Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 3, Maret 2025, Hal. 869-880
DOI: https://doi.org/10.52436/1.jpti.786
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Analisis Keamanan Steganografi Multi-Layer dengan Enkripsi Vigenère dan Caesar Cipher pada Citra Digital

Sholeh Hidayat[1], Pulung Nurtantio Andono[2]

[1,2]Teknik Informatika, Universitas Dian Nuswantoro, Indonesia
Email: [1]111202113628@mhs.dinus.ac.id, [2]Pulung@dsn.dinus.ac.id

Abstrak

Kemajuan teknologi komunikasi data menghadirkan tantangan baru terkait manipulasi dan kebocoran informasi, sehingga diperlukan metode pengamanan yang lebih efektif dan andal. Kriptografi dapat mengenkripsi pesan agar sulit dipecahkan, tetapi keberadaannya masih dapat dikenali dan berisiko dianalisis lebih lanjut. Untuk mengatasi kelemahan ini, penelitian ini mengombinasikan steganografi Least Significant Bit (LSB) dengan enkripsi multi-layer menggunakan Vigenère Cipher dan Caesar Cipher guna meningkatkan keamanan data digital. Metode ini menerapkan dua lapisan perlindungan : pertama, enkripsi ganda yang mengacak pesan sebelum penyisipan agar lebih sulit direkonstruksi; kedua, teknik steganografi LSB yang menyisipkan pesan terenkripsi ke dalam citra digital tanpa mengubah struktur visual secara mencolok. Eksperimen dilakukan dengan mengukur kualitas citra hasil steganografi menggunakan PSNR dan analisis histogram untuk menilai perubahan visual. Hasil penelitian menunjukkan bahwa metode ini mampu menyisipkan pesan secara optimal tanpa menurunkan kualitas citra secara signifikan, dengan PSNR tetap berada pada tingkat tinggi, yang menunjukkan bahwa perbedaan antara citra stego dan citra asli hampir tidak terlihat. Selain itu, analisis histogram membuktikan bahwa distribusi piksel sebelum dan sesudah penyisipan tetap stabil, sehingga metode ini sulit dideteksi oleh analisis visual. Dengan demikian, pendekatan kombinasi kriptografi dan steganografi ini terbukti efektif dalam meningkatkan keamanan data digital tanpa mengorbankan kualitas visual, sehingga dapat digunakan sebagai solusi andal untuk perlindungan informasi dalam komunikasi modern.

Kata kunci: *caesar cipher, kriptografi, LSB, steganografi, vigenere cipher*

Security Analysis of Multi-Layer Steganography with Vigenère Encryption and Caesar Cipher on Digital Images

Abstract

Advances in data communication technology present new challenges related to information manipulation and leakage, requiring more effective and reliable security methods. Cryptography can encrypt a message to make it difficult to crack, but its existence can still be recognized and risks further analysis. To overcome this weakness, this research combines Least Significant Bit (LSB) steganography with multi-layer encryption using Vigenère Cipher and Caesar Cipher to enhance digital data security. The method applies two layers of protection: first, double encryption that scrambles the message before insertion to make it more difficult to reconstruct; second, LSB steganography technique that inserts the encrypted message into the digital image without noticeably changing the visual structure. Experiments were conducted by measuring the quality of the steganographed image using PSNR and histogram analysis to assess visual changes. The results show that the method is able to optimally insert the message without significantly degrading the image quality, with the PSNR remaining at a high level, indicating that the difference between the stego-image and the original image is almost invisible. Moreover, histogram analysis proves that the distribution of pixels before and after insertion remains stable, making the method difficult to detect by visual analysis. Thus, this combined approach of cryptography and steganography proves to be effective in enhancing the stego.

Keywords: *caesar cipher*, cryptography, *LSB, steganography, vigenere cipher*

1. PENDAHULUAN

Keamanan jaringan komputer dan transmisi data menjadi aspek penting dalam pertukaran informasi rahasia sehingga perlu dilakukan secara hati – hati. Seiring berkembangnya teknologi, ancaman keamanan semakin kompleks, termasuk pencurian data dan penyadapan informasi penting, terutama di era digital yang semakin berkembang pesat. Ancaman keamanan terhadap data digital kian kompleks, mencakup berbagai bentuk serangan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

seperti pencurian data, peretasan, dan penyadapan informasi penting. Hal ini semakin diperparah dengan meningkatnya ketergantungan terhadap sistem digital dalam berbagai sektor, termasuk bisnis, pemerintahan, dan komunikasi pribadi. Suatu data yang menyangkut aspek Keputusan bisnis dan keamanan password memiliki nilai yang lebih tinggi, tentunya harus disertai dengan keamanan informasi untuk mencegah potensi kebocoran atau penyalahgunaan. Berbagai metode keamanan informasi telah dikembangkan, salah satunya melalui kombinasi kriptografi dan steganografi. Kriptografi merupakan metode pengubah teks biasa menjadi teks terenkripsi sehingga orang yang tidak terlibat tidak dapat mengetahui maknanya[1]. Dikenal sebagai bidang yang mempelajari perlindungan data, dengan tujuan menjaga keamanan serta keaslian informasi melalui penerapan metode enkripsi dan dekripsi[2]. Dengan menerapkan metode ini, data akan disamarkan sehingga ketika terjadi peretasan informasi didalamnya akan tetap terjaga kerahasiaannya.

