



Artikel Penelitian

Evaluasi Kinerja Improved Spread Spectrum Steganography pada Advanced Audio Coding

Amirul Luthfi^{a,b,*}, Novirman Jamarun^{a,c}

^a Program Studi Pendidikan Profesi Insinyur, Universitas Andalas, Limau Manis, Padang, 25163, Indonesia

^b Departemen Teknik Elektro, Universitas Andalas, Limau Manis, Padang, 25163, Indonesia

^c Fakultas Peternakan, Universitas Andalas, Limau Manis, Padang, 25163, Indonesia

INFORMASI ARTIKEL

Sejarah Artikel:

Diterima Redaksi: 11 Agustus 2024

Revisi Akhir: 12 Januari 2025

Diterbitkan Online: 14 Januari 2025

KATA KUNCI

Steganography,

Improved Spread Spectrum,

Noise Feedback,

Advanced Audio Coding

KORESPONDENSI

E-mail: amirul@eng.unand.ac.id*

ABSTRACT

Penelitian ini mengevaluasi kinerja Improved Spread Spectrum (ISS) Steganography pada Advanced Audio Coding (AAC), sebuah format kompresi audio yang efisien namun proses kompresinya yang kompleks dapat mempengaruhi akurasi teknik Steganography. Metode embedding ISS yang digunakan meliputi Maximum Distortion dan Optimum ISS serta pemanfaatan noise feedback untuk mengoptimalkan keutuhan data selama proses kompresi dan dekompresi. Penelitian ini juga melibatkan Spread Spectrum (SS) Steganography standar sebagai referensi pengukuran kinerja ISS Steganografi. Hasil penelitian menunjukkan bahwa metode Maximum Distortion ISS memberikan peningkatan kinerja yang signifikan, untuk mencapai error probability mendekati -5, ISS membutuhkan watermark energy sekitar 18 pada bitrate 80 kbps dibandingkan dengan metode SS standar yang membutuhkan watermark energy sebesar 104. Sebaliknya, metode Optimum ISS menunjukkan performa yang kurang memadai dengan error probability sekitar -0.5 pada kompresi AAC. Penggunaan noise feedback terbukti mampu mencapai kinerja optimal pada seluruh bitrate transmisi yang diuji dibandingkan dengan masukan level noise statis. Kesimpulan dari penelitian ini adalah bahwa metode Maximum Distortion ISS dengan noise feedback direkomendasikan untuk digunakan pada kanal transmisi digital dengan kompresi AAC, memberikan kinerja yang lebih baik dalam menjaga data tersembunyi selama proses kompresi dan dekompresi.

1. PENDAHULUAN

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 [1]. 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 [2].

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 [4]-[6].

Steganography dapat diterapkan dalam berbagai bentuk media, termasuk gambar, video, dan audio. Beberapa jenis Steganography yang umum digunakan meliputi Least Significant Bit (LSB) [7]-[8], phase coding [9], echo hiding [10], parity code [11], dan Spread Spectrum (SS) [12]-[13]. 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) [14]-[15].

ISS *Steganography* telah diaplikasikan pada sistem transmisi digital modern [16], 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 [17]-[19], MPEG SAOC[19]-[21], dan MPEG-H 3D Audio [21], 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 *Steganography* yang diterapkan [22].

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

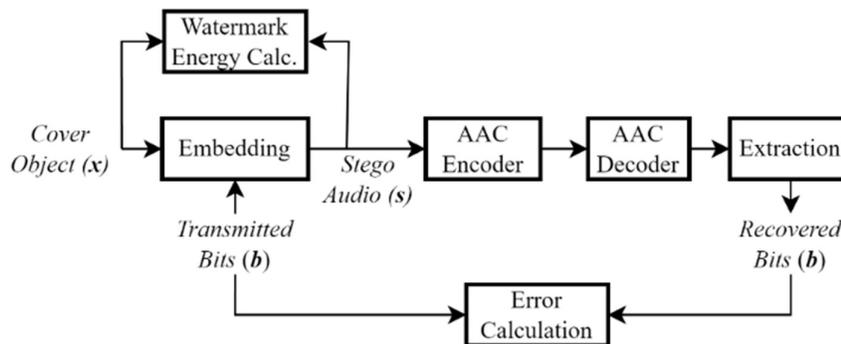
lebih tahan terhadap gangguan. Dengan mengetahui tingkat *noise* ini, proses *embedding* dapat dioptimalkan sehingga data tersembunyi dapat bertahan terhadap gangguan yang disebabkan oleh kompresi.

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.

2. METODE EVALUASI KINERJA

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.

Pengukuran kinerja ISS *Steganography* pada AAC dilakukan dengan menganalisis grafik hubungan antara *watermark energy* dan *error probability*, yang memberikan gambaran tentang kemampuan sistem dalam menjaga integritas informasi tersembunyi. Adapun *watermark energy* yang disebut juga level distorsi menggambarkan seberapa sulit sinyal *embedding* dideteksi. Sementara itu, *error probability* menggambarkan kapasitas *embedding*-nya.



