STEGANOGRAFI BERBASIS CITRA DIGITAL UNTUK MENYEMBUNYIKAN DATA MENGGUNAKAN KOMBINASI MULTI BIT LSB DENGAN HILL CIPHER

Heliawati Hamrul[1], Awaldi[2], Suhardi[3], Adi Heri[4*]

[1]heliawatihamrul@unsulbar.ac.id, [2]awald1@gmail.com,[3]suhardi@uncp.ac.id, [4*]adiheri@unsulbar.ac.id

[1,2,4]Fakultas Teknik, Program Studi Teknik Informatika, Universitas Sulawesi Barat
[3]Fakultas Teknik Komputer, Program Studi Teknik Informatika, Universitas Cokroaminoto Palopo

ABSTRAK

Penelitian ini bertujuan menghasilkan Steganografi berbasis citra digital menggunakan kombinasi Hill Chipper dan Least Significant Bit untuk pengamanan data. Tahapan penelitian terdiri atas mengidentifikasi masalah, kemudian melakukan studi literatur berkaitan dengan masalah penelitian. Lalu melakukan pengumpulan data atau sampel yang akan diteliti. Sampel yang diteliti adalah pesan atau data berbentuk teks dan cover image (citra penampung) dalam bentuk file.JPEG. Dilanjutkan dengan merancang dan mengimplementasi metode menggunakan sampel yang telah ditentukan. Pada tahap akhir dilakukan pengujian dan analisis terhadap metode yang telah dirancang. Data yang digunakan dalam penelitian ini berupa teks. File tersebut diproses melalui enkripsi, deskripsi dan penyisipan gambar, sedangkan gambar yang digunakan adalah file .JPEG dan .PNG berfungsi sebagai wadah penyisipan file teks. Penelitian ini menggunakan sistem keamanan data kriptografi Hill Cipher dan Steganografi Multi-Bit LSB. Hasil kombinasi algoritma LSB dengan Hill Cipher berhasil dengan baik dan dapat menyembunyikan data hasil enkripsi dari Hill Cipher ke dalam gambar. Pengujian pesan teks menggunakan algoritma Hill Cipher dilakukan sesuai dengan tahapan sehingga diperoleh ciphertext berupa pengacakan huruf abjad. Pesan yang diperoleh dari citra dilanjutkan dengan proses dekripsi yang bertujuan untuk mengembalikan pesan ciphertext ke bentuk semula (plaintext) melalui proses deskripsi algoritma Hill Cipher yang sesuai.

Kata kunci : Hill Cipher; Keamanan Data, Least Significant Bit, Steganografi

1. Pendahuluan

Pesatnya perkembangan teknologi sekarang ini membuat proses penyimpanan data menjadi lebih mudah. Akan tetapi, banyak orang yang kini telah meragukan keamanan apabila data disimpan di perangkat komputer. Hal ini tidak terlepas dari terjadinya berbagai tindakan penyadapan dan pemantauan oleh pihak-pihak yang tidak berkepentingan atau tidak bertanggung jawab sehingga kerahasiaannya kurang terjaga dalam mengamankan suatu data [1]. Ada beberapa seni pengamanan data salah satu di antaranya adalah kriptografi. Dalam kriptografi data/pesan rahasia akan disandikan menjadi karakter acak sehingga walaupun data/pesan diketahui oleh pihak yang tidak berkepentingan, mereka tetap tidak dapat mengetahui informasi yang sebenarnya. Kriptografi *Hill Cipher* (HC) merupakan *polyalphabeticcipher* yang dapat dikategorikan sebagai *blockcipher*, karena teks yang akan diproses dibagi menjadi suatu blok-blok dengan ukuran tertentu. Setiap karakter dalam satu blok dapat mempengaruhi karakter lainnya

dalam proses enkripsi maupun deskripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama pada blok sesudahnya.. Terdapat beberapa alasan mengapa algoritma kriptografi HC sulit untuk dipecahkan. Alasan tersebut adalah: pertama, HC menggunakan perkalian matriks untuk dasar enkripsi dan deskripsinya, jadi abjad pada *plaintext* tidak digantikan oleh abjad yang sama begitu juga dengan *ciphertext* [2]. *Steganografi* digunakan untuk menyembunyikan keberadaan pesan sedemikian rupa sehingga hanya pengirim dan penerima yang tahu akan keberadaannya. *Steganografi* sudah lama digunakan sebagai teknik untuk menyembunyikan pesan ke dalam bentuk berkas yang lain *Steganografi* sering dianggap sebagai pelengkap kriptografi dalam keamanan data [3].

