JURNAL FASILKOM
Volume 13 No. 3 | Desember 2023: 570-577

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Teknik Keamanan Data Menggunakan Metode *Vigenere Cipher* Dan Steganografi Dalam Penyisipan Pesan Teks Pada Citra

Rahmad Prayogi Harahap[1], Abdul Halim Hasugian[2]
[1,2]Ilmu Komputer, Sains dan Teknologi, Universitas Islam Negeri Sumatera Utara
[1]prayogirahmad14@gmail.com*, [2]abdulhalimhasugian@uinsu.ac.id

Abstract

Increasing data security has become a top priority in various sectors, especially in the exchange of sensitive messages and information. One method used to secure text messages is by combining the Vigenere Cipher technique and steganography in embedding text messages in images. The problem faced in this research is how to combine and apply the vigenere cipher algorithm and LSB steganography to secure text messages inserted in an image in a web-based application and to see the large size of image files that have been inserted with ciphertext and those that have not yet undergone insertion with the aim of increasing the level of security in sending text messages by combining these two methods. The Vigenere Cipher method is used to encrypt text messages, resulting in encrypted messages that are difficult to understand without the proper key. Meanwhile, steganography is used to insert text messages into images, which makes the message visually hidden in the image. By combining these two methods, text messages are not only well encrypted, but also effectively hidden in the image. This research includes the implementation and testing of the Vigenere Cipher and steganography methods on various types of images. The test results show that using these two methods together can greatly improve data security. In addition, this research also discusses challenges that may arise in combining these two methods, such as image size, image quality. The results of this research can be used as a guide to improve the security of text message exchange in various applications, such as online communication, data storage, and so on. By combining Vigenere Cipher techniques and steganography, users can ensure that their text messages are safe and protected from unauthorized access.

Keywords*: Vigenere Cipher, steganography, image, encryption, decryption.*

Abstrak

Peningkatan keamanan data telah menjadi prioritas utama dalam berbagai sektor, terutama dalam pertukaran pesan dan informasi yang sensitif. Salah satu metode yang digunakan untuk mengamankan pesan teks adalah dengan menggabungkan teknik *Vigenere Cipher* dan steganografi dalam penyisipan pesan teks pada citra. Permasalahan yang dihadapi pada penelitian ini yaitu bagaimana mengkombinasikan dan menerapkan algoritma *vigenere cipher* dan steganografi LSB untuk pengamanan pesan teks yang disisipkan pada sebuah citra dalam aplikasi berbasis web dan melihat ukuran besar file citra yang sudah disisipkan ciphertext dan yang belum mengalami penyisipan dengan tujuan untuk meningkatkan tingkat keamanan dalam penyampaian pesan teks dengan menggabungkan dua metode tersebut. Metode *Vigenere Cipher* digunakan untuk mengenkripsi pesan teks, menghasilkan pesan terenkripsi yang sulit dipahami tanpa kunci yang tepat. Sedangkan steganografi digunakan untuk menyisipkan pesan teks ke dalam citra, yang membuat pesan tersebut tersembunyi secara visual dalam citra tersebut. Dengan menggabungkan kedua metode ini, pesan teks tidak hanya terenkripsi dengan baik, tetapi juga disembunyikan secara efektif dalam citra. Penelitian ini mencakup implementasi dan pengujian metode *Vigenere Cipher* dan steganografi pada berbagai jenis citra. Hasil pengujian menunjukkan bahwa penggunaan kedua metode ini secara bersama-sama dapat meningkatkan keamanan data dengan baik. Selain itu, penelitian ini juga membahas tantangan yang mungkin timbul dalam menggabungkan kedua metode ini, seperti ukuran citra, kualitas citra. Hasil penelitian ini dapat digunakan sebagai panduan untuk meningkatkan keamanan pertukaran pesan teks dalam berbagai aplikasi, seperti komunikasi online, penyimpanan data, dan lain sebagainya. Dengan menggabungkan teknik *Vigenere Cipher* dan steganografi, pengguna dapat memastikan bahwa pesan teks mereka aman dan terlindungi dari akses yang tidak sah.

Kata Kunci: *Vigenere Cipher*, steganografi, citra, enkripsi, dekripsi.

