Kriptografi Hill Cipher dan Least Significant Bit untuk Keamanan Pesan pada Citra

Hill Cipher and Least Significant Bit for Image Messaging Security

Muhammad Husnul Arif[1], Ahmad Zainul Fanani[2]
[1,2]Jurusan Teknik Informatika, Universitas Dian Nuswantoro Semarang
Jl. Imam Bonjol 205-207 Semarang 50131
e-mail: [1] husnul.arif93@gmail.com , [2] a.zainul.fanani@dsn.dinus.ac.id

Abstrak

*Pertukaran informasi melalui dunia maya memiliki berbagai manfaat sebagai contoh estimasi waktu yang cepat, jarak fisik dan batas ruang tidak terbatas dan lain sebagainya. Namun dalam kegiatan tersebut juga dapat menimbulkan resiko keamanan dalam informasi yang bersifat rahasia. Untuk itu diperlukan pengaman yang dapat digunakan untuk melindungi data yang ditransmisikan melalui jaringan internet. Algoritma penyandian yang digunakan dengan menyandikan pesan yang akan dikirim (plaintext) tersebut menjadi pesan yang sudah teracak (ciphertext) adalah algoritma kriptografi dan steganografi. Dalam penerapannya teknik kriptografi yang akan digunakan adalah Hill Cipher. Teknik tersebut dikombinasikan dengan steganografi dengan teknik Least Significant Bit. Hasil yang didapat dari penggabungan teknik dapat menjaga kerahasiaan pesan karena orang yang tidak mengetahui kunci rahasia yang digunakan akan kesulitan untuk mendapatkan pesan yang terdapat pada stego-image ditambah lagi gambar yang sudah pernah disisipi tidak dapat digunakan sebagai cover image. Pesan berhasil disisipkan dan diekstraksi kembali pada semua sample citra baik dengan format *bmp , *png , *jpg pada resolusi 512 x 512 piksel, 256 x 256 piksel. Hasil MSE dan PSNR tidak dipengaruhi format file ataupun ukuran file, tapi dipengaruhi oleh dimensi citra. Semakin besar dimensi citra, maka MSE semakin kecil artinya kerusakan citra semakin kecil.*

Kata kunci— Keamanan, Kriptografi, Steganografi, HillCipher, Least Significant Bit.

Abstract

*Exchange of information through cyberspace has many benefits as an example fast estimated time, unlimited physical distance and space limits, etc. But in these activities can also pose a security risk for confidential information. It is necessary for the safety that can be used to protect data transmitted through the Internet. Encryption algorithm that used to encrypt message to be sent (plaintext) into messages that have been randomized (ciphertext) is cryptography and steganography algorithms. In application of cryptographic techniques that will be used is Hill Cipher. The technique is combined with steganography techniques Least Significant Bit. The result of merging techniques can maintain the confidentiality of messages because people who do not know the secret key used will be difficult to get the message contained in the stego-image and the image that has been inserted can not be used as a cover image. Message successfully inserted and extracted back on all samples with a good image formats * .bmp, * .png , * .jpg at a resolution of 512 x 512 pixels , 256 x 256 pixels. MSE and PSNR results are not influenced file format or file size, but influenced by dimensions of image. The larger dimensions of the image, then the smaller MSE that means error of image gets smaller.*

Keywords— Security, Cryptography, Steganography, Hill Cipher, Least Significant Bit.

1. PENDAHULUAN

Era globalisasi sekarang ini banyak menggunakan perkembangan teknologi karena telah banyak memberikan manfaat dalam kemajuan di berbagai aspek sosial. Sebagai contoh dalam perkembangan teknologi yang sering digunakan untuk sarana pertukaran informasi dalam hitungan

detik adalah internet. Proses pertukaran informasi sering menggunakan file dengan format digital (teks, audio, gambar, citra, video, maupun gambar). Seiring perkembangan ini, *hacker, cracker, carder, phreaker* juga turut berkembang [1].Dengan adanya hal itu diperlukan pengaman yang dapat digunakan untuk melindungi data yang ditransmisikan melalui jaringan internet [2].

Keamanan berperan penting terutama pada informasi yang akan disampaikan dengan rahasia agar terhindar dari pihak ketiga yang ingin mencuri atau memanipulasi data [3]. Dengan adanya hal tersebut diperlukan sebuah algoritma yang dapat meningkatkan keamanan maupun kerahasiaan file, yaitu dengan menyandikan pesan yang akan dikirim tersebut menjadi pesan yang sudah teracak, sehingga apabila jatuh ke tangan yang tidak diinginkan, pesan tersebut juga tidak dapat digunakan. Algoritma penyandian diatas adalah algoritma kriptografi [4].

Kriptografi Hill Cipher yang merupakan *polyalphabetic cipher* yang dapat dikategorikan sebagai *block cipher*, karena teks yang akan diproses dibagi menjadi suatu blok-blok yang mempunyai ukuran tertentu. Setiap karakter dalam satu blok dapat mempengaruhi karakter lainnya dalam proses enkripsi maupun dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama juga. Pada tahun 1929 Lester S. Hill menciptakan algoritma Hill Cipher. Algoritma ini menggunakan sebuah matriks berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill Cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Namun, algoritma ini dapat dipecahkan jika kriptanalis memiliki berkas *ciphertext* dan potongan berkas *plaintext*. Teknik kriptanalis ini disebut dengan *known-plaintext attack* [5]. Untuk itu algoritma Hill Cipher ini perlu digabungkan dengan steganografi agar keamanan data dapat terjamin kerahasiaannya [1]. Steganografi merupakan sebuah ilmu dan seni untuk menuliskan pesan yang tersembunyi sedemikian rupa sehingga pihak selain yang berhak menerima tidak mengetahui keberadaan pesan tersebut. Sebagai contoh ilmu dan seni ini sudah dipakai orang Yunani kuno dengan membuat tato yang disembunyikan dikepala pengirim pesan yang dibotaki dan menunggu sampai tumbuh rambut. Steganografi merupakan pelengkap dari kriptografi karena tujuan dari steganografi adalah menyembunyikan sebuah pesan [3] [6]. Encoding dan decoding merupakan proses yang ada dalam steganografi. Encoding merupakan proses dimana disisipkan sebuah pesan kedalam *cover image*, decoding merupakan proses ekstraksi dari *stegoimage* untuk mendapatkan pesan didalamnya. MSB (*Most Significant Bit*) merupakan salah satu metode steganografi yang mengganti bit pertama pada 1 byte. Akan tetapi metode ini dirasa kurang bagus karena mata manusia bisa merasakan perbedaan yang terjadi pada gambar tersebut. Least Significant Bit dirasa cocok karena perubahan yang dilakukan hanya mengganti byte terakhir lebih rendah atau lebih tinggi satu byte dari sebelumnya. Jadi LSB tidak mengubah warna merah, jika dimisalkan byte menyatakan warna merah [7]. Oleh karena itu, penulis ingin melakukan penggabungan kriptografi Hillcipher dan Steganografi Least Significant Bit untuk meningkatkan keamanan pesan.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi (cryptography) berasal dari Bahasa Yunani, "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu dimana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi dikalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan d*ata integrity, autentication,* dan *non-repudiation* [8].