Metode yang digunakan dalam *Steganografi* ini adalah LSB (*least significant bit*) dalam menyisipkan pesan rahasia pada citra. Dalam penelitian ini penulis akan mengacu terhadap permasalahan yang ada pada algoritma LSB dan HC yang sederhana. Oleh sebab itu penelitian ini meneliti tingkat keamanan pesan yang disisipkan pada file citra dengan mengganti metode LSB biasa menjadi *Multi-Bit LSB* dan algoritma kriptografi HC. Proses pengamanan data dengan cara mengenkripsi data berupa teks menggunakan algoritma HC, lalu disisipkan ke dalam bit RGB (*Red, Green, Blue*) dengan metode *Multi-Bit LSB.* Jika *steganolisis* berhasil mendeteksi dan menemukan data yang disisipkan tersebut, maka data tersebut aman karna masih dalam keadaan terenkripsi.

Terdapat beberapa hasil penelitian yang mengkaji tentang *Steganografi* dan HC diantaranya penelitian tentang keamanan data dan penyisipan pesan teks pada gambar menggunakan kriptografi metode HC dan *Steganografi* metode *END of FILE*, penelitian ini berhasil diimplementasikan dalam proses enkripsi dan dekripsi pesan teks yang kemudian akan disisipkan kedalam gambar. Namun pada penelitian ini dihasilkan penurunan kualitas pada gambar [2]. Penelitian yang dilakukan oleh [4], menggunakan *Steganografi* berbasis citra digital untuk menyembunyikan data menggunakan metode LSB. Dengan metode ini teks berhasil disembunyikan ke dalam gambar meskipun mengalami perubahan pada ukuran citra digital namun secara kasat mata perbedaan antara gambar sebelumnya dan sesudah disisipkan pesa tidak terlihat. Selanjutnya penelitian yang dilakukan oleh Miming Mardianti (2019) yang mengombinasikan dua teknik pengamanan data yaitu kriptografi metode *Hill Cipher* (HC) dan *Steganografi* metode *EndofFile* (EoF). Hasil yang didapat dari kombinasi penggabungan kriptografi metode HC dan *Steganografi* metode EoF berhasil diimplementasikan dalam proses enkripsi dan dekripsi pesan teks yang kemudian akan disisipkan ke dalam gambar. Pesan berhasil disisipkan dan diekstrak kembali pada semua sampel gambar baik dengan format *.jpg dan *.png serta pada resolusi 256x256 piksel dan 512x512 piksel. Pada penelitian lain mengkaji teknik keamanan data menggunakan dua algoritma, yaitu untuk memasukkan teks dalam media gambar menggunakan LSB (LeastSignificant Bit) dan Metode biner XOR untuk mengubah pesan menjadi biner dengan kata kunci XOR dan menghasilkan nilai pesan pixel dari 8 bit gambar dengan LSB (Bit paling tidak penting). Data atau teks yang telah disisipkan pada gambar berikutnya akan dikirim ke penerima, dan untuk melihat data asli, penerima pesan harus mendekripsi data dengan kunci yang sama dengan selama proses enkripsi dan penyisipan gambar dan mengambil LSB (*Least Significant Bit*), dari gambar yang

