JINACS: Volume 01 Nomor 03, 2020
(Journal of Informatics and Computer Science) ISSN : 2686-2220

Penerapan Algoritma Least Significant Bit Untuk Menyembunyikan Vigenere Cipher Text pada Citra Digital

Fino Ardiansyah Prayudi[1], Agus Prihanto[2],
[1] Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[2]Jurusan Teknik Informatika/Teknik Informatika, Universitas Negeri Surabaya
[1]finoprayudi@mhs.unesa.ac.id
[2]agusprihanto@unesa.ac.id

***Abstrak*— Pengamanan data menggunakan metode kriptografi bersifat mengacak pesan sehingga tidak mudah dimengerti, namun masih menimbulkan kecurigaan sedangkan Steganografi merupakan seni menyembunyikan informasi sehingga tidak terlihat dengan tanpa mengacak informasi tersebut. Penelitian ini bertujuan menyisipkan pesan yang dienkripsi dengan v*igenere cipher* dengan metode penyisipan 2 bit LSB (*Least Significant Bit)* pada cover gambar RGB. Hasil pengujian PSNR pada media cover gambar dengan 3 jenis yaitu: gambar background, gambar alam dan gambar rongsen dengan penyisipan data teks berukuran 10kb, 50kb, 100kb, 340kb menunjukkan bahwa PSNR pada gambar background rata-rata 51,8 persen, gambar alam rata-rata 50,6 persen, dan pada gambar rongsen rata-rata 50,7 persen, sehingga dapat disimpulkan bahwa metode 2 LSB (Least Significant Bit) yang digunakan dalam penelitian ini termasuk dalam kategori bagus atu baik karena nilai PSNR > 40 persen.**

***Kata Kunci*— Kriptografi, Steganografi, Vigenere Cipher, Least 2 LSB, RGB, PSNR.**

I. PENDAHULUAN

Pada zaman sekarang perkembangan teknologi yang semakin berkembang dengan maju memberikan dampak hampir seluruh aspek pada kehidupan manusia. Contohnya pada media komunikasi seperti telephone genggam dan laptop yang dapat terhubung di internet serta bisa mengirimkan *file* kepada setiap orang dimanapun berada. Namun pada media komunikasi yang terhubung dengan internet semuanya itu memiliki dampak positif dan negatif. Dampak positifnya ialah memudahkan untuk mengirimkan suatu *file* ke orang lain dengan cepat dan bisa mencari informasi dengan mudah. Sedangkan pada dampak negatif dari media komunikasi ialah sangatlah rawan terhadapan penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui isi dari informasi tersebut. Berbagai cara telah dilakukan untuk menjaga keamanan informasi itu menjadi factor utama ini. Maka dari itu, telah dilakukan upaya untuk mencegah penyadapan informasi dan menjaga keamanan isi pesan dari orang yang tidak berhak mengetahuinya, diantaranya teknik yang dapat digunakan yaitu dengan teknik kriptografi.

Menurut Request for Comments (RFC), kriptografi merupakan ilmu matematika yang berhubungan dengan transformasi data untuk membuat artinya tidak dapat dipahami (untuk menyembunyikan maknanya), mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. Jika transformasinya dapat dikembalikan, kriptografi juga bisa diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang dapat dipahami. Artinya, kriptografi dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas (Oppliger, 2005). Namun pada hasil enkripsi dari teknik kriptografi masih bisa dilihat dan dapat terpecahkan dengan mudah, maka dari itu orang-orang lain berfikir bagaimana caranya mengamankan pesan rahasia tetapi tidak bisa terlihat oleh orang yang tidak bersangkutan. Dengan uraian permasalahan tersebut maka salah satu upaya untuk mengamankan data yang berupa pesan teks adalah dengan melakukan penyisipan pesan teks ke dalam gambar.

