STEGANOGRAFI DENGAN MENGGUNAKAN METODE LSB DAN ALGORITMA HILL CIPHER

Sherly Gina Supratman[*1]
[1]Program Studi Magister Ilmu Komputer, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan
Telp. 021-5853753
[*1]she.al4gna@gmail.com

Abstrak

Jaringan Komunikasi seperti Internet merupakan jaringan yang tidak aman untuk mentransmisi data, seperti teks, audio,video dan citra digital. Salah satu cara untuk pengamanan data dapat dilakukan dengan menggunakan proses kriptografi dan steganografi. Penggunaan ini dengan tujuan untuk merahasiakan pesan yang dikirim dan sekaligus menghindarkan pesan tersebut dari kecurigaan pihak lain yang tidak berkepentingan.

Pesan yang digunakan dalam makalah ini adalah berupa text dengan menyisipkannya pada gambar. Pada proses kriptografi, pesan yang berupa text akan dienkrip dengan algoritma Hill Chiper, dan kemudian pesan yang telah dienkrip akan dilakukan proses steganografi pada citra digital 8 bit dengan skala 0 – 255, dengan metode Least Significant Bit (LSB).

***Kata kunci**: Kriptografi, Hill Chiper, Steganografi, Least Significant Bit*

Abstract

Communication Networks such as the Internet are unsafe networks for transmitting data, such as text, audio, video and digital imagery. One way to secure data can be done by using cryptography and steganography process. This use is for the purpose of concealing messages being transmitted and avoiding such messages from the suspicion by others who are not interested.

The message used in this paper is text by inserting it in the image. In the cryptographic process, text messages will be encrypted with the Hill Chiper algorithm, and then the encrypted message will be steganographed on 8-bit digital images on a scale of 0-255, using the Least Significant Bit (LSB) method.

***Keywords**: Cryptography, Hill Chiper, Steganography, Least Significant Bit*

1. PENDAHULUAN

Keamanan merupakan masalah dalam transmisi data pada jaringan komputer. Untuk mengamankan data digunakan proses Kriptografi dan Steganografi ataupun bisa menggunakan atau mengkombinasikan keduanya. Dalam makalah ini akan digunakan kombinasi keduanya.

2. METODE PENELITIAN

a. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti kerahasiaan data dan autentifikasi data (Menezes, Oorshot and Vanstone 1996). Selain itu kriptografi dapat diartikan sebagai seni atau ilmu dalam menyembunyikan data. Proses yang dilakukan untuk mengamankan sebuah pesan (plaintext) menjadi pesan yang tersembunyi (chipertext) disebut enkripsi. Sebaliknya untuk mengubah chipertext ke plaintext disebut dekripsi.

Algoritma kriptografi berdasarkan kunci yang dipakai, dapat dibedakan menjadi dua, yaitu kunci simetris dan kunci asimetris. Dalam makalah ini digunakan algoritma simetris yaitu Hill Chiper.

b. Algoritma Enkripsi Hill Cipher

Sebelum pesan disisipkan pada file Image, pesan harus dienkripsi terlebih dahulu baru kemudian disisipkan, enkripsi dilakukan dengan menggunakan algoritma Hill Cipher. Penggantian huruf pada pesan harus sama dengan panjang pesan yang akan diganti.

Proses enkripsi pada Hill Chiper dilakukan per blok plaintext. Ukuran blok tersebut sama dengan ukuran matriks kunci.

Berikut tahapan-tahapan dalam enkripsi Hill Chiper secara umum:

1) Sebelum membagi teks menjadi deretan blok-blok, plaintext terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25.
2) Buat matriks kunci berukuran m x m

$$K = \begin{pmatrix} k11 & k12 & ... & k1m \\ k21 & k22 & ... & k2m \\ ... & ... & ... & ... \\ kn1 & kn2 & ... & knm \end{pmatrix}$$

