JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

Implementasi Steganografi Audio dan Gambar untuk Pengamanan Informasi

Faizah Amirah Harahap[1], Nadiyah Haaniyah Hasibuan[2], Luthan Asthalariq[3*], Soty Sohaimi[4], Dhimas Hadi Valzoe[5]
[1,2,3,4,5]Universitas Malikussaleh, Indonesia
[1]faizah.240170228@mhs.unimal.ac.id, [2]nadiyah.240170188@mhs.unimal.ac.id, [3]luthan.240170208@mhs.unimal.ac.id, [4]sotty.240170239@mhs.unimal.ac.id, [5]dhimas.240170224@mhs.unimal.ac.id

ABSTRACT

The rapid advancement of information technology has increased the risk of cyberattacks on sensitive data, creating a strong demand for advanced security techniques. Steganography complements cryptography by concealing messages within digital media so that their existence is not easily detected by unauthorized parties. This study focuses on hiding text messages in audio and image files to support secure information exchange. The research aims to implement audio and image steganography using the Least Significant Bit (LSB) method. Text messages are embedded into WAV audio files and PNG image files while maintaining media quality, minimizing detectability, and preserving file size efficiency. An experimental prototyping methodology was applied, involving system design, implementation, and testing. The LSB technique embeds messages by modifying the least significant bits of audio samples or image pixels. Data were obtained through literature review and experimental embedding and extraction procedures. The results show that text messages were successfully embedded and extracted from both audio and image files without noticeable visual or auditory degradation. File sizes remained largely unchanged, and the stego media was indistinguishable from the original as long as no compression or manipulation occurred. In conclusion, LSB-based steganography is an effective approach for information security and future enhancement research.

Kata Kunci: *Steganography, Audio, Image, Information Security, Least Significant Bit (LSB)*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah meningkatkan kebutuhan akan sistem pengamanan data yang lebih canggih. Informasi sensitif seperti data pribadi, dokumen rahasia, maupun pesan penting sering menjadi target serangan siber. Selain kriptografi, steganografi hadir sebagai metode pelengkap dengan menyembunyikan pesan dalam media digital sehingga keberadaan pesan sulit dideteksi oleh pihak yang tidak berwenang (Kusuma and Prayudi 2025).

Steganografi dapat diterapkan pada berbagai media, di antaranya gambar dan audio. Pada steganografi gambar, informasi disisipkan ke dalam piksel menggunakan teknik seperti Least Significant Bit (LSB) (Learning 2025). Sedangkan pada steganografi audio, pesan disembunyikan dalam sinyal suara baik pada domain temporal maupun frekuensi (Venna 2019). Kombinasi keduanya memberikan kapasitas penyembunyian lebih besar serta keamanan berlapis (Abd, Al-thahab, and Hamad 2025).

Beberapa penelitian telah dilakukan terkait implementasi steganografi audio dan gambar. Kusuma & Prayudi (AJIE) mengembangkan metode Masking and Filtering pada spectrogram audio. Permana meneliti optimalisasi steganografi audio dalam pengamanan informasi. Penelitian lain oleh Universitas Udayana mengintegrasikan sistem enkripsi dan steganografi untuk pengamanan data suara berbasis web (Priyamdeva et al. 2024). Di tingkat internasional, penelitian IEEE tentang Audio-in-Image Steganografi (Krishnan, Ramesh, and Urs 2025) serta studi IIETA mengenai algoritma berbasis metode chaos menunjukkan efektivitas kombinasi audio dan gambar. Selain itu, ISC International Journal of Information Security memperkenalkan pendekatan bit-wise berbasis deep learning untuk meningkatkan keamanan steganografi.

KAJIAN LITERATUR

Steganografi merupakan ilmu menulis atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Kata steganography berasal dari bahasa Yunani yaitu, *steganos* yang artinya tersembunyi atau terselubung dan *graphein* yang artinya menulis (Aditya, Pratama, and Nurlifa 2010).