Gambar 1. Blok Diagram Pengukuran *Watermark Energi* dan *Error Probability*

Watermark energy diukur dengan terlebih dahulu membandingkan *cover object* (x) dan *stego audio* (s) untuk mendapatkan sinyal distorsi (D) menggunakan

$$D = s - x \quad (1)$$

Selanjutnya, *watermark energy* (WE) direpresentasikan sebagai perbandingan antara sinyal distorsi (D) dan *cover object* (x) yang dihitung menggunakan

$$WE = \frac{N \text{ var}(D)}{\text{var}(x)} \quad (2)$$

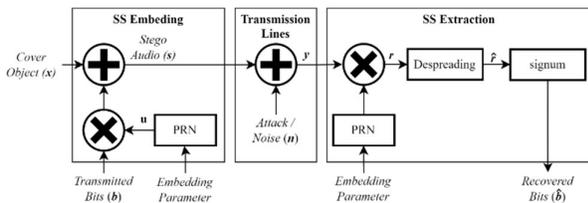
Adapun *error probability* (EP) diukur berdasarkan perbandingan jumlah bit yang *error* terhadap total seluruh bit yang ditransmisikan dan direpresentasikan dalam bentuk logaritmik basis 10 menggunakan

$$EP = \log_{10} \left(\frac{\text{Jumlah Error}}{\text{Total Bit}} \right) \quad (3)$$

Hubungan kedua variabel ini akan ditampilkan dalam bentuk grafik yang secara tidak langsung juga menyatakan hubungan antara kapasitas *embedding* dan level distorsi.

Tabel 1. Sampel Audio

No.	Parameter	Format
1.	Format	Wave Audio
2.	Sample Rate	48 kHz
3.	Bit Depth	16 bit
4.	Durasi	7781 detik
5.	Channel	Mono (satu kanal)
6.	Konten	Campuran: musik, lingkungan (<i>environment</i>), dan percakapan (<i>speech</i>)



Gambar 2. Blok Diagram Spread Spectrum Steganography.

Kinerja diukur menggunakan pada *bitrate* transmisi AAC 32 kbps, 64 kbps, dan 80 kbps. Sementara itu, bit informasi yang disisipkan (*transmitted bits*) dihasilkan oleh komputer secara acak (*random bits*) untuk memastikan data yang disisipkan bersifat seragam dan acak. Kemudian, *password* atau *key* untuk proses *embedding* juga dihasilkan secara acak oleh komputer, memastikan keamanan dan keunikan setiap proses *embedding*. Adapun *sample* audio (*cover object*) yang digunakan adalah *wave* audio yang memuat beragam jenis audio seperti yang ditampilkan pada Tabel 1.

3. MAXIMUM DISTORTION DAN OPTIMUM ISS STEGANOGRAPHY

Improved Spread Spectrum (ISS) dibangun berdasarkan *Spread Spectrum* (SS) standar dengan memodifikasi proses *embedding*. Pada SS, mengacu pada Gambar 2, proses *embedding* dilakukan menggunakan persamaan

$$s = x + ub \quad (4)$$

Sementara itu, pada ISS persamaan 4 dimodifikasi menjadi

$$s = x + (\alpha b - \lambda x)u \quad (5)$$

dengan

$$\alpha = \sqrt{\frac{N\sigma_u^2 - \lambda^2\sigma_x^2}{N\sigma_u^2}} \quad (6)$$

$$\lambda = \begin{cases} \lambda_0, & \text{jika } -\frac{\alpha}{(1-\lambda_0)} < bx < \frac{\alpha}{\lambda_0} \\ \frac{\alpha b}{x}, & \text{lainnya} \end{cases} \quad (7)$$

$$x = \frac{\langle x, u \rangle}{\|u\|} \quad (8)$$

dan

$$\lambda = \begin{cases} \lambda_0, & \text{jika } -\frac{\alpha}{(1-\lambda_0)} < bx < \frac{\alpha}{\lambda_0} \\ \frac{\alpha b}{x}, & \text{lainnya} \end{cases} \quad (9)$$

sementara itu,

$$\sigma_z^2 = \|z\|^2 = \langle z, z \rangle \quad (10)$$

$$\langle y, z \rangle = \frac{1}{N} \sum_{i=0}^{N-1} y_i z_i \quad (11)$$

Proses *embedding* ISS menggunakan persamaan 5 disebut juga sebagai *maximum distortion* ISS. Pada *optimum* ISS, level distorsi yang disebabkan oleh proses *embedding* dibatasi menggunakan

$$s = x + w(\alpha b - \lambda x)u \quad (12)$$

dengan

$$w = \begin{cases} 0, & \text{jika } bx > \frac{\alpha}{\lambda} \\ 0, & \text{jika } bx < -K \\ 1, & \text{lainnya} \end{cases} \quad (13)$$

