

IMPLEMENTASI STEGANOGRAFI DENGAN MENGGUNAKAN ALGORITMA *HILL CIPHER* UNTUK PENGAMANAN PENGIRIMAN FILE VIA *E-MAIL*

¹ Elva Santa, ²Zakaria Situmorang,
STMIK Kristen Neumann Indonesia
Jl. Letjend Jamin Ginting KM. 10,5 Medan
Penulis elvasantabangun12@gmail.com

Program Studi Teknik Informatika

ABSTRAK

Steganografi adalah ilmu dan seni yang mempelajari cara penyembunyian informasi pada suatu media sedemikian rupa sehingga keberadaannya tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Pengguna pertama (Pengirim pesan/teks) dapat mengirim media yang telah disisip informasi rahasia tersebut melalui jalur komunikasi publik, hingga dapat diterima oleh pengguna kedua (Penerima Pesan/Teks). Penerima pesan dapat mengekstraksi informasi rahasia yang ada didalamnya. Pada skripsi ini akan membahas tentang bagaimana membuat penyisipan steganografi dan bagaimana proses penyisipannya pada image (Citra) serta bagaimana menerapkan algoritma hill cipher ke dalam aplikasi steganografi yang di buat..

Kata Kunci : Steganografi, Citra Digital, Hill Cipher.

PENDAHULUAN

Keamanan dan kerahasiaan file merupakan salah satu aspek yang sangat penting dalam sistem informasi saat ini. Disebabkan pesatnya perkembangan ilmu pengetahuan dan teknologi yang memungkinkan munculnya teknik-teknik baru yang disalah gunakan oleh pihak-pihak yang mengancam keamanan dari sistem informasi tersebut. Jatuhnya informasi ke tangan yang salah dapat menimbulkan kerugian bagi pemilik informasi.

Dalam era kemajuan teknologi saat ini keamanan informasi merupakan salah satu hal penting terutama dalam masalah pengiriman informasi dan penerimaan

informasi, karena dengan perkembangan teknologi informasi yang semakin maju, semakin berkembang pula berbagai teknik kejahatan berupa perusakan maupun pencurian informasi oleh pihak yang tidak memiliki hak akses atas informasi tersebut. Ketika ingin menyampaikan atau bertukar informasi dengan orang lain maka tentu saja informasi yang dikirim telah sampai ke pihak yang dituju dengan aman. Pengertian aman disini sangat luas. Aman bisa berarti bahwa selama pengiriman informasi tentu diharapkan pesan tersebut tidak dapat dibaca oleh orang yang tidak berhak. Pengamanan terhadap informasi juga perlu ditingkatkan untuk menjamin keamanan informasi. Dalam pengamanan data ada beberapa

cara yang dapat dilakukan yakni kriptografi, steganografi dan pengiriman via *email*. Dalam hal ini akan difokuskan pada kriptografi dan steganografi.

Rumusan Masalah

Dari latar belakang yang telah dijelaskan diatas, maka rumusan masalah adalah :

1. Bagaimana menerapkan metode hill cipher pada file teks.
2. Implementasi metode hill cipher untuk keamanan file teks dengan steganografi.

Batasan Masalah

Sesuai dengan rumusan masalah yang telah dikemukakan maka batasan masalah adalah :

1. Pengamanan file pesan melalui steganografi pada teks dengan algoritma hill cipher
2. Ukuran citra maksimum 5 MB
3. Teks yang digunakan berupa karakter alphabet
4. Citra yang digunakan berformat JPG
5. File Hasil enkripsi dikirim via *e-mail*.

Metode Penelitian

Adapun teknik dalam pengumpulan data yang penulis gunakan untuk kebutuhan analisis adalah sebagai berikut :

1. Studi kepustakaan
 Dengan mengumpulkan data yang berkaitan dengan topik yang dibahas yang dilakukan dengan cara membaca buku-buku yang berkaitan dengan pengimplementasian hill cipher untuk keamanan pesan melalui citra pada email.
2. Studi Literatur
 Penulisan ini dimulai dengan studi kepustakaan dengan mengumpulkan bahan-bahan referensi baik dari buku-buku, jurnal, dan internet tentang metode hill cipher melalui citra dan konsep matematis yang mendasari serta program untuk membuat aplikasinya,

serta beberapa referensi lain untuk mencapai tujuan dari tugas akhir.

Definisi Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim, dapat tersampaikan dengan aman pada penerima dengan cara menyamarkan dalam bentuk sandi yang tidak mempunyai makna.

Analisis Dan Perancangan Sistem

Analisis citra bertujuan mengidentifikasi parameter-parameter yang diasosiasikan dengan siri (*feature*) dari objek dalam citra. Untuk selanjutnya parameter digunakan dalam menginterpretasi, analisis citra pada dasarnya terdiri dari tiga tahapan yaitu deteksi (pengamatan adanya suatu objek), segmentasi (bagian dari proses pengolahan citra), dan analisis (keterangan lebih lanjut dari objek).