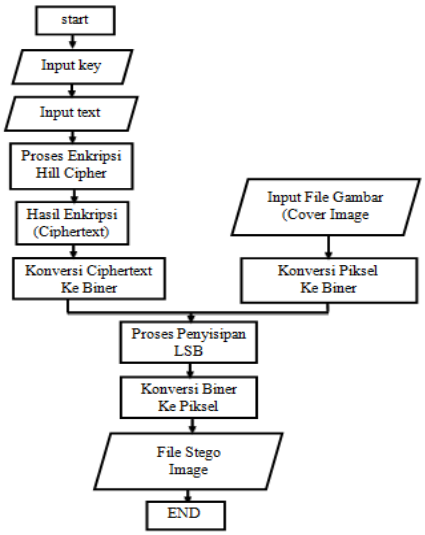
dienkripsi. Berdasarkan hasil dan tes yang dilakukan, maka proses mengenkripsi data dan menyisipkan pesan dalam gambar dapat meminimalkan data atau informasi yang akan dikirimkan atau dikirim ke penerima [5].

2. Metodologi Penelitian

Penggabungan algoritma kriptografi HC dan teknik *Steganografi Multi-Bit* LSB, sehingga dihasilkan pengembangan dari gabungan kedua algoritma tersebut untuk pengamanan pesan/data. Tahapan penelitian terdiri dari mengidentifikasi masalah, kemudian dilakukan studi literatur yang berkaitan dengan masalah penelitian.. Lalu dilakukan pengumpulan data atau sampel yang akan diteliti, dalam hal ini pesan/data dalam bentuk teks dan *cover image* (citra penampung) dalam bentuk *file.JPEG*. Dilanjutkan dengan merancang dan mengimplementasi metode menggunakan sampel yang telah ditentukan. Pada tahap akhir dilakukan pengujian dan analisis terhadap metode yang telah dirancang. Data yang digunakan dalam penelitian ini berupa teks, *file* tersebut akan diproses melalui enkripsi, deskripsi dan penyisipan pada gambar, sedangkan gambar yang akan digunakan adalah *file.JPEG* .PNG akan berfungsi sebagai wadah penyisipan *file* teks. Pada penelitian ini menggunakan alur sistem untuk keamanan data dengan menggunakan kriptografi HC dan *Steganografi Multi-Bit* LSB.

2.1 Proses Enkripsi

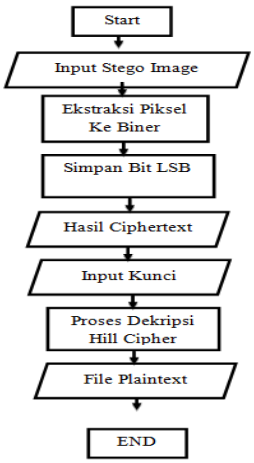
Pada rancangan sistem proses enkripsi dan deskripsi menggunakan algoritma HC, input data *plaintext* yang digunakan berupa teks setelah diubah bentuk menjadi karakter acak. Kemudian hasil enkripsi berupa *ciphertext* akan disisipkan kedalam file citra (*coverimage*) menggunakan teknik Multi-Bit LSB. Adapun diagram alur dalam proses enkripsi untuk sistem keamanan data dengan menggabungkan algoritma HC dan teknik *Steganografi Multi-Bit LSB* adalah seperti berikut :



Gambar 1. Proses Enkripsi Kombinasi HC dan Multi-Bit LSB

2.2 Proses Dekripsi

Untuk proses deskripsi atau pengembalian pesan, *ciphertext* terlebih dahulu diekstrak dari bit-bit *stegoimage.* Selanjutnya dilakukan proses deskripsi dengan metode HC. Adapun diagram alur dalam proses deskripsi untuk sistem keamanan data dengan menggabungkan algoritma HCdan teknik *Steganografi Multi-Bit LSB* adalah seperti berikut :



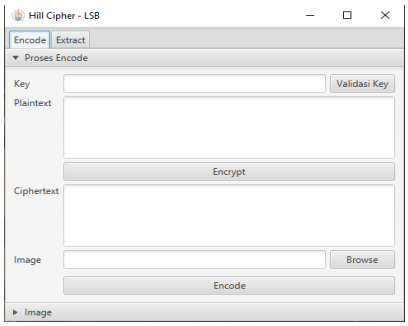
Gambar 2. Proses Deskripsi Kombinasi HC dan *Multi-Bit LSB*

Setelah proses enkripsi dan penyisipan pesan berjalan dengan baik, maka selanjutnya akan dilakukan analisa terhadap *stegoimage* dan ketahanan *filestego* terhadap *noise*. Apakah pesan dapat diekstraksi kembali atau tidak.Untuk mengetahui seberapa besar perubahan citra setelah dilakukan penyisipan pesan dapat digunakan rumus *MeanSquareError* (MSE) dan *Peak SignaltoNoise Rasio* (PSNR).

