

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi komunikasi dan informasi telah membawa perubahan signifikan dalam cara kita bertukar informasi. Dalam era digital ini, keamanan dan kerahasiaan informasi menjadi aspek yang sangat penting. Berbagai kasus kebocoran data dan serangan siber yang terjadi di berbagai sektor menunjukkan bahwa sistem informasi memiliki kerentanan yang tinggi terhadap ancaman. Contohnya saja pada tahun 2020, data pribadi lebih dari 500 juta pengguna *Facebook* berhasil dibobol [1]. Selain itu marak pula kasus serangan brute-force yaitu teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin [2]. Pada Juli 2024, seorang pengguna dengan nama 'ObamaCare' mengunggah database bernama *RockYou2024* ke forum peretas populer. Database ini berisi 9.948.575.739 kata sandi dalam bentuk teks biasa, yang dapat dengan mudah dibaca dan digunakan oleh siapa pun yang mengaksesnya [3]. Oleh karena itu, diperlukan solusi berupa metode penyembunyian data yang dapat melindungi informasi sensitif dari ancaman kebocoran dan serangan siber.

Cara untuk melindungi informasi sensitif adalah dengan menerapkan berbagai teknik penyembunyian data, seperti kriptografi dan steganografi [4]. Kriptografi merupakan teknik untuk menyembunyikan pesan rahasia dengan mengacak informasi menggunakan perhitungan matematis yang kompleks, sehingga sulit untuk dipahami [5]. Namun, dalam penerapannya, kriptografi memiliki kelemahan, yaitu pesan yang telah terenskripsi dapat dilihat dengan mudah sehingga menimbulkan kecurigaan [6]. Berbeda dengan kriptografi yang membuat pesan terlihat acak, steganografi menyembunyikan pesan dalam media lain sehingga keberadaannya lebih sulit terdeteksi [7]. Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan [8]. Dalam konteks digital, steganografi sering digunakan untuk menyisipkan pesan rahasia ke dalam berbagai jenis file seperti gambar, audio, video, atau teks, tanpa menyebabkan perubahan

yang signifikan pada file tersebut. Oleh karena itu steganografi lebih baik diterapkan daripada kriptografi karena steganografi lebih efektif dibandingkan kriptografi dalam menyembunyikan pesan rahasia.

Terdapat berbagai metode steganografi audio seperti *LSB*, *phase coding*, *parity coding*, *echo hiding*, dan *spread spectrum* [9]. *Spread Spectrum* (SS) adalah salah satu metode steganografi yang menggunakan teknik penyebaran spektrum untuk menyembunyikan informasi dalam sinyal audio [10]. Teknik ini memanfaatkan redundansi dalam sinyal audio untuk menyisipkan pesan rahasia, sehingga sulit dideteksi oleh pihak yang tidak berwenang. Namun, tantangan utama dalam SS steganografi adalah bagaimana memastikan bahwa pesan yang disisipkan tidak mengganggu kualitas sinyal audio yang asli dan tetap tidak terdeteksi [11]. Dalam steganografi audio menggunakan metode *spread spectrum*, pesan rahasia dimodulasi dengan sinyal *Pseudo Random* dan disisipkan ke dalam audio pembawa. Energi yang dihasilkan oleh sinyal *pseudo random* juga mempengaruhi proses ekstraksi pesan rahasia dari audio pembawa. Jika energinya besar, pesan akan lebih mudah diekstrak dari audio pembawa. Sebaliknya, jika energinya kecil, pesan yang diekstrak tidak akan sesuai dengan pesan yang dikirimkan [12].

Pada steganografi standar yang menggunakan sinyal audio sebagai *cover* objek, penyisipan pesan rahasia pada bagian sinyal *silent* atau kosong dapat meningkatkan risiko terdeteksinya pesan tersebut. Oleh karena itu, diterapkan *Voice Activity Detection* (VAD) untuk mengatasi masalah tersebut. *Voice Activity Detection* (VAD) adalah teknik yang digunakan untuk mendeteksi bagian-bagian dari sinyal audio yang mengandung suara atau percakapan. Dengan menggunakan VAD, kita dapat mengidentifikasi saat-saat ketika sinyal audio tidak mengandung suara dan menggunakan momen-momen tersebut untuk menyisipkan pesan rahasia [13]. Dengan demikian, penerapan VAD pada *Spread Spectrum* Steganografi diharapkan dapat meningkatkan performa steganografi dengan meminimalkan gangguan pada sinyal audio asli dan meningkatkan kerahasiaan pesan yang disisipkan [14]. Penerapan VAD dapat mengurangi nilai *watermark energy*. *Watermark energy* dinyatakan sebagai pembuktian level deteksi yang direpresentasikan sebagai perbandingan antara sinyal distorsi dan *cover object* [15]. Pada bagian audio yang tidak memiliki suara (*silent*), nilai energi watermark

