

BAB II

TINJAUAN PUSTAKA

2.1. Landasan Teori

2.1.1. Steganografi

Steganografi adalah suatu metode enkripsi teks sehingga tidak ada orang lain yang dapat memahami informasi yang terkandung dalam dokumen selain pengirim dan penerima. Baik pesan rahasia maupun media penampung diperlukan untuk steganografi (Naglaa et al, 2020). Menyembunyikan data rahasia di media digital mengubah kualitas media. Kriteria yang perlu dipertimbangkan saat menyembunyikan data meliputi:

1. Fidelity

Kualitas file kontainer tidak banyak berubah. File steganografi terlihat bagus bahkan setelah menambahkan data sensitif. Pengamat tidak menyadari bahwa file tersebut berisi data sensitif.

2. Robustness

Data tersembunyi harus mampu menahan operasi yang dilakukan pada audio kontainer, dan data tersembunyi tidak boleh rusak.

3. Recovery

Harus dimungkinkan untuk mengungkap kembali data yang tersembunyi (recovery). Karena tujuan steganografi adalah untuk menyembunyikan data, data rahasia dalam file kontainer harus diambil setiap saat untuk digunakan lebih lanjut.

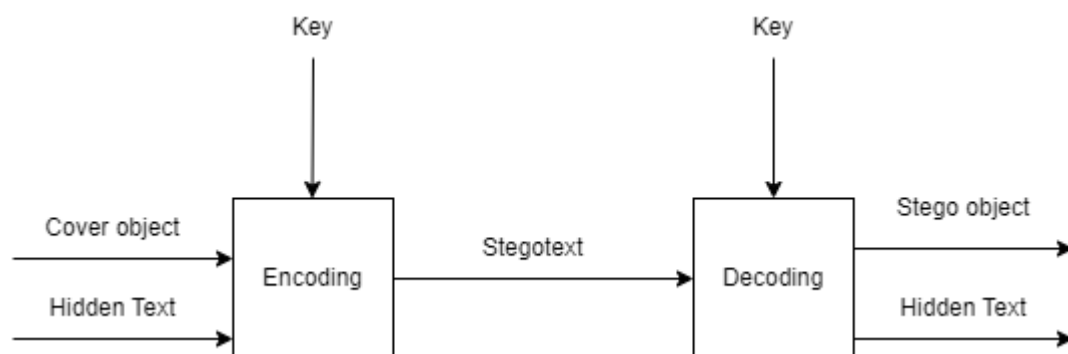
4. Konsep Steganografi

Ada beberapa istilah yang berkaitan dengan pokok bahasan steganografi:

- a. Hidden text : Pesan yang disembunyikan.
- b. cover-object : Untuk menyembunyikan Hidden text
- c. stego-object : Pesan yang sudah berisi Hidden text

Dalam steganografi hidden text yang dimaksudkan adalah teks yang akan disisipkan ke dalam cover-object yaitu file multimedia audio, video, gambar dan dokumen yang digunakan sebagai media penampung pesan yang akan disisipkan. Dari hasil encoding pesan kedalam file audio akan dihasilkan stego-object yang

merupakan file multimedia yang berisikan pesan embedding. Penyisipan pesan ke dalam media cover-object dinamakan encoding, sedangkan ekstraksi pesan dari stego-object dinamakan decoding (Nouf al - juaid, 2019). Kedua proses ini memerlukan kunci rahasia (stegokey) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan, seperti pada gambar di bawah ini:



Gambar 2.1 Proses Steganografi

Dalam proses di atas merupakan proses pada penyisipan teksnya dan untuk objeknya menggunakan file multimedia, dalam penelitian ini menambahkan file sumber image, audio, video serta dokumen. Untuk file yang di sisipinya yaitu dengan 8 file sisip pertama image, kedua png, ketiga audio wav, keempat audio mp3, kelima video MP4, ketujuh video Mpeg, kedelapan dokumen word atau pdf. Di lakukan sebanyak 32 pengujian meliputi file sumber ada 4 dan file sisip ada 8 di kalikan sehingga bisa menghasilkan 32 pengujian.

2.1.2. Algoritma Low Bit Coding

Adapun penjelasan mengenai low bit coding yaitu sebagai berikut:

1. Algoritma Low Bit Coding

Algoritma *low bit coding* adalah teknik yang digunakan dalam steganografi, di mana data disembunyikan dalam file digital seperti gambar, audio, video, dan dokumen. Metode ini bekerja dengan memodifikasi bit-bit paling tidak signifikan (Least Significant Bits atau LSB) dari data dalam file penampung (cover file). Berikut penjelasan tentang proses file sumber (image, audio, video, dan dokumen)

serta file sisip menggunakan berbagai jenis file penampung dan pengukuran kualitas setelah penyisipan:

1. Proses File Sumber dan File Sisip

File Gambar (JPEG, PNG)

Proses:

Buka file gambar.

Ubah setiap piksel gambar ke dalam format biner.

Gantikan bit paling tidak signifikan dari setiap piksel dengan bit dari file yang akan disisipkan.

Simpan gambar yang telah diubah.

Contoh:

Jika gambar memiliki piksel dengan nilai biner 10010110, dan bit yang akan disisipkan adalah 1, maka piksel yang dimodifikasi menjadi 10010111.

2. File Audio (WAV, MP3)

Proses:

Buka file audio.

Ubah data audio ke dalam bentuk biner.

Gantikan bit paling tidak signifikan dari setiap sampel audio dengan bit dari file yang akan disisipkan.

Simpan file audio yang telah diubah.

Contoh:

Jika sampel audio memiliki nilai biner 01100110, dan bit yang akan disisipkan adalah 0, maka sampel yang dimodifikasi menjadi 01100110.

3. File Video (MP4, MPEG)

Proses:

- Buka file video.

- Ubah frame video ke dalam format biner.

- Gantikan bit paling tidak signifikan dari setiap piksel dalam frame dengan bit dari file yang akan disisipkan.

- Simpan file video yang telah diubah.

Contoh:

Jika frame video memiliki piksel dengan nilai biner 11001100, dan bit yang akan disisipkan adalah 1, maka piksel yang dimodifikasi menjadi 11001101.

4. File Dokumen (DOC, PDF)

Proses:

Buka file dokumen.

Ubah data dokumen ke dalam bentuk biner.

Gantikan bit paling tidak signifikan dari setiap byte dengan bit dari file yang akan disisipkan.

Simpan file dokumen yang telah diubah.

Contoh:

Jika byte dokumen memiliki nilai biner 10101110, dan bit yang akan disisipkan adalah 1, maka byte yang dimodifikasi menjadi 10101111.

