ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.3 No.1 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

Penerapan Kombinasi Algoritma Kriptografi Vigenere Cipher dan Steganografi LSB pada Keamanan Data Teks dalam Aplikasi Google Drive

Application of the Combination of the Vigenere Cipher Cryptographic Algorithm and LSB Steganography to the Security of Text Data in the Google Drive Application

Muhamad Ariel Saputra[1], Yusuf Putra Bintang Satria[2], Zidan Lutfi Ramadhan[3]
[1 2 3] Teknik Informatika, Teknik, Universitas Pelita Bangsa
[1]muhamadarielsaputra@mhs.pelitabangsa.ac.id, [2]yusuf.pbs@mhs.pelitabangsa.ac.id,
[3]zidanlr@mhs.pelitabangsa.ac.id

Abstract

This research introduces a combination of the Vigenere Cipher cryptography algorithm and LSB steganography to enhance the security of text data in the Google Drive application. The main goal is to strengthen the safeguarding of information stored in the cloud by encrypting text using the Vigenere Cipher and hiding it within the Least Significant Bit (LSB) of an image, which is then uploaded to Google Drive. This integrated approach establishes an extra layer of security, confirming its effectiveness in reinforcing the confidentiality of text data in the cloud setting. The research findings highlight the success of the proposed methodology, emphasizing its efficiency in ensuring the privacy and security of text data stored in Google Drive

Keywords: *Cryptography, Vigenere cipher, Steganography, LSB, Google Drive*

Abstrak

Penelitian ini memperkenalkan kombinasi algoritma kriptografi Vigenere Cipher dan steganografi LSB untuk meningkatkan keamanan data teks pada aplikasi Google Drive. Tujuan utamanya adalah untuk memperkuat pengamanan informasi yang disimpan di cloud dengan mengenkripsi teks menggunakan Vigenere Cipher dan menyembunyikannya dalam Least Significant Bit (LSB) suatu gambar, yang kemudian diunggah ke Google Drive. Pendekatan terpadu ini menciptakan lapisan keamanan ekstra, yang menegaskan efektivitasnya dalam memperkuat kerahasiaan data teks di pengaturan cloud. Temuan penelitian menyoroti keberhasilan metodologi yang diusulkan, menekankan efisiensinya dalam memastikan privasi dan keamanan data teks yang disimpan di Google Drive.

Kata kunci: Kriptografi, vigenere chiper, steganografi, lsb, google drive

Pendahuluan

Di era digital yang sedang berkembang dengan pesat, keamanan data menjadi aspek yang sangat penting untuk diperhatikan, terutama dalam konteks penyimpanan dan pertukaran data melalui platform penyimpanan awan seperti Google Drive.[1]–[3] Dalam upaya menjaga kerahasiaan dan integritas data teks yang disimpan di platform ini, diperlukan pendekatan keamanan yang canggih dan efektif. Salah satu pendekatan yang menarik untuk diselidiki adalah penggabungan antara algoritma kriptografi Vigenere Cipher dan steganografi LSB (Least Significant Bit) pada data teks.[3]–[5]

Google Drive, sebagai salah satu platform unggulan untuk penyimpanan awan, telah menjadi pilihan utama bagi jutaan pengguna dalam menyimpan dan berbagi berbagai jenis data, termasuk data teks.[6]–[8] Meskipun platform ini menyediakan tingkat keamanan yang memadai, dinamika perkembangan tantangan keamanan mendorong kita untuk mempertimbangkan strategi keamanan yang lebih tangguh, terutama menghadapi ancaman *cyber* yang semakin kompleks.[2] Penggabungan algoritma kriptografi Vigenere Cipher

dan steganografi LSB muncul sebagai solusi menarik untuk meningkatkan tingkat keamanan data teks yang disimpan di Google Drive.[1]

Dalam kajian literatur terkait, banyak riset yang telah mengulas aspek keamanan data melalui penerapan algoritma kriptografi dan steganografi. Meskipun demikian, keterbatasan penelitian yang secara spesifik menggali implementasi gabungan algoritma Vigenere Cipher dan steganografi LSB dalam melindungi keamanan data teks di aplikasi Google Drive masih terlihat.[9] Evaluasi terhadap *state of the art* dalam keamanan data teks pada penyimpanan awan, analisis kesenjangan terhadap pendekatan yang telah ada, dan keunikannya dari pendekatan gabungan tersebut akan menjadi fokus utama dari penelitian kami.[7]