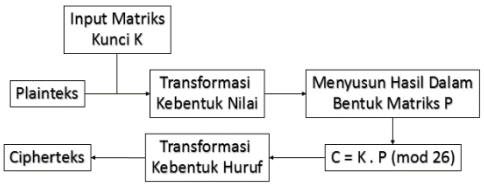
2.2 Hillcipher

Hill cipher dapat digolongkan sebagai kriptografi *polyalphabetic* yang dapat dikategorikan sebagai *block cipher,* karena teks yang akan diproses dibagi menjadi blok-blok dengan ukuran tertentu. Setiap karakter pada satu blok akan mempengaruhi hasil karakter lainnya dalam proses enkripsi maupun dekripsinya , karena karakter yang sama pada blok sebelumnya tidak akan dipetakan menjadi karakter yang sama pada blok sesudahnya. Pada tahun 1929 Lester S. Hill menciptakan

algoritma Hill Cipher. Teknik kriptografi ini diciptakan dengan maksud untuk menciptakan cipher yang tidak dapat dipecahkan menggunakan teknik anlisis frekuensi [5]. Terdapat beberapa alasan mengapa algorima kriptografi Hill Cipher sulit untuk dipecahkan. Alasan tersebut adalah sebagai berikut.

a. Hill Cipher menggunakan perkalian matriks untuk dasar enkripsi dan dekripsinya, jadi abjad pada *plaintext* tidak digantikan oleh abjad yang sama begitu juga dengan *ciphertext* [5].
b. Dengan menggunakan matriks yang lebih besar maka teknik penyembunyian pesan frekuensinya menjadi semakin tinggi [9].

Proses enkripsi pada Hill Cipher adalah [5]:
C = K . P
C = Ciphertext
K = Kunci
P = Plaintext



Gambar 1 Proses Enkripsi

Misalkan pesan yang akan dikirim adalah **'PELARIANRATU'** tetapkan indeks masing–masing karakter kedalam nilai numerik seperti A = 0 sampai Z = 25 dan menggunakan kunci matriks ordo 2x2.

$$Kunci = \begin{bmatrix} 9 & 3 \\ 7 & 6 \end{bmatrix}$$

Tabel 1 Indeks Karakter

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
13	14	15	16	17	18	19	20	21	22	23	24

Z
25

Mengubah karakter menjadi nilai numerik berdasarkan tabel indeks 1 :

$$\begin{matrix} P \\ E \end{matrix} = \begin{bmatrix} 15 \\ 4 \end{bmatrix}, \quad \begin{matrix} L \\ A \end{matrix} = \begin{bmatrix} 11 \\ 0 \end{bmatrix},$$
$$\begin{matrix} R \\ I \end{matrix} = \begin{bmatrix} 17 \\ 8 \end{bmatrix}, \quad \begin{matrix} A \\ N \end{matrix} = \begin{bmatrix} 0 \\ 13 \end{bmatrix},$$
$$\begin{matrix} R \\ A \end{matrix} = \begin{bmatrix} 17 \\ 0 \end{bmatrix}, \quad \begin{matrix} T \\ U \end{matrix} = \begin{bmatrix} 19 \\ 20 \end{bmatrix}$$

Pengerjaan menggunakan rumus enkripsi Hill Cipher, *C = K . P* mod 26 maka :

$$\begin{bmatrix} 9 & 3 \\ 7 & 6 \end{bmatrix}\begin{bmatrix} 15 \\ 4 \end{bmatrix} = \begin{bmatrix} 9.15+3.4 \\ 7.15+6.4 \end{bmatrix} = \begin{bmatrix} 147 \\ 129 \end{bmatrix} = \begin{bmatrix} 17 \\ 25 \end{bmatrix} mod\ 26 = \begin{bmatrix} R \\ Z \end{bmatrix}$$
$$\begin{bmatrix} 9 & 3 \\ 7 & 6 \end{bmatrix}\begin{bmatrix} 11 \\ 0 \end{bmatrix} = \begin{bmatrix} 9.11+3.0 \\ 7.11+6.0 \end{bmatrix} = \begin{bmatrix} 99 \\ 77 \end{bmatrix} = \begin{bmatrix} 21 \\ 25 \end{bmatrix} mod\ 26 = \begin{bmatrix} V \\ Z \end{bmatrix}$$
$$\begin{bmatrix} 9 & 3 \\ 7 & 6 \end{bmatrix}\begin{bmatrix} 17 \\ 8 \end{bmatrix} = \begin{bmatrix} 9.17+3.8 \\ 7.17+6.8 \end{bmatrix} = \begin{bmatrix} 177 \\ 167 \end{bmatrix} = \begin{bmatrix} 21 \\ 11 \end{bmatrix} mod\ 26 = \begin{bmatrix} V \\ L \end{bmatrix}$$

$$\begin{bmatrix}9 & 3\\ 7 & 6\end{bmatrix}\begin{bmatrix}0\\ 13\end{bmatrix}=\begin{bmatrix}9.0+3.13\\ 7.0+6.13\end{bmatrix}=\begin{bmatrix}39\\ 78\end{bmatrix}=\begin{bmatrix}13\\ 0\end{bmatrix} mod\ 26 =\begin{bmatrix}N\\ A\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\ 7 & 6\end{bmatrix}\begin{bmatrix}17\\ 0\end{bmatrix}=\begin{bmatrix}9.17+3.0\\ 7.17+6.0\end{bmatrix}=\begin{bmatrix}153\\ 119\end{bmatrix}=\begin{bmatrix}23\\ 15\end{bmatrix} mod\ 26 =\begin{bmatrix}X\\ P\end{bmatrix}$$
$$\begin{bmatrix}9 & 3\\ 7 & 6\end{bmatrix}\begin{bmatrix}19\\ 20\end{bmatrix}=\begin{bmatrix}9.19+3.20\\ 7.19+6.20\end{bmatrix}=\begin{bmatrix}231\\ 253\end{bmatrix}=\begin{bmatrix}23\\ 19\end{bmatrix} mod\ 26 =\begin{bmatrix}X\\ T\end{bmatrix}$$