2.1.3. File Citra

Citra (gambar) adalah gambar pada bidang berdimensi ganda. Berasal dari sudut pandang matematis, citra berfungsi sebagai mekanisme untuk menahan (melanjutkan) intensitas cahaya pada diamatra bidang. Objek memantulkan kembali sebagian dari berkas cahaya tersebut, sumber cahaya menghasilkan objek. Alat-alat optik, kamera, pemindai (scanner), mata pada manusia, dan sebagainya, mengatur pantulan cahaya ini, sehingga bayangan objek yang dikatakan citra tersebut terekam. Gambar digital ditangkap oleh kamera dan kemudian diubah menjadi format tertentu yang dikenal sebagai gambar diskrit. Hasil fotografi dari printer tidak bisa disebut sebagai foto digital namun, foto yang disimpan dalam file gambar (seperti bmp, jpg, atau png) di komputer dapat disebut sebagai foto digital (Andika & Darwis, 2020). Dalam penelitian ini citra atau gambar sebagai file sumber dan file sisip menggunakan file image jpg dan png. Berdasarkan penelitian sebelumnya yang dilakukan oleh Rika Humayrah, Andi Marwan Elhanafi, dkk mengenai pengujian terhadap dua buah citra berdasarkan penelitian tersebut pada setiap cover citra memiliki nilai MSE, dan PSNR yang berbeda. Dari Analisa pengujian diketahui bahwa jika cover citra yang digunakan sama, dengan jumlah karakter teks yang sama dan kunci yang sama, maka nilai MSE dan PSNR sama. Jika cover citra yang digunakan sama dengan jumlah karakter teks yang sama

namun kunci berbeda, maka hasil nilai MSE dan PSNR berbeda. Jika cover citra yang digunakan sama namun jumlah karakter teks berbeda dengan kunci yang sama, maka nilai MSE dan PSNR yang dihasilkan berbeda. Dapat disimpulkan bahwa jika salah satu dari bahan uji coba ada yang berbeda maka hasil MSE dan PSNR yang dihasilkan akan berbeda, hanya bahan uji coba yang memiliki semua kesamaan yang memiliki nilai MSE dan PSNR yang sama. Diketahui bahwa semakin rendah nilai MSE maka semakin baik kualitas dari stego citra, dan semakin tinggi nilai PSNR maka semakin baik pula kualitas hasil stego citra yang diencoding. Dari Analisa pengujian di atas dapat dilihat bahwa yang memiliki nilai MSE terendah dan PSNR tertinggi merupakan cover citra format. Jpg dengan nilai MSE 0.00251 dan PSNR 74.12625 decibel dan yang memiliki nilai MSE tertinggi dan PSNR terendah merupakan cover citra format.png yaitu nilai MSE 0.18888 dan PSNR 55.36899 decibel. Dapat disimpulkan bahwa dari ketiga cover citra yang memiliki kualitas citra paling baik yaitu cover citra yang berformat .jpg dan kualitas citra kurang baik yaitu cover citra yang berformat png.

2.1.4. File Audio

File audio adalah jenis file digital yang menyimpan informasi karakteristik (metafile) serta pengkodean khusus dalam menyajikan susunan audio yang ditanamkan. Format file audio ada berdasarkan sifat data yang terkandung dalam file audio, dan dapat disimpan dalam format file audio terkompresi maupun tidak terkompresi. Beberapa format file audio populer termasuk MP3, WAV, PCM, dan WMA. Dalam pengukuran tingkat akurasi dan kualitas file audio, dokumen ini digunakan sebagai bahan uji untuk menilai kualitas dan akurasi sistem pengolahan audio. Berikut ini beberapa aspek yang perlu diperhatikan dalam pengukuran tingkat akurasi dan kualitas file audio:

1. **Tingkat Akurasi:** Tingkat akurasi adalah persentase dari suara yang benar yang diterima oleh sistem pengolahan audio. Untuk menilai tingkat akurasi, suara yang benar dan salah harus diidentifikasi dan ditentukan. Suara yang benar adalah suara yang sesuai dengan kriteria yang ditetapkan, sementara suara yang salah adalah suara yang tidak sesuai.

2. **Kualitas Suara:** Kualitas suara adalah kemampuan suara untuk menyediakan informasi yang relevan, akurat, dan lengkap. Untuk menilai kualitas suara, suara harus diperiksa secara manual atau menggunakan alat pendukung. Suara yang memenuhi kriteria kualitas akan dianggap sebagai suara yang baik, sedangkan suara yang tidak memenuhi kriteria akan dianggap sebagai suara yang buruk, untuk mengukur tingkat akurasi dan kualitas file audio maka menggunakan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR).
3. **Metode Pengukuran:** Metode pengukuran tingkat akurasi dan kualitas audio dapat berupa metode manual atau otomatis. Metode manual menggunakan tenaga kerja manusia untuk menilai kualitas dan akurasi suara, sedangkan metode otomatis menggunakan alat pendukung seperti ASR (Automatic Speech Recognition) atau Speech-to-Text untuk mengidentifikasi dan mengkategorikan suara.
4. **Metrik Pengukuran:** Metrik pengukuran adalah skala atau alat yang digunakan untuk menilai tingkat akurasi dan kualitas suara. Metrik yang umum digunakan adalah kesalahan, kesalahan konfirmasi, precision, recall, F1-score, dan kesalahan kritis.

Berdasarkan penelitian yang dilakukan oleh Ibnu Utomo Wahyu Mulyono, dkk dari hasil penelitian 50 citra dan audio berdurasi 2 – 4 menit didapatkan hasil bahwa proses stegonografi telah berhasil dilakukan dan mendapatkan hasil yang baik, dimana kapasitas audio berkisar antara 195 bit sampai 32550 bit pesan. Setelah dilakukan penyisipan, stego audio memiliki MSE 0 dan PSNR tidak terhingga atau diatas 40dB, yang berarti audio tidak berubah setelah disisipi pesan maka dapat dikatakan akurasi dan kualitas dari hasil stegono itu baik. Untuk file audio di dalam penelitian di masukkan ke dalam file sumber serta file sisip wav dan mp3.

