

Teknik Penyembunyian Pesan Rahasia dengan Enkripsi *Hill Cipher* pada Citra Digital dengan Metode *Least Significant Bit* (LSB)

Muhamad Rizky Fajar Febrian¹⁾, Ghaitsa Ardelia Rosyida²⁾, Christy Atika Sari³⁾

¹⁾ Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol No.205-207, Pendrikan Kidul, Semarang 50131, Indonesia

²⁾ Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol No.205-207, Pendrikan Kidul, Semarang 50131, Indonesia

³⁾ Departement of Informatics Engineering, Universitas Dian Nuswantoro
Jl. Imam Bonjol No.205-207, Pendrikan Kidul, Semarang 50131, Indonesia

Abstract - Nowadays, technology growing rapidly. Tools and place to make information exchange is more easier. So cybercrime or cyber through internet mostly happened, so Information exchange in cyberspace becomes risky and vulnerable to theft. To reduce risk and vulnerable of data theft, how to secure data is applied. Data security can be done with crptography technique and steganography technique. Cryptography is changing data to some form that people cant's understand and steganography is hiding data inside the other form. Based on literature and some source that cryptography combined with steganography can increase data security level. One of cryptography technique is Hill Cipher. This algorithm mostly used to encrypt data in the form of text message called plaintext. Result of hill cipher algorithm is string which is difficult to people understand called ciphertext that make suspicion. Used of Least Significant Bit (LSB) method is to insert ciphertext that generated to cover image. LSB was chosen because easy to use and stego image which generated very similar with original image if seen with bare eye and the data which inserted inside it has not changed. The result of experiments have been done is measured with Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) with obtained the smalles PSNR value 51.2907 dB. It means stego image that generated pretty good.

Keywords – criptography; strgsnography; hill cipher; LSB

Abstrak - Seiring berkembangnya zaman, teknologi saat ini sudah cepat berkembang. Sarana untuk bertukar informasi menjadi lebih mudah. Sehingga cybercrime atau kejahatan melalui internet sangat sering terjadi. Pertukaran informasi di dunia maya menjadi lebih rentan dicuri. Untuk mengurangi risiko, diterapkan cara mengamankan data. Pengamanan data dapat dilakukan dengan Teknik kriptografi dan steganografi. Kriptografi adalah merubah data menjadi tidak dimengerti dan steganografi adalah menyembunyikan data dalam bentuk yang lain. Berdasarkan sumber literatur, kombinasi kriptografi

dan steganografi dapat meningkatkan level keamanan data. Salah satu algoritma kriptografi yang telah digunakan adalah Hill Cipher. Algoritma ini sering digunakan untuk mengenkripsi data berupa pesan text yang disebut ciphertext. Hasil dari algoritma tersebut adalah kata berupa huruf yang sulit untuk dimengerti yang mungkin menimbulkan kecurigaan orang lain. Digunakannya metode Least Significant Bit (LSB) adalah untuk menyisipkan ciphertext yang telah dibuat ke dalam citra berupa gambar. LSB dipilih karena mudah digunakan dan gambar stego yang tercipta tidak berbeda dengan gambar aslinya jika dilihat dengan kasat mata dan data yang tersisip didalamnya tidak mengalami perubahan. Hasil percobaan yang telah kami lakukan diukur menggunakan Mean Square Error (MSE) dan Peak Signal to Noise Ratio (PSNR) dengan diperoleh PSNR terkecil sebesar 51.2907 dB yang berarti citra stego yang dihasilkan cukup baik.

Kata Kunci – kriptografi; steganografi; hill cipher; LSB.

I. PENDAHULUAN

Dalam penggunaannya, internet memiliki dampak positif terhadap setiap orang dalam bertukar data dan informasi dengan cepat dan bebas [1]. Dampak negatifnya adalah kejahatan di dunia maya oleh pihak yang tidak bertanggung jawab juga turut meningkat sehingga perlu diadakan [2]. Maka dari itu untuk mempersulit para pihak yang tidak bertanggung jawab, banyak cara yang dapat dilakukan untuk menyembunyikan pesan atau informasi, misalnya dengan menggunakan watermarking, steganografi, kriptografi dan tanda tangan digital [3]. Steganografi adalah cara untuk menyembunyikan pesan ke konten digital lainnya [4] seperti gambar, video atau audio supaya tidak terlihat dari luar. Menurut domainnya, steganografi dibagi menjadi dua jenis yaitu domain frekuensi dan domain spasial [5]. Transformasi diskrit cosine (DCT) dan transfromasi diskrit wavelet (DWT) adalah contoh domain frekuensi yang memiliki kelebihan lebih kuat terhadap manipulasi citra [6] [7]. Metode *Least Significant Bit* (LSB) menggunakan domain spasial yang lebih rentan terhadap serangan dan informasi mudah hilang saat citra dimanipulasi. Metode steganografi disini menggunakan metode Least Significant Bit (LSB). Metode Least Significant Bit (LSB) adalah salah satu

*) Penulis korespondensi (Muhamad Rizky Fajar F)
Email: 111201710492@mhs.dinus.ac.id

algoritma paling mudah dan sederhana karena hanya mengubah nilai bit terakhir dengan bit pesan. Penerapan teknik steganografi memiliki banyak kelebihan dalam hal imperceptibility, misalnya citra yang dihasilkan sangat mirip dengan citra aslinya sehingga tidak dapat dilihat perbedaannya oleh mata manusia [3] [5]. Sedangkan kriptografi adalah teknik untuk mengenkripsi pesan sehingga pesan tidak dapat dibaca secara langsung. Namun cepatnya perkembangan pengetahuan dan teknologi memungkinkan pihak yang tidak berwenang dapat mengetahui pesan dari citra *cover* sehingga diperlukan penyandian tambahan pada pesan, seperti yang dilakukan peneliti sebelumnya dengan mengkombinasikan metode kriptografi dan steganografi, pada jurnal [5] [6] [8]. Proses enkripsi dilakukan menggunakan algoritma kriptografi tertentu.