yang mana K disebut sebagai parameter "give up" yang dihitung menggunakan

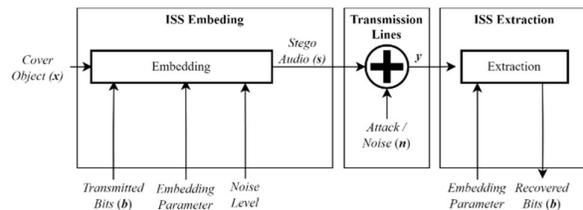
$$K = e^{-((x-\mu(x))/\sigma_n\sqrt{\alpha})^2} / \mu(x) \quad (14)$$

dan

$$\mu(x) = (\alpha - \lambda x) \quad (15)$$

Pada persamaan 14 variabel w akan mengatur transmisi dari sinyal *embedding*. Sebagaimana yang ditampilkan pada persamaan 15, nilai nol (0) pertama adalah kondisi ketika bit terdeteksi benar meskipun cover object tidak di-embedding. Sementara itu, nol (0) kedua merupakan keadaan bit tetap terdeteksi salah meskipun level energi embedding sudah maksimal. Dengan demikian distorsi atau kerusakan terhadap cover object akibat proses embedding dapat diturunkan.

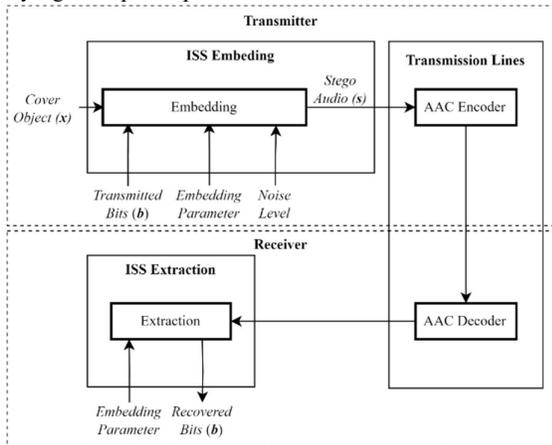
Merujuk pada persamaan 5 dan 12, salah satu variabel yang dibutuhkan dalam proses *embedding* pada ISS *steganography* adalah variabel λ . Berdasarkan persamaan 9, ISS *Steganography* membutuhkan variabel masukan tambahan berupa prakiraan *noise level* dari saluran transmisi (*n*). Noise level ini dibutuhkan untuk mendapatkan nilai σ_n yang merupakan variabel masukan untuk menghitung λ . Sehingga berbeda dengan blok diagram SS *steganography*, pada ISS *steganography* terdapat masukan tambahan berupa noise level. Sementara itu, proses extraction pada ISS *steganography* sama dengan SS *steganography*. Adapun blok diagram dari ISS *steganography* ditunjukkan pada Gambar 3.



Gambar 3. Blok Diagram Improved Spread Spectrum Steganography.

Implementasi *Improved Spread Spectrum Steganography* pada saluran transmisi digital dengan pengkode AAC dapat dilakukan dengan mengganti saluran transmisi konvensional pada Gambar 3 menjadi *encoder* dan *decoder* AAC. Pada saluran

transmisi modem yang sudah dilengkapi dengan pengkode kanal, kita dapat menganggapnya sebagai kanal ideal. Dengan demikian, kerusakan atau gangguan terhadap sinyal selama proses transmisi sebagian besar berasal dari proses kompresi oleh AAC. Hal ini berbeda dengan saluran transmisi tradisional di mana *noise* dan gangguan dapat berasal dari berbagai sumber eksternal. Sehingga penambahan *encoder* dan *decoder* AAC pada saluran transmisi sudah mewakili saluran transmisi pada sistem komunikasi digital, seperti yang ditampilkan pada Gambar 4.



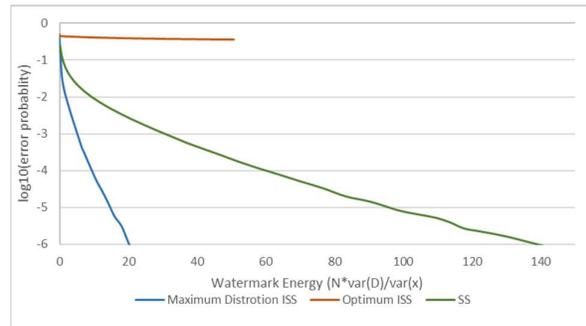
Gambar 4. Blok Diagram Implementasi ISS Steganography pada AAC

Gambar 5a menampilkan perbandingan kinerja maximum distortion ISS, optimum ISS, dan SS dengan kompresi AAC pada bitrate 80 kbps. Hasil menunjukkan bahwa maximum distortion ISS menunjukkan peningkatan performa yang signifikan dibandingkan SS standar. Bahkan, dalam error probability bernilai mendekati -5, maximum distortion ISS hanya butuh watermark energi sekitar 18, sementara SS standar membutuhkan 104. Ini menunjukkan, pada kapasitas yang sama maximum distortion ISS lebih sulit dideteksi lebih dari lima kali dibandingkan SS standar. Namun, kinerja dari optimum ISS yang lebih baik pada kanal konvensional menunjukkan performa yang buruk saat digunakan pada komunikasi digital dengan kompresi AAC. Berdasarkan data tersebut, optimum ISS bahkan tidak dapat digunakan pada kompresi AAC karena error probability yang terlalu tinggi.

