AJIE - Asian Journal of Innovation and Entrepreneurship
(e-ISSN: 2477-0574; p-ISSN: 2477-3824)
Vol. 09, Issue. 01, January 2025
DOI: 10.20885/ajie.vol9.iss1.art1

Implementasi Steganografi dengan Menggunakan Metode Masking and Filtering untuk Menyisipkan Pesan ke dalam Spectrogram Audio

Permadi Kusuma[1*], Yudi Prayudi[2]

[1,2] Program Studi Informatika, Fakultas Teknologi Industri, Universitas Islam Indonesia, Yogyakarta, Indonesia
[*]E-mail: 23917007@students.uii.ac.id

ABSTRAK

Pada saat mengirim pesan kepada pihak tertentu dan tidak ingin pesan tersebut diketahui oleh pihak lain, maka penting untuk menghindari kebocoran informasi. Namun masalah yang teridentifikasi adalah terdapat kekurangan pengetahuan untuk mendeteksi Steganografi audio yang membutuhkan teknik metode yang dapat membaca dan melihat pesan rahasia. Salah satu metode yang bisa dipakai dalam steganografi adalah *Masking and Filtering*. *Masking* sebagai media penanda pada audio yang dapat menyisipkan pesan. *Filtering* memberikan nilai pada bagian yang sudah diberikan tanda. Metode ini salah satu yang sering digunakan karena sederhana, cepat dalam proses penyisipan data, serta memiliki kapasitas penyimpanan yang cukup besar. Metode *Masking and Filtering* mampu menyembunyikan pesan dengan cara menyisipkan kedalam *Spectrogram* audio sebagai media penyimpan. *Filter* digunakan untuk memastikan pesan tersembunyi berada dalam rentang frekuensi yang telah dianalisis sebelumnya, sehingga membuat manusia tidak dapat mendengar dengan jelas audio tambahan yang sudah disisipkan yang merupakan pesan tersembunyi. Setelah penyisipan selesai, file audio disimpan dan dilakukan pengujian untuk memastikan bahwa kualitas audio tidak terganggu dan pesan tersembunyi tetap tidak terdeteksi seperti melakukan modifikasi pada file stego untuk menguji ketahanan dan keamanan pesan rahasia. Berdasarkan penelitian, steganografi sulit dideteksi oleh mata telanjang, untuk mengambil pesan yang sudah disembunyikan, maka bisa dilakukan dengan menampilkan *Spectrogram* audio yang terdapat pesan rahasia. Cara melihat pesan yang disembunyikan menggunakan aplikasi *Audacity* yang dapat melihat gelombang suara. Hasilnya pesan yang disematkan pada audio tidak mengalami kerusakan meskipun sudah dilakukan kompresi, pemotongan, dan sebagian proses yang dilakukan dalam audio.

Kata kunci: *Masking and Filtering, Spectrogram, Steganografi Audio*

ABSTRACT

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. However, the problem identified is that there is a lack of knowledge to detect audio Ste-ganography which requires technical methods that can read and view secret messages. One method that can be used in steganography is Masking and Filtering. Masking as a media marker on audio that can insert messages. Filtering gives value to the parts that have been given a mark. This method is one that is often used because it is simple, fast in the data insertion process, and has a large enough storage capacity. The Masking and Filtering method is able to hide messages by inserting them into the audio Spectrogram as a storage medium. The filter is used to ensure that the hidden message is within the previously analyzed frequency range, thus making humans unable to clearly hear the additional audio that has been inserted which is the hidden message. After the insertion is complete, the audio file is saved, and tests are performed to ensure that the audio quality is not compromised, and the hidden message remains undetected such as making modifications to the stego file to test the robustness and security of the hidden message. Based on research, steganography is difficult to detect by the naked eye, to retrieve messages that have been

hidden, it can be done by displaying an audio Spectrogram that contains a secret message. How to see the hidden message using the Audacity application that can see sound waves. The result is that the message embedded in the audio is not damaged even though compression, cutting, and some of the processes carried out in the audio have been carried out.

Keywords: *Masking and Filtering, Spectrogram, Steganografi Audio*

1. Pendahuluan

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 (Santoso dkk., 2016). 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 (Yuniati, 2023) . 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.

Ketika seorang anggota *Al-Qaeda* ditangkap di Berlin pada bulan Mei 2011, ditemukan barang bukti kartu memori dengan folder yang yang terdapat file dilindungi kata sandi dan tersembunyi. Seperti yang dilaporkan surat kabar Jerman *Die Zeit*, para ahli forensik komputer dari Kepolisian Kriminal Federal Jerman (*BKA*) mengklaim telah menemukan isinya-yang tampaknya merupakan video porno berjudul "*KickAss*." Di dalam video tersebut, mereka menemukan 141 file teks terpisah, yang berisi apa yang diklaim oleh para pejabat sebagai dokumen-dokumen yang merinci operasi *Al-Qaeda* dan rencana operasi di masa depan. Dalam kasus ini, berkas-berkas tersebut disembunyikan di dalam berkas video melalui teknik steganografi (Gallagher, 2012). Dari temuan tersebut, teroris memanfaatkan trik steganografi karena ciri-ciri steganografi yang menjadikannya kurang cocok untuk keperluan bisnis mala justru membuatnya ideal bagi teroris. Terutama, teknik ini dapat digunakan dalam metode pengiriman elektronik yang aman. Pada contoh kasus Steganografi Audio dimana pelaku menyembunyikan pesan dengan cara memasukkan informasi ke dalam bagian audio di mana suara keras akan menutupi suara yang lebih lemah. Misalnya, jika ada suara keras pada frekuensi tertentu, informasi dapat disisipkan pada frekuensi yang berdekatan, karena suara tersebut akan tertutup oleh suara keras sehingga pesan bisa tersisipkan dengan rapi.

Teknik steganografi sudah dikenal sejak lama walaupun belum menggunakan media digital. Steganografi digunakan untuk menyembunyikan data di dalam data lain. Banyak metode yang dapat digunakan untuk menyembunyikan informasi di dalam gambar, audio, dan video di antaranya adalah Metode *LSB* (*Least Significant Byte*), *Discrete Cosine Transform* (*DCT*), dan *Masking and Filtering*. Metode *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 (Rohayah, 2022) yang melakukan penelitian steganografi pada gambar dan audio. Begitupun dengan penelitian (Laksono dkk., 2024) yang memakai metode *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 metode steganografi *Discrete Cosine Transform* (*DCT*) pada penelitian (Yuniati, 2023) 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.