1. Pendahuluan

Kebutuhan akan akses informasi yang cepat muncul sebagai dampak dari pesatnya kemajuan teknologi saat ini, khususnya di bidang teknologi komunikasi. Evolusi ini sangat jelas terlihat, khususnya di media elektronik, dimana internet merupakan salah satu elemen kunci yang memberikan kontribusi signifikan terhadap hal tersebut. Manusia dapat mengkomunikasikan informasi melalui internet menggunakan perangkat teknologi seperti PC (Personal Computer) atau perangkat elektronik portabel seperti smartphone atau tablet. Insiden pencurian data termasuk dalam bahaya dengan persentase terbesar secara keseluruhan [1]. Media

P-ISSN : 2089-3353
E-ISSN : 2808-9162

sosial dan internet salah satu contoh yang banyak digunakan, oleh karena itu keamanan komunikasi menjadi semakin penting. Salah satu caranya adalah dengan menyembunyikan data sebelum mengirimkannya. Sistem informasi harus mematuhi standar ketat untuk keamanan dan kerahasiaan informasi. Sejumlah orang yang memanfaatkan fitur keamanan suatu sistem informasi telah mengembangkan teknik-teknik baru sebagai akibat dari pesatnya kemajuan informasi dan teknologi. Ketika suatu informasi dibagikan kepada orang lain, hal itu dapat menimbulkan dampak buruk bagi pemilik informasi tersebut.

Peneliti kali ini menguraikan sejumlah teknik yang mungkin dapat dimanfaatkan untuk meningkatkan keamanan data tersembunyi contohnya penyampaian informasi yang disisipkan pada sebuah gambar. Pesan atau dokumen yang disisipkan dalam file gambar dapat dipulihkan secara keseluruhan, artinya pesan yang disisipkan sebelum dan sesudah proses dekripsi memberikan hasil yang sama [2]. Beberapa kata yang berkaitan dengan keamanan pesan/data yang terkenal dalam ilmu komputer dan matematika dalam pengamanan file asli menjadi sebuah file acak dan kemudian diubah kembali menjadi pesan asli [3]. Dengan menggunakan teknik enkripsi dan kunci rahasia, kriptografi akan mengubah komunikasi menjadi ciphertext, sementara itu, pesan tersebut akan ditutupi oleh gambar dalam steganografi [4].

Tujuan utama teknik kriptografi dan steganografi adalah untuk melindungi data agar tidak diakses oleh orang yang tidak berhak. Perbedaan antara teknik ini adalah enkripsi melindungi isi pesan dengan menulis ulang, tetapi tetap terlihat karena ditulis dalam teks biasa. Algoritma *Vigenere Cipher* merupakan salah satu algoritma yang dapat diterapkan pada operasi kriptografi. *Vigenere cipher* mengenkripsi teks abjad dengan bantuan berbagai caesar sandi berdasarkan huruf dari beberapa kata kunci. Dalam teknik ini digunakan mekanisme pergeseran, yaitu menggeser karakter teks biasa dengan jumlah yang berbeda menggunakan tabel vigenere. Tabel vigenere yang diusulkan dalam teknik ini digunakan lebih lanjut untuk mengimplementasikan banyak algoritma yang berbeda. Di sisi lain, steganografi membuat pesan tidak terlihat dengan menyembunyikannya di dalam media digital [4]. Steganografi yang digunakan yaitu steganografi LSB (Least Significant Bit) yang digunakan untuk menyembunyikan informasi atau pesan rahasia ke dalam media digital, seperti gambar, audio, atau video, tanpa mengubah tampilan atau kesan visual dari media tersebut secara signifikan, jadi dalam penelitian ini pesan akan disisipkan pada sebuah citra atau gambar. Pesan yang dikodekan dalam gambar akan sulit diuraikan menggunakan salah satu dari dua teknik ini, kriptografi dan steganografi, atau kombinasi keduanya. Dalam penelitian martawireja et al., bahwa Advanced Encryption Standard (AES) dan Steganografi terbukti efektif mengubah pesan rahasia menjadi data yang sulit diidentifikasi [6]. Penelitian dari A. Rahman et al., yang menggunakan kombinasi algoritma *vigenere cipher* dan Rivest Shamir Adleman (RSA) dengan pengimplementasian menggunakan bahasa pemrograman java (Netbean) berhasil meningkatkan keamanan data dikarenakan adanya dua kombinasi dari algoritma tersebut [7].

Rumusan masalah pada penelitian ini adalah bagaimana mengkombinasikan dan menerapkan algoritma *vigenere cipher* dan steganografi LSB untuk pengamanan pesan teks yang disisipkan pada sebuah citra dalam aplikasi berbasis web dan melihat ukuran besar file citra yang sudah disisipkan ciphertext dan yang belum mengalami penyisipan. Penelitian ini bertujuan untuk pengamanan pesan teks sehingga pesan nantinya bersifat acak serta pesan dapat disisipkan pada sebuah citra yang tanpa mempengaruhi visual dari citra tersebut. Sistem mempunyai batasan yaitu pengguna harus mengetik atau mencopy sebuah pesan secara manual dan isi pesan tidak boleh mengandung simbol ataupun angka tertentu. Hasil akhir penelitian berupa aplikasi berbasis *website* yang menggunakan algoritma kriptografi *vigenere cipher* dan steganografi LSB sehingga dapat mengubah teks biasa menjadi teks acak yang disisipkan pada sebuah citra tanpa mempengaruhi visual citra tersebut dan juga dapat mendekripsikan kembali teks tersebut sehingga menambah keamanan dalam bertukar informasi.