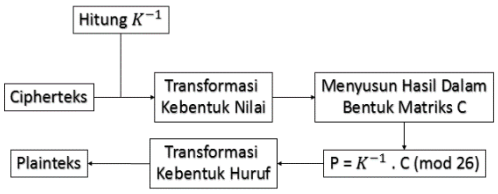
Didapatkan Ciphertext : **RZVZVLNAXPXT**

Proses dekripsi pada Hill Cipher dapat diturunkan dari persamaan [5].

$$C = K\,.\,P$$
$$K^{-1}\,.\,C = K^{-1}\,.\,K\,.\,P$$
$$K^{-1}\,.\,C = I\,.\,P$$
$$P = K^{-1}\,.\,C \quad (4)$$

Dimana untuk menentukan K^{-1} dengan menggunakan rumus :

$\frac{1}{det K} mod\ 26 = x$ *atau det K * x mod 26 = 1*



Gambar 2 Proses Dekripsi

$$det\begin{bmatrix}9 & 3\\ 7 & 6\end{bmatrix}=((9.6)-(7.3))$$
$$=(54-21)$$
$$=33\ mod\ 26$$
$$=7$$
$$\frac{1}{7} mod\ 26 = x$$
$$7.x\ mod\ 26 = 1$$
$$7.15\ mod\ 26 = 1$$
$$x = 15$$
$$K^{-1}=\frac{1}{\det K} mod\ 26\begin{bmatrix}6 & -3\\ -7 & 9\end{bmatrix}$$
$$=15\begin{bmatrix}6 & -3\\ -7 & 9\end{bmatrix}=\begin{bmatrix}90 & -45\\ -105 & 135\end{bmatrix}$$
$$=\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix} mod\ 26$$

Pengerjaan dekripsi dengan rumus

$$P = K^{-1}\,.\,C \quad (5)$$

$$\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix}\begin{bmatrix}17\\ 25\end{bmatrix}=\begin{bmatrix}12.17+7.25\\ 25.17+5.25\end{bmatrix}=\begin{bmatrix}379\\ 550\end{bmatrix}=\begin{bmatrix}15\\ 4\end{bmatrix} mod\ 26$$
$$\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix}\begin{bmatrix}21\\ 25\end{bmatrix}=\begin{bmatrix}12.21+7.25\\ 25.21+5.25\end{bmatrix}=\begin{bmatrix}427\\ 650\end{bmatrix}=\begin{bmatrix}11\\ 0\end{bmatrix} mod\ 26$$
$$\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix}\begin{bmatrix}21\\ 11\end{bmatrix}=\begin{bmatrix}12.21+7.11\\ 25.21+5.11\end{bmatrix}=\begin{bmatrix}329\\ 580\end{bmatrix}=\begin{bmatrix}17\\ 8\end{bmatrix} mod\ 26$$
$$\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix}\begin{bmatrix}13\\ 0\end{bmatrix}=\begin{bmatrix}12.13+7.0\\ 25.13+5.0\end{bmatrix}=\begin{bmatrix}156\\ 325\end{bmatrix}=\begin{bmatrix}0\\ 13\end{bmatrix} mod\ 26$$
$$\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix}\begin{bmatrix}23\\ 15\end{bmatrix}=\begin{bmatrix}12.23+7.15\\ 25.23+5.15\end{bmatrix}=\begin{bmatrix}381\\ 650\end{bmatrix}=\begin{bmatrix}17\\ 0\end{bmatrix} mod\ 26$$
$$\begin{bmatrix}12 & 7\\ 25 & 5\end{bmatrix}\begin{bmatrix}23\\ 19\end{bmatrix}=\begin{bmatrix}12.23+7.19\\ 25.23+5.19\end{bmatrix}=\begin{bmatrix}409\\ 670\end{bmatrix}=\begin{bmatrix}19\\ 20\end{bmatrix} mod\ 26$$

Sehingga didapat plaintext : **PELARIANRATU**

2.3 Least Significant Bit

Metode LSB merupakan metode steganografi yang paling sederhana dan mudah diimplementasikan. Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut [7]. Misalkan segmen pixel-pixel citra/gambar sebelum penambahan bit-bit adalah [7]:

00110011 10100010 11100010
10010110 11001001 11111001

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '**1110010111**', maka setiap bit dari pesan tersebut menggantikan posisi LSB dari segmen pixel-pixel citra menjadi (digarisbawahi):

00110011 10100011 11100011
10010111 11001000 11111001

Misalkan di sisipkan kata **'SA'** sudah enkripsi menggunakan metode *Hill Cipher*. Berikut langkah langkahnya adalah sebagai berikut.

Tiap karakter harus di ambil kode ASCII :

S = 83
A = 65

Mengkonversi kode ASCII kedalam bentuk biner :

S = 83 = 01010011
A = 65 = 01000001

Pengambilan nilai untuk penyisipan pesan

Pxl1	Pxl2	Pxl3	Pxl4	Pxl5	Pxl6
Pxl7	Pxl8	Pxl9	Pxl10	Pxl11	Pxl12
Pxl13	Pxl14	Pxl15	Pxl16	Pxl17	Pxl18
Pxl19	Pxl20	Pxl21	Pxl22	Pxl23	Pxl24
Pxl25	Pxl26	Pxl27	Pxl28	Pxl29	Pxl30
Pxl31	Pxl32	Pxl33	Pxl34	Pxl35	Pxl36

Gambar 3 Ilustrasi pixel sebuah image

Misalkan didapatkan nilai dari masing – masing piksel adalah :

