JIKUM
JURNAL ILMU KOMPUTER

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

Implementasi Hill Cipher Dan Steganografi Gambar Berbasis Web

Diva Insyarah Kausar[1], Nazwa Alviona[2], Khairatul Asyura[3], Elisabeth Dhea Chrysty Arnani Jikwa[4]
[1,2,3,4]Universitas Malikussaleh, Indonesia
[1]diva.230170087@mhs.unimal.ac.id, [2]nazwa.230170094@mhs.unimal.ac.id, [3]khairatul.230170182@mhs.unimal.ac.id, [4]elisabeth.230170132@mhs.unimal.ac.id

ABSTRACT

Information security is an important requirement in digital communications, especially in web-based systems that are vulnerable to interception. This study aims to implement the Hill Cipher algorithm and image steganography as met ods of securing web-based messages. The Hill Cipher is used to encrypt text messages, while the Least Significant Bit (LSB) method is applied to insert encrypted messages into digital images. The research methodology includes the stages of encryption, message insertion, extraction, and decryption. The test results show that messages are successfully encrypted and inserted into images without causing significant visual changes. This system enhances message security because messages are not only encrypted but also hidden. Thus, the combination of Hill Cipher and image steganography is effective as a web-based data security solution.

Keywords:
Hill Cipher, Steganography, LSB, Data Security, Web

PENDAHULUAN

Perkembangan teknologi internet dan komunikasi berbasis web telah meningkatkan pertukaran data secara signifikan, namun di sisi lain juga menimbulkan berbagai ancaman terhadap keamanan informasi. Data yang dikirim melalui jaringan publik sangat rentan terhadap penyadapan, manipulasi, dan pencurian oleh pihak yang tidak berwenang, terutama jika data tersebut tidak dilindungi dengan mekanisme keamanan yang memadai. Penyerang dapat memantau lalu lintas jaringan dan menangkap paket data yang dikirimkan dalam bentuk terbuka atau hanya terenkripsi tanpa perlindungan tambahan, sehingga berpotensi mengungkap informasi sensitif. Selain itu, komunikasi web yang hanya mengandalkan kriptografi memiliki kelemahan karena pesan terenkripsi masih dapat dikenali keberadaannya dan menjadi target serangan kriptanalisis. Kondisi ini menunjukkan bahwa sistem komunikasi web memerlukan metode pengamanan yang tidak hanya mampu mengenkripsi isi pesan, tetapi juga menyembunyikan keberadaan pesan itu sendiri agar risiko serangan dapat diminimalkan.

Hill Cipher merupakan salah satu algoritma kriptografi klasik yang menggunakan konsep aljabar linear, khususnya operasi matriks, untuk mengenkripsi pesan dalam bentuk blok sehingga menghasilkan ciphertext yang memiliki kompleksitas tinggi. Proses enkripsi dilakukan dengan mengalikan vektor plaintext dengan matriks kunci dan menerapkannya dalam operasi modulo, sehingga menyulitkan pihak tidak berwenang untuk melakukan analisis pola pesan. Meskipun Hill Cipher mampu meningkatkan keamanan isi pesan, keberadaan ciphertext masih dapat terdeteksi dalam proses komunikasi. Oleh karena itu, steganografi digunakan sebagai lapisan keamanan tambahan dengan cara menyembunyikan pesan terenkripsi ke dalam media digital seperti gambar. Steganografi gambar bekerja dengan memodifikasi bagian tertentu dari citra, seperti bit paling rendah pada nilai piksel, sehingga perubahan yang terjadi tidak terlihat secara visual. Integrasi antara Hill Cipher sebagai metode enkripsi dan steganografi sebagai teknik penyembunyian pesan terbukti dapat meningkatkan keamanan komunikasi karena pesan tidak hanya sulit dibaca, tetapi juga sulit dideteksi keberadaannya oleh pihak ketiga.