2. Metode Penelitian

Uraian berikut memberikan konteks untuk kerangka penelitian ini:

1) Studi literatur
   Proses peninjauan bahan referensi pada algoritma enkripsi Vigenere dan steganografi LSB merupakan langkah awal dalam proyek penelitian ini.
2) Pengumpulan data
   Peneliti mengumpulkan informasi dari publikasi yang berkaitan dengan steganografi LSB dan enkripsi cipher Vigenere sehubungan dengan topik yang mereka angkat.
3) Perancangan sistem
   Saat ini bahasa pemrograman PHP digunakan untuk membuat aplikasi enkripsi *Vigenere Cipher* dan steganografi LSB yang dapat menginjeksi pesan ke dalam gambar.
4) Sistem Implementasi
   Untuk memastikan bahwa penambahan pesan ke citra berjalan dengan sukses, tahap implementasi program ini memerlukan eksekusi aplikasi dan menyelesaikan proses enkripsi dan dekripsi.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

2.1. Vigenere Cipher

Algoritma kriptografi tradisional yang berasal dari abad ke-16 atau kira-kira tahun 1986 adalah sandi Vigenere. Blaise de Vigenere, seorang diplomat dan ahli kriptografi Perancis, menerbitkan rumus kriptografi ini; Namun rumusnya sudah diubah di dalam buku. Giovan Batista Belaso menulis buku pada tahun 1553 berjudul La Cifra del Sig. Giovan Batista Belaso [8]. Sebuah teknik yang disebut Vigenere Chiper menggunakan rangkaian sandi Caesar berdasarkan huruf dalam kata kunci untuk mengenkripsi teks alfabet [9]. Kriptografi tradisional menggunakan metode substitusi gabungan untuk alfabet, yang merupakan cara kerja Vigenere. Untuk mengurangi fragmentasi ciphertext, kunci Vigenere akan diiterasi hingga mencapai panjang plaintext. Namun bila menggunakan cipher Vigenere, hambatan ciphertext dan algoritma dapat diselesaikan dengan menggunakan metode analisis frekuensi [10]. Karena mudah dipahami dan diterapkan, metode enkripsi semacam ini cukup dikenal. Dimungkinkan untuk menggunakan substitusi angka hingga vigènere persegi untuk membuat teks tersandi. Metode penggantian vigènere menggunakan angka dan cara kerjanya mirip dengan kode geser dengan mengganti angka dengan huruf.

Rumus Enkripsi vigenere cipher :
$Ci = (Pi + Ki) \bmod 26$ (1)
Atau
Ci = (Pi + Ki) apabila penjumlahan Pi dan Ki lebih dari 26
Rumus Dekripsi vigenere cipher :
$Pi = (Ci - Ki) \bmod 26$ (2)
Atau
Pi = (Ci - Ki) + 26 apabila hasil pengurangan Ci dan Ki minus

Dimana :
Pi = Plainteks
Ci = Ciphertext
Ki = Key

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 1. Contoh Tabel Substitusi Algoritma Kriptografi Vigenere Cipher

Plainteks : PLAINTEXT
Cipher : CIPHER

Plain	15	11	0	8	13	19	4	23	19
Kunci	2	8	15	7	4	17	2	8	15
Hasil	17	19	15	15	17	10	6	5	8
Ciphertext	R	T	P	P	R	K	G	F	I

Gambar 2. Contoh Tabel Kriptografi dengan Algoritma Vigenere Cipher

Dengan menggunakan pendekatan penggantian angka dengan huruf di atas, ditemukan bahwa teks kunci (CIPHER) memiliki kode angka 2, 8, 15, 7, 4, 17, sedangkan teks asli (PLAINTEXT) memiliki kode angka 2 , 11, 0, 8, 13, 19, 4, 23, 19. Nomor kode ciphertext dihasilkan setelah komputasi (17, 19, 15, 17, 10, 6, 5, 8). Surat-surat tersebut menjadi RTPPRKGFI bila dikembalikan ke urutan semula. Tabula recta, juga dikenal sebagai kotak vigènere, adalah cara berbeda untuk melakukan prosedur enkripsi metode sandi vigènere.