Gambar 3. Logo Jurnal Media Informatika Budidarma

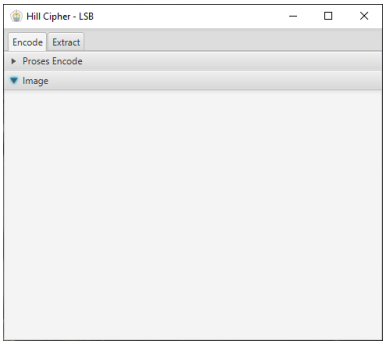
3. HASIL DAN PEMBAHASAN

Pada tab *encode* terdapat proses validasi kunci, proses enkripsi menggunakan *Hill Cipher*, dan proses penyisipan pesan menggunakan LSB. pada tab *encode* juga berisikan *forminputkey*, *forminput* pesan atau *plaintext*, *form* hasil enkripsi atau *ciphertext*, dan *form* nama *file* gambar yang akan dijadikan wadah penyisipan pesan. Adapun tampilan pada tab *encode* ditunjukkan pada gambar 4 sebagai berikut.



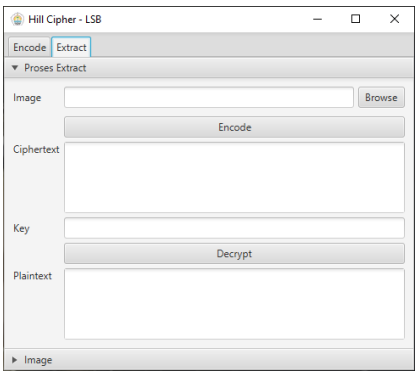
Gambar 4. Tampilan Proses Pada Tab *Encode*

Ccordian image pada tab *encode* berfungsi untuk menampilkan gambar yang akan disisipkan pesan atau wadah penyisipan pesan. Adapun tampilan *accordion iamage* pada tab *encode* ditunjukkan pada gambar 5 sebagai berikut.



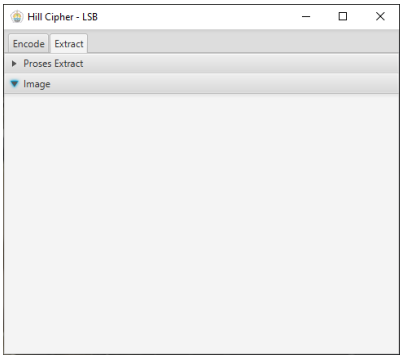
Gambar 5. Tampilan *Accordion Image* Pada Tab *Encode*

Pada tab *extract*ter dapat proses *encode* gambar, dan proses deskripsi *ciphertext.* Tab ekstrak juga berisikan *form* nama *file stegano* (gambar yang telah disisipkan pesan), *form* pesan hasil ekstrak (*ciphertext*), *form input key*, dan *form* hasil deskripsi (*plaintext*). Adapun tampilan tab ekstrak dapat dilihat pada gambar 6 sebagai berikut.



Gambar 6. Tampilan Proses Pada Tab Ekstrak

Accordian image pada tab ekstrak berfungsi untuk menampilkan gambar yang telah disisipkan pesan. Adapun tampilan *accordion image* pada tab ekstrak ditunjukkan pada gambar 7 sebagai berikut.