2.1.5. File Dokumen

File dokumen merupakan berkas elektronik yang berisi informasi atau data yang dapat disimpan, diakses, dan diterbitkan. Dalam pengukuran tingkat akurasi dan kualitas file dokumen, dokumen ini digunakan sebagai bahan uji untuk menilai

kualitas dan akurasi sistem pengolahan dokumen. Berikut ini beberapa aspek yang perlu diperhatikan dalam pengukuran tingkat akurasi dan kualitas file dokumen:

1. **Tingkat Akurasi:** Tingkat akurasi adalah persentase dari dokumen yang benar yang diterima oleh sistem pengolahan dokumen. Untuk menilai tingkat akurasi, dokumen yang benar dan salah harus diidentifikasi dan ditentukan. Dokumen yang benar adalah dokumen yang sesuai dengan kriteria yang ditetapkan, sementara dokumen yang salah adalah dokumen yang tidak sesuai.
2. **Kualitas Dokumen:** Kualitas dokumen adalah kemampuan dokumen untuk menyediakan informasi yang relevan, akurat, dan lengkap. Untuk menilai kualitas dokumen, dokumen harus diperiksa secara manual atau menggunakan alat pendukung. Dokumen yang memenuhi kriteria kualitas akan dianggap sebagai dokumen yang baik, sedangkan dokumen yang tidak memenuhi kriteria akan dianggap sebagai dokumen yang buruk.
3. **Metode Pengukuran:** Metode pengukuran tingkat akurasi dan kualitas dokumen dapat berupa metode manual atau otomatis. Metode manual adalah metode yang menggunakan tenaga kerja manusia untuk menilai kualitas dan akurasi dokumen, sedangkan metode otomatis menggunakan alat pendukung seperti OCR (Optical Character Recognition) atau ICR (Intelligent Character Recognition) untuk mengidentifikasi dan mengkategorikan dokumen.
4. **Metrik Pengukuran:** Metrik pengukuran adalah skala atau alat yang digunakan untuk menilai tingkat akurasi dan kualitas dokumen. Metrik yang umum digunakan adalah kesalahan, kesalahan konfirmasi, precision, recall, F1-score, dan kesalahan kritis.

Menurut penelitian oleh irvan maulana yusuf, carudin dkk tahun 2020, dengan judul Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen. pengembangan perangkat lunak dengan menggunakan metode Waterfall, Prototyping, Rational Unified Process (RUP), dan bahasa pemrograman Java. Juga mencakup pengamanan dokumen menggunakan algoritma steganografi dan analisis webometrics pada repositori perguruan tinggi Islam negeri. File yang bersifat rahasia atau penting yang hanya ingin diketahui oleh pihak tertentu dapat diamankan menggunakan perangkat lunak berbasis bahasa

pemrograman Java yang menerapkan algoritma Caesar Cipher dan algoritma Least Significant Bit (LSB). File dokumen yang dienkripsi dengan algoritma Caesar Cipher dilakukan dengan menggeser huruf-huruf sesuai jumlah geser yang ditentukan oleh kunci yang dimasukkan. File yang disisipkan ke dalam gambar menggunakan algoritma LSB dilakukan dengan mengubah bit paling kanan atau paling belakang pada file penampung dengan bit dari file dokumen. Dalam proses enkripsi, semua file dokumen dapat dienkripsi, tetapi dalam proses penyisipan hanya 2 dari 5 file dokumen yang dapat disisipkan. File dokumen yang akan disisipkan hanya bisa memuat maksimal 31 karakter, karena ukuran piksel file penampung dalam perangkat lunak ini adalah 250x250. Semua file dokumen yang dienkripsi, dari total 5 file, dapat didekripsi dengan baik. Dan dari 2 file yang bisa disisipkan, kedua file tersebut dapat dikembalikan saat proses ekstraksi. Untuk file dokumen di jadikan file sumber serta file sisip yaitu file doc dan pdf.

2.1.6. File Video

File video yang digunakan sebagai pengukuran tingkat akurasi dan kualitas file video adalah file video yang digunakan sebagai referensi untuk menilai tingkat akurasi dan kualitas file video lainnya. Artinya, file video yang digunakan sebagai pengukuran harus memiliki tingkat akurasi dan kualitas yang tinggi, sehingga dapat digunakan sebagai referensi untuk menilai tingkat akurasi dan kualitas file video lainnya.

File video yang digunakan sebagai pengukuran tingkat akurasi dan kualitas file video harus memenuhi beberapa kriteria, seperti:

1. Tingkat akurasi yang tinggi: File video yang digunakan sebagai pengukuran harus memiliki tingkat akurasi yang tinggi, sehingga dapat digunakan sebagai referensi yang tepat untuk menilai tingkat akurasi file video lainnya.
2. Kualitas yang tinggi: File video yang digunakan sebagai pengukuran harus memiliki kualitas yang tinggi, sehingga dapat digunakan sebagai referensi yang tepat untuk menilai kualitas file video lainnya.
3. Format yang kompatibel: File video yang digunakan sebagai pengukuran harus memiliki format yang kompatibel dengan format file video yang akan diukur, sehingga dapat digunakan sebagai referensi yang tepat.

4. Resolusi yang tinggi: File video yang digunakan sebagai pengukuran harus memiliki resolusi yang tinggi, sehingga dapat digunakan sebagai referensi yang tepat untuk menilai resolusi file video lainnya.

File video yang digunakan sebagai pengukuran tingkat akurasi dan kualitas file video dapat diperoleh dari sumber yang terpercaya, seperti sumber publik atau dari perusahaan yang bergerak dalam industri video. Setelah file video yang digunakan sebagai pengukuran telah dipilih, maka file video lainnya dapat diukur dengan menggunakan metode yang tepat, seperti metode PSNR (Peak Signal-to-Noise Ratio) atau metode MSE (Mean Square Error). Menurut penelitian oleh Jayakanth Kunhoth & Nandhini Subramanian tahun 2022, dengan judul Video steganography recent advances and challenges. Untuk permasalahannya yaitu mengenai, satu piksel dalam bingkai video sampul memiliki 8 hingga 24 bit berdasarkan formatnya video. Bingkai skala abu-abu memiliki 8 bit sedangkan bingkai warna memiliki 24 bit. Bingkai warna terdiri dari 3 saluran (RGB) dan setiap saluran terdiri dari 8 bit per piksel. Demikian pula dengan RGB bingkai rahasia video terdiri dari 8 bit per piksel untuk ketiga saluran. Bagian paling kecil dari bingkai penutup diganti dengan bagian paling signifikan dari bingkai rahasia. Selama ekstraksi, bit LSB dari stego diambil dan 0 diisi untuk mendapatkan perkiraan informasi rahasia yang dimaksud. Seiring dengan media rahasia yang berbeda, tingkatannya berbeda kapasitas persembunyian dipertimbangkan, dan nilai MSE, PSNR, dan SSIM dari kombinasi berbeda diberikan dalam Tabel. file video di jadikan file sumber serta file sisip mp4 dan mpeg.

2.1.7. Kualitas File Steganografi Multimedia

Untuk menghitung nilai akurasi dan tingkat Kualitas Steganografi Multimedia gambar, audio, video dan dokumen. Maka di lakukan dengan cara pendekatan Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR), SSIM (Structural Similarity Index) berikut penjelasan mengenai MSE dan PSNR dan SSIM:

1. MSE (*Mean Square Error*)

Mean square error adalah salah satu cara untuk menghitung nilai kedekatan antara estimator dengan nilai yang estimasi. Jika n adalah jumlah sampel, I dan Y

masing – masing adalah estimator dan nilai yang ingin diestimasi untuk tiap sampel, nilai MSE ini untuk mengukur kualitas file multimedia seperti gambar, audio, video. maka MSE dapat di rumuskan sebagai berikut :

$$MSE = \frac{1}{n} \sum_{i=1}^n (Y_i - \hat{Y}_i)^2$$

Dimana:

n = jumlah Panjang byte dalam berkas.

i = indeks byte ke i

Y_i = nilai byte pada berkas awal.

