Techno.COM, Vol. 15, No. 2, Mei 2016: 109-116

IMPLEMENTASI METODE STEGANOGRAFI LEAST SIGNIFICANT BIT DENGAN ALGORITMA HILL CIPHER PADA CITRA BITMAP

Naufal Farid[1], Bowo Nurhadiyono[2], Yuniarsi Rahayu[3]
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula I No. 5-11 Semarang, Kode Pos 50131, Telp. (024)3515261, 3520165 Fax:3569684
E-mail : noppal93@gmail.com[1], bnurha@yahoo.com[2], yuniarsi.rahayu@dsn.dinus.ac.id[3]

Abstrak

Masalah keamanan data dan informasi merupakan suatu hal yang sangat penting. Salah satu cara menjaga kerahasiaan data dan informasi adalah dengan teknik kriptografi. Akan tetapi hasil dari kriptografi berupa teks yang acak-acakan sehingga bisa menimbulkan kecurigaan terhadap pihak yang tidak berkepentingan. Salah satu solusi adalah mengkombinasikan kriptografi dengan steganografi. Penggunaan metode Hill Cipher dan Least Significant Bit (LSB) meningkatkan keamanan pesan rahasia. Pesan rahasia dienkripsi dengan algoritma Hill Cipher sebelum disisipkan dalam citra digital dengan metode LSB. Penelitian ini bertujuan untuk menyembunyikan pesan rahasia pada citra digital sekaligus menganalisa kualitas citra stego hasil penggabungan metode kriptografi Hill Cipher dan metode steganografi LSB dengan pengujian visual, PSNR dan pengujian ketahanan terhadap perubahan citra. Hasil pengujian visual citra hasil steganografi tidak mengalami perubahan banyak jika dilihat secara kasat mata,akan tetapi semakin banyak karakter pesan yang disisipkan maka nilai PSNR dan kualitas citra semakin menurun. Pada pengujian ketahanan, citra tidak dapat bertahan dari manipulasi atau perubahan pada citra, karena pesan pada citra stego tidak dapat diekstrak dengan sempurna dan plaintext hasil dekripsi tidak sesuai dengan plaintext asli.

Kata Kunci: *Kriptografi, Steganografi, Hill Cipher, Least Significant Bit*

Abstract

Security of data and information is a very important thing. One way to maintain the confidentiality of data and information is cryptography. But the results of the cryptographic text disheveled that could arouse suspicion against those who are not entitled to it. One solution is to combine cryptography with steganography. The use of the method Hill Cipher and Least Significant Bit (LSB) enhance the security of confidential messages. Secret messages encrypted with algorithms Hill Cipher before inserted in the digital image with the LSB method. This study aimed to hide secret messages in digital images simultaneously analyze stego image quality resulting from this combination Hill Cipher cryptography method and LSB steganographic method with visual testing, PSNR and testing of resistance to changes in the image. visual testing results stego image did not change when seen with eyes, but the more characters of message is pasted value of PSNR and quality of the image decreases. In the endurance test, the image can not survive from manipulation in the image, because the message of stego image can not be extracted perfectly and plaintext decryption result is not in accordance with the original plaintext.

Keywords: *Cryptography, Steganography, Hill Cipher, Least Significant Bit.*

1. PENDAHULUAN

Perkembangan teknologi informasi sangat cepat dan berpengaruh banyak bagi umat manusia. Perlunya keamanan data sangat dibutuhkan pada era teknologi seperti saat ini. Berkembangnya ilmu yang pesat dapat memunculkan cara-cara baru bagi beberapa pihak yang berniat menyalah gunakan untuk mengancam keamanan informasi seperti *hacker, cracker, carder, phreaker* dan sebagainya. Apabila informasi berada pada pihak yang salah akan menimbulkan kerugian. Informasi yang harus diperhatikan adalah keamanan bagi informasi yang rahasia[1]. Metode kriptografi dapat menjamin keamanan data informasi tersebut dengan cara mengenkripsi data tersebut dengan mengubahnya menjadi kode-kode acak yang bersifat random sehingga membuat data tersebut tidak dapat dibaca dan dimengerti oleh pihak lain [2]. Tetapi penggunaan metode enkripsi tersebut tidak selalu menjamin keamanan data tersebut dikarenakan data tersebut acak-acakan dengan kata lain dapat dianggap sebagai hal yang tidak lazim dan mencurigakan. Untuk menghindari permasalahan tersebut maka lahirlah steganografi untuk penyembunyian datanya, yang mengacu pada seberapa besar ketidakmampuan pihak ketiga dalam mendeteksi keberadaan informasi yang tersembunyi [3]. Steganografi adalah teknik penyembunyian data dalam sebuah medium yang dapat berupa jenis data apapun seperti file citra gambar, audio, video, maupun jenis data yang lainnya. Dalam hal ini penulis menggunakan metode kriptografi *Hill Cipher*. *Hill Cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Karena *Hill Cipher* tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya [1]. Dan dalam steganografi penulis menggunakan metode *Least Significant Bits (LSB),* metode ini dapat menyimpan file text pada bit yang paling rendah pada *pixel* gambar sehingga gambar yang telah disisipkan pesan tidak terlihat terjadi perubahan dan tidak menimbulkan curiga [4]