P1 : 156 = 10011100
P2 : 172 = 10101100
P3 : 124 = 01111100
P4 : 122 = 01111010
P5 : 250 = 11111010
P6 : 201 = 11001001
P7 : 108 = 01101100
P8 : 211 = 11010011
P9 : 206 = 11001110
P10 : 131 = 11001110
P11 : 167 = 10100111
P12 : 145 = 10010001
P13 : 222 = 11011110
P14 : 231 = 11100111
P15 : 204 = 11001100
P16 : 142 = 10001110

Melakukan penyisipan pesan yang sudah dikonversi ke biner "**01010011 01000001 01011001 01000001**" dengan cara mengganti bit terakhir pada biner pixel dengan biner pesan sehingga menjadi :

P1: 1001110**0** diganti 0= 1001110**0**= 156
P2 : 1010110**0** diganti 1 = 1010110**1**= 173
P3 : 0111110**0** diganti 0 = 0111110**0**= 124
P4 : 0111101**0** diganti 1 = 0111101**1**= 123
P5 : 1111101**0** diganti 0 = 1111101**0**= 250
P6 : 1100100**1** diganti 0 = 1100100**0**= 200
P7 : 0110110**0** diganti 1 = 0110110**1**= 109
P8 : 1101001**1** diganti 1 = 1101001**1**= 211
P9 : 1100111**0** diganti 0 = 1100111**0**= 206
P10 : 1100111**0** diganti 1 = 1100111**1**= 207
P11 : 1010011**1** diganti 0 = 1010011**0**= 166
P12 : 1001000**1** diganti 0 = 1001000**0**= 144
P13 : 1101111**0** diganti 0 = 1101111**0**= 222
P14 : 1110011**1** diganti 0 = 1110011**0**= 230
P15 : 1100110**0** diganti 0 = 1100110**0**= 204
P16 : 1000111**0** diganti 1 = 1000111**1**= 143

Ekstraksi LSB dilakukan dengan mengambil bit – bit terakhir dari piksel kemudian di representasikan terhadap nilai kode ASCII. Berikut tahapan proses ekstraksi dengan mengambil piksel kemudian dikonversi ke biner dan diambil bit paling akhir.

P1 : 156 = 1001110**0**= 0
P2 : 173 = 1010110**1**= 1
P3 : 124 = 0111110**0**= 0
P4 : 123 = 0111101**1**= 1
P5 : 250 = 1111101**0**= 0
P6 : 200 = 1100100**0**= 0
P7 : 109 = 0110110**1**= 1
P8 : 211 = 1101001**1**= 1
P9 : 206 = 1100111**0**= 0
P10 : 207 = 1100111**1**= 1
P11 : 166 = 1010011**0**= 0
P12 : 144 = 1001000**0**= 0
P13 : 222 = 1101111**0**= 0
P14 : 230 = 1110011**0**= 0
P15 : 204 = 1100110**0**= 0
P16 : 143 = 1000111**1**= 1

Dari penghitungan diatas diperoleh hasil dari bit terakhir yaitu sebagai berikut "**01010011 01000001**", kemudian dikonversi kedalam ASCII dan dilanjutkan ke bentuk karakter

01010011 = 83 = S
01000001 = 65 = A

Selanjutnya *chiphertext* didekripsi menggunakan algoritma *Hill Cipher*.

2.4 Pengujian

MSE merupakan hasil kesalahan rata-rata kuadrat dari citra asli dengan citra hasil. Pengujian MSE dikatakan baik jika mempunyai nilai yang rendah. Rumus untuk menghitung MSE adalah :

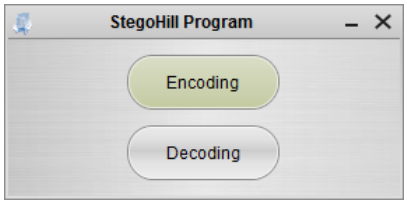
$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}| f(x,y) - g(x,y))^2 | \quad (6)$$

PSNR diukur dalam satuan 65ecibel (dB). Untuk melakukan penghitungan nilai PSNR, terlebih dahulu harus dicari nilai MSEnya. Kualitas citra dikatakan baik jika nilai PSNR semakin besar. Rumus PSNR adalah:

$$PSNR = {}^{20}\log\left(\frac{MAX}{\sqrt{MSE}}\right) \quad (7)$$

3. HASIL DAN PEMBAHASAN

Data yang digunakan untuk pesan adalah sebuah karakter abjad dengan range 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, dimana karakter tersebut akan dilakukan enkripsi menggunakan algoritma kriptografi Hill Cipher, kemudian disisipkan kedalam citra digital dan di ekstraksi kembali dari citra digital menggunakan algoritma Least Significant Bit selanjutnya didekripsi menjadi karakter pesan asli. Data citra yang digunakan untuk pengujian terdapat 3 jenis format file *.jpg *.png *.bmp dan ukuran citra 512x512 dan 256x256 yang akan dijadikan sebagai *cover-image*. Data citra yang digunakan adalah hasil dari pemotretan sendiri dan disesuaikan dengan kebutuhan penelitian.



Gambar 4 Tampilan Utama

Halaman utama adalah halaman yang akan diakses pertama pada sistem. Pada halaman utama terdapat pilihan Encoding dan Decoding. Untuk proses penyisipan pesan kedalam cover image yang akan digunakan oleh pengirim pesan menggunakan Encoding. Decoding merupakan proses ekstraksi pesan yang terdapat dalam cover image, proses ini digunakan oleh penerima pesan rahasia

Gambar 5 Input Pesan & Embbeding

Pada gambar 5 user dapat menginputkan isi pesan yang akan disisipkan ke dalam cover image. Adapun Isi dari Pesan yang akan dimasukkan kedalam cover image tersebut adalah "**UNIVERSITASDIANNUSWANTOROAKREDITASIA**".
Dengan mengisi pesan yang telah disediakan dalam textarea kita dapat menekan tombol button Embed. Setelah proses embedding maka gambar yang sudah tersisipi sebuah pesan rahasia akan ditampilkan pada JscrollPane Gambar Steganografi dan terbukanya tombol button Save dan Reset. Proses akan sukses ketika user menekan tombol button Save untuk menyimpan gambar steganografi.