$\hat{Y}_i$ = nilai byte pada berkas stego.

2. PSNR (*Peak Signal to Noise Ratio*)

Dasar yang paling penting pada audio steganografi adalah penyembunyian data tidak boleh mengubah kualitas file multimedia yang digunakan sebagai media penampung.

Peak Signal to Noise Ratio (PSNR) adalah perhitungan antara nilai maksimum dari sinyal yang di ukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya di ukur dalam satuan desibel. PSNR di gunakan untuk mengukur rasio antara berkas file multimedia yaitu gambar dan video. dengan berkas file multimedia yang telah disisipi pesan. PSNR yang rendah menunjukkan bahwa berkas file multimedia telah mengalami distorsi yang cukup besar. Kualitas file multimedia yang baik memiliki nilai PSNR Minimal 40dB.

3. SSIM (*Structural Similarity Index Measure*)

SSIM (Structural Similarity Index Measure) adalah suatu metode yang digunakan untuk mengukur kualitas file video berdasarkan perbandingan antara frame-frame video yang dihasilkan oleh proses pengolahan video. Dalam penggunaan SSIM, perbedaan antara frame-frame video yang dihasilkan oleh proses pengolahan video dibandingkan dengan frame-frame video asli, kemudian dihitung sebagai indeks kualitas. Indeks kualitas ini memberikan nilai yang

menunjukkan seberapa baik kualitas video yang dihasilkan oleh proses pengolahan video dibandingkan dengan kualitas asli. Nilai SSIM dapat berada dalam rentang 0 hingga 1, di mana nilai 1 menunjukkan kualitas yang sama persis dengan asli, sedangkan nilai 0 menunjukkan kualitas yang sangat berbeda.

SSIM digunakan untuk mengukur kualitas file video untuk tiap frame videonya dengan cara menghitung perbedaan antara frame-frame video yang dihasilkan oleh proses pengolahan video dengan frame-frame video asli. Dalam penggunaan SSIM, perbedaan antara frame-frame video dibandingkan secara struktural, termasuk perbedaan warna, kontras, dan tekstur. Nilai SSIM yang dihasilkan kemudian digunakan untuk menentukan seberapa baik kualitas video yang dihasilkan oleh proses pengolahan video dibandingkan dengan kualitas asli. Dalam beberapa aplikasi, seperti dalam pengolahan video digital, SSIM digunakan untuk mengukur kualitas video yang dihasilkan oleh proses pengolahan video. Dengan menggunakan SSIM, pengguna dapat mengetahui seberapa baik kualitas video yang dihasilkan oleh proses pengolahan video dibandingkan dengan kualitas asli. Hal ini sangat berguna dalam pengembangan teknologi pengolahan video digital, seperti dalam pengembangan algoritma pengolahan video yang lebih efektif dan efisien.

Rumus SSIM untuk membandingkan dua frame I_1 dan I_2 dalam konteks pengukuran file video adalah sebagai berikut:

$$\text{SSIM}(I_1, I_2) = \frac{(2\mu_{I_1}\mu_{I_2}+c_1)(2\sigma_{I_1 I_2}+c_2)}{(\mu_{I_1}^2+\mu_{I_2}^2+c_1)(\sigma_{I_1}^2+\sigma_{I_2}^2+c_2)}$$

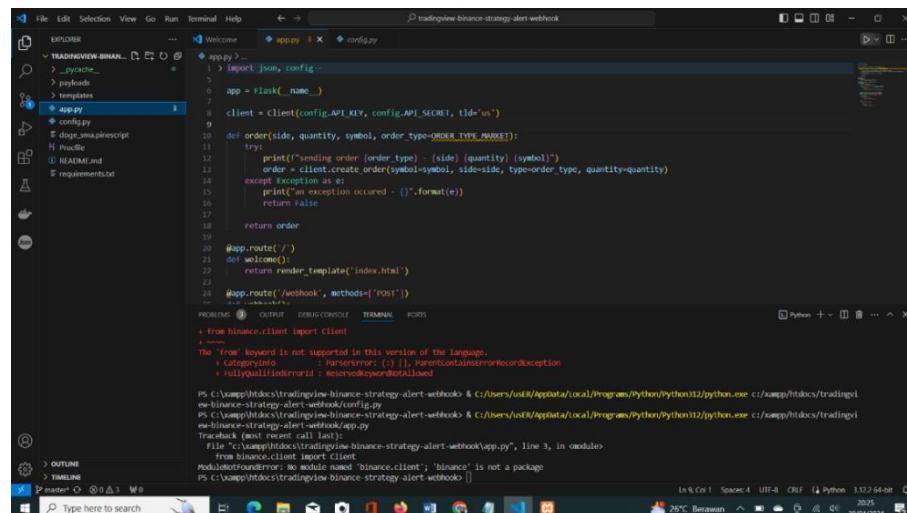
Di mana:

- μ_{I_1} dan μ_{I_2} adalah rata-rata intensitas piksel dari masing-masing frame I_1 dan I_2 .
- $\sigma_{I_1}^2$ dan $\sigma_{I_2}^2$ adalah varians dari intensitas piksel dalam masing-masing frame.
- $\sigma_{I_1 I_2}$ adalah kovarians antara intensitas piksel dalam kedua frame.
- c_1 dan c_2 adalah konstanta kecil yang ditambahkan ke penyebut untuk menghindari pembagian dengan nol.

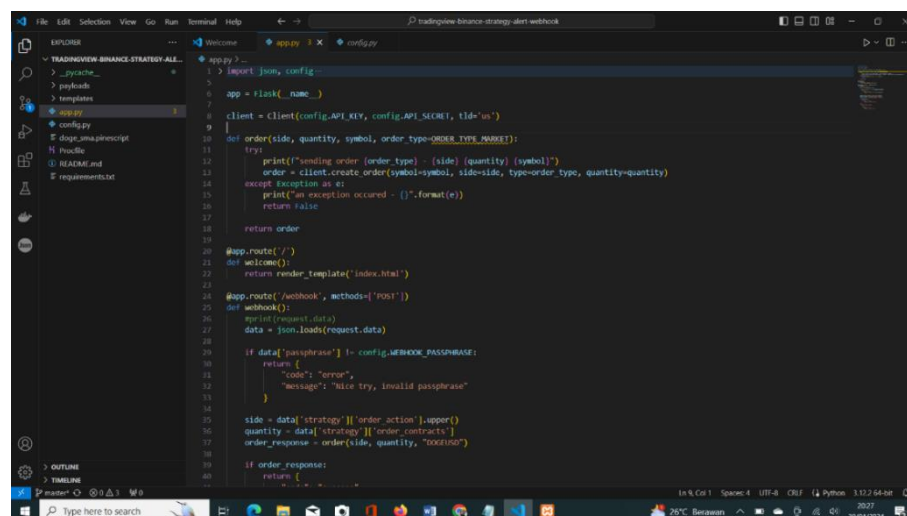
2.1.8. Visual Studio Code

Visual Studio Code adalah editor teks yang ringan dan andal yang dibuat oleh Microsoft untuk sistem operasi multiplatform, yang berarti tersedia untuk Linux, Mac, dan Windows. Editor teks ini secara langsung mendukung bahasa pemrograman JavaScript, TypeScript, dan Node.js, serta bahasa pemrograman lainnya dengan bantuan plugin yang dapat dipasang melalui marketplace Visual Studio Code seperti: C++, C#, Python, Go, Java, PHP, dan sebagainya.