2.2. Steganografi

Steganografi adalah metode untuk menyembunyikan informasi sensitif dengan membuatnya tampak seperti data biasa-biasa saja. Saat ini, steganografi biasanya mengacu pada proses menyembunyikan data atau arsip dalam media gambar digital, audio, atau video [11]. Selain itu Steganografi merupakan ilmu dan seni menyembunyikan komunikasi agar keberadaannya tidak dapat dikenali oleh indera manusia [12] Karena steganografi dan kriptologi digunakan untuk menyembunyikan informasi sensitif, keduanya terkadang keliru satu sama lain, Karena steganografi dan kriptologi digunakan untuk menyembunyikan informasi sensitif, keduanya terkadang keliru satu sama lain. Perbedaan antara keduanya adalah Steganografi melibatkan penyembunyian informasi sekaligus membuatnya seolah-olah tidak ada yang disembunyikan sama sekali sekali [13].

Pada penelitian kali ini menggunakan Steganografi Least Significant Bit (LSB) yaitu teknik yang digunakan untuk menyembunyikan pesan tersembunyi di media digital, seperti foto, musik, atau video, tanpa membahayakan keselamatan orang yang memeriksa konten tersebut. Bit rahasia pesan disimpan menggunakan teknik ini dengan menggunakan Least Significant Bit (LSB) dari suatu piksel atau sampel data di media. Menurut [11] Metode Least Significant Bit (LSB) merupakan metode steganografi yang bekerja menyisipkan pesan dengan mengganti bit terendah dalam sebuah byte media pembawa pesan. Dalam sebuah byte terdapat susunan bit, yang di dalamnya terdapat bit yang paling berarti (Most Significant Bit) dan bit yang paling kurang berarti (LSB).

Cara kerja Steganografi LSB pada gambar adalah sebagai berikut:

P-ISSN : 2089-3353
E-ISSN : 2808-9162

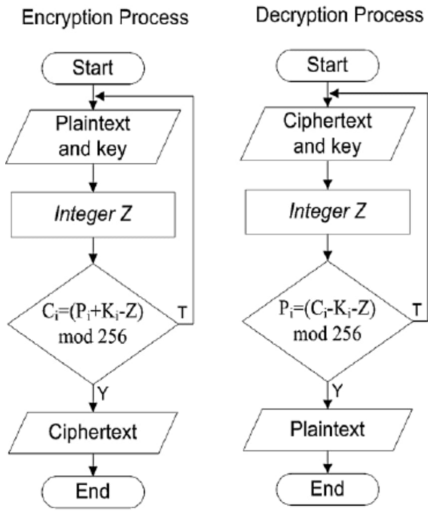
1. Pilih gambar cover: Gambar ini akan menjadi tempat menyimpan pesan rahasia. Gambar ini biasanya memiliki banyak piksel yang memberikan ruang untuk menyisipkan pesan tanpa mengganggu kualitas visual secara signifikan.
2. Ubah pesan rahasia menjadi bit-bit: Pesan rahasia yang ingin disisipkan harus diubah menjadi serangkaian bit. Misalnya, jika pesan terdiri dari teks, setiap karakter dapat diubah menjadi kode ASCII, dan kode ASCII tersebut kemudian diubah menjadi representasi biner.
3. Sisipkan bit pesan rahasia: Untuk setiap piksel dalam gambar cover, ambil bit paling tidak signifikan dari komponen warna (misalnya, red, green, atau blue) dan gantikan bit tersebut dengan bit pesan rahasia. Dengan menggunakan LSB, perubahan pada piksel tidak akan terlihat oleh mata manusia, karena perubahan tersebut sangat kecil dan hampir tidak berpengaruh pada nilai warna piksel.
4. Tandai akhir pesan: Agar proses dekripsi dapat dilakukan nanti, diperlukan tanda akhir pesan untuk menandai bahwa semua bit pesan telah disisipkan. Ini bisa berupa tanda khusus atau panjang pesan yang disisipkan sebelumnya.
5. Simpan gambar stego: Setelah semua bit pesan rahasia telah disisipkan ke dalam gambar cover, hasilnya adalah gambar stego, yaitu gambar yang menyimpan pesan rahasia.