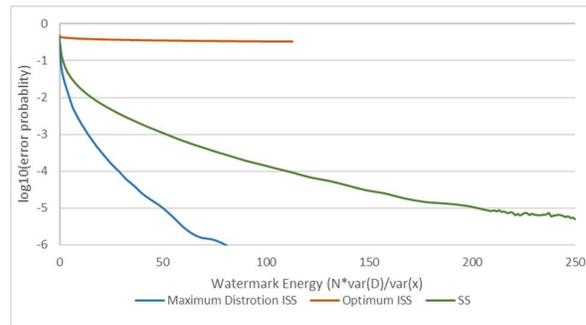
Kinerja maximum distortion ISS, optimum ISS, dan SS dengan kompresi AAC pada bitrate 64 kbps menunjukkan hal yang serupa dengan pengujian pada bitrate 80 kbps. Berdasarkan gambar 5b, terlihat watermark energy yang dibutuhkan maximum distortion ISS untuk mencapai error probability mendekati -5 adalah sekitar 50. Sedangkan SS membutuhkan watermark energy sebesar 200 untuk mencapai error probability yang sama. Sementara itu, performansi optimum ISS juga menunjukkan kinerja yang tidak baik pada bitrate 64 kbps.

Kinerja maximum distortion ISS pada bitrate 32 kbps juga meningkat secara signifikan dibandingkan SS standar, seperti yang ditampilkan pada Gambar 5c. Untuk mencapai error probability -5, maximum distortion ISS membutuhkan watermark energy sebesar 170, sedangkan SS membutuhkan watermark energy sebesar 330. Sedangkan optimum ISS pada bitrate 32 kbps juga tidak dapat digunakan karena error probability yang terlalu besar.

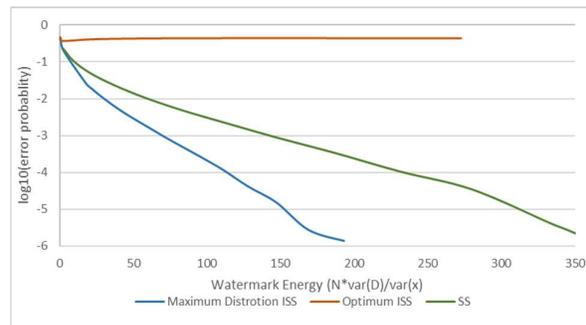
Secara keseluruhan, kinerja maximum distortion ISS pada beragam bitrate transmisi, yang diuji menunjukkan peningkatan yang signifikan dibandingkan SS standar. Peningkatannya akan semakin tinggi ketika bitrate transmisi ditingkatkan. Namun masih menunjukkan peningkatan yang signifikan hingga dua kalinya pada bitrate rendah 32 kbps. Hal ini menunjukkan bahwa maximum distortion ISS dapat digunakan sebagai metode emebeding pada saluran transmisi digital dengan kompresi AAC.



(a)



(b)



(c)

Gambar 5. Perbandingan Kinerja ISS dan SS pada AAC dengan bitrate (a) 80 kbps, (b) 64 kbps, dan (c) 80 kbps

Sementara itu, kinerja optimum ISS pada kompresi AAC menunjukkan hasil yang buruk, bahkan dalam kategori tidak dapat digunakan sebagai metode embedding. Hasil menunjukkan bahwa error probability optimum ISS berkisar pada angka -0,5, bahkan pada level watermark energy yang tinggi. Nilai error probability pada level -0,5 menyatakan bahwa 70% dari total bit yang ditransmisikan terdeteksi salah oleh sistem extraction. Hal ini menunjukkan pembatasan level distorsi pada optimum ISS tidak dapat digunakan pada sistem komunikasi digital dengan kompresi AAC.

