *Spectrogram* nada dering bawaan *Samsung Galaxy S20* yang bisa dilihat pada gambar 4.6. Pesan tersebut akan nampak jika melalui proses *Zoom in.* Selain menggunakan aplikasi *Audacity*, proses menampilkan pesan rahasia juga dilakukan menggunakan pemrograman *Python* dengan memakai fitur *Librosa*.

Tampilan menggunakan *Audacity*





Tampilan menggunakan *Python*

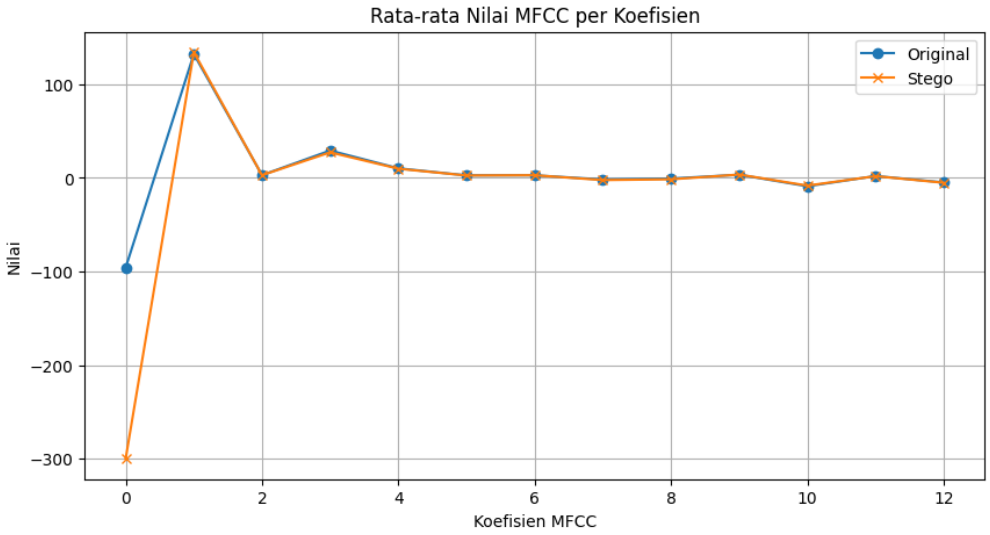
Gambar 4.6 *Zoom In Spectrogram* menampilkan gambar flashdisk

4.1.2 Analisis *MFCC (Mel-Frequency Cepstral Coefficients)*

MFCC (Mel-Frequency Cepstral Coefficients) adalah fitur audio yang mewakili karakteristik suara manusia atau ciri khas suara dalam bentuk angka-angka. *MFCC* sering digunakan dalam Pengenalan suara *(voice recognition)*, analisis sinyal audio dan deteksi perbedaan atau modifikasi dalam audio. Dengan melakukan Analisis *MFCC* maka bisa menangkap perubahan kecil dalam struktur sinyal audio stego dan audio asli. Proses Analisis *MFCC* menggunakan Pemrograman *Python* di *Google Colab.*

a. Analisis *MFCC (Mel-Frequency Cepstral Coefficients)* lagu Bernadya

Berikut ini merupakan hasil analisa *MFCC* dari audio asli lagu *Bernadya* dan hasil steganografi yang menampilkan grafik dan numerik dari kedua file.



Gambar 4.7 Perbandingan grafik *MFCC* audio asli dan steganografi lagu Bernadya

Pada grafik *MFCC* audio asli dan steganografi dari lagu Bernadya menunjukkan perbandingan nilai *MFCC Mean (rata-rata koefisien MFCC)* antara audio original dan audio stego dari lagu *Bernadya*. Dimana garis biru mewakili file audio asli, sedangkan garis oranye mewakili audio stego. Pada Sumbu X merupakan Koefisien *MFCC* dari 0 sampai 12 yang mewakili *MFCC_1* hingga *MFCC_13*. Jadi setiap titik mewakili satu koefisien. Sedangkan sumbu Y merupakan nilai rata-rata (*mean*) yang menunjukkan nilai numerik rata-rata dari masing-masing koefisien. Semakin tinggi nilainya, semakin besar karakteristik energi pada frekuensi tersebut.

Pada koefisien ke-0 (*MFCC_1*) telah terjadi perbedaan sangat besar antara Original dan Stego (turun drastis) yang mengindikasikan perubahan akibat penyisipan pesan. Koefisien ke-1 (*MFCC_2*) menampilkan nilai sangat tinggi di kedua file dan sangat mirip sehingga tidak banyak berubah atau ada sedikit perubahan, sedangkan Koefisien ke-2 sampai ke-12 (*MFCC_3 - MFCC_13*) menunjukkan pola yang hampir identik dan hanya terjadi perubahan kecil.

Tabel 4.1 Nilai MFCC Mean lagu Bernadya

Koefisien MFCC Mean	Original Mean	Stego Mean	Selisih	Keterangan
MFCC 1	-96,02	-300,23	204,20	Berubah
MFCC 2	132,44	134,43	1,99	Berubah
MFCC 3	3,00	2,91	0,09	Berubah
MFCC 4	29,28	27,36	1,92	Berubah
MFCC 5	10,27	9,85	0,42	Berubah
MFCC 6	2,72	2,61	0,11	Berubah
MFCC 7	2,79	2,89	0,10	Berubah
MFCC 8	-1,68	-2,29	0,61	Berubah
MFCC 9	-0,66	-1,44	0,79	Berubah
MFCC 10	3,42	3,60	0,18	Berubah
MFCC 11	-8,87	-8,19	0,68	Berubah
MFCC 12	2,03	1,92	0,11	Berubah
MFCC 13	-4,79	-5,18	0,39	Berubah

Kriteria penilaian dengan memberikan penilaian terhadap besar perubahan (selisih) antara audio original dan stego berdasarkan nilai *MFCC* koefisien *Mean* dan *STD*.

- Jika tidak ada perbedaan (selisih = 0), maka dianggap "Tidak berubah".
- Jika terdapat perbedaan nilai Mean (kurang atau lebih dari 2), maka dianggap "Berubah".

Berdasarkan gambar 4.7 yang menampilkan grafik *MFCC* audio asli dan steganografi dari lagu *Bernadya* telah ditemukan bahwa ada perbedaan nilai *Mean* yaitu rata-rata kekuatan suara pada tiap koefisien frekuensi yang terdapat pada audio stego dan audio asli. Tujuan Analisis *MFCC* yaitu mendeteksi perbedaan halus akibat penyisipan pesan. Nilai tersebut dapat disimpulkan memiliki selisih nilai yang berbeda yang nampak pada tabel 4.1 karena menunjukan seberapa besar selisih energi suara di setiap koefisien frekuensi. Terjadinya perbedaan, karena penyisipan pesan telah mengubah struktur frekuensi, dengan adanya perbedaan nilai *MFCC (Mel-Frequency Cepstral Coefficients)* tersebut maka dapat digunakan untuk mendukung analisis audio steganografi.