2. METODE

2.1 Jenis Penelitian

Penelitian ini adalah penelitian yang berjenis eksperimental. Penelitian eksperimental adalah penelitian dengan mencatat langsung hasil pengujian atau percobaanya dalam pengumpulan data. Untuk mendapatkan kesimpulan dilakukan pengujian visual, PSNR, dan pengujian ketahanan pada citra hasil metode kriptografi dan steganografi.

2.2 Sumber Data

Penelitian ini menggunakan data objek berupa citra yang mempunyai ekstensi bitmap (.bmp) dan citra bitmap tersebut beresolusi 512 x 512 piksel yang berasal dari internet.

2.3 Analisis Data

Pada proses penyisipan (enkripsi) teks ke dalam gambar, memilih file teks (*plaintext*) yang akan disisipkan dan dilanjutkan dengan menentukan kunci matriks *Hill Cipher.*

$C = K \cdot P$
C = Ciphertext
K = Kunci matriks
P = Plaintext

Setelah itu memilih *cover image*, nilai intensitas *pixel* citra pada *cover image*

akan dikonversi ke biner (8-bit). bit paling belakang dari nilai biner *cover image* disisipi nilai biner dari *ciphertext*. Dengan demikian pada setiap *pixel* file gambar BMP 24 bit dapat disisipkan 3 bit pesan, misalnya terdapat data *raster* original file gambar adalah sebagai berikut :

00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001

Sedangkan representasi biner huruf A adalah 01000001, dengan menyisipkannya ke dalam *pixel* di atas maka akan dihasilkan

00100110 11101001 11001000
00100110 11001000 11101000
11001000 00100111 11101001

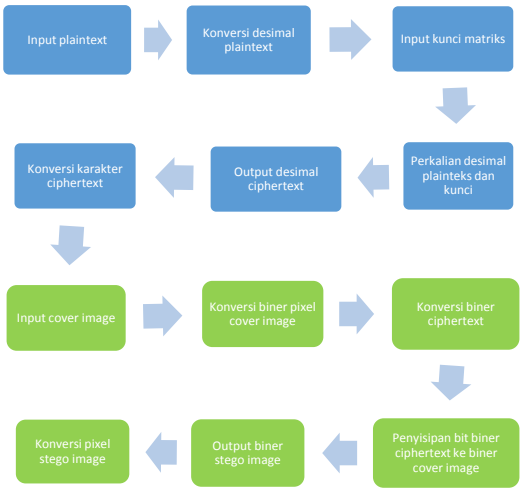
Terlihat pada bit ke delapan, enambelas dan 24 diganti dengan representasi biner huruf. Sedangkan pada proses ekstraksi (dekripsi) teks yang terkandung di dalam *stego image* dipilih dan nilai intensitas *pixel* citra akan dikonversi ke biner 8 bit. Kunci matriks dimasukkan untuk mencari modular invers yang akan dikalikan dengan matriks kunci invers guna mendapatkan matriks kunci baru.

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

Menjadi persamaan proses dekripsi:

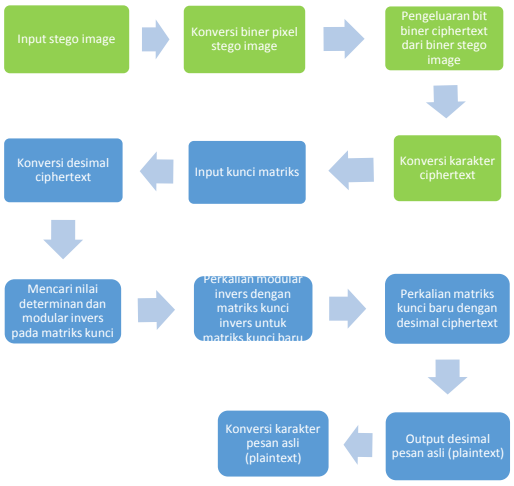
$P = K^{-1}.C$

2.4 Metode Yang Diusulkan



Gambar 1. Enkripsi Embed

Pada tahap enkripsi embed memasukkan pesan rahasia (*plaintext*) yang ingin disembunyikan dalam gambar. *Plaintext* dikonversi ke desimal berdasarkan ASCII. Memasukkan kunci matriks untuk proses enkripsi. Mengalikan setiap dua nilai desimal *plaintext* dengan kunci matriks secara berulang sampai nilai desimal *plaintext* terakhir. Perkalian menghasilkan nilai desimal *ciphertext*. Proses enkripsi diakhiri dengan konversi nilai desimal *ciphertext* ke karakter sehingga menghasilkan sebuah pesan acak-acakan (*ciphertext*). Menginputkan sebuah *cover image* sebagai awal tahap embed. Nilai intensitas *pixel cover image* dikonversi menjadi biner. *Ciphertext* yang didapatkan dari proses enkripsi dikonversi juga menjadi biner. Bit-bit biner *ciphertext* dipisah dan disisipkan untuk menggantikan bit paling belakang dari setiap *byte* di biner *cover image*. Proses penyisipan menghasilkan nilai biner penyusun *stego image*. Nilai biner dikonversi menjadi nilai intensitas *pixel* lagi sehingga menghasilkan sebuah *stego image*. Proses enkripsi *embed* sukses.



Gambar 2. Ekstrasi Dekripsi

Memilih *stego image* yang akan diekstraksi dekripsi. Nilai intensitas *pixel stego image* dikonversi ke biner. Proses ekstraksi berlangsung untuk mengeluarkan bit biner *ciphertext* dari biner *stego image.* Nilai biner *ciphertext* yang didapatkan dari proses ekstraksi dikonversi ke karakter sehingga menghasilkan pesan yang acak-acakan. Memasukkan kunci matriks untuk tahap dekripsi. *Ciphertext* dikonversi ke desimal. Mencari determinan dan modular invers dari kunci matriks yang diinputkan. Mengalikan modular invers dengan kunci matriks yang sudah diinvers untuk mendapatkan kunci matriks baru. Matriks kunci yang didapatkan dikalikan dengan nilai desimal *ciphertext.* Menghasilkan nilai desimal dari pesan asli (*plaintext*). Nilai desimal *plaintext* dikonversi menjadi karakter sehingga menampilkan pesan. sesungguhnya. Proses ekstraksi dekripsi sukses

2.5Pengujian

Pengujian dengan objek citra digital dengan tujuan untuk mengetahui kemampuan maksimal dari teknik *Hill Cipher* dan LSB terhadap komputasi saat proses enkripsi *embedding* dan dekripsi *extracting* terhadap kualitas citra. Salah satu pengujian yaitu PSNR:

$$\mathrm{MSE} = \frac{1}{M\,N}\sum_{y=1}^{M}\sum_{x=1}^{N}[\mathrm{I}\,(x,y) - \mathrm{I}'(x,y)]^2$$

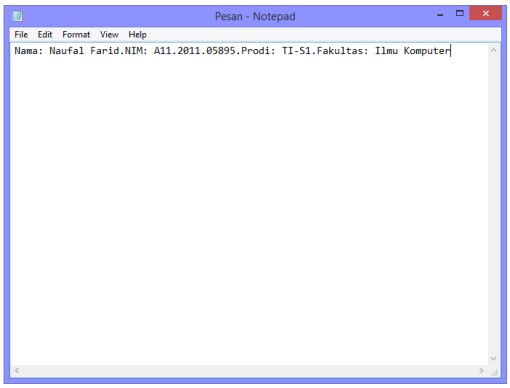
$$PSNR = 10\log_{10}\left(\frac{MAXi^2}{MSE}\right) \quad (1)$$

3. HASIL DAN PEMBAHASAN

Dalam pengujian dari algoritma *Hill Cipher* dan LSB bisa digunakan data set berupa citra digital berformat BMP dengan resolusi gambar 512 x 512 8 bit dan sebuah file teks(.txt) yang didalamnya telah tertulis sebuah pesan yang disisipkan penemuan secara logis.