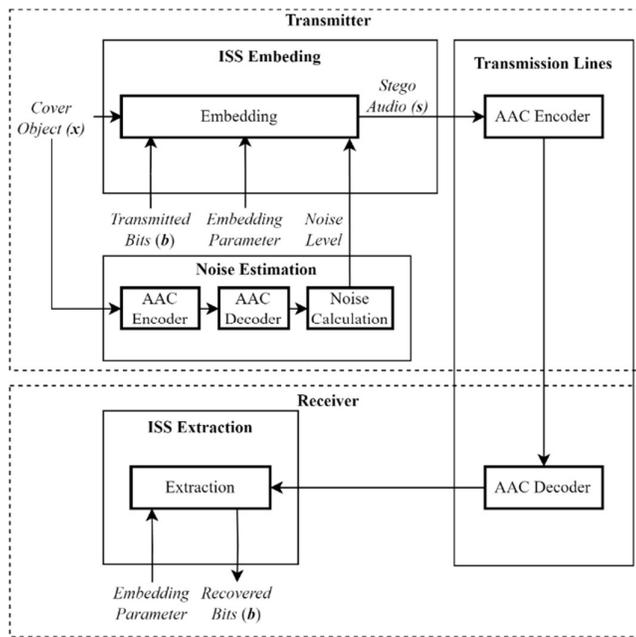
Sebagaimana dipaparkan pada persamaan 12, tidak semua sinyal embedding pada optimum ISS ditransmisikan ke receiver. Sistem seleksi frame yang di embedd pada persamaan 13 tidak dapat bekerja dengan baik pada lingkungan transmisi digital dengan kompresi perceptual. Hal ini disebabkan oleh definisi gangguan yang berbeda antara sistem komunikasi konvensional dan modern. Pada sistem komunikasi konvensional, gangguan didefinisikan sebagai perubahan sinyal akibat adanya sinyal pengganggu pada kanal transmisi. Sementara itu, pada komunikasi modern menggunakan kompresi perceptual seperti AAC, gangguan atau perubahan pada sinyal lebih dominan disebabkan oleh hilangnya komponen frekuensi pada proses kompresi.

4. IMPLEMENTASI ISS STEGANOGRAPHY PADA AAC DENGAN NOISE FEEDBACK

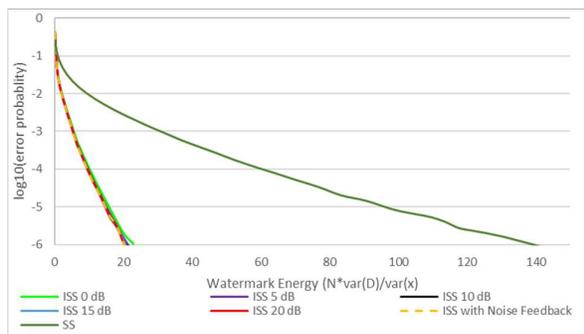
Dalam sistem transmisi audio modern, proses kompresi dan dekompresi oleh encoder dan decoder AAC menghasilkan noise

yang dapat diukur. Tingkat noise ini kemudian digunakan sebagai input pada ISS, yang memerlukan parameter tingkat noise untuk proses embedding, seperti yang ditampilkan pada Gambar 6.

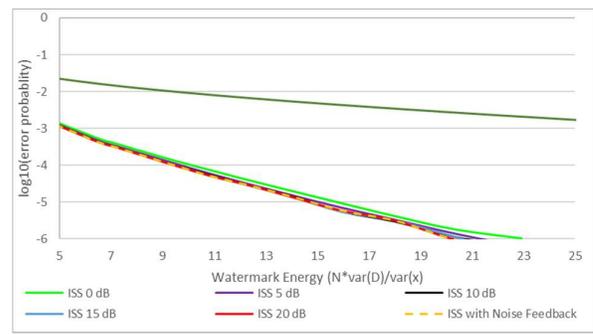
Pengukuran kinerja ini ditujukan untuk melihat seberapa besar pengaruh pemanfaatan noise feedback pada ISS Steganography. Sebagai pembanding, selain SS Steganography standar, pengujian juga melibatkan pengukuran kinerja ISS Steganography dengan memasukkan level noise dengan nilai statis pada 0 dB, 5 dB, 10 dB, 15 dB, dan 20 dB. Pengujian ISS Steganography dengan input level noise statis ini ditujukan untuk melihat besar pengaruh masukan level noise terhadap kinerja ISS. Adapun metode embeding yang digunakan pada pengujian ini adalah maximum distortion ISS Steganography. Pemilihan metode ini tentu didasarkan oleh temuan pada 4.1 yang menunjukkan bahwa maximum distortion merupakan metode embeding ISS terbaik yang dapat digunakan.



Gambar 6. Blok Diagram Implementasi ISS Steganography pada AAC dengan Noise Feedback.



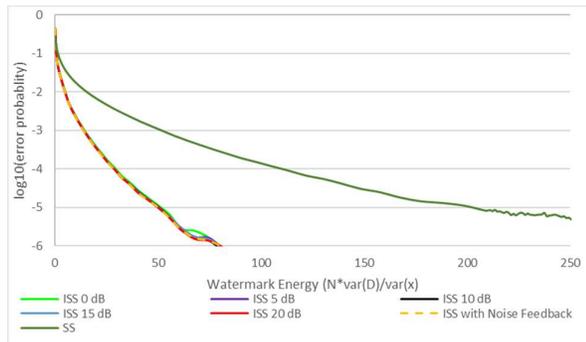
(a)



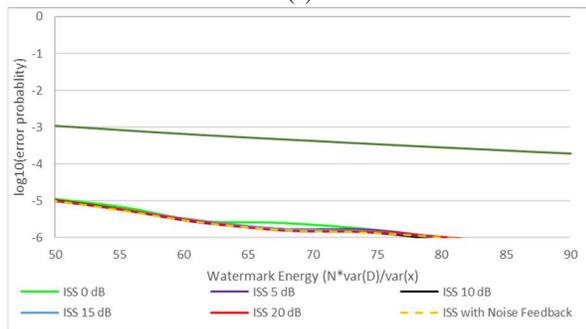
(b)

