PENGEMBANGAN DOUBLE ENKRIPSI ALGORITMA *VIGINERE CHIPHER DAN TRIPLE CULUMNER* UNTUK PENGAMANAN FILE GAMBAR

Karen Dea Nikpani[1)], Irmayani[2)], Ayu Mutia Br.Sembiring[3)], Putri Arina[4)], Achmad Fauzi[5)]
[1,2,3,4,5)]STMIK Kaputama
Jl. Veteran, No. 4A-9A, Kel. Tangsi, Kec. Binjai Kota, Kota Binjai
Email : karendeanikpani@gmail.com

ABSTRAKS

Data security, particularly for image files, is increasingly important in the digital era to protect information from unauthorized access and other threats. This study proposes a combination of the Vigenère Cipher and Triple Columnar Transposition algorithms for securing image files. The Vigenère Cipher algorithm encodes data through polyalphabetic substitution, while the Triple Columnar Transposition scrambles the data sequence to enhance confidentiality. The proposed encryption system employs a super encryption approach, where data is encrypted in layers using both algorithms. The research results show that this method improves data efficiency and security against cryptanalysis attacks while preserving the integrity of image files. Therefore, this approach is expected to provide a significant solution for securing digital data in various applications.

Keywords: *Image_File_Security, Super_Encryption, Triple_Columnar_Transposition, Vigenère_Cipher,*

1. PENDAHULUAN

Dalam era digital saat ini, kebutuhan akan pengamanan data semakin meningkat. Informasi dalam bentuk file, terutama file gambar, sering kali menjadi sasaran serangan siber seperti pencurian data dan manipulasi informasi. Oleh karena itu, diperlukan metode enkripsi yang andal untuk memastikan keamanan data tersebut.

Algoritma kriptografi menjadi salah satu solusi utama dalam menjaga kerahasiaan dan integritas data. Salah satu algoritma yang telah lama digunakan adalah Vigenère Cipher, yang dikenal karena kemampuannya dalam mengenkripsi teks menggunakan pendekatan substitusi polialfabetik. Meskipun demikian, algoritma ini memiliki kelemahan, terutama dalam menghadapi analisis frekuensi oleh pihak yang tidak berwenang [1].

Untuk meningkatkan keamanan, penggabungan beberapa algoritma kriptografi dapat memberikan solusi yang lebih robust. Salah satu pendekatan yang dapat dilakukan adalah dengan mengintegrasikan algoritma Vigenère Cipher dengan metode enkripsi lainnya, seperti Triple Columnar Transposition. Triple Columnar Transposition adalah metode enkripsi yang menggunakan teknik transposisi berulang untuk mengacak urutan data sehingga sulit untuk direkonstruksi tanpa kunci yang tepat.

Dalam penelitian ini, diusulkan penggabungan algoritma Vigenère Cipher dan Triple Columnar Transposition untuk menciptakan sistem enkripsi yang lebih kuat dalam melindungi file gambar. Penggunaan kombinasi kedua algoritma ini diharapkan mampu memberikan tingkat keamanan yang lebih tinggi, dengan memanfaatkan kelebihan masing-masing metode. Selain itu, penelitian ini juga mengevaluasi kinerja sistem enkripsi yang diusulkan dari segi kecepatan, kompleksitas, dan ketahanan terhadap serangan kriptanalisis.

Dengan adanya sistem enkripsi yang diusulkan, diharapkan dapat memberikan kontribusi nyata dalam pengembangan teknologi pengamanan data, khususnya untuk melindungi file gambar dari ancaman yang semakin kompleks di era digital ini.

Aspek kemanan data menjadi sangat krusial di era digital saat ini, terutama dengan meningkatnya volume informasi yang disimpan dan dibagikan secara daring. File gambar, yang sering kali mengandung informasi sensitive atau pribadi, adalah satu jenis data yang memerlukan perlindungan. Untuk menjaga keamanan file-file ini dari akses yang tidak di inginkan, diperlukan metode enkripsi yang handal. Algoritma Viginere yang telah digunakan sejak lama merupakan salah satu teknik enkripsi yang efektif dalam menyembunyikan pesan dengan memanfaatkan kunci yang berulang [2].