Gambar 6 Proses Ekstraksi Pesan

Pada gambar 6 merupakan proses ekstraksi pada citra stego yang menghasilkan pesan. Hasil dari ekstraksi akan dimasukkan pada textarea yang ada disamping gambar steganografi. Berikut merupakan penghitungan manual dengan $K = \begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}$, dan P adalah

UNIVERSITASDIANNUSWANTOROAKREDITASIA sebagai berikut. Mengubah karakter menjadi nilai numerik berdasarkan tabel 1, karakter dibagi menjadi blok yang setiap bloknya terdiri dari dua karakter. Sehingga karakter tersebut menjadi :

$$\begin{matrix} U \\ N \end{matrix} = \begin{bmatrix} 20 \\ 13 \end{bmatrix} \quad \begin{matrix} U \\ S \end{matrix} = \begin{bmatrix} 20 \\ 18 \end{bmatrix} \quad \begin{matrix} A \\ S \end{matrix} = \begin{bmatrix} 0 \\ 18 \end{bmatrix}$$

$$\begin{matrix} I \\ V \end{matrix} = \begin{bmatrix} 8 \\ 21 \end{bmatrix} \quad \begin{matrix} W \\ A \end{matrix} = \begin{bmatrix} 22 \\ 0 \end{bmatrix} \quad \begin{matrix} I \\ A \end{matrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix}$$

$$\begin{matrix} E \\ R \end{matrix} = \begin{bmatrix} 4 \\ 17 \end{bmatrix} \quad \begin{matrix} N \\ T \end{matrix} = \begin{bmatrix} 13 \\ 19 \end{bmatrix}$$

$$\begin{matrix} S \\ I \end{matrix} = \begin{bmatrix} 18 \\ 8 \end{bmatrix} \quad \begin{matrix} O \\ R \end{matrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

$$\begin{matrix} T \\ A \end{matrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix} \quad \begin{matrix} O \\ A \end{matrix} = \begin{bmatrix} 14 \\ 0 \end{bmatrix}$$

$$\begin{matrix} S \\ D \end{matrix} = \begin{bmatrix} 18 \\ 3 \end{bmatrix} \quad \begin{matrix} K \\ R \end{matrix} = \begin{bmatrix} 10 \\ 17 \end{bmatrix}$$

$$\begin{matrix} I \\ A \end{matrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix} \quad \begin{matrix} E \\ D \end{matrix} = \begin{bmatrix} 4 \\ 3 \end{bmatrix}$$

$$\begin{matrix} N \\ N \end{matrix} = \begin{bmatrix} 13 \\ 13 \end{bmatrix} \quad \begin{matrix} I \\ T \end{matrix} = \begin{bmatrix} 8 \\ 19 \end{bmatrix}$$

Pengerjaan menggunakan rumus enkripsi Hill Cipher, $C = K \,.\, P \ mod\ 26$ maka :

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 20 \\ 13 \end{bmatrix} = \begin{bmatrix} 7.20 + 8.13 \\ 4.20 + 9.13 \end{bmatrix} = \begin{bmatrix} 244 \\ 197 \end{bmatrix} = \begin{bmatrix} 10 \\ 15 \end{bmatrix} mod\ 26 = \begin{bmatrix} K \\ P \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 8 \\ 21 \end{bmatrix} = \begin{bmatrix} 7.8 + 8.21 \\ 4.8 + 9.21 \end{bmatrix} = \begin{bmatrix} 224 \\ 221 \end{bmatrix} = \begin{bmatrix} 16 \\ 13 \end{bmatrix} mod\ 26 = \begin{bmatrix} Q \\ N \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 4 \\ 17 \end{bmatrix} = \begin{bmatrix} 7.4 + 8.17 \\ 4.4 + 9.17 \end{bmatrix} = \begin{bmatrix} 164 \\ 169 \end{bmatrix} = \begin{bmatrix} 8 \\ 13 \end{bmatrix} mod\ 26 = \begin{bmatrix} I \\ N \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 18 \\ 8 \end{bmatrix} = \begin{bmatrix} 7.18 + 8.8 \\ 4.18 + 9.8 \end{bmatrix} = \begin{bmatrix} 190 \\ 144 \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix} mod\ 26 = \begin{bmatrix} I \\ O \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} 7.19 + 8.0 \\ 4.19 + 9.0 \end{bmatrix} = \begin{bmatrix} 133 \\ 76 \end{bmatrix} = \begin{bmatrix} 3 \\ 24 \end{bmatrix} mod\ 26 = \begin{bmatrix} D \\ Y \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 18 \\ 3 \end{bmatrix} = \begin{bmatrix} 7.18 + 8.3 \\ 4.18 + 9.3 \end{bmatrix} = \begin{bmatrix} 150 \\ 99 \end{bmatrix} = \begin{bmatrix} 20 \\ 21 \end{bmatrix} mod\ 26 = \begin{bmatrix} U \\ V \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 8 \\ 0 \end{bmatrix} = \begin{bmatrix} 7.8 + 8.0 \\ 4.8 + 9.0 \end{bmatrix} = \begin{bmatrix} 56 \\ 32 \end{bmatrix} = \begin{bmatrix} 4 \\ 6 \end{bmatrix} mod\ 26 = \begin{bmatrix} E \\ G \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 13 \\ 13 \end{bmatrix} = \begin{bmatrix} 7.13 + 8.13 \\ 4.13 + 9.13 \end{bmatrix} = \begin{bmatrix} 195 \\ 169 \end{bmatrix} = \begin{bmatrix} 13 \\ 13 \end{bmatrix} mod\ 26 = \begin{bmatrix} N \\ N \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 20 \\ 18 \end{bmatrix} = \begin{bmatrix} 7.20 + 8.18 \\ 4.20 + 9.18 \end{bmatrix} = \begin{bmatrix} 284 \\ 242 \end{bmatrix} = \begin{bmatrix} 24 \\ 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} Y \\ I \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 22 \\ 0 \end{bmatrix} = \begin{bmatrix} 7.22 + 8.0 \\ 4.22 + 9.0 \end{bmatrix} = \begin{bmatrix} 154 \\ 88 \end{bmatrix} = \begin{bmatrix} 24 \\ 10 \end{bmatrix} mod\ 26 = \begin{bmatrix} Y \\ K \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} 7.13 + 8.19 \\ 4.13 + 9.19 \end{bmatrix} = \begin{bmatrix} 243 \\ 223 \end{bmatrix} = \begin{bmatrix} 9 \\ 15 \end{bmatrix} mod\ 26 = \begin{bmatrix} J \\ P \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 7.14 + 8.17 \\ 4.14 + 9.17 \end{bmatrix} = \begin{bmatrix} 234 \\ 209 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} mod\ 26 = \begin{bmatrix} A \\ B \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 14 \\ 0 \end{bmatrix} = \begin{bmatrix} 7.14 + 8.0 \\ 4.14 + 9.0 \end{bmatrix} = \begin{bmatrix} 98 \\ 56 \end{bmatrix} = \begin{bmatrix} 20 \\ 4 \end{bmatrix} mod\ 26 = \begin{bmatrix} U \\ E \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 10 \\ 17 \end{bmatrix} = \begin{bmatrix} 7.10 + 8.17 \\ 4.10 + 9.17 \end{bmatrix} = \begin{bmatrix} 206 \\ 193 \end{bmatrix} = \begin{bmatrix} 24 \\ 11 \end{bmatrix} mod\ 26 = \begin{bmatrix} Y \\ L \end{bmatrix}$$