menjadi tinggi, yang bisa menyebabkan gangguan atau distorsi pada audio steganografi. Dengan menggunakan *Voice Activity Detection* (VAD), pesan rahasia hanya disisipkan pada bagian audio yang memiliki suara, sehingga energi watermark berkurang dan gangguan pada audio menjadi lebih kecil. Dengan begitu, pesan yang tersembunyi menjadi lebih sulit untuk dideteksi.

Penelitian ini penting dilakukan untuk mengetahui peningkatan performa steganografi dengan membandingkan penerapan *spread spectrum steganografi* yang menggunakan VAD dan tanpa VAD. Penerapan VAD pada *spread spectrum steganografi* memiliki potensi besar dalam meningkatkan performa steganografi audio, khususnya untuk aplikasi keamanan data seperti komunikasi rahasia di bidang militer, perbankan, dan layanan publik yang memerlukan tingkat privasi tinggi. Hasil akhir yang diharapkan adalah peningkatan performa *spread spectrum steganografi* melalui penerapan VAD.

1.2 Rumusan Masalah

Rumusan masalah pada penelitian ini yaitu sebagai berikut.

1. Bagaimana merancang sistem *spread spectrum* steganografi dengan VAD?
2. Bagaimana performa *spread spectrum* steganografi antara sistem yang menerapkan VAD dan sistem tanpa VAD?

1.3 Tujuan Penelitian

1. Merancang sistem *spread spectrum* steganografi dengan VAD
2. Membandingkan performa *spread spectrum* steganografi dengan VAD dan tanpa VAD.

1.4 Manfaat Penelitian

Manfaat penelitian ini dalam pengembangan teknologi steganografi audio meliputi:

1. Hasil penelitian dapat memberikan kontribusi terhadap peningkatan keamanan dalam penyembunyian informasi digital, khususnya dalam konteks audio steganografi.
2. Penelitian ini dapat menjadi referensi bagi pengembangan sistem keamanan data di berbagai sektor seperti militer, perbankan, dan layanan publik yang membutuhkan tingkat privasi tinggi.

3. Hasil penelitian dapat digunakan sebagai dasar untuk pengembangan lebih lanjut dalam teknik steganografi audio, terutama dalam aspek optimalisasi performa dan keamanan.
4. Penelitian ini berkontribusi pada pengayaan literatur ilmiah dalam bidang steganografi, khususnya mengenai penerapan VAD pada metode *spread spectrum* steganografi.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

1. Metode steganografi yang digunakan terbatas pada teknik *Spread Spectrum* Steganografi.
2. Penelitian ini akan menggunakan ukuran kualitas audio tertentu, seperti *Signal-to-Noise Ratio* (SNR) dan *watermark energy* terhadap *error probability* sehingga tidak akan mengevaluasi semua metode pengukuran kualitas audio yang ada.
3. Aplikasi yang digunakan dalam penelitian ini adalah MATLAB R2021a.

1.6 Sistematika Penulisan

Sistematika penulisan proposal penelitian ini sebagai berikut:

1. Bab I: Pendahuluan
Bab ini terdiri dari sub-bab latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
2. Bab II: Tinjauan Pustaka
Bab ini membahas tentang teori-teori pendukung yang digunakan dalam perencanaan dan pembuatan tugas akhir.
3. Bab III: Metodologi Penelitian
Bab ini membahas mengenai metode desain penelitian, metode pengumpulan data, metode analisis data.
4. Bab IV: Analisis dan Pembahasan
Bab ini berisikan hasil dan pembahasan mengenai tugas akhir yang telah dilakukan.
5. Bab V: Penutup

Bab ini berisi kesimpulan yang didapatkan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.