Tabel 4.2 Nilai MFCC *STD (Standard Deviation)* lagu Bernadya

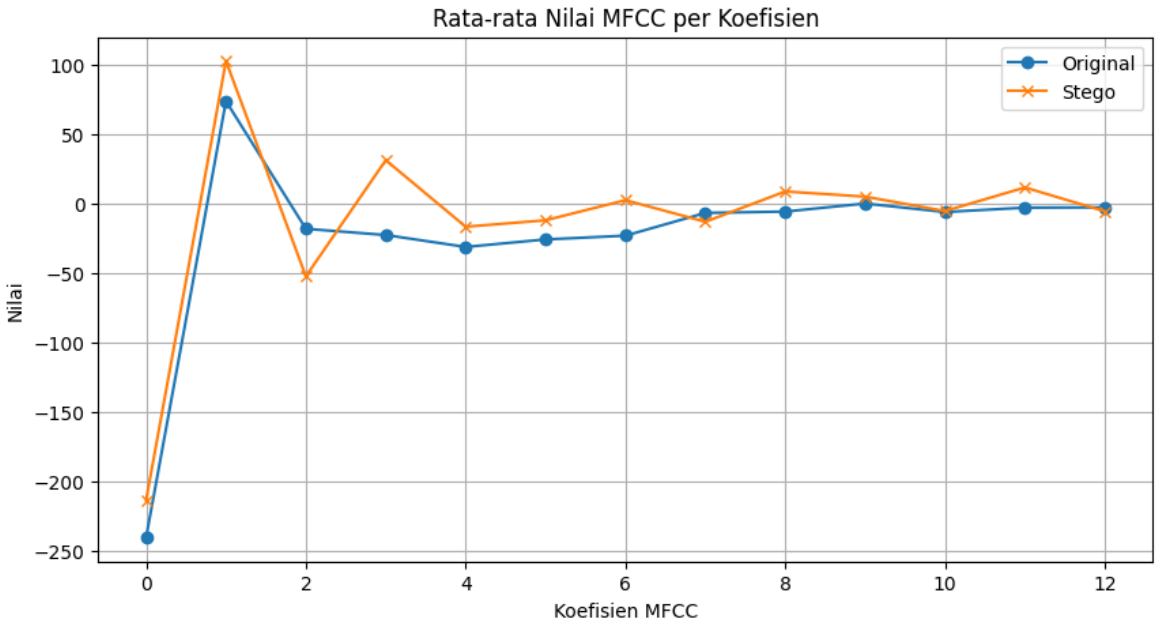
Koefisien MFCC STD	Original STD	Stego STD	Selisih	Keterangan
MFCC 1	89,18	87,54	1,64	Berubah
MFCC 2	37,31	39,93	2,62	Berubah
MFCC 3	24,32	24,69	0,37	Berubah
MFCC 4	15,75	15,82	0,07	Berubah
MFCC 5	10,59	11,93	1,34	Berubah
MFCC 6	11,60	12,59	0,99	Berubah
MFCC 7	9,41	9,97	0,56	Berubah
MFCC 8	9,11	10,01	0,90	Berubah

Koefisien MFCC STD	Original STD	Stego STD	Selisih	Keterangan
MFCC 9	8,13	8,94	0,81	Berubah
MFCC 10	9,68	9,55	0,13	Berubah
MFCC 11	8,36	9,15	0,79	Berubah
MFCC 12	7,12	7,34	0,22	Berubah
MFCC 13	7,95	8,17	0,22	Berubah

Berdasarkan tabel 4.2 telah ditemukan bahwa ada perbedaan nilai *STD (Standard deviation)* yang menunjukkan seberapa bervariasi suara di koefisien yang terdapat pada audio stego dan audio asli. Semakin tinggi nilainya, semakin banyak perubahan atau variasi suara di area frekuensi tersebut seperti yang nampak pada tabel 4.2 karena menunjukan seberapa besar selisih energi suara di setiap koefisien frekuensi. Jika audio stego dari standar deviasi lebih tinggi dari audio asli, bisa jadi ada "noise tak kasat mata" dari akibat pesan disisipkan.

b. Analisis *MFCC (Mel-Frequency Cepstral Coefficients)* nada dering Samsung

Berikut ini merupakan Analisis perbedaan *MFCC (Mel-Frequency Cepstral Coefficients)* pada audio dari nada dering *Samsung Galaxy S3* dan setelah dilakukan proses steganografi dengan menyisipkan kalimat **"nama saya permadi kusuma konsentrasi forensika digital universitas islam indonesia".** Proses Analisis *MFCC* menggunakan *Pemrograman Python di Google Colab* seperti pada gambar 4.8 dibawah ini.



Gambar 4.8 Perbandingan grafik MFCC audio asli dan steganografi nada dering Samsung *Galaxy S3*

Gambar 4.8 menunjukkan perbedaan nilai MFCC secara menyeluruh pada audio asli dan hasil. Pada grafik *MFCC* audio asli dan steganografi dari nada dering Samsung menunjukkan

perbandingan nilai *MFCC Mean (rata-rata koefisien MFCC)* antara audio original dan audio stego dari nada dering Samsung. Dimana garis biru mewakili file audio asli, sedangkan garis oranye mewakili audio stego. Pada Sumbu X merupakan Koefisien *MFCC* dari 0 sampai 12 yang mewakili *MFCC_1* hingga *MFCC_13*. Jadi setiap titik mewakili satu koefisien. Sedangkan sumbu Y merupakan nilai rata-rata (*mean*) yang menunjukkan nilai numerik rata-rata dari masing-masing koefisien. Semakin tinggi nilainya, semakin besar karakteristik energi pada frekuensi tersebut.

Pada koefisien ke-0 (*MFCC_1*) telah terjadi perbedaan nilai antara Original dan Stego yang mengindikasikan perubahan akibat penyisipan pesan dengan selisih 26,91. Koefisien ke-1 (*MFCC_2*) menampilkan selisih 28,96 di kedua file sehingga mengindikasikan adanya perubahan nilai. Sedangkan Koefisien ke-2 sampai ke-12 (*MFCC_3 - MFCC_13*) menunjukkan beberapa naik-turun antara Stego dan Original. Untuk mendapatkan analisis yang lebih mendalam, dilakukan analisis *Mean* dan *STD* pada audio asli dan hasil stego yang bisa dilihat pada tabel 4.3 dan 4.4.

Tabel 4.3 Nilai MFCC Mean nada dering *Samsung Galaxy S3*

Koefisien MFCC Mean	Original Mean	Stego Mean	Selisih	Keterangan
MFCC 1	-240,79	-213,87	26,91	Berubah
MFCC 2	74,13	103,09	28,96	Berubah
MFCC 3	-17,96	-52,24	34,28	Berubah
MFCC 4	-22,46	31,57	54,02	Berubah
MFCC 5	-31,06	-16,47	14,59	Berubah
MFCC 6	-25,64	-11,82	13,81	Berubah
MFCC 7	-22,92	2,70	25,63	Berubah
MFCC 8	-6,49	-12,91	6,43	Berubah
MFCC 9	-5,53	8,99	14,52	Berubah
MFCC 10	0,29	5,23	4,95	Berubah
MFCC 11	-5,85	-5,13	0,73	Berubah
MFCC 12	-2,71	11,86	14,56	Berubah
MFCC 13	-2,51	-5,38	2,87	Berubah

Berdasarkan gambar 4.8 yang menampilkan grafik *MFCC* audio asli dan steganografi dari nada dering *Samsung Galaxy* telah ditemukan bahwa ada perbedaan nilai Mean yaitu rata-rata kekuatan suara pada tiap koefisien frekuensi yang terdapat pada audio stego dan audio asli. Nilai tersebut dapat disimpulkan memiliki selisih nilai yang berbeda yang nampak pada tabel 4.3 karena menunjukan seberapa besar selisih energi suara di setiap koefisien frekuensi. Terjadinya perbedaan nilai, karena penyisipan pesan telah mengubah struktur frekuensi, dengan adanya perbedaan nilai *MFCC (Mel-Frequency Cepstral Coefficients)* tersebut maka dapat digunakan untuk mendukung analisis audio steganografi.

