JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Teknik Least Significant Bit (LSB) dan File Injection untuk Pengamanan Data Berbasis Web

Yasir Muammar[1], Najwa Pasya[2], Naufal Syahputra Adha[3*], Mhd Dwi Putra[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]yasir.240170072@mhs.unimal.ac.id, [2]naufal.230170174@mhs.unimal.ac.id

ABSTRAK

Keamanan pertukaran informasi di ruang siber menjadi tantangan besar seiring meningkatnya risiko penyadapan data sensitif oleh pihak yang tidak berwenang. Steganografi muncul sebagai solusi proteksi tingkat lanjut dengan menyembunyikan eksistensi pesan di dalam media digital lain sehingga tidak memicu kecurigaan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan aplikasi "SteganoSafe" berbasis web yang mampu mengamankan data teks dan dokumen di dalam file gambar serta audio. Sistem ini dikembangkan menggunakan bahasa pemrograman Python dengan *framework* Flask, serta mengandalkan dua teknik utama: *Least Significant Bit* (LSB) dan *File Injection*.

Pada metode LSB, pesan teks dikonversi menjadi biner dan disisipkan ke dalam bit paling tidak signifikan pada piksel gambar (format PNG/JPG) atau *frame* audio (format WAV). Proses ini memastikan bahwa perubahan pada media pembawa tidak dapat dideteksi secara visual maupun auditif oleh manusia. Di sisi lain, teknik *File Injection* memungkinkan penyisipan file dokumen seperti PDF atau ZIP dengan cara menggabungkan data biner file rahasia ke akhir file pembawa menggunakan separator unik sebagai penanda biner. Pengujian fungsional menunjukkan bahwa sistem berhasil melakukan enkapsulasi dan ekstraksi data dengan integritas 100% tanpa kerusakan data asli. Penggunaan antarmuka web modern dengan konsep *glassmorphism* memberikan kemudahan aksesibilitas dan pengalaman pengguna yang intuitif. Hasil penelitian menyimpulkan bahwa kombinasi algoritma LSB dan manajemen biner melalui platform web menyediakan mekanisme perlindungan data yang efisien, transparan, dan andal untuk kebutuhan komunikasi rahasia.

Kata Kunci: Steganografi, *Least Significant Bit*, Flask, Keamanan Data, *File Injection*.

PENDAHULUAN

Di era digital saat ini, pertukaran data melalui jaringan publik menghadapi ancaman keamanan yang semakin kompleks, seperti penyadapan dan manipulasi informasi oleh pihak yang tidak berwenang. Untuk menjaga kerahasiaan data, teknik keamanan informasi menjadi sangat krusial. Salah satu metode yang paling efektif selain kriptografi adalah steganografi. Berbeda dengan kriptografi yang mengubah pesan menjadi format yang tidak terbaca, steganografi bertujuan untuk menyembunyikan eksistensi pesan tersebut di dalam media digital lain sehingga tidak menimbulkan kecurigaan.Media digital yang umum digunakan sebagai pembawa (*carrier*) adalah citra dan audio karena memiliki redundansi data yang tinggi. Salah satu teknik steganografi yang populer adalah *Least Significant Bit* (LSB). Teknik ini bekerja dengan mengganti bit paling tidak signifikan pada data piksel gambar atau *frame* audio dengan bit pesan rahasia. Dalam implementasi aplikasi "SteganoSafe", metode LSB diterapkan pada file gambar berformat PNG/JPG dan file audio berformat WAV. Selain LSB, terdapat pula teknik *File Injection* yang menyisipkan dokumen utuh ke dalam file pembawa dengan memanfaatkan penggabungan biner dan separator unik.

TINJAUAN PUSTAKA

Steganografi

Steganografi berasal dari bahasa Yunani steganos (tersembunyi) dan graphein (menulis), yang secara harfiah berarti tulisan tersembunyi. Berbeda dengan kriptografi yang mengamankan pesan dengan mengubahnya menjadi sandi, steganografi berfokus pada penyembunyian eksistensi data rahasia di dalam media lain sehingga pihak ketiga tidak menyadari keberadaan informasi tersebut.