Gambar 7. Kinerja ISS Steganography dengan Noise Feedback pada AAC dengan bitrate 80 kbps

Gambar 7 menampilkan pengaruh noise feedback pada ISS Steganography di bitrate transmisi 80 kbps. Hasil pengujian menunjukkan bahwa perbedaan kinerja antara ISS Steganography yang dilengkapi dengan noise feedback tidak jauh berbeda dengan masukan noise statis. Bahkan variasi nilai noise yang di-input-kan pada sistem embedding ISS tidak memberikan pengaruh signifikan terhadap kinerjanya. Meskipun demikian, jika dilihat lebih detail, terdapat perbedaan kinerja yang disebabkan oleh perbedaan masukan level noise. Gambar 7b menunjukkan bahwa sistem embedding ISS dengan input level noise sebesar 20 dB memiliki kinerja yang sedikit lebih baik dibandingkan lainnya. Disisi lain, penggunaan noise feedback pada mampu membuat kinerja ISS Steganography pada level terbaiknya yang ditunjukkan dengan kinerja ISS Steganography dengan noise feedback sama dengan ISS Steganography dengan input level noise 20 dB.

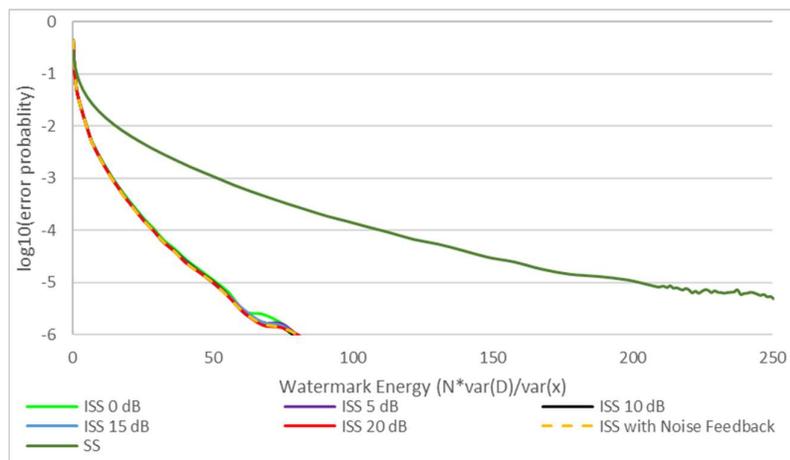


(a)



(b)

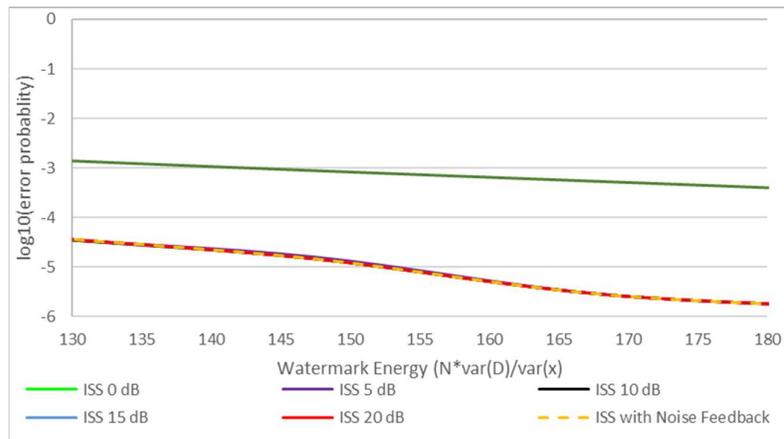
Gambar 8. Kinerja ISS Steganography dengan Noise Feedback pada AAC dengan bitrate 64 kbps



(a)

Gambar 8 yang menampilkan kinerja ISS Steganography pada bitrate 64 kbps menunjukkan trend kinerja yang serupa dengan kinerja pada bitrate 80 kbps. Dapat dilihat bahwa tidak terlihat perbedaan yang signifikan antara sistem yang dilengkapi noise feedback terhadap sistem tanpa noise feedback. Hal serupa juga terjadi terhadap variasi input level noise, yang mana besaran masukan level noise tidak memberikan perubahan yang signifikan terhadap kinerja ISS. Bahkan, jika dilihat lebih detail seperti yang ditampilkan pada Gambar 8b, pengaruh besaran level noise yang di-input-kan hanya terlihat pada masukan bernilai 0 dB. Namun demikian, noise feedback tetap memberikan hasil pengukuran kinerja terbaik.

Berbeda dengan kinerja pada bitrate tinggi, kinerja ISS dengan noise feedback pada bitrate 32 kbps menunjukkan hasil yang sangat identik, seperti yang ditampilkan pada Gambar 4.6. Hal serupa juga terjadi terhadap pengaruh masukan level noise pada embedding ISS yang menunjukkan tidak adanya pengaruh level noise yang di-input-kan terhadap kinerja ISS. Bahkan, ketika dilihat lebih detail seperti yang ditunjukkan pada Gambar 4.6.b, kinerja seluruh kondisi yang diujikan menunjukkan hasil yang hampir identik.