Dalam konteks audio forensik. Metode *Masking and Filtering* pada steganografi audio dipilih karena menawarkan beberapa keuntungan, khususnya dapat menyembunyikan informasi dengan cara yang sulit dideteksi oleh telinga manusia. Selain itu pesan steganografi yang ada pada audio aman dari modifikasi dan bisa menampung pesan dengan jumlah kata atau kalimat yang bisa disesuaikan dengan kebutuhan. Metode *Masking and Filtering* 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, metode ini memanfaatkan cara telinga dan otak memproses suara, sehingga sangat sulit dideteksi melalui pendengaran normal.

Dalam bidang forensik digital. Penerapan steganografi audio menggunakan *Metode Masking and Filtering* 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 metode *Masking and Filtering* untuk mendukung proses penyelidikan, pengumpulan bukti digital, dan pelacakan kejahatan.

Metode *Masking and Filtering* juga bisa digunakan untuk keamanan perusahaan dalam melindungi data sensitif seperti rencana bisnis, informasi produk, atau dokumen penting dari penyadapan atau kebocoran yaitu dengan menyembunyikan pesan di audio, informasi yang dianggap penting oleh perusahaan dapat tetap aman bahkan jika file tersebut jatuh ke tangan yang salah. Sedangkan manfaat yang didapat dari perlindungan privasi individu yaitu bisa menyembunyikan pesan pribadi dalam file audio agar tidak mudah diakses oleh pihak yang tidak berwenang. Data seperti informasi keuangan dan dokumen pribadi dapat dilindungi dengan menyisipkannya ke file audio untuk mencegah pencurian data.

Selain menyembunyikan informasi, penting juga untuk memastikan bahwa informasi tersebut tidak bisa diakses dengan mudah. Metode *Masking and Filtering* membuat informasi sulit ditemukan tanpa alat atau metode 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 (Fitriyah & Prayudi, 2017). Pada penelitian (El Rezen Purba & Desinta Purba, 2021) mengusulkan metode *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 metode *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 (Ro'isa & Suartana, 2019) yang menggunakan metode *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 metode pemfilteran masking ini dibatasi pada gambar yang menampilkan warna abu-abu. Pada penelitian sebelumnya, metode *Masking and Filtering* dilakukan pada steganografi gambar. Pada penelitian ini melakukan implementasi steganografi pada file audio dengan menggunakan teknik *Masking and Filtering* yang bisa memasukkan pesan teks format *Bitmap* yang sudah diubah menjadi audio ke dalam media audio yaitu lagu yang berformat *MP3*. Penelitian ini menganalisa tiga audio yang sudah disisipkan pesan steganografi. Adapun aplikasi yang digunakan untuk menganalisa dan menyisipkan pesan rahasia

adalah *Audacity* dan aplikasi yang dipakai membuat pesan rahasia ialah *CoagulaLight1666* yang bisa mengubah file gambar menjadi audio berformat *WAV*.

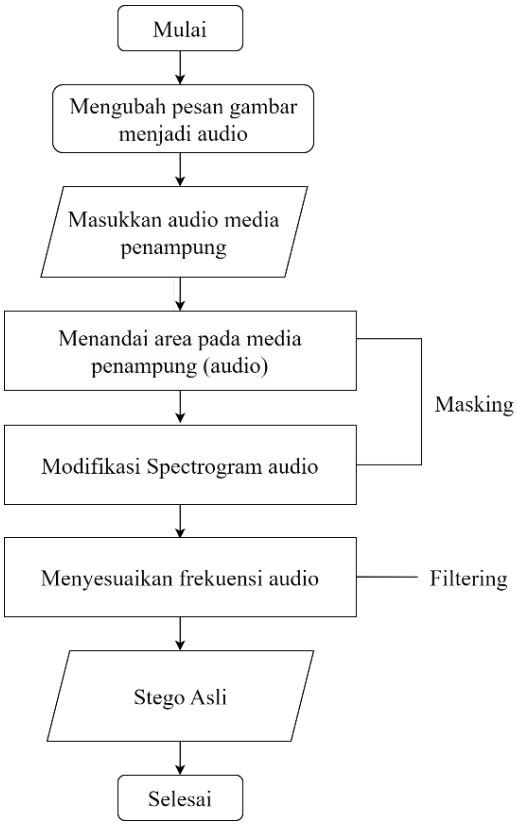
Peneliti akan membuat skenario dalam penyisipan pesan dan juga dilakukan proses analisa dan validasi perbandingan audio asli dan audio yang sudah dilakukan proses steganografi. Untuk melihat pesan yang sudah disisipkan adalah dengan cara menampilkan *Spectrogram* audio yang sudah dijadikan wadah penampung pesan melalui aplikasi *Audacity*. Dengan begitu hanya pihak yang tahu cara memunculkan *Spectrogram* yang bisa membaca pesan. Untuk mengetahui perbedaan audio setelah disisipi yaitu dengan menganalisa perbedaan *Spectrogram* pada audio yang disisipkan pesan dengan audio asli tanpa manipulasi. Peneliti juga melakukan modifikasi ketiga audio seperti memotong bagian audio, mengubah format audio, mempercepat dan memperlambat audio hasil steganografi untuk menguji ketahanan penyisipan pesan rahasia.

2. Metode Penelitian

Secara garis besar tahapan metodologi penelitian ini dapat dilihat pada Gambar 1.

Gambar 1. Metodologi yang Diusulkan

Adapun langkah-langkah steganografi dalam penelitian ini bisa dilihat pada gambar 2.



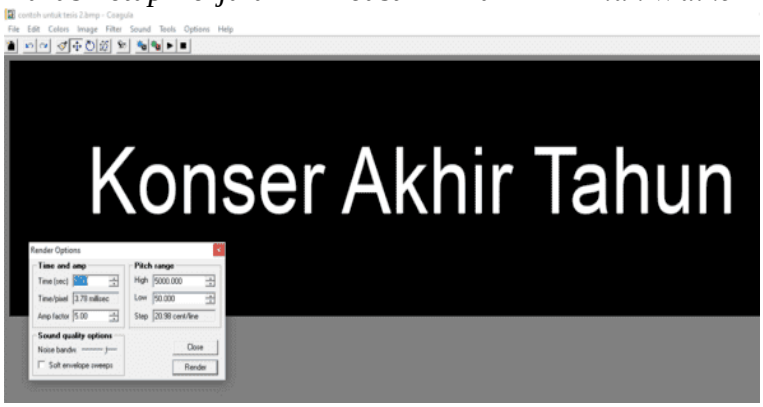
Gambar 2. *Flowchart* Metode Masking And Filtering

2.1 Pemilihan File Audio

Pada penelitian ini yang dilakukan pertama kali yaitu 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*"," Feast – *Nina"* dan *" Alan Walker - The Spectre*". Didalam audio ini sudah disisipkan pesan rahasia yang nanti akan dianalisa.