Perlindungan keamanan data teks memiliki peran yang sangat krusial dalam menjaga kerahasiaan informasi sensitif dan pribadi pengguna. Dalam menghadapi peningkatan ancaman keamanan *cyber* yang semakin kompleks, kebutuhan akan pendekatan keamanan yang inovatif dan kokoh semakin mendesak.[3] Oleh karena itu, penelitian ini dilakukan dengan tujuan mengidentifikasi potensi keamanan yang dapat diberikan oleh penggunaan kombinasi algoritma Vigenere Cipher dan steganografi LSB pada data teks yang disimpan di Google Drive.[10]–[12]

Tujuan utama dari penelitian ini adalah untuk menguji dan mengevaluasi efektivitas penggunaan kombinasi algoritma Vigenere Cipher dan steganografi LSB dalam memperkuat keamanan data teks di Google Drive.[12] Selain itu, penelitian ini berupaya mengenali potensi kelemahan atau risiko yang mungkin timbul, serta mengajukan rekomendasi perbaikan yang dapat diterapkan.[13] Dengan menguraikan *state of the art*, melakukan analisis kesenjangan, dan menjelaskan kebaruan dari pendekatan yang diusulkan, penelitian ini diharapkan dapat memberikan kontribusi positif terhadap perkembangan strategi keamanan data teks dalam aplikasi penyimpanan awan seperti Google Drive.[5]

Metode Penelitian

Desain Penelitian

Penelitian ini bertujuan untuk membuat aplikasi yang memanfaatkan gabungan antara algoritma kriptografi Vigenere Cipher dan steganografi LSB (Least Significant Bit) dengan tujuan meningkatkan tingkat keamanan data teks di aplikasi Google Drive.[8]

Penerapan Program

Penerapan ini dilakukan dengan merujuk kepada beberapa pedoman, termasuk tabel Vigenere huruf sebagai dasar acuan untuk memodifikasi algoritma Vigenere Cipher, dan tabel ASCII 8 bit sebagai dasar untuk mengonversi huruf ke dalam bilangan biner, memudahkan implementasi teknik Least Significant Bit (LSB).[9]–[11]

Vigenere Cipher, pertama kali diperkenalkan oleh Giovan Batista Belaso dalam bukunya "La Cifra del. Sig.Giovan Batista Belaso (1553)," menggunakan tabel Vigenere dan angka sebagai pengganti huruf alfabet untuk menghasilkan *ciphertext*. Dalam penerapannya. [13]–[15]

Salah satu metode steganografi paling sederhana untuk menyisipkan pesan pada media gambar adalah menggunakan Least Significant Bit (LSB). Metode ini memanfaatkan bit terakhir untuk dimodifikasi tanpa menghasilkan perubahan yang signifikan pada gambar. Proses penyisipan informasi berupa bit dilakukan pada bit terakhir (8 bit) setiap piksel. Sebagai contoh, jika pesan rahasia adalah 01000001, maka bit terakhir dari setiap piksel akan dimodifikasi. Pendekatan LSB embedding dapat digunakan untuk berbagai tujuan keamanan multimedia dan dapat diaplikasikan pada berbagai format tipe data. Oleh karena itu, LSB merupakan metode steganografi yang populer hingga saat ini.[1]–[3]

Rancangan Kegiatan

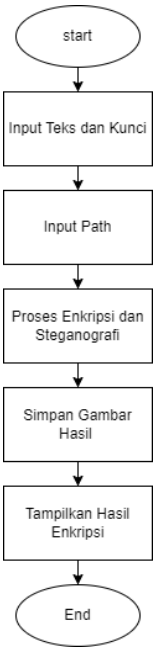
Penelitian ini akan dimulai dengan telaah mendalam terhadap literatur yang relevan dengan algoritma kriptografi Vigenere Cipher dan steganografi LSB. Fokus tahap awal ini adalah memperoleh pemahaman

yang komprehensif mengenai kemajuan terkini dan implementasi kedua algoritma tersebut dalam konteks keamanan data.[14]

Setelah mendapatkan dasar teoritis yang kokoh, langkah selanjutnya adalah mengembangkan model sistem yang mengintegrasikan algoritma kriptografi Vigenere Cipher dan steganografi LSB. Tahap ini memerlukan perancangan model yang dapat beroperasi secara efektif bersama-sama, menghasilkan tingkat keamanan optimal untuk data teks di dalam aplikasi Google Drive.