Dalam penelitian ini, bahasa pemrograman Visual Studio Code yang digunakan adalah Python dan untuk simulasinya menggunakan fungsionalitas pada terminal visual studio code.



Gambar 2.2 Terminal



Gambar 2.3 Tampilan From Editor

2.1.9. Bahasa Python

Bahasa pemrograman Python adalah bahasa pemrograman tingkat tinggi yang serbaguna, mudah dipelajari, dan sangat populer. Diciptakan pada awal 1990-an oleh Guido van Rossum, Python dirancang dengan filosofi kesederhanaan dan keterbacaan kode. Python menonjol dalam berbagai bidang, mulai dari pengembangan perangkat lunak, analisis data, kecerdasan buatan, pengembangan web, hingga pemrograman sistem.

2.2. Penelitian Terkait / State of The Art

1. Penelitian dengan judul, Pengamanan pesan menggunakan kombinasi kriptografi dan steganografi audio berbasis transformasi wavelet diskrit Dalam keamanan pesan sama tetapi di lengkapi dengan kriptografi, dalam perbedaannya yaitu tentang metodenya memakai metode transformasi wavelet untuk audio. Keamanan informasi menjadi perhatian utama akhir-akhir ini. Kriptografi dan steganografi menggunakan media audio adalah salah satu solusi untuk masalah ini. Metode steganografi yang akan digunakan adalah DWT, karena penelitian sebelumnya menunjukkan bahwa DWT dapat menghasilkan nilai PSNR yang lebih tinggi dibandingkan beberapa metode lainnya. Kelebihan dari penerapan pengamanan pesan dengan kombinasi kriptografi RSA dan steganografi audio berbasis Transformasi Wavelet Diskrit adalah proses pengamanan pesan dilakukan dengan membangkitkan kunci RSA, kemudian mengenkripsi pesan dengan kunci tersebut, dan hasil enkripsinya diamankan dalam sinyal audio hasil Transformasi Wavelet, yaitu sinyal frekuensi tinggi. Kekurangannya adalah metode penyisipan ini mengubah pesan menjadi biner dan bekerja dengan pesan teks yang sedikit, sehingga untuk mendapatkan hasil penyisipan pesan yang maksimal diperlukan upaya lebih. Manfaat penelitian ini adalah peningkatan keamanan data dan keberlanjutan penelitian agar menjadi lebih baik (Albab & Darmaji, 2023).
2. Penelitian dengan judul, Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital, Persamaanya dengan penelitiannya sama sama dengan menggunakan audio stego citra digital Perbedaannya yaitu tentang metode yang di pakai

menggunakan metode lsb (least significant bit). Kelebihan Hasil implementasi metode LSB pada keamanan audio dalam citra digital sangat efisien dan tepat. Hal ini karena teknik yang digunakan tidak menimbulkan kecurigaan dan tidak terlihat secara kasat mata. Jika citra berformat .BMP digunakan sebagai wadah dalam tahap penyisipan, ukuran citra tersebut tidak berubah. Namun, jika format yang digunakan adalah .PNG, ukurannya akan berubah karena stego citra digital yang dihasilkan berubah menjadi format .BMP. Meskipun demikian, citra yang dihasilkan secara kasat mata tetap tidak mengalami perubahan yang signifikan atau mencurigakan. Kekurangan yang perlu dikembangkan adalah menambahkan opsi data rahasia yang akan disisipkan dan diekstraksi, seperti data dokumen atau video. Sistem ini bisa lebih dikembangkan dengan menyediakan opsi file dalam berbagai format lainnya. Manfaat penelitian ini untuk keintegrasian sebuah data dan penelitian lanjutan sehingga menghasilkan penelitian yang optimal. (Akmal & Furqan, 2023).

3. Penelitian dengan judul, Teknik Steganografi Untuk Penyembunyian Pesan Teks Menggunakan Algoritma End Of File Dalam persamaanya hanya pada penyembunyian pesan Perbedaanya yaitu mengenai algoritma end of file dimana metode ini pada ukuran suatu citra digital untuk menyisipkan pesan pada file yang terakhir. Dengan keterbatasan inilah, Teknik steganografi dapat diterapkan pada berbagai media digital. Hasil yang dikeluarkan dari steganografi ini memiliki persepsi yang sama seperti bentuk aslinya, dimana dapat diproses oleh komputer tetapi tidak berlaku untuk kemampuan indera manusia. Kelebihan imperectibility memberikan hasil steganografi pada gambar, dengan metode kuesioner yang menghasilkan 70% mahasiswa dibidang komputer tidak mengetahui tentang Steganografi dan 100% menyatakan gambar hasil steganografi tidak dapat terlihat oleh indra mata manusia secara kasat mata. Pada proses pengujian tahap fidelity tidak nampak nilai MSE yang hanya menghasilkan nilai "0" dan PSNR menghasilkan nilai " ∞ " (tak hingga) dikarenakan metode yang digunakan menyisipkan pesan di akhir file tanpa merubah nilai intensitas warna pikselnya. Kekurangan Aplikasi ini diharapkan dapat diterapkan dengan format citra lainnya seperti PNG, GIF,

dll. Sehingga menjadikan lebih dinamis sedangkan untuk manfaat penelitian ini yaitu untuk meningkatkan keamanan dan privasi informasi dalam berbagai konteks, sambil mempertahankan integritas dan kualitas file asli (Darwis & Kisworo, 2019).