Kriptografi adalah sebuah teknik penyandian pesan atau pengacakan pesan menjadi bentuk yang tidak dimengerti oleh oranglain [9]. Algoritma yang digunakan penulis yaitu algoritma Hill Cipher. Algoritma hill cipher adalah salah satu kunci algoritma simetris yang memiliki bebrapa keunggulan dalam data.

Peneliti menggunakan metode kriptografi yaitu algoritma Hill Cipher untuk enkripsi pesan yang menghasilkan *ciphertext*. Hill Cipher merupakan teknik kriptografi yang kuat dan sulit dipecahkan bila tidak diketahui kunci matriksnya, namun mudah dipecahkan bila mengetahui kunci matriksnya sehingga untuk menutupi kekurangan dan menambah keamanan pesan, maka digunakan teknik penyisipan *ciphertext* kedalam citra digital berupa gambar dengan menggunakan metode steganografi yaitu Least Significant Bit (LSB).

Dalam penelitian ini, akan membahas tentang implementasi penyembunyian pesan atau informasi pada citra digital dengan menggabungkan algoritma hill cipher dan metode Least Significant Bit (LSB). Disini juga akan menganalisis kualitas hasil metode dalam berbagai hal seperti imperceptibility, ukuran stego image, dan kualitas enkripsi. Kualitas imperceptibility akan diukur dengan MSE, PSNR, dan histogram. Sedangkan kualitas enkripsi diukur dengan entropi [10].

II. LANDASAN TEORI

A. Pengolahan Citra Digital

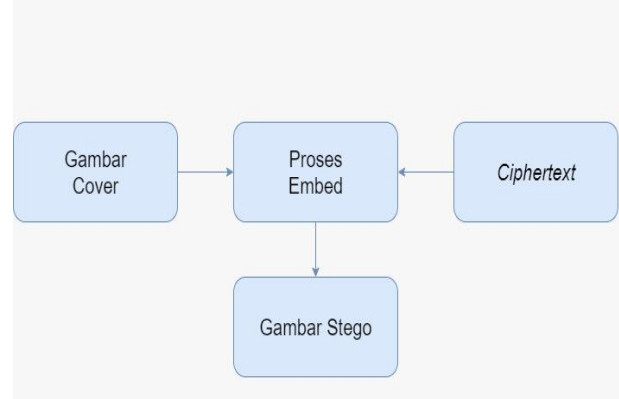
Pengolahan citra digital (*digital image processing*) adalah sebuah disiplin ilmu yang mempelajari tentang teknik-teknik mengolah citra [11]. Citra yang dimaksud disini adalah gambar diam (foto) maupun gambar bergerak. Sedangkan digital disini mempunyai maksud bahwa pengolahan citra atau gambar dilakukan secara digital menggunakan komputer [12].

B. Steganografi

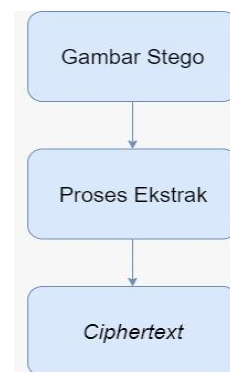
Steganografi adalah cara untuk menyembunyikan pesan ke konten digital lainnya seperti gambar, video atau audio supaya tidak terlihat dari luar. Kata steganografi berasal dari kata Yunani *Steganos* yang artinya “tersembunyi/terselubung” dan *graphein*

“menulis” sehingga kurang lebih artinya “menulis (tulisan) terselubung” [12].

Jenis steganografi menyediakan keamanan yang lebih baik dibandingkan dengan pure steganografi. Masalah utama dari menggunakan sistem steganografi adalah berbagi kunci. Jika pencuri tahu kuncinya, akan lebih mudah untuk mendeskripsi dan mengakses informasi asli. Steganografi diterapkan untuk media seperti teks, gambar, video klip, musik dan suara [13].



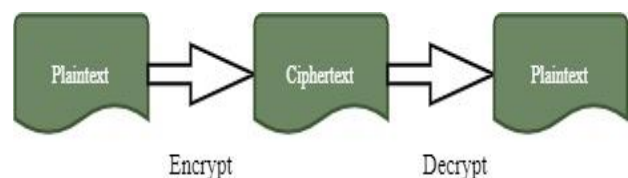
Gambar 1 Proses Embed [12]



Gambar 2 Proses Ekstrak [12]

C. Kriptografi

Kriptografi adalah teknik untuk mengenkripsi pesan sehingga pesan tidak dapat dibaca secara langsung. *Cryptos* berasal dari kata Yunani yang memiliki arti “rahasia” sementara *graphe* yang berarti “menulis”.



Gambar 3 Proses Encrypt dan Decrypt [14]

Komponen algoritma kriptografi :

1. Input : Plaintext, pesan (data/informasi) yang akan dikirim (berisi data/informasi dalam bahasa aslinya). Plaintext digunakan selama proses enkripsi biasanya dalam bentuk text.
2. Output : Ciphertext, plaintext di enkripsi dalam bentuk kode yang tidak memiliki arti dan hampir

tidak dikenali sebagai pesan atau data atau informasi.

3. Encryption : proses untuk mengubah text biasa menjadi ciphertext.
4. Description : proses mengubah kembali dari plaintext ke ciphertext.
5. Key : proses enkripsi dan deskripsi akan membutuhkan kunci, mungkin kunci publik dan kunci pribadi.

