

IMPLEMENTASI STEGANOGRAFI UNTUK KEAMANAN JARINGAN TEKNIK TERSEMBUNYI DALAM KOMUNIKASI DATA

Muh Rizky Anggara Yunan Putra¹, Bintang Putra Aryatama², Nikodemus Christiano David³, Gilang Pamungkas⁴, Indrawan Ady Saputro⁵

Prodi Informatika, STMIK Amikom Surakarta ¹⁻⁵

Email: muh.10372@mhs.amikomsolo.ac.id¹, bintang.10360@mhs.amikomsolo.ac.id²,
nikodemus.10361@mhs.amikomsolo.ac.id³, 4gilang.10367@mhs.amikomsolo.ac.id⁴,
indrawanadysaputro@gmail.com⁵

Informasi	Abstract
Volume : 2 Nomor : 10 Bulan : Oktober Tahun : 2025 E-ISSN : 3062-9624	<i>In the current digital era, where data threats are increasingly sophisticated and varied, network security measures such as steganography are essential. Steganography is a method used to conceal information within other media, such as images, audio, or video, so that the existence of the information is not detected by unauthorized parties. This method aims to maintain the confidentiality of the embedded message, ensuring that only the sender and the recipient are aware of its content. This research employs a literature study involving the collection of data from various sources, reading, noting, and processing the research materials. The results indicate that the implemented steganography method successfully embeds data with a low detection rate by third parties while maintaining good image quality. However, performance varies depending on the format and size of the digital media used. Overall, the implemented steganography method has proven effective in concealing sensitive data within digital media without compromising the quality of the media.</i> Keyword: <i>Steganography, Network Security, Data Communication.</i>

Abstrak

Di era digital saat ini, di mana ancaman terhadap data semakin canggih dan beragam, diperlukan adanya keamanan jaringan seperti steganografi. Steganografi adalah salah satu metode yang digunakan untuk menyembunyikan informasi dalam media lain, seperti gambar, audio, atau video, sehingga keberadaan informasi tersebut tidak terdeteksi oleh pihak yang tidak berwenang. Metode ini bertujuan untuk menjaga kerahasiaan pesan yang disisipkan, sehingga hanya pengirim dan penerima yang mengetahui isi pesan tersebut. Penelitian ini menggunakan studi literatur yang melibatkan pengumpulan data dari sumber pustaka, membaca, mencatat, dan pengolahan bahan penelitian. Hasil penelitian menunjukkan bahwa metode steganografi yang diimplementasikan berhasil menyisipkan data dengan tingkat deteksi yang rendah oleh pihak ketiga, serta mempertahankan kualitas citra yang baik. Namun, terdapat perbedaan kinerja pada berbagai format dan ukuran media digital, sesuai dengan bahan dan hasil eksperimen dari penulis. Secara keseluruhan, metode steganografi yang diimplementasikan terbukti efektif dalam menyembunyikan data sensitif dalam media digital tanpa mengorbankan kualitas media tersebut.

Kata Kunci: *Steganografi, Keamanan Jaringan, Komunikasi Data.*

A. PENDAHULUAN

Steganografi adalah salah satu metode yang digunakan untuk menyembunyikan informasi dalam media lain, seperti gambar, audio, atau video, sehingga keberadaan informasi tersebut tidak terdeteksi oleh pihak yang tidak berwenang. Berbeda dengan kriptografi yang menyamarkan isi pesan, steganografi bertujuan agar keberadaan pesan itu sendiri tidak terlihat. Dalam konteks digital, steganografi memanfaatkan bit-bit dalam file media untuk menyisipkan informasi tambahan tanpa mengubah tampilan atau kualitas file secara signifikan[1]. Teknik ini telah menjadi semakin relevan seiring dengan meningkatnya kebutuhan untuk melindungi data dari akses yang tidak sah, terutama dalam jaringan yang rentan terhadap penyadapan dan serangan[2].