Gambar 7. Tampilan *Accordion Image* Pada Tab Ekstrak

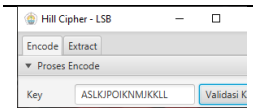
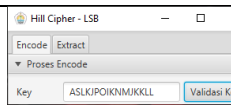
Algorima HC pada dasarnya menggunakan enkripsi perkalian matriks, di mana *key* dan *Plainteks* dikonversi ke dalam bentuk matriks kemudian dikalikan untuk menghasilkan *Ciphertext*. Pembuatan matriks *key* memiliki syarat yakni matriks *key* harus memiliki invers atau determinan matriks *key* tidak boleh sama dengan 0. Jika determinan matriks *key* sama dengan 0 atau matriks *key* tidak memiliki invers maka hasil enkripsi tidak bisa diterjemahkan atau dideskripsi ke dalam bentuk *plaintext* sebelumnya. Oleh sebab itu pada penelitian ini peneliti menambahkan button validasi *key* dengan tujuan membantu pengguna untuk mengecek apakah *key* yang dimasukkan dapat digunakan atau tidak dan jika *key* yang dimasukkan tidak memiliki invers maka secara otomatis sistem akan memberikan *key* yang valid. Ordo *key* matriks yang direkomedasikan oleh sistem akan ditentukan berdasarkan jumlah *key* yang di *input user* yang ditunjukkan pada tabel 1 berikut ini:

Tabel 1. Validasi Key

Input Key	Key Valid/Hasil
ASLKJPOIKNMJKKLL	ASLKJPOIKNMJKKLL

Adapun tampilan *input key* dan hasil validasi *key* pada sistem terlihat pada tabel 2 berikut ini:

Tabel 2. Kunci Sebelum Dan Setelah Divalidasi

Input Key	Key Valid/Hasil
	

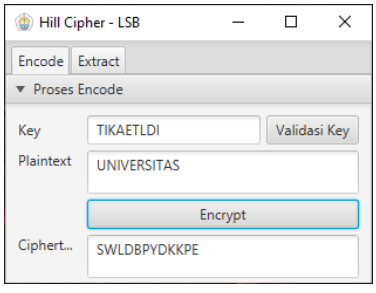
1. Proses Enkripsi Hill Cipher

Setelah *key* atau *password* tervalidasi selanjutnya mengimput pesan yang ingin dienkripsi. *Plaintext* atau pesan yang ingin dienkripsi akan dikonversi menjadi matriks untuk dikalikan dengan matriks *key*. Ordo matriks *plainteks* sama dengan ordo matriks *key*. Jika panjang matriks *PlainText* tidak mencukupi ordo matriks *key* maka matriks *PlainText* akan diisi dengan huruf (x). Panjang *key* akan mempengaruhi *CipherText* atau hasil enkripsi meskipun *PlainText* atau pesan yang dimasukkan sama. Hasil ini ditunjukkan pada tabel 3 berikut ini:

Tabel 3. Hasil Enkripsi

Plaintext	***Key***	**CipherText**
UNIVER	ASLKJPO	MFEZMJ
SITAS	IKNMJKKLL	DCMJPR

Adapun tampilan *input PlainText* dan hasil enkripsi (*CipherText*) dapat dilihat pada gambar 7 berikut.

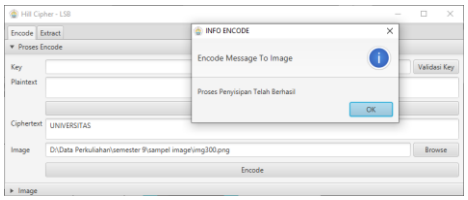


Gambar 7. Proses Enkripsi

Tabel 3. Hasil Encode LSB

CipherText	Format dan Resolusi Citra (WxH)	Hasil Encode
UNIVERSITAS	.png 300x 300	

Adapun tampilan pada sistem dapat dilihat pada gambar 8 berikut.