D. Least Significant Bit (LSB)

Metode Least Significant Bit (LSB) merupakan metode penyembunyian pesan atau informasi dalam suatu media, dengan cara menyisipkan secara langsung pesan kedalam pixel dari citra *cover* [1]. Dengan memodifikasi sebagian kecil dari bit setiap pixel, dimana posisi bit tersebut akan digantikan oleh pesan yang akan disembunyikan pada media induk terpilih [16], sehingga maka perubahan yang terjadi pada nilai warna tidak terlalu berpengaruh pada kualitas gambar, metode ini memiliki *imperceptible* yang baik sehingga pengelihat manusia tidak dapat melihat perubahan citra [4]. Penentuan dan perubahan bit tersebut dilakukan dengan cara berurutan mulai dari bit pertama sampai bit terakhir sesuai dengan panjangnya pesan yang akan disisipkan [17].

E. Hill Cipher

Hill cipher diciptakan oleh Lester S. Hill pada tahun 1929. Metode ini merupakan salah satu algoritma kriptografi kunci simetris. Dasar teori matriks yang digunakan adalah perkalian antar matriks dan invers pada matriks [15]. Menurut Sadikin (2012, hal 51) sandi *hill* merupakan sandi *polyalphabet* dengan menggunakan metode substitusi dengan perhitungan perkalian matriks. Sedangkan menurut Ariyus (2008, hal 59) kode *hill* termasuk salah satu kriptopolialfabetik, yang berarti setiap karakter alfabet bisa dipetakan ke lebih dari satu macam karakter [16].

Hill Cipher termasuk pada algoritma kriptografi yang sulit dipecahkan jika seseorang hanya mengetahui ciphertext saja tanpa mengetahui kuncinya. Namun sangat mudah dipecahkan apabila mengetahui kuncinya.

F. Citra Digital

Citra digital adalah citra yang diolah oleh komputer. Sudah banyak peralatan elektronik jaman sekarang yang menggunakan citra digital, misalnya scanner, kamera digital, mikroskop digital dan fingerprint reader. Sebagai contoh, Adobe Photoshop dan GIMP (GNU Image Manipulation Program) menyajikan berbagai fitur untuk memanipulasi citra digital [16].

Dalam hal ini citra digital yang digunakan adalah RGB (*Red, Green, Blue*). Jika masing-masing warna memiliki range 0-255, maka totalnya adalah $255^3 = 16.581.375$ (16k) variasi warna berbeda pada gambar. Color image ini terdiri dari tiga matriks yaitu red, green, blue setiap pixelnya [11].

G. MSE (*Mean Square Error*) dan PSNR (*Peak Signal Noise Ratio*)

Untuk mengetahui kelebihan dan kekurangan pada sebuah penelitian maka dilakukan pengujian metode. Sebuah citra diuji untuk mengetahui seberapa bagus kualitas citra tersebut dengan alat ukur MSE (*Mean Square Error*) dan PSNR (*Peak Signal Noise Ratio*) [6].

Mean Square Error adalah alat ukur untuk menguji kualitas citra pengukuran rata-rata kuadrat kesalahan kumulatif antara stego dan gambar asli. Error menunjukkan distorsi atau penyimpangan pada gambar.

Dihitung dengan rumus :

$$MSE = \left(\frac{1}{mn}\right)^2 \sum_{i=1}^M \sum_{j=1}^N (X_{ij} - Y_{ij})^2$$

Keterangan :

MSE = Mean Square Error

M = Baris matriks

N = Kolom matriks

X_{ij} = Nilai dari pixel pada gambar cover

Y_{ij} = Nilai dari pixel pada gambar stego

Peak Signal to Noise Ratio adalah rasio nilai maximum dari sinyal yang diukur dengan noise yang berpengaruh pada sinyal tersebut, PSNR digunakan untuk mengetahui perbandingan nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal. PSNR digunakan untuk menyatakan kualitas citra [8]. Dapat dihitung dengan rumus :

$$PSNR = 10 \log \frac{255^2}{MSE}$$

Keterangan :

PSNR = Peak Signal to Noise Ratio

dB = Desibell

H. Entropi

Entropi adalah konsep acak dimana terdapat keadaan yang kemungkinan tidak pasti. Definisi entropi yang berhubungan dengan teori informasi adalah ukuran yang menyatakan jumlah informasi di dalam pesan. Dinyatakan dalam satuan bit. Berguna untuk mengodekan elemen pesan (Munir, 2006) [10]. Dapat dihitung dengan rumus :

$$H_e = - \sum_{k=0}^n P(k) \log_2 (P(k))$$

Keterangan :

H_e = Entropi

n = Jumlah simbol yang berbeda di dalam pesan, pada citra n adalah nilai keabuan dari citra

P_k = Probabilitas kejadian simbol k

III. PEMBAHASAN

A. Pengujian Algoritma Hill Cipher

Kunci yang digunakan dalam pengujian ini menggunakan matriks kunci ordo 2x2. Pesan yang disandikan tidak ditentukan berapa banyak karakter tiap karakter harus berada diantara huruf A-Z dan besar kecilnya huruf tidak dibedakan. Kode angka berdasarkan urutan huruf misal A=0, B=1, C=3 dan seterusnya sampai Z=25 serta spasi tidak dihitung dalam penyandian. Langkah-langkah proses enkripsi pesan dilakukan sebagai berikut :

$$C = P \times K$$

C = Ciphertext

K = Matriks kunci

P = Plaintext

P = KAMU

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

1. Menghilangkan spasi antara kata
2. Jika jumlah karakter ganjil maka tiambahkan *dummy* karakter agar jumlahnya menjadi genap.
3. Merubah plaintext ke bentuk matriks angka ber ordo 1×2

$$P = \begin{bmatrix} K \\ A \end{bmatrix} \begin{bmatrix} M \\ U \end{bmatrix}$$

4. Merubah matriks plaintext ke menjadi angka berdasarkan table berikut:

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

Sehingga menjadi :

$$P = \begin{bmatrix} 10 \\ 0 \end{bmatrix} \begin{bmatrix} 12 \\ 20 \end{bmatrix}$$

