BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era digital saat ini, keamanan data menjadi isu yang sangat penting seiring dengan meningkatnya jumlah data yang dipertukarkan dan disimpan secara elektronik. Kasus-kasus kebocoran data dan serangan siber yang terjadi di berbagai sektor telah menunjukkan betapa rentannya sistem informasi terhadap ancaman. Misalnya, pada tahun 2020, sebuah serangan siber besar-besaran berhasil membobol data pribadi lebih dari 500 juta pengguna Facebook . Selain itu, serangan *ransomware* WannaCry pada tahun 2017 menginfeksi lebih dari 200.000 komputer di seluruh dunia, menyebabkan kerugian finansial yang sangat besar dan gangguan operasional yang signifikan di berbagai organisasi (Razaulla et al., 2023).

Kejadian-kejadian ini menunjukkan bahwa metode konvensional untuk melindungi data seperti enkripsi saja tidak cukup. Ada kebutuhan mendesak untuk mengembangkan teknik-teknik tambahan yang dapat memastikan kerahasiaan dan integritas data bahkan ketika enkripsi berhasil ditembus. Salah satu alternatif teknik yang dapat digunakan adalah *steganography*, yaitu seni dan ilmu menyembunyikan informasi dalam media lain sehingga keberadaannya tidak diketahui oleh pihak ketiga (Tanwar & Bisla, 2014).

Steganography dapat diterapkan dalam berbagai bentuk media, termasuk gambar, video, dan audio. Beberapa jenis *Steganografi* yang umum digunakan meliputi *Least Significant Bit* (LSB), *phase coding, echo hidding, parity code*, dan *Spread Spectrum* (SS). Least Significant Bit (LSB) adalah teknik yang menyisipkan informasi rahasia pada bit paling tidak signifikan dari piksel gambar atau sampel audio, membuat perubahan yang sangat kecil sehingga tidak dapat dideteksi oleh penglihatan atau pendengaran manusia (Hao et al., 2024). Phase coding menyisipkan informasi dengan mengubah fase sinyal pembawa, biasanya digunakan dalam steganografi audio (Sayed & Wahbi, 2024). Echo hiding menyisipkan informasi dengan menambahkan gema kecil pada sinyal audio, dimana informasi dikodekan dalam perbedaan waktu dan amplitudo dari gema tersebut (Lahiri & Tech, 2016). Parity code adalah teknik yang menggunakan

paritas (ganjil atau genap) dari sekelompok bit dalam media penutup untuk menyembunyikan informasi (Mahajan & Kour Bali, 2014). Spread Spectrum (SS) menyebarkan bit-bit informasi tersembunyi ke seluruh spektrum frekuensi sinyal penutup, membuatnya sangat tahan terhadap berbagai bentuk serangan dan noise (Kuznetsov et al., 2022).

SS steganography memiliki keunggulan dalam hal ketahanan terhadap berbagai bentuk serangan dan noise, karena teknik ini menyebarkan bit-bit informasi tersembunyi ke seluruh spektrum frekuensi sinyal penutup. Kelebihan ini membawa SS pada pengembangan lebih lanjut menjadi Improved Spread Spectrum (ISS). Teknik ISS memanfaatkan pengetahuan tentang sinyal yang digunakan oleh encoder untuk meningkatkan kinerja dengan memodulasi energi watermark yang dimasukkan untuk mengimbangi interferensi sinyal. Pendekatan ini menghasilkan peningkatan signifikan yang mana pengurangan probabilitas kesalahan sebesar sepuluh atau lebih, tergantung pada rasio sinyal terhadap noise dan probabilitas kesalahan operasi (Malvar & Florêncio, 2003).

ISS *Steganography* telah diaplikasikan pada sistem transmisi digital modern (Dwiharzandis et al., 2019), namun performansinya pada pengkodean AAC belum diketahui. Mengingat penggunaan AAC yang lebih luas dibandingkan dengan pengkodean lain, dan menjadi basis pengkodean terbaru seperti MPEG Surround (Luthfi et al., 2018), MPEG SAOC(Luthfi et al., 2017), dan MPEG-H 3D Audio, performansi ISS pada AAC perlu diketahui. AAC dikenal karena efisiensinya dalam kompresi audio, namun proses kompresi dan dekompresi yang dilakukan dapat mengakibatkan distorsi yang signifikan pada sinyal audio, yang dapat mempengaruhi keakuratan dan keandalan teknik steganografi yang diterapkan (Herre & Dick, 2019).

