IMPLEMENTASI PENGAMANAN DATA MENGGUNAKAN METODE KRIPTOGRAFI *HILL CIPHER* DAN STEGANOGRAFI *LEAST SIGNIFICANT BIT* (LSB) PADA MEDIA CITRA DIGITAL

Samy Y. Doo[1], Silvester Tena[2], Varly M Ndolu [3]

[1,2,3]*Jurusan Teknik Elektro Fakultas Sains dan Teknik Universitas Nusa Cendana*
Jalan Adisucipto-Penfui Kupang, Telp. (0380) 881557, HP.081239898101
Email: samyeverson@staf.undana.ac.id

ABSTRACT

Security in data exchange becomes absolutely necessary today. One way to do this is to use cryptography. The main force of cryptography is to randomize the message so that even if the message can be intercepted but not necessarily readable. This is at once a disadvantage because the random message can be thought to contain important information that is interesting to be analyzed far. To overcome such deficiencies, steganography becomes an interesting thing to combine. The merging method of Hill Cipher dan Least Significant Bit (LSB) method can give double protection to the data in an image or digital image. The results showed that Citra that has been through the process of steganography LSB looks the same as the original image so it is very difficult to distinguish. The MSE and PSNR values of the Stego result are best generated with the MSE 0.000306 value and the PSNR value of 83,305 dB. When without an attack (noise), the combination results in the message with the Hill Cipher Cryptographic method andthe LSB steganography method go well. At the moment of addition attack Salt and pepper noise qualitativechanges in the image. The lowest MSE and PSNR values are MSE 6.4620 and PSNR 40,061 dB.

***Keywords**: cryptography, Steganography, LSB, Hill Cipher, Salt and pepper noise*

ABSTRAK

Keamanan dalam pertukaran data menjadi hal yang mutlak diperlukan saat ini. Salah satu cara melakukannya adalah dengan menggunakan kriptografi. Kekuatan utama kriptografi adalah mengacak pesan sehingga sekalipun pesan tersebut dapat disadap tetapi tidak serta merta dapat dibaca. Hal ini sekaligus menjadi kelemahannya karena pesan yang acak tersebut bisa diduga berisi informasi penting yang menarik untuk dianalisa lebih jauh. Untuk mengatasi kekurangan tersebut maka steganografi menjadi hal menarik untuk dikombinasikan. Penggabungan metode Hill Cipher dan metode Least Significant Bit (LSB) dapat memberikan proteksi ganda pada data dalam sebuah gambar atau citra digital.
Hasil penelitian menunjukan bahwa citra yang sudah melalui proses steganografi LSB terlihat samadengan citra asli sehingga sangat sulit dibedakan. Nilai MSE dan PSNR citra hasil stego terbaik dihasilkandengan nilai MSE 0.000306 dan nilai PSNR 83.305 dB. Bila tanpa attack (noise), hasil kombinasi pada pesan dengan metode kriptografi Hill Cipher dan metode steganografi LSB berjalan baik. Pada saat penambahan attack berupa noise salt and pepper secara kualitatif terjadi perubahan pada citra. Nilai MSEdan PSNR terendah yakni MSE 6.4620 dan PSNR 40.061 dB.

***Kata kunci** : Kriptografi, Steganografi, LSB, Hill Cipher, salt and pepper noise*

1. PENDAHULUAN

Dewasa ini internet merupakan media komunikasi data yang sangat diperlukan mulai dari sekedar mencari informasi terbaru, transaksi bisnis, penawaran jasa dan lain-lain. Kemudahan dalam penggunaan serta fasilitas yang lengkap membuat internet menjadi populer di kalangan masyarakat sekarang ini. Akan tetapi seiring berkembangnya media komunikasi yang menggunakan internet maka bertambah pula

kejahatan pada internet. Permasalahannya adalah jika informasi tersebut bersifat rahasia dan hanya boleh diketahui oleh pihak tertentu maka dibutuhkan pengamanan pada datatersebut. Tujuannya supaya data yang dibawanya bisa diambil tetapi tidak dapat dibaca atau dimengerti. Cara yang bisa dilakukan untuk mengamankan data tersebut adalah dengan menggunakan metode kriptografi. Intinya data diacak sedemikian rupa agar tidak dapat dimengerti oleh yang tidak berhak [1-3].