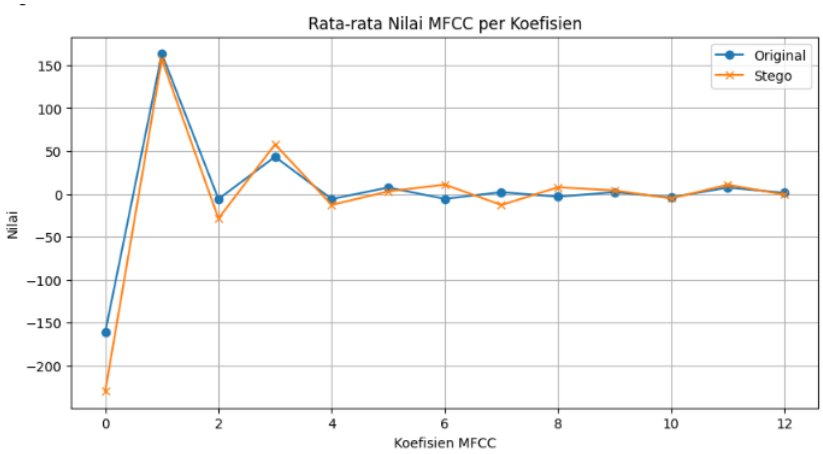
Tabel 4.4 Nilai *MFCC STD (Standard Deviation)* nada dering *Samsung Galaxy S3*

Koefisien MFCC	Original STD	Stego STD	Selisih	Keterangan
MFCC 1	141,19	145,68	4,49	Berubah
MFCC 2	37,02	42,44	5,42	Berubah
MFCC 3	26,60	32,40	5,80	Berubah
MFCC 4	18,85	47,39	28,54	Berubah
MFCC 5	15,47	19,96	4,50	Berubah
MFCC 6	13,59	17,54	3,95	Berubah
MFCC 7	13,28	16,83	3,55	Berubah
MFCC 8	12,36	14,33	1,97	Berubah
MFCC 9	14,24	17,46	3,22	Berubah
MFCC 10	12,83	12,70	0,13	Berubah
MFCC 11	10,87	8,18	2,70	Berubah
MFCC 12	14,95	10,92	4,03	Berubah
MFCC 13	15,06	12,72	2,34	Berubah

Berdasarkan tabel 4.4 telah ditemukan bahwa ada perbedaan nilai *STD (Standard deviation)* yang menunjukkan seberapa bervariasi suara di koefisien yang terdapat pada audio stego dan audio asli. Semakin tinggi nilainya, semakin banyak perubahan atau variasi suara di area frekuensi tersebut, karena menunjukan seberapa besar selisih energi suara di setiap koefisien frekuensi.

c. Analisis *MFCC (Mel-Frequency Cepstral Coefficients)* nada dering Samsung Galaxy S20

Selain menyisipkan kalimat. Peneliti juga menyisipkan gambar *Flashdisk* merk *Sandisk* pada area Spectrogram nada dering Samsung Galaxy S20. Untuk perbandingan grafik *MFCC* audio asli dengan steganografi tidak jauh berbeda, ini bisa dilihat pada gambar 4.9. Untuk tabel perbandingan dapat dilihat melalui tabel 4.5 dan tabel 4.6.



Gambar 4.9. Perbandingan grafik *MFCC* audio asli dan steganografi gambar *Flashdisk*

Gambar 4.9 menunjukkan perbedaan nilai *MFCC* secara menyeluruh pada audio asli dan hasil stego gambar *Flashdisk* merk *Sandisk* . Pada grafik *MFCC* audio asli dan steganografi dari nada dering Samsung Galaxy S20 menunjukkan perbandingan nilai *MFCC Mean (rata-rata koefisien MFCC)* antara audio original dan audio stego dari nada dering Samsung Galaxy S20. Dimana garis biru mewakili file audio asli, sedangkan garis oranye mewakili audio stego. Pada Sumbu X merupakan Koefisien *MFCC* dari 0 sampai 12 yang mewakili *MFCC_1* hingga *MFCC_13*. Jadi setiap titik mewakili satu koefisien. Sedangkan sumbu Y merupakan nilai rata-rata (*mean*) yang menunjukkan nilai numerik rata-rata dari masing-masing koefisien. Semakin tinggi nilainya, semakin besar karakteristik energi pada frekuensi tersebut.

Pada koefisien ke-0 (*MFCC_1*) telah terjadi perbedaan kecil antara Original dan Stego yang mengindikasikan perubahan akibat penyisipan pesan. Koefisien ke-1 (*MFCC_2*) menampilkan selisih 68,89 di kedua file, begitupun Koefisien ke-2 sampai ke-12 (*MFCC_3 - MFCC_13*) menunjukkan beberapa naik-turun antara Stego dan Original. Untuk mendapatkan analisis yang lebih mendalam, dilakukan analisis *Mean* dan *STD* pada audio asli dan hasil stego yang bisa dilihat pada tabel 4.5 dan 4.6.

Tabel 4.5 Nilai *MFCC* Mean steganografi gambar pada nada dering *Samsung S20*

Koefisien MFCC Mean	Original Mean	Stego Mean	Selisih	Keterangan
MFCC 1	-160,78	-229,66	68,89	Berubah
MFCC 2	163,08	156,60	6,48	Berubah
MFCC 3	-5,98	-28,62	22,64	Berubah
MFCC 4	43,22	57,60	14,39	Berubah
MFCC 5	-5,94	-12,75	6,81	Berubah
MFCC 6	7,42	2,88	4,54	Berubah
MFCC 7	-5,75	10,85	16,61	Berubah
MFCC 8	2,03	-12,91	14,94	Berubah
MFCC 9	-3,27	7,73	11,01	Berubah
MFCC 10	1,99	4,06	2,07	Berubah
MFCC 11	-4,04	-5,33	1,29	Berubah
MFCC 12	7,42	10,73	3,31	Berubah
MFCC 13	1,23	-0,91	2,14	Berubah

Tabel 4.6 Nilai *MFCC* STD steganografi gambar pada nada dering *Samsung S20*

Koefisien MFCC STD	Original STD	Stego STD	Selisih	Keterangan
MFCC 1	40,53	97,24	56,71	Berubah
MFCC 2	22,12	16,51	5,61	Berubah
MFCC 3	8,39	44,76	36,37	Berubah
MFCC 4	10,37	31,45	21,08	Berubah
MFCC 5	7,33	21,54	14,21	Berubah

Koefisien MFCC STD	Original STD	Stego STD	Selisih	Keterangan
MFCC 6	6,13	12,35	6,22	Berubah
MFCC 7	6,68	22,01	15,32	Berubah
MFCC 8	6,33	20,68	14,34	Berubah
MFCC 9	6,71	12,45	5,75	Berubah
MFCC 10	6,78	9,30	2,52	Berubah
MFCC 11	7,45	9,87	2,41	Berubah
MFCC 12	6,54	9,93	3,39	Berubah
MFCC 13	6,54	9,01	2,47	Berubah

Kriteria penilaian dengan memberikan penilaian terhadap besar perubahan (selisih) antara audio original dan stego berdasarkan nilai *MFCC* koefisien *Mean* dan *STD*.

- Jika tidak ada perbedaan (selisih = 0), maka dianggap "Tidak berubah".
- Jika terdapat perbedaan nilai Mean (kurang atau lebih dari 2), maka dianggap "Berubah".