Peran steganografi dalam keamanan jaringan sangat penting, terutama di era digital saat ini di mana ancaman terhadap data semakin canggih dan beragam. Dengan menyembunyikan informasi sensitif dalam media yang tampaknya tidak mencurigakan, steganografi dapat memberikan lapisan perlindungan tambahan terhadap data yang dikirimkan melalui jaringan publik[3]. Misalnya, gambar digital dapat digunakan untuk menyimpan file atau pesan rahasia dengan cara yang tidak terlihat oleh mata manusia. Teknik ini memungkinkan informasi sensitif untuk tetap tersembunyi, bahkan ketika file tersebut diakses oleh pihak yang tidak berwenang[4].

Namun, steganografi bukan tanpa tantangan. Salah satu kesulitan utama adalah memastikan bahwa informasi yang disembunyikan tidak terdeteksi oleh teknik steganalysis, yang bertujuan untuk menemukan data tersembunyi. Seiring dengan perkembangan teknologi, metode steganalysis terus berkembang, membuat kebutuhan akan inovasi dalam teknik steganografi semakin mendesak. Penelitian di bidang ini terus berlanjut untuk mengembangkan metode yang lebih aman dan lebih sulit untuk dideteksi, sehingga informasi dapat disembunyikan dengan tingkat keamanan yang lebih tinggi[5].

Selain itu, kombinasi antara steganografi dan teknik keamanan lainnya, seperti enkripsi, juga menjadi pendekatan yang menarik dalam menjaga kerahasiaan informasi[6]. Dengan menggabungkan steganografi untuk menyembunyikan keberadaan data dan enkripsi untuk melindungi isi data, tingkat keamanan yang dihasilkan dapat lebih tinggi dan lebih efektif. Dalam dunia yang semakin terhubung secara digital, steganografi menawarkan solusi inovatif untuk tantangan keamanan informasi, menjadikannya alat yang berharga dalam melindungi data sensitif dari ancaman yang terus berkembang[7].

B. METODE PENELITIAN

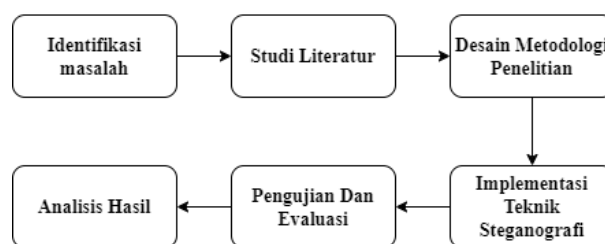
Jenis penelitian

Pada penelitian ini jenis penelitian yang akan digunakan yakni jenis penelitian studi literatur. Studi literatur yakni kumpulan tindakan yang meliputi kegiatan mengumpulkan data data dari sumber pustaka, membaca, mencatat dan pengolahan bahan penelitian. Dan studi literatur ini juga sering disebut dengan studi pustaka[8].

2.2 Steganografi

Steganografi adalah sebuah teknik menyisipkan pesan yang biasanya bersifat rahasia pada sebuah pesan yang lebih besar sehingga orang lain tidak dapat mengetahui keberadaan atau isi pesan yang disisipkan tersebut[9]. Media yang biasanya digunakan untuk melakukan steganografi atau untuk melakukan penyisipkan pesan ini dapat menggunakan berbagai jenis media yakni pesan teks, gambar atau foto, rekaman audio, dan video[10]. Dan tujuan dari steganografi ini yakni agar pesan yang di sisipkan atau disembunyikan tetap terjaga kerahasiannya dan hanya si pengirim dan si penerima lah yang mengetahui isi pesan yang di sisipkan atau disembunyikan tersebut[11].

2.3 Flowchart Alur Penelitian



Gambar 1. Alur Penelitian

2.3.1 Identifikasi masalah

Pada tahap pertama peneliti akan melakukan identifikasi masalah. Yang dimana pada penelitian ini berfokus pada menemukan masalah atau kelemahan keamanan jaringan yang dapat diatasi dengan teknik steganografi. Seperti risiko kebocoran data sensitif selama transmisi atau kebutuhan untuk melindungi komunikasi rahasia dari penyadapan adalah dua contohnya.