3) Lakukan proses enkripsi dengan rumus matematis berikut :
Secara matematis, proses enkripsi pada *Hill Cipher :*

$$C = K \,.\, P \bmod 26$$

C* = *Ciphertext
***K* = Kunci**
P* = *Plaintext

4) Konversikan kembali hasil enkripsi kedalam huruf sesuai tabel konversi

c. Algoritma Dekripsi Hill Cipher

Proses dekripsi pada Hill Chiper pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (invers) terlebih dahulu. Secara matematis, proses dekripsi pada Hill Chiper dapat diturunkan dari persamaan :

$$\mathbf{C = K \,.\, P}$$

$$\mathbf{K^{-1} \,.\, C = K^{-1} \,.\, K \,.\, P}$$

$$\mathbf{K^{-1} \,.\, C = I \,.\, P}$$

$$\mathbf{P = K^{-1} \,.\, C}$$

Menjadi persamaan proses dekripsi :

$$\mathbf{P = K^{-1} \,.\, C}$$

K-1 = [K | I]

$$K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$K^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$$

d. Steganografi

Steganografi merupakan teknik penyembunyian informasi dengan cara penyisipan pada suatu media. Kata *steganography* (steganografi) berasal dari bahasa Yunani yaitu *steganos* yang berarti menyembunyikan dan *graptos* artinya tulisan sehingga arti secara keseluruhan ialah tulisan yang disembunyikan (Stellars, 1996).

Selain itu dapat juga didefinisikan, Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Sedangkan Kriptografi menyamarkan arti dari suatu pesan, tetapi tidak menyembunyikan bahwa ada suatu pesan. Secara teori, semua file yang ada didalam komputer dapat digunakan sebagai media penampung pesan, seperti file citra berformat JPG, GIF, BMP, file audio berformat MP3, WAV, bahkan didalam sebuah video dengan format AVI, atau dalam format lainya seperti TXT, HTML, PDF.

e. *Least Significant Bit Insertion* (LSB)

Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.

3. HASIL DAN PEMBAHASAN

Proses penerapan algoritma pada transmisi data sebagai berikut:

a. Proses Enkripsi

1) Pesan yang akan disampaikan adalah **PASCABUDILUHUR**

2) Konversi huruf kedalam angka

Plaintext (P) = **PASCABUDILUHUR**

Lalu Plaintext diatas dikonversi sesuai tabel 1 menjadi :

P =

15 0 18 2 0 1 20 3 8 11 20 7 20 17

3) Plaintext tersebut akan dienkripsi dengan Hill Cipher, dengan kunci K yang merupakan matrix 2x2.
Kunci matriks yang digunakan adalah :

$$K = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix}$$

4) Proses enkripsi secara matematis :

$C = K \cdot P \bmod 26$

$$K = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix}$$

Karena matriks kunci k berukuran 2, maka plaintext dibagi menjadi blok yang masing-masing bloknya berukuran 2 karakter.

Blok 1 dari plaintext P adalah :

$$P_{1,2} = \begin{pmatrix} 15 \\ 0 \end{pmatrix}$$

$$C_{1,2} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \end{pmatrix} = \begin{pmatrix} 90 \\ 15 \end{pmatrix} \bmod 26 = \begin{pmatrix} 12 \\ \end{pmatrix}$$

Karakter yang berkorespondensi dengan 12 dan 15 adalah M dan P, maka P menjadi M dan A menjadi P.

Blok 2 dari plaintext P adalah :

$$P_{3,4} = \begin{pmatrix} 18 \\ 2 \end{pmatrix}$$

$$C_{3,4} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 18 \\ 2 \end{pmatrix} = \begin{pmatrix} 118 \\ 22 \end{pmatrix} \bmod 26 = \begin{pmatrix} 14 \\ 22 \end{pmatrix}$$

Karakter yang berkorespondensi dengan 14 dan 22 adalah O dan W, maka S menjadi C dan O menjadi W.

Blok 3 dari plaintext P adalah :

$$P_{5,6} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$C_{5,6} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$

Karakter yang berkorespondensi dengan 5 dan 2 adalah F dan C, maka A menjadi F dan B menjadi C.

Blok 4 dari plaintext P adalah :

$$P_{7,8} = \begin{pmatrix} 20 \\ 3 \end{pmatrix}$$

$$C_{7,8} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 3 \end{pmatrix} = \begin{pmatrix} 135 \\ \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

Karakter yang berkorespondensi dengan 5 dan 0 adalah F dan A, maka U menjadi F dan D menjadi A.

Blok 5 dari plaintext P adalah :

$$P_{9,10} = \begin{pmatrix} 8 \\ 11 \end{pmatrix}$$

$$C_{9,10} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 8 \\ 11 \end{pmatrix}$$

$$= \begin{pmatrix} 103 \\ 30 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 25 \\ 4 \end{pmatrix}$$

Karakter yang berkorespondensi dengan 25 dan 4 adalah Z dan E, maka I menjadi Z dan L menjadi E.