Gambar 2. Proses Penyisipan Pesan

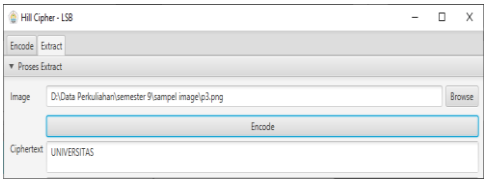
2. Proses Ekstrak LSB

Proses ekstrak digunakan untuk memisahkan *ciphertext* dengan kover gambar sehingga pada proses ini hanya memerlukan satu *forminput*. Gambar yang di ekstrak merupakan gambar hasil dari *encode* yang telah disisipkan *ciphertext*.

Tabel 5. Hasil Extrak LSB

No.	File Stegano	CipherText
1		UNIVERSITAS

Adapun tampilan pada sistem saat melakukan proses penyisipan pesan dapat dilihat pada gambar 9 berikut.



Gambar 3. Proses Ekstrak Gambar

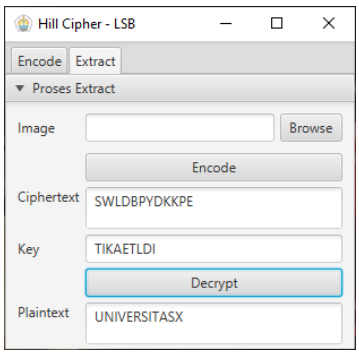
3. Proses Deskripsi Hill Cipher

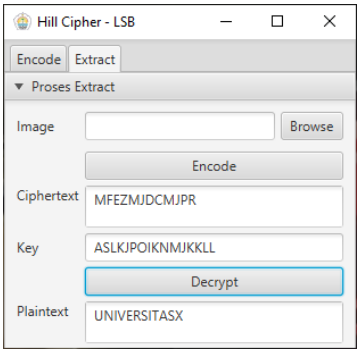
Proses deskripsi dilakukan sama seperti enkripsi namun sedikit berbeda karna pada proses ini tidak perlu melakukan validasi *key*. *User* hanya perlu memasukkan *key* atau *password* yang sama pada saat melakukan enkripsi pesan. Jika *key* untuk deskripsi tidak sama dengan *key* yang digunakan pada saat enkripsi maka hasil *plaintext* nya akan berbeda dengan *plaintext* sebelum dienkripsi, dengan kata lain kita tidak menemukan pesan asli. Setelah mengisi *keyuser* perlu mengisi *ciphertext* yang ingin dideskripsi.

Tabel 4. Hasil Deskripsi

CipherText	*Key*	PlainText
MFEZMJDCMJPR	ASLKJPOIKNMJKKLL	UNIVERSITASX

Adapun tampilan pada sistem pada saat melakukan deskripsi dapat dilihat pada gambar 10 berikut.





Gambar 4. Proses Deskripsi

Pengujian

Pada pengujian ini dicoba menguji tiap-tiap algotritma yang digunakan agar lebih mudah menganalisa kinerja dari setiap algoritma. Hasilnya akan di sajikan dalam bentuk tabel.

1. Pengujian Hill Cipher

Pada algoritma HC akan dilakukan pengujian secara manual, untuk menguji apakah algoritma yang digunakan bekerja sesuai dengan yang diharapkan. Pada pengujian ini sistem akan melakukan enkripsi menggunakan *key* 2x2, 3x3, dan 4x4 dan peneliti juga melakukan enkripsi secara manual untuk mencocokkan hasil enkripsi yang dapat dilihat dalam tabel 7 berikut ini:

Tabel 5. Hasil Enkripsi Sistem

PlanText	*Key* (2x2)	CipherText (Sistem)
INFORMATIKA	QLVR	LZAFOPB LEATB
INFORMATIKA	FLSOJRKEL	NCFFHCP VIWLP
INFORMATIKA	POIUYTGHJ NBVCFGY	YVUFXP GESXJU

2. Pengujian LSB

1) Pengujian pada citra dengan resolusi 100x100

Percobaan pertama menggunakan citra (*img 100.png*) dengan resolusi 100x100 dan ukuran 1,49 kb. Panjang teks yang akan disisipkan di mulai dari 10-100 karakter.