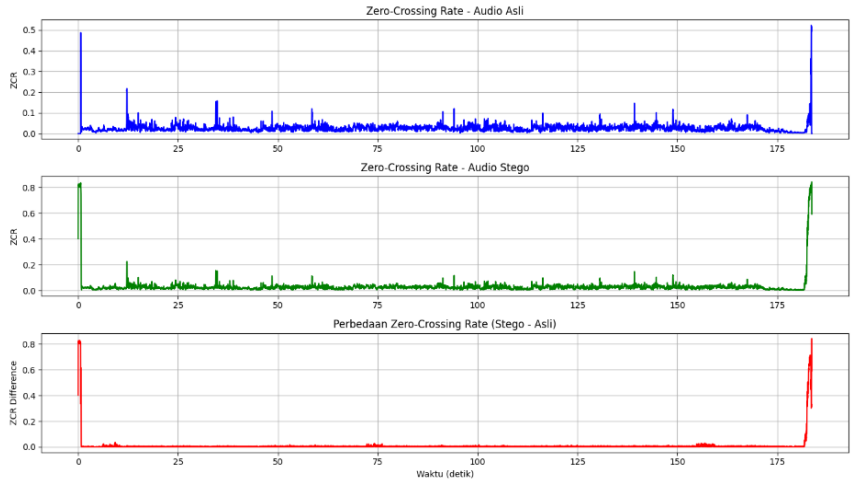
Berdasarkan tabel 4.5 dan tabel 4.6 telah ditemukan bahwa ada perbedaan nilai *Mean* dan *STD (Standard deviation)* yang menunjukkan seberapa bervariasi suara di koefisien yang terdapat pada audio stego dan audio asli. Semakin tinggi nilainya, semakin banyak perubahan atau variasi suara di area frekuensi tersebut, karena menunjukan seberapa besar selisih energi suara di setiap koefisien frekuensi. Jika audio stego dari standar deviasi lebih tinggi dari audio asli, bisa jadi ada "noise tak kasat mata" dari akibat pesan disisipkan.

Pada analisis *MFCC (Mel-Frequency Cepstral Coefficients)* dari audio steganografi lagu *Bernadya* yang terdapat pesan "konser akhir tahun", "pal putih" dan "31 desember", nada dering *Samsung Galaxy* yang terdapat pesan "nama saya permadi kusuma konsentrasi forensika digital universitas islam indonesia" dan nada dering *Samsung Galaxy S20* yang disisipkan gambar *Flashdisk* merk *Sandisk* dengan audio asli secara menyeluruh. Ditemukan nilai *MFCC Mean* dan *STD* dengan hasil yang berbeda dengan audio aslinya. Sehingga pada analisis *MFCC* ini disimpulkan bahwa audio asli dan hasil stego mengalami perbedaan akibat adanya proses steganografi.

4.1.3 Analisis *ZCR (Zero-Crossing Rate)*

Analisis ini didasarkan pada seberapa sering sinyal audio melintasi garis nol dalam satuan waktu. Dengan membandingkan *ZCR* antara audio asli dan audio yang telah disisipi pesan, maka dapat melihat apakah ada peningkatan atau pola yang tidak biasa. Jika karakteristik audio asli dan hasil stego tersebut menunjukkan tingkat perbedaan yang besar, maka dapat disimpulkan bahwa *Analisis Zero-Crossing Rate* dari audio asli dan hasil stego adalah berbeda. Proses Analisis *ZCR* menggunakan Pemrograman *Python* di *Google Colab.*

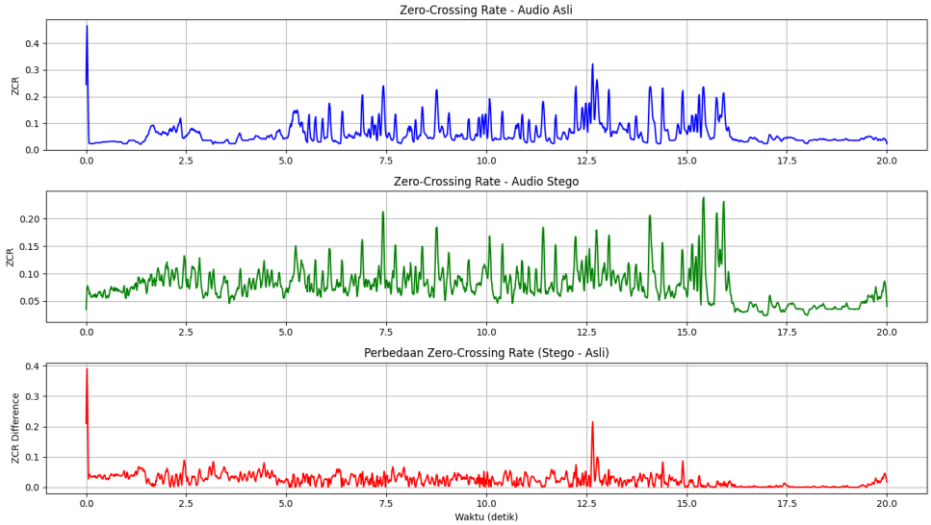
a. Analisis Steganografi *Zero-Crossing Rate* lagu Bernadya



Gambar 4.10 Grafik *ZCR* audio asli dan steganografi Bernadya

Pada tahapan ini, analisis *ZCR* di gunakaan untuk melihat pola umum audio asli dengan hasil stego dari lagu *Bernadya*. Grafik pertama (biru) menunjukkan *ZCR* dari audio asli, kedua (hijau) dari audio stego, dan ketiga (merah) mewakili perbandingan dari audio asli dan stego. Jika ada lonjakan atau pola perbedaan yang tidak biasa di grafik ketiga, itu bisa mengindikasikan adanya penyisipan data. Sehingga pada tahapan ini kan jelas terlihat tingkat suatu energi dari masing-masing audio. Apabila menunjukkan adanya perbedaan grafik antara audio stego dengan audio asli maka dapat disimpulkan bahwa file tersebut memiliki spectrogram yang berbeda.

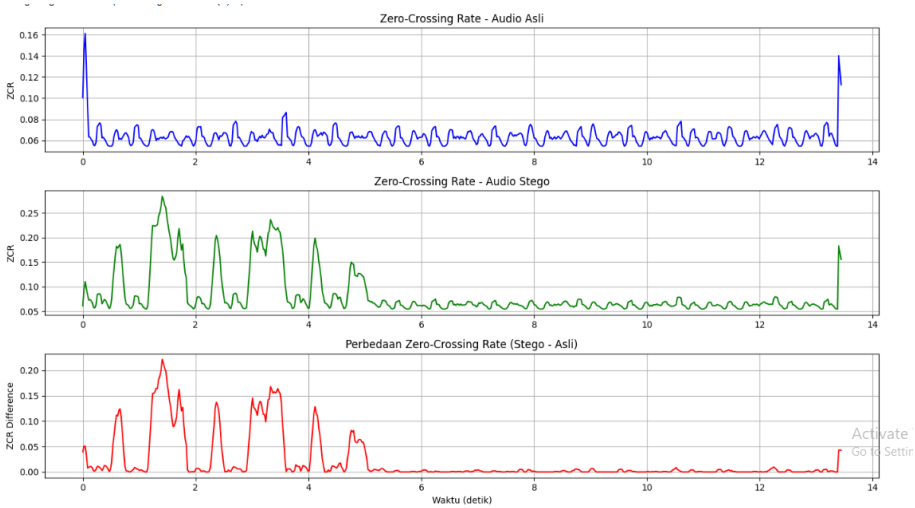
b. Analisis Steganografi *Zero-Crossing Rate* nada dering *Samsung*



Gambar 4.11 Grafik *ZCR* audio asli dan steganografi nada dering Samsung S3

Gambar 4.11 menunjukkan tingkat perbedaa grafik audio asli dan stego dari nada dering Samsung yang terdapat pesan "nama saya permadi kusuma konsentrasi forensika digital

universitas islam indonesia". Pada gambar tersebut terlihat pola perbedaan yang tidak biasa pada Grafik pertama (biru) menunjukkan *ZCR* dari audio asli, kedua (hijau) dari audio stego, dan ketiga (merah) mewakili perbandingan dari audio asli dan stego. Selain menyisipkan pesan dalam bentuk kalimat, dilakukan juga penyisipan gambar *Flashdisk*. Berikut grafik audionya yang bisa dilihat pada gambar 4.12.