Steganografi Dalam Pengamanan Informasi Digital

Steganografi merupakan salah satu teknik pengamanan informasi yang berfokus pada penyembunyian keberadaan pesan rahasia di dalam suatu media pembawa (carrier), sehingga pihak lain tidak menyadari adanya pesan tersebut. Berbeda dengan kriptografi yang hanya menyamarkan isi pesan, steganografi bertujuan menyamarkan eksistensi pesan itu sendiri. Pada jurnal Implementasi Steganografi pada Berkas Audio WAV, dijelaskan bahwa

E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

steganografi memanfaatkan karakteristik media digital untuk menyisipkan pesan tanpa menimbulkan kecurigaan dari pihak luar.

Lebih lanjut, penelitian tersebut menyebutkan bahwa media audio menjadi salah satu carrier yang efektif karena keterbatasan sistem pendengaran manusia dalam mendeteksi perubahan kecil pada sinyal suara. Hal ini menyebabkan perbedaan antara audio asli dan audio stego sulit dikenali secara subjektif oleh pendengar. Oleh karena itu, steganografi audio banyak digunakan sebagai solusi pengamanan informasi yang bersifat rahasia.

Steganografi Audio Menggunakan Metode Low Bit Coding dan LSB

Salah satu metode steganografi audio yang paling umum digunakan adalah Low Bit Coding atau Least Significant Bit (LSB). Metode ini bekerja dengan cara mengganti bit paling rendah pada setiap sampel audio dengan bit pesan rahasia. Pada jurnal Implementasi Steganografi pada Berkas Audio WAV, dijelaskan bahwa bit yang diganti merupakan bit yang memiliki pengaruh paling kecil terhadap kualitas suara, sehingga penyisipan pesan tidak menurunkan kualitas audio secara signifikan.

Hasil pengujian dalam jurnal tersebut menunjukkan bahwa pesan yang disisipkan dapat diekstraksi kembali dengan baik selama tidak terjadi perubahan pada audio stego. Penelitian ini juga menyimpulkan bahwa ukuran berkas audio sebelum dan sesudah proses steganografi tetap sama, sehingga teknik ini efisien dari sisi penyimpanan data.

Namun demikian, audio stego tidak tahan terhadap kompresi dan manipulasi amplitudo, yang menyebabkan pesan tidak dapat diekstraksi kembali setelah audio mengalami perubahan tersebut.

Kombinasi Steganografi Audio dengan Algoritma AES

Untuk meningkatkan tingkat keamanan pesan, steganografi sering dikombinasikan dengan algoritma kriptografi. Salah satu penelitian yang membahas kombinasi tersebut adalah jurnal Implementasi Steganografi Pesan Teks ke Dalam File Audio (.MP3) dengan Algoritma Advanced Encryption Standard dan Least Significant Bit. Dalam jurnal ini dijelaskan bahwa pesan teks terlebih dahulu dienkripsi menggunakan algoritma AES 128-bit sebelum disisipkan ke dalam media audio menggunakan metode LSB (It 2019).

AES merupakan algoritma kriptografi yang telah distandarisasi oleh NIST dan dikenal memiliki tingkat keamanan tinggi. Proses enkripsi AES melibatkan beberapa tahapan utama seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey yang dilakukan secara berulang hingga sepuluh ronde untuk kunci 128-bit. Dengan mekanisme tersebut, pesan yang telah diekstraksi dari audio stego tetap tidak dapat dibaca tanpa kunci dekripsi yang benar.

Hasil penelitian menunjukkan bahwa kombinasi AES dan LSB mampu meningkatkan keamanan pesan secara signifikan. Walaupun pihak tidak berwenang berhasil mengekstraksi data dari audio stego, isi pesan tetap terlindungi karena masih berada dalam bentuk ciphertext.

Steganografi Gambar dan Audio Menggunakan RC4 dan LSB

Selain AES, algoritma RC4 juga banyak digunakan dalam steganografi karena kecepatan prosesnya yang tinggi. Pada jurnal Jurnal ELTIKOM: Steganography of Image and Audio Using RC4 and LSB, dijelaskan bahwa RC4 memiliki keunggulan dalam hal throughput, waktu enkripsi, dan efisiensi penggunaan memori dibandingkan AES, khususnya untuk data berukuran besar (Elektro 2023).