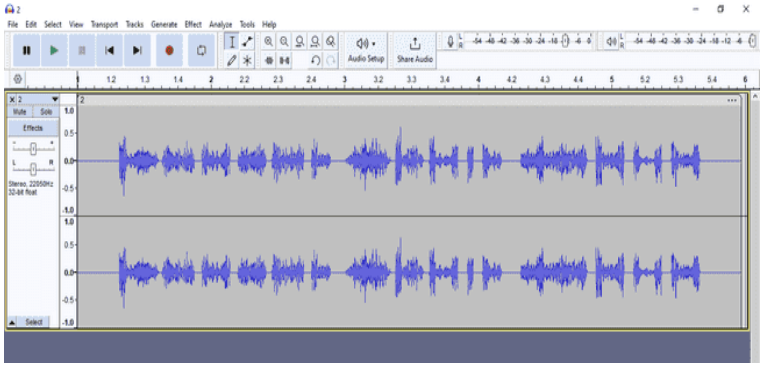
2.2 Melakukan Masking

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 simulasi dari pesan terorisme yang akan ditemukan di Daerah Istimewa Yogyakarta. Pesan yang disembunyikan merupakan gambar yang sudah diubah ke bentuk audio sehingga pesan dapat disisipkan ke dalam musik. Terdapat tiga pesan yang akan disisipkan pada tiga file musik, pesan yang pertama bertuliskan "*Konser Akhir Tahun*" yang artinya akan diadakan kegiatan tahun baru. Sedangkan pesan yang kedua bertuliskan "*Pal Putih*" yang merupakan julukan dari Tugu Jogja. Dan pesan yang ketiga yaitu "*31 Desember*" yang merupakan tanggal terjadinya kegiatan. Ketiga pesan tersebut disisipkan pada nada dering "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*". "*Feast – Nina*" dan "*Alan Walker – The Spectre*".



Gambar 3. Tampilan aplikasi *CoagulaLight1666*

Pada gambar 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*. Seperti pada gambar 4.



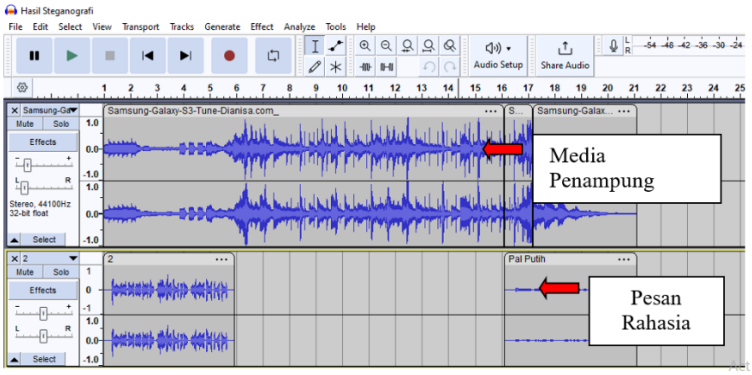
Gambar 4. Tampilan aplikasi *Audacity*

2.3 Proses Filtering

Setelah menentukan area di mana pesan bisa disisipkan, proses filtering dilakukan untuk mengurangi atau menghilangkan komponen frekuensi yang tidak diperlukan, atau menyesuaikan sinyal audio sehingga penyisipan pesan tidak merusak kualitas audio asli. Filter dapat digunakan untuk memastikan bahwa pesan tersebut tersembunyi dalam rentang frekuensi yang telah dipilih sebelumnya, agar manusia tidak mendengar dengan jelas audio tambahan yang sudah disisipkan yang merupakan pesan tersembunyi.

2.4 Penyisipan Pesan

Selanjutnya pesan rahasia kemudian disisipkan ke dalam file audio pada bagian yang sudah dipilih dan difilter sebelumnya. Teknik penyisipan bisa menggunakan berbagai metode, seperti menyisipkan pesan ke dalam area *Spectrogram* audio sebagai area yang ingin di masking dan difilter. Dengan memasukkan nada pada frekuensi tingkat daya yang rendah, penyisipan data tersembunyi yang diekstraksi tercapai (Achmady & Qadriah, 2020).



Gambar 5. Proses penyisipan Steganografi pada Audio

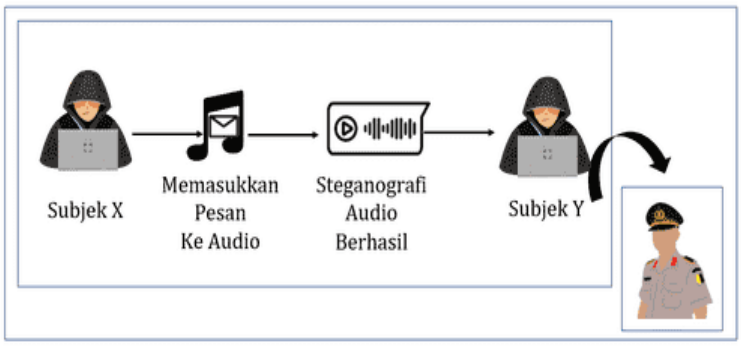
2.5 Penyimpanan dan Pengujian

Setelah penyisipan selesai, file audio disimpan dan dilakukan pengujian untuk memastikan bahwa kualitas audio tidak terganggu dan pesan tersembunyi tetap tidak terdeteksi. Pada penelitian ini melibatkan analisa *Spectrogram* dan juga uji coba file hasil steganografi dengan melakukan modifikasi pada file audio.

3. Hasil dan Pembahasan

3.1 Skenario Kasus

Diperlukan skenario kasus dengan melibatkan file audio yang sudah disisipkan pesan tersembunyi sehingga bisa menemukan pesan pada audio tersebut. Ilustrasi kasus dapat dilihat Gambar 6.