II. PENELITIAN TERKAIT

Dalam melakukan enkripsi dan dekripsi,berbagai cara telah dilakukan oleh penelitian sebelumnya. Penelitian yang dilakukan oleh Taronisokhi Zebua (Zebua,Taronisokhi 2015) dengan judul "Penerapan Metode LSB-2 untuk Menyembunyikan *Ciphertext* pada Citra Digital". Dimana pada penelitian ini menggabungkan antara teknik kriptografi dengan teknik steganografi yang menggunakan metode LSB (Least Significant Bit)-2 yang dimana letak penyisipan bitnya sebelah kanan sendiri ke 7. Pada teknik ini mampu memberikan tingkat keamanan pesan rahasia yang rumit untuk dipecahkan karena keamanannya ganda yang artinya jika pesan yang disisipkan gambar dikeluarkan maka masih berbentuk sebuah cipherteks bukan plainteks. Setelah mendapatkan hasil cipherteks lalu di dekripsi dengan teknik kriptografi [1].

Penelitian yang berbeda dilakukan oleh Yudhi Ardian(Ardian, Yudhi 2013) dengan judul "Perbandingan Metode LSB,LSB+1,dan MSB Pada Steganografi Citra Digital". Dimana hasil dari teknik steganografi citra hasil dengan metode LSB(*Least Significant Bit*) gambar yang sudah disisipkan pesan tidak terlihat berbeda dengan gambar aslinya dan citra hasil dengan metode LSB (*Least Significant Bit*) +1 yang sudah disisipkan pesan tidak terlihat berbeda dengan gambar aslinya tetapi letak penyisipannya berbeda dengan metode LSB (*Least Significant Bit*) biasa. Sedangkan citra hasil dengan menggunakan metode MSB(*Most Significat Bit*) gambar

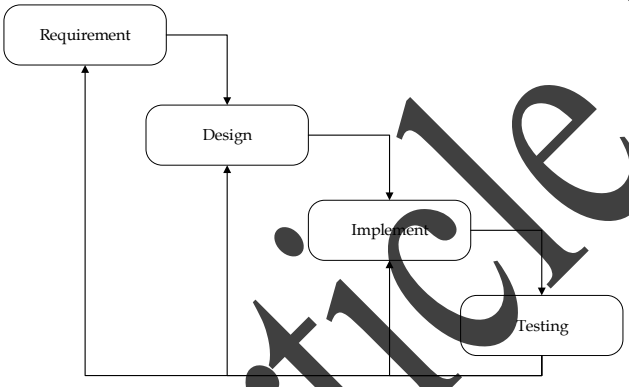
yang sudah disisipkan pesan dengan gambar aslinya terlihat sangat berbeda dan letak penyisipannya juga berbeda. [2].

Satwinder Singh dan Varinder Kaur Attri telah melakukan penelitian enkripsi dan dekripsi dengan judul "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm". Dimana hasil penelitian tersebut tidak ada yang bisa mengamati penggunaan steganografi untuk menyembunyikan data dalam gambar cover dan perubahan yang begitu minimal yang mata manusia bahkan tidak bisa melihat karena penyisipan bit pada gambar hanya sedikit. Perubahan gambar dilakukan di tingkat *pixel* yang hampir tidak terlalu mencolok yang mengarah ke keamanan yang lebih tinggi [3].

Lekso Budi Handoko,dkk telah melakukan penelitian dengan judul " Digital Signature Pada Citra Menggunakan RSA dan Vigenere Cipher berbasis MD5". Berdasarkan hasil penelitian tersebut membuktikan bahwa citra yang digunakan pada penelitian ini dapat ter-*signature* dengan baik dan tidak bisa dibaca [4].

III. METODOLOGI PENELITIAN

Berikut ini merupakan alur jalannya diagram penelitian untuk melakukan proses "Penerapan Algoritma Least Significant Bit untuk Menyembunyikan Vigenere Ciphr TextPada Citra Digital" :