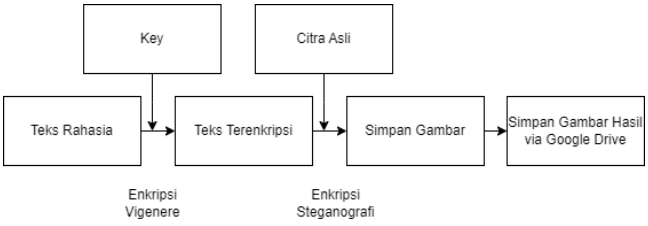
Proses implementasi model sistem yang telah dirancang akan menjadi tahap berikutnya. Melalui langkah ini, model sistem akan diwujudkan dalam bentuk nyata, memfasilitasi proses enkripsi dan dekripsi data teks menggunakan kombinasi algoritma kriptografi dan steganografi.

Tahap terakhir dalam rancangan kegiatan ini adalah evaluasi terhadap keberhasilan dan tingkat keamanan dari metode yang diimplementasikan. Pengujian menyeluruh akan mencakup aspek-aspek seperti enkripsi, dekripsi, dan analisis potensi kelemahan yang mungkin muncul. Hasil evaluasi akan dianalisis secara mendalam untuk memberikan gambaran yang tajam mengenai efektivitas metode yang telah diaplikasikan.



Gambar 1 Tahap Rancangan

Enkripsi dalam sistem ini disesuaikan dengan metode yang diimplementasikan, yaitu menggunakan metode Vigenere Cipher. Proses penyandian dan penyisipan pesan teks dilakukan dengan memanfaatkan metode Vigenere Cipher, yang kemudian dikombinasikan dengan Metode LSB steganografi. Proses ini secara khusus diterapkan pada data gambar dalam aplikasi Google Drive, sebagaimana diilustrasikan dalam Gambar 1.



Gambar 2 Tahap Penyandian

Pada gambar 2 terlihat proses enkripsi dan steganografi dengan menggunakan unsur-unsur seperti kunci, citra asli, teks rahasia, dan teks terenkripsi. Proses dimulai dengan pemilihan kunci dan citra asli, diikuti oleh penulisan dan enkripsi teks rahasia menggunakan algoritme Vigenere. Teks terenkripsi kemudian disimpan dan dimasukkan ke dalam citra asli melalui teknik steganografi. Penerapan proses ini bermanfaat dalam berbagai konteks, terutama terkait dengan keamanan, privasi, dan penyimpanan informasi rahasia.

Ruang Lingkup atau Objek Penelitian

Fokus penelitian ini adalah metode penelitian yang diperlukan untuk mencapai tujuan utama, yaitu menciptakan aplikasi yang menggunakan kombinasi algoritma kriptografi Vigenere Cipher dan steganografi LSB untuk meningkatkan tingkat keamanan data teks di aplikasi Google Drive.[15]

Tempat Penelitian

Lokasi penelitian mencakup lingkungan akademik dan pusat penelitian yang memiliki fasilitas yang sesuai untuk melaksanakan penelitian ini, seperti laboratorium komputer dan akses internet.

Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan menerapkan algoritma kriptografi Vigenere Cipher dan steganografi LSB untuk mengamankan dan menyembunyikan informasi pada data teks.[16]

Teknik Analisis Penelitian

Analisis penelitian melibatkan uji coba serta evaluasi terhadap keberhasilan dan tingkat keamanan dari metode yang diimplementasikan. Selain itu, dilakukan perbandingan hasil dengan metode lain yang relevan.[4], [9] Dalam penelitian ini, peneliti mengadopsi pendekatan interdisiplin untuk menghasilkan aplikasi yang menggabungkan algoritma kriptografi Vigenere Cipher dan steganografi LSB. Harapannya, penelitian ini dapat memberikan kontribusi positif dalam meningkatkan keamanan data teks di aplikasi Google Drive.[1], [3]