Beberapa penelitian terdahulu menunjukkan bahwa integrasi kriptografi dan steganografi mampu meningkatkan tingkat keamanan informasi secara signifikan dibandingkan penggunaan salah satu metode saja. Penelitian yang membahas penggabungan algoritma kriptografi dengan steganografi menyimpulkan bahwa enkripsi berfungsi melindungi isi pesan, sementara steganografi berperan menyamarkan keberadaan pesan sehingga lebih sulit dideteksi oleh pihak tidak berwenang. Pada aspek steganografi gambar, metode Least Significant Bit (LSB) merupakan teknik yang paling banyak digunakan karena implementasinya sederhana dan mampu menyisipkan data tanpa menimbulkan perubahan visual yang mencolok pada citra digital. Selain itu, beberapa penelitian terkait Hill Cipher menunjukkan bahwa algoritma ini efektif dalam mengenkripsi pesan berbasis blok dengan memanfaatkan operasi matriks, sehingga menghasilkan ciphertext yang memiliki tingkat kerumitan tinggi. Namun, penelitian-penelitian tersebut umumnya masih membahas metode secara terpisah atau belum diimplementasikan secara optimal pada sistem berbasis web, sehingga diperlukan penelitian yang mengintegrasikan Hill Cipher dan steganografi LSB dalam satu sistem untuk meningkatkan keamanan komunikasi web

Berdasarkan kajian terhadap penelitian-penelitian sebelumnya, masih terdapat beberapa celah penelitian yang dapat dikembangkan. Sebagian besar penelitian tentang kriptografi dan steganografi hanya membahas salah satu metode secara terpisah atau belum mengintegrasikannya secara optimal dalam satu sistem yang utuh. Penelitian steganografi

JIKUM
JURNAL ILMU KOMPUTER

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

gambar dengan metode Least Significant Bit (LSB) umumnya berfokus pada teknik penyisipan dan kualitas citra, namun belum banyak dikombinasikan dengan algoritma enkripsi berbasis matriks seperti Hill Cipher. Di sisi lain, penelitian mengenai Hill Cipher lebih menekankan pada aspek enkripsi dan dekripsi pesan tanpa mempertimbangkan upaya penyamaran keberadaan pesan saat proses transmisi. Selain itu, implementasi kedua metode tersebut pada sistem berbasis web masih terbatas, padahal komunikasi web memiliki tingkat kerentanan yang tinggi terhadap penyadapan. Oleh karena itu, diperlukan penelitian yang mengintegrasikan Hill Cipher dan steganografi gambar berbasis LSB dalam sebuah sistem web untuk meningkatkan keamanan komunikasi secara menyeluruh.

Penelitian ini bertujuan untuk mengimplementasikan dan mengintegrasikan algoritma Hill Cipher sebagai metode enkripsi dengan steganografi gambar menggunakan teknik Least Significant Bit (LSB) dalam sebuah sistem berbasis web guna meningkatkan keamanan komunikasi data. Hill Cipher digunakan untuk mengamankan isi pesan melalui proses enkripsi, sedangkan steganografi gambar berfungsi untuk menyembunyikan pesan terenkripsi ke dalam citra digital sehingga keberadaan pesan tidak mudah terdeteksi. Melalui implementasi berbasis web, penelitian ini juga bertujuan untuk menunjukkan bahwa kombinasi kedua metode tersebut dapat diterapkan secara praktis pada lingkungan komunikasi modern yang rentan terhadap penyadapan. Selain itu, penelitian ini diharapkan dapat memberikan gambaran mengenai efektivitas penggabungan kriptografi dan steganografi dalam menjaga kerahasiaan data tanpa menurunkan kualitas visual gambar secara signifikan.

METODE PENELITIAN

Penelitian ini mengimplementasikan enkripsi dan dekripsi berbasis web menggunakan HTML, CSS, dan JavaScript. Sehingga bisa langsung dijalankan lewat browser tanpa perlu instalasi tambahan. Sistem yang dikembangkan dalam penelitian ini merupakan sistem pengamanan data berbasis web yang dirancang untuk mengintegrasikan proses enkripsi dan steganografi gambar. Sistem ini menerima dua jenis input utama, yaitu pesan teks dan gambar digital yang berfungsi sebagai media penampung. Pesan teks terlebih dahulu dienkripsi menggunakan algoritma Hill Cipher untuk mengamankan isi pesan, kemudian hasil enkripsi tersebut disisipkan ke dalam gambar menggunakan metode steganografi. Proses penyisipan dilakukan sedemikian rupa sehingga tidak menimbulkan perubahan visual yang signifikan pada gambar. Output yang dihasilkan oleh sistem ini berupa stego-image, yaitu gambar yang telah mengandung pesan terenkripsi dan siap untuk dikirimkan melalui media komunikasi berbasis web.