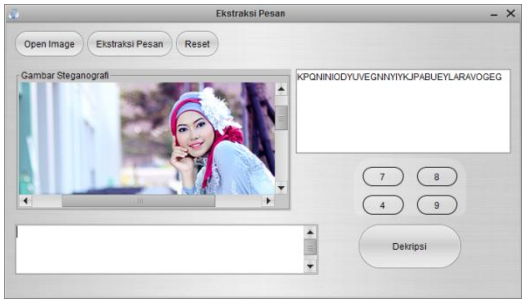
$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 4 \\ 3 \end{bmatrix} = \begin{bmatrix} 7.4 + 8.3 \\ 4.4 + 9.3 \end{bmatrix} = \begin{bmatrix} 52 \\ 43 \end{bmatrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix} mod\ 26 = \begin{bmatrix} A \\ R \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 8 \\ 19 \end{bmatrix} = \begin{bmatrix} 7.8 + 8.19 \\ 4.8 + 9.19 \end{bmatrix} = \begin{bmatrix} 208 \\ 203 \end{bmatrix} = \begin{bmatrix} 0 \\ 21 \end{bmatrix} mod\ 26 = \begin{bmatrix} A \\ V \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 0 \\ 18 \end{bmatrix} = \begin{bmatrix} 7.0 + 8.18 \\ 4.0 + 9.18 \end{bmatrix} = \begin{bmatrix} 144 \\ 162 \end{bmatrix} = \begin{bmatrix} 14 \\ 6 \end{bmatrix} mod\ 26 = \begin{bmatrix} O \\ G \end{bmatrix}$$

$$\begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}\begin{bmatrix} 8 \\ 0 \end{bmatrix} = \begin{bmatrix} 7.8 + 8.0 \\ 4.8 + 9.0 \end{bmatrix} = \begin{bmatrix} 56 \\ 32 \end{bmatrix} = \begin{bmatrix} 4 \\ 6 \end{bmatrix} mod\ 26 = \begin{bmatrix} E \\ G \end{bmatrix}$$

Dari hasil perhitungan enkripsi Hill Cipher dari rumus *C = K . P Mod 26* diperoleh Ciphertext : KPQNINIODYUVEGNNYIYKJPABUEYLARAVOGEG. Pada proses ekstraksi gambar menghasilkan Ciphertext yang sama pada perhitungan manual. Maka proses penyisipan berhasil dilakukan pada gambar cover image.



Gambar 7 Input Kunci Matriks

Proses memasukkan inputan nilai yang akan dijadikan kunci untuk mendapatkan hasil plainteks. Proses ini digunakan oleh user penerima pesan. Rumus mendapatkan pesan asli adalah $P = K^{-1} . C$ dimana K^{-1} didapatkan dari kunci yang telah di inputkan pertama kali saat peyisipan pesan dilakukan.

$$K = \begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix}$$

Dengan Kunci tersebut, akan dicari K^{-1} sebagai berikut :

$$\begin{aligned} det \begin{bmatrix} 7 & 8 \\ 4 & 9 \end{bmatrix} &= ((7.9) - (4.8)) \\ &= (63 - 32) \\ &= 31 \ mod \ 26 \\ &= 5 \end{aligned}$$

$$\begin{aligned} \frac{1}{5} \ mod \ 26 &= x \\ 5.x \ mod \ 26 &= 1 \\ 5.21 \ mod \ 26 &= 1 \\ x &= 21 \end{aligned}$$

$$K^{-1} = \frac{1}{det \, K} \ mod \ 26 \begin{bmatrix} 9 & -8 \\ -4 & 7 \end{bmatrix}$$

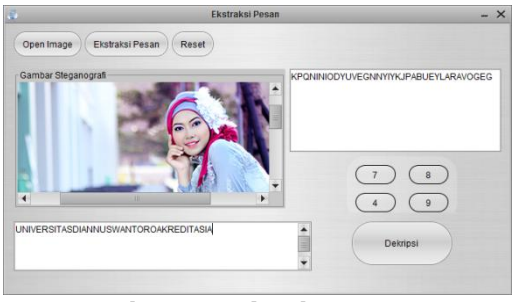
$$= 21 \begin{bmatrix} 9 & -8 \\ -4 & 7 \end{bmatrix} = \begin{bmatrix} 189 & -168 \\ -84 & 147 \end{bmatrix}$$

$$= \begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix} \ mod \ 26$$

Dari perhitungan pencarian K^{-1} didapatkan Kunci matriks yang akan dijadikan sebagai proses dekripsi cipherteks adalah :

$$K^{-1} = \begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}$$

Kunci Invers matriks tersebut nantinya akan digunakan untuk proses dekripsi pesan.