4. Penelitian dengan judul, Optimasi Steganografi Berbasis Citra Digital Menggunakan Modifikasi Bit Dalam persamaanya dengan steganografi citra digital dan memodifikasi bit Perbedaanya yaitu dengan metode LSB untuk pesan berupa citra ke cover berupa citra. Untuk meningkatkan kemampuan LSB dalam menyisipkan pesan berupa citra ke cover berupa citra, ditambahkan algoritma Modifikasi Bit pada cover dan pesan sebelum dilakukan penyisipan menggunakan metode LSB. Kelebihan proses penyisipan dengan citra cover dan citra pesan menggunakan format antara JPG dan JPG atau antara PNG dan PNG berdasarkan pengujian performansi menggunakan koefisien korelasi dan PSNR yang menghasilkan nilai tertinggi adalah penyisipan dengan format PNG berjumlah 1 bit. Pada proses ekstraksi menggunakan format JPG atau PNG berdasarkan pengujian performansi menghasilkan koefisien korelasi tertinggi dan MAPE terendah adalah proses ekstraksi dengan format PNG berjumlah 4 bit. Kekurangan bahwa pesan yang disisipkan pada penelitian ini hanya disisipkan namun pesan tidak terenkripsi yang artinya saat pesan didapat oleh orang lain selain penerima maka pesan akan langsung diketahui, Untuk selanjutnya bisa dikembangkan manfaat penelitiannya yaitu meningkatkan tingkat keamanan pesan yang disembunyikan, membuatnya lebih sulit untuk dideteksi dan dipecahkan oleh pihak yang tidak berwenang (Putra & Gaffar, 2020).
5. Penelitian dengan judul, Implementasi Kripto-Steganografi Salsa20 dan BPCS untuk Pengamanan Data Citra Digital Dalam persamaanya hanya saja pengamanan pada data citra, Perbedaanya yaitu Dalam metode menggunakan chipper dan kriptografi. Kelebihan Hybrid teknik kriptografi Salsa20 dan teknik steganografi BPCS telah berhasil dilakukan dengan baik. Hal ini dapat dilihat pada keberhasilan proses enkripsi-penyisipan pesan serta proses dekripsi pembongkaran pesan rahasia yang mencapai 100%, dimana citra yang

disisipkan adalah identik sama dengan citra yang diekstrak dari sebuah citra stego sebelumnya. kekurangannya Berdasarkan hasil pengujian terhadap tiga komponen citra digital yang meliputi nilai MSE sebesar 16,21259, dan nilai PSNR mencapai +44,08686 dB. Sementara dari analisa grafik histogram dapat dilihat bahwa sebaran intensitas piksel citra cover yang sudah disisipkan pesan rahasia dengan yang belum bisa dikatakan identik serupa (Irawan et al, 2020).

6. Penelitian ini berjudul, Implementasi Enkripsi AES Cipher dan Discrete Wavelet Transform Dalam Metode Steganografi persamaan dari teknik steganografi melakukan ekstraksi gambar. Perbedaan ini hanya menampilkan gambar dan metodenya memakai wavelet transform kelebihan Dengan mengenkripsi hidden image menggunakan algoritma AES dan steganografi least significant bit, informasi mengenai hidden image tetap terjaga karena hidden image berbentuk ciphertext. Tanpa adanya kunci yang tepat, data tetap berupa ciphertext. kekurangan hanya memiliki 2 perbandingan image asli dan hidden image. Manfaat penelitiannya yaitu untuk perlindungan dan penyembunyian data dalam berbagai aplikasi digital. Ini menawarkan peningkatan signifikan dalam keamanan informasi sambil memastikan kualitas dan integritas data tetap terjaga (Antono et al, 2020)
7. Penelitian ini berjudul, Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Cipher dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman Java Persamaanya hanya dalam penyembunyian pesan. perbedaanya menggunakan metode lsb dan rivest code 4. kelebihan Hasil aplikasi penyisipan pesan rahasia pada gambar berjalan dengan baik Pesan atau dokumen yang disisipkan pada file gambar dan file audio dapat diambil kembali secara penuh. kekurangan Dengan metode LSB (Least Significant Bit), citra yang disisipkan pada pesan atau dokumen tidak terlalu banyak menunjukkan perbedaan dengan citra berwarna. Untuk manfaat penelitian ini yaitu menawarkan solusi yang aman dan efisien untuk penyembunyian data dalam citra digital, menggabungkan kekuatan teknik steganografi dan enkripsi. Dengan implementasi dalam bahasa pemrograman Java, penelitian ini tidak hanya relevan untuk aplikasi praktis tetapi juga

berkontribusi pada pengembangan teknologi keamanan informasi yang lebih baik (Wiranata & Aldisa, 2021).

8. Penelitian ini berjudul, Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamanan Informasi pada Citra Digital persamaanya hanya sama dengan pengamanan data saja tidak ada proses penyisipan data. Perbedaanya yaitu memakai metode lsb dan hanya memfokuskan pada citra digital saja. Kelebihanya. Hasil dari implementasi penyisipan dan menyembunyian pesan dengan metode steganografi LSB dan algoritma vigenere cipher pada citra digital dapat berjalan dengan baik. Citra yang disisipkan pesan (stego image) tidak mengalami perubahan yang signifikan dari citra asli. Kekuranganya yaitu Pada penelitian ini penulis hanya menggunakan citra digital (gambar) sebagai media penampung dan teks sebagai pesan, diharapkan penelitian selanjutnya dapat menggunakan media audio, video dan lainlain sebagai media penampung maupun pesan yang akan disisipkan. Untuk manfaat penelitiannya yaitu memberikan solusi yang efektif dan efisien untuk menyembunyikan pesan rahasia. Ini tidak hanya meningkatkan keamanan dan privasi informasi tetapi juga menjaga kualitas dan integritas media digital, menjadikannya relevan untuk berbagai aplikasi praktis dan pengembangan teknologi masa depan (Yanti & Budayawan, 2023).
9. Penelitian ini berjudul, Steganografi Metode Least Significant BIT (LSB) Pada Mpeg Spatial Audio Object Coding persamaanya mengenai object audio saja. perbedaanya penelitian ini memfokuskan pada mpeg dan audio yang bersifat object coding. Kelebihanya Metode LSB pada MPEG SAOC menghasilkan kualitas suara yang cukup baik karena nilai SNR masing-masing audio tersebut diatas 20 dB. Proses ini tidak menyebabkan perubahan yang berarti pada kualitas suara, sehingga pada kualitas suara yang terdengar tidak dapat dibedakan dengan audio aslinya. kekuranganya steganografi menggunakan metode Least Significant Bit (LSB) pada MPEG Spatial Audi Object Coding(SAOC). Dengan menggunakan proses steganografi, audio yang dihasilkan tidak begitu memiliki perubahan, untuk manfaat penelitian ini yaitu meningkatkan keamanan dan privasi informasi, menjaga kualitas dan integritas

file audio, serta memberikan kontribusi penting dalam pengembangan teknologi steganografi dan keamanan informasi (Farhani & Dwiharzandis, 2022).