Variabel Pengujian

Mean Square Error (MSE)

MSE adalah metrik analisis kuantitatif yang digunakan untuk mengevaluasi kualitas citra yang dihasilkan dan keunggulan suatu metode yang diterapkan. Dalam matriks citra berukuran m * n, B1 dan B2 mewakili matriks citra. Secara sederhana, Mean Square Error (MSE) mengukur rata-rata dari selisih kuadrat antara sinyal piksel citra hasil pemrosesan dengan sinyal asli. Nilai MSE yang lebih rendah menunjukkan tingkat kesalahan yang lebih kecil dan kualitas citra yang lebih baik. MSE memiliki nilai nol. Rumus MSE dapat dinyatakan di dalam gambar 3.

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i,j) - g(i,j)]^2$$

Gambar 3 Rumus MSE

Peak Signal to Noise Ratio(PSNR)

PSNR, atau Peak Signal-to-Noise Ratio, merupakan metrik kualitas citra yang mengukur sejauh mana citra yang dihasilkan oleh suatu sistem mendekati citra aslinya. Nilai PSNR yang tinggi mengindikasikan kualitas citra yang lebih baik. Perhitungan PSNR menggunakan rumus seperti gambar 4.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}$$

Gambar 4 Rumus PSNR

Hasil dan Pembahasan

Dalam aplikasi yang dikembangkan berdasarkan prinsip algoritma Vigenere yang dikombinasikan dengan steganografi gambar menggunakan teknik LSB pada keamanan teks dalam aplikasi google drive, langkah-langkah yang harus dilakukan mencakup proses sebagai berikut:

Inisialisasi Algoritma Vigenere:

Langkah awal melibatkan memulai algoritma Vigenere dengan menetapkan kunci kriptografi yang akan digunakan untuk melindungi teks data. Seperti yang sudah ditentukan pada table vigenere chipper, yang terdapat pada gambar 5.

	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 Tabel Vigenere

Enkripsi Data Teks:

Penerapan algoritma Vigenere digunakan untuk mengenkripsi data teks yang akan disimpan atau ditukar. Proses ini melibatkan penggunaan kunci sebagai kunci enkripsi untuk menjaga keamanan konten teks.

Tabel 1 Hasil yang disisipkan pada citra

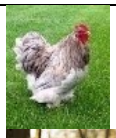
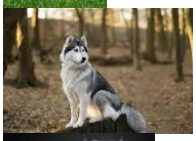
No	Nama Citra	Pesan Teks	Kunci	Pesan Teks Hasil Dekripsi
1	Ayam.png	Universitas pelita bangsa	xavier	Universitas pelita bangsa
2	Anjing.png	Saya sedang makan	lancelot	Saya sedang makan
3	Kucing.png	https://ecampus.pelitabangsa.ac.id/pb/login	yve	https://ecampus.pelitabangsa.ac.id/pb/login

Informasi pada citra awal diubah menjadi bentuk terenkripsi dengan menggunakan suatu kunci, dan selanjutnya berhasil dikembalikan ke bentuk aslinya melalui proses dekripsi. Kunci yang sesuai memiliki peran krusial dalam memastikan keberhasilan proses dekripsi dan mengembalikan teks ke bentuk semula. Penerapan steganografi LSB digunakan untuk menyematkan data teks yang sudah dienkripsi ke dalam gambar. Dalam teknik ini, setiap piksel pada gambar berperan sebagai tempat penyimpanan untuk. Sebagian dari data teks tersebut. Seperti yang disajikan pada tabel 1

Pemilihan Gambar Penyimpanan:
Penetapan citra sebagai media penyimpanan data hasil enkripsi menjelaskan langkah di mana citra dipilih sebagai tempat untuk menyimpan teks yang telah melalui proses enkripsi. Dalam situasi ini, citra tidak hanya bertindak sebagai alat penyimpanan, tetapi juga berperan sebagai sarana untuk menyembunyikan informasi yang telah dienkripsi dengan aman.