Gambar 8 Hasil Dekripsi Pesan

Setelah proses input kunci selesai , proses selanjutnya adalah mendekripsi cipherteks. Pengerjaan dekripsi dengan rumus :

$$P = K^{-1} . C \qquad (8)$$

$$K^{-1} = \begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}$$

Cipherteks = KPQNINIODYUVEGNNYIYKJPABUEYLARAVOGEG

Kemudian dilanjutkan dengan dibaginya karakter cipherteks menjadi 2 blok , agar dapat diproses ke pengerjaan dekripsi pesan.

$$\begin{matrix} K \\ P \end{matrix} = \begin{bmatrix} 10 \\ 15 \end{bmatrix} \qquad \begin{matrix} Y \\ I \end{matrix} = \begin{bmatrix} 24 \\ 8 \end{bmatrix} \qquad \begin{matrix} O \\ G \end{matrix} = \begin{bmatrix} 14 \\ 6 \end{bmatrix}$$

$$\begin{matrix} Q \\ N \end{matrix} = \begin{bmatrix} 16 \\ 13 \end{bmatrix} \qquad \begin{matrix} Y \\ K \end{matrix} = \begin{bmatrix} 24 \\ 10 \end{bmatrix} \qquad \begin{matrix} E \\ G \end{matrix} = \begin{bmatrix} 4 \\ 6 \end{bmatrix}$$

$$\begin{matrix} I \\ N \end{matrix} = \begin{bmatrix} 8 \\ 13 \end{bmatrix} \qquad \begin{matrix} J \\ P \end{matrix} = \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

$$\begin{matrix} I \\ O \end{matrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix} \qquad \begin{matrix} A \\ B \end{matrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\begin{matrix} D \\ Y \end{matrix} = \begin{bmatrix} 3 \\ 24 \end{bmatrix} \qquad \begin{matrix} U \\ E \end{matrix} = \begin{bmatrix} 20 \\ 4 \end{bmatrix}$$

$$\begin{matrix} U \\ V \end{matrix} = \begin{bmatrix} 20 \\ 21 \end{bmatrix} \qquad \begin{matrix} Y \\ L \end{matrix} = \begin{bmatrix} 24 \\ 11 \end{bmatrix}$$

$$\begin{matrix} E \\ G \end{matrix} = \begin{bmatrix} 4 \\ 6 \end{bmatrix} \qquad \begin{matrix} A \\ R \end{matrix} = \begin{bmatrix} 0 \\ 17 \end{bmatrix}$$

$$\begin{matrix} N \\ N \end{matrix} = \begin{bmatrix} 13 \\ 13 \end{bmatrix} \qquad \begin{matrix} A \\ V \end{matrix} = \begin{bmatrix} 0 \\ 21 \end{bmatrix}$$

Pengerjaan dekripsi dengan rumus

$$P = K^{-1} . C$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 10 \\ 15 \end{bmatrix} = \begin{bmatrix} 7.10 + 14.15 \\ 20.10 + 17.15 \end{bmatrix} = \begin{bmatrix} 280 \\ 455 \end{bmatrix} = \begin{bmatrix} 20 \\ 13 \end{bmatrix} mod\ 26 = \begin{bmatrix} U \\ N \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 16 \\ 13 \end{bmatrix} = \begin{bmatrix} 7.16 + 14.13 \\ 20.16 + 17.13 \end{bmatrix} = \begin{bmatrix} 294 \\ 541 \end{bmatrix} = \begin{bmatrix} 8 \\ 21 \end{bmatrix} mod\ 26 = \begin{bmatrix} I \\ V \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 8 \\ 13 \end{bmatrix} = \begin{bmatrix} 7.8 + 14.13 \\ 20.8 + 17.13 \end{bmatrix} = \begin{bmatrix} 238 \\ 381 \end{bmatrix} = \begin{bmatrix} 4 \\ 17 \end{bmatrix} mod\ 26 = \begin{bmatrix} E \\ R \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} 7.8 + 14.14 \\ 20.8 + 17.14 \end{bmatrix} = \begin{bmatrix} 252 \\ 398 \end{bmatrix} = \begin{bmatrix} 18 \\ 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} S \\ I \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 3 \\ 24 \end{bmatrix} = \begin{bmatrix} 7.3 + 14.24 \\ 20.3 + 17.24 \end{bmatrix} = \begin{bmatrix} 357 \\ 468 \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} T \\ A \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 20 \\ 21 \end{bmatrix} = \begin{bmatrix} 7.20 + 14.21 \\ 20.20 + 17.21 \end{bmatrix} = \begin{bmatrix} 434 \\ 757 \end{bmatrix} = \begin{bmatrix} 18 \\ 3 \end{bmatrix} mod\ 26 = \begin{bmatrix} S \\ D \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 4 \\ 6 \end{bmatrix} = \begin{bmatrix} 7.4 + 14.6 \\ 20.4 + 17.6 \end{bmatrix} = \begin{bmatrix} 112 \\ 182 \end{bmatrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} I \\ A \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 13 \\ 13 \end{bmatrix} = \begin{bmatrix} 7.13 + 14.13 \\ 20.13 + 17.13 \end{bmatrix} = \begin{bmatrix} 273 \\ 481 \end{bmatrix} = \begin{bmatrix} 13 \\ 13 \end{bmatrix} mod\ 26 = \begin{bmatrix} N \\ N \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 7.24 + 14.8 \\ 20.24 + 17.8 \end{bmatrix} = \begin{bmatrix} 280 \\ 616 \end{bmatrix} = \begin{bmatrix} 20 \\ 18 \end{bmatrix} mod\ 26 = \begin{bmatrix} U \\ S \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 24 \\ 10 \end{bmatrix} = \begin{bmatrix} 7.24 + 14.10 \\ 20.24 + 17.10 \end{bmatrix} = \begin{bmatrix} 308 \\ 650 \end{bmatrix} = \begin{bmatrix} 22 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} W \\ A \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 9 \\ 15 \end{bmatrix} = \begin{bmatrix} 7.9 + 14.15 \\ 20.9 + 17.15 \end{bmatrix} = \begin{bmatrix} 273 \\ 435 \end{bmatrix} = \begin{bmatrix} 13 \\ 19 \end{bmatrix} mod\ 26 = \begin{bmatrix} N \\ T \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 7.0 + 14.1 \\ 20.0 + 17.1 \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix} = \begin{bmatrix} 14 \\ 17 \end{bmatrix} mod\ 26 = \begin{bmatrix} O \\ R \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 20 \\ 4 \end{bmatrix} = \begin{bmatrix} 7.20 + 14.4 \\ 20.20 + 17.4 \end{bmatrix} = \begin{bmatrix} 196 \\ 468 \end{bmatrix} = \begin{bmatrix} 14 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} O \\ A \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 24 \\ 11 \end{bmatrix} = \begin{bmatrix} 7.24 + 14.11 \\ 20.24 + 17.11 \end{bmatrix} = \begin{bmatrix} 322 \\ 667 \end{bmatrix} = \begin{bmatrix} 10 \\ 17 \end{bmatrix} mod\ 26 = \begin{bmatrix} K \\ R \end{bmatrix}$$