5. Mengkalikan P (plaintext) dengan K (kunci):

$$C = K \times P$$

$$= \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \times \begin{bmatrix} 10 \\ 0 \end{bmatrix} = \begin{bmatrix} 20 \\ 10 \end{bmatrix}; \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \times$$

$$\begin{bmatrix} 12 \\ 20 \end{bmatrix} = \begin{bmatrix} 84 \\ 92 \end{bmatrix}$$

6. Mencari sisa hasil bagi dengan modulo 26 masing-masing blok matriks

$$\begin{bmatrix} 20 \\ 10 \end{bmatrix} \mod 26 = \begin{bmatrix} 20 \\ 10 \end{bmatrix}$$

$$\begin{bmatrix} 84 \\ 92 \end{bmatrix} \mod 26 = \begin{bmatrix} 6 \\ 14 \end{bmatrix}$$

7. Mengubah matriks angka ke menjadi karakter dengan table konversi

$$\begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{bmatrix} U \\ K \end{bmatrix}; \begin{bmatrix} 6 \\ 14 \end{bmatrix} = \begin{bmatrix} G \\ O \end{bmatrix}$$

8. Ciphertext yang dihasilkan :

$$\begin{bmatrix} U \\ K \end{bmatrix} \begin{bmatrix} G \\ O \end{bmatrix}$$

$$C = 'UKGO'$$

Setelah dilakukan proses *encrypt* selesai dilakukan, maka untuk *decrypt ciphertext* menjadi *plaintext* matriks kunci harus di invers kan terlebih dahulu. Berikut langkah-langkah yang dilakukan untuk *decrypt* suatu pesan :

$$P = K^{-1} \times C$$

1. Mencari determinan matriks kunci

2. Mencari invers matriks (K^{-1})

$$K^{-1} = \begin{bmatrix} 6 & 15 \\ 5 & 16 \end{bmatrix}$$

3. Mengubah ciphertext ke matriks 1×2

$$\begin{bmatrix} 20 \\ 10 \end{bmatrix} \begin{bmatrix} 6 \\ 14 \end{bmatrix}$$

4. Mengkalikan invers kunci dengan matriks angka ciphertext

$$= K^{-1} \times C$$

$$\begin{bmatrix} 6 & 15 \\ 5 & 16 \end{bmatrix} \times \begin{bmatrix} 20 \\ 10 \end{bmatrix} = \begin{bmatrix} 270 \\ 260 \end{bmatrix} \mod 26 \begin{bmatrix} 10 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 6 & 15 \\ 5 & 16 \end{bmatrix} \times \begin{bmatrix} 6 \\ 14 \end{bmatrix} = \begin{bmatrix} 246 \\ 254 \end{bmatrix} \mod 26 \begin{bmatrix} 12 \\ 20 \end{bmatrix}$$

5. Merubah ordo matriks menjadi $n \times 1$

$$P = [10 \ 0 \ 12 \ 20]$$

6. Merubah matriks angka menjadi karakter sesuai table konversi

$$P = [K \ A \ M \ U]$$

B. Pengujian Metode *Least Significant Bit* (LSB)

Pengujian Metode *Least Significant Bit* (LSB) dalam pembahasan ini dijelaskan bagaimana proses penyisipan pesan cipher ke dalam citra gambar. Gambar yang digunakan adalah gambar berwarna 24 bit, yaitu gambar yang terdiri dari 3 warna (R,G,B) masing masing warna mempunyai kedalaman warna sebesar 8 bit, maka pesan akan disisipkan ke dalam bit R, bit G dan bit B tiap-tiap piksel. Di bawah ini adalah langkah-langkah proses steganografi untuk menyisipkan pesan kedalam citra gambar dengan algoritma LSB dengan menggunakan UKGO sebagai ciphertext yang telah dibuat sebelumnya menggunakan algoritma kriptografi Hill Cipher. Langkah pertama mengubah ciphertext menjadi biner sebagai berikut :

Teks	Biner
K	01001011
A	01000001
M	01001101
U	01010101

Table 1 Merubah karakter ke biner

Setelah diubah kedalam biner lalu pesan akan disisipkan kedalam gambar pada warna (RBG) dengan metode lsb dengan nilai biner (sample) gambar sebagai berikut :

01110111	01110110	01110100	01000111
01110011	01110100	01110110	01110110
01110100	01110110	01110111	01110011
10110111	11110111	01110111	11110111
11010111	01110110	11110111	01110110
11110111	10110111	11111111	01110111
01110100	11000111	11110111	00010111
10110111	11110111	01110111	11110111

Table 2 Kode biner gambar cover

0111011 <u>0</u>	01110110	01110100	0100011 <u>0</u>
01110011	0111010 <u>1</u>	0111011 <u>1</u>	0111011 <u>1</u>
01110100	01110110	0111011 <u>0</u>	0111001 <u>0</u>
1011011 <u>0</u>	1111011 <u>0</u>	0111011 <u>0</u>	11110111
11010111	01110110	11110111	01110110
1111011 <u>0</u>	1011011 <u>0</u>	11111111	01110111
0111010 <u>1</u>	1100011 <u>0</u>	1111011 <u>0</u>	0001011 <u>0</u>
10110111	11110111	01110111	11110111

Table 3 Kode biner gambar setelah disisipi pesan

Langkah terakhir, menggabungkan layer RGB yang telah disisipi pesan biner menjadi sebuah gambar stego kemudian disimpan.