Tabel 6. Penyisipan Teks Pada Citra Img100.Png

Resolusi Citra (W x H)	Panjang Karakter	Nilai MSE	Nilai PSNR
100 x 100	10	9.5E-4	78.3535675 5579062
100 x 100	20	0.0019	75.3432675 991508
100 x 100	30	0.00275	73.7374766 7037648
100 x 100	40	0.00355	72.6285200 7812816
100 x 100	50	0.004575	71.5268926 2465444
100 x 100	60	0.00535	70.8472657 8846681
100 x 100	70	0.006225	70.1894100 5100136
100 x 100	80	0.007125	69.6029549 2187362
100 x 100	90	0.007975	69.1134966 9138691
100 x 100	100	0.008825	68.6736564 6808051

Tabel 8 menunjukkan nilai parameter MSE dan PSNR pada setiap citra dengan jumlah sisipan yang berbeda. Di samping itu citra (*coverimage*) mengalami perubahan ukuran yang awalnya 1,49 kb berkurang menjadi 1,07 kb setelah disisipi 10-90 karakter. Untuk penyisipan 100 karakter berkurang menjadi 1.08 kb.

2) Pengujian pada citra dengan resolusi 200x200

Percobaan kedua menggunakan citra (img200.png) dengan resolusi 200x200 dan ukuran 2,67 kb. Panjang teks yang akan disisipkan di mulai dari 10-100 karakter.

Tabel 9. Penyisipan Teks Pada Citra Img200.Png

Resolusi Citra (W x H)	Panjang Karakter	Nilai MSE	Nilai PSNR

200 x 200	10	2.375E-4	84.37416746907026
200 x 200	20	4.75E-4	81.36386751243045
200 x 200	30	6.875E-4	79.75807658365609
200 x 200	40	8.875E-4	78.64911999140779
200 x 200	50	0.00114375	77.54749253793405
200 x 200	60	0.0013375	76.86786570174644
200 x 200	70	0.00155625	76.21000996428099
200 x 200	80	0.00178125	75.62355483515324
200 x 200	90	0.00199375	75.13409660466654
200 x 200	100	0.00220625	74.69425638136013

Tabel 9 menunjukkan nilai parameter MSE dan PSNR pada setiap citra dengan jumlah sisipan yang berbeda. Di samping itu citra (*coverimage*) mengalami perubahan ukuran yang awalnya 2,67 kb berkurang menjadi 1,99 kb setelah disisipi 10, 20, 30, 50, 80, dan 90 karakter. Untuk penyisipan 40, 60, 70, dan 100 karakter berkurang menjadi 2,00 kb.

3) Pengujian pada citra dengan resolusi 300x300

Percobaan ketiga menggunakan citra (img300.png) dengan resolusi 300x300 dan ukuran 4,18 kb. Panjang teks yang akan disisipkan di mulai dari 10-100 karakter.

Tabel 7. Penyisipan Teks Pada Citra Img300.Png

Resolusi Citra (W x H)	Panjang Karakter	Nilai MSE	Nilai PSNR
300 x 300	10	1.0555555555555555E-4	87.895992650 18387
300 x 300	20	2.111111111111111E-4	84.885692693 54406
300 x 300	30	3.0555555555555555E-4	83.279901764 76973
300 x 300	40	3.9444444444444444E-4	82.170945172 52141
300 x 300	50	5.083333333333333E-4	81.069317719 04769
300 x 300	60	5.944444444444444E-4	80.389690882 86007
300 x 300	70	6.916666666666667E-4	79.731835145 39461
300 x 300	80	7.916666666666666E-4	79.145380016 26687
300 x 300	90	8.861111111111111E-4	78.655921785 78017
300 x 300	100	9.805555555555555E-4	78.216081562 47376

Tabel 10 menunjukkan nilai parameter MSE dan PSNR pada setiap citra dengan jumlah sisipan yang berbeda. Di samping itu citra (*coverimage*) mengalami perubahan ukuran yang awalnya 4,18 kb berkurang menjadi 3,12 kb setelah disisipi 10-100 karakter.