Gambar 4.12 Grafik *ZCR* audio asli
dan steganografi nada dering Samsung Galaxy S20

Gambar 4.12 menunjukkan tingkat perbedaa grafik audio asli dan stego dari nada dering Samsung Galaxy S20 yang terdapat pesan stego. Pada gambar tersebut terlihat pola perbedaan yang tidak biasa pada Grafik pertama (biru) menunjukkan *ZCR* dari audio asli, kedua (hijau) dari audio stego, dan ketiga (merah) mewakili perbandingan dari audio asli dan stego. Pada analisis *ZCR (Zero-Crossing Rate)* dari audio yang dianalisis yaitu lagu *Bernadya*, nada dering *Samsung Galaxy*, dan nada dering *Samsung Galaxy S20* dengan audio stego secara menyeluruh, ditemukan perbandingan grafik *ZCR* dengan hasil yang berbeda dengan audio aslinya. Sehingga pada analisis *ZCR (Zero-Crossing Rate)* disimpulkan bahwa audio asli dan hasil stego mengalami perbedaan akibat adanya proses steganografi.

4.2 Hasil pengujian penyisipan informasi rahasia ke dalam audio

Berikut merupakan tabel hasil penyisipan informasi rahasia ke dalam lagu Bernadya dengan Samsung.

Tabel 4.7 Hasil penyisipan informasi rahasia ke dalam audio

Isi informasi rahasia	Size audio stego	Audio penampung (mp3)	Size audio asli	Size audio hasil stego	Hasil
Konser Akhir Tahun, Pal Putih, 31 Desember.	1.03 MB	Lagu Bernadya - Hidup Harus Tetap Berjalan.mp3	7.01 mb	33.6 mb	Berhasil
Nama saya Permadi Kusuma konsentrasi forensika digital Universitas Islam Indonesia	1.25 mb	Nada Dering Samsung Galaxy S3.mp3	317 kb	3.36 mb	Berhasil
	432 kb	Nada Dering Samsung Galaxy S20 Ultra.mp3	263 kb	1.23 mb	Berhasil

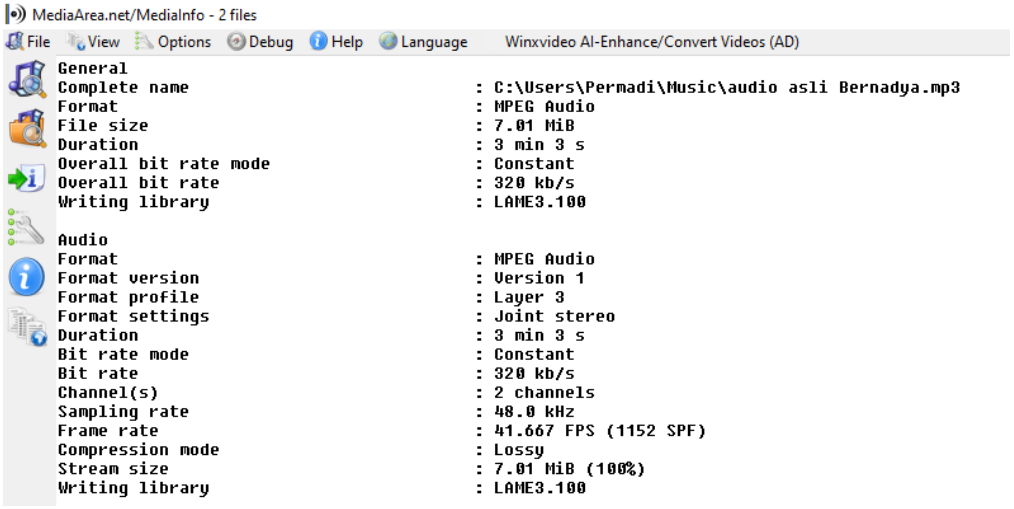
Pada Tabel 4.7 menampilkan ukuran audio setelah dilakukan proses stego dapat menambah size lagu, seperti pada lagu *Bernadya* yang awalnya 7.01 MB menjadi 33.6 MB dan Nada Dering *Samsung* 317 kb menjadi 3.36 mb. Selain teks, proses steganografi dilakukan juga pada gambar flashdisk dengan size 432 kb pada audio sampel nada dering *Samsung Galaxy S20* dengan size 263 kb menjadi 1.23 mb. Hasil yang didapat menunjukkan penyisipan ketiga informasi rahasia ke dalam lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*" , "Nada Dering *Samsung Galaxy S3"*, dan "Nada dering *Samsung Galaxy S20*" telah berhasil. Untuk mengetahui penyebab audio mengalami perubahan size maka dilakukan analisis meta data.

4.2.1 Analisis Metadata

Analisis metadata audio asli dan hasil stego dilakukan guna melihat perbedaan metadata dari kedua file dikarenakan terdapat penambahan size setelah dilakukan proses steganografi. Analisis metadata menggunakan *Software Mediainfo*. Metadata yang tampil berisi informasi rinci seperti format file, sample rate, durasi, *bitrate*, dan channel, yang semuanya dapat memengaruhi ukuran akhir file. Dengan membandingkan metadata sebelum dan sesudah penyisipan pesan, peneliti dapat mengidentifikasi apakah peningkatan ukuran disebabkan

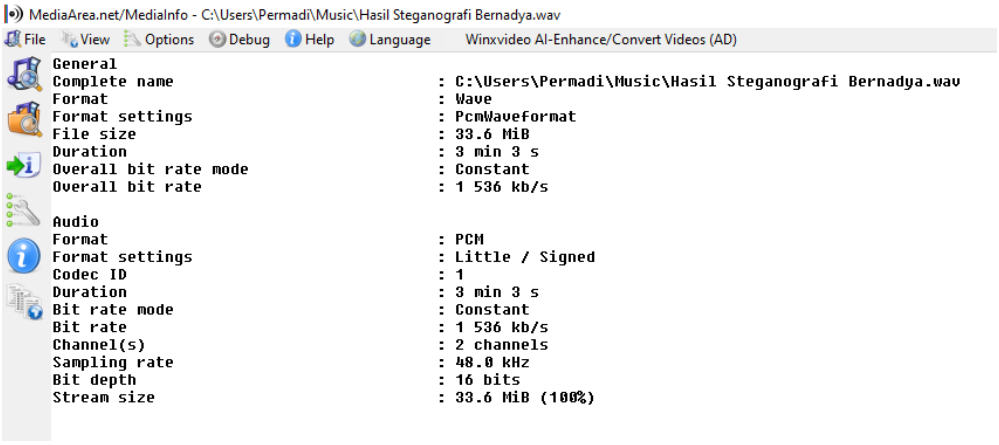
oleh perubahan pada parameter teknis seperti peningkatan *bitrate*, penambahan channel, atau penggunaan format encoding yang berbeda (dari *MP3* ke *WAV*).

1. Analisis metadata lagu Bernadya



Gambar 4.13 Metadata audio asli lagu Bernadya

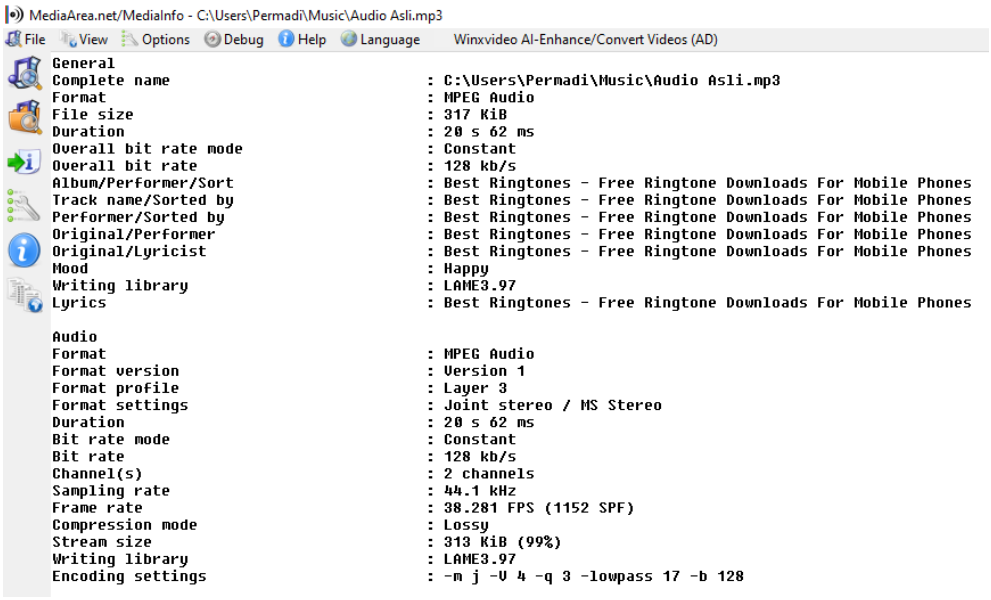
Pada gambar 4.13 menampilkan metadata dari file lagu *Bernadya* yang belum dilakukan proses steganografi. Size audio memiliki ukuran 7.01 mb dengan durasi 3 menit 3 detik. *Overall bit rate* 320 kb/s.