2.3.2 Studi literatur

Pada tahap ini peneliti akan mengumpulkan dan mengkaji literatur yang relevan untuk mendapatkan pemahaman yang lebih baik mengenai konteks, ide, dan metode yang terkait steganografi dan keamanan jaringan. Ini termasuk mempelajari secara menyeluruh berbagai metode steganografi, seperti aplikasi mereka saat ini, dan bagaimana metode ini dapat

digunakan untuk meningkatkan keamanan jaringan.

2.3.3 Desain Metodologi Penelitian

Pada tahap ini peneliti akan membuat metodologi penelitian setelah sebelumnya memahami konteks melalui tinjauan literatur. Ini meliputi keputusan mengenai metode steganografi yang akan digunakan, desain eksperimental atau sistem yang akan dibuat, dan rencana untuk mengkaji dan mengevaluasi metode tersebut dalam lingkungan jaringan yang dituju.

2.3.4 Implementasi teknik steganografi

Pada tahap ini, metode steganografi yang telah dipilih dan direncanakan dimasukkan ke dalam sistem jaringan. Implementasi ini mencakup pengkodean atau penyesuaian metode untuk memenuhi kebutuhan jaringan tertentu, serta memasukkannya ke dalam proses komunikasi data saat ini yang nantinya untuk menyembunyikan data secara aman.

2.3.5 Pengujian dan Evaluasi

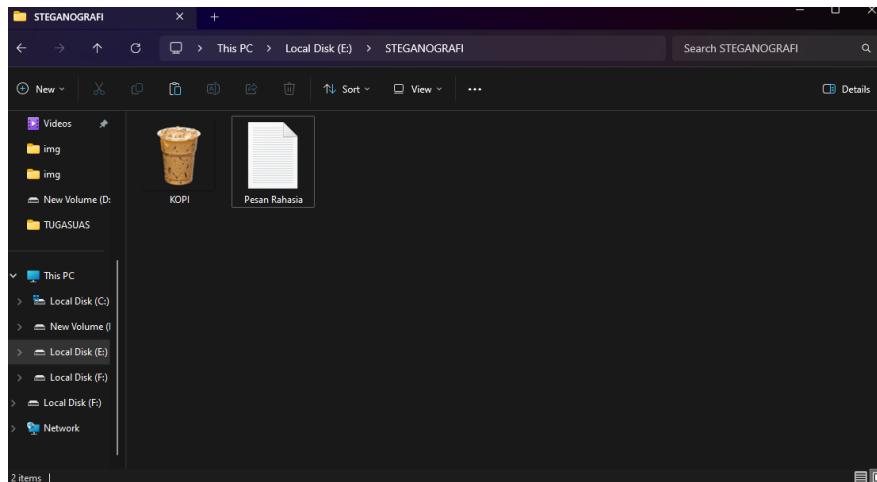
Pada tahap ini setelah melakukan implementasi, metode akan diuji untuk memastikan keberhasilannya dalam melindungi data. Pengujian ini dilakukan untuk mengevaluasi sejauh mana steganografi dapat mencegah akses tidak sah ke data yang telah disembunyikan dan bagaimana metode ini mempengaruhi kinerja jaringan secara keseluruhan[12].

2.3.6 Analisis hasil

Pada tahap ini peneliti akan melakukan analisis hasil yang dimana peneliti akan mengetahui apakah metode steganografi ini berjalan sesuai dengan tujuan atau tidak.