Teknik lain yang dapat dikombinasikan untuk data hiding yaitu steganografi. Steganografi merupakan teknik sekaligus ilmu yang digunakan untuk menyembunyikan pesan dengan cara tertentu tanpa terdeteksi oleh pihak lain[3]. Steganografi mengurangi kecurigaan karena pesan yang disamarkan disembunyikan di media lain[4]. teknik ini menyembunyikan pesan kedalam media penampung seperti citra digital sehingga pesan rahasia tidak akan diketahui selain pengirim dan penerima[5]. Proses steganografi yang baik harus memenuhi beberapa kriteria utama, yaitu fidelity, imperceptibility, dan recovery[6]. Fidelity mengacu pada kualitas file host yang tetap terjaga tanpa banyak perubahan signifikan setelah disisipkan pesan. Imperceptibility mencakup file hasil steganografi sulit dibedakan dari file host asli, sehingga keberadaan pesan tersembunyi tidak terdeteksi secara kasat mata. Recovery memastikan bahwa pesan yang telah disisipkan kedalam host dapat di ekstraksi Kembali dengan akurat, menjaga keakuratan dan integritas informasi yang disembunyikan[7].

Penelitian penelitian sebelumnya telah membahas aspek keamanan dalam penyembunyian pesan guna melindungi kerahasiaan informasi. [1] menerapkan algoritma LSB dan transposisi kolom untuk penyembunyian pesan, [8] menggunakan Vigenere Cipher sebagai pengaman pada proses deskripsi Steganografi Least Significant Bit, [9][10] dan [11] menggunakan Metode Least Significant Bit (LSB) untuk menyembunyikan file pesan dalam gambar. Studi terdahulu telah menunjukkan hasil yang baik dalam hal penyembunyian pesan untuk menjaga kerahasiaan informasi. Namun, tingkat keamanannya masih belum optimal karena belum menerapkan pendekatan perlindungan multi-layer. Tanpa adanya enkripsi berlapis sebelum proses steganografi, pesan yang tersembunyi lebih rentan terhadap upaya ekstraksi atau serangan kriptanalisis. Oleh karena itu, diperlukan metode yang lebih aman dengan kombinasi beberapa teknik kriptografi guna meningkatkan ketahanan data terhadap ancaman keamanan.

Pada Penelitian kali ini ditujukan untuk memperkuat keamanan data teks dengan mengkombinasikan metode kriptografi dan steganografi. Metode yang digunakan mencakup Enkripsi multi-layer menggunakan Vigenere Cipher dan Caesar Cipher untuk meningkatkan kompleksitas enkripsi. Metode steganografi LSB untuk menyisipkan pesan terenkripsi ke dalam citra digital tanpa merusak kualitas citra secara signifikan. Kombinasi kedua metode ini diharapkan dapat meningkatkan keamanan data teks berupa pesan atau informasi yang menggunakan media gambar sebagai media penyampaian pesan dan dapat mempersulit pihak-pihak yang tidak bertanggung jawab mencuri data dengan membuka pesan. Secara eksplisit, tujuan dari penelitian ini adalah mengembangkan metode penyembunyian pesan yang lebih aman melalui kombinasi enkripsi berlapis dan steganografi, sehingga memastikan kerahasiaan serta integritas informasi yang disisipkan dalam citra digital.

2. METODE PENELITIAN

Dalam tahapan penelitian pengembangan sistem keamanan menggunakan steganografi LSB yang dikombinasi dengan kriptografi vigenere dan caesar cipher. Pada proses enkripsi pertama akan dieksekusi menggunakan vigenere lalu caesar cipher dengan kata kunci yang dimasukkan. Tahapan penelitian meliputi proses enkripsi, penyisipan pesan ke dalam citra digital, ekstraksi pesan, serta evaluasi efektivitas metode yang diterapkan.

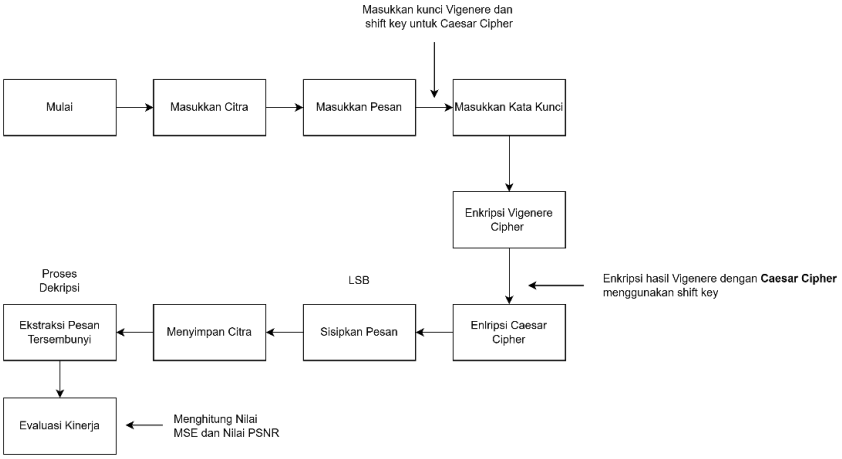
2.1. Tahapan Penelitian

Proses enkripsi pesan dimulai dengan mengenkripsi teks menggunakan algoritma Vigenère Cipher dengan kunci yang dimasukkan oleh pengguna. Hasil enkripsi pertama kemudian diproses lebih lanjut menggunakan Caesar Cipher dengan kunci yang sama atau berbeda, sesuai dengan parameter pengujian. Ciphertext yang dihasilkan dari proses ini akan menjadi pesan rahasia yang disisipkan ke dalam citra digital menggunakan metode Least Significant Bit (LSB). Proses steganografi ini menghasilkan citra stego yang menyimpan pesan rahasia dalam bit-bit terkecil dari piksel gambar.

Pada tahap ekstraksi dan dekripsi, citra stego diekstraksi untuk memperoleh ciphertext tersembunyi, yang kemudian didekripsi secara berurutan, dimulai dengan Vigenère Cipher, diikuti oleh Caesar Cipher, hingga diperoleh kembali pesan asli. Untuk menilai efektivitas metode ini, dilakukan evaluasi menggunakan Mean

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Squared Error (MSE) dan Peak Signal-to-Noise Ratio (PSNR) guna mengukur kualitas citra setelah penyisipan pesan. Selain itu, analisis histogram juga digunakan untuk membandingkan distribusi intensitas piksel antara citra asli dan citra stego, sehingga dapat memberikan gambaran lebih lanjut mengenai perubahan visual akibat proses steganografi. Validasi dilakukan dengan menganalisis hasil perhitungan PSNR, MSE, dan histogram, yang kemudian dibandingkan dengan metode steganografi dan kriptografi lainnya guna menilai efektivitas pendekatan yang digunakan.