Penerapan metode Tiple Columner Transposition dapat meningkatkan keamanan dengan mengacak posisi karakter dalam pesan yang telah di enkripsi. Kombinasi kedua teknik ini dapat memberikan solusi yang lebih kuat untuk melindungi file gambar, Sehingga dapat meningkatkan tingkat keaamanan data dan kerahasiaan data gambar yang disimpan.

Penelitian ini bertujuan untuk mengeksplorasi kedua algoritma tersebut dalam pengamanan file gambar, Serta menganalisis efektivitasnya dalam menghadapi serangan yang terjadi. Melalui penelitian ini, diharapkan dapat memberikan kontribusi yang signifikan dalam bidang keamanan data, Khususnya dalam pengelolaan file gambar yang semakin banyak digunakan di dalam berbagai aplikasi, mulai dari media social sehingga penyimpanan berbasis cloud.

Dalam upaya melindungi data dan informasi, Terdapat dua syarat penting yang harus di penuhi, yaitu kerahasiaan dan integritas data. Kerahasiaan merujuk pada upaya untuk menjaga agar data yang dikirimkan kepada penerima tidak dapat di akses oleh pihak lain, serta membatasi akses bagi individu yang berusaha mengetahui atau merusak isi data tersebut. Sementara itu, Integritas data berkaitan dengan memastikan bahwa data tetap utuh dan sampai kepada penerima tanpa mengalami modifikasi oleh pihak yang tidak berwenang, tanpa izin dari pemilik informasi [3].

Penelitian yang akan digunakan bertujuan untuk meningkatkan system keamanan dengan memanfaatkan dua metode , yaitu metode viginere dan metode Triple columner. Metode viginere akan digunakan untuk menyandikan kunci, Sementara metode Triple columner akan di terapkan untuk menyandikan gambar.

Dalam melakukan super enkripsi menggunakan Triple columner, langkah pertama dengan menuliskan karakter dari gambar asli dalam orientasi baris dengan panjang karakter yang sama. Selanjutnya karakter tersebut di tulis dengan orientasi

kolom, Sehingga di hasilkan gambar yang telah disandikan. Untuk proses dekripsi jumlah baris dapat di hitung dengan memberi panjang kunci.

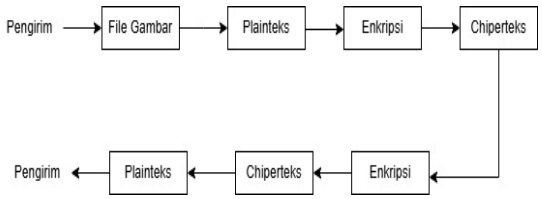
2. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimen untuk menguji efektivitas pengamanan file gambar dengan kombinasi algoritma Vigenère Cipher dan Triple Columnar Transposition. Tahapan metode penelitian dijelaskan sebagai berikut:

1. **Tahap Persiapan**
   a. Mengumpulkan data berupa file gambar dalam format JPEG yang akan digunakan sebagai sampel.
   b. Menentukan kunci enkripsi untuk masing-masing algoritma.
   c. Mengembangkan perangkat lunak berbasis bahasa pemrograman Python untuk implementasi algoritma.
2. **Tahap Implementasi**
   a. Proses Enkripsi: File gambar dikonversi menjadi representasi bilangan hexadecimal, kemudian dienkripsi menggunakan algoritma Vigenère Cipher dan Triple Columnar Transposition secara berurutan.
   b. Proses Dekripsi: Data yang telah dienkripsi diuji kembali untuk memastikan dapat didekripsi hingga menghasilkan file gambar asli.
3. **Tahap Evaluasi**
   a. Mengukur kinerja algoritma dari segi waktu proses enkripsi dan dekripsi.
   b. Mengevaluasi tingkat keamanan dengan melakukan analisis ketahanan terhadap serangan brute force dan analisis frekuensi.
   c. Membandingkan hasil enkripsi terhadap parameter kualitas gambar, seperti Peak Signal-to-Noise Ratio (PSNR) untuk memastikan bahwa proses enkripsi tidak merusak data.
4. **Tahap Analisis Data**
   a. Mengolah dan menganalisis data hasil pengujian menggunakan metode statistik deskriptif.
   b. Menyimpulkan efektivitas metode yang diusulkan berdasarkan hasil eksperimen.

Dengan desain penelitian ini, diharapkan sistem enkripsi yang diusulkan dapat memberikan solusi pengamanan data gambar yang lebih efektif dan efisien.