Tantangan utama dalam penggunaan ISS pada AAC adalah memastikan bahwa data tersembunyi tetap terjaga selama proses kompresi dan dekompresi yang kompleks. Hal ini memerlukan optimasi proses embedding dan ekstraksi, serta penanganan noise yang tepat. Terdapat dua metode yang dapat digunakan pada sistem embedding ISS, yaitu metode Maximum Distortion dan Optimum ISS. Metode Maximum Distortion mengoptimalkan kekuatan sinyal embedding dengan memaksimalkan distorsi yang dapat ditoleransi oleh sistem, sementara metode

Optimum ISS bertujuan untuk menyeimbangkan antara distorsi dan ketahanan terhadap noise.

Selain itu, dengan menambahkan AAC decoder pada sisi pengirim, level noise saat sinyal ditransmisikan dapat dihitung. Teknik ini dikenal sebagai noise feedback. Noise feedback memungkinkan sistem untuk mengukur tingkat noise yang dihasilkan oleh proses kompresi dan dekompresi AAC, sehingga dapat digunakan untuk menyesuaikan proses embedding agar lebih tahan terhadap gangguan. Dengan mengetahui tingkat noise ini, proses embedding dapat dioptimalkan sehingga data tersembunyi dapat bertahan terhadap gangguan yang disebabkan oleh kompresi.

Penelitian ini bertujuan untuk mengevaluasi kinerja ISS Steganography pada AAC dengan menggunakan metode Maximum Distortion dan Optimum ISS, serta memanfaatkan noise feedback untuk meningkatkan keandalan sistem. Evaluasi dilakukan dengan mengukur hubungan antara watermark energy dan error probability pada berbagai bitrate kompresi AAC. Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan sistem steganografi yang lebih aman dan efisien untuk aplikasi multimedia modern.

1.2. Perumusan Masalah

Penelitian ini mengatasi masalah dari implementasi *Improved Spread Spectrum* (ISS) *Steganography* pada *Advanced Audio Coding* (AAC), yaitu:

1. Bagaimana kinerja metode *Maximum Distortion* ISS dibandingkan dengan *Spread Spectrum* (SS) *Steganography* standar pada berbagai *bitrate*?
2. Bagaimana performa metode Optimum ISS pada lingkungan transmisi digital dengan kompresi AAC?
3. Seberapa besar pengaruh penggunaan *noise feedback* terhadap kinerja ISS *Steganography* pada AAC?
4. Bagaimana ISS *Steganography* dapat dioptimalkan untuk memastikan data tersembunyi tetap terjaga selama proses kompresi dan dekompresi AAC?

1.3. Tujuan

Penelitian ini memiliki beberapa tujuan, yaitu:

1. Mengevaluasi kinerja metode *Maximum Distortion* ISS dibandingkan dengan SS *Steganography* standar pada berbagai *bitrate*.
2. Menentukan performa metode *Optimum* ISS dalam lingkungan transmisi digital dengan kompresi AAC.
3. Mengukur pengaruh penggunaan *noise feedback* terhadap kinerja ISS *Steganography* pada AAC.
4. Mengoptimalkan ISS *Steganography* untuk memastikan data tersembunyi tetap terjaga selama proses kompresi dan dekompresi AAC.

1.4. Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Pengujian dilakukan pada berbagai *bitrate* AAC, yaitu 32 kbps, 64 kbps, dan 80 kbps.
2. Sampel audio yang digunakan adalah dalam format *Wave* Audio dengan *sample rate* 48 kHz, *bit depth* 16 bit, durasi 7781 detik, dan *mono channel*.
3. Pengujian dilakukan dengan menggunakan metode *Maximum Distortion* ISS dan *Optimum* ISS.
4. Proses embedding dan ekstraksi dilakukan menggunakan MATLAB.
5. Proses kompresi AAC menggunakan aplikasi Neroencoder.
6. Hanya menggunakan SS *Steganography* sebagai metode pembanding.

1.5. Sistematika Penulisan

Penulisan penelitian ini disusun secara sistematis untuk memberikan gambaran yang jelas dan terstruktur tentang keseluruhan proses penelitian. Sistematika penulisan terdiri dari beberapa bab yang dirinci sebagai berikut:

BAB I Pendahuluan, berisi latar belakang, tujuan penelitian, batasan masalah, penelitian terkait , dan sistematika penulisan.

BAB II Penjelasan teori yang berhubungan *Improved Spread Spectrum Steganography* dan *Advanced Audio Coding*.

BAB III Metodologi Penelitian, berisikan rancangan implementasi sistem dan langkah-langkah pengujian beserta penjelasan mengenai penelitian yang dilakukan.

BAB IV Hasil dan Pembahasan, berisikan analisis hasil penelitian.

BAB V Penutup, berisikan beberapa kesimpulan dan saran yang bisa ditarik dan disampaikan yang didasari dari hasil penelitian.