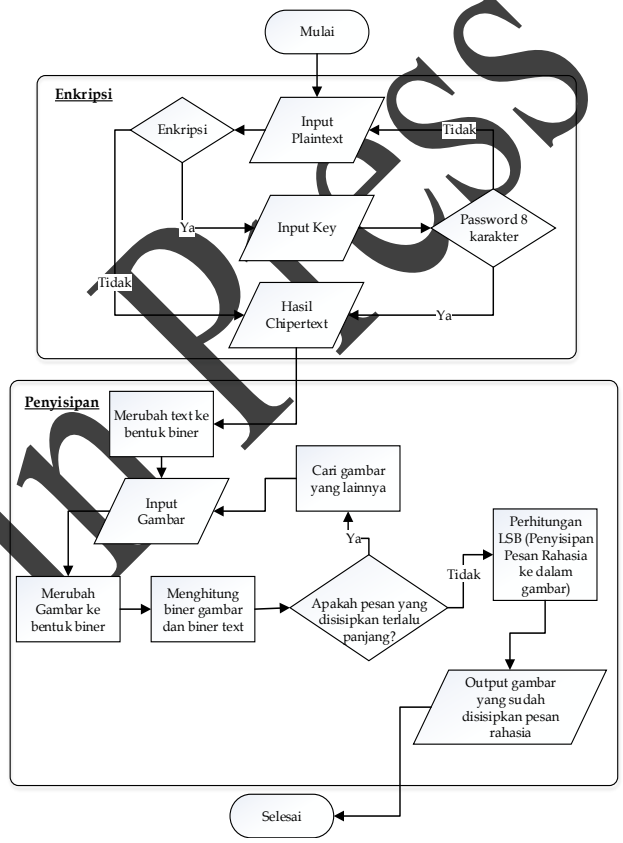


Gbr. 1 Metode Penelitian

Penelitian mengenai proses enkripsi dan dekripsi teks menggunakan algoritma Vigenere Cipher. Sedangkan untuk menyembunyikan pesan dalam gambar menggunakan 2 bit algoritma LSB (*Least Significant Bit*), maka pengujiannya meliputi PSNR(Peak Signal Noise), histogram, hasil penyisipan pesan dengan dan tanpa menggunakan kriptografi. Adapun tahapan yang dilakukan pada penelitian ini adalah sebagai berikut :

A. Proses Enkripsi dan Penyisipan Pesan dalam Gambar

Pada tahap ini merupakan sebuah alur proses dimana pesan asli atau plainteks dienkripsi menggunakan algoritma vigenere cipher agar menjadi pesan berbentuk acak (plainteks) atau tidak bisa dibaca oleh pengguna selain yang bersangkutan. Pada proses ini juga bisa bisa langsung disisipkan pesan ke dalam gambar jadi tidak melalui proses enkripsi (proses dengan menggunakan algoritma *vigenere cipher*) dan pesan asli tersebut disisipkan pada gambar dengan menggunakan algoritma 2 bit LSB (*Least Significant Bit*). Setelah proses enkripsi menghasilkan cipherteks atau pesan yang tidak bisa dibaca masuk ke dalam proses selanjutnya yaitu proses penyisipan pesan dengan menggunakan algoritma 2 bit LSB (*Least SIgnificant Bit*). Pada proses enkripsi dan penyisipan pesan dalam gambar bisa dilihat pada Gbr. 2 berikut ini :



Gbr. 2 Alur Proses Enkripsi dan Penyisipan Pesan dalam Gambar

Berikut merupakan langkah-langkah dalam proses enkripsi dan penyisipan pesan dalam gambar :

1. Masukkan gambar yang akan disisipkan pesan rahasia dengan format gambar jpg,bmp,png dan format berukuran 800 * 600 pixel.
2. Masukan *plaintext* yang mau dienkripsi atau tidak,apabila tidak dienkripsi maka langsung keluar hasilnya di kolom *ciphertext*, sedangkan kalau dienkripsi maka masukan kunci untuk mengenkripsi *plaintext* tersebut.
3. Masukan kunci minimal delapan karakter untuk enkripsi *plaintext*, jika masukan kunci kurang dari delapan karakter maka program tidak bisa berjalan atau tidak bisa keluar hasil *ciphertext*.
4. Pada proses ini diperoleh dari setiap karakter yang telah dimasukan tersebut dijadikan decimal. Setelah itu kata

kunci yang sudah dimasukan dijadikan decimal juga. Kemudian dihitung dengan rumus *ciphertext* = (*plaintext* + kunci) mod 256.

