BAB I PENDAHULUAN

1.1. Latar Belakang

Dalam era digital saat ini, keamanan data menjadi aspek yang sangat krusial, terutama karena meningkatnya frekuensi pelanggaran privasi dan serangan siber yang berdampak luas pada kehidupan sosial. Misalnya, pada Januari 2023, T-Mobile mengumumkan kebocoran data yang memengaruhi lebih dari 37 juta pelanggan, menambah daftar panjang insiden serupa yang meresahkan masyarakat dan menurunkan kepercayaan publik terhadap sistem komunikasi digital [1]. Kebocoran data dan penyalahgunaan informasi tidak hanya mengancam keamanan organisasi dan individu, tetapi juga menimbulkan kekhawatiran sosial terkait kepercayaan masyarakat terhadap teknologi digital [2].

Berbagai insiden keamanan data menunjukkan bahwa metode tradisional seperti enkripsi saja tidak menjamin perlindungan informasi secara menyeluruh. Hal ini mengindikasikan adanya kebutuhan mendesak untuk mengembangkan teknik pengamanan tambahan yang mampu menjamin kerahasiaan dan integritas data meskipun kunci enkripsi telah berhasil ditembus. Salah satu alternatif yang menjanjikan adalah *steganography*, yaitu seni dan ilmu untuk menyembunyikan informasi dalam media lain sehingga keberadaannya tidak terdeteksi oleh pihak yang tidak berwenang [3].

Steganography dapat diterapkan pada berbagai media, seperti gambar, video, dan audio, dengan masing-masing teknik memiliki keunggulan tersendiri dalam menyembunyikan informasi rahasia. Salah satu metode yang paling umum adalah *Least Significant Bit* (LSB), di mana data disisipkan ke dalam bit paling rendah dari sampel audio atau *pixel* gambar sehingga perubahannya sangat minimal dan hampir tidak terdeteksi oleh indera penglihatan atau pendengaran [4]-[6]. Teknik lain, seperti *phase coding*, menyembunyikan informasi dengan cara memodifikasi fase sinyal pembawa [7], sedangkan *echo hiding* memanfaatkan efek gema dengan menambahkan *delay* dan mengubah amplitudo untuk mengkodekan pesan rahasia [8], [9]. Begitu pula, metode *parity coding* menggunakan nilai paritas dari sekelompok bit dalam media untuk menyisipkan informasi secara tersembunyi [10]. Selain itu, metode *spread spectrum* juga digunakan dalam *steganography*, di mana informasi rahasia disebar ke seluruh spektrum frekuensi, sehingga sulit untuk dideteksi dan tampak seperti *noise* biasa [11], [12].

Peran *steganography* dalam audio digital sangat signifikan, terutama untuk aplikasi komunikasi rahasia. Di antara berbagai metode *steganography* audio,

Spread Spectrum (SS) *steganography* telah banyak digunakan karena kemampuannya dalam menyebarkan sinyal *watermark* ke seluruh spektrum audio sehingga meningkatkan ketahanan terhadap serangan dan gangguan [13]. Lebih lanjut, *Improved Spread Spectrum* (ISS) *steganography* dikembangkan sebagai upaya untuk meningkatkan performa SS, sehingga *watermark* yang disisipkan menjadi lebih tahan terhadap *noise* dan distorsi, terutama pada proses kompresi audio modern [14], [15]. Penelitian terkait *Spread Spectrum* (SS) *steganography* pada audio umumnya berfokus pada bagaimana teknik ini dapat mempertahankan pesan tersembunyi meskipun mengalami proses kompresi dan gangguan lain di saluran transmisi. Misalnya, pada Tugas Akhir "Optimalisasi *Spread Spectrum Steganography* Menggunakan *Improved Closed Loop* untuk Menyembunyikan Informasi secara Aman" [16], dibahas bagaimana metode *closed-loop* dapat meningkatkan ketahanan *watermark* terhadap berbagai bentuk serangan dengan menyesuaikan parameter *embedding* secara adaptif. Sementara itu, jurnal "Evaluasi Kinerja *Improved Spread Spectrum Steganography* pada *Advanced Audio Coding"* [14] menekankan uji coba pada kompresi *Advanced Audio Coding* (AAC) untuk melihat seberapa efektif metode SS beserta variannya, seperti *Improved Spread Spectrum* (ISS) dalam menjaga *watermark* di tengah distorsi yang dihasilkan oleh proses kompresi. Dari kedua studi tersebut, dapat disimpulkan bahwa pengujian SS *Steganography* pada audio mencakup aspek kapasitas penyisipan, ketahanan terhadap kompresi (misalnya AAC), dan kemampuan sistem mempertahankan *watermark* meskipun terjadi gangguan, yang diukur melalui parameter kualitas audio (SNR dan ODG) serta keberhasilan ekstraksi *watermark*.