Langkah ekstraksi gambar stego

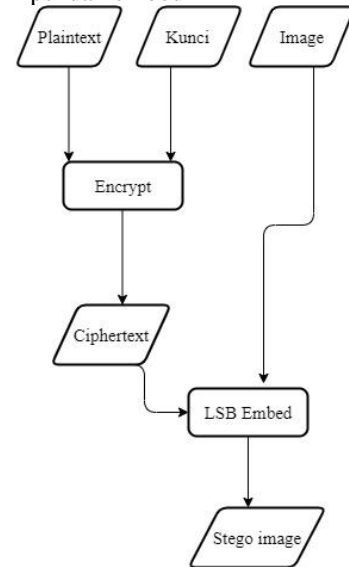
Untuk proses ekstraknya adalah mengambil nilai paling kanan dari biner yang disisipkan. Data biner yang telah diambil isi pesannya dimana nilai tersebut adalah sebagai berikut :

Teks	Biner
K	01001011
A	01000001
M	01001101
U	01010101

Table 4 Hasil Stego

Terdapat beberapa tahapan penelitian yaitu :

1. Tahap enkripsi dan embed

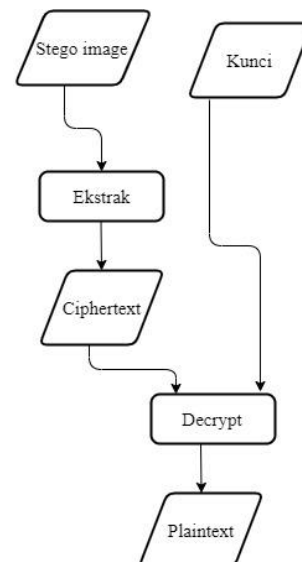


Gambar 4 Proses encrypt dan embed

Berikut merupakan langkah dari proses encrypt dan embedding :

- 1) Masukkan *plaintext* dan kunci yang akan disembunyikan
- 2) Setelah memasukkan *plaintext* dan kunci akan dilakukan proses *encrypt* dengan hill cipher
- 3) Setelah di *encrypt* akan menghasilkan *chiphertext* untuk dimasukkan dalam gambar
- 4) Akan dilakukan proses embedding menggunakan algoritma LSB dan menghasilkan gambar stego

2. Tahap ekstrak dan dekripsi



Gambar 5 Proses decrypt dan ekstrak

Berikut merupakan langkah dari proses ekstrak dan decrypt :





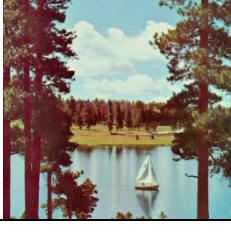
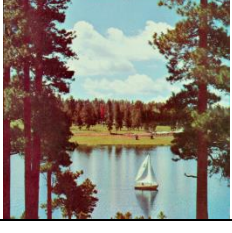
- 1) Masukkan gambar stego untuk melakukan proses ekstraksi
- 2) Setelah ekstrak selesai akan menghasilkan *ciphertext*
- 3) Akan dilakukan proses *decrypt* dengan memasukkan kunci
- 4) Setelah proses *decrypt* selesai akan menghasilkan *plaintext* dengan menggunakan hill cipher

IV. HASIL

A. Citra Digital yang Digunakan

Peneliti menggunakan dua macam ukuran citra *cover*, yaitu dengan ukuran 512 x 512 pixel dan 16 x 16 pixel. Ukuran pesan yang digunakan adalah 240 karakter, 480 karakter, dan 9600 karakter untuk *cover* dengan ukuran 512 x 512 dan 90 karakter untuk *cover* dengan ukuran 16 x 16. Citra *cover* yang digunakan pada penelitian ini terdapat pada Table 5, Table 6 dan Table 7 untuk citra berukuran 512 x 512 dan pada Table 12, Table 13 dan Table 14 untuk citra berukuran 16 x 16 beserta gambar stego yang dibuat.

B. Hasil Penyisipan Pesan (*Stego Image*) dan Uji Kualitas Citra Berukuran 512 x 512

No	Gambar cover	Gambar Stego
a.		
b.		
c.		

d.		
e.		

Table 5 Hasil Penyisipan Pesan dengan 240 Karakter pada citra berukuran 512 x 512



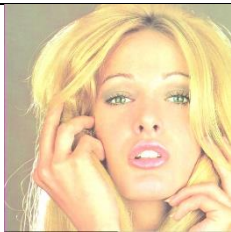
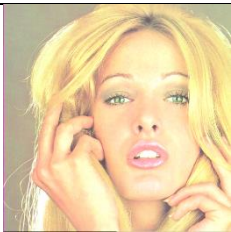
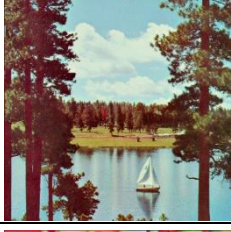
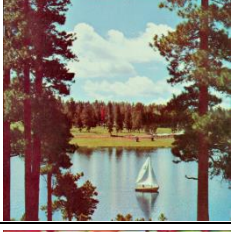


No	Gambar cover	Gambar Stego
a.		
b.		
c.		
d.		



Table 6 Hasil Penyisipan Pesan dengan 480 Karakter pada citra berukuran 512 x 512