2.3. Citra

Citra atau Gambar, dalam istilah teknis, adalah gambar bidang dua dimensi (dwimatra). Jika dilihat dari satu sisi Dari sudut pandang matematis, bayangan pada bidang matriks ganda merupakan fungsi kontinu (lanjutan) dari intensitas cahaya. Item disinari oleh sumber cahaya, dan item tersebut memantulkan kembali sebagian cahayanya. Mata manusia dan kamera adalah dua contoh peralatan yang digunakan dalam optik yang merekam pantulan cahaya ini. Pemindai (scanner), dan sebagainya, untuk merekam gambar suatu benda yang disebut gambar [14]. Menurut jurnal dari [15] Gambar digital terdiri dari sekelompok piksel yang dapat diproses oleh komputer. Gambar sering kali mengalami degradasi, meskipun mengandung banyak informasi. Contoh degradasi ini antara lain cacat atau noise, warna yang terlalu kontras, kurang tajam, buram, dan lain sebagainya. Tentu saja, ketika jumlah informasi yang disampaikan oleh gambar berkurang, jenis gambar ini semakin sulit untuk dipahami. Gambar tersebut harus diubah menjadi versi dengan kualitas lebih tinggi agar gambar yang terganggu dapat dengan mudah dipahami baik oleh manusia maupun mesin. Pemrosesan gambar adalah bidang penelitian yang terlibat dalam hal ini. Gambar digital terdiri dari kumpulan '0' dan '1' di setiap piksel. Berikut beberapa format gambar digital: bmp, png, gif, dan jpeg.

3. Hasil dan Pembahasan

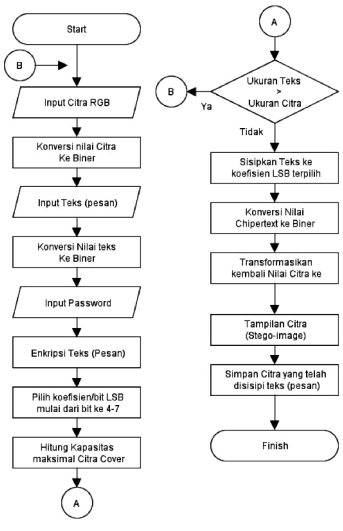
3.1 flowchart enkripsi dan dekripsi vigenere cipher



Gambar 3. Flowchart Enkripsi dan Dekripsi Vigenere Cipher

Proses Enkripsi dan Dekripsi dimana: Pi = plaintext Ci = ciphertext Z = Nilai Integer Positif dan K = Kunci Proses pengubahan dokumen (plaintext) menjadi ciphertext dijelaskan dengan penggunaan mod 256 = nomor kode ASCII berdasarkan alur enkripsi pada Gambar . Proses ini dimulai dengan input plaintext dan kunci, menentukan nilai Z yang diberikan pada subkunci, kemudian menerapkan rumus Ci= (Pi+Ki-Z) mod 256, dimana hasil yang diperoleh dari penerapan rumus ini adalah ciphertext. Teks sandi, kunci awal, dan nilai Z dimasukkan untuk memulai proses dekripsi. Ciphertext tersebut kemudian diubah kembali ke bentuk aslinya menggunakan rumus dekripsi Pi= (Ci-Ki-Z) mod 256.

3.2 Flowchart Proses Penyisipan Teks kedalam Gambar



Gambar 4. Flowchart Proses Penyisipan Teks kedalam Gambar

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Pada flowchart penjelasan alur proses penyisipan teks ke dalam gambar, gambar telah dipilih oleh peneliti, nilai piksel gambar (Cover-Image) akan selalu diubah ke dalam bentuk biner (8 bit). Kemudian akan memasukkan atau memilih file teks (plaintext) yang akan disisipkan dan akan dilanjutkan dengan menghasilkan pseudo-number Vigenere Cipher. Maka proses penyematan selesai, sistem akan menghitung kapasitas gambar sampul, kemudian sistem menolak melanjutkan dan akan meminta pengurangan jumlah pesan. Jika cover-image dapat menampung maka sistem akan terus memproses konversi nilai bilangan Binary Chiper-teks (Stego-image) menjadi nilai bilangan desimal dan konversi nilai desimal menjadi nilai piksel akan dikonversi dan pada akhirnya akan menyimpan (menyimpan) file Gambar Sampul. gambar yang telah disisipkan dengan pesan (Chiper-text).

3.3 Flowchart Proses Pengekstrakan Teks pada Gambar

Gambar 5. Flowchart Proses Pengekstrakan Teks pada Gambar

Untuk mengekstrak teks dari gambar, pertama-tama akan dipilih stego-image dengan nilai pikselnya. Selanjutnya akan diubah menjadi bilangan biner 8-bit, dan prosesnya akan selalu diakhiri dengan pembuatan bilangan semu Vigenere Cipher. Pesan (teks biasa) kemudian akan ditampilkan ketika nilai biner diubah dari biner ke desimal menggunakan nilai yang terdapat pada bit terakhir (LSB) setiap piksel.