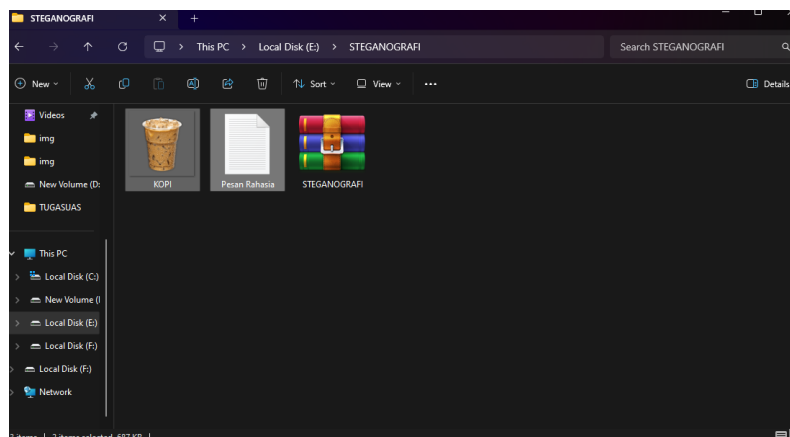
C. HASIL DAN PEMBAHASAN

Pada bagian ini, akan dibahas hasil eksperimen yang telah dilakukan terkait implementasi metode steganografi pada media digital. Analisis dilakukan terhadap beberapa parameter utama, termasuk kapasitas penyembunyian data, kualitas citra yang dihasilkan, dan tingkat keamanan pesan yang disisipkan. Hasil eksperimen menunjukkan bahwa metode steganografi yang diimplementasikan berhasil menyisipkan data dengan tingkat deteksi yang rendah oleh pihak ketiga, serta mempertahankan kualitas citra yang baik. Namun, terdapat perbedaan kinerja pada berbagai format dan ukuran media digital, berikut bahan dan hasil eksperimen dari penulis.



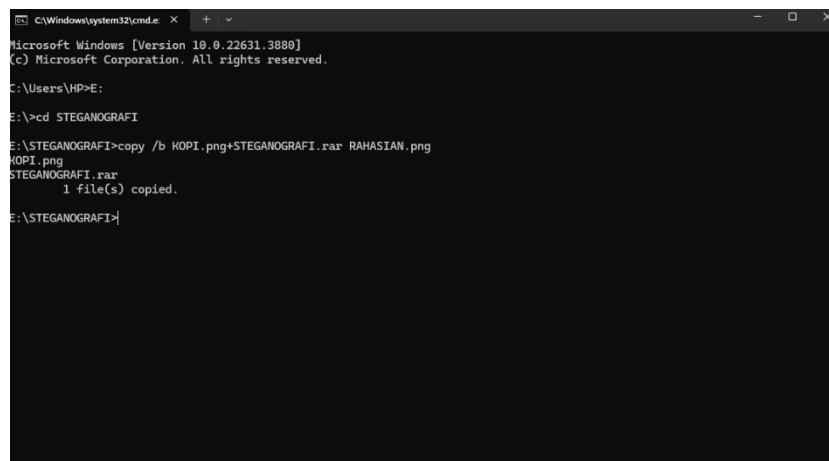
Gambar 2. Bahan untuk Steganografi

Pada gambar diatas merupakan bahan yang akan dipakai oleh penulis untuk melakukan penyisipan file ke dalam gambar atau steganografi. Berikut langkah selanjutnya yang dilakukan oleh penulis.



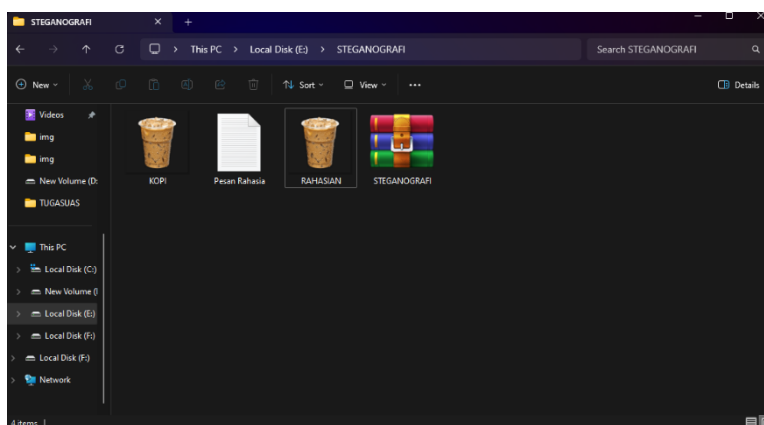
Gambar 3. Bahan di buat File Rar

Pada gambar 3 , select bahan KOPI dan Pesan Rahasia lalu klik kanan , pilih winrar , lalu Add to STEGANOGRAFI, untuk menjadikan file tersebut menjadi satu dalam file rar.