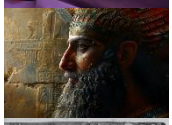
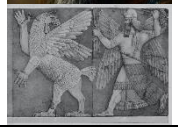
Gambar 1. Tahapan Penelitian

2.2. Karakteristik Dataset

Dataset yang digunakan berupa citra digital dalam format PNG, karena format ini memungkinkan proses steganografi tanpa mengalami kompresi yang dapat mengubah bit-bit pesan. Beberapa citra yang digunakan dalam penelitian ini mencakup berbagai karakteristik untuk mendukung analisis metode yang diterapkan

.

Tabel 1. Citra yang digunakan

Nama Citra	Gambar Citra	Ukuran	Ukuran(KB)
Citra A		512 * 384	280
Citra B		640*427	462
Citra C		512*377	409

2.3. Parameter Pengujian

a. MSE (Mean Squared Error) merupakan metrik yang digunakan untuk menghitung rata-rata perbedaan kuadrat antara citra asli dan citra stego. Semakin kecil nilai MSE, semakin sedikit perubahan yang terjadi pada citra stego, sehingga kualitasnya tetap terjaga dan perbedaan dengan citra asli menjadi lebih sulit dikenali. Nilai MSE yang rendah menunjukkan bahwa metode steganografi yang digunakan mampu menyisipkan pesan dengan distorsi minimal terhadap gambar asli.

b. PSNR (Peak Signal-to-Noise Ratio) adalah ukuran yang digunakan untuk mengevaluasi tingkat perbedaan antara citra asli dan citra stego dalam satuan desibel (dB). Nilai PSNR yang lebih tinggi menunjukkan bahwa kualitas citra stego tetap baik dan hampir menyerupai citra aslinya, sehingga perubahan akibat penyisipan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

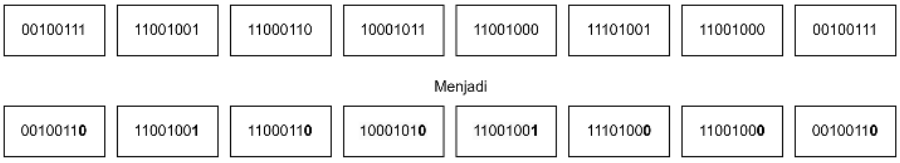
pesan tidak mudah dideteksi oleh pengamat maupun sistem analisis gambar. PSNR menjadi indikator penting dalam menentukan sejauh mana steganografi dapat mempertahankan kualitas visual citra tanpa mengurangi efektivitas penyisipan pesan rahasia.

c. Analisis Histogram digunakan untuk mengamati distribusi intensitas piksel dalam citra sebelum dan sesudah proses steganografi. Dengan membandingkan histogram citra asli dan citra stego, dapat diketahui apakah terjadi perubahan yang signifikan pada distribusi piksel akibat penyisipan pesan. Histogram yang tidak mengalami perubahan mencolok menunjukkan bahwa metode steganografi yang digunakan berhasil menyembunyikan pesan tanpa mengganggu pola distribusi warna dan tingkat kecerahan citra, sehingga lebih sulit untuk dideteksi oleh teknik analisis forensik gambar.

2.4. Steganografi LSB (Least Significant Bit)

Steganografi berasal dari kata yunani "stegos" yang bermakna tersembunyi, "graphein" yang bermakna tulisan. Steganografi telah digunakan selama berabad-abad untuk melindungi data dengan praktik menyembunyikan informasi rahasia dalam pesan non-rahasia[12]. Citra digital bayak digunakan sebagai media penampung untuk menyisipkan pesan pada bit bit pixel di dalam citra tersebut. Karena indra manusia memiliki keterbatasan terhadap warna, penggunaan gambar digital sebagai media penampung memiliki kelebihan. Dengan keterbatasan ini, sulit bagi orang untuk membedakan antara gambar digital asli dan gambar digital yang mengandung pesan rahasia[13].

Least Significant Bit (LSB) adalah teknik mengganti bit yang paling kanan dengan bit yang dimiliki data untuk disembunyikan. Setiap byte (1 byte) terdiri dari 8 bit yang disusun dalam urutan b7b6b5b4b3b2b1b0. Bit b0 memiliki nilai terkecil atau tidak signifikan (Least Significant Bit/LSB), sedangkan bit b7 memiliki nilai tersebar atau paling signifikan (Most Significant Bit/MSB)[14]. Karena pergantian bit hanya dilakukan di paling akhir maka perubahan pada data tidak akan terlihat signifikan sehingga stego yang dihasilkan tetap mirip dengan media asli sebelum disisipkan data tersembunyi dan perbedaannya sulit dikenali. Contoh proses penyisipan pesan yang berbentuk data biner dengan nilai bit 01001000.