Data Flow Diagram (DFD)

Data flow diagram adalah salah satu tool yang paling penting bagi seorang analisis sistem untuk membuat gambaran sistem secara logika. Pendekatan analisis terstruktur diperkenalkan oleh oleh DeMarco (1978) dan Gane Sarson (1979) melalui buku metodeologi struktur analisis dan desain sistem informasi.

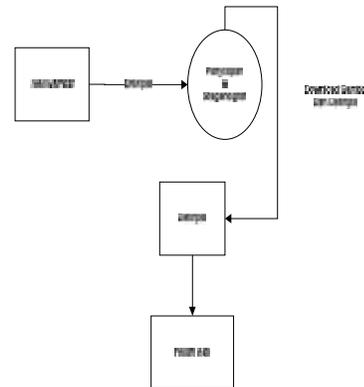
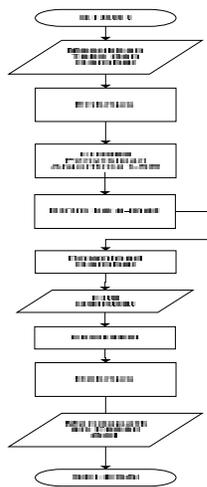


Diagram Konteks

Dari gambar di atas dapat dijelaskan bahwa pengirim terlebih dahulu memasukan gambar dan teks yang akan di enkripsi sehingga hasil chipertekstnya akan muncul setelah itu penyisipan teks ke citra dengan LSB akan dilakukan. Setelah itu proses stego image akan dijalankan jika prosesnya sudah selesai kirim citra yang sudah dienkripsi menggunakan email hasil dekripsi akan muncul.



Flowchart

Dari gambar Flowchart di atas adalah proses berjalannya pengiriman file yang akan dilakukan menggunakan algoritma hill cipher melalui proses ini kita akan mengetahui kemana proses pengiriman file berlangsung. Tahap pertama lakukan start setelah itu masukkan teks dan gambar yang akan di enkripsi setelah gambar dan teks telah dimasukkan maka lakukan tahap enkripsi setelah di enkripsi lakukan proses penyisipan teks yang akan dikirim setelah hasil penyisipan muncul.

Proses Enkripsi Dan Penyisipan

Misalkan terdapat *plaintext* P = STMIKNEUMANN, dan kunci K = $\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$

Sebelum membagi teks menjadi deretan blok-blok, pesan terlebih dahulu dikonversi menjadi angka-angka unik antara 0 hingga 25, sesuai table 3.1:

Tabel 3.1 Konversi Alfabet ke Angka

A	B	C	D	E	F	G	H
0	1	2	3	4	5	6	7
I	J	K	L	M	N	O	P
8	9	10	11	12	13	14	15
Q	R	S	T	U	V	W	X
16	17	18	19	20	21	22	23
Y	Z						
24	25						

- a. Bagi *plaintext* P menjadi matriks 2 x 1 dan konversi menjadi angka sesuai Tabel 3.1. dihasilkan sebagai berikut :

$$\begin{pmatrix} S \\ T \end{pmatrix} = \begin{pmatrix} 18 \\ 19 \end{pmatrix}$$

$$\begin{pmatrix} M \\ I \end{pmatrix} = \begin{pmatrix} 12 \\ 8 \end{pmatrix}$$

$$\begin{pmatrix} K \\ N \end{pmatrix} = \begin{pmatrix} 10 \\ 13 \end{pmatrix}$$

$$\begin{pmatrix} E \\ U \end{pmatrix} = \begin{pmatrix} 4 \\ 20 \end{pmatrix}$$

$$\begin{pmatrix} M \\ A \end{pmatrix} = \begin{pmatrix} 12 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} N \\ N \end{pmatrix} = \begin{pmatrix} 13 \\ 13 \end{pmatrix}$$

- b. Selanjutnya kalikan setiap angka dengan matriks kunci

$$K = \begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 18 \\ 19 \end{pmatrix} = \begin{pmatrix} 36 + 19 \\ 54 + 76 \end{pmatrix} = \begin{pmatrix} 55 \\ 130 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 12 \\ 8 \end{pmatrix} = \begin{pmatrix} 24 + 8 \\ 36 + 32 \end{pmatrix} = \begin{pmatrix} 32 \\ 68 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 10 \\ 13 \end{pmatrix} = \begin{pmatrix} 20 + 13 \\ 30 + 52 \end{pmatrix} = \begin{pmatrix} 33 \\ 82 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 4 \\ 20 \end{pmatrix} = \begin{pmatrix} 8 + 20 \\ 12 + 80 \end{pmatrix} = \begin{pmatrix} 28 \\ 92 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 24 + 0 \\ 36 + 0 \end{pmatrix} = \begin{pmatrix} 24 \\ 36 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 13 \\ 13 \end{pmatrix} = \begin{pmatrix} 26 + 13 \\ 39 + 52 \end{pmatrix} = \begin{pmatrix} 39 \\ 91 \end{pmatrix}$$