Blok 6 dari plaintext P adalah :

$$P_{11,12} = \begin{pmatrix} 20 \\ 7 \end{pmatrix}$$

$$C_{11,12} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 7 \end{pmatrix}$$

$$= \begin{pmatrix} 155 \\ 34 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 25 \\ 8 \end{pmatrix}$$

Karakter yang berkorespondensi dengan 25 dan 8 adalah Z dan I, maka U menjadi Z dan H menjadi I.

Blok 7 dari plaintext P adalah :

$$P_{13,14} = \begin{pmatrix} 20 \\ 17 \end{pmatrix}$$

$$C_{13,14} = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 20 \\ 17 \end{pmatrix}$$

$$= \begin{pmatrix} 205 \\ 54 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 23 \\ 2 \end{pmatrix}$$

Karakter yang berkorespondensi dengan 23 dan 2 adalah X dan C, maka U menjadi X dan R menjadi C.

Setelah melakukan enkripsi semua blok pada plaintext P maka dihasilkan ciphertext C sebagai berikut :

Plaintext (P) =

15 0 18 2 0 1 20 3 8 11 20 7 20 17

Plaintext (P) = PASCABUDILIHUR

Ciphertext (C) =

12 15 14 22 5 2 5 0 25 4 25 8 23 2

Ciphertext (C) = MPOWFCFAZEZIXC

b. Proses Dekripsi

Dengan menggunakan kunci :

$$K = \begin{pmatrix} 6 & 5 \\ 1 & 2 \end{pmatrix}$$

,maka proses dekripsi diawali dengan mencari invers dari matriks K. Mencari invers dapat dilakukan dengan menggunakan metode operasi baris (row operation) atau metode determinan.

$$[\,K \mid I\,] = \left(\begin{array}{cc|cc} 6 & 5 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{array}\right) \text{(R1-5R2)}$$

$$= \left(\begin{array}{cc|cc} 1 & -5 & 1 & -5 \\ 1 & 2 & 0 & 1 \end{array}\right) \text{(R2-R1)}$$

$$= \left(\begin{array}{cc|cc} 1 & -5 & 1 & -5 \\ 0 & 7 & -1 & 6 \end{array}\right) \text{ (15R2)}$$

$$= \left(\begin{array}{cc|cc} 1 & -5 & 1 & -5 \\ 0 & 105 & -15 & 90 \end{array}\right) \text{ (mod 26)}$$

$$= \left(\begin{array}{cc|cc} 1 & 21 & 1 & 21 \\ 0 & 1 & 11 & 12 \end{array}\right) \text{ R1-21R2}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & -230 & -231 \\ 0 & 1 & 11 & 12 \end{array}\right) \text{ mod26}$$

$$= \left(\begin{array}{cc|cc} 1 & 0 & 4 & 3 \\ 0 & 1 & 11 & 12 \end{array}\right)$$

$$K^{-1} = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix}$$

Setelah melakukan perhitungan, didapat matriks K^{-1} yang merupakan invers dari matriks K, yaitu :

$$K^{-1} = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix}$$

Chipertext C :
(MPOWFCFAZEZIXC)
akan didekripsi dengan menggunakan kunci dekripsi K^{-1} dengan persamaan $P = K^{-1} . C$.

Proses dekripsi ini dilakukan per block seperti proses pada enkripsi. Sebelum melakukan proses dekripsi pertama-tama ubahlah C kedalam numerik sesuai dengan tabel konversi.

Proses Dekripsi dilakukan sebagai berikut :
$P = K^{-1} . C \pmod{26}$

Blok 1 dari chipertext C adalah :

$$C(1,2) = \begin{pmatrix} 12 \\ 15 \end{pmatrix}$$

$$P(1,2) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 12 \\ 15 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \text{ x}12) + (3\text{x}15) \\ (11\text{x}12) + (12\text{x}15) \end{pmatrix}$$

$$= \begin{pmatrix} 93 \\ 312 \end{pmatrix} \text{ mod } 26$$

$$= \begin{pmatrix} 15 \\ 0 \end{pmatrix}$$

Hasil P(1,2) = 15 dan 0 , jika dilihat pada tabel konversi adalah P dan A
Blok 2 dari chipertext C adalah :

$$C(3,4) = \begin{pmatrix} 14 \\ 22 \end{pmatrix}$$

$$P(3,4) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 14 \\ 22 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \text{ x } 14) + (3\text{x}22) \\ (11\text{x}14) + (12\text{x}22) \end{pmatrix}$$