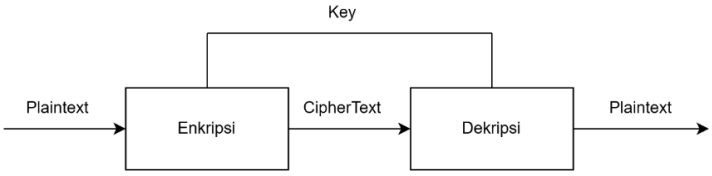
Gambar 2. Alur penyisipan pesan LSB

2.5. Kriptografi Vigenere Cipher

Kriptografi berasal dari kata-kata Yunani "crypto", yang berarti "rahasia" dan "graphia", yang berarti "tulis", adalah disiplin ilmu atau seni yang digunakan untuk menjaga keamanan pesan yang dikirim dari pengirim ke penerima[15]. Kriptografi adalah bidang ilmu yang mempelajari cara menyandikan data atau informasi agar tetap aman dan rahasia[16]. Berfokus pada pengamanan informasi dengan berbagai Teknik seperti enkripsi dan dekripsi. Beberapa aspek penting yang dipelajari dalam kriptografi seperti kerahasiaan data, integritas data, dan autentifikasi data. Kerahasiaan data memastikan bahwa data hanya tersedia untuk pihak berwenang. Integritas data bertujuan menjaga data tidak rusak dan diubah Ketika proses transmisi atau penyimpanan. Autentifikasi data memastikan verifikasi identitas pengirim dan data yang diterima berasal dari sumber yang valid.

Kombinasi dari beberapa aspek tersebut menjadikan kriptografi sebagai pondasi penting untuk menjaga keamanan informasi pada komunikasi digital. Kriptografi terdiri dari 4 komponen utama yaitu : plaintext, ciphertext, key, dan algorithm. Plaintext adalah pesan dalam bentuk yang dapat dibaca dan dipahami, sedangkan ciphertext adalah hasil enkripsi berupa teks yang tampak acak dan tidak dapat dibaca tanpa dekripsi., key berfungsi sebagai parameter penting untuk menjaga kerahasiaan informasi, dan algorithm adalah metode yang digunakan untuk proses enkripsi dan dekripsi.

p-ISSN: 2775-4227
e-ISSN: 2775-4219



Gambar 3. Alur kriptografi

Algoritma vigenere cipher merupakan pengembangan dari metode algoritma kriptografi caesar cipher, yang berfungsi menyandikan teks alfabet berdasarkan huruf-huruf pada kata kunci dengan menggunakan deretan sandi caesar[8]. Kelebihan algoritma ini adalah tidak rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi[17]. Metode vigenere terbagi menjadi dua Teknik substitusi yaitu angka dan huruf[15]. Teknik angka yaitu substitusi yang dilakukan dengan mengganti huruf alphabet dengan angka sedangkan Teknik huruf merupakan pengembangan dari Caesar cipher, namun pergeseran huruf dalam enkripsi berubah setiap periode nya. Tabula recta merupakan Teknik yang digunakan untuk mengenkripsi pesan yang berperan dalam menentukan teks sandi berdasarkan kunci tertentu.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

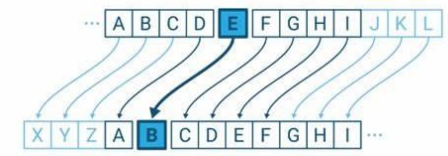
Gambar 5. Teknik angka vigenere cipher

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 5. Teknik huruf vigenere cipher

2.6. Kriptografi Caesar Cipher

Algoritma Caesar Cipher adalah metode dalam kriptografi simetris yang digunakan sebelum perkembangan kriptografi kunci publik[18]. Caesar Cipher merupakan metode sederhana yang banyak digunakan dalam teknik enkripsi[19]. Metode ini diterapkan dengan menetapkan aturan pergeseran kunci ke kanan atau kiri sesuai instruksi.



Gambar 6. Teknik enkripsi caesar cipher

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Contoh :
Plaintext = SATU
Kunci = 3
Hasil = VDWX

2.7. Mean Squared Error (MSE) dan Peak Signal to Noise Ratio (PSNR)

Mean Squared Error (MSE) adalah ukuran kesalahan kuadrat rata-rata yang dihitung dengan membandingkan perbedaan nilai piksel antara citra asli dan citra hasil pada posisi piksel yang identik[11]. Nilai MSE dapat dihitung menggunakan rumus berikut:

$$MSE = \frac{1}{NM}\sum_{x=1}^{N}\sum_{y=1}^{M}\big(p(x,y) - q(x,y)\big)^2 \quad (1)$$

Keterangan:
$p(x, y)$: Nilai piksel citra asli koordinat (x, y)
$q(x, y)$: Nilai piksel stego image pada koordinat (x, y)
M : panjang citra (dalam pixel)
N : Lebar citra (dalam pixel)

Peak Signal to Noise Ratio (PSNR) adalah rasio antara nilai maksimum suatu sinyal dengan tingkat noise yang mempengaruhinya. PSNR biasanya diukur dalam satuan decibel (dB) untuk menilai kualitas rekonstruksi citra atau sinyal[6]. Nilai PSNR dapat dihitung menggunakan rumus berikut:

$$PSNR = 10.log\frac{M^2}{MSE} \quad (2)$$

Keterangan:
M : Nilai piksel tertinggi
MSE : Kesalahan Kuadrat Rata-rata

Analisis kualitas gambar dapat dilihat dari kedua nilai ini. nilai PSNR yang lebih tinggi menunjukkan kualitas gambar yang lebih baik, dan nilai MSE yang lebih rendah menunjukkan kualitas gambar yang lebih baik[20].

3. HASIL

3.1. Hasil Proses Penyembunyian

Beberapa penelitian sebelumnya juga menerapkan metode LSB, tetapi dengan pendekatan enkripsi yang berbeda. Sebagai contoh, penelitian oleh [1] menggunakan kombinasi LSB dan Transposisi Kolom yang menghasilkan nilai PSNR terbaik sebesar 61.9142 dB pada citra dengan panjang teks tersembunyi 500 karakter. Sementara itu, penelitian ini mencapai nilai PSNR tertinggi sebesar 69.95462 dB yang menunjukkan bahwa kualitas gambar hasil steganografi lebih baik dibandingkan metode tersebut. Selain itu, penelitian oleh [10] dan [3] menunjukkan bahwa penggunaan LSB tanpa enkripsi tambahan dapat mencapai akurasi ekstraksi 100%. Namun, keamanan metode tersebut belum sepenuhnya terjamin karena tidak menerapkan perlindungan berlapis. Ketidakhadiran enkripsi sebelum proses steganografi membuat pesan tersembunyi lebih rentan terhadap deteksi oleh algoritma analisis steganografi yang lebih canggih. Oleh karena itu, penelitian ini mengusulkan pendekatan baru dengan menerapkan kombinasi enkripsi Vigenère Cipher dan Caesar Cipher sebelum penyisipan pesan ke dalam citra digital menggunakan metode steganografi Least Significant Bit (LSB).