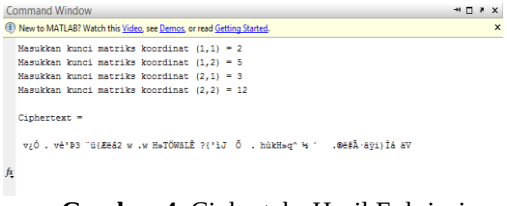
3.1 Penyisipan Pesan

Sebuah pesan yang berisi data penulis yang berjumlah 75 karakter dijadikan plainteks dalam penelitian ini.



Gambar 3. Plainteks Yang Akan Disisipkan

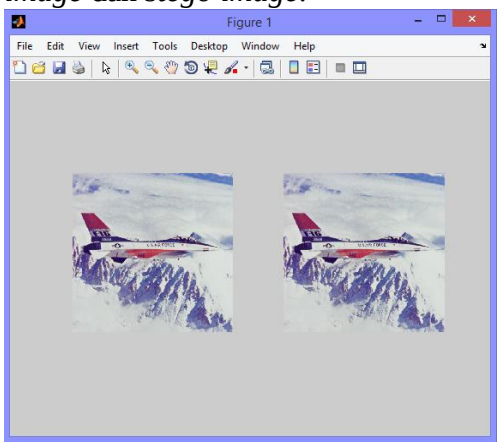
Proses enkripsi *Hill Cipher* berlangsung setelah kunci matriks dimasukkan dan menghasilkan sebuah *cipherteks* yang acak.



Gambar 4. Cipherteks Hasil Enkripsi

Proses *embed* LSB berlangsung untuk menyisipkan *cipherteks* ke dalam

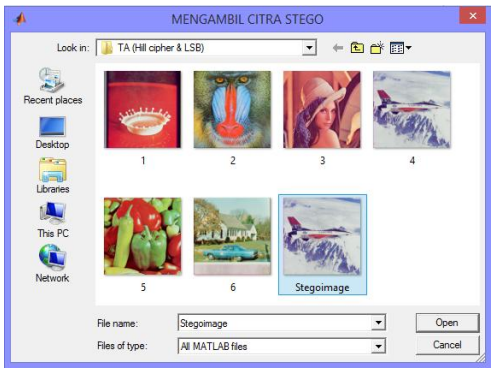
gambar. Penyisipan berhasil dan keluar tampilan berupa perbandingan *cover image* dan *stego image*.



Gambar 5. Cover Image dan Stego Image

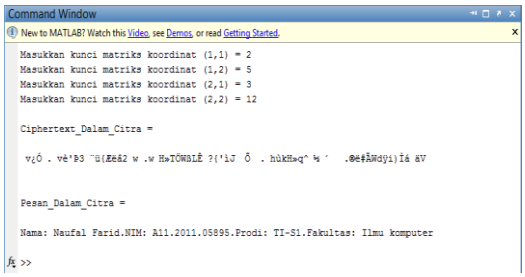
3.2 Pengeluaran Pesan

Mengambil *stego image* yang akan diproses ekstrasi dan dekripsi guna mendapatkan pesan asli kembali dari dalam gambar.



Gambar 6. Mengambil Stego Image

Proses ekstrasi LSB berlangsung dan memasukkan kunci dekripsi *Hill Cipher*. Output berupa *cipherteks* yang sekaligus didekripsi dan menjadi plainteks yang asli. Pesan asli berhasil dikeluarkan dari *stego image.*



Gambar 7. Hasil Ekstrasi Dekripsi

3.3 Pengujian Visual

Dengan pengujian visual dapat dilihat dengan kedua mata nampak tidak terlihat perbedaan sedikitpun dari *cover image* dan *stego image* yang dibandingkan.

Tabel 1: Pengujian Visual

Citra Asli	Citra Hasil Penyisipan
	

3.3 Pengujian PSNR

Setelah uji perhitungan PSNR dengan menyisipkan beberapa sampel dengan jumlah karakter plainteks yang berbeda, maka mendapatkan hasil seperti berikut.

Tabel 2: Pengujian PSNR

Jumlah Karakter	PSNR (db)
75	88,18
95	87,13
115	86,37
135	85,59
170	84,71

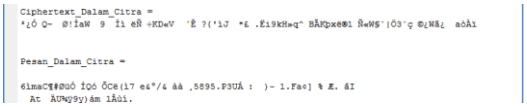
Semakin banyak jumlah karakter pesan yang disisipkan ke dalam citra stego maka nilai PSNR akan semakin menurun.