5. Pada proses ini menghasilkan sebuah *ciphertext* yang tidak bisa dibaca oleh seseorang.
6. Gambar yang sudah disimpan pada program akan ditampung ke sebuah *variable array* gambar dua dimensi.
7. Pada proses ini semuanya akan dihitung dari banyaknya nilai biner gambar dan nilai binernya *ciphertext*, apabila nilai binernya *ciphertext* lebih banyak dari nilai biner gambar maka pesan yang disisipkan pada gambar tidak bisa masuk dan akan disuruh mencari media *cover* gambar yang lainnya.
8. Perhitungan least significant bit, Pada proses ini nilai dua bit setiap biner dari karakter huruf ciphertext akan diambil dan akan disisipkan pada nilai dua bit trakhir bagian gambar. Misalkan karakter huruf ciphertext "A" akan disisipkan pada gambar :

   Ciphertext A = 01000001 dan nilai gambar sebagai berikut:

   01100000 01100000 01100000 01100000 01100000 01100000 01100000 01100000

   Akan menjadi :

   01100001 01100000 01100000 01100001 01100000 01100000 01100000 01100000
9. Hasil yang dikeluarkan dari proses perhitungan *Least Significant Bit* adalah gambar yang sama tetapi sudah disisipkan pesan rahasia.

B. Proses Pengambilan Pesan dan Dekripsi

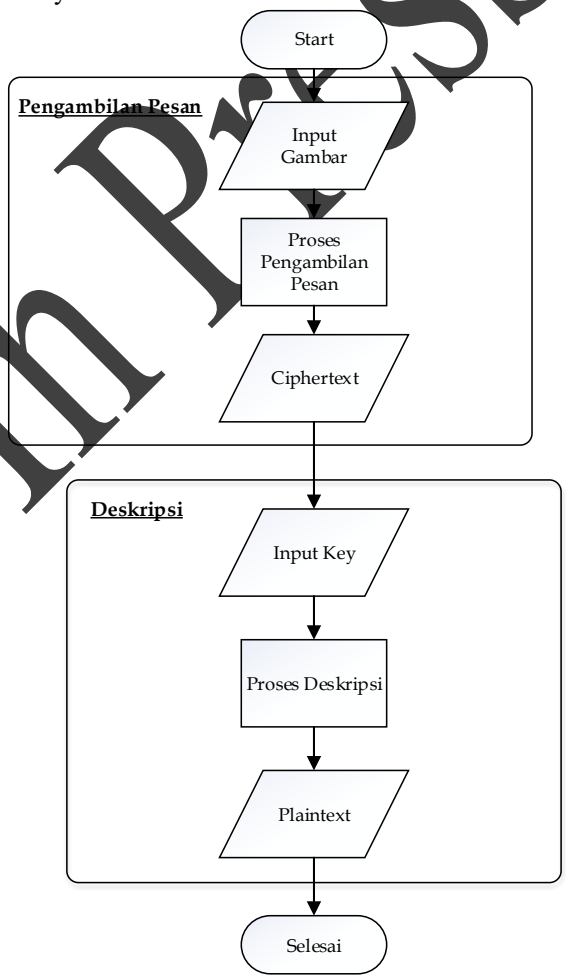
Pada tahap proses pengambilan pesan ini merupakan proses untuk mengambil pesan pada gambar yang sudah disisipkan pesan dengan menggunakan algoritma 2 bit LSB (*Least Significant Bit*). Setelah itu dilihat hasilnya, jika bentuknya plainteks tidak masuk ke dalam proses dekripsi pesan yang artinya tidak memakai proses dekripsi pesan yang menggunakan algoritma *vigenere cipher*. Tetapi jika pengeluarannya hasilnya cipherteks atau pesan yang tidak bisa dibaca(acak) maka melewati proses selanjutnya yaitu proses dekripsi pesan yang menggunakan algoritam vigenere cipher agar pesan yang tidak bisa dibaca(acak) tersebut bisa kembali seperti pesan aslinya. Bisa dilihat pada Gbr 3 sebagai berikut ini :