Steganografi dengan Teknik LSB:
Menandakan bahwa pembahasan akan melibatkan tinjauan mendalam terhadap elemen-elemen krusial yang membentuk sifat citra. Dalam analisis ini, perhatian difokuskan pada aspek-aspek seperti nama file, dimensi citra (lebar x tinggi), dan ukuran file dalam kilobita (KB). Informasi ini dianggap signifikan untuk mengenali pengaruh citra terhadap kapasitas penyimpanan dan kualitas visualnya, dan juga relevan dengan tujuan atau kebutuhan penggunaan citra tersebut. Pemanfaatan metode LSB (Least Significant Bit) dalam steganografi melibatkan penggunaan bit-bit paling tidak signifikan pada setiap piksel gambar untuk menyimpan bit-bit data teks yang telah dienkripsi. Proses ini memungkinkan penyembunyian data tanpa memberikan dampak yang berlebihan pada kualitas visual dari gambar.

Tabel 2 Citra yang digunakan

No	Nama Citra	Gambar Citra	Ukuran Citra	Ukuran Citra (KB)
1	Ayam.png		205*246	13 KB
2	Anjing.png		276*183	7 KB
3	Kucing.png		238*211	6 KB

Memberikan pandangan holistik mengenai ciri-ciri citra, termasuk rincian seperti nama file, dimensi, dan ukuran file. Data ini memiliki nilai penting dalam penilaian dampak citra terhadap kapasitas penyimpanan serta kualitas visual, sesuai dengan keperluan dan tujuan penggunaannya, seperti yang tertera pada tabel 2.

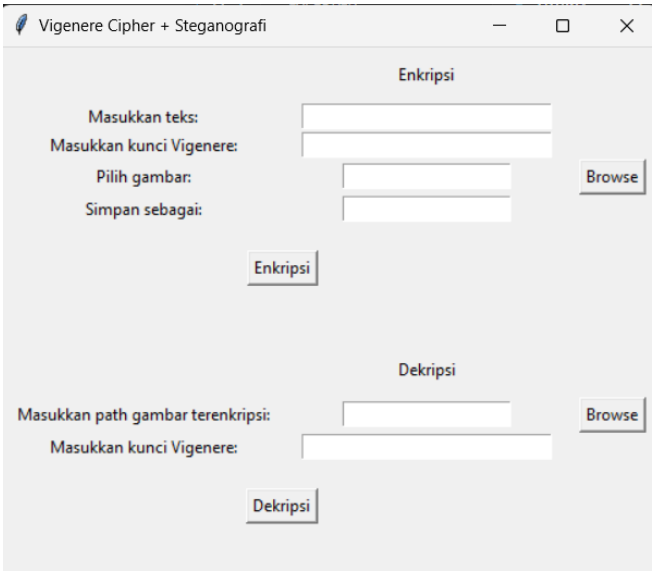
Tabel 3 Detail citra terenkripsi

No	Nama Citra	Nama Citra Terenkripsi	Pesan teks	MSE	PSNR
1	Ayam.png	Ayam-encrypted.png	Universitas pelita bangsa	0.000813	79.029854
2	Anjing.png	Anjing-encrypted.png	Saya sedang makan	0.000527	80.904718
3	Kucing.png	Kucing-encrypted.png	https://ecampus.pelitabangsa.ac.id/pb/login	0.001161	77.480229

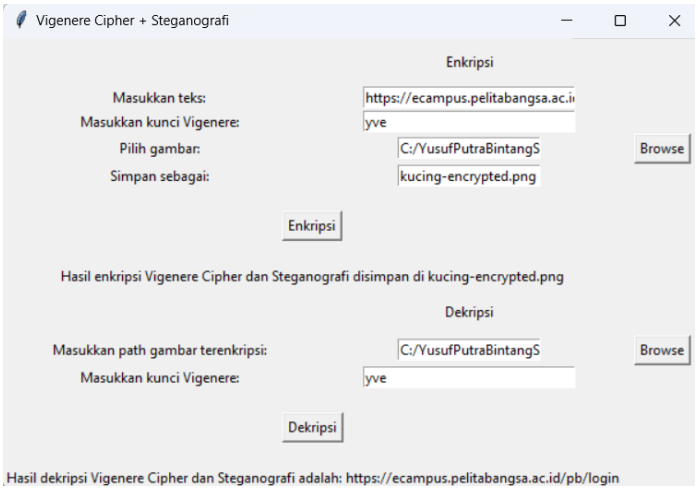
Kami telah menganalisis dimana pada tabel 3 tedapat informasi mengenai hasil kinerja proses enkripsi, mencakup nama file, teks terenkripsi, dan penilaian numerik seperti MSE dan PSNR. Evaluasi ini bermanfaat untuk mengukur sejauh mana kemampuan enkripsi dalam menjaga kualitas citra dan sejauh mana citra terenkripsi mampu merepresentasikan citra asli. terlihat bahwa nilai MSE relatif kecil dan nilai PSNR cukup tinggi untuk setiap citra, menunjukkan bahwa proses steganografi yang dilakukan memberikan hasil yang baik dengan sedikit distorsi pada citra stego. Hal ini menandakan bahwa pesan teks berhasil disisipkan ke dalam citra dengan baik tanpa mengorbankan kualitas citra secara signifikan. Di mana suatu gambar yang telah di pilih untuk dijadikan penyimpanan sebuah teks untuk diamankan