Dalam penelitian tersebut, pesan rahasia dienkripsi menggunakan RC4 kemudian disisipkan ke dalam media gambar PNG dan audio WAV menggunakan metode LSB. Hasil pengujian menunjukkan bahwa ukuran file sebelum dan sesudah proses steganografi tidak mengalami perubahan yang signifikan, serta pesan dapat diekstraksi kembali dengan tingkat keberhasilan 100%.

Selain itu, kualitas media stego tetap terjaga dengan nilai PSNR rata-rata di atas 30 dB, yang menunjukkan bahwa perbedaan antara media asli dan media stego sulit dideteksi secara visual maupun auditori. Hal ini membuktikan bahwa kombinasi RC4 dan LSB efektif digunakan untuk steganografi pada media gambar dan audio.

Analisis Perubahan Karakteristik Audio Stego

Kajian lain membahas aspek deteksi perubahan karakteristik audio setelah proses steganografi. Pada jurnal yang menganalisis audio stego menggunakan pendekatan spectrogram, MFCC, dan Zero-Crossing Rate (ZCR), dijelaskan bahwa audio stego mengalami peningkatan bitrate akibat perubahan format dari MP3 ke WAV serta adanya penyatuan data pesan dengan audio asli (Elektro 2023).

Meskipun secara teknis terdapat perubahan nilai MFCC dan ZCR, penelitian tersebut menyimpulkan bahwa perubahan tersebut tidak mudah dikenali oleh pendengaran manusia. Teknik masking yang digunakan dalam steganografi memperhatikan bit-depth audio sehingga pesan disisipkan pada frekuensi yang tidak sensitif bagi telinga manusia.

Dengan demikian, steganografi audio tetap efektif dalam menjaga kerahasiaan informasi tanpa menurunkan kualitas audio secara signifikan.

JIKUM
JURNAL ILMU KOMPUTER

E-ISSN: 3090-739X
Volume 2, **Number** 1, Mei 2026

METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen berbasis implementasi dengan pendekatan prototyping, di mana sistem steganografi audio dan gambar dirancang, diimplementasikan, dan diuji untuk mengetahui keberhasilan penyembunyian informasi.

Rancangan Kegiatan Penelitian

Rancangan kegiatan penelitian ini dilakukan dengan beberapa tahapan. Tahapan pertama, mencari studi literatur terkait dengan steganografi audio dan gambar serta metode Least Significant Bit (LSB). Kedua, perancangan sistem steganografi audio dan gambar. Ketiga, mengimplementasikan metode steganografi pada media audio dan gambar. Keempat, melakukan pengujian dan analisis hasil steganografi dan terakhir melakukan penarikan kesimpulan.

Bahan dan Alat Utama

Bahan yang digunakan :

- File audio digital
- File gambar digital
- Pesan teks sebagai informasi rahasia

Alat yang digunakan :

- Laptop
- Sistem operasi Windows
- Bahasa pemrograman python
- Perangkat lunak pendukubg (IDE) atau text editor

Teknik Pengumpulan Data

Data yang dikumpulkan melalui referensi dari jurnal dan artikel ilmiah yang berkaitan dengan steganografi audio dan gambar. Kemudian pengumpulan data juga melalui eksperimen yaitu dengan melakukan penyisipan pesan rahasia pada media audio dan gambar serta mencatat hasil dari pengujian eksperimen.

Definisi Operasional Variabel

- Media Audio : File audio digital yang digunakan sebagai media penyisipan pesan.
- Media Gambar : File citra digital yang digunakan sebagai media penyisipan pesan.
- Pesan Rahasia : Informasi berupa teks yang disisipkan ke dalam media.
- Audio Stego dan Citra Strgo : Media yang telah disisipkan pesan rahasia.
- Keberhasilan Steganografi : Kemampuan sistem dalam menyisipkan dan mengekstraksi pesan dengan baik tanpa merusak kualitas media.

HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil implementasi sistem steganografi audio dan gambar menggunakan metode Least Significant Bit (LSB) serta pembahasan terhadap keberhasilan penyisipan pesan, kualitas media stego, dan keterbatasan sistem yang dikembangkan.