Enkripsi dan dekripsi adalah dua proses yang digunakan dalam penelitian kriptografi. Proses enkripsi menyandikan pesan yang disebut ciphertext. Proses dekripsi mengembalikan ciphertext ke pesan asli atau plaintext. Begitu juga dengan enkripsi, dekripsi membutuhkan kunci. Studi ini menggunakan kunci simetris, yang berarti pengirim dan penerima pesan menggunakan kunci yang sama [4]. Pengirim pesan melakukan enkripsi dan penerima melakukan dekripsi. Bahasa pemrograman yang digunakan dalam penelitian adalah Q/C++ Frame Work. Huruf yang digunakan adalah huruf kapital. Gambar 2 menunjukkan skema umum proses enkripsi dan dekripsi.



Gambar.1 Skema Umum Enkripsi dan Dekripsi

2. 1 Double Enkripsi

Super enkripsi merupakan teknik dalam kriptografi yang melibatkan dua algoritma enkripsi secara berurutan untuk meningkatkan pengamanan file gambar.

Dalam proses super enkripsi , gambar yang telah di enkripsi dengan satu algoritma kemudian akan di enkripsi lagi menggunakan algoritma lain. Penerapan super enkripsi yaitu, penggunakan dua algoritma, data dapat di enkripsi pertama kali menggunakan algoritma Vigenere Chiper dan kemudian di enkripsi lagi menggunakan Algoritma Triple Columner [4].

2.2 Pengertian Kriptografi

"Kriptografi" adalah istilah yang berasal dari bahasa Yunani, dari kata "cryptós" yang berarti "rahasia" dan "graphein" yang berarti "kata tulisan." Karena itu, kriptografi secara umum didefinisikan sebagai tulisan rahasia. Berbagai sumber literatur memberikan berbagai definisi kriptografi. Namun, buku-buku terbaru mendefinisikan kriptografi sebagai ilmu yang mempelajari cara mengirimkan pesan secara rahasia sehingga hanya orang yang dimaksud yang dapat menghapus dan membaca atau memahami pesan tersebut [5].

Kriptografi adalah bidang ilmu yang mempelajari cara mengamankan data untuk melindungi kerahasiaan, integritas, dan autentikasi data dari bahaya seperti penyadapan atau manipulasi. Dalam proses enkripsi, algoritma dan kunci tertentu digunakan untuk mengubah data asli (plaintext) menjadi bentuk yang sulit dipahami (ciphertext). Sebaliknya, proses dekripsi mengembalikan ciphertext ke bentuk plaintext dengan menggunakan kunci yang tepat [6]. Oleh karena itu, kriptografi menjadi alat penting untuk melindungi data digital di berbagai industri, seperti perbankan, komunikasi, dan penyimpanan data sensitif.

Oleh karena itu, kriptografi adalah seni dan ilmu yang bertujuan untuk menjaga keamanan pesan; secara umum, kriptografi adalah teknik pengamanan informasi di mana informasi diubah dengan kunci tertentu sehingga menjadi informasi baru yang tidak dapat dipahami oleh orang yang tidak berhak menerimanya, dan hanya orang yang berhak menerimanya yang dapat mengubahnya [7].

2.2 Viginere Chipher

Salah satu sistem sandi polialfabetik yang paling sederhana, Vigenere cipher, mengenkripsi sekaligus sebuah teks yang terdiri dari beberapa hurul. Seperti kripto Caesar, kripto Vigenere menggunakan substitusi dengan fungsi shift. Keamanan cipher Vigenere tergantung pada jumlah kunci yang digunakan [6].

Enkripsi

Enkripsi (penyandian) dengan sandi Vigenère juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus, yaitu: C(PK), mod 256.. (3)

Dekripsi

Untuk melakukan proses dekripsi, dimana cipherteks akan diubah ke plainteks digunakan rumus sebagai berikut:

P=(CK); mod 256.. (4)

Keterangan: Ci adalah huruf ke-i pada teks tersandi, Pi adalah huruf ke-i pada teks terang, Ai adalah huruf ke-i pada kata kunci, dan mod adalah operasi pembagian).