Simpan Gambar Termodifikasi ke dalam Aplikasi Google Drive:
Hasil akhir dari proses ini adalah gambar yang telah diubah dengan menyematkan data teks, kemudian disimpan dalam aplikasi Google Drive. Gambar tersebut berfungsi sebagai representasi visual yang mengandung informasi tersembunyi, yang dapat diambil kembali melalui proses dekripsi yang sesuai.

Desain Antarmuka
Antarmuka merupakan suatu sarana komunikasi antara pengguna dan sistem dengan tujuan membuat penggunaan sistem menjadi lebih mudah. Berikut adalah perancangan antarmuka untuk menerapkan kriptografi menggunakan kombinasi Vigenere Cipher dan metode steganografi LSB pada aplikasi Google Drive. Sebagaimana ilustrasi antarmuka pada program aplikasi terdapat pada gambar 6 dan gambar 7.



Gambar 6 Antarmuka Grafis Pengguna (GUI) untuk proses enrypt dan decrypt



Gambar 7 Program dijalankan

Kesimpulan
Kombinasi antara algoritma Vigenere Cipher dan steganografi LSB terbukti meningkatkan tingkat keamanan data teks dalam aplikasi Google Drive. Pendekatan metodologi yang diusulkan efektif dalam menjaga

kerahasiaan dan keamanan data teks yang disimpan di platform Google Drive. Penelitian ini memberikan kontribusi positif terhadap pengembangan strategi keamanan data teks dalam konteks penyimpanan awan seperti Google Drive. Sebagai saran untuk penelitian mendatang, disarankan untuk menguji metode ini pada berbagai jenis file dan ukuran data guna mengevaluasi kehandalan dalam skenario yang lebih luas.

Ucapan Terima Kasih

Kami mengucapkan terima kasih atas undangan untuk mengirimkan jurnal untuk Seminar Nasional Sains dan Teknologi Ke-3 di Universitas Pelita Bangsa. Kami sangat menghargai peluang ini untuk berbagi hasil penelitian kami tentang meningkatkan keamanan data teks di Google Drive dengan menggabungkan algoritma Vigenere Cipher dan steganografi LSB. Kami berharap penelitian ini dapat memberikan kontribusi positif dalam pengembangan strategi keamanan data teks di platform penyimpanan cloud. Terima kasih atas kesempatan yang diberikan.

Daftar Rujukan

[1] D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwan, "Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi," *Jurnal Sains dan Teknologi (JSIT)*, vol. 3, no. 1, pp. 47–52, Jan. 2023, doi: 10.47233/jsit.v3i1.483.

[2] S. Garg, V. Jindal, H. Bhatia, R. Johari, and S. Gupta, "Community oriented socio-behavioural PentaPlicative Cipher Technique," *Egyptian Informatics Journal*, vol. 24, no. 1, pp. 71–80, Mar. 2023, doi: 10.1016/j.eij.2022.12.001.

[3] M. Minarni and R. Redha, "IMPLEMENTASI LEAST SIGNIFICANT BIT (LSB) DAN ALGORITMA VIGENERE CIPHER PADA AUDIO STEGANOGRAFI," *Jurnal Sains dan Teknologi: Jurnal Keilmuan dan Aplikasi Teknologi Industri*, vol. 20, no. 2, p. 168, Dec. 2020, doi: 10.36275/stsp.v20i2.268.