$$= \begin{pmatrix} 122 \\ 418 \end{pmatrix} \text{ mod } 26$$

$$= \begin{pmatrix} 18 \\ 2 \end{pmatrix}$$

Hasil P(3,4) = 18 dan 2 , jika dilihat pada tabel konversi adalah S dan C
Blok 3 dari chipertext C adalah :

$$C(5,6) = \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$

$$P(5,6) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 5 \\ 2 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \text{ x}5) + (3\text{x}2) \\ (11\text{x}5) + (12\text{x}2) \end{pmatrix}$$

$$= \begin{pmatrix} 26 \\ 79 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Hasil P(5,6) = 0 dan 1 , jika dilihat pada tabel konversi adalah A dan B

Blok 4 dari chipertext C adalah :

$$C(7,8) = \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

$$P(7,8) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 5 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \times 5) + (3 \times 0) \\ (11 \times 5) + (12 \times 0) \end{pmatrix}$$

$$= \begin{pmatrix} 20 \\ 55 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 20 \\ 3 \end{pmatrix}$$

Hasil P(7,8) = 20 dan 3 , jika dilihat pada tabel konversi adalah U dan D

Blok 5 dari chipertext C adalah :

$$C(9,10) = \begin{pmatrix} 25 \\ 4 \end{pmatrix}$$

$$P(9,10) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 25 \\ 4 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \times 25) + (3 \times 4) \\ (11 \times 25) + (12 \times 4) \end{pmatrix}$$

$$= \begin{pmatrix} 112 \\ 323 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 8 \\ 11 \end{pmatrix}$$

Hasil P(9,10) = 8 dan 11 , jika dilihat pada tabel konversi adalah I dan L

Blok 6 dari chipertext C adalah :

$$C(11,12) = \begin{pmatrix} 25 \\ 8 \end{pmatrix}$$

$$P(11,12) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 25 \\ 8 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \times 25) + (3 \times 8) \\ (11 \times 25) + (12 \times 8) \end{pmatrix}$$

$$= \begin{pmatrix} 124 \\ 371 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 20 \\ 7 \end{pmatrix}$$

Hasil P(11,12) = 20 dan 7 , jika dilihat pada tabel konversi adalah U dan H

Blok 7 dari chipertext C adalah :

$$C(13,14) = \begin{pmatrix} 23 \\ 2 \end{pmatrix}$$

$$P(13,14) = \begin{pmatrix} 4 & 3 \\ 11 & 12 \end{pmatrix} \begin{pmatrix} 23 \\ 2 \end{pmatrix}$$

$$= \begin{pmatrix} (4 \times 23) + (3 \times 2) \\ (11 \times 23) + (12 \times 2) \end{pmatrix}$$

$$= \begin{pmatrix} 98 \\ 277 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 20 \\ 17 \end{pmatrix}$$

Hasil P(13,14) = 20 dan 17 , jika dilihat pada tabel konversi adalah U dan R

Setelah melakukan dekripsi semua blok pada chipertext C maka dihasilkan plaintext sebagai berikut :

Ciphertext (C) =

12 15 14 22 5 2 5 0 25 4 25 8 23 2

Ciphertext (C) = MPOWFCFAZEZIXC

Plaintext (P) =

15 0 18 2 0 1 20 3 8 11 20 7 20 17

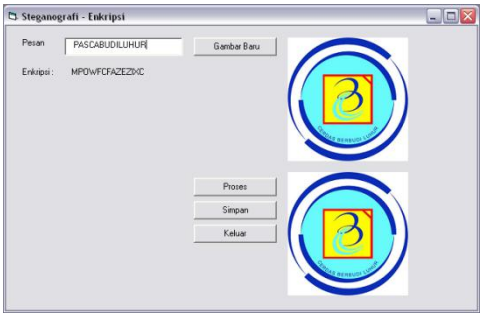
Plaintext (P) = PASCABUDILIHUR

c. Percobaan

Pada percobaan ini penulis menggunakan aplikasi *Microsoft Visual Studio*. Berikut ini penulis lampirkan hasil *screenshot* dari percobaan enkripsi menggunakan metode LSB dan Algoritma Cipher Hill.