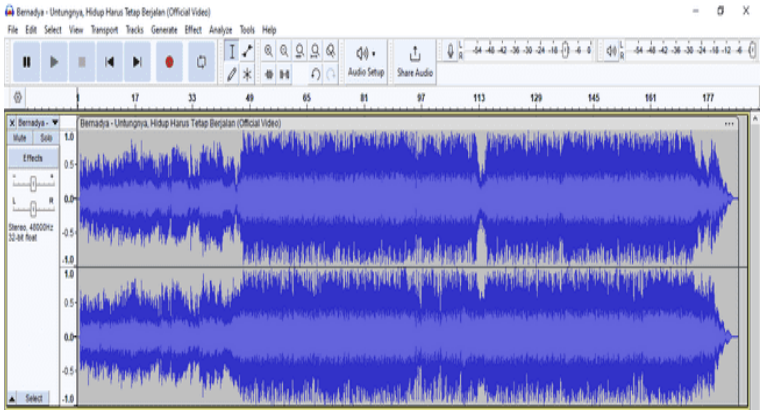
Gambar 6. Skenario kasus

Deskripsi kasusnya dimana X merupakan orang yang menyisipkan pesan ke dalam audio yang berisi pesan terorisme yang akan dikirim ke temannya yaitu Y melalui pesan *Whatsapp*. Polisi menemukan pesan tersebut dan mencoba menganalisa isi pesan yang tersimpan di dalam file audio.

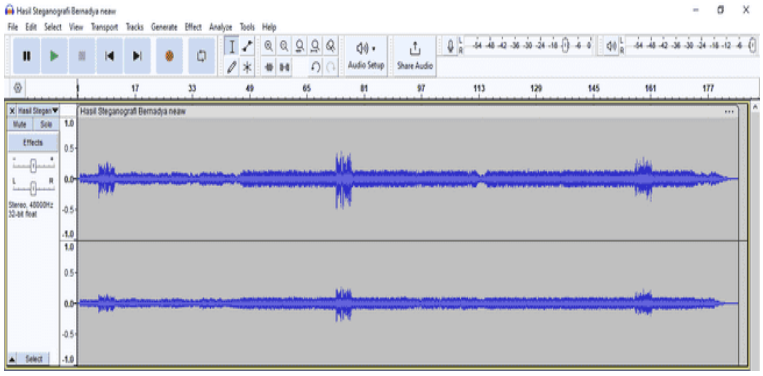
Barang bukti yang ditemukan berupa barang bukti elektronik yaitu *Smartphone* sebagai alat menerima pesan audio yang dari file audio tersebut adalah dugaan informasi rahasia.

3.2 Perbandingan Sinyal Audio Asli Dengan Hasil Stego-Audio

Sinyal audio ditampilkan dalam bentuk representasi gelombang suara yang terlihat menyerupai aliran listrik. Pada pengujian ini, sinyal audio asli dibandingkan dengan sinyal audio hasil stego-audio yang dapat dilihat melalui penglihatan mata manusia. Gambar 7 merupakan sinyal audio asli dari lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*" sedangkan gambar 8 adalah tampilan sinyal audio yang sudah disisipkan pesan rahasia.



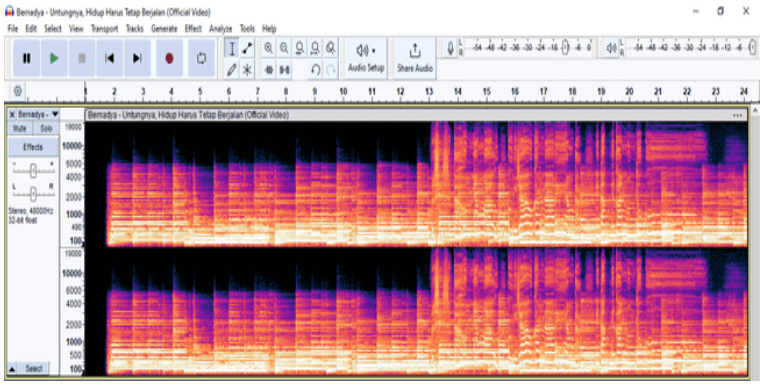
Gambar 7. Sinyal audio asli



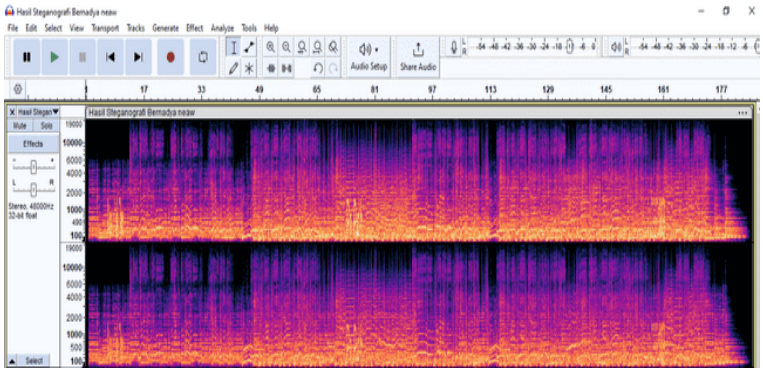
Gambar 8. Sinyal audio hasil steganografi

3.3 Analisis Spectrogram

Teknik steganografi pada berkas audio memanfaatkan kelemahan pendengaran manusia, karena kualitas suara antara berkas audio asli dengan berkas audio yang telah disisipkan pesan rahasia tidak jauh berbeda (Darwis, 2015). Pada tahapan ini analisis *Spectrogram* dilakukan guna melihat pola gelombang suara yang diucapkan dari formant setiap kalimat. Dikarenakan *Spectrogram* memperlihatkan hal-hal yang bersifat detail, maka sebagian ahli berpendapat bahwa *Spectrogram* merupakan sidik jari suara (*voice fingerprint*). Spread spectrum memiliki kelebihan yaitu memiliki ketahanan terhadap jamming dan interferensi. Misalnya sinyal yang dibuat mengalami kerusakan ditengah jalan, informasi yang disampaikan masih dapat dipersepsi. Sehingga cocok dipakai untuk steganografi audio yang format filenya mungkin mengalami kompresi dan pengeditan lainnya (Nugraha, 2011). Berikut contoh tampilan Spectrogram audio asli dan hasil Steganografi.