Pada dasarnya, kriptografi memiliki dua prosesyaitu enkripsi dan dekripsi. Pesan yang dapat dibaca disebut *plaintext*, sedangkan teknik untuk membuat pesan tidak dapat dibaca disebut enkripsi. Pesan yang sudah melewati tahap enkripsi disebut *ciphertext*. Setelah itu, pesan akan dikirim ke tujuan dan pesan akan didekripsi. Dekripsi adalah teknik mengubah *ciphertext* menjadi *plaintext*, dan diperlukan *key* yaitu kode yang digunakan untuk melakukan enkripsi atau dekripsi suatu pesan. Kriptografi hanya membuat pesan menjadi acak dan tidak dapat dibaca. Keadaan ini tertunya menimbulkan ketertarikan orang untuk mencoba menemukan pesan dibalik data acak tersebut. Hal inilah yang menjadi kelemahan utama kriptografi. Untuk mengatasi hal tersebut maka sebuah ciphertext disembunyikan dalam media yang sama ataupun berbeda. Teknik ini dikenal dengan nama steganografi.. Steganografi adalah seni dan ilmu menyembunyikan data pada media lain sebagai *cover* sehingga terlihat samar [4].

Pada penelitian ini, metode kriptografi menggunakan algoritma *Hill Cipher*. Algoritma ini merupakan salah satu algoritma kriptografi yang memanfaatkan aritmatika modulo dan matriks [5, 6]. Setiap karakter pada *plaintext* dan *ciphertext* dikonversikan ke dalam angka. *Hill Cipher* memanfaatkan matriks *n x n* sebagai kunci.Setelah itu pesan akan disembunyikan dengan teknik steganografi. Dalam hal ini, pesan akan ditumpangkan ke media stegano yang dapatberupa *file image* atau audio sehingga orang lain tidak dapat mengetahui bahwa di dalam media tersebut terdapat pesan rahasia. Upaya untuk meminimalisir perubahan kualitas *cover* dapat dilakukan dengan penyisipan pada bit terakhir (*Least Significant Bit*) [7-9].

2. METODE PENELITIAN

Pada penelitian ini dilakukan beberapa kombinasi percobaan untuk melihat pengaruh jumlah bit informasi yang diproses dengan kriptografi dan steganografi terhadap kualitas citra yang dipakai sebagai media stegano. Beberapa perlakuan tersebut termasuk dengan penambahan sinyal acak atau noise ke gambar yang dipakaisebagai media stegano. Contoh penambahan noise pada gambar 1.Terlihat bahwa ada perubahan yang signifikan akibat noise gaussian tersebut.

Gambar 1. Citra yang terkena *noise Gaussian*

Gambar 2. memperlihatkan perubahan yang lebih parah akibat noise *salt and pepper*.

Salt and Pepper noise juga sering disebut *impuls noise*, merupakan *noise* yang disebabkangangguan yang tajam dan tiba-tiba pada sinyal citra. Citra akan tampak berupa titik-titik(piksel) hitam atau putih (atau keduanya yang tersebar pada citra). Pada penelitian ini digunakan noise salt and pepper sebagai pengganggu untuk melihat apakah data yang dirusak dengan noise tersebut masih bisa dibacaatau tidak setelah diekstrak kembali.

Gambar 2. Citra yang terkena *noise salt and pepper*

1. Parameter Pengujian

2.1.1 Mean Square Error (MSE)

MSE merupakan tolak ukur analisiskuantitatif yang digunakan untuk menilai kualitas sebuah citra keluaran dan keunggulan sebuah metode yang digunakan. Ukuran matriks citra m * n, B_1 dan B_2 merupakan matriks citra. Dengan kata lain *Mean Square Error* (MSE) adalah kesalahan kuadrat rata- rata sinyal-sinyal piksel citra hasil pemrosesan sinyal terhadap sinyal asli. Untuk nilai terbaik MSE adalah sama

dengan nol. MSE dapatdirumuskan sebagai berikut:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(B_1(i,j) - (B_2(i,j)^2 \quad (2.8)$$

Dimana :

m : baris matriks citra hasil pemrosesan

n : kolom matriks citra hasil pemrosesan

B_2 : piksel citra hasil pemrosesan

B_1 : piksel citra asli

2.1.2 *Peak Signal to Noise Ratio (PSNR)*

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut, dalam satuan desibel (dB). Semakin besar parameter PSNR semakin mirip dengan citra asli(Hidayat,2013). Untuk menentukan nilai PSNR digunakan persamaan berikut ini:

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

Adapun kriteria kualitas citra dilihat dari PSNR terdapat pada Tabel 1.