3.4 Perhitungan manual enkripsi dan dekripsi vigenere cipher

Proses perhitungan enkripsi dengan memakai rumus Ci = (Pi + Ki) mod 26 Atau Ci = (Pi + Ki) apabila penjumlahan Pi dan Ki lebih dari 26.

Tabel 1. Perhitungan enkripsi

Plaintexs	R	A	P	A	T
Key	T	R	A	P	A
Nilai plaintext	17	0	15	0	19
Nilai key	19	17	0	15	0
Hasil	36	17	15	15	19
Ciphertext	K	R	P	P	T

Proses perhitungan dekripsi Pi = (Ci - Ki) mod 26 Atau Pi = (Ci - Ki) + 26 apabila hasil pengurangan Ci dan Ki minus.

Tabel 2. Perhitungan dekripsi

Ciphertext	K	R	P	P	T
Key	T	R	A	P	A
Nilai ciphertext	10	17	15	15	19
Nilai key	19	17	0	15	0
Hasil	17	26	41	26	45
Plainteks	R	A	P	A	T

3.5 Tampilan Aplikasi

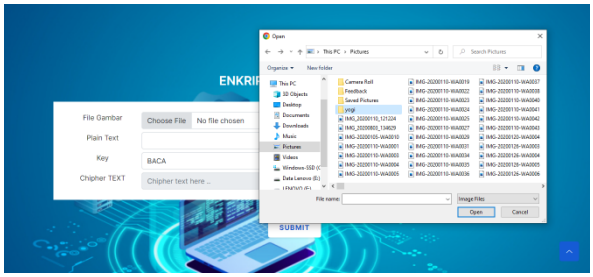
Gambar 6. Tampilan halaman utama

Tampilan diatas merupakan tampilan utama dari sistem aplikasi, pada tampilan ini pengguna dapat memilih ingin melakukan enkripsi atau dekripsi.

P-ISSN : 2089-3353
E-ISSN : 2808-9162

Gambar 7. Tampilan halaman enkripsi

Tampilan diatas merupakan tampilan enkripsi, dimana pengguna terlebih dahulu menginput file citra yang ingin disisipkan pesan kemudian membuat sebuah plainteks atau data asli yang ingin disampaikan, selanjutnya memasukkan sebuah key atau kunci sehingga nanti akan menhasilkan ciphertext dari data asli tersebut.

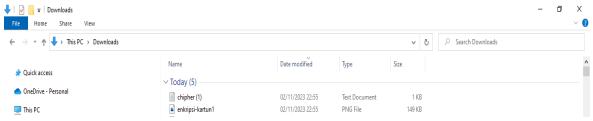


Gambar 8.Tampilan pilih file citra

Tampilan diatas merupakan tampilan pilih file citra yang akan kita sisipkan pesan, setelah kita klik kita akan diarahkan pada folder perangkat yang dipakai.

Gambar 9. Tampilan hasil enkripsi

Tampilan diatas merupakan tampilan hasil enkripsi pesan yang telah disisipkan pada file citra, untuk menghasilkan sebuah ciphertext dan penyisipan pesan pada file citra pengguna harus memasukkan pesan yang ingin disampaikan dan sebuah key atau kunci pada tampilan sistem, setelah berhasil dilakukan pengguna harus melakukan "submit" dimana file citra dan key akan otomatis ter-download ke perangkat pennguna.

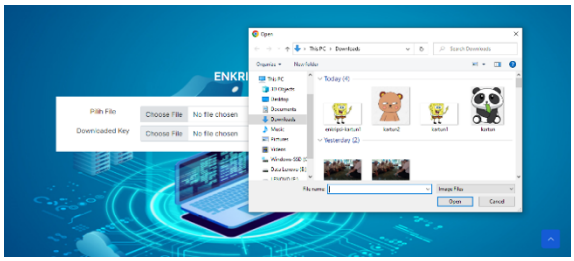


Gambar 10. *Tampilan download hasil file citra yang sudah di enkripsi*

Tampilan diatas merupakan tampilan file citra dan key yang sudah otomatis ter-download keperangkat pengguna.

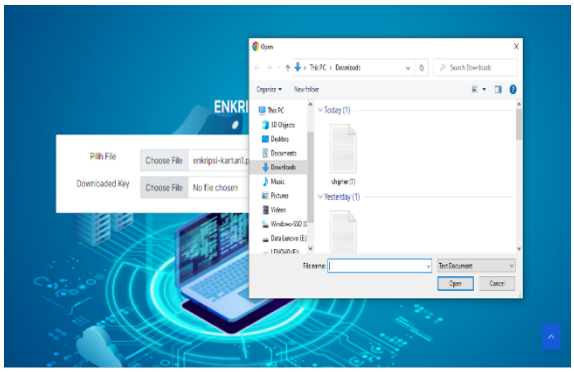
Gambar 11. *Tampilan Dekripsi*

Tampilan diatas merupakan tampilan pesan yang ingin di dekripsi, dimana pengguna akan menginput sebuah file citra dan sebuah key sehingga nantinya akan menampilkan pesan tersembunyi yang ada pada file citra tersebut.