Hasil Implementasi Steganografi Audio

Implementasi steganografi audio dilakukan dengan menyisipkan pesan teks ke dalam file audio digital berformat WAV menggunakan metode Least Significant Bit (LSB). Proses penyisipan dilakukan dengan memodifikasi bit paling rendah pada setiap sampel audio sehingga perubahan yang terjadi tidak berpengaruh signifikan terhadap kualitas suara (Bahuguna and Jain 2021).

Berdasarkan hasil pengujian, pesan teks berhasil disisipkan ke dalam media audio tanpa mengubah ukuran file audio secara signifikan. Audio stego yang dihasilkan memiliki karakteristik suara yang hampir identik dengan audio asli. Secara subjektif, perbedaan antara audio asli dan audio stego tidak dapat dikenali oleh pendengaran manusia.

Selain itu, proses ekstraksi pesan dari audio stego menunjukkan hasil yang optimal. Pesan teks yang disisipkan dapat diekstraksi kembali secara utuh dan sesuai dengan pesan asli selama file audio stego tidak mengalami proses kompresi atau manipulasi lanjutan.

Hasil Implementasi Steganografi Gambar

Pada steganografi gambar, pesan teks disisipkan ke dalam file citra digital menggunakan metode LSB dengan cara mengganti bit paling rendah pada nilai piksel citra. Media gambar yang digunakan mampu menampung pesan

JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, Number 1, Mei 2026

rahasia tanpa menimbulkan perubahan visual yang mencolok.

Hasil pengujian menunjukkan bahwa citra stego yang dihasilkan tetap memiliki kualitas visual yang baik dan sulit dibedakan dari citra asli secara kasat mata. Tidak ditemukan perbedaan warna atau detail gambar yang signifikan setelah proses penyisipan pesan. Proses ekstraksi pesan dari citra stego juga berhasil dilakukan dengan baik, di mana pesan dapat diperoleh kembali secara utuh dan akurat.

Hasil Pengujian Keberhasilan Steganografi

Keberhasilan sistem steganografi dianalisis berdasarkan beberapa parameter, yaitu keberhasilan penyisipan pesan, keberhasilan ekstraksi pesan, perubahan ukuran file, serta kualitas media stego. Ringkasan hasil pengujian ditampilkan pada Tabel 1.

Figure

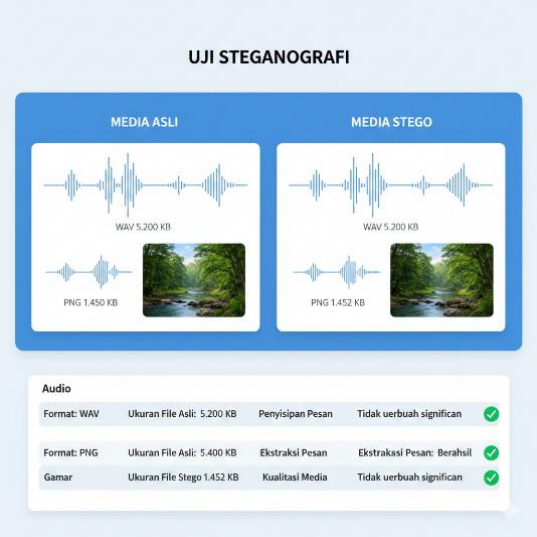

Fig. 1 Hasil Pengujian Steganografi Audio dan Gambar

Table

Table 1. Hasil Pengujian Steganografi Audio dan Gambar

MEDIA UJI	FORMAT FILE	UKURAN FILE ASLI	UKURAN FILE STEGO	PENYISIPAN PESAN	EKSTRAKSI PESAN	KUALITAS MEDIA
Audio	WAV	5.200KB	5.200KB	Berhasil	Berhasil	Tidak Berubah Signifikan
Gambar	PNG	1.450KB	1.452KB	Berhasil	Berhasil	Tidak Berubah Signifikan

KESIMPULAN

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa metode steganografi menggunakan Least Significant Bit (LSB) pada media audio dan gambar mampu menyembunyikan pesan teks dengan baik tanpa menurunkan kualitas media secara signifikan. Pesan rahasia dapat disisipkan dan diekstraksi kembali dengan tingkat keberhasilan yang tinggi selama media stego tidak mengalami kompresi atau manipulasi lanjutan.