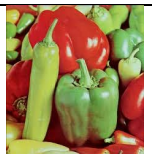
Tabel 1. Kriteria kualitas Citra dari nilai PSNR (*Intenational Journal of Database Manage System* Vol 4**.** IEEE)

Cover image	Stego Image	Amount of data embedded	MSE %	PSNR (dB)	Amount of data extracted
clover (35 KB)	stegclover (35 KB)	4267 bytes	0.48	51.28	4267 bytes
flower (43 KB)	stegflower (43 KB)	4513 bytes	0.41	51.93	4513 bytes
bud (47 KB)	stegbud (47 KB)	5075 bytes	0.43	51.69	5075 bytes

Secara umum, nilai PSNR dengan kisaran di bawah 30 dB termasuk dalam *low quality* dan terdapat banyak distorsi pada citra hasil penyisipan pesan. Pada tabel diatas nilai PSNR berada pada nilai konsisten berada pada nilai diatas 51 dB. Nilai PSNR dengan kisaran 51 ke atas termasuk dalam *high quality* dan gambar hasil penyisipan sulit pesan dibedakan oleh mata manusia.

Bebarapa citra yang dipakai untuk penelitian ini.

Tabel 2. Citra yang dipakai

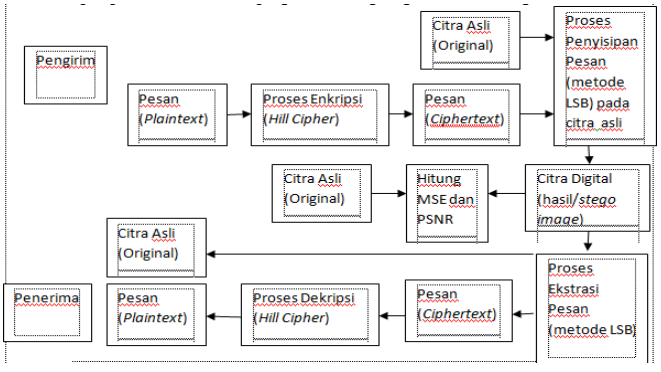
Nama citra uji	Gambar citra	Ukuran Citra	Ukuran citra (KB)
Lenna.*bmp*		252 * 252	186.1
Lada.*bmp*		225 * 225	148.588
Bunga.*bmp*		229 * 220	147.865
Tebing.*bmp*		264 * 177	147.322
Windows.*bmp*		420 * 280	344.584

Citra yang dipakai pada penelitian ini sengaja diambil yang berbeda ukuran supaya bila dilihat berapa rata-rata pixel yang mampu ditampung oleh citra tersebut.

3. HASIL DAN PEMBAHASAN

3.1 Diagram Blok Sistem

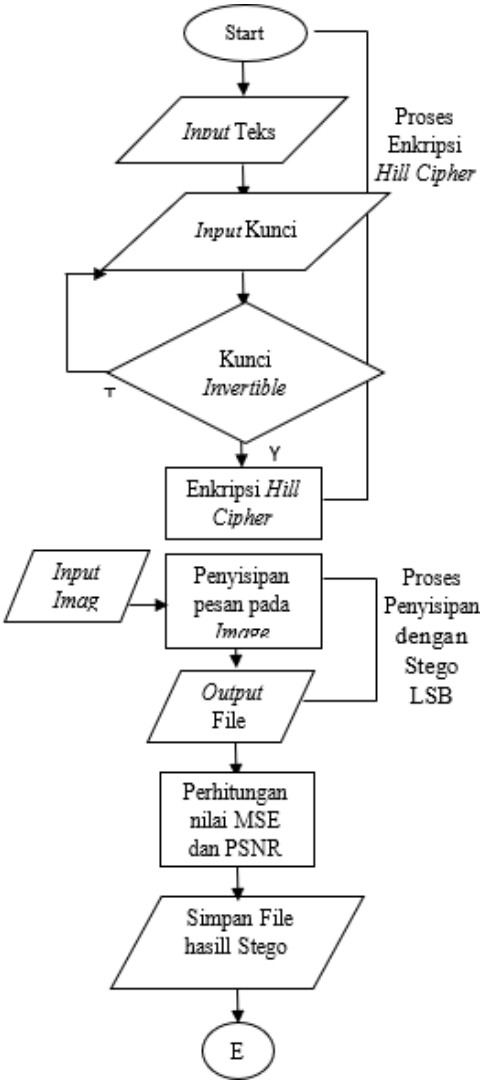
Tahapan proses kombinasi kriptografi dan steganografi adalah sebagai berikut:



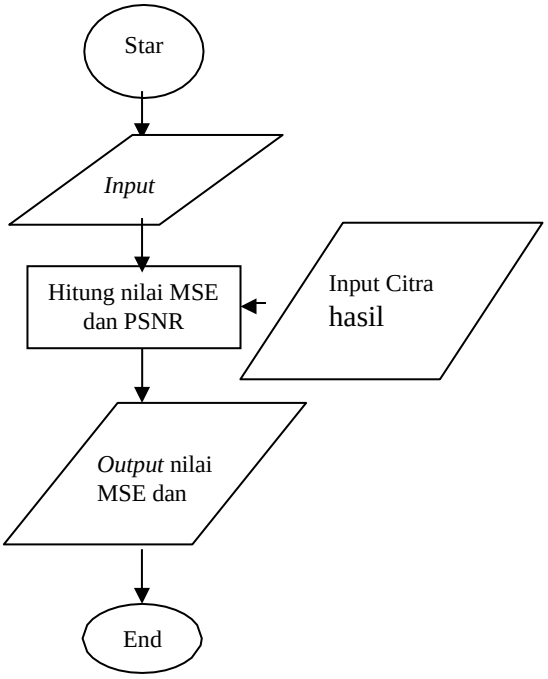
Gambar 3. Bagan Perencangan Kombinasi Kriptografi dan Steganografi

3.2 Diagram Alur (Flowchart) Aplikasi

Pada pembuatan aplikasi ini, dibutuhkan suatu teknik perancangan yang mempunyai struktur yang baik, biasanya diawali dengan pembuatan diagram alur (flowchart). Diagram alur digunakan untuk menggambarkan terlebih dahulu apa yang harus dikerjakan sebelum mulai merancang atau membuat suatu sistem. Sistem mulai bekerja dengan membaca teks yang akan diproses dengan kriptografi Hill Cipher. Setelah itu maka ditentukan kunci yang akan dipakai. Kunci ini harus diingat karena akan diminta lagi saat proses dekripsi di penerima. Setelah teks dan kuncinya dimasukan maka proses selanjutnya adalah enkripsi dengan algoritma kriptografi. Hasil enkripsi selanjutnya diteruskan ke blok steganografi. Hasil enkripsi menjadi masukan buat algoritma steganografi. Pada bagian ini mulai dilakukan proses penyisipan. Setiap karakter akan dipecah menjadi kode ASCII untuk bisa disisipkan ke dalam stegano image. Setiap bit data diisi 1 per 1 pada bit yang terakhir dari setiap pixel citra dengan teknik yang bervariasi dalam penempatan bit informasi dalam citra.



Gambar 4. *Flowchart* Untuk Proses Enkripsi dan Penyisipan

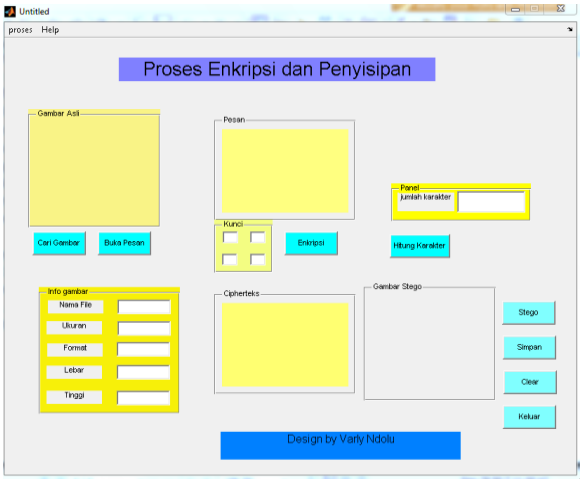


Gambar 5. *Flowchart* Untuk Proses Perhitungan MSE dan PSNR Untuk Proses Enkripsi dan Penyisipan