Berikut merupakan langkah-langkah dalam proses pengambilan pesan dalam gambar dan dekripsi pesan :

1. Masukan gambar yang sudah disisipkan gambar.
2. Pada proses ini nilai setiap dua bit terakhir pada gambar akan diambil dan setelah diambil dijadikan satu sampai jumlahnya delapan bit akan menjadi sebuah decimal. Hasil decimal tersebut akan membentuk sebuah huruf karakter sebuah pesan yang asli. Contohnya seperti dibawah ini :

   Bit yang terkandung pada gambar disisipkan pesan : 01100001 01100000 01100000 01100001 01100000 01100000 01100000 01100000

   Kemudian hasil dari dua bit terakhir diambil satu persatu sampai menjadi delapan bit,yaitu : 01000001 pada bit tersebut dijadikan decimal menjadi 65 dan dirubah menjadi huruf "A"
3. Pada proses ini hasil output dari proses pengambilan pesan yaitu huruf "A".
4. Masukan kunci yang sama seperti proses enkripsi.
5. Pada proses ini hasil *ciphertext* tadi dijadikan *decimal* dan *input* kunci tadi juga dijadikan *decimal*. Untuk mendapatkan *plaintext* membutuhkan rumus *plaintext* = (*ciphertext* – kunci) mod 256. Setelah dimasukan ke dalam rumus tersebut akan mengeluarkan pesan aslinya.



Gbr. 3 Alur Proses Pengambilan Pesan dan Dekripsi Pesan

6. Hasil dari proses dekripsi menghasilkan *plaintext* huruf karakter "a".
7. Selesai.

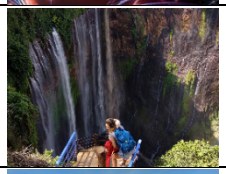
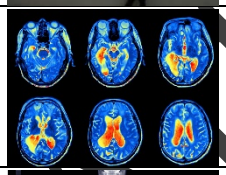
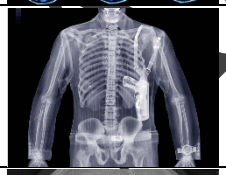
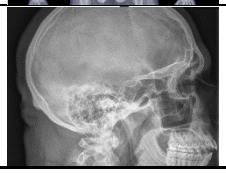
IV. HASIL DAN PEMBAHASAN

A. Data Penelitian

Pada tahap pertama dalam melakukan penelitian ini adalah penentuan dan persiapan data yang perlu diuji coba yaitu gambar yang sudah disiapkan untuk menjadi uji coba dalam proses enkripsi pesan dengan menggunakan

algoritma vigenere cipher, penyisipan pesan dalam gambar dengan menggunakan algoritma 2 bit LSB (*Least Significant Bit*), pengambilan pesan dan dekripsi dengan algoritma yang sama seperti proses enkripsi pesan dan proses penyisipan pesan dalam gambar. Pada tabel III berikut merupakan kumpulan data yang diuji coba :

TABEL I
DATA GAMBAR PENELITIAN

No.	Gambar	Dimensi File	Ukuran File
1.		800x600	223 KB
2.		800x600	556 KB
3.		800x600	269 KB
4.		800x600	999 KB
5.		800x600	893 KB
6.		800x600	265 KB
7.		800 x 600	537 KB
8.		800 x 600	354 KB
9.		800 x 600	329 KB

B. Hasil Pengujian

Dalam hal ini telah dilakukan pengujian enkripsi, penyisipan pesan pada gambar, pengambilan pesan pada gambar, dekripsi dan PSNR (Peak Signal Noise Ratio) terhadap sistem yang telah dibuat. Pengujian ini dilakukan dengan menyisipkan pesan tersembunyi dengan ukuran 10 Kb, 50 Kb, 100 Kb dan 340 Kb terhadap 3 jenis gambar yaitu computer generate, gambar foto (natural), dan foto CT-Scan. Hasil analisis dan pengujian yang diperoleh dapat dilihat berdasarkan perbandingan gambar sebelum proses penyisipan dan setelah disisipkan menggunakan algoritma *Least Significant Bit* adalah sebagai berikut :