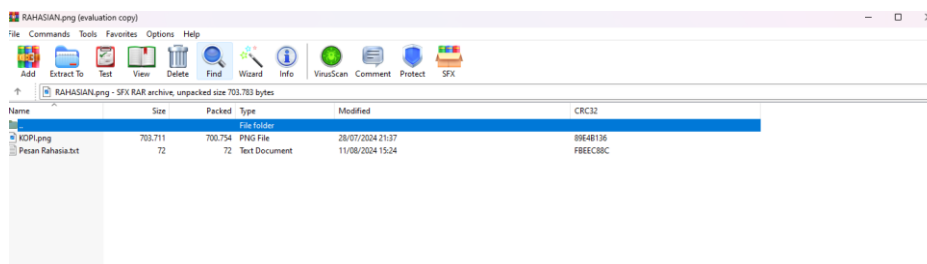
Gambar 4. Eksperimen Steganogafi dengan CMD

Pada gambar diatas penulis melakukan eksperimn steganografi , yang dilakukan secara berurutan , pada awal masukan data drive pada kompute, pada komputer penulis ternamai oleh data drive E: , lalu ketikan cd STEGANOGRAFI yang berfungsi sebagai menavigasi kan atu mengarahkan e folder STEGANOGRAFI. Setelah folder STEGANOGRAFI sudah terbuka, lalu ketikan seperti digambar 4 copy /b KOPI.png+STEGANOGRAFI.rar RAHASIAN.png , penjelesan tersebut mengcopy file kopi png dan file STEGANOGRAFI.rar tersebut , dan RAHASIAN.png merupakan file baru yang dibuat yang berupa duplicat gambar KOPI yang bertujuan untuk menyimpan file rar didalam gambar RAHASIAN.png.



Gambar 5. Hasil Eksperimen dari CMD

Gambar diatas merupakan hasil eksperimen dari CMD yang melakukan steganografi untuk menyisipkan file rar kedalam gambar RAHASIAN.



Gambar 6. Isi file dalam gambar RAHASIAN

Gambar diatas menunjukan isi didalam gambar RAHASIAN.png, untuk mengetahui isi didalam gambar tersebut tidak sembarang membuka seperti biasa. Jika di klik dua kali pada gambar RAHASIAN , maka akan muncul gambar kopi saja . Untuk membuka nya ,memerlukan aplikasi pihak ketika yaitu Winrar, Klik kanan pada file RAHASIAN , lalu pilih open with pilih Winrar, maka akan muncul file Pesan Rahasia dan KOPI yang sudah berhasil disisipkan ke dalam gambar tersebut.

D. KESIMPULAN

Metode steganografi yang telah diimplementasikan menunjukkan efektivitas yang signifikan dalam menyembunyikan data sensitif dalam berbagai media digital, tanpa mengorbankan kualitas asli dari media tersebut. Keunggulan utama dari teknik ini adalah kemampuannya untuk menambah lapisan keamanan ekstra dalam jaringan, terutama dalam melindungi data dari akses tidak sah yang mungkin terjadi. Berdasarkan hasil pengujian, metode ini cenderung memiliki tingkat deteksi yang rendah oleh pihak ketiga, yang menjadi salah satu faktor penting dalam keberhasilannya. Namun, perlu dicatat bahwa performa dari teknik ini dapat bervariasi tergantung pada format dan ukuran media yang digunakan, yang menjadi pertimbangan penting dalam penerapannya. Meskipun demikian, meski steganografi terbukti efektif dalam berbagai kasus, tantangan besar masih ada dalam hal mengantisipasi dan mencegah deteksi oleh teknik steganalisis yang semakin maju dan berkembang, yang terus berupaya untuk mengungkap data tersembunyi dengan metode yang lebih canggih..