Algoritma Least Significant Bit (LSB)

Algoritma *Least Significant Bit* (LSB) adalah salah satu metode steganografi spasial yang paling populer. Prinsip kerjanya adalah mengganti bit terakhir (bit yang memiliki bobot paling kecil) pada data media pembawa dengan bit pesan rahasia.

- **LSB pada Citra:** Pada gambar digital RGB, setiap piksel terdiri dari tiga komponen warna (Merah, Hijau, Biru) yang masing-masing berukuran 8 bit. Modifikasi bit terakhir pada komponen warna ini hanya akan mengubah nilai intensitas warna sebesar 1 tingkat, sehingga tidak terlihat secara visual oleh mata manusia.

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

- **LSB pada Audio:** Pada file audio berformat WAV, data suara disimpan dalam bentuk biner. Algoritma menyisipkan bit pesan ke dalam *frame bytes* audio secara berurutan.

File Injection dan Delimiter

Teknik *File Injection* bekerja pada level biner dengan cara menyambungkan data file rahasia ke bagian akhir file pembawa tanpa merusak struktur header file asli. Untuk memisahkan antara data asli dan data yang disisipkan, digunakan sebuah *delimiter* atau separator unik. Dalam implementasi sistem ini, digunakan separator biner <<--SEC-->> untuk membedakan isi file pembawa dengan file rahasia saat proses ekstraksi dilakukan.

Flask Framework

Flask adalah *micro-framework* berbasis Python yang digunakan untuk membangun aplikasi web secara cepat dan efisien. Flask menyediakan alat untuk menangani rute HTTP, pemrosesan formulir, dan manajemen file yang diunggah oleh pengguna. Dalam penelitian ini, Flask berperan sebagai jembatan antara logika steganografi di *backend* dengan antarmuka pengguna di *frontend*.

METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini mencakup perancangan arsitektur sistem berbasis web dan implementasi algoritma steganografi pada modul backend.

Alur Kerja Sistem

Sistem berjalan dengan mengikuti alur proses dari input pengguna hingga menghasilkan output berupa file yang telah disisipi pesan (*stego-object*). Proses ini terdiri dari beberapa tahapan utama:

1. **Input:** Pengguna mengunggah file pembawa (*cover file*) dan memasukkan pesan atau file rahasia melalui antarmuka web.
2. **Preprocessing:** Sistem memvalidasi format file dan mengonversi pesan teks menjadi deretan bit biner.
3. **Embedding:** Logika steganografi menyisipkan data rahasia ke dalam media pembawa menggunakan metode LSB atau *File Injection*.
4. **Output:** Sistem menyediakan tautan unduhan untuk file hasil proses atau menampilkan pesan yang berhasil diekstraksi ke layar.

Implementasi Algoritma LSB (Teks)

Algoritma *Least Significant Bit* (LSB) digunakan untuk menyisipkan pesan teks ke dalam media citra dan audio.

- **LSB pada Citra Digital**

  Pada media citra, sistem terlebih dahulu mengubah gambar ke dalam mode RGB. Setiap karakter pesan ditambahkan *delimiter* ##### kemudian dikonversi ke format biner 8-bit. Proses penyisipan dilakukan dengan mengganti bit terakhir dari setiap komponen warna (Red, Green, Blue) pada piksel gambar. Secara matematis, operasi ini dapat dirumuskan sebagai berikut:

  $$P' = (P\ AND\ 254)\ OR\ B$$

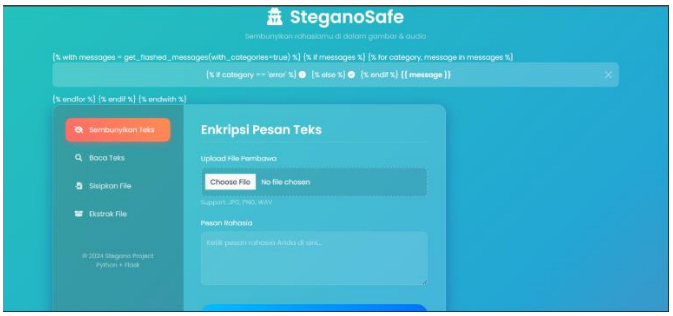
  Di mana P adalah nilai asli piksel, B adalah bit pesan yang akan disisipkan, dan P' adalah nilai piksel baru.
- **Implementasi Teknik File Injection**