10. Penelitian ini berjudul, Deteksi Posisi Penyisipan Pesan Text Pada Steganografi Audio Dengan Metode Mfcc Dan Decison Tree, persamaanya yaitu dengan penyisipan text pada staganografi. Perbedaanya hanya menggunakan metode MFCC dan decision tree. Kelebihanya yaitu Metode MFCC dan Decsion Tree dapat diimplementasikan dalam sistem steganalisis dan sistem deteksi posisi audio tersteganografi. Pada pengujian pengaruh ciri statistik didapatkan bahwa ciri statistik Sekwness menjadi ciri statistik terbaik. Pada pengujian sistem steganalisis dihasilkan akurasi terbaik sebesar 67,52%. Untuk akurasi deteksi posisi didapat sebesar 94,73% dan deteksi terhadap letak posisi didapat akurasi sebesar 46,58%. Kekuranganya yaitu tidak adanya metode yang sangat signifikan sehingga isinya hanya berupa tingkat akurasi. Untuk manfaat penelitiannya yaitu untuk mendeteksi dan melindungi data audio dari manipulasi dan penyisipan pesan yang tidak sah. Ini meningkatkan keamanan dan integritas informasi audio, memberikan kontribusi penting dalam pengembangan teknologi deteksi steganografi dan keamanan informasi (Wicaksono et al., 2020).
11. Penelitian ini berjudul, Pengaruh Kapasitas Dimensi Citra Watermark Terhadap Audio Watermarking Dengan Perpaduan Metode Dwt (Discrete Wavelet Transform) Dan Svd (Singular Value Decomposition) persamaanya yaitu dengan adanya audio mp3. perbedaanya yaitu mengenai metode dwt dan svd singular value decomposition. kelebihanya Semakin besar ukuran piksel dari gambar yang dijadikan watermark, maka semakin menurun kualitas dari audio yang dapat dilihat pada penurunan nilai PSNR audio, pada watermark berukuran 10×10 piksel kualitas audio dapat lebih baik dengan rata-rata nilai PSNR 56 hingga 57 dB untuk jenis genre audio jazz, rock, dan classic, sementara watermark berukuran 40×40 dan 50×50 piksel kualitas audio sangat menurun dengan rata-rata nilai PSNR 10 sampai 14 dB untuk jenis genre audio yang sama. Kekurangan hanya dapat disimpulkan bahwa serangan pada audio

berupa amplify, resampling dan invert hampir tidak mengubah watermark hasil dari penyisipan. Hal ini dapat dilihat dari nilai histogram error yang semakin mendekati nol yang berarti watermark hasil dari penyisipan tidak jauh merubah watermark hasil serangan. Untuk manfaat penelitiannya yaitu untuk meningkatkan kapasitas penyisipan tanpa mengorbankan kualitas audio. Ini membawa manfaat yang nyata dalam melindungi keaslian konten digital dan meningkatkan keamanan informasi secara keseluruhan (Dan, 2019).

12. Penelitian ini berjudul, Pengamanan Audio Rindik Bali Menggunakan Metode Least Significant Bit Berbasis Android, persamaanya dalam melakukan stegano seperti encoding dan decoding. perbedaanya yaitu mengenai metode lsb. kelebihanya yaitu Pada pengujian ini memiliki rata – rata 71.896 dB untuk PSNR dan 0,831 untuk nilai MSE. Hasil tersebut memperlihatkan bahwa pada proses penyisipan pesan menggunakan teknik LSB berhasil dengan baik dalam menyisipkan data teks pada audio. Pada pengujian black box untuk menguji menghasilkan penilaian yang baik, Pada pengujiannya setiap fitur yaitu steganografi dan ekstraksi didapatkan hasil yang sesuai dengan harapan yang diinginkan. Pada pengujian UAT untuk menguji persepsi dari sisi pengguna, menunjukan hasil yang baik dengan nilai rata-rata 94% dari tiap poin yang pertanyaan yang ada. Kekuranganya yaitu tidak adanya saran di dalam isi jurnal tersebut seharusnya ada, untuk manfaat penelitiannya yaitu untuk ketahanan terhadap serangan dan dari penelitian sebelumnya supaya bisa menjadi lebih baik (Jayantia et al., 2022).
13. Penelitian dengan judul, Perbandingan Teknik Steganografi Domain Spasial Dengan Domain Transformasi Pada Audio, Dalam persamaanya yaitu sama seperti menghitung kualitas audio setelah di sisipi, perbedaanya hanya membandingkan metode Least Significant Bit (LSB) dan Spread Spectrum (SS) dan di buktikan dengan nilai SNR yang di hasilkan metode spread spectrum lebih besar atau lebih baik di bandingkan dengan metode least significant bit. kelebihanya mampu mengimlementasikan hasil perbandingan antara metode lsb dan ss nilai perbedaanya itu mencapai 8db, tetapi kualitas pesan yang didapatkan pada hasil ekstraksi kedua metode sama baiknya,

kekurangan kurangnya proses setelah di sisipi tidak memakai nilai MSE hanya memakai nilai PSNR. Untuk manfaat penelitian ini memberikan kontribusi penting dalam pemahaman tentang teknik steganografi dalam domain spasial dan domain transformasi pada audio. Ini memberikan pandangan yang jelas tentang kelebihan dan kekurangan masing-masing pendekatan, membantu dalam pengembangan aplikasi keamanan informasi yang lebih efisien dan efektif (Ulum et al., 2021).

14. Penelitian dengan judul, Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab, Dalam persamaanya yaitu tentang menghitung kualitas png dengan memakai pendekatan MSE dan PSNR, perbedaanya tidak ada proses decoding dan encoding hanya pengukuran saja. kelebihanya yaitu menggunakan metode least significant bit mengakhirkan bit yang ada dan hitunganya sangat baik dan relevan, kekuranganya yaitu aplikasi matlab yang digunakan untuk Tools tidak dapat menjelaskan secara praktis tidak di jelaskan bagian sourcodenya hanya flowchart saja. Untuk manfaat penelitian ini memberikan kontribusi yang berharga dalam pengembangan dan penerapan teknik steganografi pada citra digital menggunakan Matlab. Ini membuka peluang untuk meningkatkan keamanan informasi, memperluas pengetahuan dalam bidang steganografi, dan memfasilitasi pengembangan aplikasi steganografi yang lebih canggih dan efektif (Laksono et al., 2024).
15. Penelitian dengan judul, Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital, Dalam persamaanya yaitu tentang steganogaraifi menghitung kualitas audio, perbedaanya yaitu data dokumen maupun video. Sistem ini bisa jauh lebih dikembangkannya lagi dengan cara yakni dibuatnya opsi file yang mempunyai berbagai macam format lainnya seperti halnya format .JPEG, .GIF, .TIFF, serta juga .JPG. Kelebihan pada teknik yang digunakan steganografi terhadap file audio dengan berkas audio stego citra digital dan diakhiri rangkaian metode Least Significant Bit (LSB). Dapat disimpulkan bahwa hasil dari implementasi metode LSB yang diterapkan pada keamanan audio ke dalam citra digital

sangat memiliki efisien dan tepat. Hal ini dikarenakan hasil dari teknik yang digunakan tidak menimbulkan kecurigaan serta tidak terlihat dalam kasat mata. Jika mempergunakan citra yang formatnya itu .BMP teruntuk dijadikannya suatu wadah pada tahapan penyisipan, maka dengan demikian tidaklah mengubah ukuran dari citra tersebut. Namun jika yang dipergunakan memiliki format .PNG teruntuk dijadikannya suatu wadah pada tahapan penyisipan, maka daripada itu bakal mengalaminya perubahan terkait dengan ukurannya, dikarenakan stego citra digital yang dihasilkan berubah jadi format .BMP. Kekurangannya yaitu kurangnya kecepatan dalam menghitung extration time dan insertion time. Untuk manfaat penelitiannya yaitu memberikan kontribusi yang berharga dalam pengembangan dan penerapan teknik steganografi audio menggunakan metode LSB. Ini membuka peluang untuk meningkatkan keamanan informasi, memfasilitasi komunikasi aman, dan memperluas pemahaman tentang keamanan digital dalam konteks audio (Akmal & Furqan, 2023).