SARAN

Penelitian lebih lanjut diperlukan untuk mengembangkan teknik steganografi yang lebih canggih dan sulit dideteksi oleh metode steganalisis terbaru. Selain itu, disarankan agar steganografi dikombinasikan dengan teknik keamanan lainnya, seperti enkripsi, guna meningkatkan tingkat perlindungan data secara keseluruhan. Dalam penelitian di masa depan, penting juga untuk mempertimbangkan penggunaan berbagai format media dan kondisi jaringan yang berbeda, sehingga keandalan dan fleksibilitas metode steganografi dapat diuji secara menyeluruh dan mendalam..

E. DAFTAR PUSTAKA

- Mohammad Imron and Aditiya Pratama, "InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan," vol. 6, no. 2, 2022, doi: 10.30743/infotekjar.v6i2.4346.
- A. Giawa, B. Nadeak, and R. K. Hondro, "IMPLEMENTASI STEGANOGRAFI DENGAN METODE LEAST SIGNIFICANT BIT UNTUK KEAMANAN DATA PESAN TEKS MENGGUNAKAN ALGORITMA ONE TIME PAD," Jurnal Pelita Informatika, vol. 6, no. 4, 2018.
- M. Yusron Rafi and P. Rosyani, "KEAMANAN DATA MENGGUNAKAN TEKNIK STEGANOGRAFI DENGAN METODE END OF FILE (EOF)," 2023. [Online]. Available: <http://ojsamik.amikmitragama.ac.id>
- T. Sinta Peringkat et al., "APLIKASI KEAMANAN DOCUMENT DIGITAL MENGGUNAKAN

- ALGORITMA STEGANOGRAFI DISCRETE COSINE TRANSFORM (DCT) PADA PERUSAHAN ALAT BERAT,” vol. 5, no. 2, 2020, [Online]. Available: www.budiluhur.ac.id
- L. Ali Fitriani, “(media cetak) Analisa Keamanan Data Teks Dengan Menerapkan Kriptografi RSA dan Steganografi LSB,” *Journal of Computer System and Informatics (JoSYC)*, vol. 1, no. 2, 2020.
- R. Fanry Siahaan, P. Marpaung, I. Febrian, and W. Putri, “Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer) Analisis Daya Tahan Keamanan Data Pada Steganografi Berbasis Teks Dalam Struktur Kalimat Bahasa Indonesia,” *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, vol. 22, no. 2, 2023, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jis/index>
- B. : Journal, S. Siaulhak, and S. Kasma, “Siaulhak, Safwan Kasma Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory,” 2023.
- Dewi Laksmiati, “IMPLEMENTASI STEGANOGRAFI IMAGE PROCESSING DAN ENKRIPSI AES MENGGUNAKAN OPENSTEGO,” *Jurnal AKRAB JUARA*, vol. 6, no. 1, pp. 30–40, 2021.
- Anggraeni Eka Putri, Aghistina Kartikadewi, and Lina Audina Abdul Rosyid, “Implementasi Kriptografi Dengan Algoritma Advanced Encryption Standard (AES) 128 Bit Dan Steganografi Menggunakan Metode End Of File (EOF) Berbasis Java Desktop Pada Dinas Pendidikan Kabupaten Tangerang,” vol. 3, no. 2, 2020.
- Hermansa, Rusydi Umar, and Anton Yudhana, “Pangamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra,” *Jurnal Sains Komputer & Informatika (J-SAKTI)*, vol. 4, no. 1, 2020.
- B. : Journal, S. Siaulhak, and S. Kasma, “Siaulhak, Safwan Kasma Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory,” 2023.
- D. Anggara and A. S. Sembiring, “PENINGKATAN KEAMANAN DATA TEKS TERENKRIPSI ALGORITMA LUCIFER MENGGUNAKAN STEGANOGRAFI GIFSHUFFLE PADA CITRA,” *KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer)*, vol. 3, no. 1, Nov. 2019, doi: 10.30865/komik.v3i1.1626.