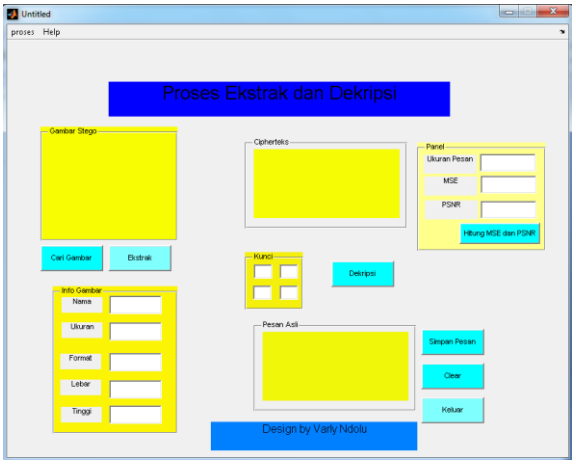
Proses selanjutnya adalah membandingkankualitas citra sebelum disisipi dan setelah dimasukan bit informasi. Pada level ini dilakukan perhitungan MSE dan PSNR. Nanti nilainyadibanding dengan standar MOS.

3.3 Desain Antar Muka

Antar muka adalah alat komunikasi antara *user* dan sistem agar sistem lebih mudah dan bisa digunakan *user*. Berikut rancangan antar muka untuk Implementasi kriptografi menggunakan metode *Hill Cipher* dan Metode steganografi LSB pada media citra digital.



Gambar 6. GUI untuk proses enkripsi



Gambar 7. GUI Untuk proses ekstrak dan Dekripsi

3.4 Hasil Pengujian

Pengujian dilakukan untuk mengetahui apakah file dapat menampung pesan teks tanpa adanya perubahan ukuran pada citra awal. Kemudian melakukan perbandingan antara ukuran media penampung dan ukuran pesan, apakah metode kriptografi *Hill Cipher* dan metode steganografi LSB masih bisa berjalan baik, jika informasi ukuran pesan teks dinaikkan.
Kemudian acuan dari pengujian dari ini dilihat dari dua aspek, yakni:

1. Membandingkan kualitas citra hasil penyisipan dengan citra awal apabila dilihat secara kasat mata.
2. pengukuran menggunakan *Peak Signal-to-Noise Ratio* (PSNR) dan *Mean Square Error* (MSE) untuk mengevaluasi perbedaan antara citra hasil penyisipan dan citra awal.

Tabel 3. Hasil pesan standar disisipkan pada citra

NO	Pesan Asli (*Plaintext*)	Kunci (*Key*)	Pesan Hasil Enkripsi (*Ciphertext*)	Pesan Hasil Ektraksi (*Ciphertext*)	Pesan Hasil Dekripsi (*Plaintext*)
1	Kriptografi *Hill Cipher*	[3 2;2 5]	'4}f>w{lQ$-ZuR, G}fd-h^	'4}f>w{lQ$-ZuR, G}fd-h^	Kriptografi *Hill Cipher*
2	Kriptografi *Hill Cipher*	[5 5;2 5]	T4fVwl($vZnRl G$fF-7^	T4fVwl($vZnRl G$fF-7^	Kriptografi *Hill Cipher*
3	Steganografi Least Significant Bit(LSB)	[6 5;5 6]	Z{')2?c[WF7:C\K]{Z?=gb7:[Y@F yB`rGNS:	Z{')2?c[WF7:C\K]{Z?=gb7:[Y@F yB`rGNS:	Steganografi Least Significant Bit(LSB)
4	Steganografi Least Significant Bit(LSB)	[3 5;1 10]	"Cu1.s5;~`$F~bGG>4#5<N$FQQs^ t"#\$jN4	"Cu1.s5;~`$F~bGG>4#5<N$FQQs^ t"#\$jN4	Steganografi Least Significant Bit(LSB)
5	TEKNIK ELEKTRO	[11 3;9 6]	,2Bu#Q X3U-S".w	,2Bu#Q X3U-S".w	TEKNIK ELEKTRO

Tabel 3 memperlihatkan bahwa pesan asli (*plaintext*) dengan pesan hasil enkripsi dan ekstrasi sangat berbeda, sehingga sulit bagi pihak lain untuk membaca. Dengan demikian maka, walaupunpihak lain telah berhasil mengekstrak pesan dengan metode LSB, namun pesan tidak langsung dapat dibaca. Demikian juga penggunaan kunci yang berbeda akan menghasilkan hasil (*ciphertext*) yang berbeda. Hal ini akan menyulitkan pihak lain untuk mengetahui pesan yang telah disisipkan.
Pengujian juga dilihat berdasarkan kriteria kualitatif dan kuantitatif. Adapun hasilnya dapat dilihat pada Tabel 4.2