a. *Hasil PSNR(Peak Signal Noise Ratio)*

Berdasarkan hasil pengujian yang telah dilakukan terhadap gambar dengan menggunakan pengujian pada perbandingan antara gambar asli dan gambar yang telah disisipkan pesan menggunakan pengujian PSNR (Peak Signal Noise Ratio) yang menghasilkan sebuah grafik perbandingan tersebut. PSNR (Peak Signal Noise Ratio) sering juga dinyatakan dalam skala logaritmik dalam satuan decibel (dB). Anabila nilai PSNR (Peak Signal Noise Ratio) berada dibawah 30 dB maka itu berarti perbandingan terlihat jelas berbeda dengan gambar aslinya. Akan tetapi jika kualitas dan tingkat kemiripan gambar yang tinggi maka PSNR (Peak Signal Noise Ratio) berada pada nilai 40dB dan diatasnya karena sedikit atau tidak ada perbedaan pada gambarnya. Hasil pengujian yang dilakukan pada penyisipan pesan pada gambar warna menghasilkan yang dapat ditaliskan pada Tabel II berikut ini :

TABEL II
PERBANDINGAN UKURAN GAMBAR

Jenis	File Ke	Size File Teks (Kb)			
		10	50	100	340
Computer Generate	1	59.9855 dB	52.9923 dB	49.9642 dB	44.6677 dB
	2	57.1218 dB	50.1542 dB	47.1422 dB	44.2929 dB
	3	61.8280 dB	54.8704 dB	51.7765 dB	46.3347 dB
Rata-Rata		**59,6471 dB**	**52,6723 dB**	**49,6276 dB**	**45,0984 dB**
Gambar Foto (Natural)	4	60.0173 dB	53.0346 dB	50.0269 dB	44.6869 dB
	5	52.9304 dB	50.4330 dB	48.5266 dB	44.2085 dB
	6	56.8172 dB	52.1798 dB	49.5740 dB	44.5659 dB
Rata-Rata		**56,5883 dB**	**51,8825 dB**	**49,3758 dB**	**44,4871 dB**
CT-Scan	7	59.8540 dB	53.0380 dB	49.9727 dB	44.6627 dB
	8	59.0624 dB	49.8098 dB	48.1053 dB	45.0842 dB

Jenis	File Ke	Size File Teks (Kb)			
		10	50	100	340
	9	57.1848 dB	50.1693 dB	47.1485 dB	44.3136 dB
Rata-Rata		58,7004 dB	51,0057 dB	48,4088 dB	44,6868 dB

Dari hasil Tabel II maka dapat disimpulkan bahwa hasil pengujian penyisipan pesan terhadap jenis gambar (computer generate, gambar foto (natural), ct-scan) dengan menggunakan PSNR (Peak Signal Noise Ratio) mendapatkan dengan hasil rata-rata yang diperoleh pada file teks 10 Kb, 50 Kb, 100 Kb, 340 Kb yang disisipkan pada gambar dengan menggunakan 2 bit LSB (*Least Significant Bit*), bahwa computer generate memiliki PSNR (Peak Signal Noise Ratio) lebih tinggi yang artinya memiliki kualitas yang lebih baik.

b. Hasil Penyisipan dengan Kriptografi Vigenere Cipher

Berdasarkan hasil yang dilakukan pada enkripsi dengan algoritma vigenere cipher. Jika menginputkan teks "Konveksi" dengan password "12345678" maka akan mendapatkan hasil pesan yang tidak bisa dibaca atau berbentu cipherteks yaitu "|¡¡ªš¡ª¡". Dan disisipkan pada Gbr 16 dengan menggunakan algoritma 2 bit LSB (*Least Significant Bit)* maka pesan tersebut tidak bisa terlihat.