3.4 Pengujian Ketahanan

Pengamatan ini, manipulasi atau perubahan citra yang dlakukan yaitu perubahan pada kecerahan, ketajaman, rotasi dan *resize.*

3.4.1 Perubahan Kecerahan

Perubahan kecerahan pada citra stego, menggunakan 4 sampel yang mempunyai tingkat kecerahan yang berbeda. Jika plainteks yang berada dalam *stego image* berhasil diekstrak dan dekrip dengan sempurna, maka data tidak rusak akibat perubahan kecerahan.



Gambar 8. Contoh Hasil Ekstrasi Stego Image Brightness -5

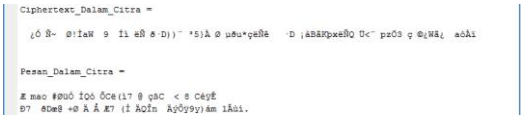
Hasil pengamatan dengan manipulasi beberapa tingkat kecerahan mendapat kesimpulan *stego image* tidak tahan terhadap manipulasi kecerahan citra dari tingkat -5 sampai +25, dikarenakan plainteks dalam *stego image* tidak bisa diekstrak dan dekrip dengan sempurna. Data plainteks tersebut telah rusak akibat perubahan tingkat *brightness* pada *stego image.* Nilai PSNR citra yang didapat akan semakin menurun dengan semakin banyaknya tingkat perubahan nilai *brightness*.

Tabel 3: Pengujian Perubahan Brightness

Nilai Ketajaman	Hasil Uji	Hasil PSNR (db)
-5	Failed	48,74
+5	Failed	48,74
+10	Failed	42,79
+25	Failed	33,88

3.4.2 Perubahan Ketajaman

Perubahan ketajaman pada citra stego, menggunakan 4 sampel yang mempunyai tingkat ketajaman yang berbeda. Jika plainteks yang berada dalam stego image berhasil diekstrak dan dekrip dengan sempurna, maka data tidak rusak akibat perubahan ketajaman.



Gambar 9. Contoh Hasil Ekstrasi Stego Image Contrast -5

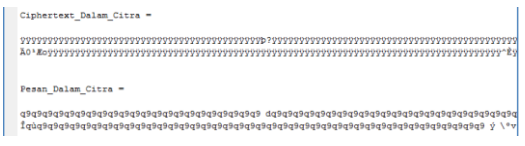
Hasil pengamatan dengan manipulasi beberapa tingkat ketajaman mendapat kesimpulan *stego image* tidak tahan terhadap manipulasi ketajaman citra dari tingkat -5 sampai +25, dikarenakan plainteks dalam *stego image* tidak bisa diekstrak dan dekrip dengan sempurna. Data plainteks tersebut telah rusak akibat perubahan tingkat *contrast* pada *stego image*. Nilai PSNR citra yang didapat akan semakin menurun dengan semakin banyaknya tingkat perubahan nilai *contrast*.

Tabel 4: Pengujian Perubahan Contrast

Nilai Kecerahan	Hasil Uji	Hasil PSNR (db)
-5	Failed	32,24
+5	Failed	32,33
+10	Failed	27,63
+25	Failed	21,87

3.4.3 Perubahan Rotasi

Perubahan rotasi pada citra stego, menggunakan 4 sampel yang mempunyai derajat rotasi yang berbeda. Jika plainteks yang berada dalam *stego image* berhasil diekstrak dan dekrip dengan sempurna, maka data tidak rusak akibat perubahan rotasi.



Gambar 10. Contoh Hasil Ekstrasi Stego Image Rotasi 45°

Hasil pengamatan dengan manipulasi beberapa tingkat rotasi mendapat kesimpulan *stego image* tidak tahan terhadap manipulasi rotasi citra dari

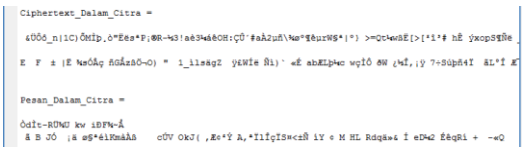
tingkat 45° sampai 180°, dikarenakan plainteks dalam *stego image* tidak bisa diekstrak dan dekrip dengan sempurna. Data plainteks tersebut telah rusak akibat perubahan tingkat rotasi pada *stego image*. Nilai PSNR pada saat rotasi 45° dan 135° tidak dapat dihitung oleh aplikasi PSNR Calculator dikarenakan ukuran pada rotasi 45° dan 135° berubah menjadi 725 x 725 px yang diakibatkan kemiringan citra sehingga citra stego tidak sesuai dengan citra yang asli yang berukuran 512 x 512. Sementara pada saat perubahan rotasi 90° dan 180° didapat nilai PSNR sebesar 11,83 db dan 11,26 db.