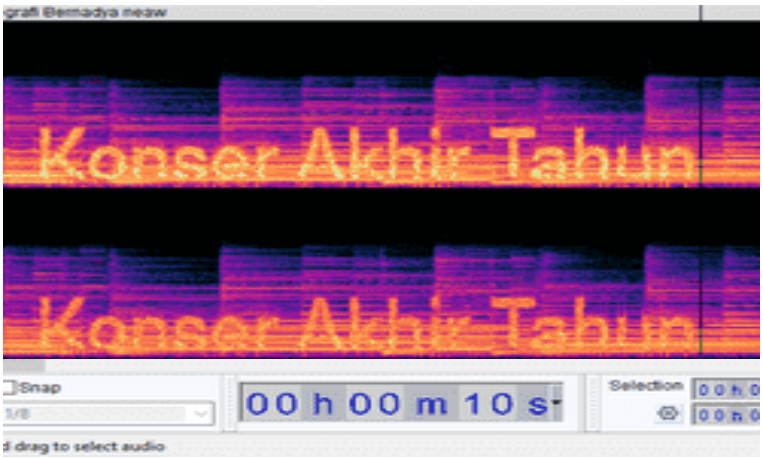
Gambar 9. Spectrogram audio asli



Gambar 10. *Spectrogram* hasil stego

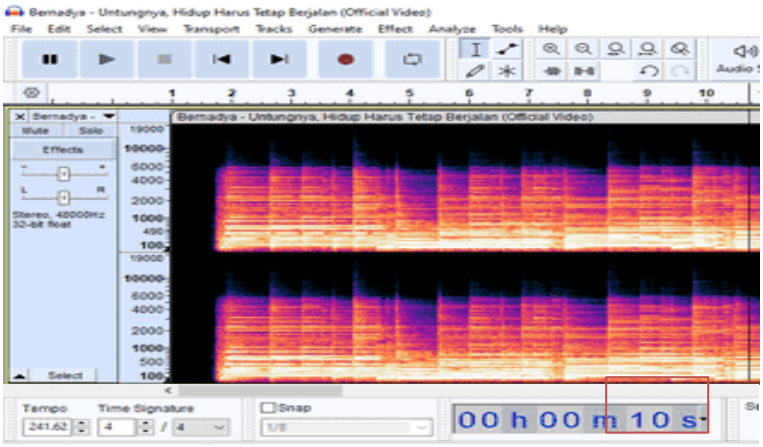
3.4 Mendeteksi Pesan yang disisipkan pada Spectrogram

Untuk mendeteksi bukti digital pada pesan yang disisipkan di area *Spectrogram.* Maka dilakukan *Zoom In* untuk memperbesar area *Spectrogram* audio supaya dapat dengan jelas melihat isi pesan yang dengan sengaja disisipkan pelaku. Seperti pada gambar dibawah ini menggunakan aplikasi *Audacity* dan menggunakan tools *Zoom In*.



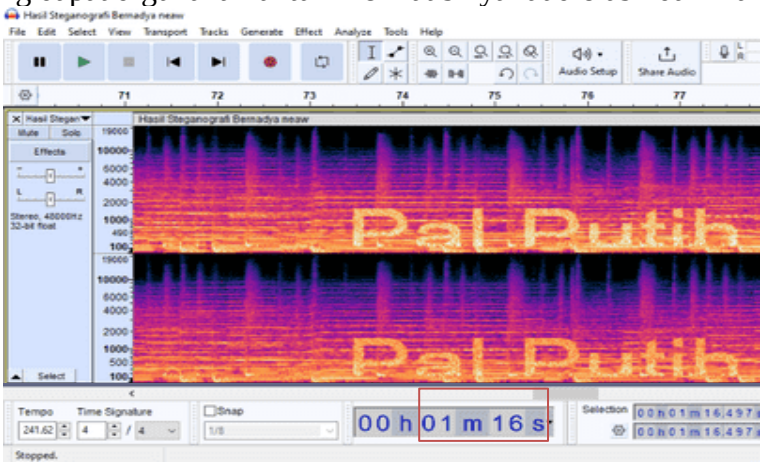
Gambar 11. Tampilan *Zoom In Spectrogram* hasil stego detik ke-6 sampai detik ke-10

Pada gambar 11, ditemukan tulisan yaitu *"Konser Akhir Tahun"* yang terdiri dari tiga kata dan memiliki arti yaitu akan diadakan kegiatan tahun baru. Tulisan tersebut ditemukan pada detik ke 6 sampai detik ke 10 pada lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*" yang sudah dilakukan proses Steganografi.



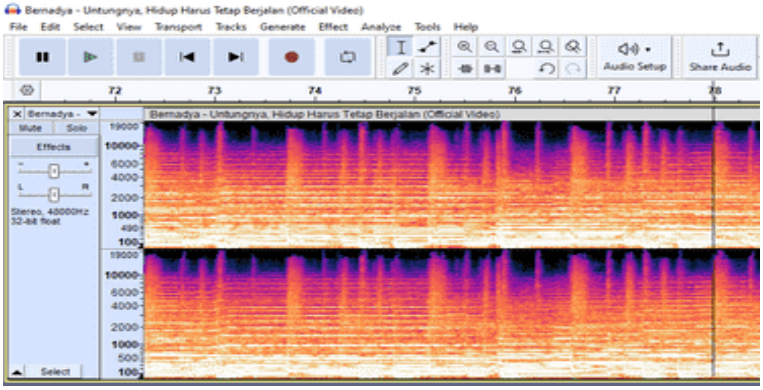
Gambar 12. Tampilan *Zoom In Spectrogram* audio asli detik ke-6 sampai detik ke-10

Pada Gambar 12, menampilkan proses *Zoom In* pada audio asli dari lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*" tidak ditemukan pesan rahasia di detik ke enam sampai detik ke sepuluh. Sedangkan pada audio hasil steganografi telah ditemukan pesan rahasia yang sudah disisipkan pada area *Spectrogram* dari lagi lagu tersebut. Analisa *Spectrogram* ini menggunakan aplikasi *Audacity* yang dapat digunakan untuk melihat sinyal audio asli dan manipulasi.



