BAB I PENDAHULUAN

1.1 Latar Belakang

Saat ini kebutuhan komunikasi dengan kecepatan tinggi dan kapasitas yang sangat besar di bidang telekomunikasi [1]. Teknologi informasi saat ini telah berkembang dengan sangat cepat. Selain itu, adanya internet saat ini mempermudah komunikasi jarak jauh. Setiap detik, internet dan media lainnya mengirimkan berjuta-juta data. Internet adalah cara terbaik untuk berkomunikasi dengan orang-orang di tempat yang jauh dan membutuhkan komunikasi yang cepat [2]. Di era komputer dan internet saat ini, menjaga keamanan sistem informasi telah menjadi hal yang sangat penting dalam berbagai aspek kehidupan. Hal ini terutama berlaku untuk informasi yang memiliki nilai tinggi, seperti yang terkait dengan keputusan bisnis, keamanan nasional, atau kepentingan publik. Banyak pihak pasti tertarik untuk mengakses informasi tersebut [3].

Keamanan dan kerahasiaan adalah aspek krusial dalam proses pertukaran pesan atau informasi melalui internet. Seiring dengan kemajuan teknologi, kejahatan siber juga berkembang dengan berbagai metode seperti interupsi, penyadapan, modifikasi, hingga fabrikasi [4]. Tanpa perlindungan yang memadai, pihak lain dapat dengan mudah mengakses informasi yang dikirimkan melalui internet, seperti yang terjadi pada kasus kebocoran data di Bank Syariah Indonesia (BSI) [5]. Insiden tersebut melibatkan akses tidak sah terhadap data pelanggan, termasuk kata sandi, yang menyebabkan kerugian besar bagi perusahaan maupun nasabahnya. Kasus ini menjadi pengingat bahwa perlindungan terhadap informasi harus mengutamakan keamanan, keakuratan, dan kesulitan untuk dideteksi selama proses pengiriman. Oleh karena itu, diperlukan sebuah metode yang dapat memberikan perlindungan terhadap pesan atau informasi dengan mengutamakan keamanan, keakuratan, dan kesulitan untuk dideteksi selama proses pengiriman informasi. Salah satu teknik yang dapat digunakan untuk menangani masalah ini adalah steganografi.

Steganografi adalah salah satu metode paling populer saat ini untuk menangani masalah keamanan data. Teknik ini merupakan seni dan ilmu dalam menyembunyikan pesan ke dalam media lain, sehingga hanya pengirim dan penerima yang menyadari keberadaan pesan rahasia tersebut, sementara pihak lain tidak menyadarinya [6] Tiga kriteria utama dalam menilai kinerja metode steganografi adalah kekukuhan, keamanan, dan kapasitas menyembunyikan informasi. Dalam proses steganografi, struktur pesan rahasia tidak diubah sebaliknya, pesan tersebut disisipkan ke dalam media penutup yang bersifat netral atau tidak bermakna (hanya berfungsi sebagai pembawa). Steganografi memiliki teknik untuk menyembunyikan keberadaan pesan sekunder pada pesan utama.

Pesan utama disebut dengan sinyal pembawa atau pesan pembawa, sinyal pembawa dapat berupa teks, audio, gambar dan video [7].

Steganografi audio adalah salah satu steganografi yang menggunakan file audio sebagai media penutup untuk membawa sebuah pesan rahasia yang dikirimkan melalui sinyal audio yang telah dimodifikasi agar tidak mencolok [8]. Proses penyisipan dalam teknik steganografi membutuhkan perhitungan menggunakan metode tertentu serta pemilihan jenis objek yang akan digunakan sebagai wadah penyimpanan data. Ada banyak teknik yang dapat digunakan dalam steganografi, diantaranya adalah *Least Significant Bit* (LSB), *Redundant Pattern Encoding*, *Echo Hiding*, dan *Spread spectrum. Teknik Least Significant Bit* (LSB) adalah metode yang digunakan untuk menyembunyikan pesan dalam steganografi. Algoritma LSB ini merupakan salah satu metode paling populer dalam steganografi audio. Algoritma ini bekerja dengan memodifikasi bit-bit terakhir pada beberapa *byte* dalam file audio, sehingga memungkinkan penyembunyian urutan *byte* yang berisi data rahasia [9].

Namun, teknik LSB rentan terhadap serangan dan dapat diekstraksi dengan mudah. Untuk mengatasinya, LSB dikembangkan lebih lanjut dengan menggunakan bilangan acak, yang dikenal sebagai teknik *redundant pattern encoding*. Teknik ini memanfaatkan media gambar sebagai tempat menyembunyikan pesan. Metode penyisipan yang digunakan melibatkan penggandaan (redundansi) pada informasi atau pesan yang akan disembunyikan, dengan catatan bahwa pesan hasil penggandaan tetap identik atau utuh seperti aslinya. Pesan tersebut kemudian disebarkan ke seluruh bagian file penampung (*cover file*) [10]. *Echo hiding* merupakan teknik penyembunyian pesan di dalam sinyal melalui pembentukan gema. Pesan disamarkan dengan mengatur tiga parameter dalam gema, yaitu besarnya amplitudo awal, tingkat penurunan redaman, dan pengaturan waktu. Adanya pengaturan waktu antara gema dan sinyal asli membuat gema bercampur dengan sinyal tersebut, sehingga sulit dibedakan oleh sistem pendengaran manusia yang tidak dapat memisahkan gema dari sinyal asli [11]. Selanjutnya, steganografi dengan metode *Spread spectrum* [12].