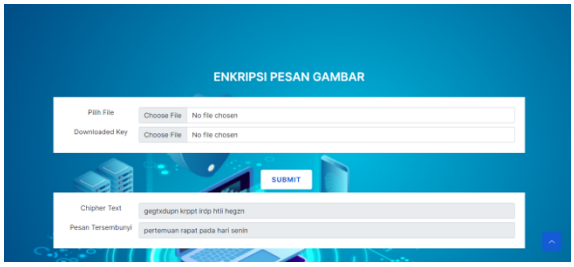
Gambar 12. Tampilan pilih file citra yang ingin di dekripsi

Tampilan diatas merupakan tampilan pilih file citra yang akan di dekripsi, sistem akan mengarahkan pengguna pada sebuah folder pada perangkat.



Gambar 13. Tampilan pilih Key

Tampilan diatas merupakan tampilan pilih key yang akan di dekripsi, sistem akan mengarahkan pengguna pada sebuah folder pada perangkat.



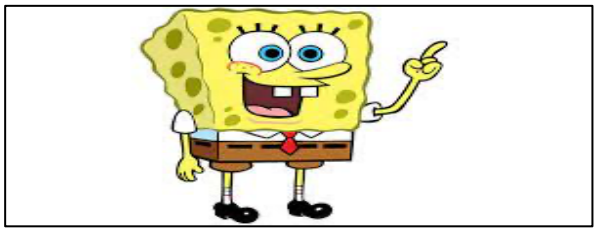
gambar 14. Tampilan hasil teks yang sudah di dekripsi

P-ISSN : 2089-3353
E-ISSN : 2808-9162

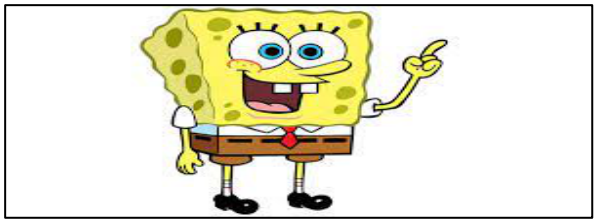
Tampilan diatas merupakan tampilan file citra yang sudah didekripsi, pada tampilan tersebut pengguna harus benar benar memasukkan file citra dan key yang sesuai sehingga pesan tersembunyi pada file dapat diketahui.

Gambar 15. Tampilan halaman yang tidak ada pesan tersembunyi

Tampilan diatas merupakan tampilan apabila pengguna menginput sebuah file citra dan key yang tidak sesuai dengan enkripsi pesan yang sudah dibuat, sehingga sistem akan menampilkan "Tidak ada Data".



Gambar 16. *Tampilan file asli*



Gambar 17. *Tampilan file yang sudah di sisipkan pesan teks*

Tampilan diatas merupakan tampilan visual file citra yang belum mengalami penyisipan dan yang sudah mengalami penyisipan, pada tampilan tersebut visual dari citra yang sudah disisipkan pesan tidak terlihat mengalami perubahan dan sama persis dengan file aslinya hanya saja ukuran file citra menjadi lebih besar.

Tabel 3. Perbandingan ukuran file asli dan file yang sudah di enkripsi

No	kapasitas gambar sebelum encoding	kapasitas gambar setelah encoding
1	62,2 KB	848 KB
2	112 KB	799 KB
3	63,1 KB	803 KB
4	98,2 KB	801 KB
5	63,3 KB	803 KB
6	94,5 KB	1.151 KB
7	110 KB	803 KB
8	237 KB	2.935 KB
9	82,4 KB	801 KB
10	64,4 KB	677 KB
11	60,6 KB	788 KB
12	96,6 KB	902 KB
13	82,5 KB	741 KB
14	173 KB	797 KB
15	64,6 KB	803 KB

Pada tabel diatas merupakan perbandingan file asli dan file yang sudah disisipkan pesan dalam bentuk ukuran kilobyte (KB), penulis mengambil sampel dalam 15 file citra yang akan disisipkan pesan, adapun pesan yang disisipkan terdiri dari 27-30 huruf, dari hasil pengujian ukuran file asli dan file yang telah disisipkan mengalami penaikan ukuran dari file aslinya sekitar 10 kali lebih besar dari file aslinya.