$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 0 \\ 17 \end{bmatrix} = \begin{bmatrix} 7.0 + 14.17 \\ 20.0 + 17.17 \end{bmatrix} = \begin{bmatrix} 238 \\ 289 \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \end{bmatrix} mod\ 26 = \begin{bmatrix} E \\ D \end{bmatrix}$$
$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 0 \\ 21 \end{bmatrix} = \begin{bmatrix} 7.0 + 14.21 \\ 20.0 + 17.21 \end{bmatrix} = \begin{bmatrix} 294 \\ 357 \end{bmatrix} = \begin{bmatrix} 8 \\ 19 \end{bmatrix} mod\ 26 = \begin{bmatrix} I \\ T \end{bmatrix}$$
$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 14 \\ 6 \end{bmatrix} = \begin{bmatrix} 7.14 + 14.6 \\ 20.14 + 17.6 \end{bmatrix} = \begin{bmatrix} 182 \\ 382 \end{bmatrix} = \begin{bmatrix} 0 \\ 18 \end{bmatrix} mod\ 26 = \begin{bmatrix} A \\ S \end{bmatrix}$$
$$\begin{bmatrix} 7 & 14 \\ 20 & 17 \end{bmatrix}\begin{bmatrix} 4 \\ 6 \end{bmatrix} = \begin{bmatrix} 7.4 + 14.6 \\ 20.4 + 17.6 \end{bmatrix} = \begin{bmatrix} 112 \\ 182 \end{bmatrix} = \begin{bmatrix} 8 \\ 0 \end{bmatrix} mod\ 26 = \begin{bmatrix} I \\ A \end{bmatrix}$$

Hasil dari pengerjaan dekripsi dari perkalian matriks K^{-1} dengan cipherteks mendapatkan cipherteks sebagai berikut :
Cipherteks : UNIVERSITASDIANNUSWANTOROAKREDITASIA

No	Nama File	Citra	Ukuran (Kb)	Status Embed	MSE	PNSR (dB)
1	J1-512		620Kb	Sukses	0.0011	83.7769
2	J2-256		157Kb	Sukses	0.0044	77.7563
3	P4-512		317Kb	Sukses	0.0011	83.7769
4	P3-256		157Kb	Sukses	0.0044	77.7563
5	B4-512		769Kb	Sukses	0.0011	83.7769
30	B5-256		193Kb	Sukses	0.0044	77.7563

Gambar 9 Hasil Percobaan

4. KESIMPULAN

Setelah dilakukan implementasi penyisipan pesan baik enkripsi, dekripsi, embedded, ektraksi dan pengujian maka peneliti menyimpulkan bahwa :

1. Penggabungan teknik kriptografi Hill Cipher dan steganografi Least Significant Bit dapat membantu menjaga kerahasiaan pesan karena orang yang tidak mengetahui kunci rahasia yang digunakan akan kesulitan untuk mendapatkan pesan yang terdapat pada *stego-image*. Dan gambar yang sudah pernah disisipi oleh pesan tidak dapat digunakan kembali sebagai cover image.
2. Pesan berhasil disisipkan dan diekstraksi kembali pada semua sample citra baik dengan format *bmp , *png , *jpg dan pada resolusi 512 x 512 piksel, 256 x 256 piksel.
3. Hasil pengujian pada citra digital menggunakan MSE dan PNSR tidak dipengaruhi oleh format file *jpg, *bmp, dan *png dan juga pada ukuran file. Akan tetapi, dipengaruhi oleh dimensi citra tersebut, pesan yang sama disisipkan ke dalam media citra yang berbeda yang dimensinya sama, hasil kualitas citra yang dihasilkan cenderung sama. Semakin besar dimensi citra yang digunakan, maka MSE-nya semakin kecil, artinya nilai kerusakan citra semakin kecil. Sedangkan nilai PSNR-nya (kualitas citra) semakin besar.

5. SARAN

Dalam penelitian ini masih memiliki beberapa kekurangan dan kelemahan yang dapat dikembangkan dalam penelitian selanjutnya. Saran bagi penelitian selanjutnya yaitu sebagai berikut :

1. Masih terbatas dengan 26 karakter yakni A-Z sehingga kombinasi masih terbatas dibandingkan 256 karakter yang dapat dikombinasikan dengan simbol – simbol.

2. Peneliti dapat menggembangkan menggunakan kunci matriks dengan ordo 3x3.

DAFTAR PUSTAKA

[1] S. dan E. Utami, "Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher Dan Fungsi Hash MD5," dalam *Seminar Nasional Teknologi 2007 (SNT 2007)*, Yogyakarta, 2007.

[2] E. Setyaningsih , "PENYANDIAN CITRA MENGGUNAKAN METODE PLAYFAIR CIPHER," *Jurnal Teknologi*, vol. 2, no. 2, pp. 213-217, 2009.

[3] M. M. Amin, "Image Steganography Dengan Metode Least Significant Bit," *CSRID JOURNAL*, vol. 6, no. 1, pp. 1-64, 2014.

[4] V. Yuniati, G. Indriyanta dan A. Rachmat, "Enkripsi Dan Dekripsi Dengan Algoritma AES 256 Untuk Semua Jenis File," *Jurnal Informatika*, vol. 5, no. 1, pp. 22-31, 2009.

[5] A. H. Hasugian, "Implementasi Algoritma Hill Cipher Dalam Penyandian Data," *Pelita Innformatika Budi Darma*, vol. 4, no. 2, pp. 115-122, 2013.

[6] T. Cahyadi, "IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA JPEG," *TRANSIENT*, vol. 1, no. 4, pp. 281-288, 2012.

[7] B. Rakhmat dan M. Fairuzabadi, "STEGANOGRAFI MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN KOMBINASI ALGORITMA KRIPTOGRAFI VIGENERE DAN RC4," *Jurnal Dinamika Informatika*, vol. 5, no. 2, pp. 1-17, 2010.

[8] R. Munir, Kriptografi, Bandung: Informatika Bandung, 2006.

[9] W. Stallings, CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES ANDPRACTICE FIFTH EDITION, United States: Prentice Hall, 2006.