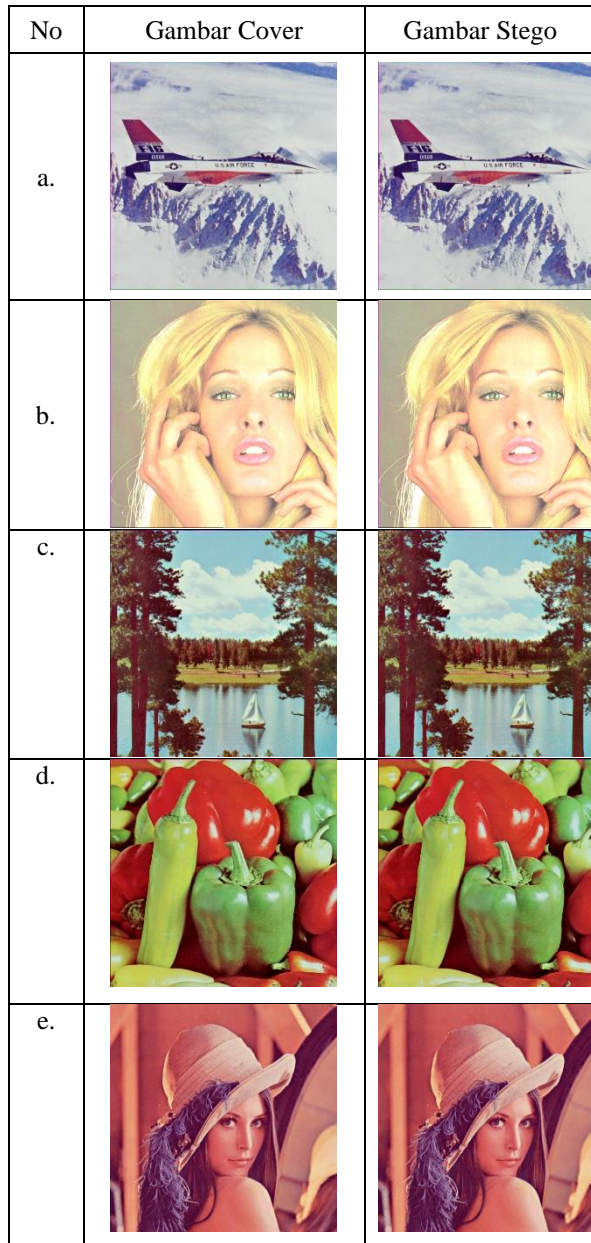


Table 8 Hasil Penyisipan Pesan dengan 9600 Karakter pada citra berukuran 512 x 512

Jika table-table diatas diamati dan dilihat dengan benar, tidak terdapat perbedaan saat dilihat secara kasat mata pada citra stego maupun citra *cover*. Hal tersebut membuat kualitas citra stego sangat baik. Tetapi tentunya diperlukan alat ukur untuk menentukan kualitas stego, yaitu *Peak Signal Noise Ratio* (PSNR) dan *Mean Square Error* (MSE). PSNR digunakan untuk membandingkan kualitas citra sebelum dan sesudah dilakukan penyisipan pesan., sedangkan MSE digunakan untuk mengetahui nilai kesalahan kuadrat rata-rata antara citra sebelum dan sesudah.

No	Ukuran	Max	Pesan	MSE	PSNR	Entropi
a.	512 x 512	98112	240	0,0012	77,1974	6,4288
b.	512 x 512	98112	240	0,0013	76,9380	6,6639
c.	512 x 512	98112	240	0,0012	77,2874	7,7639
d.	512 x 512	98112	240	0,0012	77,4780	7,6709
e.	512 x 512	98112	240	0,0013	77,0831	5,6954
Rata-rata				0,0012	77,1968	6,8446

Table 7 Hasil Pengujian Table 5

No	Ukuran	Max	Pesan	MSE	PSNR	Entropi
a.	512 x 512	98112	480	0,0024	74,2930	6,4288
b.	512 x 512	98112	480	0,0026	74,0511	6,6640
c.	512 x 512	98112	480	0,0024	74,2794	7,7639
d.	512 x 512	98112	480	0,0024	74,3760	7,6710
e.	512 x 512	98112	480	0,0025	74,1076	5,7058
Rata-rata				0,0025	74,2214	6,8467

Table 9 Hasil Pengujian Table 6

No	Ukuran	Max	Pesan	MSE	PSNR	Entropi
a.	512 x 512	98112	9600	0,0490	61,2316	6,4298
b.	512 x 512	98112	9600	0,0491	61,2183	6,6644
c.	512 x 512	98112	9600	0,0493	61,1989	7,7639
d.	512 x 512	98112	9600	0,0487	61,2551	7,6715
e.	512 x 512	98112	9600	0,0492	61,2134	5,9404
Rata-rata				0,0491	61,2235	6,8940

Table 10 Hasil Pengujian Table 7

Ukuran	Max	Pesan	Avg MSE	Avg PSNR	Avg Entropy
512 x 512	98112	240	0,0013	77,1968	6,8446
512 x 512	98112	480	0,0025	74,2214	6,8467
512 x 512	98112	9600	0,0491	61,2235	6,8940

Table 11 Ratio Perbedaan Kualitas Nilai MSE dan PSNR berdasarkan Jumlah Pesan yang Disisipkan Pada Citra Berukuran 512 x 512

Dapat dilihat dari Tabel 11 nilai PSNR akan semakin kecil karena semakin banyak pesan yang disisipkan berarti semakin banyak pula bit yang berubah pada citra *cover*. Pada citra berukuran 512 x 512 yang

dapat menampung pesan sebanyak 98112 karakter, saat disisipi pesan sebanyak 240 karakter rata-rata PSNR yang didapat sebesar 77.1968 dB, saat disisipi pesan sebanyak 480 karakter rata-rata PSNR sebesar 74.2214 dB dan 61.2235 untuk rata-rata PSNR yang didapat saat disisipi 9600 karakter. Dari hasil tersebut, nilai PSNR tetap berada di atas 40 dB yang berarti kualitas citra stego yang tercipta sangat baik.

C. Hasil Penyisipan Pesan (*Stego Image*) dan Uji Kuaitas Citra Berukuran 16 x 16




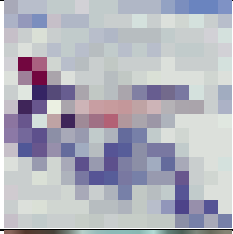
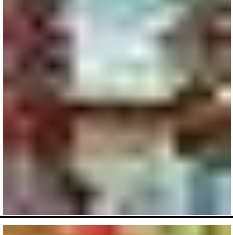
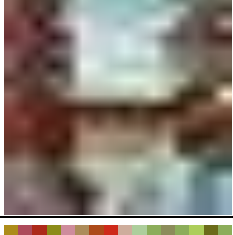
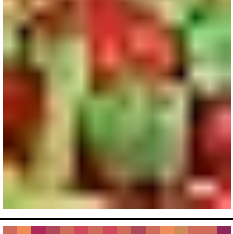
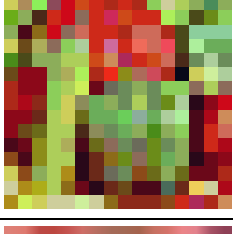
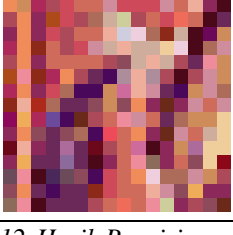
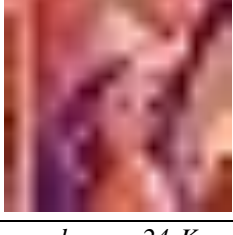
No	Gambar cover	Gambar Stego
a.		
b.		
c.		
d.		
e.		