(b)

Gambar 9. Kinerja ISS Steganography dengan Noise Feedback pada AAC dengan bitrate 32 kbps

Secara garis besar, terlihat bahwa noise feedback secara konsisten mampu menghasilkan kinerja terbaik dibandingkan sistem dengan input level noise yang statis. Hal ini disebabkan oleh perbedaan definisi noise pada ISS yang didefinisikan sebagai tambahan sinyal yang tidak diinginkan pada saat transmisi sinyal. Sementara itu, sebagaimana yang disampaikan pada 4.1, noise pada saluran transmisi digital modern lebih dominan terhadap kerusakan sinyal akibat proses kompresi.

Disisi lain, meskipun ISS dengan noise feedback memiliki kinerja identik yang cenderung identik, namun pada bitrate 80 kbps hasil pengujian menunjukkan adanya konsistensi untuk menghasilkan kinerja terbaik. Sistem embedding ISS dengan noise feedback mampu menjamin kinerja terbaik dari ISS Steganography. Bahkan ISS Steganography dengan noise feedback mampu mencapai error probability -6 dengan watermark energy sebesar 20, dibandingkan ISS dengan masukan level noise 0 dB yang membutuhkan watermark energy sebesar 22,5. Dengan demikian, ISS Steganography dengan noise feedback dapat dijadikan opsi untuk di aplikasikan dalam pengiriman data rahasia.

5. KESIMPULAN

Penelitian ini menunjukkan bahwa metode Maximum Distortion Improved Spread Spectrum (ISS) dengan noise feedback memberikan peningkatan kinerja yang signifikan dibandingkan dengan metode Spread Spectrum (SS) standar. Sedangkan, penggunaan Optimum ISS dalam lingkungan kompresi Advanced Audio Coding (AAC) tidak direkomendasikan. Hasil penelitian mengindikasikan bahwa metode Maximum Distortion ISS mencapai error probability mendekati -5 dengan watermark energy sekitar 18 pada bitrate 80 kbps, jauh lebih efisien dibandingkan metode SS standar yang membutuhkan watermark energy sebesar 104 untuk error probability yang sama. Sebaliknya, metode Optimum ISS menunjukkan performa yang tidak memadai dengan error probability sekitar -0.5 dalam kompresi AAC. Penggunaan noise feedback terbukti mampu memastikan ISS Steganography berada pada kinerja yang terbaik dan optimal. Dengan demikian, metode Maximum Distortion ISS dengan noise feedback direkomendasikan untuk digunakan pada kanal transmisi digital dengan kompresi AAC.

DAFTAR PUSTAKA

- [1] "Facebook Data Breach: Here's What To Do Now." Accessed: Aug. 05, 2024. [Online]. Available: <https://www.forbes.com/sites/kateoflahertyuk/2021/04/06/facebook-data-breach-heres-what-to-do-now/>
- [2] S. Razaulla et al., "The Age of Ransomware: A Survey on the Evolution, Taxonomy, and Research Directions," *IEEE Access*, vol. 11, pp. 40698–40723, 2023, doi: [10.1109/ACCESS.2023.3268535](https://doi.org/10.1109/ACCESS.2023.3268535).
- [3] G. K. Murthy and T. Kanimozhi, "Methodologies in Steganography and Cryptography—Review," *Studies in Computational Intelligence*, vol. 1117, pp. 205–214, 2024, doi: [10.1007/978-3-031-43009-1_18](https://doi.org/10.1007/978-3-031-43009-1_18).
- [4] A. Arshad, N. Siddiqui, and S. Islam, "Advancement on Steganography: A Review," *Lecture Notes in Networks and Systems*, vol. 819, pp. 51–65, 2024, doi: [10.1007/978-981-99-7820-5_5](https://doi.org/10.1007/978-981-99-7820-5_5).
- [5] V. A. Rajgure and V. T. Gaikwad, "Steganography and Steganalysis : Different Approaches," *International Journal of Electronics Signals and Systems*, pp. 165–170, Jan. 2012, doi: [10.47893/ijess.2012.1032](https://doi.org/10.47893/ijess.2012.1032).