Tabel 5: Pengujian Perubahan Rotasi

Nilai Rotasi (derajat)	Hasil Uji	Hasil PSNR (db)
45	Failed	Incompatible size
90	Failed	11,83
135	Failed	Incompatible size
180	Failed	11,26

3.4.4 Perubahan Ukuran (Resize)

Perubahan ukuran atau *resize* pada citra stego, menggunakan 4 sampel yang mempunyai ukuran yang berbeda. Jika plainteks yang berada dalam *stego image* berhasil diekstrak dan dekrip dengan sempurna, maka data tidak rusak akibat *resize.*



Gambar 11. Contoh Hasil Ekstrasi Stego Image Resize 120 x 120 px

Hasil pengamatan dengan manipulasi beberapa tingkat ukuran mendapat kesimpulan *stego image* tidak tahan terhadap manipulasi ukuran citra dari tingkat 120 x 120 px sampai 1024 x 1024 px, dikarenakan plainteks dalam *stego image* tidak bisa diekstrak dan dekrip dengan sempurna. Data plainteks tersebut telah rusak akibat perubahan *size* pada stego image. Nilai PSNR pada semua sample manipulasi perubahan *size* tidak dapat dihitung oleh aplikasi PSNR Calculator dikarenakan ukuran piksel citra stego tidak sesuai dengan citra yang asli yang mempunyai ukuran 512 x 512 px.

Tabel 6: Pengujian Perubahan size

Nilai Pixels (px)	Hasil Uji	Hasil PSNR (db)
120 x 120	Failed	Incompatible size
480 x 480	Failed	Incompatible size
720 x 720	Failed	Incompatible size
1024 x 1024	Failed	Incompatible size

4. KESIMPULAN DAN SARAN

Dari pengujian yang telah dilakukan dalam pengamatan ini, penulis mendapat kesimpulan sebagai berikut :

1. Penggabungan metode kriptografi *Hill Cipher* dan steganografi *Least Significant Bit* (LSB) dapat meningkatkan keamanan pada pesan dalam bertukar informasi.
2. Pengimplementasian metode *Hill Cipher* dengan *Least Significant Bit*(LSB) dari pengujian visual kualitas dari citra sebelum dan sesudah disisipkan pesan melalui proses steganografi tidak terlihat perbedaannya dan tidak terlihat banyak mengalami perubahan. Dan dari pengujian PSNR semakin banyak jumlah karakter pesan yang disisipkan ke dalam citra stego maka

nilai PSNR akan semakin menurunyang artinya kualitas citra semakin jelek.

3. Dari pengujian *stego image* yang dilakukan yaitu manipulasi nilai kecerahan, ketajaman, rotasi dan ukuran, *plaintext* hasil proses ektrasi dekripsi berantakan dan tidak sesuai dengan *plaintext* yang asli, hal itu berarti pesan pada citra stego rusak tidak bisa diekstraksi dengan sempurna. Sehingga menghasilkan kesimpulan bahwa citra stego tidak dapat bertahan dari perubahan atau manipulasi.

Adapun saran penelitian sebagai berikut:

1. Penelitian menggunakan citra bitmap yaitu yang berekstensi (.bmp) sebagai *cover image*, Untuk pengembangan bisa diperluas lagi menggunakan format yang lain seperti PNG dan JPG.
2. Media penyembunyian pesan dalam pengamatan menggunakan gambar/citra digital, untuk selanjutnya bisa dikembangkan dengan mengunakan media lain misalnya video dan audio.
3. Pengujian *stego image* dalam pengamatan hanya memanipulasi nilai *brightness*, *contrast*, *resize* dan *rotation.* Dapat dikembangkan lagi dengan pengujian lain seperti memanipulasi *exposure* dan *saturation.*

DAFTAR PUSTAKA

[1] Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. STIMIK Budi Dharma.

[2] Nikken Prima Puspita. (2013). Kriptografi Hill Cipher Dengan Menggunakan Operasi Matriks. Universitas Diponegoro.

[3] Y. Kurniawan, Kriptografi Keamanan Internet dan Jaringan Telekomunikasi, Bandung: Informatika, 2004.

[4] Utomo, T. P. (2011). Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online. UIN Sunan Gunung Djati Bandung.