Algoritma Hill Cipher merupakan metode kriptografi klasik berbasis aljabar linear yang bekerja dengan memanfaatkan operasi matriks untuk melakukan proses enkripsi dan dekripsi pesan.

Konversi Huruf ke Angka

Plaintext yang berupa teks terlebih dahulu dikonversi ke dalam bentuk numerik dengan menggunakan aturan alfabet, yaitu A = 0, B = 1, C = 2, hingga Z = 25. Karakter selain huruf diabaikan atau disesuaikan agar panjang plaintext dapat dibagi sesuai ukuran matriks kunci. Hasil konversi ini kemudian dikelompokkan ke dalam blok-blok vektor sesuai dengan ordo matriks kunci yang digunakan.

Penentuan Matriks Kunci

Matriks kunci merupakan matriks persegi berordo $n \times n$yang digunakan sebagai kunci enkripsi dan dekripsi. Matriks kunci harus memiliki determinan yang relatif prima terhadap modulo 26 agar memiliki invers matriks. Keberadaan invers matriks kunci sangat penting karena digunakan pada proses dekripsi untuk mengembalikan ciphertext menjadi plaintext.

Proses Enkripsi

Proses enkripsi dilakukan dengan mengalikan vektor plaintext dengan matriks kunci menggunakan operasi matriks. Hasil perkalian tersebut kemudian dimodulo 26 untuk menghasilkan vektor ciphertext. Secara matematis, proses enkripsi dinyatakan dengan persamaan $C = K \times P \bmod 26$, di mana Padalah vektor plaintext, K adalah matriks kunci, dan C adalah vektor ciphertext. Hasil ciphertext selanjutnya dikonversi kembali ke dalam bentuk huruf.

Proses Dekripsi

Proses dekripsi bertujuan untuk mengembalikan ciphertext ke bentuk plaintext semula. Dekripsi dilakukan dengan mengalikan vektor ciphertext dengan invers dari matriks kunci, kemudian hasilnya dimodulo 26. Persamaan dekripsi dinyatakan sebagai $P = K^{-1} \times C \bmod 26$. Hasil perhitungan ini kemudian dikonversi kembali dari bentuk numerik ke bentuk huruf sehingga diperoleh plaintext asli.

Steganografi Least Significant Bit (LSB) merupakan teknik penyembunyian pesan dengan memanfaatkan bit paling rendah pada nilai piksel citra digital. Pada citra berformat RGB, setiap piksel terdiri dari tiga komponen warna, yaitu merah (Red), hijau (Green), dan biru (Blue), yang masing-masing direpresentasikan dalam bentuk biner.

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

Bit paling rendah dari setiap komponen warna tersebut digunakan sebagai media penyisipan data karena perubahan pada bit ini tidak menimbulkan perbedaan visual yang signifikan pada gambar.

Penyisipan Bit pada Piksel

Proses penyisipan dimulai dengan mengonversi ciphertext hasil enkripsi Hill Cipher ke dalam bentuk biner. Selanjutnya, bit-bit pesan biner tersebut disisipkan ke dalam bit LSB dari nilai piksel gambar secara berurutan. Setiap bit pesan menggantikan satu bit LSB pada komponen warna piksel, sehingga perubahan nilai piksel sangat kecil dan sulit dideteksi oleh penglihatan manusia. Proses ini dilakukan hingga seluruh bit pesan berhasil disisipkan ke dalam gambar.

Proses Embedding

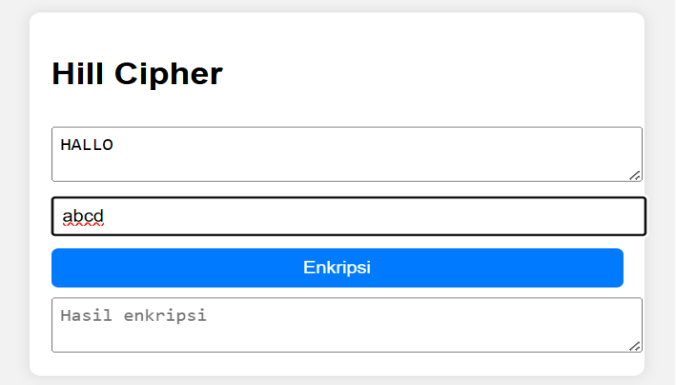
Embedding merupakan tahap utama dalam steganografi, yaitu proses penyatuan pesan rahasia ke dalam citra penampung. Pada tahap ini, sistem membaca gambar input, mengganti bit LSB pada piksel dengan bit pesan terenkripsi, kemudian menyimpan hasilnya sebagai stego-image. Stego-image yang dihasilkan secara visual tampak sama dengan gambar asli, namun telah mengandung pesan rahasia di dalamnya.