Pengujian pada penelitian ini dilakukan dengan tiga jenis citra sebagai media penyisipan pesan dengan berbagai panjang karakter. Hasil pengujian, termasuk nilai PSNR, akurasi ekstraksi, dan analisis histogram disajikan untuk membandingkan efektivitas metode yang diusulkan.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Tabel 2. Gambar Hasil Stegano

No	Cover Image	Panjang Karakter	Stego Image
1	 Citra A	500	
2	 Citra A	1000	
3	 Citra A	1500	
4	 Citra B	500	
5	 Citra B	1000	
6	 Citra B	1500	
7	 Citra C	500	
8	 Citra C	1000	
9	 Citra C	1500	

Hasil pengujian menunjukkan bahwa pesan berhasil disisipkan dengan baik dalam citra tanpa menyebabkan perubahan visual yang mencolok pada citra asli. Penyisipan pesan tidak mengubah struktur gambar secara signifikan, yang mengindikasikan bahwa metode ini cukup efisien dan tidak mudah terdeteksi secara visual.

3.2. Hasil Proses Ekstraksi

Proses ekstraksi berhasil mendapatkan kembali pesan yang telah disisipkan dengan tingkat akurasi 100%. Hal ini menunjukkan bahwa metode yang diajukan mampu mempertahankan integritas pesan dengan cara yang optimal. Hasil ekstraksi menunjukkan bahwa pesan yang telah disisipkan dalam citra steganografi dapat diperoleh kembali dengan tingkat akurasi 100%, tanpa adanya perubahan atau kehilangan informasi. Keberhasilan ini

p-ISSN: 2775-4227
e-ISSN: 2775-4219

menegaskan bahwa metode yang digunakan mampu menjaga integritas dan keakuratan pesan secara optimal selama proses penyisipan dan ekstraksi. Hal ini mengindikasikan bahwa kombinasi teknik Least Significant Bit (LSB) steganografi dengan Vigenere Cipher dan Caesar Cipher yang diterapkan dalam penelitian ini tidak merusak atau mengubah pesan asli selama proses encoding dan decoding. Dengan kata lain, setiap karakter yang disisipkan tetap dapat direkonstruksi secara sempurna setelah diekstrak, tanpa adanya kesalahan atau degradasi informasi.

Keberhasilan ini juga menunjukkan bahwa algoritma yang digunakan telah diimplementasikan dengan baik dan tidak mengalami error propagasi yang dapat mengganggu proses dekripsi. Selain itu, ketahanan terhadap perubahan struktur gambar memastikan bahwa metode ini tidak hanya efisien dalam menyisipkan pesan, tetapi juga andal dalam mengembalikan pesan yang telah disisipkan. Secara keseluruhan, hasil ini membuktikan bahwa metode steganografi yang diajukan memiliki kehandalan tinggi dalam menyembunyikan dan mengekstrak informasi, sehingga dapat digunakan dalam aplikasi yang membutuhkan keamanan dan kerahasiaan data tanpa mengorbankan integritas pesan.