d. Proses Enkripsi

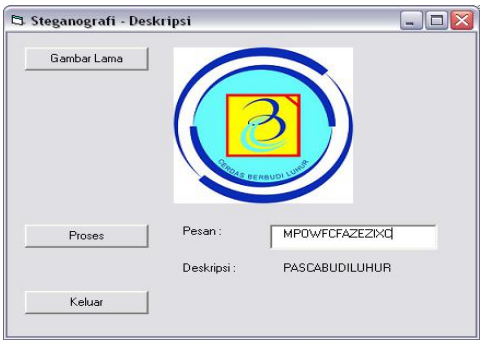
Pada screenshot ini merupakan tampilan proses enkripsi dari pesan: PASCABUDILUHUR yang menghasilkan teks MPOWFCFAZEZIXC



Gambar 1. Proses Enkripsi

e. Proses Deskripsi

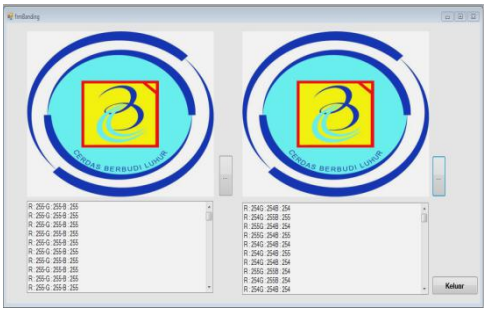
Pada screenshot ini merupakan tampilan proses deskripsi dari pesan: MPOWFCFAZEZIXC yang menghasilkan teks PASCABUDILUHUR



Gambar 2. Proses Deskripsi

f. Perbandingan Gambar

Pada screenshot ini merupakan tampilan perbandingan dari dua citra gambar yang belum dan sudah di enkripsi.



Gambar 3. Perbandingan Gambar

Pada perbandingan gambar tersebut bisa dilihat perbedaan RGB setiap gambar. Dimana ada yang berkurang setelah gambar tersebut di enkripsi. Berbeda dengan yang lainnya, pada percobaan ini citra gambar hasil enkripsi memiliki size yang sama dengan citra gambar yang sebelumnya tidak di enkripsi.

4. KESIMPULAN

Proses enkripsi pada Hill Cipher dapat dilakukan dengan langkah awal mengkonversi teks pesan kedalam bentuk angka yang telah dibuat pada tabel konversi. Lalu tentukan kunci sebagai pengali dengan nilai Plainteks (P) pada sistem matematis dalam menghitung enkripsi tersebut.

Proses deskripsi dapat dilakukan sama seperti proses enkripsi tapi, pada proses ini nilai kunci (K) harus di invers terlebih dahulu baru dapat dikalikan dengan nilai chiperteks (C). Kemudian hasil perhitungan dikonversikan kembali untuk mendapatkan pesan Plainteks (P).

5. SARAN

Hill Cipher yang dijelaskan dalam paper ini merupakan contoh sederhana dari kriptografi yang memanfaatkan kode ASCII. Beberapa tulisan telah menjelaskan algoritma hill chipper yang sedikit berbeda dan tidak menggunakan ASCII sebagai pengkonversi karakter pada teksnya.

Paper ini masih bisa dikembangkan lebih luas dengan memperluas asumsi matriks kuncinya. Misalnya determinan matriks kunci

tidak harus 1 dan -1 sehingga hasil invers matriks bukan merupakan bilangan bulat. Masalah ini dapat diselesaikan dengan menggunakan Modular aritmatika yaitu *reciprocal* atau *multiplicative inverse.*

DAFTAR PUSTAKA

[1] Dika Santosa, Egar. Implementasi Algoritma Caesar Cipher dan Hill Cipher pada Database Sistem Inventori TB Mitra Jepara. Teknik Informatika Universitas Dian Nuswantoro. Semarang.

[2] Nugraha, Ivan. Studi Analisis Mengenai Aplikasi Matriks dalam Kriptografi Hill Cipher. Teknik Informatika Institut Teknologi Bandung. Bandung.

[3] Prihastomo, Yoga. Komputasi Terapan Steganografi. 2011. Universitas Budi Luhur Jakarta.

[4] Prima Puspita, Niken. Dan Bahtiar Nurdin. Kriptografi Hill Cipher dengan Menggunakan Operasi Matriks. Jurusan Matematika FMIPA UNDIP. Semarang.

[5] Satria Alasi, Tomy. Penerapan Hill Cipher pada Keamanan Pesan Teks. Komunitas Elearning Ilmu Komputer.

[6] Suryani, Esti., Sri Martini, Titin., Kombinasi Kriptografi Dengan Hill Chiper Dan Steganografi Dengan LSB untuk Keamanan Data Teks, Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Magelang