Proses Ekstraksi

Proses ekstraksi dilakukan untuk mengambil kembali pesan yang tersembunyi di dalam stego- image. Sistem membaca kembali bit LSB dari setiap piksel sesuai urutan penyisipan, kemudian menyusun bit-bit tersebut menjadi data biner. Data biner hasil ekstraksi selanjutnya dikonversi kembali ke bentuk ciphertext, yang kemudian didekripsi menggunakan algoritma Hill Cipher untuk memperoleh plaintext asli.

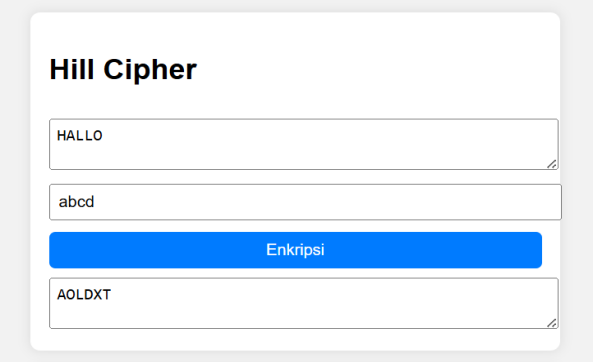
HASIL DAN PEMBAHASAN

Proses Enkripsi Hill Cipher



Gambar 1. Proses Input Plaintext

Pada halaman ini, pengguna diarahkan memasukkan plaintext yang ingin dienkripsi dan key. Yang dimana “HALLO” sebagai plaintext dan “abcd” sebagai key.



Gambar 2. Hasil Output Enkripsi

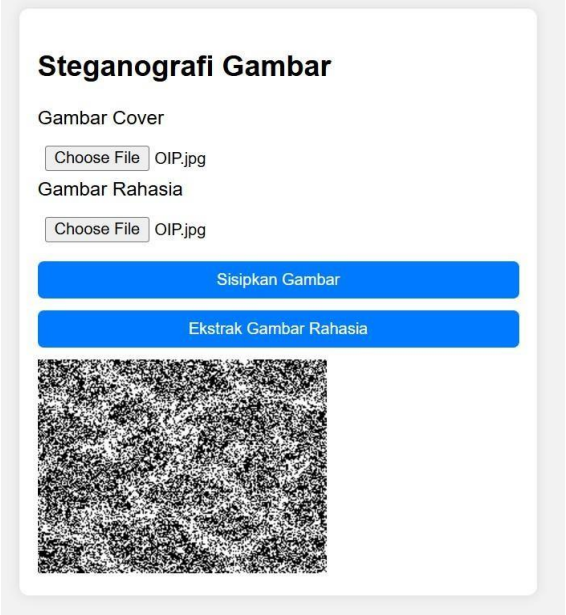
JIKUM
JURNAL ILMU KOMPUTER
E-ISSN: 3090-739X
Volume 2, **Number** 2, November 2026

Pada halaman ini, “AOLDXT” adalah hasil output enkripsi.

Tampilan Stego-Image

Gambar 3. Input Gambar Yang Akan Diekstrak

Pada tampilan ini, pengguna diarahkan untuk menginput dan menyisipkan gambar yang nantinya akan diekstrak dan direpresentasikan dalam bentuk biner.