Gambar 4.14 Metadata audio stego lagu Bernadya

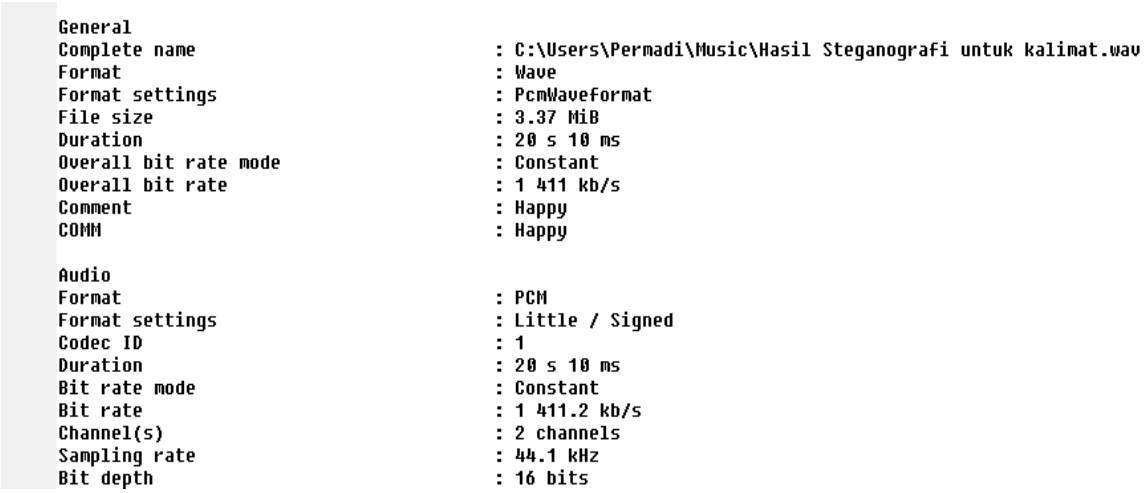
Pada gambar 4.14 menampilkan metadata dari file lagu *Bernadya* yang sudah dilakukan proses steganografi. Size audio memiliki ukuran 33.6 mb dengan durasi 3 menit 3 detik. *Overall bit rate* 1536 kb/s.

2. Analisis metadata nada dering Samsung Galaxy S3



Gambar 4.15 Metadata nada dering *Samsung Galaxy S3*

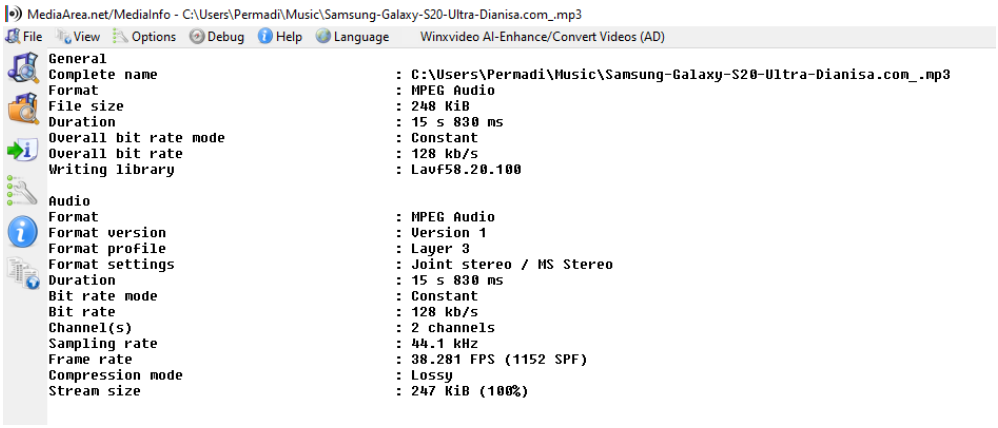
Pada gambar 4.15 menampilkan metadata dari file nada dering *Samsung* Galaxy S3 yang belum dilakukan proses steganografi. Size audio memiliki ukuran 317 kb dengan durasi 20 detik. *Overall bit rate* 128 kb/s.



Gambar 4.16 Metadata audio stego nada dering *Samsung Galaxy S3*

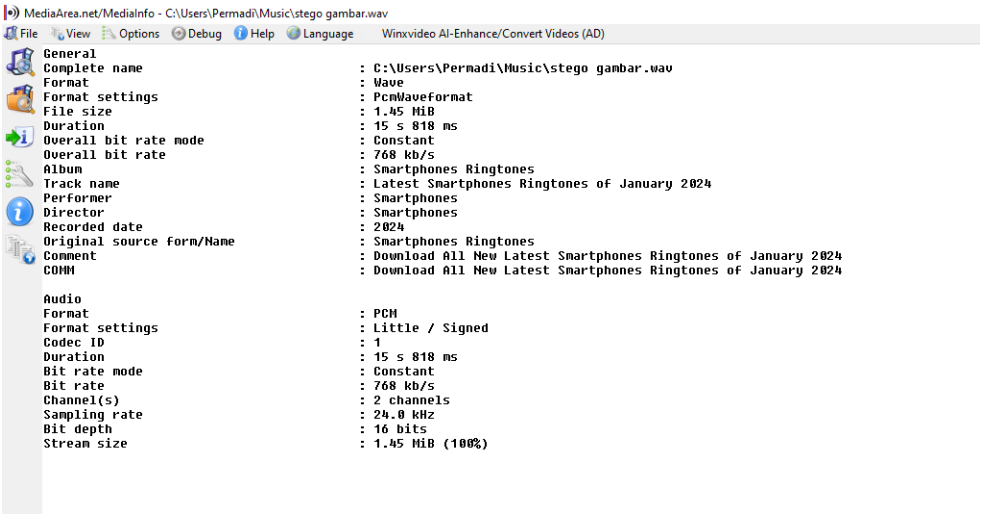
Pada gambar 4.16 menampilkan metadata dari file nada dering Samsung *Galaxy S3* yang sudah dilakukan proses steganografi. Hasilnya file stego yang terdapat pesan rahasia dalam bentuk teks memiliki size audio 3.37 mb dengan durasi 20 detik. *Overall bit rate* 1411 kb/s.

3. Analisis metadata nada dering *Samsung Galaxy S20*



Gambar 4.17 Metadata audio nada dering *Samsung Galaxy S20*

Pada gambar 4.17 menampilkan metadata dari file nada dering *Samsung Galaxy S20* yang belum dilakukan proses steganografi. Size audio memiliki ukuran 248 kb dengan durasi 15 detik. Overall bit rate 128 kb/s.



Gambar 4.18 Metadata audio stego nada dering *Samsung Galaxy S20*

Pada gambar 4.18 menampilkan metadata dari file nada dering Samsung Galaxy S20 yang sudah dilakukan proses steganografi. Hasilnya file stego yang terdapat pesan rahasia dalam bentuk gambar memiliki size audio 1.45 mb dengan durasi 15 detik. *Overall bit rate* 768 kb/s.