2.3 Triple Columner

Salah satu jenis sandi transposisi adalah koloner. Sandi kolom bekerja dengan menulis ulang teks asli dengan orientasi baris dan panjang karakter yang sama, kemudian menulis ulang teks sandi dengan orientasi kolom. Sadikin (2012) Metode Triple Columner menggunakan tiga jenis kunci yang berbeda, yang masing-masing digunakan dalam proses enkripsi dan dekripsi.

2.4 File Gambar

Gambar atau citra adalah gambaran, kemiripan, atau imitasi dari suatu objek. Cirta yang dihasilkan oleh sistem perekaman data dapat bersifat digital, yang dapat disimpan secara langsung pada media penyimpanan, atau optik, seperti foto[9].Dalam penelitian ini, format file gambar adalah jpeg.

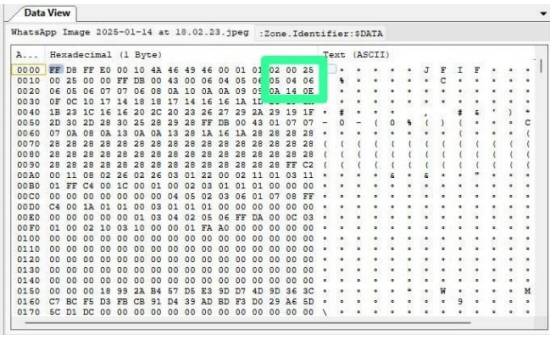
3. HASIL DAN PEMBAHASAN

3. 1 Proses Enkripsi

Mengubah gambar digital menjadi bentuk yang tidak dapat dikenali dengan menggunakan kunci dekripsi yang tepat. Gambar berikut dipilih Enkripsi file gambar adalah proses penting untuk melindungi privasi, mencegah akses tidak sah, atau kerahasiaan data gambar dengan untuk menghasilkan bilangan hexadecimal:

Gambar 2. File Gambar Format Jpeg

Nilai hexadecimal dari gambar diatas akan dienkripsi dengan Binary Viewer, program tambahan. Nilai hexadecimal dari file gambar yang telah dikonversi, misalnya dengan menggunakan matriks 3 x 3, dapat ditemukan di sini:



Gambar Hasil Nilai Hexadesimal

Pada gambar diatas merupakan hasil nilai asciii hexadesimal yang di peroleh, matriks 3x3 yang akan dienkripsi (Plaintext) : 02 00 25 05 04 06 0A 14 0E .

File gambar akan dipotong menjadi blok bilangan hexadesimal setelah mendapatkan nilai ascii ascii. Kemudian, blok-blok ini akan dikonversikan ke dalam bilangan ASCII.

Tabel 1. Konversi Hexadesimal file gambar kedalam kode ASCII Decimal

Bilangan Hexadecimal	Plainteks(Ascii)Decimal
02	2
00	0
25	37
05	5
04	4
06	6
0A	10
14	20
0E	14

3. 1. 1 Proses Enkripsi Algoritma

Membangkitkan kunci adalah langkah pertama Algoritmaa autokey cipher.Algoritma ini memiliki pasangan kunci untuk setiap karakter data awal [2], yang berarti panjang kunci harus sama

dengan panjang plainteks. Namun, format plainteks biasanya berbeda dengan format kunci. Agar proses enkripsi dan dekripsi.
Plainteks : 2 0 37 5 4 6 10 20 14
Kunci : 66 105 110 106 97 105 66 105 110
Mod : 256
Cipherteks :…..?
Rumus : Ci = (Pi + Ki) mod 256
C1 = (Pi + Ki) mod 256
= (2 + 66) mod 256
= 68 -> D
C2 = (0 + 105) mod 256
= (105) mod 256
= 105 -> i
C3 = (37 + 110) mod 256
= (147) mod 256
= 147 -> []
C4 = (5 + 106) mod 256
= (111) mod 256
= 111 -> o
C5 = (4 + 97) mod 256
= (101) mod 256
= 101 -> e
C6 = (6 + 105) mod 256
= (111) mod 256
= 111 -> o
C7 = (10 + 66) mod 256
= (76) mod 256
= 76 -> L
C8 = (20 + 105) mod 256
= (125) mod 256
= 125 -> }
C9 = (14 + 110) mod 256
= (124) mod 256
= 124 -> |
Maka Chiperteks yang dihasilkan adalah **Di[]oeoL}|**