Selain itu, ukuran file sebelum dan sesudah proses steganografi tidak mengalami perubahan yang berarti, sehingga metode ini efisien dari sisi penyimpanan data. Dengan demikian, steganografi audio dan gambar dapat digunakan sebagai `metode ini dengan mengombinasikan teknik steganografi dan kriptografi yang lebih kuat serta menguji ketahanan sistem terhadap berbagai jenis serangan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada **Universitas Malikussaleh** atas dukungan dan fasilitas yang diberikan dalam pelaksanaan penelitian ini. Penulis juga menyampaikan apresiasi kepada dosen pengampu mata kuliah yang telah memberikan bimbingan, arahan, serta masukan yang berharga selama proses penyusunan penelitian.

Selain itu, penulis mengucapkan terima kasih kepada seluruh pihak yang telah berkontribusi dalam penyediaan data dan membantu kelancaran penelitian ini,

REFERENSI

Abd, Aliaa Sadoon, Osama Qasim Jumah Al-thahab, and Ahmed A. Hamad. 2025. "New Approach in Steganography Algorithm by Using Audio and Image as Secure Information Based on Chaotic Method." 15(2):349–58. https://iieta.org/journals/ijsse/paper/10.18280/ijsse.150216

Aditya, Yogie, Andhika Pratama, and Alfian Nurlifa. 2010. "Studi Pustaka Untuk Steganografi Dengan Beberapa Metode." 2010(Snati):32–35. https://journal.uii.ac.id/Snati/article/download/1955/1730

Bahuguna, Sushma, and Sandeep Jain. 2021. "A REVIEW OF LSB-BASED AUDIO." 12(3):1–7. https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_12_ISSUE_3/IJCET_12_03_001.pdf

Elektro, Jurnal Teknik. 2023. "STEGANOGRAPHIC ANALYSIS OF AUDIO AND IMAGE." 7(1):67–78. https://share.google/EEezUHXgKEy2k93Wf

It, Jurnal. 2019. "IMPLEMENTASI STEGANOGRAFI PESAN TEKS KE DALAM FILE AUDIO (. MP3) DENGAN ALGORITMA ADVANCED ENCRYPTION STANDARD DAN LEAST." 10(2):122–39. https://share.google/xe5EpwoWBfp7EWkCb

Krishnan, A. Aravind, Yukta Ramesh, and Udbhav Urs. 2025. "Audio-in-Image Steganography Using Analysis and Resynthesis Sound Spectrograph." 13(January). https://share.google/JCZgT9VMQ5gjSWK3A

Kusuma, Permadi, and Yudi Prayudi. 2025. "Implementasi Steganografi Dengan Menggunakan Metode Masking and Filtering Untuk Menyisipkan Pesan Ke Dalam Spectrogram Audio." 9(January):1–15. doi: 10.20885/ajie.vol9.iss1.art1. https://journal.uii.ac.id/ajie/article/view/38039

Learning, Using Deep. 2025. "IS e C Ure." doi: 10.22042/isecure.2025.214367. https://www.isecure-journal.com/article_214367.html

Priyamdeva, A. A. Putu, Arya Maheswara, Gusti Made, Arya Sasmita, and A. A. Ketut Agung. 2024. "Perancangan Integrasi Sistem Enkripsi Dan Steganografi Untuk Pengamanan Data Suara Manusia Berbasis Web." 5(1). https://journal.uii.ac.id/ajie/article/view/38039

Venna, Farah Chikita. 2019. "Implementasi Steganografi Audio Pada File Wav Dengan Metode Redundant Pattern Encoding (Rpe) Berbasis Android." https://repository.uinjkt.ac.id/dspace/bitstream/123456789/47958/1/FARAH%20CHIKITA%20VENNA-FST.pdf