4. KESIMPULAN

Berdasarkan hasil dari penelitian, penyembunyian pesan pada citra digital dengan mengkombinasikan algoritma *hillcipher* dan metode *Least Significant Bit*, dapat diambil beberapa kesimpulan:

1. Hasil dari kombinasi algoritma LSB dengan HC telah berhasil dengan baik dan dapat menyembunyikan data hasil enkripsi dari HC ke dalam gambar.
2. Pengujian pesan teks menggunakan algoritma HC dapat dilakukan sesuai dengan alur atau tahapan-tahapan sehingga memperoleh

ciphertext yang berupa pengacakan huruf abjad.

Pesan yang didapatkan dari citra dilanjutkan dengan dekripsi yang bertujuan untuk mengembalikan pesan *ciphertext* ke bentuk semula (*plaintext)* melalui proses deskripsi algoritma HC yang sesuai.

Daftar Pustaka

[1] Maxim, B. R., & Pressman, R. S. (2014). *Software Engineering: A Practitioner'S* Syahril, M., & Jaya, H. (2019). Aplikasi Steganografi Pengamanan Data Nasabah Di Standard Chartered Bank Menggunakan Metode Least Significant Bit Dan Rc4. 505-506

[2] Mardianti, M., Sutardi, & Aksara, F. (2019). Keamanan Dan Penyisipan Pesan Teks Pada Gambar Dengan Kriptografi Metode Hill Cipher Dan Steganografi Metode End Of File.

[3] Simbolon, G. (2019). Analisis Kinerja Kombinasi Steganografi Multi-Bit Lsb Dengan Algoritma Kriptografi Modified Vernam.fakultas ilmu komputer dan teknologi informasi, medan

[4] Hafiz, A. (2019). Steganografi Berbasisis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb).

[5] Yulius Nahak, T., Friden Elefri, N., & Ariyus, D. (2019). Combination Of Xor Binary Algorithm And Steganography Using Least Significant Bit (Lsb) Method For Data Security. Vol 8, No 2 (2019)

[6] Andika, D., & Darwis, D. (2020). Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi. Jurnal Ilmiah Infrastruktur Teknologi Informasi, 1(2), 19-23.

[7] Darwis, D., Wamiliana, W., & Junaidi, A. (2017). Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End Of File. In Prosiding Seminar Nasional METODE KUANTITATIF 2017 (Vol. 1, No. 1, pp. 228-240). Jurusan Matematika FMIPA Unila.

[8] Kumar, S. (2018). Securing Data At Rest Using Hill Cipher And Xor Based Operations.

[9] Laila, N., & Sinaga, A. S. R. (2019). Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra. ScientiCO: Computer Science and Informatics Journal, 1(2), 47-58.

[10] Munir, R. (2006). Kriptografi. Bandung: Informatika Bandung.

[11] Rismawati , N., & Femy Mulya, M. (2019). Analisis Dan Perancangan Simulasi Enkripsi Dan Dekripsi Pada Algoritma Steganografi Untuk Penyisipan Pesan Text Pada Image Menggunakan Metode Least Significant Bit (Lsb) Berbasis Cryptool2.

[12] Sathish Shet, K., Aswath, A. R., Hanumantharaju, M. C., & Gao, X. Z. (2017). Design and development of new reconfigurable architectures for LSB/multi-bit image steganography system. Multimedia Tools and Applications, 76(11), 13197-13219.

[13] Sharma, N., & Chirgaiya, S. (2014). A novel approach to Hill cipher. International Journal of Computer Applications, 108(11), 975-8887.

[14] Toorani, M., & Falahati, A. (2009, July). A secure variant of the Hill cipher. In 2009 IEEE Symposium on Computers and Communications (pp. 313-316). IEEE.

[15] Utomo, T. P. (2012). Steganografi Gambar dengan Metode Least Significant Bit untuk proteksi komunikasi pada media online (Doctoral dissertation, UIN Sunan Gunung Djati Bandung).

[16] Ziaurrahman, M., Utami, E., & Wahyu Wibwo, F. (2019). Modifikasi Kriptografi Klasik Vigenere Cipher Menggunakanone Time Pad Dengan Enkripsi Berlanjut.