4. Kesimpulan

Berdasarkan penerapan keamanan data menggunakan kriptografi *vigenere cipher* dan steganografi LSB, maka dapat diambil kesimpulan bahwa metode *vigenere cipher* dan steganografi dapat dikombinasikan dalam pengamanan pesan rahasia yang disisipkan pada sebuah citra yang diawali dengan pengacakan sebuah pesan asli menjadi ciphertext dengan menggunakan algoritma *vigenere cipher* dan selanjutnya pesan disisipkan pada sebuah citra dengan menggunakan steganografi LSB sehingga pesan yang disampaikan bersifat acak dan dapat dikembalikan menjadi pesan awal tanpa adanya perubahan pada pesan. Berdasarkan hasil pengujian ukuran file asli dan file yang telah disisipkan mengalami penaikan ukuran dari file aslinya tetapi tampilan visual citra asli dan tampilan visual citra yang sudah dilakukan penyisipan tidak mengalami perubahan. Saran dari peneliti yaitu, dalam pengembangan sistem selanjutnya, sistem ini dapat

P-ISSN : 2089-3353
E-ISSN : 2808-9162

dikembangkan dalam bentuk platform lain seperti aplikasi berbasis *android* dan keterbaruan dalam metode yang lebih modern.

Daftar Rujukan

[1] Fatma Yulia, Harun Mukhtar and Muhammad Taufik "Jurnal fasilkom," vol. 7, pp. 255–259, 2018.

[2] 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.

[3] Arianto Bagus, Harso Kurniadi and iin Kurniasari "Jurnal Fasilkom," vol. 13, no. 2, pp. 259–268, 2023.

[4] A. Saraswat, C. Khatri, Sudhakar, P. Thakral, and P. Biswas, "An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication," *Procedia Comput. Sci.*, vol. 92, pp. 355–360, 2016, doi: 10.1016/j.procs.2016.07.390.

[5] Z. S. Younus and M. K. Hussain, "Image steganography using exploiting modification direction for compressed encrypted data," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2951–2963, 2022, doi: 10.1016/j.jksuci.2019.04.008.

[6] A. R. H. Martawireja, R. Ridwan, A. P. Hafidzin, and M. Taufik, "Proteksi Keamanan Data pada Quick Response (QR) Code," *J. Teknol. dan Rekayasa Manufaktur*, vol. 3, no. 2, pp. 99–110, 2021, doi: 10.48182/jtrm.v3i2.58.

[7] A. Rahman *et al.*, "ALGORITMA VIGENERE CIPHER DAN RIVEST SHAMIR ADLEMAN (RSA) BERBASIS DESKTOP Dan Rivest Shamir Adleman (Rsa) Berbasis Desktop Dan Rivest Shamir Adleman (Rsa) Berbasis Desktop," vol. 1, no. 2, pp. 801–806.

[8] J. Karman and A. Nurhasan, "Perancangan Sistem Keamanan Data Inventory Barang Di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Cipher," *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 29–36, 2019, doi: 10.32767/jti.v11i1.451.

[9] Y. Wiharto and A. Irawan, "Sistem Kehadiran Menggunakan Quick Respone Code Dengan Enkripsi Algorithm Message Digest 5 dan Vigenere Cipher Pada SpeedCom IT Consulting," *J. Sist. Komput. dan Kecerdasan Buatan*, vol. II, no. 1, p. 42, 2018.

[10] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.

[11] M. Minarni and R. Redha, "Implementasi Least Significant Bit (Lsb) Dan Algoritma Vigenere Cipher Pada Audio Steganografi," *J. Sains dan Teknol. J. Keilmuan dan Apl. Teknol. Ind.*, vol. 20, no. 2, p. 168, 2020, doi: 10.36275/stsp.v20i2.268.

[12] R. N. Pahlawan, R. Y. Dillak, and J. Sine, "1 , 2 , 3," vol. 5, no. 1, pp. 5–9, 2019.

[13] Y. Anshori, A. Y. E. Dodu, and M. Purwaningsih, "Aplikasi Steganografi pada Media Citra Digital Menggunakan Metode Least Significant Bit (LSB)," *SATIN - Sains dan Teknol. Inf.*, vol. 5, no. 1, pp. 1–10, 2019, doi: 10.33372/stn.v5i1.435.

[14] L. Hakim, "IMPLEMENTASI STEGANOGRAFI PADA CITRA DIGITAL DAN KRIPTOGRAFI ALGORITMA HILL CHIPPER UNTUK PENGAMANAN INFORMASI BERUPA TEXT," vol. V, no. 1, 2018.

[15] J. T. Informatika and S. A. Bangsa, "Penyembunyian Pesan dalam Gambar dengan Teknik," vol. IV, no. 1, pp. 51–56, 2018.