Tabel 4. Kriteria kualitatif dan kuantitatif

Nama citra	Pesan teks	MSE	PSNR (db)
Lenna.*bmp*	Kriptografi *Hill Cipher*	0.000897581	78.6001
Lada.*bmp*	Steganografi Least Significant Bit (LSB)	0.00146173	76.4821
Bunga.*bmp*	TEKNIK ELEKTRO	0.000674871	79.8386
Tebing.bmp	1000 Karakter	0.000537121	80.8301
Windows.*bmp*	1000000 Karakter	0.000306122	83.2719

(a)

(b)

Gambar 8. a) citra sebelum disisipi pesan, b) citra sesudah disisipi pesan

Gambar 8 memperlihatkan kondisi imagesebelum diproses dengan kriptografi dan sreganografi dan setelah diproses. Sepintas terlihatbahwa tidak ada perbedaan yang signifikan antara kedua image. Tetapi saat dilihat secara kuantitatif maka sebenarnya ada perbedaan. Nilai MSE dan PSNR adalah 0.000306 dan 83.305 dB. Hal ini menjelaskan bahwa nilai MSE yang mendekati nol dan nilai PSNR diatas 60 dB merupakan nilai yang baik sehubungan dengan kualitas image. Seluruh pengujian yang dilakukan dengan tidak menggunakan noise.

3.5 Pengujian dengan noise pada teks standar

Adapun pengujian berikutnya dilakukan dengan penambahan *noise salt and pepper* dengan nilai 0.01

Tabel 5. Pengujian pesan teks standar dengan noise salt and pepper 0.01

NO	Pesan Asli (*Plaintext*)	Kunci (Key)	Pesan Hasil enkripsi (*Ciphertext*)	Pesan Hasil ekstrasi (*Ciphertext*)	Pesan hasil dekripsi (Plaintext)
1	Kriptografi *Hill Cipher*	[9 8;8 9]	w@[bXSYd!&5 r;>( ][bXUJ0	w@[bXSYd!&5 r;>( ][bXUJ0	Kriptografi *Hill Cipher*
2	Kriptografi *Hill Cipher*	[50 7;5 3]	Dn2B{v:>2Z4 (t6I (2Boz2'	Dn2B{v:>2Z4 (t6I (2Boz2'	Kriptografi *Hill Cipher*
3	Steganografi Least Significant Bit(LSB)	[4 9;3 13]	j:-32jU/OZ7V !RAM-r=WW@7Vq1xq c,hwI$_:	j:-32jU/OZ7V !RAM-r=WW@7Vq1xq c,hwI$_:	Steganografi Least Significant Bit(LSB)
4	Steganografi Least Significant Bit(LSB)	[15 12; 4 9]	W(kY%*E#*W4o TAaW\ ?IiN14ocyt6 L=.48[<1	W(kY%*E#*W4o TAaW\ ?IiN14ocyt6 L=.48[<1	Steganografi Least Significant Bit(LSB)
5	TEKNIK ELEKTRO	[12 9;7 8]	{r`{-U dA[94|.+	{r`{-U äAK94|.+	TEKNIK ?¡CTRO
6	TEKNIK ELEKTRO	[13 3;5 6]	4"8+sm B_?Y[p,{	4"<+sm B_?Y[p,{	TE5pIK ELEKTRO

Dari Tabel 5. terlihat bahwa pesan asli(*plaintext*) dengan pesan hasil enkripsi dan ekstrasi sangat berbeda, sehingga sulit bagi pihak lain untuk membaca. Dengan demikian maka,walaupun pihak lain telah berhasil mengekstrak pesan dengan metode LSB, namun pesan tidak langsung dibaca. Ketika ditambahkan *noise salt and pepper* dengan nilai 0.01, pesan yang terdapat dalam citra, masih dapat diambil kembali dari citra yang terkena *noise salt and pepper* tetapi pada percobaan ke 5 dan 6 terjadi perubahan informasi pada saat pesan didekripsikan kembali. Hal ini terjadi karena *noise* tersebut merusak bit terakhir yang terdapat pada citra sehingga pada saat didekripsikan, beberapa karakter mengalami kerusakan.
Nilai PSNR dan MSE diperlihatkan pada tabel 6.