Dari analisis metadata audio asli dan stego dapat diketahui bahwa proses steganografi audio melalui *Spectrogram* dapat menambah *Overall bit rate* audio Lagu *Bernadya* yang awalnya 320 kb/s menjadi 1536 kb/s, nada dering *Samsung Galaxy S3* 128 kb menjadi 1411

kb/s, dan nada dering *Samsung Galaxy S20* 248 kb/s menjadi 768 kb/s. Menurut sumber dari *Wikipedia*, standar *bitrate* untuk lagu berformat *MP3* bervariasi antara 32 kbps hingga 320 kbps, tergantung pada kualitas kompleksitas audio. *Bitrate* yang umum digunakan untuk musik adalah 128 kbps sebagai kualitas minimum, 192–256 kbps untuk kualitas sedang, dan 320 kbps sebagai bitrate tertinggi yang mendekati kualitas CD. Sedangkan pada buku [36] dengan judul *" Diminishing returns of higher mp3 bit"* menjelaskan bahwa sebagian besar pendengar audio tidak dapat membedakan antara file *MP3* dengan *bitrate* 128 kbps dan audio tanpa kompresi. Namun, pada bitrate 48 kbps, perbedaan kualitas menjadi jelas. Ini menunjukkan bahwa 128 kbps dianggap sebagai titik optimal antara kualitas dan ukuran file untuk audio umum, termasuk nada dering.

Adanya penambahan bitrate pada audio stego dikarenakan adanya perubahan format audio *MP3* ke *WAV*. Format *WAV* menyimpan data lebih banyak per detik dibanding *MP3*. sehingga *WAV* membawa lebih banyak data per detik dibandingkan MP3. Selain itu, analisis *MFCC (Mel-Frequency Cepstral Coefficients)* nilai *Mean dan* Standar Deviasi menampilkan grafik dan nilai numerik audio asli dengan hasil stego yang berbeda yaitu terdapat perubahan pada setiap koefisien. Pada analisis *ZCR (Zero-Crossing Rate)* juga menunjukkan perbandingan pada grafik *ZCR* audio asli dan stego, sehingga dapat disimpulkan bahwa ukuran audio bertambah setelah dilakukan proses steganografi dikarenakan adanya perubahan format audio misalnya *MP3* ke *WAV* dan juga adanya penyatuan file stego yang digabung dengan file audio asli.

BAB 5

Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil yang didapat pada proses Steganografi dengan menggunakan teknik Masking dapat ditarik beberapa kesimpulan:

1. Implementasi steganografi ke dalam *Spectrogram* audio lagu Bernadya, nada dering Samsung dan nada dering *Samsung Galaxy S20* menggunakan teknik *Masking* melalui *Spectrogram* audio telah berhasil. Teknik masking terbukti dapat diimplementasikan secara efektif untuk menyisipkan pesan tersembunyi ke dalam spectrogram audio. Dalam konteks forensik digital, pendekatan kuantitatif memungkinkan identifikasi adanya perubahan yang mengindikasikan pesan tersembunyi, meskipun tidak terdengar oleh telinga manusia.
2. Berdasarkan analisis steganografi audio yang dilakukan menunjukkan bahwa Spectrogram memperlihatkan pola visual tambahan yang tidak terdapat pada audio asli. Parameter akustik seperti *MFCC (Mel-Frequency Cepstral Coefficients) dan ZCR (Zero-Crossing Rate)* juga menunjukkan perbedaan nilai rata-rata dan standar deviasi yang berbeda, sehingga mengindikasikan adanya modifikasi spektrum akibat proses penyisipan. Selain itu, metadata file audio asli dengan stego menunjukkan perubahan size dan *Overall bit rate* pada audio stego. Sehingga hasil analisis menunjukkan karakteristik audio asli berbeda dibandingkan dengan hasil stego.
3. Pada teknik *Masking* yang diimplementasikan pada media audio masih terdapat kekurangan yaitu hasil analisis menunjukkan bahwa karakteristik audio asli dengan audio stego memiliki perbedaan pada gelombang suara, size audio dan *Overall bit rate*.

5.2 Saran

Adapun saran-saran yang bisa diberikan dari hasil penelitian ini adalah sebagai berikut:

1. Teknik steganograf masking masih sangat tergantung dengan perbaikan kualitas audio dari file media penampung yang diperoleh, sehingga diperlukan kajian yang lebih lanjut dalam memperbaiki kualitas audio agar penyisipan pesan berhasil tanpa menimbulkan kecurigaan pihak lainnya.
2. Perlu studi lanjutan untuk mengembangkan deteksi otomatis visual pattern *spectrogram*.
3. Penentuan hasil pengujian pada teknik masking masih dilakukan secara eksperimen, sehingga hasil analisis tergantung dari pengujian yang dipakai.

4. Pada penelitian terkait steganografi selanjutnya, diharap bisa mencoba jenis audio yang berbeda seperti rekaman suara dan juga menggunakan deteksi steganografi otomatis berbasis *Machine Learning (ML)*.

Daftar Pustaka

[1] S. Santoso, A. Arisman, and W. Sentanu, "Steganografi Audio (Wav) Menggunakan Metode Lsb (Least Significant Bit)," *CCIT J.*, vol. 9, no. 2, pp. 214–224, 2016, doi: 10.33050/ccit.v9i2.500.

[2] T. Y. Moh Azhar Ulum, "Implementasi Audio Steganografi Menggunakan Algoritma Discrete Cosine Transform," *J. Teknoinfo*, vol. 17, no. 1, p. 10, 2023, doi: 10.33365/jti.v17i1.2232.

[3] Andi Nugroho, "Peretas Bereksperimen Tanam Malware di File Audio WAV." indonesia. [Online]. Available: https://cyberthreat.id/read/3414/Peretas-Bereksperimen-Tanam-Malware-di-File-Audio-WAV

[4] S. Rohayah, "Implementasi Teknik Steganography Pada File Gambar Dan Audio Dengan Menggunakan Metode LSB," *OKTAL J. Ilmu Komput. dan Sci.*, vol. 2, no. 2, pp. 496–503, 2022, [Online]. Available: https://journal.mediapublikasi.id/index.php/oktal/article/view/1073/948

[5] A. W. Laksono, S. Suhada, and A. Zakaria, "Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab," vol. 4, no. 1, 2024.

[6] N. Q. Fitriyah and Y. Y. Prayudi, "Implementasi Steganografi Audio File Wav Dengan Metode Discrete Cosine Transform (DCT)," *Pros. SENSEI*, vol. 1, no. 1, pp. 144–153, 2017.

[7] D. El Rezen Purba and Desinta Purba, "Text Insertion By Utilizing Masking-Filtering Algorithms As Part of Text Message Security," *J. Info Sains Inform. dan Sains*, vol. 11, no. 1, pp. 1–4, 2021, doi: 10.54209/infosains.v11i1.18.

[8] F. Ro'isa and I. M. Suartana, "Implementasi Steganografi dengan Menggunakan Metode Masking and Filtering untuk Menyisipkan Gambar ke dalam Citra Digital," *J. Informatics Comput. Sci.*, vol. 1, no. 01, pp. 9–15, 2019, doi: 10.26740/jinacs.v1n01.p9-15.

[9] P. Kusuma and Y. Prayudi, "Implementasi Steganografi Dengan Menggunakan Metode Masking And Filtering Untuk Menyisipkan Pesan Ke Dalam Spectrogram Audio," *Ajie*, vol. 9, no. January, pp. 1–15, 2025, doi: 10.20885/ajie.vol9.iss1.art1.

[10] D. A. N. Suryadi, N. Yuniarti, and S. D. N. Faridah, "Perbandingan Metode LSB dan DCT dalam Implementasi Steganografi pada Citra Digital," *Researchgate*, no.