Metode *Spread spectrum* dalam steganografi terinspirasi oleh skema komunikasi *spread spectrum*, di mana sinyal dengan pita sempit ditransmisikan ke dalam kanal pita lebar melalui penyebaran frekuensi [13]. *Spread spectrum* memiliki keunggulan dalam hal ketahanan terhadap berbagai bentuk serangan dan gangguan *noise* karena teknik ini menyebarkan bit-bit informasi tersembunyi ke seluruh spektrum frekuensi dari sinyal penutup.

Dalam proses penyembunyian data, bit-bit informasi yang telah melalui proses penyebaran akan dimodulasi menggunakan sinyal pseudo-noise yang dihasilkan secara acak berdasarkan kunci penyembunyian. Hasil modulasi ini kemudian ditambahkan sebagai *noise* pada bit-bit terakhir dalam berkas media. Pada pihak penerima, sinyal tersebut diambil kembali dengan menggunakan replika sinyal *pseudo-noise* yang telah disinkronkan. Media yang telah memuat informasi

rahasia tersebut terlebih dahulu melalui proses penyaringan (*pre-filtering*) untuk memperoleh *noise*. *Noise* yang diperoleh kemudian dimodulasi dengan sinyal pseudo-noise untuk menghasilkan bit-bit yang berkorelasi. Bit-bit yang berkorelasi ini kemudian dianalisis melalui perhitungan tertentu untuk mendapatkan informasi asli yang tersembunyi [14].

Penggunaan metode *Spread spectrum* (SS) dalam steganografi audio memiliki dampak langsung terhadap kualitas bit-bit yang diekstraksi pada tahap penerimaan. Karena metode ini menyebarkan informasi rahasia ke seluruh spektrum frekuensi menggunakan sinyal *pseudo-noise*, keberhasilan deteksi bit tergantung pada kekuatan sinyal *watermark* relatif terhadap noise dan distorsi audio. Jika *Watermark Energy* yang digunakan tidak mencukupi, sinyal *watermark* akan melebur dengan noise latar atau terhapus akibat proses kompresi dan manipulasi audio, sehingga bit-bit yang diekstraksi cenderung mengalami kesalahan (*bit error*). Hal ini menyebabkan peningkatan nilai *Bit Error Rate* (BER), menurunkan akurasi pesan yang diterima, dan berisiko menyebabkan kehilangan informasi secara keseluruhan. Hal ini menunjukkan bahwa tanpa penguatan sinyal *watermark* melalui *Watermark Energy* yang optimal atau teknik adaptif lainnya, kualitas dan keandalan bit-bit yang diekstraksi dalam metode *Spread Spectrum* konvensional sangat terbatas, terutama dalam lingkungan dengan gangguan atau proses transformasi sinyal.[15], [16]

Untuk meningkatkan kinerja dan ketahanan metode ini, dikembangkanlah teknik steganografi *Improved Spread spectrum* (ISS), yang merupakan pengembangan dari *Spread spectrum* khususnya pada *MPEG Spatial Audio Object Coding* (SAOC). ISS terbukti memberikan peningkatan yang signifikan dalam menekan kesalahan pada bit-bit pesan rahasia jika dibandingkan dengan *spread spectrum*, sehingga mampu menjaga integritas data yang disisipkan dengan lebih baik. [17]

Pada penelitian sebelumnya metode *spread spectrum*, kualitas audio berubah berdasarkan banyaknya data yang disisipkan. Semakin banyak data yang disisipkan, maka nilai kualitas audio semakin kecil, tetapi keamanan data lebih terjamin karena menggunakan kode penyebar yang tidak diketahui oleh pihak lain [18]. Penelitian lain menunjukkan bahwa teknik penyisipan data dapat diterapkan secara efektif tanpa mengurangi *bitrate* atau kualitas audio. Kemampuan teknik ini untuk melindungi data dari gangguan dan serangan juga terbukti kuat selama evaluasi. Dengan demikian, metode ISS pada *MPEG Spatial Audio Object Coding* (SAOC) efektif dalam meningkatkan kapasitas penyisipan data dan ketahanan terhadap deteksi serta gangguan, sambil mempertahankan kualitas audio yang tinggi [19].