  Berbeda dengan LSB, teknik File Injection digunakan untuk menyembunyikan file dokumen (seperti PDF atau ZIP) di dalam media pembawa apa pun tanpa mempedulikan struktur internal bit media tersebut.
  a) **Penyisipan:** Sistem membaca seluruh data biner dari file pembawa dan file rahasia.
  b) **Separator:** Di antara kedua data biner tersebut, disisipkan sebuah konstanta separator <<--SEC-->> sebagai penanda batas akhir file asli.
  c) **Penggabungan:** Hasil akhirnya adalah satu file tunggal yang berisi gabungan biner: [Data_Pembawa] + [Separator] + [Data_Rahasia].

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

PEMBAHASAN

Hasil Implementasi Sistem



Gambar 1. Implementasi sistem

Berdasarkan hasil implementasi, sistem SteganoSafe berhasil dikembangkan sebagai aplikasi steganografi berbasis web yang mampu menyembunyikan dan mengekstraksi data rahasia pada media digital. Gambar di atas menunjukkan tampilan antarmuka utama aplikasi pada menu **Enkripsi Pesan Teks**, di mana pengguna dapat mengunggah file pembawa berupa gambar atau audio serta memasukkan pesan rahasia yang akan disembunyikan.

Fungsi penyembunyian pesan teks pada media gambar (PNG dan JPG) menggunakan metode **Least Significant Bit (LSB)** dengan memodifikasi bit terakhir pada kanal warna RGB. Hasil pengujian menunjukkan bahwa pesan teks berhasil disisipkan dan dapat diekstraksi kembali secara utuh tanpa mengalami perubahan isi. Secara visual, citra hasil steganografi tidak menunjukkan perbedaan yang signifikan dibandingkan citra asli, sehingga keberadaan pesan sulit terdeteksi oleh pengamatan langsung.

Pada media audio berformat WAV, sistem menerapkan metode LSB pada byte audio. Hasil pengujian menunjukkan bahwa kualitas suara tetap terjaga dan tidak mengalami distorsi yang terdengar, sementara pesan teks dapat diekstraksi kembali dengan akurat menggunakan penanda akhir pesan (delimiter). Hal ini menunjukkan bahwa metode yang digunakan cukup efektif dalam menjaga integritas media pembawa. Selain penyembunyian pesan teks, sistem juga menyediakan fitur penyisipan file rahasia dan ekstraksi file. File rahasia berhasil digabungkan dengan file pembawa menggunakan teknik file injection dan dapat diekstraksi kembali sesuai dengan ekstensi yang dipilih oleh pengguna.

Pembahasan

Hasil pengujian menunjukkan bahwa metode LSB yang diterapkan pada sistem SteganoSafe efektif dalam menyembunyikan informasi rahasia tanpa mengubah kualitas media secara signifikan. Penggunaan delimiter khusus memudahkan proses identifikasi akhir pesan saat proses ekstraksi, sehingga tingkat keberhasilan pengambilan data menjadi lebih tinggi.

Namun demikian, sistem ini masih memiliki keterbatasan dari sisi keamanan tingkat lanjut. Pesan yang disisipkan belum melalui proses enkripsi kriptografis, sehingga apabila metode steganografi berhasil diidentifikasi, isi pesan masih dapat dibaca. Oleh karena itu, pengembangan selanjutnya dapat dilakukan dengan mengombinasikan algoritma kriptografi sebelum proses penyisipan data.