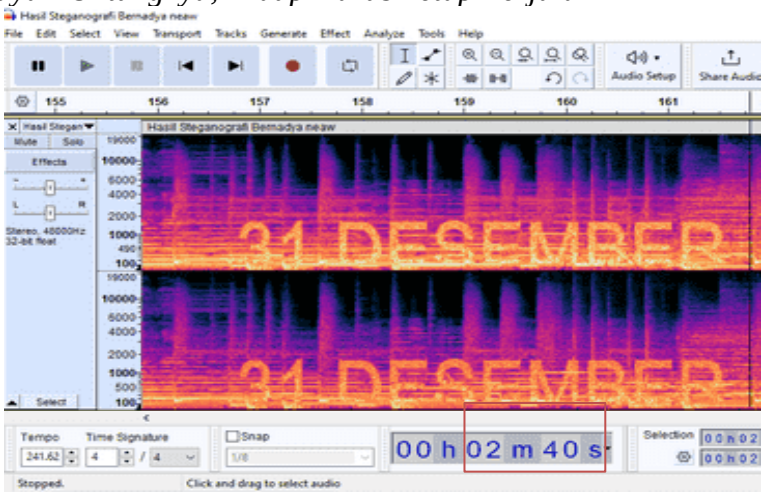
Gambar 13. Tampilan *Zoom In Spectrogram* hasil stego Pada durasi 1 menit 12 detik sampai 1 menit 16 detik

Selanjutnya pada gambar 13 dilakukan proses *Zoom In* pada durasi satu menit dua belas belas detik sampai satu menit enam belas detik. Hasilnya ditemukan barang bukti digital berupa hasil stego yang sengaja disisipkan pada *Spectrogram* yang bertuliskan *"Pal Putih"* yang terdiri dari dua kata dan memiliki arti dari Tugu Jogja yang merupakan salah satu ikon terkenal di kota Yogyakarta. Analisa *Spectrogram* ini menggunakan aplikasi *Audacity* yang dapat digunakan untuk melihat sinyal audio asli dan manipulasi.



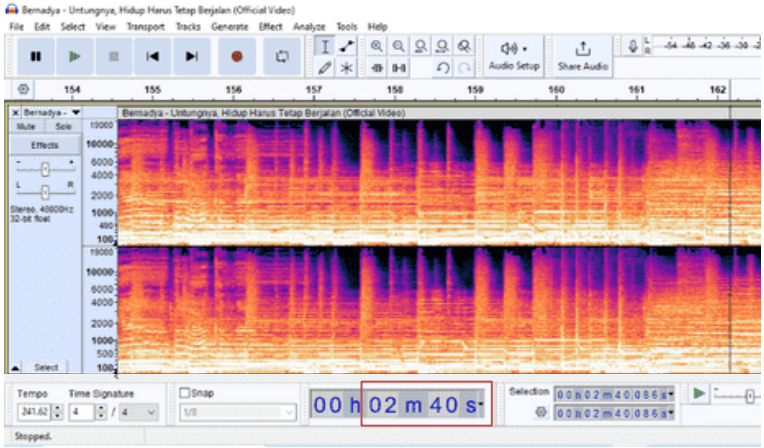
Gambar 14. Tampilan *Zoom In Spectrogram* audio asli Pada durasi 1 menit 12 detik sampai 1 menit 16 detik

Pada gambar 14 terlihat perbedaan *Spectrogram* dari audio manipulasi dan audio asli, hasilnya pada saat menampilkan proses *Zoom In* pada audio asli tidak ditemukan pesan rahasia pada durasi yang sama dimana ditemukan pesan *"Pal Putih"* yang terdiri dari dua kata. Sedangkan pada audio hasil steganografi telah ditemukan pesan rahasia yang sudah disisipkan pada area *Spectrogram* dari lagi lagu *Bernadya - Untungnya, Hidup Harus Tetap Berjalan*".



Gambar 15. Tampilan *Zoom In Spectrogram* hasil stego Pada durasi 2 menit 35 detik sampai 2 menit 40 detik

Pada gambar 15. Pesan steganografi juga ditemukan pada durasi dua menit tiga puluh lima detik sampai dua menit empat puluh detik. Adapun isi pesan yang ditemukan bertuliskan *"31 Desember"*. Sedangkan di audio asli dari lagu *"Bernadya"* tidak ditemukan pesan rahasia pada durasi yang sama. Seperti pada gambar 16. Analisa *Spectrogram* ini menggunakan aplikasi *Audacity* yang dapat digunakan untuk melihat sinyal audio asli dan manipulasi.



Gambar 16. Tampilan *Zoom In Spectrogram* audio asli Pada durasi 2 menit 35 detik sampai 2 menit 40 detik

Pada gambar 16 terlihat perbedaan *Spectrogram* dari audio manipulasi dan audio asli yang pada saat menampilkan proses *Zoom In* pada audio asli dan tidak ditemukan pesan rahasia pada durasi yang sama dimana ditemukan pesan *"31 Desember"* yang terdiri dari dua kata. Sedangkan pada audio hasil steganografi telah ditemukan pesan rahasia yang sudah disisipkan pada area *Spectrogram* dari lagu *Bernadya - Untungnya, Hidup Harus Tetap Berjalan*".

3.5 Hasil Pengujian Penyisipan Informasi Rahasia ke dalam Audio

Proses penyisipan dikatakan berhasil apabila ukuran informasi rahasia yaitu audio lebih kecil dibandingkan ukuran cover audio. Jika ukuran informasi rahasia yang disisipkan memiliki size lebih besar dari kapasitas cover audio maka hasilnya tidak dapat dilakukan proses penyisipan pesan rahasia.

Tabel 1. Hasil ketepatan penyisipan informasi rahasia (audio) ke dalam audio

Isi informasi rahasia	Ukuran informasi rahasia	Audio penampung (mp3)	Ukuran audio sebelum disisipi pesan	Ukuran audio setelah disisipi pesan	Hasil
Konser Akhir Tahun	427 KB	Bernadya	7.01 MB	33.6 MB	Berhasil
Pal Putih	439 KB	Feast – Nina	10.7 MB	47.6 MB	Berhasil
31 Desember	439 KB	Alan Walker	802 KB	17.2 MB	Berhasil

Pada Tabel 1 menampilkan ukuran audio setelah dilakukan proses stego dapat menambah size lagu, seperti pada lagu *Bernadya* yang awalnya 7.01 MB menjadi 33.6 MB. Begitupun dengan lagu *Feast – Nina* dari ukuran 10.7 MB menjadi 47.6 MB dan *Alan Walker* yang awalnya memiliki size 802 KB menjadi 17. 2 MB, ketiga audio berformat MP3, adapaun hasil yang didapat menunjukkan penyisipan ketiga informasi rahasia ke dalam lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan*" , "*Feast – Nina*" dan "*Alan Walker – The Spectre*" telah berhasil disisipkan.