3. 1.2 Proses Enkripsi Algoritma Triple Columner

Triple Columner dengan pesan Di[]oeoL}| dan kunci satu yang digunakan yaitu BINJAI.
Kunci 2 adalah MEDAN
Kunci 3 GUMIT

Table 1. enkripsi menggunakan kunci 1

B	I	N	J	A	I
2	3	6	5	1	4
D	i	[]	0	e	0
L	}	1			

Chiphertext yang di dapat = eDLi}oo[]1

Tabel 2. Enkripsi menggunakan kunci 2

M	E	D	A	N
4	3	2	1	5
e	D	L	i	}
0	0	[]	I	

Chiphertext yang di dapat = ilL[]Doeo}

Tabel 3. Enkripsi menggunakan kunci 3

G	U	M	I	T
1	5	3	2	4
i	I	L	[]	0
0	e	0	}	

Chiphertext yang di dapat = io[]}LoD|e

1.3 Dekripsi Algoritma Triple Columner

Tahapan proses Dekripsi dengan metode Triple Columner. Ciphertext3 merupakan hasil penyandian pesan pada tahap akhir. Untuk melakukan proses dekripsi, maka dimulai dengan melakukan dekripsi ciphertext3.

Table 4. Dekripsi menggunakan kunci 1

B	I	N	J	A	I
2	3	6	5	1	4
D	i	[]	0	e	0
L	}	1			

Chiphertext yang di dapat = **eDLi}oo[]1**

Tabel 5. Dekripsi menggunakan kunci 2

M	E	D	A	N
4	3	2	1	5
e	D	L	i	}
0	0	[]	I	

Chiphertext yang di dapat = ilL[]Doeo}

Tabel 6 Dekripsi menggunakan kunci 3

G	U	M	I	T
1	5	3	2	4
i	I	L	[]	0
0	e	0	}	

Chiphertext yang di dapat = io[]}LoD|e

5. KESIMPULAN

Kesimpulan pada penelitian ini adalah:

1. Dapat meningkatkan keamanan file foto atau gambar dengan menggabungkan dua algoritma kriptografi, Vigenere Chiper dan Triple Columner. Sebagai tahap pertama enkripsi, algoritma Triple Columner digunakan.
2. Pada Proses dekripsi dilakukan secara terbalik, mulai dari Vigenere Chiper dan kembali ke Triple Columner, sehingga hanya kunci yang tepat yang dapat digunakan untuk memulihkan data asli. Metode ini meningkatkan perlindungan data dari akses yang tidak diinginkan.

DAFTAR PUSTAKA

[1] S. Sinurat and Maranatha Pasaribu, "Text Encoding Using Cipher Block Chaining Algorithm," *J. Info Sains Inform. dan Sains*, vol. 11, no. 2, pp. 13–17, 2021, doi: 10.54209/infosains.v11i2.42.

[2] N. Hapifah Purba, "Kombinasi Algoritma Cipher Block Chaining dan Triangle Chain Cipher dalam Penyandian File Text," *Bull. Comput. Sci. Res.*, vol. 2, no. 2, pp. 47–52, 2022, doi: 10.47065/bulletincsr.v2i2.155.

[3] M. Afsari, D. I. Mulyana, A. Damaiyanti, and N. Sa'adah, "Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text," *J. Pendidik. Sains dan Komput.*, vol. 2, no. 01, pp. 70–82, 2022, doi: 10.47709/jpsk.v2i01.1381.

[4] J. H. Sinaga, M. Pangaribuan, F. Fazly, I. Rivaldo, and I. Gunawan, "Penerapan Enkripsi Dan Deskripsi Menggunakan Algoritma Data Encryption Standart Dengan Pemograman Matlab," *J. Media Inform.*, vol. 4, no. 1, pp. 63–69, 2022, doi: 10.55338/jumin.v4i1.468.

[5] M. Hidayat, M. Tahir, A. Sukriyadi, A. Sulton, C. A. S. A, and S. A. F, "Penerapan kriptografi," vol. 2, no. 3, pp. 35–41, 2023.

[6] A. Ariska and W. Wahyuddin, "Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard)," *J. Sintaks Log.*, vol. 2, no. 2, pp. 9–19, 2022, doi: 10.31850/jsilog.v2i2.1734.

[7] L. Silalahi and A. Sindar, "Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 182–186, 2020, doi: 10.32672/jnkti.v3i2.2413.