Pada metode *Improved Spread Spectrum* (ISS) konvensional, proses penyisipan memerlukan sebuah parameter penting, *noise level*. Parameter ini sering kali hanya berupa nilai yang diasumsikan. Masalahnya, nilai asumsi tersebut sering kali tidak akurat dan tidak mencerminkan tingkat *noise* yang sebenarnya (*actual noise*) yang dihasilkan. Ketidakcocokan antara *noise* yang diasumsikan dan *noise* yang sebenarnya inilah yang menjadi kelemahan utama, karena dapat menyebabkan kegagalan dalam proses ekstraksi data.

Untuk mengatasi permasalahan ini, penggunaan *noise feedback* dalam ISS *steganography* diperkenalkan sebagai solusi. *Noise feedback* memungkinkan sistem untuk mengukur tingkat *noise* yang dihasilkan selama proses kompresi, sehingga parameter *embedding* dapat disesuaikan.

Penggunaan *noise feedback* ini belum dieksplorasi secara mendalam dalam konteks *audio coding*, sehingga penelitian ini bertujuan untuk mengisi kekosongan tersebut dengan mengkaji pengaruh *noise feedback* terhadap kinerja ISS *steganography* pada AAC dan Opus. Evaluasi kinerja dilakukan melalui pengukuran *Signal-to-Noise Ratio* (SNR) dan *Objective Difference Grade* (ODG),

yang masing-masing mengindikasikan seberapa besar pesan tersembunyi dipertahankan dan perbedaan antara sinyal asli dengan sinyal hasil *embedding* [17].

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana pengaruh *input noise level* pada ISS *steganography* pada AAC dan Opus?
2. Bagaimana pengaruh penggunaan *noise feedback* terhadap kinerja ISS *steganography* pada AAC dan Opus, yang diukur melalui parameter SNR dan ODG?

1.3.Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Mengetahui pengaruh *input noise level* pada *Improved Spread Spectrum* terhadap keberhasilan ekstraksi data dalam *steganography* audio.
2. Menganalisis kinerja *noise feedback* pada ISS dalam mempertahankan data setelah proses kompresi audio.

1.4. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam bidang keamanan informasi digital, khususnya pada teknik *steganography* audio. Adapun manfaat yang dapat diperoleh dari penelitian ini adalah:

1. Memberikan pemahaman mendalam tentang pengaruh *input noise level* pada teknik ISS (*Improved Spread Spectrum*) terhadap ketahanan data tersembunyi dalam proses *steganography* audio yang telah mengalami kompresi Opus dan AAC.
2. Mengetahui pengaruh dari mekanisme *noise feedback* dalam mengoptimalkan parameter *embedding*, sehingga dapat meningkatkan ketahanan data tersembunyi terhadap distorsi proses kompresi.

1.5. Batasan Masalah

Agar penelitian lebih terfokus dan terarah, beberapa batasan masalah yang diterapkan adalah sebagai berikut:

1. Pengujian dilakukan pada beberapa *frame size*, yaitu 512, 1024, 2048, 5120, dan 10240 sampel.
2. Pengujian dilakukan pada beberapa variasi nilai *noise level*, yaitu 0 dB, 5 dB, 10 dB, 15 dB, 20 dB.
3. Pengujian dilakukan pada beberapa *bitrate*, yaitu 32 kbps, 64 kbps, 80 kbps, 128 kbps.
4. Penelitian hanya dilakukan pada dua *codec* audio, yaitu *Advanced Audio Coding* (AAC) dan Opus.

5. Proses kompresi AAC menggunakan aplikasi Nero Encoder, dan Opus menggunakan aplikasi Opus Encoder.
6. Evaluasi kinerja sistem *steganography* dilakukan dengan mengukur parameter *Signal-to-Noise Ratio* (SNR) dan *Objective Difference Grade* (ODG) sebagai indikator utama.
7. Proses *embedding* dan ekstraksi diimplementasikan menggunakan algoritma ISS yang dimodifikasi, dengan simulasi dilakukan di lingkungan laboratorium menggunakan MATLAB.
8. Asumsi bahwa error kanal dalam komunikasi digital dapat diabaikan karena adanya mekanisme pengiriman ulang, sehingga kerusakan pada sinyal dihasilkan terutama oleh proses kompresi.

1.6. Sistematika Penulisan

Sistematika penulisan laporan penelitian disusun sebagai berikut:

BAB I PENDAHULUAN

Bab I berisi tentang uraian latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, dan sistematika penulisan laporan.

BAB II TINJAUAN PUSTAKA

Bab II berisi teori yang mendukung pembuatan penelitian ini seperti teori mengenai konsep yang digunakan untuk menyelesaikan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab III berisi jenis dan metode penelitian yang digunakan dalam penelitian, perancangan sistem, dan variabel penelitian.

BAB IV ANALISIS DAN PEMBAHASAN

Bab IV berisi hasil penelitian pemaparan dan penjelasan mengenai hasil pengujian, dan analisis dari hasil pengujian tersebut.

BAB V PENUTUP

BAB V berisi kesimpulan yang diambil dari penelitian beserta saran yang disampaikan penulis berdasarkan hasil analisis dan pembahasan dari penelitian.