- c. Melakukan operasi Mod 26 kepada setiap matriks angka tersebut agar dapat dikonversi menggunakan Tabel 3.1 maka dihasilkan sebagai berikut :

$$\begin{pmatrix} 55 \\ 130 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 32 \\ 68 \end{pmatrix} \bmod 26 = \begin{pmatrix} 6 \\ 16 \end{pmatrix}$$

$$\begin{pmatrix} 33 \\ 82 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 4 \end{pmatrix}$$

$$\begin{pmatrix} 28 \\ 92 \end{pmatrix} \bmod 26 = \begin{pmatrix} 2 \\ 14 \end{pmatrix}$$

$$\begin{pmatrix} 24 \\ 36 \end{pmatrix} \bmod 26 = \begin{pmatrix} 24 \\ 10 \end{pmatrix}$$

$$\begin{pmatrix} 39 \\ 91 \end{pmatrix} \bmod 26 = \begin{pmatrix} 13 \\ 13 \end{pmatrix}$$

HASIL DAN PEMBAHASAN

Form Menu Utama

Pada form gambar 4.1 menu utama dalam program ini terdapat menu-menu pilihan yang mempermudah pemakai untuk menggunakannya. Dapat terlihat pada tabel 4.1 adapun tampilan form menu utama tersebut adalah sebagai berikut. Menu yang pertama adalah menu steganografi yang merupakan menu yang masuk untuk tahap dimana proses jalannya program di menu berikutnya seangkan yang ke dua adalah menu exit yang berarti menu untuk keluar dari menu utama.

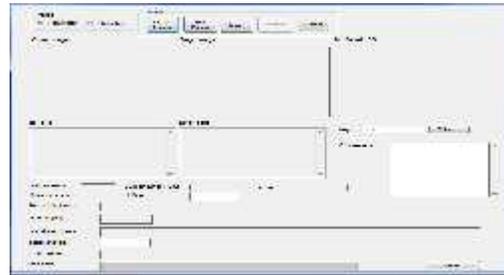


Gambar 1 Form Menu Utama

Tampilan Form Hasil Program

Pada form gambar 4.2 terlihat bahwa Hasil program ini akan memproses gambar dan teks yang akan disisip dengan cara klik open image setelah itu pilih gambar yang akan disisip, setelah itu klik file pesan pilih pesan yang akan disisip

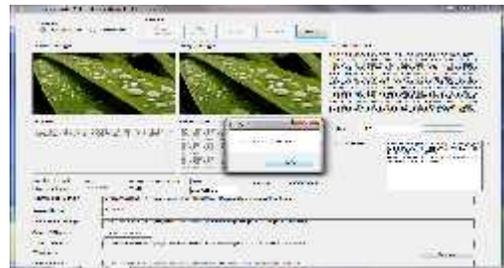
maka akan muncul tombol di enkripsi lalu klik tombol enkripsi setelah di enkripsi akan dilakukan proses penyisipan dengan cara klik sisip maka proses penyisipan akan berjalan.



Gambar 2 Tampilan Form Hasil Program

Tampilan Hasil Penyisipan Citra

Terlihat pada gambar 4.3 dibawah akan melakukan proses penyisipan hasil teks yang disisip melalui gambar setelah pemrosesan penyisipan maka gambar yang disisip akan muncul beserta teks yang disisip serta jumlah huruf, dimensi cover, jumlah biner huruf, lama waktu proses penyisipan, ukuran gambar akan muncul setelah terjadi penyisipan. Tahap pertama pilih gambar dan teks yang akan disisip.



Gambar 3 Tampilan Hasil Penyisipan Citra

Kesimpulan

Berdasarkan hasil penelitian yang dilakukan oleh penulis maka dapat disimpulkan bahwa

1. Aplikasi ini dapat digunakan untuk keamanan pesan atau data yang akan dikirim dan akan lebih aman dan mudah.
2. Dengan aplikasi steganografi ini relatif lebih aman karena di enkripsi terlebih dahulu sehingga di lakukan penyisipan teks lalu di dekripsi.

Daftar Pustaka

Darma Putra , 2010 **“Pengolahan Citra Digital”**, Penerbit Andi, Yogyakarta, Edisi I,
 Munir, Ariyus Dony, **“Keamanan Multimedia”**, Penerbit C.V ANDI OFFEST, Yogyakarta 55281

Munir, Rinaldi, , 2006 **“Diktat Kuliah IF5054 Kriptografi”**, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika.

Ariyus Dony, 2008 **“Pengantar Ilmu Kriptografi”** Penerbit Andi Yogyakarta

Rinaldi, 2006 **“Steganografi”** Indonesia, Bandung: PD STENOS,

Menurut Jogiyanto H.M. 2001 : 196.” **perancangan sistem”** di akses pada tanggal 10 April 2015

Thearon Willis, Bryan Newsome,2010.”**Begining Microsoft Visual Basic 2010”**, Wiley Publishing, Bandung