July, pp. 1–5, 2022, [Online]. Available: https://www.researchgate.net/publication/362091653_Perbandingan_Metode_LSB_dan_DCT_dalam_Implementasi_Steganografi_pada_Citra_Digital?_sg=83w3ZWL_kuyid_2VK8BOVQtrgYK8s7s89H4U3EkIgTno2PTofBLIqtlH2Z77YzAXbsRRyhteX6TCX6g&_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6I

[11] Lilik Widyawati, "IMPLEMENTASI METODE STEGANOGRAFI SLT-DCT PADA CITRA UNTUK MENINGKATKAN KUALITAS CITRA STEGANOGRAFI," pp. 1–19, 2019.

[12] G. Ria, "Studi Perbandingan Steganografi pada Audio , Video , dan Gambar," p. 9, 2010.

[13] A. D. Hendrata and A. Prihanto, "Analisis Kualitas Suara Stego Audio Penyisipan Informasi Tersembunyi dengan Metode Least Significant Bit," *J. Informatics Comput. Sci.*, vol. 2, no. 03, pp. 178–184, 2021, doi: 10.26740/jinacs.v2n03.p178-184.

[14] I. D. Lestari, H. Halimatusha'diah, and F. A. Puji Lestari, "Penggunaan Media Audio, Visual, Audiovisual, dalam Meningkatkan Pembelajaran kepada Guru-guru," *J. PkM Pengabdi. Kpd. Masy.*, vol. 1, no. 01, p. 55, 2018, doi: 10.30998/jurnalpkm.v1i01.2361.

[15] N. Faujiah, Septiani. A.N, T. Putri, and U. Setiawan, "Kelebihan dan Kekurangan Jenis-Jenis Media Pembelajaran," *J. Telekomun. Kendala dan List.*, vol. 3, no. 2, pp. 81–87, 2022.

[16] Mustika, "Media Pembelajaran Sistem Audio Untuk Pemberdayaan Pendidikan Di Komunitas Masyarakat," *J. Masy. Telemat. dan Inf.*, vol. 6, no. 1, pp. 57–68, 2015.

[17] Z. Abidin, "Eksperimentasi Media Audio-Visual Pada Pembelajaran Bahasa Arab Dalam Meningkatkan Maharatul Istima' Di MTsN Sleman Kota D.I.Yogyakarta.," *J. Fak. Tarb. UIN Sunan Kalijaga Yogyakarta*, 2009.

[18] S. Putri, Vera Rizchi Cahyani, "Analisis Rekaman Suara Menggunakan Teknik Audio Forensik Untuk Keperluan Barang Bukti Digital," *Unnes Phys. J.*, vol. 3, no. 1, pp. 51–59, 2014.

[19] H. Hendra and S. Rasio henim, "Teknik Audio Forensik untuk Analisis Rekaman Suara sebagai Barang Bukti Digital," *J. Komput. Terap.*, vol. 7, no. 2, pp. 210–217, 2021, doi: 10.35143/jkt.v7i2.4981.

[20] A. Subki, M. N. Karim, and B. Imran, "Analisis Rekaman Suara pada Aplikasi

Magic Call dengan Metode Forensik Audio untuk Mendapatkan Bukti Digital," *J. SAINTEKOM*, vol. 13, no. 2, pp. 111–122, 2023, doi: 10.33020/saintekom.v13i2.373.

[21] Hermann von Helmholtz, "Sensations of Tone as a Physiological Basis for the Theory of Music," *J. Res. Music Educ.*, vol. 3, no. 1, pp. 74–74, 1955, doi: 10.2307/3344431.

[22] G. M. Marevson, "Implementasi Audio Steganografi dalam Penyembunyian Pesan Rahasia," 2024.

[23] Abdul Fadhil Al Mudzaki, "STEGANOGRAFI AUDIO BERBASIS QR CODE MENGGUNAKAN METODE LEAST SIGNIFICANT BIT (LSB), DISCRETE COSINE TRANSFORM (DCT), DAN DISCRETE WAVELET TRANSFORM (DWT)," *AT-TAWASSUTH J. Ekon. Islam*, vol. VIII, no. I, pp. 1–19, 2023.

[24] S. Rahman *et al.*, *Python : Dasar Dan Pemrograman Berorientasi Objek*. 2023.

[25] T. M. Kadarina and M. H. Ibnu Fajar, "Pengenalan Bahasa Pemrograman Python Menggunakan Aplikasi Games Untuk Siswa/I Di Wilayah Kembangan Utara," *J. Abdi Masy.*, vol. 5, no. 1, p. 11, 2019, doi: 10.22441/jam.2019.v5.i1.003.

[26] Elsa Nandita and Yahfizham Yahfizham, "Komparasi Stabilitas dan Efektifitas Phyton dengan C++ Sebagai Algoritma Pemrograman Pemecahan Masalah pada Programmer Pemula," *J. Arjuna Publ. Ilmu Pendidikan, Bhs. dan Mat.*, vol. 1, no. 6, pp. 104–115, 2023, doi: 10.61132/arjuna.v1i6.298.

[27] V. Wahyuningtyas, "Implementasi Ekstraksi Fitur untuk Klasifikasi Suara Urban Menggunakan Deep Learning," *Sains, Apl. Komputasi dan Teknol. Inf.*, vol. 3, no. 1, pp. 10–17, 2021.

[28] B. McFee *et al.*, "Librosa: Audio and Music Signal Analysis in Python, In the Proceedings of the 14th Python in Science Conference, Austin, Texas, 6 - 12 July 2014," *Scipy*, no. Scipy, pp. 18–24, 2015.

[29] "Visualisasi File Audio Menggunakan Librosa."

[30] N. Aisyah *et al.*, "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," *J. Esensi Infokom J. Esensi Sist. Inf. dan Sist. Komput.*, vol. 6, no. 1, pp. 22–27, 2022, doi: 10.55886/infokom.v6i1.452.

[31] L. Q. Sayed Achmady, "OPTIMALISASI STEGANOGRAFI AUDIO UNTUK PENGAMANAN INFORMASI," *Sci. Total Environ.*, vol. 9, no. 1, pp. 1–10, 2020,

[Online]. Available: https://doi.org/10.1016/j.scitotenv.2021.147444%0Ahttps://doi.org/10.1016/j.soilbio.2021.108211%0Ahttps://doi.org/10.1016/j.watres.2021.117597%0Ahttps://doi.org/10.1016/j.scitotenv.2021.147016%0Ahttps://doi.org/10.1016/j.scitotenv.2021.147133%0Ahttps://do

[32] N. A. Kevin Putra Dirgantoro, Bambang Hidayat, "PERBANDINGAN STEGANALISIS SINYAL WICARA BERFORMAT .WAV ANTARA METODE ANALISIS CEPSTRAL DAN MEL-FREQUENCYCEPSTRAL COEFFICIENT (MFCC)," vol. 3, no. 2, pp. 56–63, 2018.

[33] K. M. Kyi, "Audio Features Based Steganography Detection in WAV File the Creative Commons Attribution License (CC BY 4.0)," *Int. J. Trend Sci. Res. Dev. Int. J. Trend Sci. Res. Dev.*, vol. 3, no. 5, pp. 1691–1694, 2019, doi: 10.31142/ijtsrd26807.

[34] S. Bhalshankar and A. K. Gulve, "Audio Steganography: LSB Technique Using a Pyramid Structure and Range of Bytes," 2015, [Online]. Available: http://arxiv.org/abs/1509.02630

[35] M. C. Ghane, M. D. Uribarri, R. Djemai, D. Dunsin, and I. I. Araujo, "A Novel Hybrid Method for Effective Identification and Extraction of Digital Evidence Masked by Steganographic Techniques in WAV and MP3 Files," *J. Inf. Secur. Cybercrimes Res.*, vol. 6, no. 2, pp. 89–104, 2023, doi: 10.26735/izbk9372.

[36] E. Persson, "Diminishing returns of higher mp3 bit rates," 2022.