4. PEMBAHASAN

4.1. Analisis Keamanan dengan MSE dan PSNR

Tabel 2. Hasil MSE dan PSNR

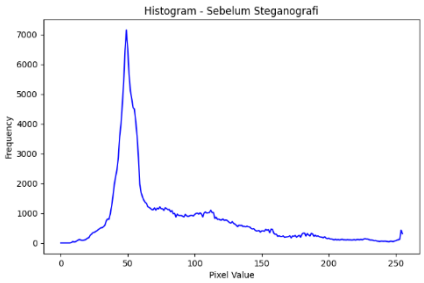
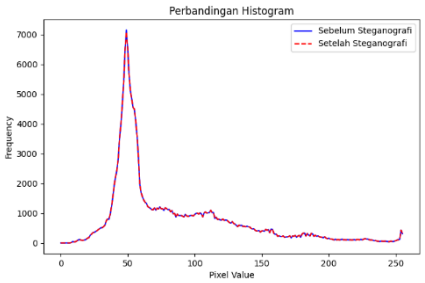
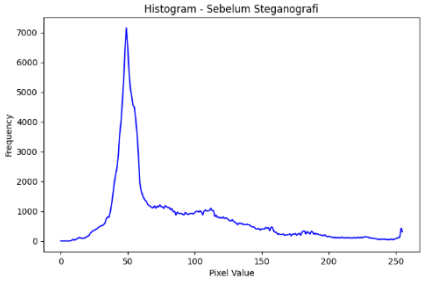
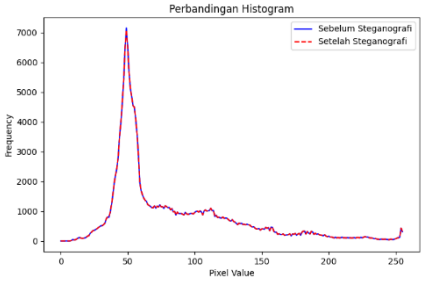
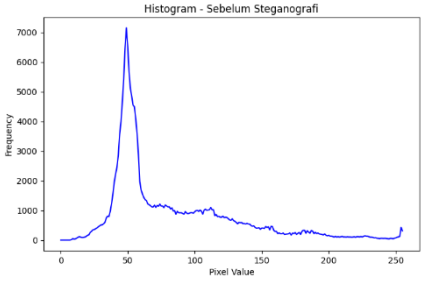
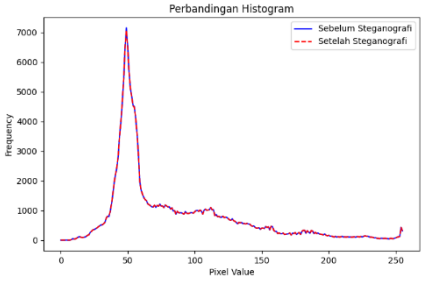
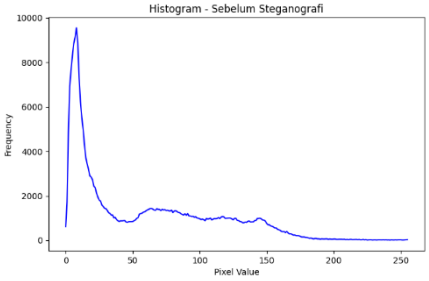
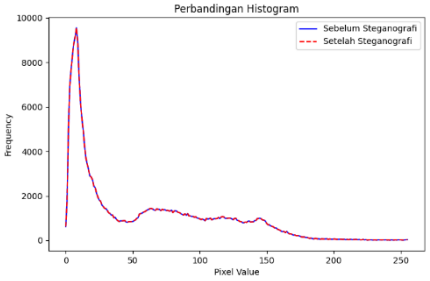
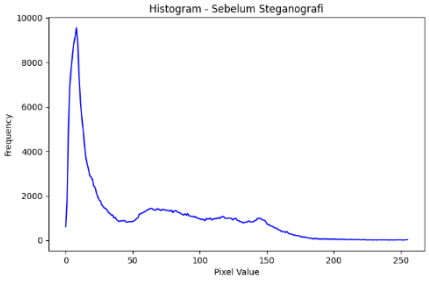
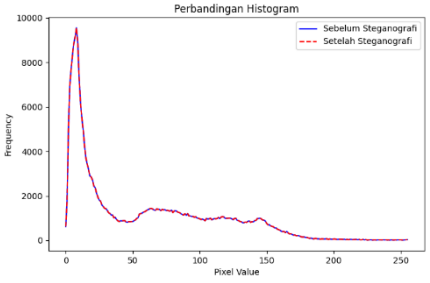
No	Stegano Image	Panjang Pesan	PSNR	MSE
1	Citra A	500 karakter	69.69248 dB	0.00698
2	Citra A	1000 karakter	66.48119 dB	0.01462
3	Citra A	1500 karakter	63.63152 dB	0.02818
4	Citra B	500 karakter	69.95462 dB	0.00657
5	Citra B	1000 karakter	66.68459 dB	0.01395
6	Citra B	1500 karakter	63.84900 dB:	0.02680
7	Citra C	500 karakter	69.70292 dB	0.00696
8	Citra C	1000 karakter	66.45679 dB	0.01470
9	Citra C	1500 karakter	63.61161 dB	0.02831

Hasil pengujian menunjukkan bahwa semakin banyak karakter yang disisipkan, nilai PSNR mengalami sedikit penurunan dan nilai MSE meningkat. Namun, nilai PSNR tetap dalam kategori sangat baik (di atas 60 dB), yang menunjukkan bahwa kualitas citra tidak mengalami penurunan yang signifikan. Contohnya pada Citra A, ketika panjang pesan 500 karakter, PSNR = 69.69248 dB dengan MSE = 0.00698, namun ketika panjang pesan bertambah menjadi 1500 karakter, PSNR turun menjadi 63.63152 dB dan MSE meningkat menjadi 0.02818. Pola yang sama terjadi pada Citra B dan C, di mana semakin banyak informasi yang disisipkan, semakin besar distorsi yang terjadi pada citra hasil steganografi. Perbedaan MSE dan PSNR pada Berbagai Citra mengindikasikan bahwa karakteristik struktur gambar memengaruhi bagaimana data steganografi disisipkan dan berdampak pada kualitas akhir. Nilai PSNR lebih dari 60 dB mengindikasikan bahwa distorsi yang dihasilkan dari proses steganografi sangat kecil dan sulit dikenali oleh mata manusia. Dengan kata lain, meskipun terdapat perubahan dalam citra akibat penyisipan pesan, perubahan tersebut tidak signifikan secara visual. Nilai MSE yang sangat kecil (kurang dari 0.03) menandakan bahwa rata-rata perbedaan antara citra asli dan citra steganografi sangat rendah. Dengan demikian, metode steganografi yang digunakan cukup efisien dalam menjaga kualitas gambar.