Table 12 Hasil Penyisipan Pesan dengan 24 Karakter pada Citra Berukuran 16 x16





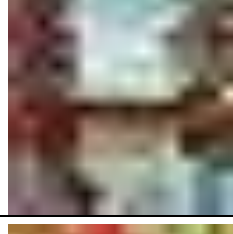
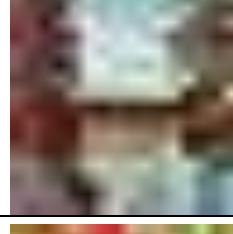
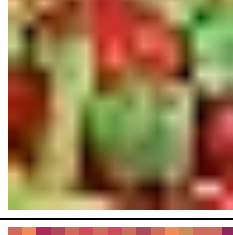
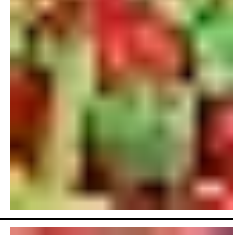
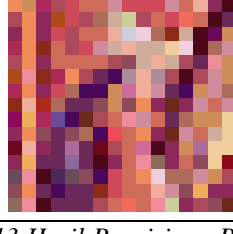

No	Gambar cover	Gambar Stego
a.		
b.		
c.		
d.		
e.		

Table 13 Hasil Penyisipan Pesan dengan 48 Karakter pada Citra Berukuran 16 x 16

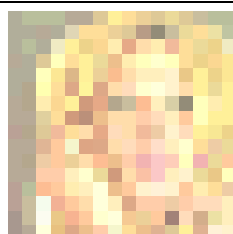
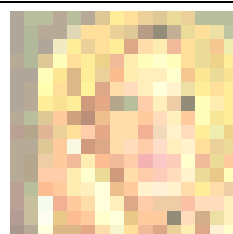
No	Gambar cover	Gambar Stego
a.		



Table 14 Hasil Penyisipan Pesan dengan 89 Karakter pada Citra Berukuran 16 x 16

Jika table-table diatas diamati dan dilihat dengan benar, terdapat sedikit perbedaan saat dilihat secara kasat mata pada citra stego maupun citra *cover*. Hal tersebut membuat kualitas citra stego cukup baik. Tetapi tentunya diperlukan alat ukur untuk menentukan kualitas stego, yaitu *Peak Signal Noise Ratio* (PSNR) dan *Mean Square Error* (MSE). PSNR digunakan untuk membandingkan kualitas citra sebelum dan sesudah dilakukan penyisipan pesan., sedangkan MSE digunakan untuk mengetahui nilai kesalahan kuadrat rata-rata antara citra sebelum dan sesudah.

No	Ukuran	Max	Pesan	MSE	PSNR	Entropy
a.	16 x 16	90	24	0,1276	57,0220	6,5723
b.	16 x 16	90	24	0,1484	56,4154	6,6800
c.	16 x 16	90	24	0,1367	56,7725	7,4858
d.	16 x 16	90	24	0,1549	56,2289	7,5549
e.	16 x 16	90	24	0,1367	56,7725	7,4824
Rata-rata				0,1409	56,6423	7,1551

Table 15 Hasil Pengujian Table 12

No	Ukuran	Max	Pesan	MSE	PSNR	Entropy
a.	16 x 16	90	48	0,2656	53,8881	6,6149
b.	16 x 16	90	48	0,2591	53,9959	6,6788
c.	16 x 16	90	48	0,2382	54,3599	7,4869
d.	16 x 16	90	48	0,2813	53,6399	7,6399
e.	16 x 16	90	48	0,2852	53,5800	7,4941
Rata-rata				0,2659	53,8928	7,1829

Table 16 Hasil Pengujian Table 13

No	Ukuran	Max	Pesan	MSE	PSNR	Entropy
a.	16 x 16	90	89	0,4570	51,5313	6,6604
b.	16 x 16	90	89	0,4805	51,3142	7,5032
c.	16 x 16	90	89	0,4831	51,2907	6,5643
d.	16 x 16	90	89	0,4505	51,5937	7,5174
e.	16 x 16	90	89	0,4596	51,5067	6,6092
Rata-rata				0,4661	51,4473	6,9709

Table 17 Hasil Pengujian Table 14

Ukuran	Max	Pesan	Avg MSE	Avg PSNR	Avg Entropy
16 x 16	90	24	0,1409	56,6423	7,1551
16 x 16	90	48	0,0025	53,8928	7,1829
16 x 16	90	89	0,4661	51,4473	6,9709

Table 18 Ratio Perbedaan Kualitas Nilai MSE dan PSNR berdasarkan Jumlah Pesan yang Disisipkan Pada Citra Berukuran 16 x 16

Berdasarkan Table 18, saat pengujian dilakukan pada citra berukuran 16 x 16 yang dapat menampung sampai 90 karakter pesan, saat lakukan penyisipan pesan sebanyak 24 karakter menghasilkan nilai rata-rata PSNR sebesar 56.6423, saat 48 karakter pesan disipkan nilai rata-rata PSNR bernilai 53.8928 sedangkan nilai rata-rata PSNR yang didapat setelah menyisipkan 89 karakter bernilai 51.4473. Ini berarti nilai rata-rata PSNR tetap berada di atas 40 dB walaupun citra *cover* yang digunakan berukuran kecil dan jumlah karakter yang disisipkan mencapai maksimum karakter.