Gambar 4. Hasil Ekstrak Gambar

Analisis Keamanan

Pada sistem ini menunjukkan bahwa penggabungan algoritma Hill Cipher dan steganografi gambar menggunakan metode Least Significant Bit (LSB) mampu memberikan perlindungan data berlapis. Hill Cipher berperan dalam mengamankan isi pesan dengan mengubah plaintext menjadi ciphertext yang sulit dipahami tanpa mengetahui matriks kunci yang digunakan. Dengan mekanisme enkripsi berbasis matriks, pola asli pesan menjadi tidak mudah dianalisis oleh pihak tidak berwenang. Selain itu, penerapan steganografi LSB menambah tingkat keamanan dengan menyembunyikan keberadaan pesan terenkripsi ke dalam citra digital, sehingga pesan tidak tampak secara eksplisit dalam proses komunikasi. Pihak ketiga yang melakukan penyadapan hanya akan melihat file gambar biasa tanpa menyadari adanya informasi rahasia di dalamnya. Meskipun metode LSB memiliki keterbatasan terhadap manipulasi atau kompresi gambar, kombinasi dengan enkripsi Hill Cipher tetap mampu meminimalkan risiko kebocoran informasi karena pesan yang berhasil diekstraksi tanpa kunci tetap tidak dapat dibaca. Dengan demikian, sistem ini efektif dalam meningkatkan keamanan komunikasi berbasis web dengan memadukan teknik enkripsi dan penyembunyian pesan.

JIKUM
JURNAL ILMU KOMPUTER

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

KESIMPULAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa tujuan penelitian ini telah tercapai. Sistem berbasis web yang mengintegrasikan algoritma Hill Cipher dan steganografi gambar menggunakan metode Least Significant Bit (LSB) berhasil dikembangkan dan diuji sesuai dengan perancangan. Sistem mampu mengenkripsi pesan teks dan menyisipkannya ke dalam citra digital, serta melakukan proses ekstraksi dan dekripsi untuk mengembalikan pesan ke bentuk semula dengan baik.

Hasil pengujian menunjukkan bahwa metode yang digunakan dalam penelitian ini berjalan dengan baik dan efektif. Algoritma Hill Cipher berhasil mengamankan isi pesan melalui proses enkripsi berbasis matriks, sedangkan metode steganografi LSB mampu menyembunyikan pesan terenkripsi ke dalam gambar tanpa menimbulkan perubahan visual yang signifikan. Kombinasi kedua metode tersebut memberikan lapisan keamanan tambahan, sehingga pesan tidak hanya sulit dibaca tetapi juga sulit dideteksi keberadaannya dalam komunikasi berbasis web.

Meskipun sistem yang dikembangkan telah berfungsi dengan baik, masih terdapat beberapa hal yang dapat dikembangkan pada penelitian selanjutnya. Metode steganografi dapat ditingkatkan dengan menggunakan teknik berbasis domain frekuensi, seperti Discrete Cosine Transform (DCT) atau Discrete Wavelet Transform (DWT), agar lebih tahan terhadap manipulasi dan kompresi gambar. Selain itu, algoritma kriptografi yang digunakan dapat diganti atau dikombinasikan dengan algoritma modern untuk meningkatkan tingkat keamanan sistem secara keseluruhan.

REFERENSI

A. K. Mandal and S. Banerjee, “A Review on the Integration of Cryptography and Steganography for Enhanced Information Security,” *International Journal of Scientific Research in Mathematical and Statistical Sciences (IJSRMS)*, vol. 12, no. 1, pp. 1–7, 2025.

M. K. Jha, R. Kumar, and P. Singh, “A Comprehensive Overview of Digital Image Steganography for Secure Communication,” *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 2, pp. 45–55, 2025.

R. K. Sharma and A. Verma, “Implementation of Image Steganography Using Least Significant Bit (LSB) Method,” *International Journal of Computer Applications*, vol. 179, no. 25, pp. 6–10, 2024.

S. N. Huda, A. Fauzan, and R. Pratama, “Analysis of Hill Cipher Algorithm for Text Encryption,” *Jurnal Informatika dan Sistem Informasi*, vol. 10, no. 2, pp. 112–119, 2024.

D. P. Sari and M. A. Nugroho, “Web-Based Secure Communication Using Cryptography and Image Steganography,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 1, pp. 33–41, 2025.

A. Rahman, I. Maulana, and F. Hidayat, “Evaluation of Steganography Image Quality Using LSB Method,” *Jurnal RESTI*, vol. 9, no. 3, pp. 487–494, 2025.

P. K. Das and S. Mukherjee, “Performance Analysis of Classical Cryptographic Algorithms for Data Security,” *International Journal of Computer Science and Network Security*, vol. 24, no. 4, pp. 98–104, 2024.