Penelitian sebelumnya menunjukkan bahwa penyisipan data dalam audio memengaruhi kualitas audio secara langsung semakin besar kapasitas data yang disisipkan, semakin terdegradasi kualitas audio. Degradasi audio ini dapat menyebabkan sinyal hasil *embedding* menjadi lebih mudah terdeteksi. Ketika

proses penyisipan mengubah struktur audio secara signifikan, perubahan tersebut dapat menarik perhatian dan memungkinkan pihak ketiga untuk mendeteksi adanya modifikasi pada file audio.

Dalam steganografi audio, panjang frame adalah jumlah sampel dalam satu blok yang digunakan untuk menyisipkan data rahasia. Panjang frame sangat berpengaruh terhadap kualitas audio, kapasitas penyisipan data, dan keamanan pesan tersembunyi. Jika panjang frame besar, data yang disisipkan akan tersebar lebih luas sehingga perubahannya hampir tidak terdengar dibandingkan dengan audio aslinya. Namun, akibatnya kapasitas penyisipan data menjadi lebih kecil. Sebaliknya, jika panjang frame kecil, lebih banyak data bisa disisipkan, tetapi perubahan pada audio akan lebih jelas terdengar, sehingga lebih mudah terdeteksi.[20]

Penelitian terhadap pengaruh panjang frame dalam steganografi audio sangat penting untuk memastikan efisiensi dan efektivitas proses penyisipan data. Panjang frame memengaruhi tiga aspek utama, yaitu kualitas audio, kapasitas pesan rahasia, dan tingkat keamanan data yang disisipkan. Panjang frame yang tidak optimal dapat menyebabkan degradasi audio yang mencolok, kapasitas penyisipan yang terbatas, atau bahkan meningkatkan risiko deteksi pesan tersembunyi. Dengan memahami bagaimana panjang frame memengaruhi aspek-aspek tersebut, metode *embedding* dapat dioptimalkan untuk menjaga keseimbangan antara kualitas audio yang tinggi, kapasitas penyisipan yang memadai, dan keamanan data yang lebih baik. Penelitian ini juga penting untuk mengembangkan teknik steganografi yang lebih andal dan adaptif terhadap kebutuhan aplikasi modern, seperti komunikasi rahasia dan perlindungan informasi sensitif. Oleh karena itu, ini disusun dalam Tugas Akhir yang berjudul "Analisis Pengaruh Panjang Frame pada Metode *Spread Spectrum* terhadap Kualitas Audio dan Kapasitas Data dalam Steganogafi Audio."

1.2 Rumusan Masalah

Dalam tugas akhir ini dirumuskan beberapa masalah, yaitu:

1. Bagaimana pengaruh panjang frame terhadap kualitas audio pada steganografi audio metode *spread spectrum*?
2. Bagaimana panjang frame memengaruhi kapasitas penyisipan data dalam steganografi audio metode *spread spectrum*?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menganalisis pengaruh variasi panjang frame dalam metode *spread spectrum* terhadap kualitas audio pada steganografi audio.
2. Mengidentifikasi kapasitas maksimum penyisipan data yang dapat dicapai dengan variasi panjang frame dalam metode *spread spectrum* tanpa mengorbankan kualitas audio.

3. Mengevaluasi bagaimana perubahan panjang frame memengaruhi kualitas audio dan kapasitas penyisipan data setelah audio pembawa dikompresi ke dalam format AAC dan dikonversi kembali ke .WAV.

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Penelitian ini menguji variasi panjang frame dalam rentang 1024 hingga 140288 sampel untuk menganalisis pengaruhnya terhadap kualitas audio dan kapasitas penyisipan data.
2. Sampel audio yang digunakan berformat .wav, memiliki durasi 270 detik, dengan laju pengambilan sampel (*sample rate*) sebesar 48 kHz.
3. Pesan yang disisipkan berupa teks yang telah dikonversi menjadi deretan bit digital.
4. Audio hasil penyisipan dikompresi menggunakan format *Advanced Audio Coding* (AAC) dengan Nero AAC Codec.
5. Pengujian dilakukan dengan tiga variasi *bitrate*, yaitu 32 *kbps*, 64 *kbps*, dan 128 *kbps*.
6. Metode penyisipan data yang digunakan adalah *spread spectrum*.
7. Seluruh proses *embedding* dan ekstraksi data dilakukan menggunakan perangkat lunak MATLAB R2022a.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat dalam mengembangkan teknik steganografi audio berbasis *spread spectrum* dengan menentukan panjang frame optimal yang menjaga keseimbangan antara kualitas audio dan kapasitas penyisipan data.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika sebagai berikut.

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang, rumusan masalah, tujuan penelitian, batasan masalah, manfaat penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi tentang teori dasar yang mendukung dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang penjelasan dan langkah-langkah mengenai penelitian yang dilakukan.

BAB IV HASIL DAN ANALISA

Bab ini membahas tentang hasil dan pembahasan mengenai tugas akhir yang telah dilakukan.

BAB V PENUTUP

Bab ini berisikan kesimpulan dan saran dari penulis setelah melakukan penelitian untuk penelitian selanjutnya.