3.6 Pengujian Modifikasi Hasil Steganografi

Setelah penyisipan rahasia berhasil maka perlu dilakukan ujicoba yaitu mengedit atau melakukan modifikasi ketiga audio yang sudah dilakukan proses steganografi. Ini dilakukan agar bisa melihat tingkat keberhasilan pesan setelah mengalami hasil modifikasi masih tetap terbaca dan tidak mengalami kerusakan. Terdapat empat pengujian yang dilakukan yaitu memotong (cut), merubah ukuran (*Resize*), mengubah kecepatan audio, dan mengubah format audio yang sudah disisipi dengan informasi rahasia.

Tabel 2. Hasil Modifikasi (Cut Audio)

Isi Informasi Rahasia	Ukuran Informasi Rahasia	Audio Penampung	Hasil
Konser Akhir Tahun	427 KB	Bernadya - Untungnya, Hidup Harus Tetap Berjalan	Tidak berhasil
Pal Putih	439 KB	Feast - Nina	Tidak berhasil
31 Desember	439 KB	Alan Walker – The Spectre	Tidak berhasil

Pada tabel 2 merupakan hasil ujicoba modifikasi memotong (Cut) bagian audio yang terdapat pesan rahasia. Terdapat tiga audio yang sudah dilakukan proses steganografi, adapun hasilnya adalah informasi rahasia akan hilang jika area *Spectrogram* yang menampilkan pesan rahasia audio itu di *Cut* atau dipotong. Namun jika durasi audio yang dipotong tidak di area *Spectrogram* yang terdapat pesan rahasia, maka pesan tersebut masih tetap terbaca.

Tabel 3.

Hasil Modifikasi (Kompresi dan Mengubah Format Audio) pada lagu "Bernadya - Untungnya, Hidup Harus Tetap Berjalan"

Nama File	Size Audio Stego	Size Audio Setelah Dikompres	Format Audio	Hasil
Bernadya	33.6 MB	2.80 MB	MP3	Berhasil

		2.41 MB	OGG	Berhasil
		14.2 MB	Flac	Berhasil
		2.86 MB	M4a	Tidak berhasil
		286 KB	AMR	Tidak berhasil
		30.8 MB	WAV	Berhasil

Tabel 4. Hasil Modifikasi (Kompresi dan Mengubah Format Audio) pada lagu "Feast – Nina"

Nama File	Size Audio Stego	Size Audio Setelah Dikompres	Format Audio	Hasil
Feast - Nina	47.6 MB	4.31 MB	MP3	Berhasil
		3.95 MB	OGG	Berhasil
		55.5 MB	Flac	Berhasil
		5.42 MB	M4a	Tidak berhasil
		442 KB	AMR	Tidak berhasil
		47.6 MB	WAV	Berhasil

Tabel 5. Hasil Modifikasi (Kompresi dan Mengubah Format Audio) pada lagu "Alan Walker – The Spectre"

Nama File	Size Audio Stegp	Size Audio Setelah Dikompres	Format Audio	Hasil
Alan Walker – The Spectre	17.2 MB	3.13	MP3	Berhasil
		2.44	OGG	Berhasil
		9.62 MB	Flac	Berhasil
		3.18	M4a	Tidak berhasil
		320 KB	AMR	Tidak berhasil
		10.3 MB	WAV	Berhasil

Tabel 6. Hasil Analisa dari ketiga lagu setelah dilakukan Modifikasi *Audio*

Audio Stego	Jumlah Format Audio	Berhasil	Tidak Berhasil
Bernadya - Untungnya, Hidup Harus Tetap Berjalan	6	4	2
Feast - Nina	6	4	2
Alan Walker – The Spectre	6	4	2

Dari pengujian hasil kompresi dan mengubah format audio yang sudah dilakukan proses setanografi bisa dilihat pada tabel 6. Telah dilakukan enam kali pengujian dan hasilnya empat yang berhasil dan dua tidak berhasil. Pada audio dari lagu "*Bernadya - Untungnya, Hidup Harus Tetap Berjalan"*, "*Feast-Nina"* dan "*Alan Walker – The Spectre"* telah dilakukan enam kali kompresi sekaligus mengubah format audio yang sebelumnya berformat *WAV* diubah menjadi format *MP3, OGG, Flac, M4a, AMR dan WAV*.

Setelah audio stego di kompres dan diubah format audio menjadi *M4a* dan *AMR*, ketiga file audio tidak dapat dibuka di Audacity sehingga pesan steganografi tidak bisa dibuka. Jika audio di kompres dan diubah format menjadi *MP3, OGG, Flac dan WAV* dapat berjalan lancar dan bisa membuka dan melihat pesan rahasia pada *Spectrogram* audio. Pengujian ini menggunakan tools dari

online-audio-converter.com dan *s25.aconvert.com* untuk memodifikasi audio. Sedangkan untuk membuka audio agar bisa melihat pesan rahasia menggunakan aplikasi *Audacity*.

Tabel 7. Hasil Modifikasi *Clip Speed* Lagu *Bernadya - Untungnya, Hidup Harus Tetap Berjalan*

Perlambat audio	Hasil	Percepat audio	Hasil
Clip Speed 80%	Berhasil	Clip Speed 130%	Berhasil
Clip Speed 70%	Berhasil	Clip Speed 150%	Berhasil
Clip Speed 50%	Berhasil	Clip Speed 170%	Berhasil
Clip Speed 40%	Berhasil	Clip Speed 190%	Berhasil
Clip Speed 30%	Berhasil	Clip Speed 250%	Berhasil
Clip Speed 10%	Berhasil	Clip Speed 270%	Berhasil

Hasil pengujian pada tabel 7 menghasilkan *Clip Speed* audio hasil stego dapat membaca pesan rahasia di *Spectrogram.* Meskipun tempo suara pada audio berubah setelah diperlambat dan dipercepat tetap bisa menampilkan pesan rahasia. Pengujian menggunakan aplikasi *Audacity*.

Tabel 8. Hasil Modifikasi *Clip Speed* dari Lagu *Feast – Nina*

Perlambat audio	Hasil	Percepat audio	Hasil
Clip Speed 80%	Berhasil	Clip Speed 130%	Berhasil
Clip Speed 70%	Berhasil	Clip Speed 150%	Berhasil
Clip Speed 50%	Berhasil	Clip Speed 170%	Berhasil
Clip Speed 40%	Berhasil	Clip Speed 190%	Berhasil
Clip Speed 30%	Berhasil	Clip Speed 250%	Berhasil
Clip Speed 10%	Berhasil	Clip Speed 270%	Berhasil

Hasil pengujian pada tabel 8 menghasilkan *Clip Speed* audio dari hasil stego lagu *Feast - Nina* dapat membaca pesan rahasia di *Spectrogram.* Meskipun tempo suara pada audio berubah setelah diperlambat dan dipercepat tetap bisa menampilkan pesan rahasia. Pengujian menggunakan aplikasi *Audacity*.