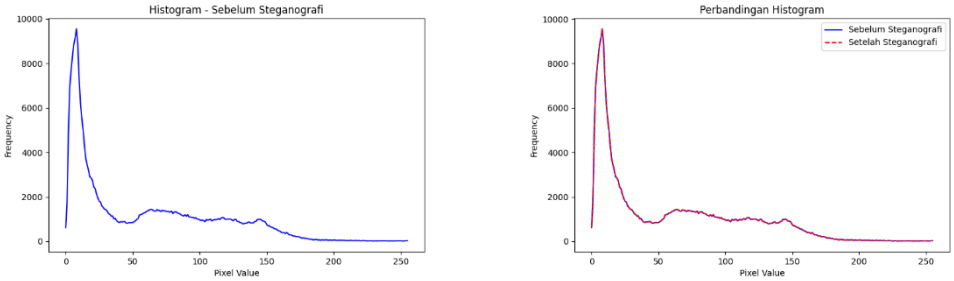
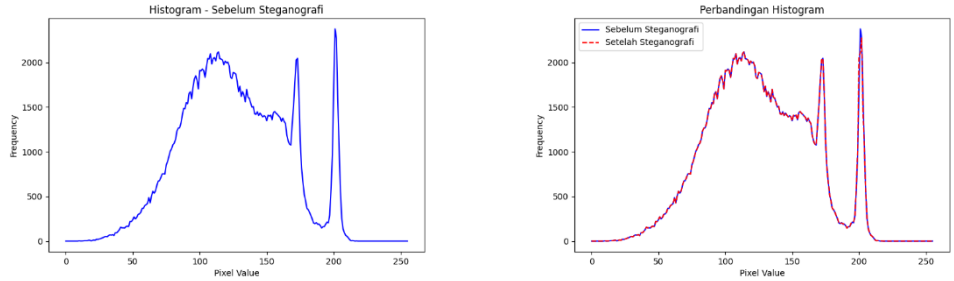
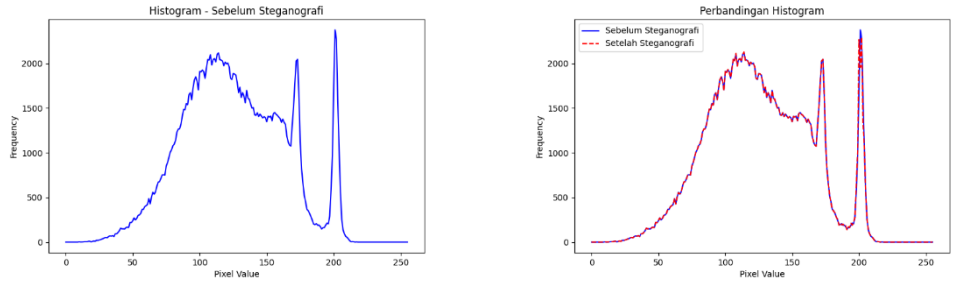
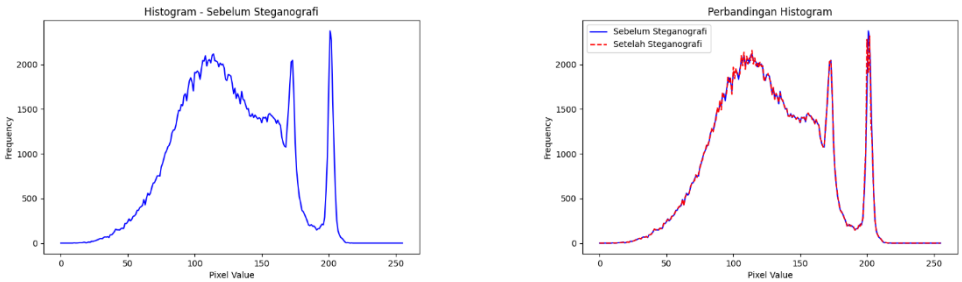
4.2. Analisis Histogram

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Tabel 3. Hasil Analisis Histogram

No	Panjang Karakter	Frequency Cover Image	Frequency (Cover-Stego) Image
1	500		
		Citra A	
2	1000		
		Citra A	
3	1500		
		Citra A	
4	500		
		Citra B	
5	1000		

p-ISSN: 2775-4227
e-ISSN: 2775-4219

6	1500	Citra B	
7	500	Citra B	
8	1000	Citra C	
9	1500	Citra C	

Dari hasil analisis histogram yang ditampilkan dalam Tabel 3, terlihat bahwa frekuensi piksel pada gambar cover (gambar sebelum steganografi) dan gambar cover-stego (gambar perbandingan setelah steganografi) memiliki pola yang serupa, meskipun terdapat sedikit perbedaan pada beberapa panjang karakter. Hasil ini dilihat dari beberapa faktor yaitu :

1. Konsistensi Pola Histogram

Pada setiap kategori panjang karakter (500, 1000, dan 1500), nilai frekuensi menunjukkan bahwa perubahan akibat penyisipan pesan relatif kecil. Hal ini menunjukkan bahwa metode steganografi yang digunakan tidak menyebabkan perubahan signifikan dalam distribusi piksel.

2. Perbedaan pada Beberapa Citra

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Citra A, B, dan C menunjukkan tren yang hampir serupa, dengan sedikit variasi pada perubahan frekuensi. Perubahan ini dapat disebabkan oleh ukuran pesan yang disisipkan atau karakteristik gambar yang berbeda (misalnya, kontras, tekstur, dan kompleksitas warna).

3. Keamanan Metode Steganografi

Jika perbedaan histogram antara cover image dan cover-stego tidak signifikan, maka metode steganografi yang digunakan cukup aman karena sulit dideteksi melalui analisis histogram. Namun, jika ada pola perubahan yang berulang atau cukup besar, hal ini dapat menjadi celah keamanan, di mana pihak ketiga dapat mengenali keberadaan pesan tersembunyi.

4. Implikasi terhadap Keakuratan Penyisipan Pesan

Semakin besar panjang karakter pesan yang disisipkan, kemungkinan perubahan histogram juga meningkat, meskipun dalam tabel ini perubahan tersebut masih dalam batas wajar. Oleh karena itu, penggunaan metode Least Significant Bit (LSB) atau teknik lain yang mempertahankan struktur histogram tetap penting untuk memastikan keamanan informasi tersembunyi.

Secara keseluruhan, hasil ini membuktikan bahwa metode steganografi yang diajukan memiliki kehandalan tinggi dalam menyembunyikan dan mengekstrak informasi, sehingga dapat digunakan dalam aplikasi yang membutuhkan keamanan dan kerahasiaan data tanpa mengorbankan integritas pesan.