Gbr. 4 Tampilan Gambar Penyisipan Menggunakan Kriptografi Vigenere Cipher

Demikian mengembalikan pesan dengan cara masukkan gambar yang sudah disisipkan pesan lalu ekstrak pesan menggunakan 2 bit *Least Significant Bit.* Hasil ekstrak pesan tersebut berbentuk cipherteks atau pesan yang tidak bisa dibaca yaitu "|¡¡ªš¡ª¡". Pesan cipherteks atau pesan yang masih belum bisa dibaca tersebut di enkripsi dengan menggunakan Vigenere cipher dan masukkan password yang sama seperti proses enkripsi awal pesan yaitu "12345678". Maka menghasilkan pesan plainteks atau pesan aslinya yang bisa dibaca yaitu "Konveksi".

c. Hasil Penyisipan Tanpa Menggunakan Kriptografi Vigenere Cipher

Berdasarkan hasil yang dilakukan diinputkan teks "Konveksi" dan tidak melalui proses enkripsi dengan menggunakan algoritma vigenere cipher. Maka pesan inputan "Konveksi" langsung disisipkan pada Gbr 17 dengan menggunakan algoritma 2 bit LSB (*Least Significant Bit)* maka pesan tersebut tidak bisa terlihat.

Gbr. 5 Tampilan Gambar Penyisipan Tanpa Menggunakan Kriptografi Vigenere Cipher

Demikian mengembalikan pesan dengan cara memasukkan gambar yang sudah disisipkan pesan lalu ekstrak pesan menggunakan 2 bit *Least Significant Bit.* Maka menghasilkan pesan plainteks yang bisa terbaca langsung yaitu "Konveksi".

V. KESIMPULAN

Berdasarkan hasil uji coba yang telah dilakukan mengenai penyembunyian *vigenere cipher text* pada citra digital dengan menggunakan algoritma *Least Significant Bit*, kesimpulan yang diperoleh dari seluruh proses dan hasil pembahasan penelitian yang telah dilakukan adalah sebagai berikut :

1. Hasil pengujian pengaruh besarnya terhadap hasil steganografi pada jenis gambar (computer generate, gambar foto (natural), ct-scan) dengan menggunakan PSNR mendapatkan hasil dengan rata-rata yang diperoleh pada file teks 10 Kb, 50 Kb, 100 Kb, 340 Kb yang disisipkan pada gambar, bahwa computer generate memiliki PSNR lebih tinggi yang artinya memiliki kualitas yang lebih baik dari pada jenis gambar foto(natural) dan ct-scan. Sedangkan hasil pengujian histogram bahwa semakin besarnya pesan yang disisipkan pada gambar RGB maka semakin terlihat perbedaan grafik gambar asli dengan gambar yang sudah disisipkan pesan.

2. Hasil pengujian ekstraksi pesan dalam gambar tanpa menggunakan kriptografi *Vigenere Cipher* menghasilkan pesan plainteksnya. Sedangkan hasil pengujian ektraksi pesan dalam gambar menggunakan kriptografi *Vigenere Cipher* menghasilkan cipherteks

sehingga membutuhkan tambahan ektraksi lagi untuk mendapatkan plainteks.

VI. UCAPAN TERIMA KASIH

Puji syukur serta rasa terima kasih saya haturkan kepada Allah SWT yang selalu memberi kemudahan dan kelancaran dalam mengerjakan jurnal ini tanpa halangan. Semua pihak yang terkait dan senantiasa memberikan saran serta memberikan semangat sehingga jurnal ini dapat terselesaikan dengan baik.

REFERENSI

[1] R. Munir, Kriptografi, Bandung: Informatika Bandung, 2006, pp. 1-5.

[2] Arubusman, "Sejarah, Prinsip Kerja dan Teknik Steganografi," 29 September 2007. [Online]. Available: http://www.kajianpustaka.com/2017/09/sejarah-prinsip-kerja-teknik-steganografi.html.

[3] Kromodimoeljo, "Bab 2 Tinjauan Pustaka," repository.usu.ac.id, 2010.

[4] Johnson, "Bab2 Landasan Teori," 1995.

[5] Basuki, *Bab 2 Landasan Teori,* 2005.

[6] Kulkarni, *Bab 2 Landasan Teori,* 2001.

[7] B. Pranoto, "Bab 2 Landasan Teori," library.binus.ac.id, Jakarta, 2011.

[8] A. Solichin, "Mengukur Kualitas Citra Hasil Steganografi," 16 April 2015.