Tabel 9. Hasil Modifikasi *Clip Speed* Lagu *Alan Walker -The Spectre*

Perlambat audio	Hasil	Percepat audio	Hasil
Clip Speed 80%	Berhasil	Clip Speed 130%	Berhasil
Clip Speed 70%	Berhasil	Clip Speed 150%	Berhasil
Clip Speed 50%	Berhasil	Clip Speed 170%	Berhasil
Clip Speed 40%	Berhasil	Clip Speed 190%	Berhasil
Clip Speed 30%	Berhasil	Clip Speed 250%	Berhasil
Clip Speed 10%	Berhasil	Clip Speed 270%	Berhasil

Hasil pengujian pada tabel 9 menghasilkan *Clip Speed* audio dari hasil stego lagu *Alan Walker* dapat membaca pesan rahasia di *Spectrogram.* Meskipun tempo suara pada audio berubah setelah diperlambat dan dipercepat tetap bisa menampilkan pesan rahasia. Pengujian menggunakan aplikasi *Audacity*.

Tabel 10. Hasil Analisa dari ketiga lagu setelah dilakukan Modifikasi *Clip Speed Audio*

Audio Stego	Memperlambat audio	Mempercepat audio
Bernadya - Untungnya, Hidup Harus Tetap Berjalan	Pesan tetap terbaca	Pesan tetap terbaca
Feast - Nina	Pesan tetap terbaca	Pesan tetap terbaca
Alan Walker – The Spectre	Pesan tetap terbaca	Pesan tetap terbaca

Dari tabel analisa audio hasil steganografi di atas dapat diketahui bahwa file yang sudah dilakukan proses modifikasi *Clip Speed* yaitu memperlambat dan mempercepat audio hasilnya tidak mengganggu isi pesan rahasia yang sudah dimasukkkan ke dalam *Spectrogram*. Sehingga informasi yang ada masih tetap terbaca.

4. Kesimpulan

Berdasarkan hasil dan pembahasan pada proses Steganografi dengan menggunakan metode *Masking and Filtering* dapat disimpulkan bahwa penyisipan informasi rahasia (audio) ke dalam *Spectrogram* audio dapat dilakukan dengan menggunakan metode *Masking and Filtering*. Pesan yang disisipkan juga dapat dibaca dengan jelas sehingga bisa dijadikan bukti digital. Berdasarkan pengujian steganografi yang dilakukan menunjukkan bahwa pesan rahasia pada audio bisa dibaca dengan jelas setelah melalui beberapa modifikasi audio seperti melakukan kompresi, mengubah format audio dan *Clip Speed audio*. Meskipun ada kendala dimana audio stego tidak dapat dibuka saat diubah ke format *M4a* dan *AMR*. Penyebab audio berformat *M4a* dan *AMR* tidak dapat dibuka dikarenakan aplikasi *Audacity* tidak mendukung format audio tersebut. Namun audio masih bisa diputar menggunakan aplikasi *VLC Media Player*, agar bisa melihat pesan yang sudah disisipkan pada audio maka solusinya ialah mengubah audio berformat *M4a* dan *AMR* menjadi audio yang bisa dibuka di *Audacity* misalnya audio berformat *MP3, OGG, Flac dan WAV*. Pada metode *Masking and Filtering* yang diimplementasikan pada media audio masih terdapat kekurangan yaitu hasil analisisa menunjukkan bahwa karakteristik audio memiliki tingkat perbedaan pada gelombang suara dan bentuk *Spectrogram* dibandingkan dengan rekaman audio asli meskipun suara tersebut berasal dari file yang sama.

Daftar Pustaka

Achmady, S., & Qadriah, L. (2020). Optimalisasi steganografi audio untuk pengamanan informasi. *Science of the Total Environment*, *9*(1), 1–10.

Darwis, D. (2015). Implementasi Steganografi pada Berkas Audio Wav untuk Penyisipan Pesan Gambar Menggunakan Metode Low Bit Coding. *EXPERT: Jurnal Manajemen Sistem Informasi dan Teknologi*, *5*(1). https://doi.org/10.36448/jmsit.v5i1.715

El Rezen Purba, D., & Desinta Purba. (2021). Text Insertion by Utilizing Masking-Filtering Algorithms as Part of Text Message Security. *Jurnal Info Sains: Informatika dan Sains*, *11*(1), 1–4. https://doi.org/10.54209/infosains.v11i1.18

Fitriyah, N. Q., & Prayudi, Y. Y. (2017). Implementasi Steganografi Audio File Wav Dengan Metode Discrete Cosine Transform (DCT). *Prosiding SENSEI*, *1*(1), 144–153.

Gallagher, S. (2012). *Steganography: How al-Qaeda hid secret documents in a porn video*. Ars Technica. https://arstechnica.com/information-technology/2012/05/steganography-how-al-qaeda-hid-secret-documents-in-a-porn-video

Laksono, A. W., Suhada, S., & Zakaria, A. (2024). *Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab*. *4*(1).

Nugraha, R. M. (2011). Implementasi Direct Sequence Spread Spectrum Steganography pada Data Audio. *Transform*.

Rohayah, S. (2022). Implementasi Teknik Steganography Pada File Gambar Dan Audio Dengan Menggunakan Metode LSB. *OKTAL: Jurnal Ilmu Komputer dan Science*, *2*(2), 496–503.

Ro'isa, F., & Suartana, I. M. (2019). Implementasi Steganografi dengan Menggunakan Metode Masking and Filtering untuk Menyisipkan Gambar ke dalam Citra Digital. *Journal of Informatics and Computer Science (JINACS)*, *1*(01), 9–15. https://doi.org/10.26740/jinacs.v1n01.p9-15

Santoso, S., Arisman, A., & Sentanu, W. (2016). Steganografi Audio (Wav) Menggunakan Metode Lsb (Least Significant Bit). *CCIT Journal*, *9*(2), 214–224. https://doi.org/10.33050/ccit.v9i2.500

Yuniati, T. (2023). Implementasi audio steganografi menggunakan algoritma discrete cosine transform. *Jurnal Teknoinfo*, *17*(1), 10. https://doi.org/10.33365/jti.v17i1.2232