- [6] R. Tanwar and M. Bisla, "Audio steganography," ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology, pp. 322–325, 2014, doi: [10.1109/ICROIT.2014.6798347](https://doi.org/10.1109/ICROIT.2014.6798347).
- [7] C. Hao, X. Yang, Q. Ma, D. Qu, R. Wang, and T. Zhang, "Quantum audio LSB steganography with entanglement-assisted modulation," *Quantum Inf Process*, vol. 23, no. 3, Mar. 2024, doi: [10.1007/S11128-024-04312-1](https://doi.org/10.1007/S11128-024-04312-1).
- [8] "AES Engineering Briefs Forum » MPEG Surround Encoder with Steganography Feature for Data Hiding Based on LSB Method." Accessed: Aug. 05, 2024. [Online]. Available: <https://secure.aes.org/forum/pubs/ebriefs/?elib=20351>
- [9] M. H. Sayed and T. M. Wahbi, "Information Security for Audio Steganography Using a Phase Coding Method," *European Journal of Theoretical and Applied Sciences*, vol. 2, no. 1, pp. 634–647, Jan. 2024, doi: [10.59324/EJTAS.2024.2\(1\).55](https://doi.org/10.59324/EJTAS.2024.2(1).55).
- [10] S. Lahiri and B. Tech, "Audio Steganography using Echo Hiding in Wavelet Domain with Pseudorandom Sequence," *Int J Comput Appl*, vol. 140, no. 2, pp. 975–8887, 2016.
- [11] M. Mahajan and S. Kour Bali, "Combination of Steganography Using Parity Encoding and Spread Spectrum Technique," *International Journal Of Research In Electronics And Computer Engineering*, vol. 2, 2014.
- [12] A. Kuznetsov, A. Onikiychuk, O. Peshkova, T. Gancarczyk, K. Warwas, and R. Ziubina, "Direct Spread Spectrum Technology for Data Hiding in Audio," *Sensors (Basel)*, vol. 22, no. 9, May 2022, doi: [10.3390/S22093115](https://doi.org/10.3390/S22093115).
- [13] A. Anjana Krishnan, C. Satheesh Chandran, S. Kamal, and M. H. Supriya, "Spread spectrum based encrypted audio steganographic system with improved security," 2nd International Conference on Circuits, Controls, and Communications, CCUBE 2017 - Proceedings, pp. 109–114, Jun. 2018, doi: [10.1109/CCUBE.2017.8394128](https://doi.org/10.1109/CCUBE.2017.8394128).
- [14] H. S. Malvar and D. A. F. Florêncio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, Apr. 2003, doi: [10.1109/TSP.2003.809385](https://doi.org/10.1109/TSP.2003.809385).
- [15] Malvar and Florencio, "An improved spread spectrum technique for robust watermarking," pp. IV–IV, Jun. 2003, doi: [10.1109/ICASSP.2002.1004617](https://doi.org/10.1109/ICASSP.2002.1004617).
- [16] A. Dwiharzandis, A. Luthfi, and I. Elfritri, "Perancangan dan Analisis Kinerja Steganography pada MPEG SAOC Menggunakan Improved Spread Spectrum," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 3, no. 3, pp. 560–566, Dec. 2019, doi: [10.29207/RESTI.V3I3.1356](https://doi.org/10.29207/RESTI.V3I3.1356).
- [17] A. Luthfi, F. Mustaqim, and I. Elfritri, "Studi dan Analisis Kinerja Mpeg Surround pada Bitrate 256 – 400 Kbps," *Jurnal Nasional Teknik Elektro*, vol. 5, no. 3, pp. 325–331, Oct. 2016, doi: [10.25077/JNTE.V5N3.302.2016](https://doi.org/10.25077/JNTE.V5N3.302.2016).
- [18] A. Luthfi, A. K. Permana, O. Saputra, and I. Elfritri, "Experimental Study of MPEG Surround for Stereo Audio Transmission," in 2018 International Conference on Information Technology Systems and Innovation, ICITSI 2018 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Jul. 2018, pp. 531–535. doi: [10.1109/ICITSI.2018.8695996](https://doi.org/10.1109/ICITSI.2018.8695996).
- [19] J. Breebaart, G. Hotho, J. Koppens, E. Schuijers, W. Oomen, and S. Van De Par, "Background, Concept, and Architecture for the Recent MPEG Surround Standard on Multichannel Audio Compression*," *J. Audio Eng. Soc*, vol. 55, no. 5, 2007.
- [20] A. Luthfi, H. D. Laksono, and I. Elfritri, "Rendering matrix extraction in MPEG SAOC encoder for delivery of multiple multi-channel audio objects," 2017 IEEE 6th Global Conference on Consumer Electronics, GCCE 2017, vol. 2017-January, pp. 1–2, Dec. 2017, doi: [10.1109/GCCE.2017.8229371](https://doi.org/10.1109/GCCE.2017.8229371).
- [21] A. Luthfi and I. Elfritri, "Analisis Kemampuan Mpeg Spatial Audio Object Coding untuk Reproduksi Audio Multikanal," *Jurnal Nasional Teknik Elektro*, vol. 6, no. 2, pp. 97–103, Jul. 2017, doi: [10.25077/JNTE.V6N2.383.2017](https://doi.org/10.25077/JNTE.V6N2.383.2017).
- [22] J. Herre and S. Dick, "Psychoacoustic models for perceptual audio coding-A tutorial review," *Applied Sciences (Switzerland)*, vol. 9, no. 14, Jul. 2019, doi: [10.3390/APP9142854](https://doi.org/10.3390/APP9142854).