PSNR (dB)	Kualitas Citra
60	Sangat baik (tanpa derau)
50	Baik (terdapat sejumlah derau tapi kualitas citra masih bagus.
40	Cukup baik (terdapat butiran halus atau seperti salju di dalam citra
30	Kurang baik (terdapat banyak derau)
20	Tidak baik (tidak dapat digunakan)

Table 19 Kualitas Citra berdasarkan Jangkauan PSNR [8]

Dari seluruh pengujian, bahwa nilai PSNR yang didapatkan akan selalu menurun, seiring dengan banyaknya karakter yang disisipkan dengan metode *Least Significant Bit* (LSB) karena semakin banyak karakter pesan yang disisipkan maka akan semakin banyak pula bit yang berubah, namun nilai PSNR akan selalu diatas 40 Db walaupun jumlah karakter yang disisipkan mencapai jumlah karakter yang mampu ditampung oleh citra *cover*, ini terjadi karena setiap karakter yang disisipkan hanya akan merubah 1 bit terakhir pada *cover image*. Ini menunjukkan bahwa citra stego yang dihasilkan baik, meskipun derau terlihat tetapi kualitas citra masih bagus, sesuai dengan Table 19.

V. KESIMPULAN

Dari hasil percobaan, dapat disimpulkan bahwa gabungan dari algoritma Hill Cipher dan metode Least Significant Bit (LSB) menghasilkan kualitas kualitas citra stego yang baik. Metode Hill Cipher akan menyandikan pesan text menjadi ciphertext dengan kunci yang telah ditentukan. Kemudian, ciphertext yang tercipta disisipkan kedalam citra *cover* menggunakan algoritma LSB. Hasil dari pengujian menggunakan PSNR dan MSE, menghasilkan nilai PSNR terkecil 51.4473 dB yang menandakan citra stego yang dihasilkan berkualitas baik dan sulit dibedakan dengan citra *cover*, metode hill cipher yang digunakan juga sulit untuk dipecahkan selama kunci yang digunakan tidak diketahui.

DAFTAR PUSTAKA

- [1] D. R. I. M. Setiadi dan E. H. Rachmawanto, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *Journal of Applied Intelligent System*, vol. 2, pp. 1-11, 2017.
- [2] A. Susanto, D. R. I. M. Setiadi, C. A. Sari dan E. H. Rachmawanto, "Hybrid Method using HWT-DCT for Image Watermarking," *International Conference on Cyber and IT Service Management (CITSM)*, 2017.
- [3] D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto dan C. A. Sari, "Fast and efficient image watermarking algorithm using discrete tchebichef transform," *International Conference on Information Technology for Cyber and IT Service Management (CITSM)*, 2017.
- [4] E. H. Rachmawanto, D. R. I. M. Setiadi, R. S. Amin dan C. A. Sari, "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," *International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2017.
- [5] C. Irawan, D. R. I. M. Setiadi, C. A. Sari dan E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image Using LSB Steganography and OTP Encryption," *1st International Conference on Informatics and Computational Sciences (ICICoS)*, 2017.
- [6] A. Setyono, D. R. I. M. Setiadi dan M. , "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," *4th Int. Conf. on Information Tech., Computer, and Electrical Engineering (ICITACEE)*, 2017.
- [7] M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari dan S. Astuti, "An Improved Secure Image Hiding Technique Using PN-Sequence Based on DCT-OTP," *1st International Conference on Informatics and Computational Sciences (ICICoS)*, 2017.
- [8] S. T, "A Secure DCT Image Steganography Based on Public-Key Cryptography," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, pp. 2039-2043, 2013.
- [9] A. E. Handoyo, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari dan A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *Jurnal Teknologi dan Sistem Komputer*, vol. 6, pp. 37-43, 2018.
- [10] E. Setyaningsih, Kriptografi & Implementasinya Menggunakan MATLAB, Yogyakarta: ANDI, 2015.
- [11] R. Kusumanto dan A. N. Tompunu, "Pengolahan Citra Digital untuk Mendeteksi Obyek menggunakan Pengolahan Warna Model Normalisasi RGB," *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011 (Semantik 2011)*, 2011.
- [12] T. Sutoyo, E. Mulyanto dan V. Suhartono, Teori Pengolahan Citra Digital, Yogyakarta: ANDI, 2009.
- [13] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto dan D. R. I. M. Setiadi, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," *International Conference on Innovative and Creative Information Technology (ICITech)*, 2017.
- [14] M. Sitorus, "Teknik Steganografi dengan Metode Least Significant Bit (LSB)," *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, vol. 11, p. 54, 2015.
- [15] J. I. Sari dan H. T. Sihotang, "Implementasi Penyembunyian Pesan pada Citra Digital dengan Menggabungkan Algoritma Hill Cipher dan Metode Least Significant Bit (LSB)," *Jurnal Manajemen dan Informatika Pelita Nusantara*, vol. 1, pp. 1-8, 2017.
- [16] M. M. Kurdi, A. M. Zeki dan I. A. Elzein, "Least Significant Bit (LSB) and Random Right Circular Shift (RRCF) in Digital Watermarking," *12th International Computer Engineering Conference (ICENCO)*, 2016.

- [17] K. A. Al-Affandy, E.-S. M. El-Rabie, O. S. F. Ahmed Elmhawwy dan G. M. El-Banby, "High Securiy Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography," *IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 400-404, 2016.
- [18] A. M. H. Pardede, H. Manurung dan D. Filina, "Algoritma Vigenere Cipher dan Hill Cipher dalam Aplikasi Keamanan Data pada File Dokumen," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 1, pp. 26-33, 2017.
- [19] A. Kadir dan A. Susanto, *Teori dan Aplikasi Pengolahan Citra*, Yogyakarta: ANDI, 2013.