Dari sisi antarmuka, desain berbasis web yang sederhana dan interaktif memudahkan pengguna dalam mengoperasikan sistem tanpa memerlukan pemahaman teknis yang mendalam. Dengan demikian, sistem SteganoSafe tidak hanya berfungsi sebagai alat penyembunyian data, tetapi juga sebagai media pembelajaran dalam memahami konsep steganografi berbasis web.

KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan pengujian sistem, dapat disimpulkan bahwa aplikasi SteganoSafe berhasil dikembangkan sebagai sistem steganografi berbasis web yang mampu menyembunyikan dan mengekstraksi data rahasia pada media digital. Sistem ini menerapkan metode Least Significant Bit (LSB) pada media gambar dan audio, serta teknik file injection untuk penyisipan file rahasia, yang terbukti dapat berfungsi dengan baik sesuai dengan tujuan penelitian.

Hasil pengujian menunjukkan bahwa pesan teks yang disisipkan dapat diekstraksi kembali secara utuh tanpa mengalami perubahan isi. Selain itu, kualitas media pembawa, baik gambar maupun audio, tidak mengalami perubahan yang signifikan secara visual maupun auditif, sehingga keberadaan data rahasia sulit terdeteksi melalui pengamatan langsung.

Dari sisi implementasi, penggunaan platform berbasis web memberikan kemudahan akses dan penggunaan bagi pengguna tanpa memerlukan pengetahuan teknis yang mendalam. Antarmuka yang sederhana dan interaktif mendukung

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

proses steganografi secara efektif dan efisien. Meskipun demikian, sistem ini masih memiliki keterbatasan pada aspek keamanan tingkat lanjut karena belum mengintegrasikan algoritma kriptografi untuk mengenkripsi pesan sebelum proses steganografi. Oleh karena itu, pengembangan selanjutnya disarankan untuk mengombinasikan teknik steganografi dengan metode kriptografi guna meningkatkan tingkat keamanan dan kerahasiaan data yang disembunyikan.

REFERENSI

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. *IBM Systems Journal, 35*(3–4), 313–336. https://doi.org/10.1147/sj.353.0313

Behl, A., & Behl, K. (2017). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford, UK: Oxford University Press.

Bishop, M. (2018). *Computer security: Art and science* (2nd ed.). Boston, MA: Addison-Wesley.

Chandramouli, R., Kharrazi, M., & Memon, N. (2004). Image steganography and steganalysis: Concepts and practice. *Lecture Notes in Computer Science, 2939*, 35–49. https://doi.org/10.1007/978-3-540-24676-3_3

Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing, 90*(3), 727–752. https://doi.org/10.1016/j.sigpro.2009.08.010

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). *Digital watermarking and steganography* (2nd ed.). Burlington, MA: Morgan Kaufmann.

Fridrich, J. (2009). *Steganography in digital media: Principles, algorithms, and applications*. Cambridge, UK: Cambridge University Press.

Grinberg, M. (2018). *Flask web development: Developing web applications with Python*. Sebastopol, CA: O'Reilly Media.

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer, 31*(2), 26–34. https://doi.org/10.1109/2.658787

Kaur, R., & Kaur, S. (2014). Image steganography techniques: A review. *International Journal of Advanced Research in Computer Science and Software Engineering, 4*(1), 344–348.

Morkel, T., Eloff, J. H. P., & Olivier, M. S. (2005). An overview of image steganography. *Proceedings of the Fifth Annual Information Security South Africa Conference*, 1–11.

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A survey. *Proceedings of the IEEE, 87*(7), 1062–1078. https://doi.org/10.1109/5.771065

Provos, N., & Honeyman, P. (2003). Hide and seek: An introduction to steganography. *IEEE Security & Privacy, 1*(3), 32–44. https://doi.org/10.1109/MSECP.2003.1203220

Swain, G., & Lenka, S. K. (2014). A novel approach to RGB channel based image steganography technique. *International Arab Journal of e-Technology, 3*(4), 181–186.

Wayner, P. (2009). *Disappearing cryptography: Information hiding: Steganography & watermarking* (3rd ed.). San Francisco, CA: Morgan Kaufmann.