[4] Kartika Yulianti, Alvira Firjan Humaira, and R. Marwati, "Implementasi Kriptografi Secret Sharing Scheme dan Steganografi Audio Least Significant Bit (LSB)," *JMT : Jurnal Matematika dan Terapan*, vol. 5, no. 1, pp. 1–11, Feb. 2023, doi: 10.21009/jmt.5.1.1.

[5] B. A. Esttaifan, "A Modified Vigenère Cipher based on Time and Biometrics features," *Journal of Engineering*, vol. 29, no. 6, pp. 128–139, Jun. 2023, doi: 10.31026/j.eng.2023.06.10.

[6] M. Mohamed, M. Mofaddel, and T. Abd El-Naser, "Comparison Study Between Simple LSB and Optimal LSB Image Steganography," *Sohag Journal of Sciences*, vol. 8, no. 1, pp. 29–33, Jan. 2023, doi: 10.21608/sjsci.2022.165686.1036.

[7] D. E. Wijayanti and W. Romadlon, "Keamanan Pesan Menggunakan Kriptografi dan Steganografi Least Significant Bit pada File Citra Digital," *Euler : Jurnal Ilmiah Matematika, Sains dan Teknologi*, vol. 10, no. 2, pp. 181–192, Oct. 2022, doi: 10.34312/euler.v10i2.16646.

[8] S. A. Jebur, A. K. Nawar, L. E. Kadhim, and M. M. Jahefer, "Hiding Information in Digital Images Using LSB Steganography Technique," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 7, pp. 167–178, 2023, doi: 10.3991/ijim.v17i07.38737.

[9] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Applied Sciences*, vol. 13, no. 21, p. 11771, Oct. 2023, doi: 10.3390/app132111771.

[10] T. Alawiyah, R. Ardianto, and D. S. Purnia, "Implementasi Vigenere Cipher Sebagai Pengaman Pada Proses Deskripsi Steganografi Least Significant Bit," *JURNAL INFORMATIKA*, vol. 7, no. 1, 2020, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji. doi: https://doi.org/10.31311/ji.v7i1.6431

[11] T. K. Watimena, "KEAMANAN DATA MENGGUNAKAN METODE LSB DAN ENKRIPSI VIGENERE," *Jurnal Teknologi Informasi*, vol. 4, no. 1, 2020. doi: https://doi.org/10.36294/jurti.v4i1.1253

[12] R. Toyib and Y. Darnita, "16 No.1 Februari 2020 Pengamanan Data Teks Dengan Menggunakan Algoritma Zero-Knowledge Proof." doi: https://doi.org/10.37676/jmi.v16i1.1114

[13] L. C. Purba, M. Zarlis, I. Gunawan, S. Sumarno, and Z. M. Nasution, "PENGGUNAAN ALGORITMA LSB DAN VIGENERE UNTUK PENGAMANAN DATA MELALUI POLA CITRA DIGITAL," *TECHSI - Jurnal Teknik Informatika*, vol. 13, no. 2, p. 53, Oct. 2021, doi: 10.29103/techsi.v13i2.5162.

[14] T. Alawiyah, R. Ardianto, and D. S. Purnia, "Implementasi Vigenere Cipher Sebagai Pengaman Pada Proses Deskripsi Steganografi Least Significant Bit," *JURNAL INFORMATIKA*, vol. 7, no. 1, 2020, [Online]. Available: http://ejournal.bsi.ac.id/ejurnal/index.php/ji. doi: https://doi.org/10.31311/ji.v7i1.6431

[15] S. Rahman *et al.*, "Multi Perspectives Steganography Algorithm for Color Images on Multiple-Formats," *Sustainability (Switzerland)*, vol. 15, no. 5, Mar. 2023, doi: 10.3390/su15054252.

[16] D. Chaudhari, H. Patel, A. Ghosh, N. Patil, V. Pawar, and Y. Sonawane, "A Survey on Image Steganography using LSB Algorithm," Elsevier-SSRN, 2023. [Online]. Available: https://ssrn.com/abstract=4671618. doi: https://doi.org/10.2139/ssrn.4671618