5. KESIMPULAN

Metode Steganografi LSB yang dikombinasikan dengan Vigenère Cipher dan Caesar Cipher terbukti efektif dalam meningkatkan keamanan pesan tersembunyi, dengan nilai PSNR di atas 60 dB dan akurasi ekstraksi 100%, memastikan integritas data tetap terjaga. Analisis histogram menunjukkan perubahan piksel minimal, menjadikannya aman dari deteksi steganalisis dasar. Metode ini dapat diterapkan dalam komunikasi rahasia, namun perlu memperhatikan kapasitas penyisipan untuk menjaga keseimbangan antara keamanan dan kualitas citra. Penelitian selanjutnya dapat mengeksplorasi AES, RSA, atau steganografi berbasis transformasi frekuensi (DCT, DWT) guna meningkatkan ketahanan terhadap serangan serta efisiensi penyembunyian pesan.

DAFTAR PUSTAKA

[1] J. Matematika, F. Mipa, and U. Jember, "Penyembunyian Pesan Terenkripsi pada Citra menggunakan Algoritma LSB dan Transposisi Kolom," vol. 6, no. 1, pp. 25–30, 2022.

[2] C. Umam, M. Muslih, and D. Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," *Seminar Nasional Teknologi …*. prosiding.stekom.ac.id, 2022. [Online]. Available: https://prosiding.stekom.ac.id/index.php/SEMNASTEKMU/article/download/160/172

[3] Aqilah Syaima' Fadel, Rianto David Saputra, Y. Fatma, and Risky Nanda Putra, "Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital," *J. CoSciTech (Computer Sci. Inf. Technol.*, vol. 5, no. 1, pp. 36–41, 2024, doi: 10.37859/coscitech.v5i1.6759.

[4] F. Kurniawan, Z. Sitorus, and R. R. Putra, "COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY IN IMPROVING TEXT DATA SECURITY USING DES (DATA ENCRYOTION STANDARD) AND LSB (LEAST SIGNIFICANT BIT) METHODS," pp. 352–362, 2023.

[5] S. Fajriati Romli, A. Id Hadiana, and F. Rakhmat Umbara, "Penerapan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Spread Spectrum Untuk Mengamankan Pesan Dalam Gambar," *DES 2023 J. Informatics Commun. Technol.*, vol. 5, no. 2, pp. 196–209, 2023.

[6] R. Fahmi, N. Imanudin, I. Kustiawan, and S. Elvyanti, "Steganografi Citra Digital Menggunakan Pendekatan Least Significant Bit dan Discrete Cosine Transform," *Semin. Nas. Tek. …*, no. 207, pp. 1–5, 2023, [Online]. Available: https://snte.fortei.org/list/index.php/snte/article/view/48%0Ahttps://snte.fortei.org/list/index.php/snte/article/download/48/50

[7] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher," *J. Masy. Inform.*, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[8] T. Alawiyah, R. Ardianto, and D. S. Purnia, "Implementasi Vigenere Cipher Sebagai Pengaman Pada Proses Deskripsi Steganografi Least Significant Bit," *J. Inform.*, vol. 7, no. 1, pp. 37–45, 2020, doi: 10.31311/ji.v7i1.6431.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[9] M. N. Al Jumah and S. Sarimuddin, "Jurnal Informatika dan Rekayasa Perangkat Lunak Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar," vol. 6, no. 1, pp. 102–108, 2024.

[10] N. F. Hasan, C. N. Dengen, and D. Ariyus, "Analisis Histogram Steganografi Least Significant Bit Pada Citra Grayscale," *Digit. Zo. J. Teknol. Inf. dan Komun.*, vol. 11, no. 1, pp. 20–29, 2020, doi: 10.31849/digitalzone.v11i1.3413.

[11] Veriarinal and R. Wanandi, "Implementasi Sistem Steganografi Citra Dengan Metode Substitusi LSB (Least Significant Bit)," *J. Multidisiplin Saintek*, vol. 2, no. 11, pp. 5–24, 2024.

[12] J. Saputra, U. Faruq, and Y. D. Cahyono, "OPTIMALISASI STEGANOGRAFI DENGAN MENGGUNAKAN," vol. 8, no. 5, pp. 11065–11068, 2024.

[13] I. U. W. Mulyono, A. Susanto, and Y. Kusumawati, "Lsb Stegano Pada Kombinasi Kritpografi Simetris Caesar-Vigenere," *Din. Rekayasa*, vol. 16, no. 2, pp. 139–146, 2020, doi: 10.20884/1.dr.2020.16.2.318.

[14] I. M. Yusup, C. Carudin, and I. Purnamasari, "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen," *J. Tek. Inform. dan Sist. Inf.*, vol. 6, no. 3, pp. 434–441, 2020, doi: 10.28932/jutisi.v6i3.2817.

[15] A. C. Frobenius and E. R. Hidayat S. H. S, "Steganografi LSB Dengan Modifikasi Kriptografi: Caesar, Vigenere, Hill Cipher dan Playfair Pada Image," *Melek IT Inf. Technol. J.*, vol. 6, no. 1, pp. 33–40, 2020, doi: 10.30742/melek-it.v6i1.301.

[16] N. A. Karima, A. N. Aisyah, H. V Silla, and ..., "Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit," *J. Masy. …*, 2024, [Online]. Available: https://ejournal.undip.ac.id/index.php/jmasif/article/view/60836

[17] A. Junikhah, "Implementasi Vigenere Cipher Pada Aplikasi Myprichat End-To-End Encrypted Sms Berbasis Android," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 7, no. 3, pp. 680–691, 2022, doi: 10.29100/jipi.v7i3.3012.

[18] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *J. Educ.*, vol. 5, no. 3, pp. 8563–8573, 2023, doi: 10.31004/joe.v5i3.1647.

[19] A. Hasanah *et al.*, "Implementasi Algoritma Caesar Cipher untuk Pengamanan Pesan Menggunakan Java NetBeans," *Digit. Transform. Technol.*, vol. 3, no. 1, pp. 1–9, 2023, [Online]. Available: https://doi.org/10.47709/digitech.v3i1.2305

[20] T. Pustaka, "OPTIMASI STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB) METODE OPERASI PERGESERAN BIST," vol. 8, no. 5, pp. 11055–11059, 2024.