2.3. Matrik Penelitian

Tabel 2.1 Matrik Penelitian

N0	Nama, Tahun dan Judul	Tools/Metode							
		Visual Studio code	Microsoft Visual Studio	Low bit coding	Enkripsi Aes	Discrete Wavelet Transform	Decision tree	Least significant bit (LSB)	End Of File
1.	(Albab & Darmaji, 2023) Pengamanan pesan menggunakan kombinasi kriptografi dan steganografi audio berbasis transformasi wavelet diskrit	√				√			
2.	(Antono et al, 2020) "Implementasi Enkripsi AES Cipher dan Discrete Wavelet Transform Dalam Metode Steganografi."				√	√			

7.	(Wiranata & Aldisa, 2021) "Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA."				√			√		
8.	(Yanti & Budayawan, 2023) Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi pada Citra Digital."				√					
9.	(Farhani & Dwiharzandis, 2022) "Steganografi metode least significant bit (lsb) pada mpeg spatial				√					

	audio object coding."									
10.	(Wicaksono et al., 2020) "Deteksi Posisi Penyisipan Pesan Text Pada Steganografi Audio Dengan Metode MFCC Dan Decision Tree."						√			
11.	(Dan, 2019) Pengaruh Kapasitas Dimensi Citra Watermark Terhadap Audio Watermarking Dengan Perpaduan Metode Dwt (Discrete Wavelet Transform) Dan Svd (Singular Value Decomposition).					√				
12.	(Jayantia et al., 2022) Pengamanan Audio Rindik Bali Menggunakan Metode Least Significant Bit Berbasis Android.	√						√		

13.	(Ulum et al., 2021) Perbandingan Teknik Steganografi Domain Spasial Dengan Domain Transformasi Pada Audio.					√			√	
14.	(Laksono et al., 2024) Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab.							√		
15.	(Akmal & Furqan, 2023) Implementasi Metode Least Significant Bit Dalam Teknik Steganografi pada Berkas Audio Dengan Stego Citra Digital.							√		
	Tugas Akhir		√	√						

2.4. Penelitian Terdekat

Berdasarkan dari penelitian sebelumnya maka penelitian terdekatnya yaitu Deteksi Posisi Penyisipan Pesan Text Pada Steganografi Audio Dengan Metode Mfcc Dan Decison Tree, persamaanya yaitu dengan penyisipan text pada

steganografi. perbedaanya hanya menggunakan metode MFCC dan decision tree hanya saja dalam file audio, tidak semua file multimedia. kelebihanya yaitu Metode MFCC dan Decsion Tree dapat diimplementasikan dalam sistem steganalisis dan sistem deteksi posisi audio tersteganografi. Pada pengujian pengaruh ciri statistik didapatkan bahwa ciri statistik Sekwness menjadi ciri statistik terbaik. Pada pengujian sistem steganalisis dihasilkan akurasi terbaik sebesar 67,52%. Untuk akurasi deteksi posisi didapat sebesar 94,73% dan deteksi terhadap letak posisi didapat akurasi sebesar 46,58%. Kekuranganya yaitu tidak adanya metode yang sangat signifikan sehingga isinya hanya berupa tingkat akurasi.

2.5. Relevansi Penelitian

Penelitian yang dilakukan memiliki relevansi atau keterkaitan dengan penelitian terkait sebelumnya. Perbandingan terkait relevansi penelitian dapat dilihat di bawah ini:

Penelitian Jawad Salahuddin tahun 2022, Judul A Study on Image, Audio and Video steganography. Masalah penelitian menyajikan sebuah web aplikasi yang memungkinkan pengguna untuk melakukan steganografi pada gambar, audio dan video bersama enkripsi yang kuat untuk pesan teks rahasia yang akan tertanam dalam multimedia. Penelitian ini dilakukan agar aplikasi web tersebut dapat dikembangkan dan memudahkan pengguna berbagi informasi sensitif tanpa khawatir informasi tersebut akan dicuri oleh penyerang.

Penelitian ini dapat ditingkatkan lebih lanjut karena setiap modul dienkapsulasi dan diimplementasikan sebagai perpustakaan yang dapat diimpor. 1) Steganografi teks: Ini adalah jenis steganografi di mana teks dapat dikodekan di dalamnya setiap huruf dari teks lain di dalam file teks. 2) Steganografi gambar: Dalam steganografi jenis ini, kami menggunakan gambar sebagai objek sampul dan menyembunyikan teks di dalam gambar. Semakin besar resolusi gambar, semakin banyak data yang kita dapat simpan di dalamnya. 3) Steganografi audio: Steganografi audio telah digunakan sejak lama untuk melindungi audio terhadap replikasi yang tidak sah. Ini juga disebut penandaan air audio. 4) Steganografi video: Ini adalah jenis steganografi yang menggunakan video sebagai sampul media untuk secara diam-diam menyematkan teks ke dalamnya. Karena video adalah

kumpulan gambar diam, kosinus diskrit transform adalah yang paling umum digunakan untuk menyembunyikan data di setiap gambar video. 5) Steganografi jaringan: Ini melibatkan penyembunyian data dalam protokol jaringan seperti TCP, UDP dll. Untuk penelitian yang di atas adalah pembandingan maka penelitian yang diteliti oleh penulis yang berjudul, Steganografi Pengukuran tingkat akurasi dan kualitas file multimedia menggunakan algoritma low bit coding. Masalah penelitiannya yaitu untuk mengukur tingkat akurasi dan kualitas file multimedia menggunakan algoritma low bit coding dan cara melakukan pengujian dengan parameter Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR). untuk mencapai nilai akurasi dan kualitas file multimedia. Objek Penelitian yaitu format multimedia seperti audio, video, gambar dan dokumen. algoritma/metode yang dipakai yaitu algoritma low bit coding. Batasanya Jenis file citra digital yang digunakan adalah format JPEG, Jenis file audio maksimal 8mb, Jenis file video maksimal 1080p dan file dokumen maksimal 1mb.