Tabel 6. Kinerja sistem ketika ditambah *noise salt and pepper* dengan nilai 0.01

Nama citra	Pesan teks	MSE	PSNR (dB)
Lenna.*bmp*	Kriptografi *Hill Cipher*	1.28182	47.0525
Lada.*bmp*	Steganografi Least Significant Bit(LSB)	1.39739	46.6776
Bunga.*bmp*	TEKNIK ELEKTRO	1.03142	47.9964
Tebing.*bmp*	UNDANA	1.21292	47.2925
Windows.*bmp*	1000000 Karakter	1.21025	47.3021

a **b**

Gambar 9 a) citra sebelum disisipi pesan, b) citra sesudah disisipi pesan dan diberi noise *salt and pepper* 0.01

Gambar 9 a dan b terlihat bahwa *file image* yang telah disisipi pesan teks dan diberi *attack* dengan *noise salt and pepper*, terlihat pada gambarterdapat bintik-bintik pada gambar sehingga jika dilihat secara kualitas terjadi perbedaan yang sangat besar antara gambar yang sudah disisipidengan gambar yang diberi *noise*. Pengujian ditambah *noise* ini

terjadi penurunan jika dilihat secara kuantitatif dari nilai MSE dan PSNR terjadi penurunan yaitu MSE 2.38696 dan PSNR 77.804 dB ketika disisipi pesan dan ditambahkan *attack* MSE menjadi 1.3716 dan PSNR 44.3863 dB menjelaskan bahwa nilai dari MSE yang diatas nol dan nilai PSNR diatas 40 dB termaksud dalam kategori *reasonable*.

4. KESIMPULAN

Setelah melakukan pengujian aplikasi dengan metode kriptografi *Hill cipher* dan metode steganografi LSB, beberapa kesimpulan diperoleh sebagai berikut:

1. Pengamanan data menggunakan metode kriptografi *Hill Cipher* menghasilkan *ciphertext* dalam keadaan yang acak, sehingga informasi tersebut tidak dapat dibaca denganmudah.
2. Citra yang melalui metode steganografi LSB terlihat sama dengan citra asli sehingga sangat sulit dibedakan. Nilai MSE dan PSNR citra hasil stego terbaik didapat dengan nilai MSE 0.000306122 dan nilai PSNR 83.2719 dB. Sehingga pengujian dengan tanpa *attack*metode kriptografi *Hill Cipher* dan metode steganografi LSB berjalan baik
3. Pada saat penambahan *attack* dengan *noise salt and pepper* secara kualitatif terjadi perubahan pada citra. Nilai MSE dan PSNR terendah yakni MSE 6.32889dan PSNR 40.1175 dB. Terjadi perubahan informasi sebelumnya pada saat diekstrak dan didekripsi kembali akibat penambahan *noise* tersebut merusak bit informasi yang tersimpan pada citra stego tersebut.

DAFTAR PUSTAKA

[1] Fachrurrozi, Erwin, "Pemrosesan Citra Berwarna dan Aplikasi dengan Java, Skripsi, Universitas Sriwijaya. Palembang. Surabaya, 2016.
[2] Gunadi, Kartika, "Aplikasi Metode Steganografi pada Citra Digital dengan Menggunakan Metode LSB (Least Significant Bit). Surabaya, 2015.
[3] Hidayat, Erwin, "Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak secara Kuantitatif dan Visual. Semarang, 2013.
[4] Laskar, Shamin, "High Capacity data Hiding using LSB Steganography and encryption. International Journal Of Database Manage System Vol 4. IEEE, 2012.
[5] Kromodimoeljo, Sentot, "Teori dan Aplikasi Kriptografi, Buku Teks, Jakarta: SPK IT Consulting, 2009.
[6] Hernawati, Kuswari, "Implementasi Cipher Vigenere pada Kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler. Yogyakarta, 2014.
[7] Monica, Finna, "Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (Least Significant Bit) Visual Basic 6, Bandung, 2016.
[8] Maulana, Ahmad, "Data Hiding Steganography pada File Image Menggunakan Metode Least Significant Bit (LSB). Surabaya, 2014.
[9] Monica, Finna, "Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (Least Significant Bit) Visual Basic 6. Bandung, 2016.

.